

	DIN EN 61508-1 (VDE 0803-1)	
	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

Einsprüche bis 2009-08-31
Vorgesehen als Ersatz für
DIN EN 61508-1
(VDE 0803-1):2002-11
Ersatz für
E DIN IEC 61508-1
(VDE 0803-1):2006-07

Entwurf

Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 1: Allgemeine Anforderungen (IEC 65A/522/CDV:2008); Deutsche Fassung FprEN 61508-1:2008

Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements (IEC 65A/522/CDV:2008); German version FprEN 61508-1:2008

Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 1: Prescriptions générales (CEI 65A/522/CDV:2008); Version allemande FprEN 61508-1:2008

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 122 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 61508-1:2008 „Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 1: Allgemeine Anforderungen“ (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/522/CDV:2008 „Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements“ unverändert in den Entwurf FprEN 61508-1:2008 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 61508-1 (VDE 0803-1):2002-11 wurden folgende Änderungen vorgenommen:

- a) Hinweis auf erforderliche IT-Sicherheit zum Erreichen der funktionalen Sicherheit Rahmen der Gefährdungs- und Risikoanalyse;
- b) Anhang B „competence of persons“ wurde mit Änderungen in den Abschnitt 6 „Management der funktionalen Sicherheit“ verschoben;
- c) Ersatz von „Sicherheitsbezogenes System anderer Technologie“ und „externe Einrichtung zur Risikominderung“ durch „andere risikoreduzierende Maßnahmen“;
- d) Definition des Ausfallgrenzwertes verbessert (7.6.2.9);
- e) Behandlung der „Spezifikation der Sicherheitsanforderungen des E/E/PE-Systems“ (Abschnitt 7.10) im Teil 1 anstatt im Teil 2;
- f) Ausschluss von Medizingeräten (IEC 60601) im Anwendungsbereich (gilt für die Teile 1 bis 3).

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
–	ISO/IEC Guide 51: 1999	–	–
–	IEC Guide 104:1997	–	–
FprEN61508-2:2008	65A/523/CDV:2008	E DIN EN 61805-2 (VDE 0803-2) in Vorbereitung	(VDE 0803-2)
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/TS 61000-1-2:2008	–	–
–	ISO/IEC 13335-1:2004	DIN ISO/IEC 13335-1:2006	–
–	ISO/IEC TR 13335-3:1998 zurückgezogen	–	–
–	ISO/IEC TR 13335-4:2000 zurückgezogen	–	–
–	ISO/IEC TR 13335-5:2001	–	–
–	ISO/IEC TR 19791:2006	–	–
–	ISO/IEC 15408-1:2007	DIN ISO/IEC 15408-1:2007	–
–	ISO/IEC 15408-2:2007	DIN ISO/IEC 15408-2:2007	–
–	ISO/IEC 15408-3:2007	DIN ISO/IEC 15408-3:2007	–

Tabelle NA.1 (fortgesetzt)

Europäische Norm	Internationale Norm	Deutsche Norm	Klassifikation im VDE-Vorschriftenwerk
–	ISO/IEC 17799 Technical Corrigendum 1:2007	–	–
–	IEC 62443 IEC 65/360/NP + IEC 65/366A/RVN	–	–

Nationaler Anhang NB (informativ)

Literaturhinweise

E DIN EN 61805-2 (VDE 0803-2), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 2: Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische*

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*

DIN ISO/IEC 13335-1:2004, *Informationstechnik – Sicherheitsverfahren – Management von Sicherheit in der Informations- und Kommunikationstechnik (IuK) – Teil 1: Konzepte und Modelle für IuK-Sicherheit (ISO/IEC 13335-1:2004, Text Englisch)*

DIN ISO/IEC 15408-1, *Informationstechnik – IT-Sicherheitsverfahren – Evaluationskriterien für IT-Sicherheit - Teil 1: Einführung und allgemeines Modell; Text Englisch*

DIN ISO/IEC 15408-2, *Informationstechnik – IT-Sicherheitsverfahren – Evaluationskriterien für IT-Sicherheit - Teil 2: Funktionale Sicherheitsanforderungen; Text Englisch*

DIN ISO/IEC 15408-3, *Informationstechnik – IT-Sicherheitsverfahren – Evaluationskriterien für IT-Sicherheit - Teil 3: Anforderungen an die Vertrauenswürdigkeit; Text Englisch*

Deutsche Fassung

Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer
Systeme –
Teil 1: Allgemeine Anforderungen

Inhalt

	Seite
Einleitung	3
1 Anwendungsbereich	5
2 Normative Verweisungen	8
3 Begriffe und Abkürzungen	8
4 Übereinstimmung mit dieser Norm	9
5 Dokumentation	9
5.1 Ziele	9
5.2 Anforderungen	9
6 Management der funktionalen Sicherheit	11
6.1 Ziele	11
6.2 Anforderungen	11
7 Anforderungen zum Gesamt-Sicherheitslebenszyklus	14
7.1 Allgemeines	14
7.2 Konzept	25
7.3 Definition des gesamten Anwendungsbereiches	25
7.4 Gefährdungs- und Risikoanalyse	26
7.5 Anforderungen zur Gesamtsicherheit	28
7.6 Zuordnung der Anforderungen an die Gesamtsicherheit	31
7.7 Planung des Gesamtbetriebs und der gesamten Instandhaltung	36
7.8 Planung der Gesamtvalidierung der Sicherheit	38
7.9 Planung der Gesamtinstallation und Gesamtinbetriebnahme	39
7.10 Spezifikation der Sicherheitsanforderungen des E/E/PE-Systems	40
7.11 Sicherheitsbezogene E/E/PE-Systeme: Realisierung	42
7.12 Andere risikomindernde Maßnahmen: Spezifikation und Realisierung	43
7.13 Gesamtinstallation und Gesamtinbetriebnahme	43
7.14 Gesamtvalidierung der Sicherheit	44
7.15 Gesamtbetrieb, gesamte Instandhaltung und Reparatur	44
7.16 Gesamtmodifikation und gesamte Nachrüstung	48
7.17 Außerbetriebnahme oder Ausmusterung	50
7.18 Verifikation	52
8 Beurteilung der funktionalen Sicherheit	52

	Seite
8.1 Ziel	52
8.2 Anforderungen	53
Anhang A (informativ) Beispiel einer Dokumentationsstruktur	57
A.1 Allgemeines	57
A.2 Dokumentenstruktur des Sicherheitslebenszyklus	58
A.3 Physikalische Dokumentenstruktur.....	61
A.4 Liste der Dokumente.....	62
Literaturhinweise	63
Bilder	
Bild 1 – Gesamtrahmen dieser Norm.....	7
Bild 2 – Gesamt-Sicherheitslebenszyklus.....	15
Bild 3 – Sicherheitslebenszyklus des E/E/PE-Systems (in der Realisierungsphase).....	16
Bild 4 – Software-Sicherheitslebenszyklus (in der Realisierungsphase).....	17
Bild 5 – Verhältnis des Gesamt-Sicherheitslebenszyklus zu dem Sicherheitslebenszyklus des E/E/PE-Systems und dem Software-Sicherheitslebenszyklus	17
Bild 6 – Zuordnung der Anforderungen an die Gesamtsicherheit an die sicherheitsbezogenen E/E/PE-Systeme und anderen risikomindernden Maßnahmen.....	33
Bild 7 – Beispiel eines Modells der Betriebs- und Instandhaltungstätigkeiten.....	47
Bild 8 – Beispiel eines Modells des Betriebs- und Instandhaltungsmanagements.....	48
Bild 9 – Beispiel eines Modells eines Modifikationsverfahrens.....	50
Bild A.1 – Strukturierung von Informationen für Anwendergruppen in Sätze von Dokumenten.....	62
Tabellen	
Tabelle 1 – Gesamt-Sicherheitslebenszyklus: Übersicht.....	18
Tabelle 2 – Sicherheits-Integritätslevel: Ausfallgrenzwerte für eine Sicherheitsfunktion, die in der Betriebsart mit niedriger Anforderungsrate betrieben wird.....	34
Tabelle 3 – Sicherheits-Integritätslevel: Ausfallgrenzwerte für eine Sicherheitsfunktion, die in der Betriebsart mit hoher Anforderungsrate oder in der Betriebsart mit kontinuierlicher Anforderung betrieben wird	34
Tabelle 4 – Minimale Unabhängigkeitsgrade der Personen, welche die Beurteilung der funktionalen Sicherheit ausführen (Phasen 1 bis 8 und 12 bis einschließlich 16 des Gesamt- Sicherheitslebenszyklus (siehe Bild 2))	56
Tabelle 5 – Minimale Unabhängigkeitsgrade der Personen, welche die Beurteilung der funktionalen Sicherheit ausführen (Phasen 9 und 10 des Gesamt-Sicherheitslebenszyklus einschließlich aller Phasen des Sicherheitslebenszyklus des E/E/PE-Systems und des Software- Sicherheitslebenszyklus (siehe Bilder 2, 3 und 4)).....	56
Tabelle A.1 – Beispiel einer Dokumentationsstruktur für Informationen bezüglich des Gesamt- Sicherheitslebenszyklus	58
Tabelle A.2 – Beispiel einer Dokumentationsstruktur für Informationen bezüglich des Sicherheitslebenszyklus des E/E/PE-Systems.....	59
Tabelle A.3 – Beispiel einer Dokumentationsstruktur für Informationen bezüglich des Software- Sicherheitslebenszyklus	60

Einleitung

Systeme, die aus elektrischen und/oder elektronischen Bauteilen bestehen, werden seit vielen Jahren verwendet, um Sicherheitsfunktionen in vielen Anwendungsbereichen auszuführen. Auf Rechnern basierende Systeme (allgemein ausgedrückt programmierbare elektronische Systeme) 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 die Sicherheitsintegrität 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 Diese Internationale Norm behandelt diejenigen Gesichtspunkte, die zu betrachten sind, wenn elektrische/elektronische/programmierbare elektronische (E/E/PE) Systeme zur Ausführung von Sicherheitsfunktionen eingesetzt werden. Ein Hauptziel dieser Norm ist die Entwicklung anwendungsspezifischer internationaler Normen durch die für ein Anwendungsgebiet verantwortlichen Technischen Komitees zu unterstützen. Dies wird es erlauben, alle wichtigen Einflussgrößen dieses Anwendungsgebietes vollständig zu berücksichtigen und damit dessen besonderen Erfordernissen nachzukommen. Ein zweites Ziel dieser Norm ist es, die Entwicklung sicherheitsbezogener E/E/PE-Systeme zu ermöglichen, für die keine anwendungsspezifischen internationalen Normen bestehen.

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

1.2 Insbesondere:

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

ANMERKUNG 1 Für einfache sicherheitsbezogene E/E/PE-Systeme können bestimmte, in dieser Norm festgelegte Anforderungen unnötig sein, und eine Befreiung von der Normerfüllung in Bezug auf solche Anforderungen ist möglich (siehe 4.2 und Definition eines einfachen sicherheitsbezogenen E/E/PE-Systems in 3.4.4 der IEC 61508-4).

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

- b) ist diese Norm allgemein gültig und auf alle sicherheitsbezogenen E/E/PE-Systeme, unabhängig von der Anwendung, anwendbar;
- c) behandelt diese Norm das Erreichen eines tolerierbaren Risikos durch Anwendung sicherheitsbezogener E/E/PE-Systeme, aber sie behandelt nicht Gefährdungen, die von der E/E/PE-Einrichtung selbst ausgehen (zum Beispiel elektrischer Schlag);
- d) gilt diese Norm für alle Typen sicherheitsbezogener E/E/PE-Systeme, einschließlich Schutzsysteme und Leit- oder Steuerungssysteme,
- e) behandelt diese Norm nicht E/E/PE-Systeme, bei denen:
- ein einzelnes E/E/PE-System allein fähig ist, das tolerierbare Risiko zu erreichen; und
 - die erforderliche Sicherheitsintegrität der Sicherheitsfunktionen des einzelnen E/E/PE-Systems geringer als die Sicherheitsintegrität ist, die für den Sicherheits-Integritätslevel 1 (dem geringsten Sicherheits-Integritätslevel in dieser Norm) festgelegt ist;
- f) befasst sich diese Norm hauptsächlich mit den sicherheitsbezogenen E/E/PE-Systemen, deren Ausfall einen Einfluss auf die Sicherheit von Personen und/oder die Sicherheit der Umwelt haben könnte – es ist jedoch bekannt, dass die Auswirkungen von Ausfällen auch ernsthafte wirtschaftliche Auswirkungen haben können. In solchen Fällen kann diese Norm verwendet werden, um ein beliebiges E/E/PE-System, das zum Schutz von Einrichtungen oder Produkten verwendet wird, festzulegen;

ANMERKUNG 3 Siehe 3.1.1 der IEC 61508-4.

- g) betrachtet diese Norm sicherheitsbezogene E/E/PE-Systeme und andere risikomindernde Maßnahmen, damit die Spezifikation der Sicherheitsanforderungen für die sicherheitsbezogenen E/E/PE-Systeme in einer systematischen, risikoorientierten Art und Weise festgelegt werden kann;
- h) verwendet diese Norm als technischen Rahmen das Modell eines Gesamt-Sicherheitslebenszyklus, um diejenigen Tätigkeiten systematisch zu behandeln, die für die Sicherstellung der funktionalen Sicherheit der sicherheitsbezogenen E/E/PE-Systeme notwendig sind;

ANMERKUNG 4 Die frühen Phasen des Gesamt-Sicherheitslebenszyklus betrachten notwendigerweise auch andere risikomindernde Maßnahmen (wie auch die sicherheitsbezogenen E/E/PE-Systeme), damit die Spezifikation der Sicherheitsanforderungen für die sicherheitsbezogenen E/E/PE-Systeme in einer systematischen, risikoorientierten Art und Weise entwickelt werden kann.

