

	DIN EN 61508-4 (VDE 0803-4)	DIN
	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.	VDE

ICS 01.040.35; 35.240.50

Einsprüche bis 2009-08-31

Entwurf

Vorgesehen als Ersatz für
DIN EN 61508-4
(VDE 0803-4):2002-11
Ersatz für
E DIN IEC 61508-4
(VDE 0803-4):2006-07

**Funktionale Sicherheit sicherheitsbezogener
elektrischer/elektronischer/programmierbarer elektronischer Systeme –
Teil 4: Begriffe und Abkürzungen
(IEC 65A/525/CDV:2008);
Deutsche Fassung FprEN 61508-4:2008**

Functional safety of electrical/electronic/programmable electronic safety-related systems –
Part 4: Definitions and abbreviations
(IEC 65A/525/CDV:2008);
German version FprEN 61508-4:2008

Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables
relatifs à la sécurité –
Partie 4: Définitions et abréviations
(CEI 65A/525/CDV:2008);
Version allemande FprEN 61508-4:2008

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 68 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 61508-4:2008 „Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 4: Begriffe und Abkürzungen“ (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/525/CDV:2008 „Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations“ unverändert in den Entwurf FprEN 61508-4:2008 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 beigefügt. 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 61508-4 (VDE 0803-4):2002-11 wurden folgende Änderungen vorgenommen:

- a) Aufnahme von Begriffen, die für die Behandlung der ASICs nach DIN EN 61508-2 (VDE 0803-2) erforderlich sind;
- b) Hinzufügung von Begriffen, die zur Beurteilung der Eigenschaften der systematischen Eignung der Software nach DIN EN 61508-3 (VDE 0803-3) erforderlich sind;
- c) neue Begriffe und neue Definitionen für vorhandene Begriffe zur Klarstellung der vorhandenen Anforderungen, wie z. B.: systematische Eignung, Gesamtsicherheitsfunktionen, Ausfall eines unbeteiligten Bauteils und Ausfall ohne Auswirkung.

Nationaler Anhang NA (informativ)

Zusammenhang mit Europäischen und Internationalen Normen

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

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

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

Tabelle NA.1

Europäische Norm	Internationale Norm	Deutsche Norm	Klassifikation im VDE-Vorschriftenwerk
–	IEC 60050(191):1990	a)	–
–	IEC 60051(351):2006	a)	–
FprEN61508-1:2008	65A/522/CDV:2008	E DIN EN 61805-1 (VDE 0803-1) in Vorbereitung	(VDE 0803-1)
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)
–	ISO/IEC Guide 51:1999	–	–
–	IEC Guide 104:1997	–	–
–	ISO/IEC 2382-14:1998	–	–
–	ISO 8402:1994	–	–
a) "Internationales Elektrotechnisches Wörterbuch - Deutsche Ausgabe", im Rahmen der Datenbankanwendung DIN-TERM zu beziehen über Beuth Verlag.			

Nationaler Anhang NB (informativ)

Literaturhinweise

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

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 Systeme*

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

Deutsche Fassung

Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer
Systeme –
Teil 4: Begriffe und Abkürzungen

Inhalt

	Seite
Einleitung	2
1 Anwendungsbereich	4
2 Normative Verweisungen	6
3 Begriffe und Abkürzungen	6
3.1 Sicherheitsbezogene Begriffe	8
3.2 Einrichtungen und Geräte	10
3.3 Systeme: allgemeine Aspekte	14
3.4 Systeme: sicherheitsbezogene Aspekte	16
3.5 Sicherheitsfunktionen und Sicherheitsintegrität	18
3.6 Fehler, Ausfall und Abweichung	21
3.7 Lebenszyklustätigkeiten	27
3.8 Bestätigung von Sicherheitsmaßnahmen	27
Literaturhinweise	32
Bilder	
Bild 1 – Gesamtrahmen der IEC 61508	5
Bild 2 – Programmierbares elektronisches System (PES): Struktur und Begriffe	15
Bild 3 – Elektrisch/elektronisch/programmierbares elektronisches System (E/E/PES): Struktur und Begriffe	15
Bild 4 – Ausfallmodell	23
Tabellen	
Tabelle 1 – In dieser Norm verwendete Abkürzungen	7