ANMERKUNG 5 Obwohl der Gesamt-Sicherheitslebenszyklus vornehmlich mit sicherheitsbezogenen E/E/PE-Systemen befasst ist, kann er auch einen technischen Rahmen für die Betrachtung eines beliebigen sicherheitsbezogenen Systems liefern, ungeachtet der Technologie dieses Systems (zum Beispiel Mechanik, Hydraulik oder Pneumatik).

- i) legt diese Norm nicht die Sicherheits-Integritätslevel für spezifische Anwendungen (welche sich auf ausführliche Informationen und Kenntnis über die spezifische Anwendung stützen müssen) fest. Die für die spezifischen Anwendungen verantwortlichen technischen Komitees müssen, wenn dies angebracht ist, die Sicherheits-Integritätslevel in anwendungsspezifischen Normen festlegen;
- j) liefert diese Norm allgemeine Anforderungen für sicherheitsbezogene E/E/PE-Systeme, für die keine anwendungsspezifischen Normen vorhanden sind;
- k) enthält diese Norm nicht die Vorsichtsmaßnahmen, die notwendig sein können, um zu verhindern, dass unberechtigte Personen die funktionale Sicherheit von sicherheitsbezogenen E/E/PE-Systemen schädigen und/oder anderweitig ungünstig beeinflussen;
- l) fordert diese Norm, dass boshafte und nicht autorisierte Handlungen während der Gefährdungs- und Risikoanalyse zu betrachten sind. Der Anwendungsbereich der Analyse schließt alle relevanten Phasen des Sicherheitslebenszyklus ein.

ANMERKUNG 6 Andere IEC/ISO-Normen betrachten dieses Thema gründlich, siehe ISO/IEC 13335, ISO/IEC TR 19791, IEC 62443.

- m) legt diese Norm keine Anforderungen zur Entwicklung, Ausführung, Pflege und/oder Anwendung von IT-Sicherheitsregeln oder IT-Sicherheitsdiensten fest, die benötigt werden, um eine IT-Sicherheitsregel zu erfüllen, die von dem sicherheitsbezogenen E/E/PE-System gefordert sein könnte,

ANMERKUNG 7 Andere IEC/ISO-Normen betrachten dieses Thema gründlich, siehe ISO/IEC 13335, ISO/IEC TR 19791, IEC 62443. [Die Referenzierung solcher Normen hat in Übereinstimmung mit IEC/ISO-Regeln zu erfolgen.]

- n) trifft diese Norm nicht auf medizinische Einrichtungen gemäß der Normenreihe IEC 60601 zu.

1.3 Dieser Teil der IEC 61508 beinhaltet die allgemeinen Anforderungen, die auf alle Teile anwendbar sind. Andere Teile der IEC 61508 konzentrieren sich mehr auf spezifische Themen:

- die Teile 2 und 3 enthalten zusätzliche und besondere Anforderungen für sicherheitsbezogene E/E/PE-Systeme (für Hardware und Software);
- Teil 4 enthält Begriffe und Abkürzungen, die in der ganzen Norm verwendet werden;
- Teil 5 liefert anhand von Beispielen Hinweise für die Anwendung von Teil 1 zur Festlegung von Sicherheits-Integritätsleveln;
- Teil 6 liefert Hinweise für die Anwendung der Teile 2 und 3;
- Teil 7 enthält einen Überblick über Verfahren und Maßnahmen.

1.4 Die Teile 1, 2, 3 und 4 dieser Norm sind Sicherheits-Grundnormen, dieser Status ist aber im Zusammenhang mit einfachen sicherheitsbezogenen E/E/PE-Systemen nicht anwendbar (siehe 3.4.4 von Teil 4). Als Sicherheits-Grundnormen sind sie zur Verwendung durch technische Komitees bei der Erstellung von Normen gemäß den in *IEC Guide 104* und *ISO/IEC Guide 51* enthaltenen Grundsätzen vorgesehen. Die Teile 1, 2, 3 und 4 sind ebenfalls zur Verwendung als eigenständige Veröffentlichungen vorgesehen. Die horizontale Sicherheitsfunktion dieser internationalen Norm trifft nicht auf medizinische Einrichtungen gemäß der Normenreihe IEC 60601 zu.

ANMERKUNG 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.

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

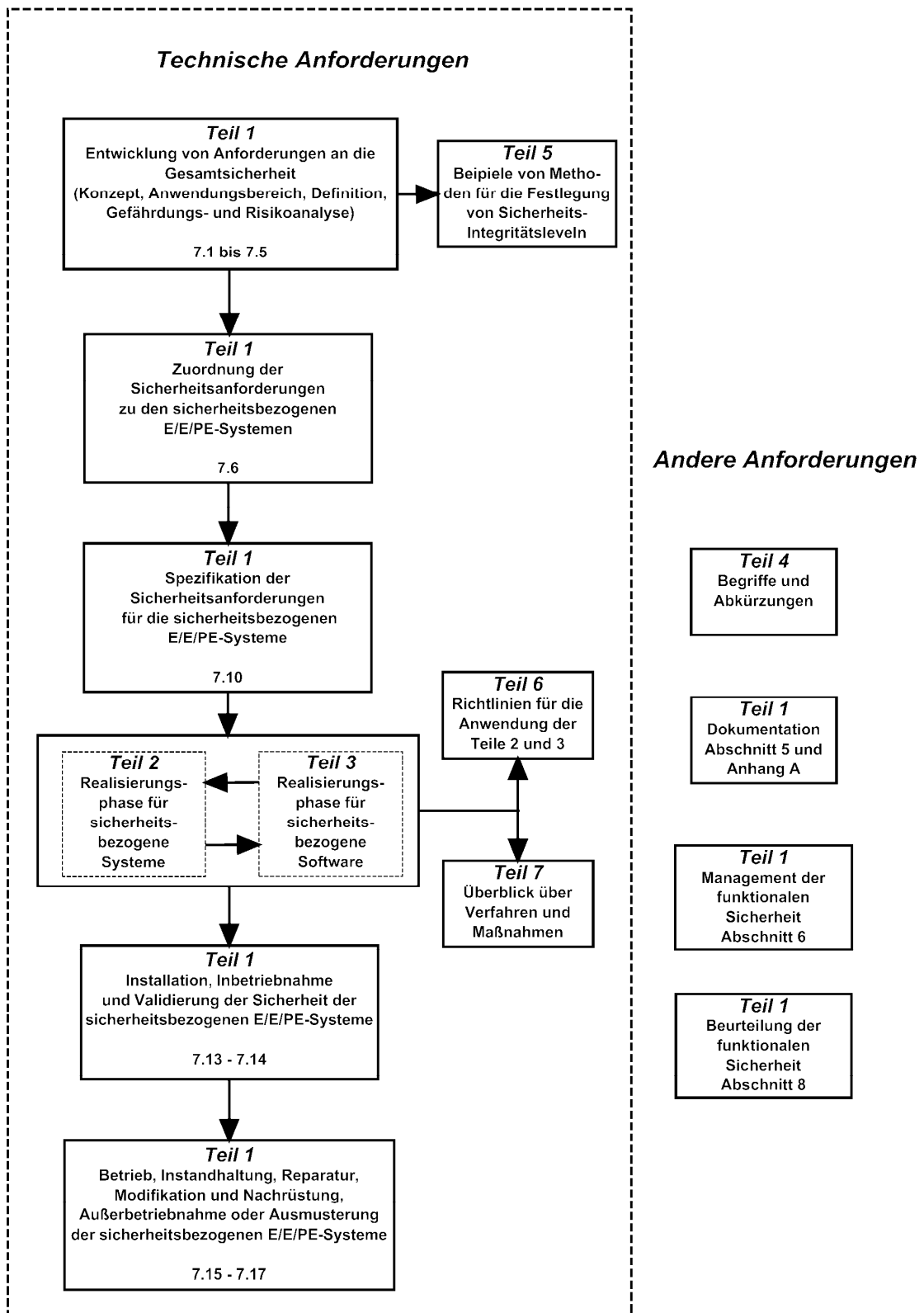


Bild 1 – Gesamtrahmen dieser Norm

2 Normative Verweisungen

Die folgenden 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).

ISO/IEC Guide 51:1999, *Safety aspects – Guidelines for their inclusion in standards*

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

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

IEC 61508-3:—, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements*¹⁾

IEC 61508-4:—, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations*¹⁾

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

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*

ISO/IEC 13335-1:2004, *Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management*

ISO/IEC TR 13335-3:1998, *Information technology – Guidelines for the management of IT Security – Part 3: Techniques for the management of IT Security*

ISO/IEC TR 13335-4:2000, *Information technology – Guidelines for the management of IT Security – Part 4: Selection of safeguards*

ISO/IEC TR 13335-5:2001, *Information technology – Guidelines for the management of IT Security – Part 5: Management guidance on network security*

ISO/IEC TR 19791, *Information technology- Security techniques-security assessment of operational systems*

ISO/IEC 15408, Teil 1 bis 3, *Information technology - Security techniques - Evaluation criteria for IT security*

ISO/IEC 17799, *Information technology - Security techniques - Code of practice for information security management*

IEC 62443: *Security for industrial process measurement and control - Network and system security* (65/360/NP und 65/366A/RVN)

3 Begriffe und Abkürzungen

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

¹⁾ Noch zu veröffentlichen.

4 Übereinstimmung mit dieser Norm

4.1 Um Übereinstimmung mit dieser Norm zu erreichen, muss dargelegt werden, dass die Anforderungen entsprechend den erforderlichen festgelegten Kriterien (zum Beispiel der Sicherheits-Integritätslevel) erfüllt worden sind, und somit die Ziele jedes Abschnitts oder Unterabschnitts erreicht worden sind.

4.2 Diese Norm legt die Anforderungen für sicherheitsbezogene E/E/PE-Systeme fest und ist erstellt worden, um den gesamten Komplexitätsbereich, der mit solchen Systemen verbunden ist, zu umfassen. Für einfache sicherheitsbezogene E/E/PE-Systeme (siehe 3.4.4 der IEC 61508-4), für die verlässliche Felderfahrungen vorliegen, die das notwendige Vertrauen ergeben, dass die erforderliche Sicherheitsintegrität erreicht werden kann, sind jedoch die folgenden Alternativen vorhanden:

- in anwendungsspezifischen Normen, welche die Anforderungen von IEC 61508-1 bis IEC 61508-7 umsetzen, können bestimmte Anforderungen unnötig sein, und eine Befreiung von der Normerfüllung in Bezug auf solche Anforderungen ist akzeptabel;
- wird diese Norm in solchen Situationen, in denen keine anwendungsspezifische internationale Norm vorhanden ist, direkt angewendet, so können bestimmte in dieser Norm festgelegte Anforderungen unnötig sein, und eine Befreiung von der Normerfüllung in Bezug auf solche Anforderungen ist akzeptabel, vorausgesetzt, dass dies begründet ist.

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

4.3 Anwendungsspezifische internationale Normen für sicherheitsbezogene E/E/PE-Systeme, die innerhalb des Rahmens dieser Norm entwickelt werden, müssen die Anforderungen von ISO/IEC Guide 51 und IEC Guide 104 berücksichtigen.

5 Dokumentation

5.1 Ziele

5.1.1 Das erste Ziel der Anforderungen dieses Abschnitts ist es, die notwendigen Informationen festzulegen, die dokumentiert werden müssen, damit alle Phasen des Gesamt-Sicherheitslebenszyklus, des Sicherheitslebenszyklus des E/E/PE-Systems und des Software-Sicherheitslebenszyklus wirkungsvoll ausgeführt werden können.

5.1.2 Das zweite Ziel der Anforderungen dieses Abschnitts ist es, die zu dokumentierenden Informationen festzulegen, damit das Management der funktionalen Sicherheit (siehe Abschnitt 6), die Verifikation (siehe 7.18) und die Beurteilung der funktionalen Sicherheit (siehe Abschnitt 8) wirkungsvoll ausgeführt werden können.

ANMERKUNG 1 In dieser Norm befassen sich Anforderungen zur Dokumentation im Wesentlichen mit Informationen und nicht mit deren Gestalt und Aussehen. Die Informationen müssen nicht in physikalischen Dokumenten vorhanden sein, es sei denn, dass dies ausdrücklich in dem entsprechenden Unterabschnitt erwähnt wird.

ANMERKUNG 2 Dokumentation kann in verschiedenen Formen vorhanden sein (zum Beispiel auf Papier, Film oder jedem Datenmedium, das auf Bildschirmen oder Anzeigeeinrichtungen dargestellt werden kann).

ANMERKUNG 3 Siehe Anhang A bezüglich möglicher Dokumentationsstrukturen.

ANMERKUNG 4 Siehe Hinweis [7] in den Literaturhinweisen.

5.2 Anforderungen

5.2.1 Die Dokumentation muss hinreichende Informationen zu jeder abgeschlossenen Phase des Gesamt-Sicherheitslebenszyklus, des Sicherheitslebenszyklus des E/E/PE-Systems und des Software-

Sicherheitslebenszyklus enthalten, welche für eine wirkungsvolle Erfüllung nachfolgender Phasen und Verifikationstätigkeiten notwendig sind.

ANMERKUNG Der Umfang ausreichender Informationen hängt von einer Anzahl von Faktoren ab, welche die Komplexität, den Umfang von sicherheitsbezogenen E/E/PE-Systemen und die Anforderungen bezüglich der speziellen Anwendung einschließen.

5.2.2 Die Dokumentation muss hinreichende Informationen, die für das Management der funktionalen Sicherheit (Abschnitt 6) erforderlich sind, enthalten.

ANMERKUNG Siehe Anmerkungen zu 5.1.2.

5.2.3 Die Dokumentation muss hinreichende Informationen, die für die Ausführung einer Beurteilung der funktionalen Sicherheit erforderlich sind, enthalten, zusammen mit den Informationen und den Ergebnissen, die aus jeder Beurteilung der funktionalen Sicherheit abgeleitet wurden.

ANMERKUNG Siehe Anmerkungen zu 5.1.2.

5.2.4 Wenn nicht in der Planung der funktionalen Sicherheit begründet oder in anwendungsspezifischen Normen festgelegt, müssen die Informationen, die dokumentiert werden müssen, so sein, wie es in den verschiedenen Abschnitten dieser Norm festgelegt ist.