Einleitung

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

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

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

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

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

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

- legt Anforderungen für die Vermeidung und Beherrschung von systematischen Fehlern fest, die auf Erfahrung und Urteilsvermögen beruhen, das durch praktische Erfahrung in der Industrie gewonnen wurde. Wenn auch die Wahrscheinlichkeit des Auftretens systematischer Ausfälle im Allgemeinen nicht quantifiziert werden kann, erlaubt die Norm jedoch für eine festgelegte Sicherheitsfunktion den Anspruch zu erheben, dass der mit der Sicherheitsfunktion verbundene Ausfallgrenzwert als erreicht betrachtet werden kann, wenn alle Anforderungen dieser Norm erfüllt worden sind;
- lässt einen weiten Bereich von Prinzipien, Verfahren und Maßnahmen zu, um funktionale Sicherheit für sicherheitsbezogene E/E/PE-Systeme zu erreichen, verwendet aber nicht das Fail-Safe-Konzept, das genutzt werden kann, wenn das Ausfallverhalten eindeutig definiert und das Niveau der Komplexität verhältnismäßig niedrig ist. Das Fail-Safe-Konzept wurde wegen des weiten Bereiches der Komplexität von sicherheitsbezogenen E/E/PE-Systemen, die im Rahmen der Norm behandelt werden, als ungeeignet betrachtet.

1 Anwendungsbereich

1.1 Dieser Teil der IEC 61508 beinhaltet die Begriffe und Beschreibungen der Benennungen, die in den Teilen 1 bis 7 dieser Norm verwendet werden.

1.2 Die Begriffe sind unter allgemeinen Überschriften zusammengefasst, so dass verwandte Ausdrücke innerhalb des Zusammenhanges zueinander verstanden werden können. Jedoch sollte angemerkt werden, dass nicht beabsichtigt war, durch diese Überschriften den Definitionen eine Bedeutung hinzuzufügen.

1.3 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 nach IEC Guide 104 und ISO/IEC Guide 51 vorgesehen. Die Teile 1, 2, 3 und 4 sind ebenfalls zur Verwendung als eigenständige Norm vorgesehen. Die horizontale Sicherheitsfunktion dieser internationalen Norm trifft nicht auf medizinische Einrichtungen nach der Normenreihe IEC 60601 zu.

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

1.4 Bild 1 zeigt den gesamten Rahmen für die Teile 1 bis 7 der IEC 61508 und zeigt die Rolle, die IEC 61508-4 zum Erreichen der funktionalen Sicherheit der sicherheitsbezogenen E/E/PE-Systeme spielt.

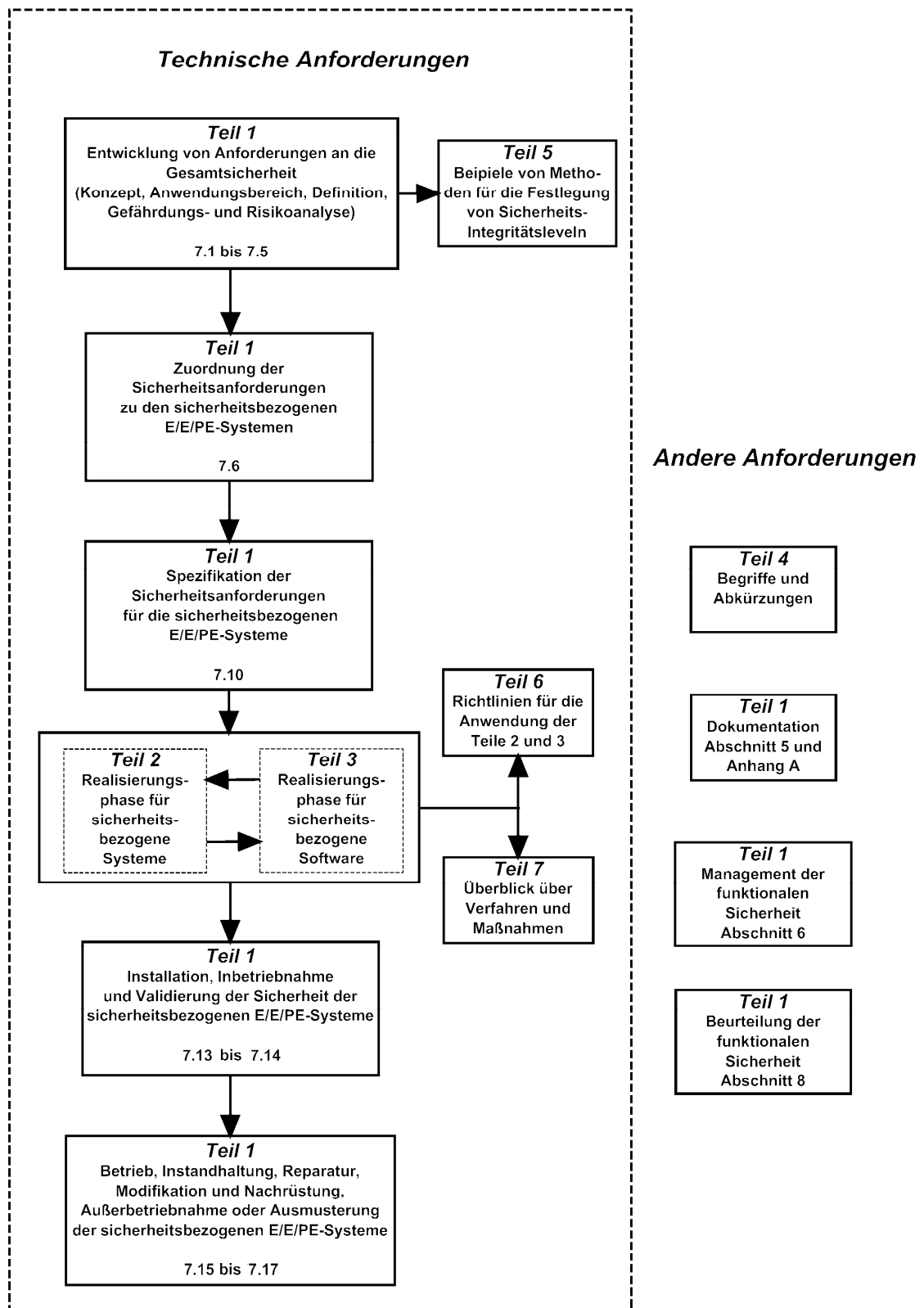


Bild 1 – Gesamtrahmen der IEC 61508

2 Normative Verweisungen

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

IEC 60050(191):1990, *International Electrotechnical Vocabulary (IEV) – Chapter 191: Dependability and quality of service*

IEC 60051(351):2006, *International Electrotechnical Vocabulary (IEV) – Chapter 351: Automatic control*

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

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

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

ANMERKUNG Für eine Einleitung 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].

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

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

ISO/IEC 2382-14:1998, *Data processing – Vocabulary – Part 14: Reliability, maintainability and availability*

ISO 8402:1994, *Quality management and quality assurance – Vocabulary*

3 Begriffe und Abkürzungen

Für die Anwendung dieser Internationalen Norm gelten die nachfolgenden Begriffe und die in Tabelle 1 aufgeführten Abkürzungen.

Tabelle 1 – In dieser Norm verwendete Abkürzungen

Abkürzung	Beschreibung	Definition und/oder Beschreibung der Benennung
ALARP	so niedrig wie vernünftigerweise möglich (en: as low as reasonably practicable)	IEC 61508-5, Anhang B
ASIC	anwendungsspezifischer integrierter Schaltkreis (en: application specific integrated circuit)	3.2.15
CPLD	komplexer programmierbarer Logikbaustein (en: complex programmable logic device)	
DC	Diagnosedeckungsgrad (en: diagnostic coverage)	3.8.6
€EPLD	(elektronisch) löscht- und programmierbarer Logikbaustein (en: (electrically) erasable programmable logic device)	
E/E/PE	elektrisch/elektronisch/programmierbar elektronisch (en: electrical/electronic/programmable electronic)	3.2.13, Beispiel: sicherheitsbezogenes E/E/PE-System
E/E/PES	elektrisch/elektronisch/programmierbar elektronisches System (en: electrical/electronic/programmable electronic system)	3.3.3
EEPROM	elektronisch löscht- und programmierbarer Festwertspeicher (en: electrically erasable and programmable read only memory)	
EPROM	löscht- und programmierbarer Festwertspeicher (en: erasable and programmable read only memory)	
EUC	EUC-Einrichtung (en: equipment under control)	3.2.1
FPGA	field programmable Gate-Array	
GAL	Generic Array Logic	
HFT	Hardware-Fehlertoleranz (en: hardware fault tolerance)	IEC 61508-2, 7.4.4
MooN	Architektur mit M aus N Kanälen (en: M out of N) (zum Beispiel ist 1oo2 eine Architektur mit 1 aus 2 Kanälen, wobei jeder der beiden Kanäle die Sicherheitsfunktion ausführen kann)	IEC 61508-6, Anhang B
MooND	Architektur mit M aus N Kanälen mit Diagnose	IEC 61508-6, Anhang B
PAL	Programmable Array Logic	
PE	programmierbar elektronisch (en: programmable electronic)	3.2.12
PES	programmierbares elektronisches System (en: programmable electronic system)	3.3.1
PFD	Wahrscheinlichkeit eines gefahrbringenden Ausfalls bei Anforderung (en: probability of dangerous failure on demand)	3.6.17
PFDavg	mittlere Wahrscheinlichkeit eines gefahrbringenden Ausfalls bei Anforderung (en: average probability of dangerous failure on demand)	3.6.18
PFH	mittlere Häufigkeit eines gefahrbringenden Ausfalls pro Stunde (en: average frequency of dangerous failure [h ⁻¹] per hour)	3.6.19