5.2.5 Die Verfügbarkeit der Dokumentation muss für die Aufgaben, die im Hinblick auf die Abschnitte dieser Norm ausgeführt werden müssen, ausreichend sein.

ANMERKUNG Jede betroffene Partei braucht nur die Informationen zu besitzen, die notwendig sind, um eine besondere, nach dieser Norm erforderliche Tätigkeit auszuführen.

5.2.6 Die Dokumentation muss:

- genau und knapp sein;
- von denjenigen Personen, die sie verwenden müssen, einfach zu verstehen zu sein;
- den Zweck erfüllen, wofür sie erstellt worden ist;
- verfügbar und pflegbar sein.

5.2.7 Die Dokumentation oder der Informationssatz muss Titel oder Namen haben, die auf den Anwendungsbereich des Inhalts hinweisen, und eine Art von Registereinteilung, die einen sofortigen Zugriff auf die nach dieser Norm erforderlichen Informationen erlaubt.

5.2.8 Die Struktur der Dokumentation darf firmeneigene Verfahren und die Arbeitspraxis von speziellen Anwendungsbereichen berücksichtigen.

5.2.9 Die Dokumentation oder der Informationssatz muss einen Revisionsindex (Versionsnummern) haben, um die Identifizierung der verschiedenen Versionen eines Dokuments zu ermöglichen.

5.2.10 Die Dokumentation oder der Informationssatz muss entsprechend gegliedert werden, um die Suche nach relevanten Informationen zu ermöglichen. Es muss möglich sein, die letzte Revision (Version) eines Dokuments oder Informationssatzes zu identifizieren.

ANMERKUNG Die physikalische Struktur der Dokumentation kann aufgrund mehrerer Faktoren variieren, wie zum Beispiel des Umfangs eines Systems, seiner Komplexität und organisatorischer Anforderungen.

5.2.11 Alle relevanten Dokumente müssen unter einem angemessenen System der Dokumentenlenkung überarbeitet, geändert, überprüft und genehmigt werden.

ANMERKUNG Werden automatische oder halbautomatische Werkzeuge für die Erstellung der Dokumentation verwendet, können spezielle Verfahren notwendig sein, um sicherzustellen, dass effektive Maßnahmen für das Versionsmanagement oder anderer Kontrollaspekte der Dokumente vorhanden sind.

6 Management der funktionalen Sicherheit

6.1 Ziele

6.1.1 Das erste Ziel der Anforderungen dieses Abschnitts ist es, die Verantwortlichkeiten im Management der funktionalen Sicherheit derer festzulegen, die Verantwortung für ein sicherheitsbezogenes E/E/PE-System oder für eine oder mehrere Phasen des Gesamt-Sicherheitslebenszyklus, des Sicherheitslebenszyklus des E/E/PE-Systems und des Software-Sicherheitslebenszyklus haben.

6.1.2 Das zweite Ziel der Anforderungen dieses Abschnitts ist es, die Tätigkeiten festzulegen, die von denen mit Verantwortung im Management der funktionalen Sicherheit auszuführen sind.

ANMERKUNG Die organisatorischen Maßnahmen, die in diesem Abschnitt behandelt werden, liefern die effektive Ausführung der technischen Anforderungen und sind nur auf das Erreichen und Bewahren der funktionalen Sicherheit der sicherheitsbezogenen E/E/PE-Systeme ausgerichtet. Die technischen Anforderungen, die zum Erhalt der funktionalen Sicherheit notwendig sind, werden als Teil der vom Hersteller des sicherheitsbezogenen E/E/PE-Systems gelieferten Informationen spezifiziert.

6.2 Anforderungen

6.2.1 Eine Organisation mit Verantwortung für ein sicherheitsbezogenes E/E/PE-System oder für eine oder mehrere Phasen des Gesamt-Sicherheitslebenszyklus, des Sicherheitslebenszyklus des E/E/PE-Systems und des Software-Sicherheitslebenszyklus muss eine oder mehrere Personen bestimmen, die Gesamtverantwortung trägt/tragen für:

- das System und für diese Lebenszyklusphasen;
- die Koordination der sicherheitsbezogenen Tätigkeiten, die in diesen Phasen ausgeführt werden;
- die Schnittstellen zwischen diesen Phasen und anderen Phasen, die von anderen Organisationen ausgeführt werden;
- für die Umsetzung der Anforderungen aus 6.2.2 bis 6.2.11 und 6.2.13;
- die Koordination der Beurteilungen der funktionalen Sicherheit (siehe 6.2.12 b) und Abschnitt 8) – insbesondere wo diejenigen, die die Beurteilung der funktionalen Sicherheit ausführen, sich zwischen den Phasen unterscheiden – einschließlich Kommunikation, Planung und Integration der Dokumentation, der Beurteilungen und der Empfehlungen;
- die Sicherstellung, dass die funktionale Sicherheit erreicht und in Übereinstimmung mit den Zielen und Anforderungen dieser Norm aufgezeigt wird.

ANMERKUNG Verantwortung für sicherheitsbezogene Tätigkeiten oder für Phasen des Sicherheitslebenszyklus kann auf andere Personen, insbesondere auf solche mit relevantem Sachverstand, delegiert werden. Unterschiedliche Personen können für unterschiedliche Tätigkeiten und Anforderungen verantwortlich sein. Die Verantwortung für die Koordination und für die gesamte funktionale Sicherheit sollte jedoch bei einer oder einer geringen Anzahl von Personen liegen, die über genügend Managementautorität verfügen.

6.2.2 Die Vorgehensweise und die Strategie zum Erreichen der funktionalen Sicherheit müssen festgelegt werden, gemeinsam mit den Mitteln zur Bewertung deren Ausführung und den Mitteln, mit denen sie innerhalb der Organisation mitgeteilt werden.

6.2.3 Alle Personen, Abteilungen und Organisationen, die für die Ausführung von Tätigkeiten in den zutreffenden Phasen des Gesamt-Sicherheitslebenszyklus, des Sicherheitslebenszyklus des E/E/PE-Systems oder des Software-Sicherheitslebenszyklus verantwortlich sind (einschließlich Personen, die für Verifikation und Beurteilung der funktionalen Sicherheit zuständig sind und, wo zutreffend, Genehmigungsbehörden oder Sicherheitsüberwachungsorgane), müssen identifiziert werden und ihre Verantwortlichkeiten müssen ihnen vollständig und eindeutig mitgeteilt werden.

6.2.4 Es müssen Verfahren entwickelt werden zur Definition welche Informationen zwischen relevanten Parteien mitgeteilt werden müssen, und wie diese Kommunikation stattfindet.

ANMERKUNG Siehe Abschnitt 5 zu Dokumentationsanforderungen.

6.2.5 Es müssen Verfahren entwickelt werden zur Sicherstellung einer unverzüglichen Verfolgung und zufrieden stellenden Lösung von Empfehlungen bezüglich der sicherheitsbezogenen E/E/PE-Systeme, einschließlich derer, die von Folgendem herrühren:

- a) Gefährdungs- und Risikoanalyse (siehe 7.4);
- b) Beurteilung der funktionalen Sicherheit (siehe Abschnitt 8);
- c) Verifikationstätigkeiten (siehe 7.18);
- d) Validierungstätigkeiten (siehe 7.8 und 7.14);
- e) Konfigurationsmanagement (siehe 6.2.10), 7.16 und IEC 61508-2 und IEC 61508-3);
- f) Bericht und Analyse von Vorkommnissen (siehe 6.2.6).

6.2.6 Es müssen Verfahren entwickelt werden zur Sicherstellung, dass alle erkannten Gefährdungssituationen analysiert werden und dass Empfehlungen erfolgen, um die Wahrscheinlichkeit des wiederholten Auftretens zu minimieren.

6.2.7 Es müssen Anforderungen für periodische Audits festgelegt werden, einschließlich:

- a) der Häufigkeit der Audits der funktionalen Sicherheit;
- b) dem Grad der Unabhängigkeit derjenigen, die die Audits durchführen;
- c) der notwendigen Dokumentation und nachfolgender Tätigkeiten.

6.2.8 Es müssen Verfahren entwickelt werden für:

- a) die Einleitung von Modifikationen der sicherheitsbezogenen E/E/PE-Systeme (siehe 7.16.2.2);
- b) den Erhalt von Zustimmung und Ermächtigung zu Modifikationen.

6.2.9 Es müssen Verfahren entwickelt werden für die Bewahrung genauer Informationen zu den Gefährdungen und gefährlichen Vorfällen, Sicherheitsfunktionen und sicherheitsbezogenen E/E/PE-Systemen.

6.2.10 Es müssen Verfahren entwickelt werden für das Konfigurationsmanagement der sicherheitsbezogenen E/E/PE-Systeme während den Phasen des Gesamt-Sicherheitslebenszyklus, des Sicherheitslebenszyklus des E/E/PE-Systems und des Software-Sicherheitslebenszyklus, einschließlich insbesondere:

- a) dem Punkt, im Hinblick auf spezifische Phasen, an dem eine formale Konfigurationskontrolle ausgeführt werden muss;
- b) den Verfahren, die für eine eindeutige Bestimmung aller Bestandteile eines Gegenstands (Hardware und Software) angewendet werden müssen;
- c) den Verfahren zur Verhinderung, dass nicht zugelassene Komponente zum Einsatz kommen,

6.2.11 Wo angemessen müssen Training und Informationen für Hilfsdienste bereitgestellt werden.

6.2.12 Diejenigen Personen, die Verantwortung für eine oder mehrere Phasen des Gesamt-Sicherheitslebenszyklus, des Sicherheitslebenszyklus des E/E/PE-Systems und des Software-Sicherheitslebenszyklus haben, müssen im Hinblick auf diejenigen Phasen, für die sie Verantwortung haben und in Übereinstimmung mit den in 6.2.1 bis 6.2.11 definierten Verfahren, alle Managementtätigkeiten und technischen Tätigkeiten festlegen, die notwendig sind, um das Erreichen, das Darstellen und den Erhalt der funktionalen Sicherheit der sicherheitsbezogenen E/E/PE-Systeme sicherzustellen, einschließlich:

- a) der ausgewählten Maßnahmen und Methoden, die angewendet werden, um die Anforderungen eines speziellen Abschnitts oder Unterabschnitts zu erfüllen (siehe IEC 61508-2, IEC 61508-3 und IEC 61508-6);
- b) der Tätigkeiten zur Beurteilung der funktionalen Sicherheit und der Art und Weise wie das Erreichen der funktionalen Sicherheit denjenigen dargestellt wird, die die Beurteilung der funktionalen Sicherheit ausführen (siehe Abschnitt 8);

ANMERKUNG Es sollten angemessene Verfahren für die Beurteilung der funktionalen Sicherheit verwendet werden, um Folgendes zu definieren:

- die Auswahl einer angemessenen Organisation, Person oder Personen, mit einem angemessenen Grad von Unabhängigkeit;
 - das Entwerfen und das Ändern von Richtlinien für Beurteilungen der funktionalen Sicherheit;
 - die Auswechslung derjenigen, die die Beurteilung der funktionalen Sicherheit ausführen, an irgendeinem Punkt des Lebenszyklus eines Systems;
 - die Lösung von Kontroversen bezogen auf diejenigen, die die Beurteilungen der funktionalen Sicherheit ausführen.
- c) der Verfahren zur Analyse der Betriebs- und Instandhaltungsleistung, insbesondere für:
- die Erkennung systematischer Fehler, welche die funktionale Sicherheit gefährden können, einschließlich der während routinemäßiger Instandhaltung verwendeten Verfahren, die wiederkehrende Fehler erkennen können;
 - die Beurteilung, ob die Anforderungsraten und die Ausfallraten während des Betriebs und der Instandhaltung mit den während des Entwurfs des Systems gemachten Annahmen übereinstimmen.

6.2.13 Es müssen Verfahren entwickelt werden, um sicherzustellen, dass alle Personen mit Verantwortlichkeiten gemäß 6.2.1 und 6.2.3 (d. h. einschließlich aller Personen, die an irgendeiner Tätigkeit des Gesamt-Sicherheitslebenszyklus, des Sicherheitslebenszyklus des E/E/PE-Systems oder des Software-Sicherheitslebenszyklus, einschließlich der Tätigkeiten zur Verifikation, zum Management der funktionalen Sicherheit und zur Beurteilung der funktionalen Sicherheit, beteiligt sind) eine angemessene Kompetenz haben müssen (d. h. Ausbildung, technisches Wissen, Erfahrung und Qualifikationen) in Bezug auf die speziellen, von ihnen auszuführenden Aufgaben. Solche Verfahren müssen Anforderungen zur Auffrischung, Aktualisierung und fortlaufenden Beurteilung der Befähigung einschließen.

6.2.14 Die Angemessenheit der Befähigung muss in Bezug auf die jeweilige Anwendung unter Beachtung der folgenden Faktoren betrachtet werden:

- a) die Verantwortlichkeiten der Personen;
- b) der erforderliche Grad der Überwachung;
- c) die möglichen Auswirkungen beim Auftreten eines Ausfalls der sicherheitsbezogenen E/E/PE-Systeme – je größer die Auswirkungen, desto strenger muss die Festlegung der Kompetenz sein;
- d) die Sicherheits-Integritätslevel der sicherheitsbezogenen E/E/PE-Systeme – je höher die Sicherheits-Integritätslevel, desto strenger muss die Festlegung der Kompetenz sein;
- e) der Neuigkeitsgrad des Entwurfs, der Entwurfsverfahren oder der Anwendung – je neuer oder unerprobter diese sind, desto strenger muss die Festlegung der Kompetenz sein;
- f) frühere Erfahrungen und ihre Relevanz in Bezug auf die speziellen auszuführenden Aufgaben und der verwendeten Technologie – je größer die erforderliche Kompetenz, desto besser müssen die Kompetenzen aus früheren Erfahrungen zu den für die speziellen auszuführenden Tätigkeiten erforderlichen Kompetenzen passen;
- g) die Art der Kompetenz passend zu den Umständen (zum Beispiel Qualifikationen, Erfahrungen, relevante Ausbildung und folgende Praxis, Führungsverhalten und Entscheidungsfähigkeiten);
- h) angemessene Kenntnisse des Anwendungsbereiches und der Technologie;
- i) angemessene Kenntnisse der Technologie für sicherheitsrelevanten Einsatz;
- j) Kenntnis des Rahmens der gesetzlichen und der Sicherheitsbestimmungen;
- k) Relevanz der Qualifikationen in Bezug auf die speziellen auszuführenden Tätigkeiten.

ANMERKUNG Hinweis [8] in den Literaturhinweisen enthält ein Beispiel für die Handhabung der Kompetenz für sicherheitsbezogene E/E/PE-Systeme.

6.2.15 Die Kompetenz und Befähigung aller Personen mit Verantwortlichkeiten definiert gemäß 6.2.1 und 6.2.3 muss dokumentiert werden.

6.2.16 Die als Ergebnis von 6.2.2 bis 6.2.15 festgelegten Tätigkeiten müssen ausgeführt und überwacht werden.

6.2.17 Lieferanten, die Produkte an eine Organisation mit Gesamtverantwortung für eine oder mehrere Phasen des Gesamt-Sicherheitslebenszyklus, des Sicherheitslebenszyklus des E/E/PE-Systems oder des Software-Sicherheitslebenszyklus (siehe 6.2.1) liefern oder Dienstleistungen für sie erbringen, müssen Produkte oder Dienstleistungen nach den Festlegungen dieser Organisation liefern oder erbringen und sie müssen ein angemessenes Qualitätsmanagementsystem haben.

7 Anforderungen zum Gesamt-Sicherheitslebenszyklus

7.1 Allgemeines

7.1.1 Einleitung

7.1.1.1 Diese Norm verwendet als technischen Rahmen einen Gesamt-Sicherheitslebenszyklus (siehe Bild 2), um auf systematische Art und Weise alle Tätigkeiten zu behandeln, die zum Erreichen der erforderlichen Sicherheitsintegrität für die Sicherheitsfunktionen, die von den sicherheitsbezogenen E/E/PE-Systemen ausgeführt werden, notwendig sind.

ANMERKUNG Für den Anspruch auf Übereinstimmung mit dieser Norm sollte der Gesamt-Sicherheitslebenszyklus als Grundlage verwendet werden. Es kann jedoch ein von dem im Bild 2 gezeigten verschiedener Gesamt-Sicherheitslebenszyklus verwendet werden, vorausgesetzt, die Ziele und Anforderungen jedes Abschnitts dieser Norm werden erfüllt.

7.1.1.2 Der Gesamt-Sicherheitslebenszyklus enthält folgende Mittel zum Erreichen des tolerierbaren Risikos:

- sicherheitsbezogene E/E/PE-Systeme;
- andere risikomindernde Maßnahmen.

7.1.1.3 Die Realisierungsphase des sicherheitsbezogenen E/E/PE-Systems aus dem Gesamt-Sicherheitslebenszyklus wird erweitert und in Bild 3 gezeigt. Dieser Teil des Sicherheitslebenszyklus des E/E/PE-Systems bildet den technischen Gesamtrahmen für IEC 61508-2. Der in Bild 4 gezeigte Teil des Software-Sicherheitslebenszyklus bildet den technischen Gesamtrahmen für IEC 61508-3. Die Beziehung des Gesamt-Sicherheitslebenszyklus zum Sicherheitslebenszyklus des E/E/PE-Systems und zum Software-Sicherheitslebenszyklus für sicherheitsbezogene Systeme wird in Bild 5 gezeigt.

7.1.1.4 Die Abbildungen des Gesamt-Sicherheitslebenszyklus, des Sicherheitslebenszyklus des E/E/PE-Systems und des Software-Sicherheitslebenszyklus (Bilder 2 bis 4) sind vereinfachte Betrachtungen der Realität und zeigen als solche nicht alle Iterationen bezüglich der speziellen Phasen oder Zwischenphasen. Iterationen sind aber innerhalb des Gesamt-Sicherheitslebenszyklus, des Sicherheitslebenszyklus des E/E/PE-Systems und des Software-Sicherheitslebenszyklus ein notwendiger und wichtiger Teil der Entwicklung.

7.1.1.5 Tätigkeiten in Bezug auf das Management der funktionalen Sicherheit (Abschnitt 6), Verifikation (7.18) und Beurteilung der funktionalen Sicherheit (Abschnitt 8) werden nicht in dem Gesamt-Sicherheitslebenszyklus, dem Sicherheitslebenszyklus des E/E/PE-Systems oder dem Software-Sicherheitslebenszyklus gezeigt. Dies erfolgte, um die Komplexität der Bilder der Sicherheitslebenszyklen zu reduzieren. Diese Tätigkeiten müssen, wo erforderlich, in den relevanten Phasen des Gesamt-Sicherheitslebenszyklus, des Sicherheitslebenszyklus des E/E/PE-Systems und des Software-Sicherheitslebenszyklus berücksichtigt werden.

ANMERKUNG 1 Tätigkeiten in Bezug auf **Verifikation, Management der funktionalen Sicherheit** und **Beurteilung der funktionalen Sicherheit** sind zur besseren Übersicht nicht gezeigt, gehören jedoch zu allen Phasen des Gesamt-Sicherheitslebenszyklus, des Sicherheitslebenszyklus des E/E/PE-Systems und des Software-Sicherheitslebenszyklus.

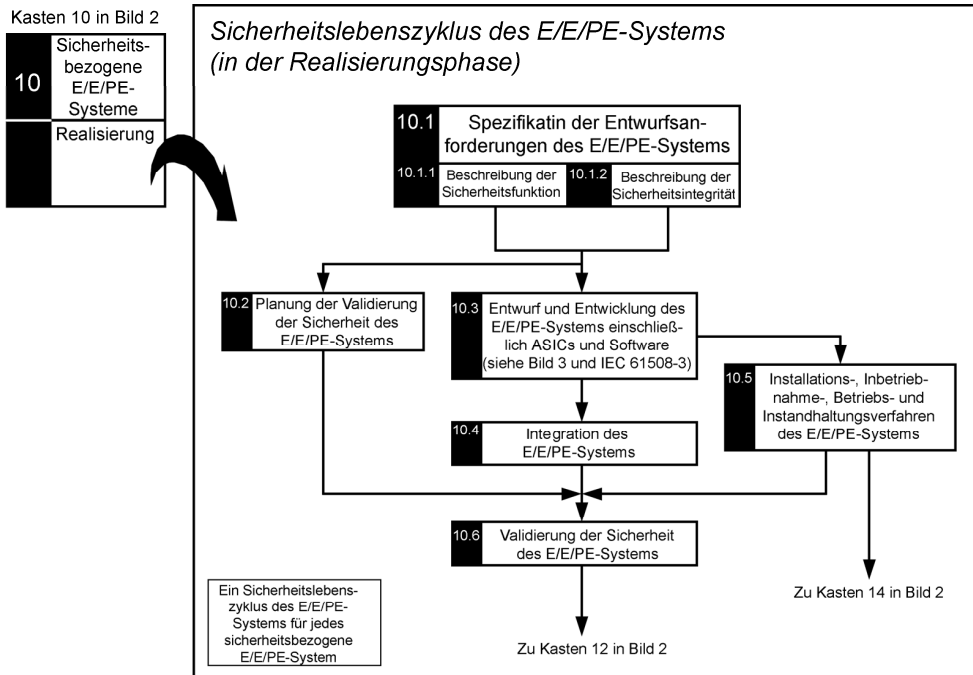
ANMERKUNG 2 Die durch den Kasten 11 dargestellte Phase, liegt außerhalb des Anwendungsbereiches dieser Norm.

ANMERKUNG 3 IEC 61508-2 und IEC 61508-3 behandeln Kasten 10 (Realisierung), sie beschäftigen sich jedoch auch, wo zutreffend, mit Aspekten der programmierbaren Elektronik (Hardware und Software) der Kästen 13, 14 und 15.

ANMERKUNG 4 Siehe Tabelle 1 für eine Beschreibung der Ziele und des Anwendungsbereiches der durch jeden Kasten dargestellten Phase.

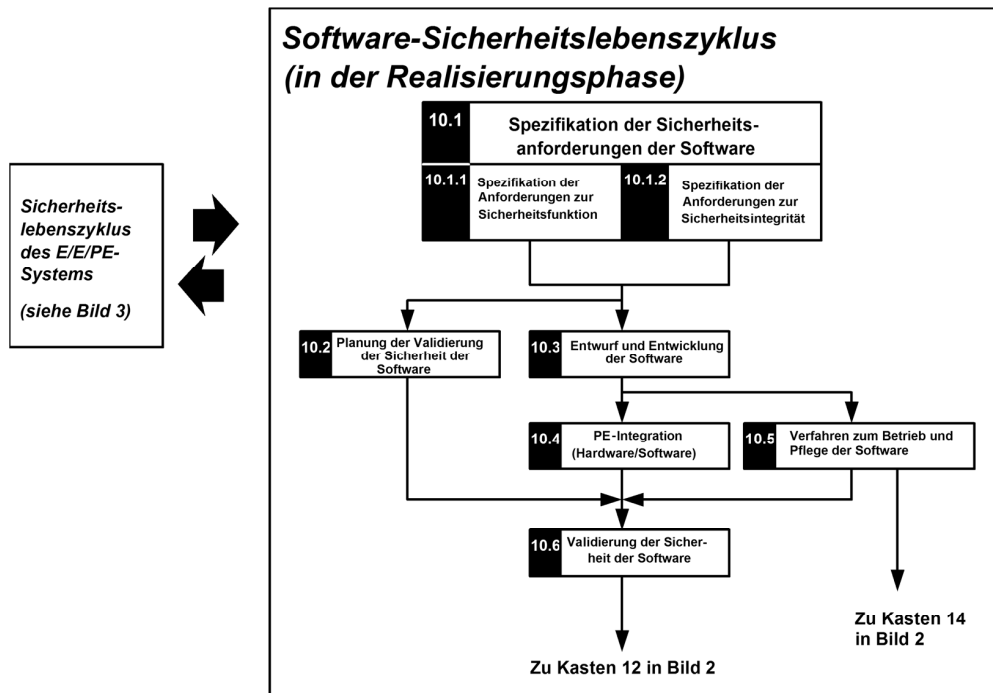
ANMERKUNG 5 Die zum Gesamtbetrieb, Instandhaltung, Reparatur, Modifikation, Nachrüstung und Außerbetriebnahme oder Ausmusterung notwendigen technischen Anforderungen werden als Teil der vom Hersteller des sicherheitsbezogenen E/E/PE-Systems gelieferten Informationen festgelegt.

Bild 2 – Gesamt-Sicherheitslebenszyklus



ANMERKUNG 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) enthalten, die spezifisch für das sicherheitsbezogene E/E/PE-System sind.

Bild 3 – Sicherheitslebenszyklus des E/E/PE-Systems (in der Realisierungsphase)



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

Bild 4 – Software-Sicherheitslebenszyklus (in der Realisierungsphase)

Kasten 10 des Gesamt-Sicherheitslebenszyklus
(siehe Bild 2)

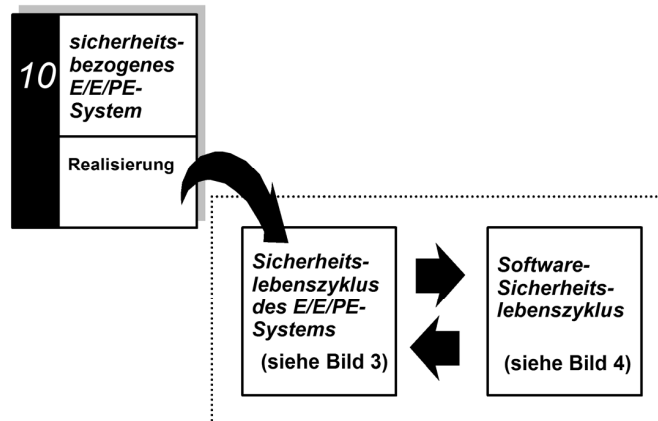


Bild 5 – Verhältnis des Gesamt-Sicherheitslebenszyklus zu dem Sicherheitslebenszyklus des E/E/PE-Systems und dem Software-Sicherheitslebenszyklus

7.1.2 Ziele und Anforderungen: Allgemeines

7.1.2.1 Die Ziele und Anforderungen für die Phasen des Gesamt-Sicherheitslebenszyklus sind in 7.2 bis 7.17 enthalten. Die Ziele und Anforderungen für die Phasen des Sicherheitslebenszyklus des E/E/PE-Systems und des Software-Sicherheitslebenszyklus sind in IEC 61508-2 beziehungsweise IEC 61508-3 enthalten.

ANMERKUNG 7.2 bis 7.17 stehen in Beziehung zu speziellen Kästen (Phasen) in Bild 2. Auf die speziellen Kästen wird in Anmerkungen zu diesen Unterabschnitten verwiesen.

7.1.2.2 Für alle Phasen des Gesamt-Sicherheitslebenszyklus zeigt Tabelle 1:

- die zu erreichenden Ziele;
- den Anwendungsbereich der Phase;
- den Verweis auf den Unterabschnitt, der die jeweiligen Anforderungen enthält;
 - die erforderlichen Eingaben zu der Phase;
 - die Ergebnisse, die erforderlich sind, um die Anforderungen zu erfüllen.