Tabelle 1 (fortgesetzt)

Abkürzung	Beschreibung	Definition und/oder Beschreibung der Benennung
PLA	programmierbare logische Anordnung (en: programmable logic array)	
PLD	programmierbarer Logikbaustein (en: programmable logic device)	
PLS	programmierbare logische Ablaufsteuerung (en: programmable logic sequencer)	
PML	programmierbare Makro-Logik (en: programmable macro logic)	
RAM	Speicher mit wahlfreiem Zugriff (en: random-access memory)	
ROM	Festwertspeicher (en: read-only memory)	
SFF	Anteil sicherer Ausfälle (en: safe failure fraction)	3.6.15
SIL	Sicherheits-Integritätslevel (en: safety integrity level)	3.5.8
SPS	Speicherprogrammierbare Steuerung (en: programmable logic controller, PLC)	IEC 61508-6, Anhang E
VHDL	Verilog Hardwarebeschreibungssprache (en: verilog hardware description language)	IEC 61508-2, Anhang F, Anmerkung 2

3.1 Sicherheitsbezogene Begriffe

3.1.1

Schaden

en: harm

physische Verletzung oder Schädigung der Gesundheit von Menschen oder Schädigung von Gütern oder der Umwelt

[ISO/IEC Guide 51:1999, Definition 3.3]

3.1.2

Gefährdung

en: hazard

potentielle Schadensquelle

[ISO/IEC Guide 51:1999, Definition 3.5]

ANMERKUNG Der Begriff schließt die Gefährdungen von Personen ein, die innerhalb einer kurzen Zeitspanne entstehen (zum Beispiel durch Feuer und Explosion), und auch die, die eine Langzeitwirkung auf die Gesundheit einer Person haben (zum Beispiel durch Freisetzung einer giftigen Substanz).

3.1.3

Gefährdungssituation

en: hazardous situation

Umstand, durch den Personen, Güter oder die Umwelt einer oder mehreren Gefährdungen oder gefährlichen Vorfällen ausgesetzt sind

[ISO/IEC Guide 51:1999, Definition 3.6, modifiziert]

3.1.4

gefährlicher Vorfall

en: hazardous event)

Vorfall, der zu einem Schaden führen kann

ANMERKUNG Ob ein gefährlicher Vorfall zu einem Schaden führt, hängt davon ab, ob Personen, Güter oder die Umwelt den Auswirkungen des gefährlichen Vorfalls ausgesetzt sind und im Fall von Schaden von Personen, ob irgendeine derart ausgesetzte Person den Auswirkungen des Vorfalls ausweichen kann, nachdem dieser aufgetreten ist.

3.1.5

Schadensereignis

en: harmful event

Ereignis, durch das eine Gefährdungssituation zu einem Schaden führt oder gefährlicher Vorfall, der zu einem Schaden führt

ANMERKUNG Aus ISO/IEC Guide 51, Definition 3.4 angepasst, um einen gefährlichen Vorfall zuzulassen.

3.1.6

Risiko

en: risk

Kombination aus der Wahrscheinlichkeit, mit der ein Schaden auftritt, und dem Ausmaß dieses Schadens

[ISO/IEC Guide 51:1999, Definition 3.2]

ANMERKUNG Für die weitere Diskussion dieses Begriffs siehe Anhang A der IEC 61508-5.

3.1.7

tolerierbares Risiko

en: tolerable risk

Risiko, das basierend auf den aktuellen gesellschaftlichen Wertvorstellungen in einem gegebenen Zusammenhang akzeptiert wird

[ISO/IEC Guide 51:1999, Definition 3.7]

ANMERKUNG Siehe Anhang B der IEC 61508-5.

3.1.8

Restrisiko

en: residual risk

das trotz Schutzmaßnahmen verbleibende Risiko

[ISO/IEC Guide 51:1999, Definition 3.9]

3.1.9

EUC-Risiko

en: EUC risk

Risiko, das durch die EUC oder seine Wechselwirkung mit dem EUC-Leit- oder Steuerungssystem entsteht

ANMERKUNG 1 Risiko ist in diesem Zusammenhang verbunden mit dem speziellen Schadensereignis, das durch sicherheitsbezogene E/E/PE-Systeme und andere risikomindernde Maßnahmen in ausreichender Weise zu vermindern ist (d. h. das Risiko, das mit der funktionalen Sicherheit verbunden ist).