Tabelle 1 – Gesamt-Sicherheitslebenszyklus: Übersicht

Phase des Sicherheitslebenszyklus		Ziele	Anwendungsbereich	Unterabschnitt der Anforderungen	Eingaben	Ergebnisse
Kastennummer in Bild 2	Titel					
1	Konzept	7.2.1: Einen Grad an Verständnis der EUC und deren Umgebung (physikalische, gesetzgebende usw.) zu entwickeln, der ausreichend ist, um die anderen Tätigkeiten des Sicherheitslebenszyklus zufrieden stellend ausführen zu können.	EUC und ihre Umgebung (physikalische, gesetzgebende usw.).	7.2.2	Alle notwendigen relevanten Informationen, um die Anforderungen dieses Unterabschnitts zu erfüllen.	Informationen bezüglich der EUC, deren Umgebung und Gefährdungen.
2	Definition des gesamten Anwendungsbereiches	7.3.1: Die Grenze der EUC und des EUC-Leit- oder Steuerungssystems festzulegen. Den Anwendungsbereich der Gefährdungs- und Risikoanalyse (zum Beispiel Prozessgefährdungen, Umweltgefährdungen usw.) festzulegen.	EUC und ihre Umgebung.	7.3.2	Informationen bezüglich der EUC, deren Umgebung und Gefährdungen.	Definierter Anwendungsbereich der Gefährdungs- und Risikoanalyse.

Tabelle 1 (fortgesetzt)

Phase des Sicherheitslebenszyklus		Ziele	Anwendungsbereich	Unterabschnitt der Anforderungen	Eingaben	Ergebnisse
Kastennummer in Bild 2	Titel					
3	Gefährdungs- und Risikoanalyse	7.4.1: Die Gefährdungen, Gefährdungssituationen und Schadensereignisse in Bezug auf die EUC und das EUC-Leit- oder Steuerungssystem (in allen Betriebsarten) für alle vernünftigerweise vorhersehbaren Umstände, einschließlich Fehlerbedingungen und Fehlanwendung, zu bestimmen. Die Abläufe von Ereignissen zu bestimmen, die zu den Schadensereignissen führen. Die mit den Schadensereignissen verbundenen EUC-Risiken zu bestimmen.	Der Anwendungsbereich hängt von der erreichten Phase im Gesamt-Sicherheitslebenszyklus, Sicherheitslebenszyklus des E/E/PE-Systems und Software-Sicherheitslebenszyklus ab (da es notwendig sein kann, mehr als eine Gefährdungs- und Risikoanalyse auszuführen). Für die einleitende Gefährdungs- und Risikoanalyse wird der Anwendungsbereich so sein, wie durch das Ergebnis der Definition des gesamten Anwendungsbereiches definiert.	7.4.2	Definierter Anwendungsbereich der Gefährdungs- und Risikoanalyse.	Beschreibung und Informationen in Bezug auf die Gefährdungs- und Risikoanalyse.
4	Anforderungen zur Gesamtsicherheit	7.5.1: Die Spezifikation der Anforderungen zur Gesamtsicherheit für die sicherheitsbezogenen E/E/PE-Systeme und anderen risikomindernden Maßnahmen, im Hinblick auf die Anforderungen zur Sicherheitsfunktion und den Anforderungen zur Sicherheitsintegrität, zu entwickeln, um die erforderliche funktionale Sicherheit zu erreichen.	Wie durch das Ergebnis der Definition des gesamten Anwendungsbereiches definiert.	7.5.2	Beschreibung und Informationen in Bezug auf die Gefährdungs- und Risikoanalyse.	Spezifikation der Anforderungen zur Gesamtsicherheit im Hinblick auf die Anforderungen zur Sicherheitsfunktion und die Anforderungen zur Sicherheitsintegrität.

Tabelle 1 (fortgesetzt)

Phase des Sicherheitslebenszyklus		Ziele	Anwendungsbereich	Unterabschnitt der Anforderungen	Eingaben	Ergebnisse
Kastennummer in Bild 2	Titel					
5	Zuordnung der Anforderungen an die Gesamtsicherheit	7.6.1: Die in der Spezifikation der Anforderungen zur Gesamtsicherheit (sowohl die Anforderungen zur Sicherheitsfunktion, als auch die Anforderungen zur Sicherheitsintegrität) enthaltenen Sicherheitsfunktionen den vorgesehenen sicherheitsbezogenen E/E/PE-Systemen und anderen risikomindernden Maßnahmen zuzuordnen. Jeder Sicherheitsfunktion, die von einem sicherheitsbezogenen E/E/PE-System ausgeführt wird, einen Sicherheits-Integritätslevel zuzuordnen.	Wie durch das Ergebnis der Definition des gesamten Anwendungsbereiches definiert.	7.6.2	Spezifikation der Anforderungen zur Gesamtsicherheit im Hinblick auf die Anforderungen zur Sicherheitsfunktion und die Anforderungen zur Sicherheitsintegrität.	Informationen und Ergebnisse der Zuordnung der Anforderungen an die Gesamtsicherheit.
6	Planung des Gesamtbetriebs und der gesamten Instandhaltung	7.7.1: Einen Plan für Betrieb und Instandhaltung der sicherheitsbezogenen E/E/PE-Systeme zu entwickeln, um sicherzustellen, dass die erforderliche funktionale Sicherheit während des Betriebs und der Instandhaltung aufrechterhalten wird.	EUC, das EUC-Leit- oder Steuerungssystem und menschliche Faktoren. Sicherheitsbezogene E/E/PE-Systeme.	7.7.2	Informationen und Ergebnisse der Zuordnung der Anforderungen an die Gesamtsicherheit.	Plan für den Betrieb und die Instandhaltung der sicherheitsbezogenen E/E/PE-Systeme.
7	Planung der Gesamtvalidierung der Sicherheit	7.8.1: Einen Plan zu entwickeln, um die Gesamtvalidierung der Sicherheit der sicherheitsbezogenen E/E/PE-Systeme zu unterstützen.	EUC, das EUC-Leit- oder Steuerungssystem und menschliche Faktoren. Sicherheitsbezogene E/E/PE-Systeme.	7.8.2	Informationen und Ergebnisse der Zuordnung der Anforderungen an die Gesamtsicherheit.	Plan zur Unterstützung der Validierung der sicherheitsbezogenen E/E/PE-Systeme.

Tabelle 1 (fortgesetzt)

Phase des Sicherheitslebenszyklus		Ziele	Anwendungsbereich	Unterabschnitt der Anforderungen	Eingaben	Ergebnisse
Kastennummer in Bild 2	Titel					
8	Planung der Gesamtinstallation und Gesamteinbetriebnahme	7.9.1: Einen Plan für die kontrollierte Installation der sicherheitsbezogenen E/E/PE-Systeme zu entwickeln, um sicherzustellen, dass die erforderliche funktionale Sicherheit erreicht wird. Einen Plan für die kontrollierte Inbetriebnahme der sicherheitsbezogenen E/E/PE-Systeme zu entwickeln, um sicherzustellen, dass die erforderliche funktionale Sicherheit erreicht wird.	EUC und das EUC-Leit- oder Steuerungssystem. Sicherheitsbezogene E/E/PE-Systeme.	7.9.2	Informationen und Ergebnisse der Zuordnung der Anforderungen an die Gesamtsicherheit.	Plan für die Installation der sicherheitsbezogenen E/E/PE-Systeme. Plan für die Inbetriebnahme der sicherheitsbezogenen E/E/PE-Systeme.
9	Spezifikation der Sicherheitsanforderungen des E/E/PE-Systems	7.10.1: Die Anforderungen für jedes sicherheitsbezogene E/E/PE-System, im Hinblick auf die Spezifikation der Anforderungen zur E/E/PE-Sicherheitsfunktion und die Spezifikation der Anforderungen zur E/E/PE-Sicherheitsintegrität festzulegen, um die erforderliche funktionale Sicherheit zu erreichen.	Sicherheitsbezogene E/E/PE-Systeme.	7.10.2	Informationen und Ergebnisse der Zuordnung der Anforderungen an die Gesamtsicherheit.	Spezifikation der Sicherheitsanforderungen des E/E/PE-Systems. Gemachte Annahmen hinsichtlich anderer risikomindernder Maßnahmen, die während der Lebensdauer der EUC gehandhabt werden müssen.
10	Sicherheitsbezogene E/E/PE-Systeme: Realisierung	7.11.1 und Teile 2 und 3: Sicherheitsbezogene E/E/PE-Systeme zu erstellen, die der Spezifikation der Sicherheitsanforderungen des E/E/PE-Systems (umfasst die Spezifikation der Anforderungen zur Sicherheitsfunktion des E/E/PE-Systems und die Spezifikation der Anforderungen zur Sicherheitsintegrität des E/E/PE-Systems) entsprechen.	Sicherheitsbezogene E/E/PE-Systeme.	7.11.2, IEC 61508-2 und IEC 61508-3	Spezifikation der Sicherheitsanforderungen des E/E/PE-Systems.	Realisierung jedes sicherheitsbezogenen E/E/PE-Systems entsprechend der Spezifikation der Sicherheitsanforderungen des E/E/PE-Systems.

Tabelle 1 (fortgesetzt)

Phase des Sicherheitslebenszyklus		Ziele	Anwendungsbereich	Unterabschnitt der Anforderungen	Eingaben	Ergebnisse
Kastennummer in Bild 2	Titel					
11	Andere risikomindernde Maßnahmen: Spezifikation und Realisierung	7.12.1: Andere risikomindernde Maßnahmen zu erstellen, um die Anforderungen zur Sicherheitsfunktion und die Anforderungen zur Sicherheitsintegrität, die für solche Systeme festgelegt sind, zu erfüllen (außerhalb des Anwendungsbereiches dieser Norm).	Andere risikomindernde Maßnahmen.	7.12.2	Spezifikation der Sicherheitsanforderungen anderer risikomindernder Maßnahmen (außerhalb des Anwendungsbereiches und in dieser Norm nicht weiter betrachtet).	Realisierung aller anderen risikomindernden Maßnahmen entsprechend den Sicherheitsanforderungen für diese Maßnahme.
12	Gesamtinstallation und Gesamtinbetriebnahme	7.13.1: Die sicherheitsbezogenen E/E/PE-Systeme zu installieren. Die sicherheitsbezogenen E/E/PE-Systeme in Betrieb zu nehmen.	EUC und das EUC-Leit- oder Steuerungssystem. Sicherheitsbezogene E/E/PE-Systeme.	7.13.2	Plan für die Installation der sicherheitsbezogenen E/E/PE-Systeme. Plan für die Inbetriebnahme der sicherheitsbezogenen E/E/PE-Systeme.	Vollständig installierte sicherheitsbezogene E/E/PE-Systeme. Vollständig in Betrieb genommene sicherheitsbezogene E/E/PE-Systeme.
13	Gesamtvalidierung der Sicherheit	7.14.1: Validieren, dass die sicherheitsbezogenen E/E/PE-Systeme die Spezifikation der Anforderungen zur Gesamtsicherheit, im Hinblick auf die Anforderungen zur Gesamt-Sicherheitsfunktion und die Anforderungen zur Gesamt-Sicherheitsintegrität, unter Berücksichtigung der Zuordnung der Sicherheitsanforderungen für die nach 7.6 entwickelten sicherheitsbezogenen E/E/PE-Systeme, erfüllen.	EUC und das EUC-Leit- oder Steuerungssystem. Sicherheitsbezogene E/E/PE-Systeme.	7.14.2	Plan der Gesamtvalidierung der Sicherheit für die sicherheitsbezogenen E/E/PE-Systeme. Informationen und Ergebnisse der Zuordnung der Anforderungen an die Gesamtsicherheit.	Bestätigung, dass alle sicherheitsbezogenen E/E/PE-Systeme die Spezifikation der Anforderungen zur Gesamtsicherheit unter Berücksichtigung der Zuordnung der Sicherheitsanforderungen für die sicherheitsbezogenen E/E/PE-Systeme, erfüllen.

Tabelle 1 (fortgesetzt)

Phase des Sicherheitslebenszyklus		Ziele	Anwendungsbereich	Unterabschnitt der Anforderungen	Eingaben	Ergebnisse
Kastennummer in Bild 2	Titel					
14	Gesamtbetrieb, gesamte Instandhaltung und Reparatur	7.15.1: Sicherzustellen, dass die funktionale Sicherheit der sicherheitsbezogenen E/E/PE-Systeme auf dem festgelegten Grad aufrechterhalten wird. Sicherstellen, dass die technischen Anforderungen, die für den Gesamtbetrieb, die gesamte Instandhaltung und die Reparatur der sicherheitsbezogenen E/E/PE-Systeme notwendig sind, festgelegt und denjenigen zur Verfügung gestellt werden, die für den zukünftigen Betrieb und die Instandhaltung der sicherheitsbezogenen E/E/PE-Systeme verantwortlich sind.	EUC und das EUC-Leit- oder Steuerungssystem. Sicherheitsbezogene E/E/PE-Systeme.	7.15.2	Plan des Gesamtbetriebs und der gesamten Instandhaltung für die sicherheitsbezogenen E/E/PE-Systeme.	Fortsetzung des Erreichens der erforderlichen funktionalen Sicherheit für die sicherheitsbezogenen E/E/PE-Systeme. Chronologische Dokumentation des Betriebs, der Reparatur und der Instandhaltung der sicherheitsbezogenen E/E/PE-Systeme.
15	Gesamtmodifikation und gesamte Nachrüstung	7.16.1: Verfahren zu definieren, die notwendig sind, um sicherzustellen, dass die funktionale Sicherheit für die sicherheitsbezogenen E/E/PE-Systeme, sowohl während als auch nach der Ausführung der Modifikations- und Nachrüstungsphase, angemessen ist.	EUC und das EUC-Leit- oder Steuerungssystem. Sicherheitsbezogene E/E/PE-Systeme.	7.16.2	Anforderung zur Modifikation oder Reparatur unter Anwendung der Verfahren für das Management der funktionalen Sicherheit.	Erreichen der erforderlichen funktionalen Sicherheit für die sicherheitsbezogenen E/E/PE-Systeme, sowohl während als auch nach der Ausführung der Modifikations- und Nachrüstungsphase. Chronologische Dokumentation der Modifikation und der Nachrüstung der sicherheitsbezogenen E/E/PE-Systeme.