ANMERKUNG 2 Das EUC-Risiko wird in Bild A.1 der IEC 61508-5 dargestellt. Der Hauptzweck der Bestimmung des EUC-Risikos ist die Festlegung eines Bezugspunkts für das Risiko, ohne Berücksichtigung sicherheitsbezogener E/E/PE-Systeme und anderer risikomindernder Maßnahmen.

ANMERKUNG 3 Die Beurteilung dieses Risikos schließt die damit verbundenen menschlichen Faktoren mit ein.

3.1.10

Grenzrisiko

en: target risk

Risiko, das vorgesehen ist, für eine spezielle Gefährdung unter Berücksichtigung des EUC-Risikos zusammen mit den sicherheitsbezogenen E/E/PE-Systemen und den anderen risikomindernden Maßnahmen erreicht zu werden

3.1.11

Sicherheit

en: safety

Freiheit von nicht akzeptiertem Risiko

[ISO/IEC Guide 51:1999, Definition 3.1]

3.1.12

funktionale Sicherheit

en: functional safety

Teil der Gesamtsicherheit, bezogen auf die EUC und das EUC-Leit- oder Steuerungssystem, der von der korrekten Funktion des sicherheitsbezogenen E/E/PE-Systems und anderer risikomindernder Maßnahmen abhängt

3.1.13

sicherer Zustand

en: safe state

Zustand der EUC, in dem die Sicherheit erreicht ist

ANMERKUNG Beim Übergang von einem potentiell gefährlichen Zustand zum endgültigen sicheren Zustand kann die EUC eine Anzahl von Sicherheits-Zwischenzuständen durchlaufen. Für einige Situationen existiert ein sicherer Zustand nur so lange, wie die EUC einer kontinuierlichen Steuerung unterliegt. Solch eine kontinuierliche Steuerung kann für einen kurzen oder einen unbestimmten Zeitraum erfolgen.

3.1.14

vernünftigerweise vorhersehbare Fehlanwendung

en: reasonably foreseeable misuse

Verwendung eines Produktes, Verfahrens oder einer Dienstleistung in einer Art, die von einem Lieferanten nicht vorgesehen ist, die sich jedoch aus leicht vorhersehbaren menschlichen Verhaltensweisen ergeben kann

[ISO/IEC Guide 51:1999, Definition 3.14]

3.2 Einrichtungen und Geräte

3.2.1

EUC-Einrichtung

en: equipment under control

EUC

Einrichtung, Maschine, Apparat oder Anlage, verwendet zur Fertigung, Stoffumformung, zum Transport, zu medizinischen oder anderen Tätigkeiten

ANMERKUNG Das EUC-Leit- oder Steuerungssystem ist getrennt und unterschiedlich zur EUC.

3.2.2

Umgebung

en: environment

alle relevanten Parameter, die das Erreichen der funktionalen Sicherheit in der spezifischen zu betrachtenden Anwendung und in jeder Phase des Sicherheitslebenszyklus beeinflussen können

ANMERKUNG Dies beinhaltet zum Beispiel die physikalische Umgebung, die Betriebsumgebung, die gesetzgebende Umgebung und die Umgebung der Instandhaltung.

3.2.3

Funktionseinheit

en: functional unit

Einheit aus Hardware oder Software oder beidem, die zur Durchführung einer angegebenen Aufgabe geeignet ist

[ISO/IEC 2382-14-01-01]

ANMERKUNG In IEC 191-01-01 wird die allgemeinere Benennung „Einheit“ an Stelle von Funktionseinheit verwendet. Eine Einheit kann manchmal Menschen einschließen.

3.2.4

Anwendung

en: application

die eher auf die EUC als auf das E/E/PE-System bezogene Aufgabe

3.2.5

Software

en: software

geistiges Produkt, das aus Programmen, Verfahren, Daten, Regeln und allen dazugehörigen Beschreibungen besteht, die zur Arbeit mit einem Datenverarbeitungssystem gehören

ANMERKUNG 1 Software ist unabhängig vom Medium, auf dem sie gespeichert ist.

ANMERKUNG 2 Diese Definition ohne Anmerkung 1 unterscheidet sich von ISO 2382-1 (Verweis [7] in den Literaturhinweisen) durch das hinzugefügte Wort „Daten“.

3.2.6

Systemsoftware

en: system software

Teil der Software eines PE-Systems, der sich auf die Funktion des programmierbaren Geräts selbst und die durch das programmierbare Gerät bereitgestellten Dienste bezieht, im Gegensatz zu der Anwendungssoftware, welche die Funktionen festlegt, die eine zu der EUC gehörende Aufgabe ausführt

ANMERKUNG Für Beispiele siehe IEC 61508-7.