Tabelle 1 (fortgesetzt)

Phase des Sicherheitslebenszyklus		Ziele	Anwendungsbereich	Unterabschnitt der Anforderungen	Eingaben	Ergebnisse
Kastennummer in Bild 2	Titel					
16	Außerbetriebnahme oder Ausmusterung	7.17.1: Verfahren zu definieren, die notwendig sind, um sicherzustellen, dass die funktionale Sicherheit für die sicherheitsbezogenen E/E/PE-Systeme unter den Umständen während und nach den Tätigkeiten der Außerbetriebnahme oder Ausmusterung der EUC angemessen ist.	EUC und das EUC-Leit- oder Steuerungssystem. Sicherheitsbezogene E/E/PE-Systeme.	7.17.2	Anforderung zur Außerbetriebnahme oder Ausmusterung unter Anwendung der Verfahren für das Management der funktionalen Sicherheit.	Erreichen der erforderlichen funktionalen Sicherheit für die sicherheitsbezogenen E/E/PE-Systeme, sowohl während als auch nach den Außerbetriebnahme- oder Ausmusterungstätigkeiten. Chronologische Dokumentation der Außerbetriebnahme- oder Ausmusterungstätigkeiten.

7.1.3 Ziele

7.1.3.1 Das erste Ziel der Anforderungen dieses Unterabschnitts ist es, in einer systematischen Art und Weise die Phasen, die im Gesamt-Sicherheitslebenszyklus betrachtet werden müssen, zu strukturieren, um die erforderliche funktionale Sicherheit der sicherheitsbezogenen E/E/PE-Systeme zu erreichen.

7.1.3.2 Das zweite Ziel der Anforderungen dieses Unterabschnitts ist es, Schlüsselinformationen, die für die funktionale Sicherheit der sicherheitsbezogenen E/E/PE-Systeme während des Gesamt-Sicherheitslebenszyklus relevant sind, zu dokumentieren.

ANMERKUNG Siehe Abschnitt 5 für Anforderungen zur Dokumentation und Anhang A für ein Beispiel zur Struktur der Dokumentation. Die Struktur der Dokumentation kann firmeneigene Verfahren und die Arbeitspraxis von speziellen Anwendungsbereichen berücksichtigen.

7.1.4 Anforderungen

7.1.4.1 Bild 2 zeigt den festgelegten Gesamt-Sicherheitslebenszyklus, der als Basis zur Erlangung von Übereinstimmung mit dieser Norm verwendet werden muss. Falls ein anderer Gesamt-Sicherheitslebenszyklus verwendet wird, muss dieser während der Planung der funktionalen Sicherheit festgelegt werden, und alle Ziele und Anforderungen jedes Abschnitts oder Unterabschnitts in dieser Norm müssen erreicht werden.

ANMERKUNG Die Teile des Sicherheitslebenszyklus des E/E/PE-Systems und des Software-Sicherheitslebenszyklus, welche die Realisierungsphase des Gesamt-Sicherheitslebenszyklus bilden, sind in IEC 61508-2 beziehungsweise IEC 61508-3 festgelegt.

7.1.4.2 Die Anforderungen für das Management der funktionalen Sicherheit (siehe Abschnitt 6) müssen gleichzeitig mit den Phasen des Gesamt-Sicherheitslebenszyklus einhergehen.

7.1.4.3 Jede Phase des Gesamt-Sicherheitslebenszyklus muss angewendet und die Anforderungen müssen erfüllt werden, außer es liegt eine Begründung für eine Abweichung vor.

7.1.4.4 Jede Phase des Gesamt-Sicherheitslebenszyklus muss in elementare Tätigkeiten, mit für jede Phase festgelegtem Anwendungsbereich, festgelegten Eingaben und Ergebnissen, aufgeteilt werden.

7.1.4.5 Der Anwendungsbereich und die Eingaben für jede Phase des Gesamt-Sicherheitslebenszyklus müssen wie in Tabelle 1 festgelegt sein.

7.1.4.6 Die Ergebnisse jeder Phase des Gesamt-Sicherheitslebenszyklus müssen den in Tabelle 1 festgelegten Ergebnissen entsprechen, außer die Planung der funktionalen Sicherheit liefert eine Begründung oder in der anwendungsspezifischen Norm ist anderes festgelegt.

7.1.4.7 Die Ergebnisse jeder Phase des Gesamt-Sicherheitslebenszyklus müssen die für jede Phase festgelegten Ziele und Anforderungen erfüllen (siehe 7.2 bis 7.17).

7.1.4.8 Die für jede Phase des Gesamt-Sicherheitslebenszyklus zu erfüllenden Anforderungen zur Verifikation sind in 7.18 festgelegt.

7.2 Konzept

ANMERKUNG Diese Phase entspricht Kasten 1 in Bild 2.

7.2.1 Ziel

Das Ziel der Anforderungen dieses Unterabschnitts ist es, einen Grad an Verständnis der EUC und deren Umgebung (physikalische, gesetzgebende usw.) zu entwickeln, der ausreichend ist, um die anderen Tätigkeiten des Sicherheitslebenszyklus zufrieden stellend ausführen zu können.

7.2.2 Anforderungen

7.2.2.1 Es müssen gründliche Kenntnisse der EUC, ihrer erforderlichen Leit- oder Steuerungsfunktionen und ihrer physikalischen Umgebung erworben werden.

7.2.2.2 Die möglichen Gefährdungsquellen, Gefährdungssituationen und Schadensereignisse müssen bestimmt werden.

7.2.2.3 Es müssen Informationen über die ermittelten Gefährdungen eingeholt werden (zum Beispiel Dauer, Intensität, Giftigkeit, Grenze der Exposition, mechanische Kraft, Explosivität, Reaktionsfreudigkeit, Brennbarkeit usw.).

7.2.2.4 Es müssen Informationen über die aktuellen Sicherheitsvorschriften (national und international) eingeholt werden.

7.2.2.5 Es müssen Gefährdungen, Gefährdungssituationen und Schadensereignisse durch Wechselwirkung mit anderen Einrichtungen oder Systemen der EUC (installiert oder noch zu installieren) betrachtet werden.

7.2.2.6 Die in 7.2.2.1 bis 7.2.2.5 gewonnenen Informationen und Ergebnisse müssen dokumentiert werden.

7.3 Definition des gesamten Anwendungsbereiches

ANMERKUNG Diese Phase entspricht Kasten 2 in Bild 2.

7.3.1 Ziele

7.3.1.1 Das erste Ziel der Anforderungen dieses Unterabschnitts ist es, die Grenze der EUC und des EUC-Leit- oder Steuerungssystems festzulegen.

7.3.1.2 Das zweite Ziel der Anforderungen dieses Unterabschnitts ist es, den Anwendungsbereich der Gefährdungs- und Risikoanalyse (zum Beispiel Prozessgefährdungen, Umweltgefährdungen usw.) festzulegen.

7.3.2 Anforderungen

7.3.2.1 Die Grenze der EUC und des EUC-Leit- oder Steuerungssystems muss definiert werden, um alle Einrichtungen und Systeme zu berücksichtigen (einschließlich Menschen, wo dazugehörig), die mit den relevanten Gefährdungen und Gefährdungssituationen in Verbindung stehen.

ANMERKUNG Es können mehrere Iterationen zwischen der Definition des gesamten Anwendungsbereiches und der Gefährdungs- und Risikoanalyse notwendig sein.

7.3.2.2 Die physikalischen Einrichtungen, einschließlich der EUC und des EUC-Leit- oder Steuerungssystems, die in den Anwendungsbereich der Gefährdungs- und Risikoanalyse eingeschlossen werden müssen, müssen festgelegt werden.

ANMERKUNG Siehe Hinweise [9] und [10] in den Literaturhinweisen.

7.3.2.3 Die externen Ereignisse, die in der Gefährdungs- und Risikoanalyse berücksichtigt werden müssen, müssen festgelegt werden.

7.3.2.4 Die Einrichtungen und Systeme, die mit den Gefährdungen und den gefährlichen Vorfällen in Verbindung stehen, müssen festgelegt werden.

7.3.2.5 Die Art von auslösenden Ereignissen, die betrachtet werden müssen (zum Beispiel Bauteilausfälle, Verfahrensfehler, menschliches Versagen, abhängige Ausfallmechanismen, die das Auftreten von Unfallketten verursachen können), müssen festgelegt werden.

7.3.2.6 Die in 7.3.2.1 bis 7.3.2.5 gewonnenen Informationen und Ergebnisse müssen dokumentiert werden.

7.4 Gefährdungs- und Risikoanalyse

ANMERKUNG Diese Phase entspricht Kasten 3 in Bild 2.

7.4.1 Ziele

7.4.1.1 Das erste Ziel der Anforderungen dieses Unterabschnitts ist es, die Gefährdungen, gefährlichen Vorfälle und Gefährdungssituationen in Bezug auf die EUC und das EUC-Leit- oder Steuerungssystem (in allen Betriebsarten) für alle vernünftigerweise vorhersehbaren Umstände, einschließlich Fehlerbedingungen und Fehlanwendung, zu bestimmen.

7.4.1.2 Das zweite Ziel der Anforderungen dieses Unterabschnitts ist es, die Abläufe von Ereignissen zu bestimmen, die zu den in 7.4.1.1 bestimmten gefährlichen Vorfällen führen.

7.4.1.3 Das dritte Ziel der Anforderungen dieses Unterabschnitts ist es, die mit den in 7.4.1.1 bestimmten gefährlichen Vorfällen verbundenen EUC-Risiken zu bestimmen.

ANMERKUNG 1 Dieser Unterabschnitt ist notwendig, damit die Sicherheitsanforderungen für die sicherheitsbezogenen E/E/PE-Systeme auf einer systematischen, risikobasierenden Vorgehensweise beruhen. Wird die EUC und das EUC-Leit- oder Steuerungssystem nicht betrachtet, so kann dies nicht erfolgen.

ANMERKUNG 2 In Anwendungsbereichen, in denen gültige Annahmen über die mit den gefährlichen Vorfällen und deren Auswirkungen verbundenen Risiken gemacht werden können, kann die nach diesem Unterabschnitt (und 7.5) erforderliche Analyse durch die Ersteller anwendungsspezifischer Versionen dieser Norm durchgeführt und in vereinfachte grafische Anforderungen eingebettet werden. Die Anhänge E und G der IEC 61508-5 enthalten Beispiele solcher Methoden.

7.4.2 Anforderungen

7.4.2.1 Es muss eine Gefährdungs- und Risikoanalyse durchgeführt werden, welche die Informationen aus der Phase der Definition des gesamten Anwendungsbereiches (siehe 7.3) berücksichtigen muss. Wenn zu späteren Zeitpunkten in den Phasen des Gesamt-Sicherheitslebenszyklus, des Sicherheitslebenszyklus des E/E/PE-Systems und des Software-Sicherheitslebenszyklus Entscheidungen getroffen werden, welche die Grundlage ändern, auf der frühere Entscheidungen getroffen wurden, muss eine weitere Gefährdungs- und Risikoanalyse durchgeführt werden.

ANMERKUNG 1 Zur Anleitung siehe Hinweise [9] und [10] in den Literaturhinweisen.

ANMERKUNG 2 Es kann notwendig sein, mehr als eine Gefährdungs- und Risikoanalyse auszuführen.

ANMERKUNG 3 Als ein Beispiel für die Notwendigkeit, Gefährdungs- und Risikoanalysen innerhalb des Gesamt-Sicherheitslebenszyklus weiterzuführen, kann die Analyse einer EUC, die ein sicherheitsrelevantes Ventil enthält, betrachtet werden. Eine Gefährdungs- und Risikoanalyse könnte zwei Abläufe von Ereignissen, die zu gefährlichen Vorfällen führen, bestimmen und "Ausfall des Ventils im geschlossenen Zustand" und "Ausfall des Ventils im geöffneten Zustand" umfassen. Wenn der ausführliche Entwurf des EUC-Leit- oder Steuerungssystems, welches das Ventil steuert, analysiert wird, könnte jedoch eine neue Ausfallart "Ventil oszilliert" entdeckt werden, die einen neuen, zu einem gefährlichen Vorfall führenden Ereignisablauf, mit sich bringt.

7.4.2.2 Die Beseitigung oder Minderung von Gefährdungen muss in Erwägung gezogen werden.

ANMERKUNG Obwohl es nicht im Anwendungsbereich dieser Norm liegt, ist es von primärer Bedeutung, dass erkannte Gefährdungen der EUC an der Quelle beseitigt werden, zum Beispiel durch die Anwendung von inhärent sicheren Prinzipien und die Anwendung bewährter Praktiken.

7.4.2.3 Die Gefährdungen, gefährlichen Vorfälle und Gefährdungssituationen der EUC und des EUC-Leit- oder Steuerungssystems müssen unter allen vernünftigerweise vorhersehbaren Umständen (einschließlich Fehlerbedingungen, vernünftigerweise vorhersehbarer Fehlanwendung und böswilliger oder nicht autorisierter Handlung) festgelegt werden. Dieses muss alle relevanten menschlichen Faktoren einschließen und muss ungewöhnlichen und selten genutzten Betriebsarten der EUC besondere Aufmerksamkeit schenken. Wenn die Gefährdungsanalyse identifiziert, dass eine böswillige oder nicht autorisierte Handlung, die eine Bedrohung der IT-Sicherheit darstellt, als vernünftigerweise vorhersehbar gilt, sollte eine Bedrohungsanalyse zur IT-Sicherheit durchgeführt werden.

ANMERKUNG 1 Zu vernünftigerweise vorhersehbarer Fehlanwendung siehe 3.1.11 der IEC 61508-4.

ANMERKUNG 2 Für Anleitung zur Erkennung von Gefährdungen einschließlich der Anleitung zur Darstellung und Analyse der menschlichen Faktoren, siehe Hinweis [11] in den Literaturhinweisen.

ANMERKUNG 3 Für Anleitung zur IT-Sicherheitsrisikenanalyse siehe ISO/IEC 13335 und IEC 62443.

ANMERKUNG 4 Böswillige oder nicht autorisierte Handlung schließt Bedrohungen der IT-Sicherheit ein.