3.2.7

Anwendungssoftware

en: application software

Anwendungsdaten

en: application data

Konfigurationsdaten

en: configuration data

der Teil der Software eines programmierbaren elektronischen Systems, der eher die Funktionen festlegt, die eine zu der EUC gehörende Aufgabe ausführt, als die Funktion des programmierbaren Geräts selbst und die durch das programmierbare Gerät bereitgestellten Dienste

3.2.8

bereits existierende Software

en: pre-existing software

ein Software-Element, das bereits existiert und nicht speziell für das laufende Projekt oder SRS entwickelt wurde

ANMERKUNG Die Software könnte ein handelsüblich verfügbares Produkt sein oder sie könnte von einer Organisation für ein vorheriges Produkt oder System entwickelt worden sein. Bereits existierende Software kann oder kann nicht in Übereinstimmung mit den Anforderungen dieser Norm entwickelt worden sein.

3.2.9

Daten

en: data

Informationen, die in einer Art und Weise dargestellt werden, die zur Kommunikation, Interpretation oder Verarbeitung durch Rechner geeignet ist

ANMERKUNG 1 Daten können die Form von statischen Informationen (zum Beispiel Konfiguration eines Sollwertes oder der Darstellung von geographischen Informationen) annehmen, oder sie können die Form von Anweisungen annehmen, um eine Abfolge von bereits existierenden Funktionen festzulegen.

ANMERKUNG 2 Für Beispiele siehe IEC 61508-7.

3.2.10

Online-Software-Hilfswerkzeug

en: software on-line support tool

ein Software-Werkzeug, das das SRS während seiner Laufzeit direkt beeinflussen kann

3.2.11

Offline-Software-Hilfswerkzeug

en: software off-line support tool

ein Software-Werkzeug, das eine Phase des Software-Entwicklungslebenszyklus unterstützt und das nicht das SRS während seiner Laufzeit direkt beeinflussen kann. Offline-Software-Werkzeuge können in die folgenden Klassen unterteilt werden:

- **T1**
erzeugt keine Ausgaben, die direkt oder indirekt zum ausführbaren Code (einschließlich Daten) des sicherheitsbezogenen Systems beitragen können;

ANMERKUNG Beispiele für T1 sind: ein Texteditor, ein Hilfswerkzeug zur Beschreibung der Anforderungen oder des Entwurfs ohne Möglichkeiten der automatischen Codegenerierung und Konfigurationsmanagementwerkzeuge.

- **T2**
unterstützt die Prüfung oder die Verifikation des Entwurfs oder ausführbaren Codes, wobei Abweichungen im Werkzeug zum Versagen der Fehlererkennung führen können, aber keine Abweichungen direkt in der ausführbaren Software erzeugen können;

ANMERKUNG Beispiele für T2 sind: eine Prüfeinrichtung mit Testgenerator, ein Werkzeug zur Messung der Testabdeckung und ein Werkzeug zur statischen Analyse.

- **T3**
erzeugt Ausgaben, die direkt oder indirekt zum ausführbaren Code (einschließlich Daten) des sicherheitsbezogenen Systems beitragen können.

ANMERKUNG Beispiele für T3 sind: ein Werkzeug zur Veränderung von Festwerten während des Betriebs des Systems; ein optimierender Compiler, bei dem die Beziehung zwischen dem Quelltext und dem erzeugten Objektcode nicht offensichtlich ist; ein Compiler, der ein ausführbares Laufzeitpaket in den ausführbaren Code einbindet.

3.2.12

Programmierbar elektronisch

en: programmable electronic

PE

auf Rechnertechnologie basierend, die aus Hardware, Software und aus Eingabe- und/oder Ausgabe-einheiten bestehen kann

ANMERKUNG Diese Benennung beinhaltet mikroelektronische Einrichtungen, basierend auf einer oder mehreren Zentraleinheiten (CPUs) zusammen mit zugehörigen Speichern usw.

BEISPIEL Die folgenden Geräte sind alle programmierbare elektronische Geräte:

- Mikroprozessoren;
- Mikrokontroller;
- programmierbare Steuerungen;
- Speicherprogrammierbare Steuerungen (SPS);
- anwendungsspezifische integrierte Schaltkreise (ASICs);
- andere rechnergestützte Einrichtungen (zum Beispiel intelligente Sensoren, Übertrager, Aktoren).