ANMERKUNG 5 Die Gefährdungs- und Risikoanalyse sollte auch berücksichtigen, ob die Aktivierung einer Sicherheitsfunktion durch eine Anforderung oder eine Fehlauslösung eine neue Gefährdung herbeiführt. In einer solchen Situation kann es notwendig sein, eine neue Sicherheitsfunktion zu entwickeln, um diese Gefährdung zu behandeln.

7.4.2.4 Die Abläufe von Ereignissen, die zu den in 7.4.2.3 bestimmten gefährlichen Vorfällen führen, müssen festgelegt werden.

ANMERKUNG Im Allgemeinen lohnt sich die Betrachtung, ob irgendeiner der Abläufe von Ereignissen durch Modifikationen des Prozessentwurfs oder der Einrichtungen beseitigt werden kann.

7.4.2.5 Die Wahrscheinlichkeit der gefährlichen Vorfälle für die in 7.4.2.3 festgelegten Bedingungen muss bewertet werden.

ANMERKUNG Die Wahrscheinlichkeit eines speziellen gefährlichen Vorfalles kann quantitativ oder qualitativ ausgedrückt werden (siehe 7.4.2.8 und IEC 61508-5).

7.4.2.6 Die Auswirkungen, die mit den in 7.4.2.3 festgelegten gefährlichen Vorfällen verbunden sind, müssen bestimmt werden.

7.4.2.7 Das EUC-Risiko muss für jeden festgelegten gefährlichen Vorfall bewertet oder abgeschätzt werden.

7.4.2.8 Die Anforderungen aus 7.4.2.1 bis 7.4.2.7 können durch die Anwendung von entweder qualitativen oder quantitativen Methoden der Gefährdungs- und Risikoanalyse erfüllt werden (siehe IEC 61508-5).

7.4.2.9 Die Angemessenheit der Methoden und der Umfang, in dem diese Methoden angewendet werden müssen, hängen von einer Anzahl von Faktoren ab. Diese schließen ein:

- die speziellen Gefährdungen und deren Auswirkungen;
- die Komplexität der EUC und des EUC-Leit- oder Steuerungssystems;
- den Anwendungsbereich und dort bewährte Praktiken;
- die Anforderungen von gesetzlichen Bestimmungen und Sicherheitsbestimmungen;
- das EUC-Risiko;
- die Verfügbarkeit korrekter Daten, auf denen die Gefährdungs- und Risikoanalyse basieren muss.

7.4.2.10 Die Gefährdungs- und Risikoanalyse muss Folgendes betrachten:

- jeder ermittelte gefährliche Vorfall und die Komponenten, die dazu beitragen;
- die Auswirkungen und die Wahrscheinlichkeit der Abläufe von Ereignissen, mit denen jeder gefährliche Vorfall verbunden ist;
- das tolerierbare Risiko für jeden gefährlichen Vorfall;
- die ergriffenen Maßnahmen zur Reduzierung oder Beseitigung von Gefährdungen und Risiken;
- die Annahmen, die während der Analyse der Risiken getroffen wurden, einschließlich geschätzter Anforderungsraten und Ausfallraten der Einrichtungen. Jedes Zugeständnis, das für betriebliche Beschränkungen oder menschliches Eingreifen gewährt wird, muss genau beschrieben werden.

7.4.2.11 Die Informationen und Ergebnisse, welche die Gefährdungs- und Risikoanalyse bilden, müssen dokumentiert werden.

7.4.2.12 Die Informationen und Ergebnisse, welche die Gefährdungs- und Risikoanalyse bilden, müssen während des Gesamt-Sicherheitslebenszyklus, von der Phase der Gefährdungs- und Risikoanalyse bis hin zur Phase der Außerbetriebnahme oder Ausmusterung für die EUC und das EUC-Leit- oder Steuerungssystem gepflegt werden.

ANMERKUNG Die Pflege von Informationen, die sich aus den Ergebnissen der Phase der Gefährdungs- und Risikoanalyse ergeben, ist ein Schlüssel zum Nachverfolgen des Fortschritts bei offenen Problemen der Gefährdungs- und Risikoanalyse.

7.5 Anforderungen zur Gesamtsicherheit

ANMERKUNG Diese Phase entspricht Kasten 4 in Bild 2.

7.5.1 Ziel

Das Ziel der Anforderungen dieses Unterabschnitts ist es, die Spezifikation der Anforderungen zur Gesamtsicherheit für die sicherheitsbezogenen E/E/PE-Systeme und anderen risikomindernden Maßnahmen im Hinblick auf die Anforderungen zur Gesamt-Sicherheitsfunktion und die Anforderungen zur Gesamt-Sicherheitsintegrität zu entwickeln, um die erforderliche funktionale Sicherheit zu erreichen.

ANMERKUNG In Anwendungsbereichen, in denen gültige Annahmen über die Risiken, wahrscheinlichen Gefährdungen, Schadensereignisse und deren Auswirkungen gemacht werden können, kann die nach diesem Unterabschnitt (und 7.4) erforderliche Analyse durch die Ersteller anwendungsspezifischer Versionen dieser Norm durchgeführt und in vereinfachte grafische Anforderungen eingebettet werden. Die Anhänge D und E der IEC 61508-5 enthalten Beispiele solcher Methoden.

7.5.2 Anforderungen

7.5.2.1 Basierend auf den gefährlichen Vorfällen, die aus der Gefährdungs- und Risikoanalyse abgeleitet werden, muss ein Satz aller notwendigen Gesamt-Sicherheitsfunktionen entwickelt werden. Dies muss die Spezifikation der Anforderungen zur Gesamt-Sicherheitsfunktion bilden.

ANMERKUNG 1 Es wird notwendig sein, eine Gesamt-Sicherheitsfunktion für jeden gefährlichen Vorfall zu entwerfen.

ANMERKUNG 2 Die auszuführenden Gesamt-Sicherheitsfunktionen werden in dieser Phase nicht in technologiebezogenen Angaben festgelegt, da die Methoden und Maßnahmen der Ausführung der Gesamt-Sicherheitsfunktionen erst später bekannt sein werden. Während der Zuordnung der Anforderungen an die Gesamtsicherheit (siehe 7.6) kann die Beschreibung der Sicherheitsfunktionen unter Umständen geändert werden, um die spezielle Methode der Ausführung widerzuspiegeln.

BEISPIEL Beispiele für Gesamt-Sicherheitsfunktionen sind die Verhinderung des Übersteigens der Temperatur in Behälter X über 250 °C und die Verhinderung des Überschreitens der Geschwindigkeit von Antrieb Y über 3000 U/min.

7.5.2.2 Wenn Bedrohungen der IT-Sicherheit identifiziert worden sind, sollte eine Gefährdungsanalyse durchgeführt werden, um die Anforderungen zur IT-Sicherheit festzulegen.

ANMERKUNG Anleitung ist in ISO/IEC 13335 und IEC 62443 enthalten.

7.5.2.3 Für jede Gesamt-Sicherheitsfunktion muss eine Anforderung des Zielwerts der Sicherheitsintegrität bestimmt werden, die dazu führen wird, dass das tolerierbare Risiko erreicht wird. Jede Anforderung kann in quantitativer und/oder qualitativer Art und Weise bestimmt werden. Dies muss die Spezifikation der Anforderungen zur Gesamt-Sicherheitsintegrität bilden.

ANMERKUNG 1 Die Spezifikation der Anforderungen zur Gesamt-Sicherheitsintegrität ist eine Zwischenstufe zur Bestimmung der Ausfallgrenzwerte und der zugehörigen Sicherheits-Integritätslevel für die durch die sicherheitsbezogenen E/E/PE-Systemen zu implementierenden Sicherheitsfunktionen. Einige der qualitativen Methoden, die zur Bestimmung der Sicherheits-Integritätslevel (siehe IEC 61508-5, Anhänge D und E) verwendet werden, gehen direkt von den Risikoparametern auf die Sicherheits-Integritätslevel über. In solchen Fällen sind die Anforderungen zur Sicherheitsintegrität eher implizit, als im Einzelnen aufgeführt, da sie in der Methode selbst enthalten sind.

ANMERKUNG 2 Das EUC-Risiko kann entweder durch Verminderung der Auswirkungen des gefährlichen Vorfalls (dieses wird bevorzugt) oder durch Verminderung der Rate der gefährlichen Vorfälle vermindert werden, d. h. durch Verminderung der Rate gefahrbringender Ausfälle der EUC und des EUC-Leit- oder Steuerungssystems (aber siehe 7.5.2.4).

ANMERKUNG 3 Die erforderliche Verminderung der Häufigkeit des Schadensereignisses kann durch zusätzliche Maßnahmen erreicht werden, die sicherheitsbezogene E/E/PE-Systeme und/oder andere risikomindernde Maßnahmen, einschließlich sicherheitsbezogene Systeme anderer Technologie oder organisatorische Maßnahmen wie Fluchtmöglichkeiten, Betriebs- oder Aufenthaltsdauer, umfassen.

ANMERKUNG 4 Um dem Kriterium des tolerierbaren Risikos zu genügen, kann es bei der Bestimmung des Zielwerts der Sicherheitsintegrität für jede Sicherheitsfunktion notwendig sein, zu berücksichtigen, dass eine Person Risiken aus anderen Quellen ausgesetzt sein kann.

ANMERKUNG 5 Für Situationen, in denen eine anwendungsspezifische internationale Norm vorhanden ist, die angemessene Methoden für die direkte Bestimmung der Anforderungen zur Sicherheitsintegrität beinhaltet, können solche Normen verwendet werden, um die Anforderungen dieses Unterabschnitts zu erfüllen.

7.5.2.4 Die Anforderungen zur Gesamt-Sicherheitsintegrität müssen festgelegt werden, im Hinblick auf

- die erforderliche Risikominderung, um das tolerierbare Risiko zu erreichen; oder
- die tolerierbare Rate gefährlicher Vorfälle, um das tolerierbare Risiko zu erreichen.

7.5.2.5 Wenn bei der Beurteilung des EUC-Risikos angenommen wird, dass die Rate gefahrbringender Ausfälle des EUC-Leit- oder Steuerungssystems kleiner als 10^{-5} gefahrbringende Ausfälle pro Stunde ist, muss das EUC-Leit- oder Steuerungssystem als ein sicherheitsbezogenes System gemäß den Anforderungen dieser Norm betrachtet werden.

ANMERKUNG Wenn zum Beispiel eine Rate gefahrbringender Ausfälle zwischen 10^{-6} und 10^{-5} gefahrbringende Ausfälle pro Stunde für das EUC-Leit- oder Steuerungssystem in Anspruch genommen wird, dann wird das EUC-Leit- oder Steuerungssystem als ein sicherheitsbezogenes E/E/PE-System betrachtet und die Anforderungen gemäß Sicherheits-Integritätslevel 1 müssten erfüllt werden.

7.5.2.6 In Fällen, in denen Ausfälle des EUC-Leit- oder Steuerungssystems eine Anforderung an ein oder mehrere sicherheitsbezogene E/E/PE-Systeme und/oder andere risikomindernde Maßnahmen stellen und es nicht beabsichtigt ist, das EUC-Leit- oder Steuerungssystem als sicherheitsbezogenes System zu bezeichnen, müssen die folgenden Anforderungen zutreffen:

- a) die Rate gefahrbringender Ausfälle, die für das EUC-Leit- oder Steuerungssystem in Anspruch genommen wird, muss sich auf Daten stützen, die durch eine der folgenden Möglichkeiten erworben wurden:
 - aktuelle Betriebserfahrung zum EUC-Leit- oder Steuerungssystem in einer gleichartigen Anwendung;
 - eine Zuverlässigkeitsanalyse, die nach einem anerkannten Verfahren ausgeführt wurde;
 - eine industrielle Datenbank zur Zuverlässigkeit von allgemeinen Einrichtungen;
- b) die Rate gefahrbringender Ausfälle, die für das EUC-Leit- oder Steuerungssystem in Anspruch genommen werden kann, darf nicht kleiner als 10^{-5} gefahrbringende Ausfälle pro Stunde sein;

ANMERKUNG 1 Siehe 7.5.2.5.

- c) alle vernünftigerweise vorhersehbaren gefahrbringenden Ausfallarten des EUC-Leit- oder Steuerungssystems müssen bei der Entwicklung der Spezifikation der Anforderungen zur Gesamtsicherheit in Betracht gezogen werden;
- d) das EUC-Leit- oder Steuerungssystem muss unabhängig von den sicherheitsbezogenen E/E/PE-Systemen und anderen risikomindernden Maßnahmen sein.

ANMERKUNG 2 Vorausgesetzt, die sicherheitsbezogenen Systeme sind unter Berücksichtigung der normalen Anforderungsrate vom EUC-Leit- oder Steuerungssystem entworfen worden, um eine ausreichende Sicherheitsintegrität zu liefern, dann ist es nicht notwendig, das EUC-Leit- oder Steuerungssystem als sicherheitsbezogenes System zu bezeichnen (und daher werden seine Funktionen nicht als Sicherheitsfunktionen im Zusammenhang dieser Norm bezeichnet). In einigen Anwendungen, besonders dort wo eine sehr hohe Sicherheitsintegrität erforderlich ist, kann es angemessen sein, die Anforderungsrate dadurch zu reduzieren, dass das EUC-Leit- oder Steuerungssystem so entworfen wird, dass die Ausfallrate niedriger als normal ist. In solchen Fällen, wenn die beanspruchte Ausfallrate kleiner als der obere Grenzwert der Sicherheitsintegrität für Sicherheits-Integritätslevel 1 (siehe Tabelle 3) ist, wird das Leit- oder Steuerungssystem ein sicherheitsbezogenes System und die Anforderungen dieser Norm treffen zu.

7.5.2.7 Falls die Anforderungen aus 7.5.2.6 a) bis einschließlich d) nicht erfüllt werden können, muss das EUC-Leit- oder Steuerungssystem als sicherheitsbezogenes System bezeichnet werden. Der Sicherheits-Integritätslevel von Funktionen des EUC-Leit- oder Steuerungssystems muss von der Rate gefahrbringender

Ausfälle, die für das EUC-Leit- oder Steuerungssystem in Übereinstimmung mit Tabelle 3 (siehe Anmerkung 3) in Anspruch genommen wird, hergeleitet werden. In solchen Fällen müssen die Anforderungen dieser Norm entsprechend dem zugeordneten Sicherheits-Integritätslevel auf das EUC-Leit- oder Steuerungssystem angewendet werden.