3.2.13

Elektrisch/elektronisch/programmierbar elektronisch

en: electrical/electronic/programmable electronic

E/E/PE

basierend auf elektrischer (E) und/oder elektronischer (E) und/oder programmierbarer elektronischer (PE) Technologie

ANMERKUNG Dieser Begriff umfasst alle Geräte oder Systeme, die auf elektrischen Prinzipien arbeiten.

BEISPIEL Elektrische/elektronische/programmierbare elektronische Geräte beinhalten:

- elektromechanische Einrichtungen (elektrisch);
- nichtprogrammierbare elektronische Einrichtungen (elektronisch);
- elektronische Einrichtungen basierend auf Rechnertechnologie (programmierbar elektronisch) – siehe 3.2.5.

3.2.14

Programmiersprache mit eingeschränktem Sprachumfang

en: limited variability language

Software-Programmiersprache für kommerzielle und industrielle programmierbare elektronische Steuerungen mit einem auf die spezielle Anwendung begrenzten Leistungsspektrum, deren Darstellungsart textuell oder graphisch ist oder Eigenschaften von beiden enthält

BEISPIEL Die folgenden Sprachen nach IEC 61131-3 (Verweis [8] in den Literaturhinweisen) und anderen Quellen sind solche mit eingeschränktem Sprachumfang, die für Anwendungsprogramme für ein SPS-System verwendet werden:

- Kontaktplan: eine graphische Sprache, die aus einer Serie aus Eingangssymbolen (die ein Verhalten wie das eines Öffners oder Schließers darstellen) besteht, die durch Linien mit Ausgangssymbolen (die den Stromfluss andeuten) verbunden sind (dargestellt durch ein Verhalten ähnlich denen von Relais);
- Boolesche Algebra: eine maschinennahe Sprache basierend auf booleschen Operatoren wie z. B. UND, ODER und NICHT mit der Fähigkeit, einige mnemonischen Anweisungen anzufügen;
- Funktionsbausteinsprache: erlaubt dem Anwender zusätzlich zu booleschen Operatoren die Verwendung komplizierterer Funktionen wie z. B. Datenübertragung, Blockübertragung Lesen/Schreiben, Schieberegister und sequentielle Anweisungen;
- Ablaufsprache: eine graphische Darstellung eines sequentiellen Programms, die aus miteinander verbundenen Schritten, Aktionen und gerichteten Verbindungen mit Transitionsbedingungen besteht.

3.2.15

Anwendungsspezifischer integrierter Schaltkreis

en: application specific integrated circuit

ASIC

integrierter Schaltkreis, der für spezielle Funktionen entworfen und hergestellt wird, wobei die Funktionalität durch den Produktentwickler definiert wird

ANMERKUNG Der allein stehende Begriff ASIC deckt alle Arten der nachfolgenden integrierten Schaltkreise ab.

- vollständig kundenspezifisches ASIC (en: full custom ASIC): ASIC mit einer durch den Produktentwickler definierten Funktionalität, wobei der Entwurf und die Herstellung ähnlich zu einem normalen integrierten Schaltkreis sind (siehe Anmerkung)

Ein normaler integrierter Schaltkreis wird in großen Stückzahlen hergestellt und kann für unterschiedliche Anwendungen verwendet werden. Funktionalität, Validierung, Produktion und Produktionstests sind ausschließlich in der Hand des Halbleiterherstellers. Manuelle Veränderungen und Optimierungen auf Layoutebene werden häufig durchgeführt, um die erforderliche Fläche zu verringern. Sie werden nicht für sicherheitsbezogene Systeme entworfen. Häufige Änderungen im Produktionsprozess, in der Verfahrenstechnik und im Layout sind zur Kosten- und Ertragsoptimierung sehr wahrscheinlich. Die Anzahl der Bauteile, die mit einer bestimmten Überarbeitung des Prozesses oder der Maske gefertigt wird, ist nicht öffentlich bekannt.

- Core-Based-ASIC (en: core based ASIC): ASIC basierend auf vorentworfenen oder generierten Makro-Cores, die durch zusätzliche Logik unterstützt werden

BEISPIEL 1 Standard-Mikroprozessor-Cores, Peripherie-Bauteile, Kommunikationsschnittstellen, Analogblöcke, I/O-Zellen mit speziellen Funktionen sind Beispiele für vorentworfenen Makros.

BEISPIEL 2 Eine Vielzahl ähnlicher Bauteile, wie in Beispiel 1 erwähnt, sind Beispiele für vorentworfenen Makros, die als geistiges Eigentum (en: Intellectual Property, IP) bekannt sind, mit dem Unterschied, dass die Entwurfsdaten aus einer Hardwarebeschreibungssprache (VHDL, Verilog), wie für Cell-Based-ASIC beschrieben, bestehen.