ANMERKUNG Siehe 7.5.2.5 und ebenso 7.6.2.10.

7.6 Zuordnung der Anforderungen an die Gesamtsicherheit

ANMERKUNG Diese Phase entspricht Kasten 5 in Bild 2.

7.6.1 Ziele

7.6.1.1 Das erste Ziel der Anforderungen dieses Unterabschnitts ist es, die in der Spezifikation der Anforderungen zur Gesamtsicherheit (sowohl die Anforderungen zur Gesamt-Sicherheitsfunktion, als auch die Anforderungen zur Gesamt-Sicherheitsintegrität) enthaltenen Gesamt-Sicherheitsfunktionen den vorgesehenen sicherheitsbezogenen E/E/PE-Systemen und anderen risikomindernden Maßnahmen zuzuordnen.

ANMERKUNG Andere risikomindernde Maßnahmen werden notwendigerweise betrachtet, da die Zuordnung an die sicherheitsbezogenen E/E/PE-Systeme nicht erfolgen kann, wenn diese nicht berücksichtigt worden sind.

7.6.1.2 Das zweite Ziel der Anforderungen dieses Unterabschnitts ist es, jeder Sicherheitsfunktion, die von einem sicherheitsbezogenen E/E/PE-System ausgeführt werden soll, einen Ausfallgrenzwert und einen zugehörigen Sicherheits-Integritätslevel zuzuordnen.

7.6.2 Anforderungen

7.6.2.1 Die vorgesehenen sicherheitsbezogenen Systeme, die zum Erreichen der erforderlichen funktionalen Sicherheit eingesetzt werden müssen, müssen festgelegt werden. Das tolerierbare Risiko kann erreicht werden durch:

- sicherheitsbezogene E/E/PE-Systeme; und/oder
- andere risikomindernde Maßnahmen.

ANMERKUNG Diese Norm ist nur anwendbar, wenn das tolerierbare Risiko zumindest teilweise durch ein sicherheitsbezogenes E/E/PE-System erreicht wird.

7.6.2.2 Im Rahmen der Zuordnung der Gesamt-Sicherheitsfunktionen an die vorgesehenen sicherheitsbezogenen E/E/PE-Systeme und anderen risikomindernden Maßnahmen müssen die vorhandenen Fertigkeiten und Ressourcen in allen Phasen des Gesamt-Sicherheitslebenszyklus betrachtet werden.

ANMERKUNG 1 Die volle Tragweite der Anwendung sicherheitsbezogener Systeme, die komplexe Technologie verwenden, wird oft unterschätzt. So erfordert zum Beispiel die Realisierung von komplexer Technologie in allen Phasen, von der Spezifikation bis hin zum Betrieb und zur Instandhaltung, einen höheren Grad an Kompetenz. Die Verwendung von anderen, einfacheren technologischen Lösungen kann genauso effektiv sein und kann wegen der reduzierten Komplexität besondere Vorteile haben.

ANMERKUNG 2 Die Verfügbarkeit von Fertigkeiten und Ressourcen für Betrieb und Instandhaltung und die Betriebsumgebung können kritisch bezüglich des Erreichens der erforderlichen funktionalen Sicherheit während des tatsächlichen Betriebs sein.

7.6.2.3 Jede Gesamt-Sicherheitsfunktion mit ihrer nach 7.5 entwickelten, zugehörigen Anforderung zur Gesamt-Sicherheitsintegrität muss einer oder mehreren der vorgesehenen sicherheitsbezogenen E/E/PE-Systemen und/oder anderen risikomindernden Maßnahmen zugeordnet werden, damit das tolerierbare Risiko für die Sicherheitsfunktion erreicht wird. Diese Zuordnung ist iterativ und wenn sich herausstellt, dass das tolerierbare Risiko nicht erreicht werden kann, dann müssen die Spezifikationen für das EUC-Leit- oder Steuerungssystem, für die vorgesehenen sicherheitsbezogenen E/E/PE-Systeme und für die anderen risikomindernden Maßnahmen geändert und die Zuordnung wiederholt werden.

ANMERKUNG 1 Die Entscheidung, eine spezielle Gesamt-Sicherheitsfunktion einem oder mehreren sicherheitsbezogenen E/E/PE-Systemen oder anderen risikomindernden Maßnahmen zuzuordnen, hängt von einer Anzahl von Faktoren ab, jedoch insbesondere von deren Anforderung zur Gesamt-Sicherheitsintegrität. Je beschwerlicher die Anforderung zur Sicherheitsintegrität ist, desto wahrscheinlicher wird die Funktion auf mehr als ein sicherheitsbezogenes E/E/PE-System und/oder andere risikomindernde Maßnahmen geteilt werden.

ANMERKUNG 2 Bild 6 zeigt den Ansatz zur Zuordnung der Anforderungen an die Gesamtsicherheit.

7.6.2.4 Die in 7.6.2.3 beschriebene Zuordnung muss so erfolgen, dass alle Gesamt-Sicherheitsfunktionen zugeordnet werden und die Ausfallgrenzwerte für jede Sicherheitsfunktion definiert werden (gemäß den in 7.6.2.10 festgelegten Anforderungen).

7.6.2.5 Die Anforderungen zur Sicherheitsintegrität jeder Sicherheitsfunktion müssen festgelegt werden im Hinblick auf:

- die mittlere Wahrscheinlichkeit eines gefahrbringenden Ausfalls bei Anforderung der Sicherheitsfunktion für eine Betriebsart mit niedriger Anforderungsrate; oder
- die Rate gefahrbringender Ausfälle der Sicherheitsfunktion (h^{-1}) für eine Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung.

7.6.2.6 Die Zuordnung der Anforderungen zur Sicherheitsintegrität muss unter Verwendung angemessener Methoden zur Kombination von Wahrscheinlichkeiten ausgeführt werden.

ANMERKUNG 1 Die Zuordnung der Sicherheitsanforderungen kann in qualitativer und/oder quantitativer Art und Weise ausgeführt werden.

ANMERKUNG 2 Wenn mehrere sicherheitsbezogene E/E/PE-Systeme und/oder andere risikomindernde Maßnahmen notwendig sind, um das tolerierbare Risiko zu erreichen, hängt das tatsächlich erreichte Risiko von den systemischen Abhängigkeiten zwischen sicherheitsbezogenen E/E/PE-Systemen und/oder anderen risikomindernden Maßnahmen ab (siehe IEC 61508-5 (A.5.4) zu weiteren Einzelheiten in Bezug auf Abhängigkeiten und wie diese analysiert werden können).

7.6.2.7 Die Zuordnung muss unter Berücksichtigung der Möglichkeit von Ausfällen infolge gemeinsamer Ursache fortgeführt werden. Wenn das EUC-Leit- oder Steuerungssystem, die sicherheitsbezogenen E/E/PE-Systeme und anderen risikomindernden Maßnahmen für die Zuordnung als unabhängig behandelt werden müssen, dann:

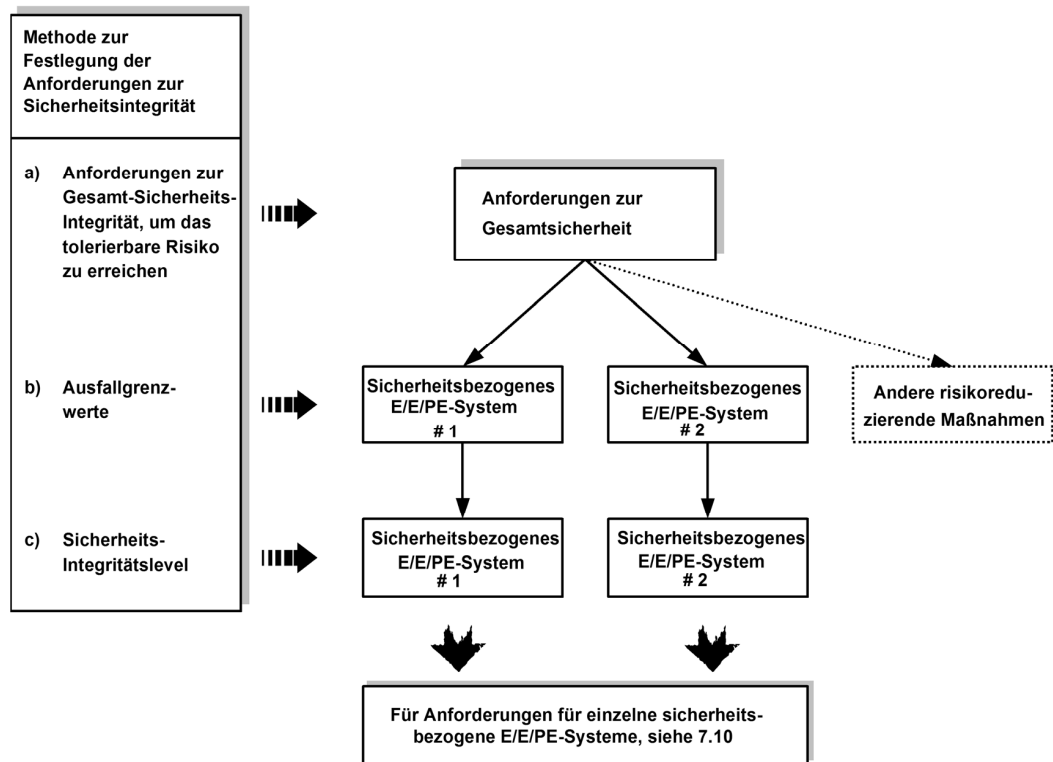
- müssen sie derart unabhängig sein, dass die Wahrscheinlichkeit gleichzeitiger Ausfälle von zwei oder mehreren dieser verschiedenen Systeme oder Maßnahmen ausreichend gering ist im Vergleich zur erforderlichen Sicherheitsintegrität;
- müssen sie funktional verschiedenartig sein (d. h. Verwendung vollständig verschiedener Lösungswege, um die gleichen Ergebnisse zu erzielen);
- müssen sie auf verschiedenartigen Technologien basieren (d. h. Verwendung unterschiedlicher Typen von Einrichtungen, um die gleichen Ergebnisse zu erzielen);

ANMERKUNG 1 Es muss berücksichtigt werden, dass für Systeme hoher Sicherheitsintegrität mit besonders schweren Auswirkungen bei einem Ausfall, trotz Verschiedenartigkeit der Technologien, besondere Vorsichtsmaßnahmen gegen Ereignisse gemeinsamer Ursachen mit geringer Wahrscheinlichkeit, wie zum Beispiel Flugzeugabstürze und Erdbeben, getroffen werden müssen.

- dürfen sie keine gemeinsamen Teile, Dienste oder Versorgungssysteme (zum Beispiel Stromversorgungen) verwenden, deren Ausfall zu einer gefahrbringenden Ausfallart aller Systeme führen kann;
- dürfen keine gemeinsamen Betriebs-, Instandhaltungs- oder Prüfverfahren verwendet werden.

ANMERKUNG 2 Diese Norm befasst sich im Besonderen mit der Ausführung der Sicherheitsanforderungen, die den sicherheitsbezogenen E/E/PE-Systemen zugeordnet werden. Es werden Anforderungen festgelegt, wie dieses erfolgen muss. Die Ausführung der Sicherheitsanforderungen, die anderen risikomindernden Maßnahmen zugeordnet werden, ist deshalb in dieser Norm nicht im Detail betrachtet.

Im Rahmen der Analyse gemeinsamer Ursachen müssen begrenzende und einschränkende Bedingungen für die Realisierung von sicherheitsbezogenen E/E/PE-Systemen wie der Aspekt notwendiger Trennung verschiedener Kanäle eines E/E/PE-Systems, Teilsystems oder Elements, zum Beispiel durch Abstand, überprüft werden – dies kann zum Beispiel dazu führen, zwei Kanäle/Mikroprozessoren auf einer Leiterplatte oder On-Chip-Redundanz (siehe IEC 61508-2, Anhang E) nicht zu erlauben.



ANMERKUNG 1 Mit jeder Gesamt-Sicherheitsfunktion sind vor der Zuordnung Anforderungen zur Gesamt-Sicherheitsintegrität verbunden (siehe 7.5.2.3).

ANMERKUNG 2 Eine Gesamt-Sicherheitsfunktion kann mehr als einem sicherheitsbezogenen System zugeordnet werden.

ANMERKUNG 3 Ein qualitativer Ansatz zur Bestimmung der Sicherheits-Integritätslevel umgeht die Festlegung der Anforderungen zur Sicherheitsintegrität als Ausfallgrenzwerte.

Bild 6 – Zuordnung der Anforderungen an die Gesamtsicherheit an die sicherheitsbezogenen E/E/PE-Systeme und anderen risikomindernden Maßnahmen

7.6.2.8 Können nicht alle Anforderungen in 7.6.2.7 erfüllt werden, dürfen die sicherheitsbezogenen E/E/PE-Systeme und die anderen risikomindernden Maßnahmen nicht als unabhängig in Bezug auf die Zuordnung der Sicherheit behandelt werden. Die Zuordnung muss stattdessen relevante Ausfälle infolge gemeinsamer Ursache zwischen dem EUC-Leit- oder Steuerungssystem, den sicherheitsbezogenen E/E/PE-Systemen und den anderen risikomindernden Maßnahmen berücksichtigen.

ANMERKUNG 1 Für weitere Informationen zur Analyse abhängiger Ausfälle siehe Hinweise [12] und [13] in den Literaturhinweisen.

ANMERKUNG 2 Ausreichende Unabhängigkeit ist geschaffen, wenn gezeigt wird, dass die Wahrscheinlichkeit eines abhängigen Ausfalls für die sicherheitsbezogenen E/E/PE-Systeme im Vergleich zu den Anforderungen zur Gesamt-Sicherheitsintegrität hinreichend gering ist (siehe 7.6.2.7).