BEISPIEL 3 Embedded-RAM, -ROM, -EEPROM oder -FLASH sind Beispiele für generierte Makros. Für die generierten Blöcke wird angenommen, dass sie aufgrund eines auf Entwurfsregeln basierenden Aufbaus korrekt sind. Vorentworfenen oder generierten Makros sind prozessspezifisch, können aber auf unterschiedliche Technologien übertragen werden. In den meisten Fällen sind die Makro-Cores nicht mit den handelsüblichen Bauteilen identisch (unterschiedlicher Prozess, von Drittanbietern angeboten).

- Cell-Based-ASIC (en: cell based ASIC): ASIC basierend auf Logikprimitiven (wie UND, ODER, Flip-Flop, Latch) entnommen aus einer Zellbibliothek

Die Netzliste auf Gatterebene, welche die Logikprimitiven und die Verbindungen enthält, wird normalerweise von einer Hardwarebeschreibungssprache (VHDL, Verilog) unter Verwendung von Synthesewerkzeugen erzeugt. Die Funktions- und Timing-Eigenschaften der Logikprimitiven werden in der Zellbibliothek gekennzeichnet. Diese Parameter werden zum Betreiben des Synthesewerkzeugs und auch zur Simulation verwendet. Zusätzlich werden Entwurfswerkzeuge verwendet, um die Zellen zu platzieren und die Verbindungen zu verlegen.

- Gate-Array (en: gate array): vorgefertigte Halbleitermaster mit einer festgelegten Anzahl von Zellen, die einen gemeinsamen Ausgangspunkt für unterschiedliche Bauteile bereitstellen
Die Funktionalität wird durch die Verbindungsmatrix (Metall-Layer) zwischen den vorgefertigten Zellen definiert. Der Entwurfsprozess ist dem eines Cell-Based-ASIC sehr ähnlich, während der Entwurfsschritt durch einen Routing-Schritt ersetzt wird, um die bereits vorhandenen Zellen zu verbinden.
- field programmable Gate-Array (en: field programmable gate array, FPGA): standardisierter integrierter Schaltkreis mit einmal programmierbaren oder mehrfach programmierbaren Elementen, um die Verbindungen zwischen den Funktionsblöcken zu definieren und die Funktionalität der einzelnen Blöcke zu konfigurieren
Aufgrund der physikalischen Eigenschaften der programmierbaren Elemente ist es nicht möglich, einmal programmierbare FPGAs vollständig während der Produktion zu testen.
- programmierbarer Logikbaustein (en: programmable logic device, PLD): standardisierter integrierter Schaltkreis mit geringer oder mittlerer Komplexität mit einmal programmierbaren oder elektrisch löschbaren Elementen (Fuses), um die kombinatorische Logik, gewöhnlich basierend auf einer AND/OR-Matrix, und konfigurierbare Speicherelemente zu definieren
PLDs liefern aufgrund ihrer regelmäßigen Struktur ein voraussagbares Timing und eine garantierte maximale Arbeitsfrequenz im synchronen Entwurf.
Typen von PLDs sind zum Beispiel PAL, GAL, PML, (E)EPLD, PLA, PLS.
- komplexer programmierbarer Logikbaustein (en: complex programmable logic device, CPLD): mehrere PLD-ähnliche Blöcke auf einem einzelnen Chip, verbunden durch eine programmierbare Verbindungsmatrix (Crossbar)
Das programmierbare Logikelement ist in den meisten Fällen neu programmierbar (EPROM oder EEPROM).

3.3 Systeme: allgemeine Aspekte

3.3.1

Programmierbares elektronisches System

en: programmable electronic system

PES

System zur Steuerung, zum Schutz oder zur Überwachung, basierend auf einem oder mehreren programmierbaren elektronischen Geräten, einschließlich aller Elemente des Systems wie z. B. Energieversorgung, Sensoren und anderen Eingabegeräten, Datenverbindungen und anderen Kommunikationswegen sowie Aktoren und anderen Ausgabeeinrichtungen (siehe Bild 2)

ANMERKUNG Die Struktur eines PES zeigt Bild 2 a). Bild 2 b) zeigt, wie ein PES in dieser Internationalen Norm dargestellt wird, mit der programmierbaren Elektronik als eine Einheit getrennt von den Sensoren und Aktoren der EUC und ihren Schnittstellen; die programmierbare Elektronik könnte jedoch an mehreren Stellen im PES vorkommen. Bild 2 c) zeigt ein PES mit zwei getrennten Einheiten der programmierbaren Elektronik. Bild 2 d) zeigt ein PES mit zwei programmierbaren Elektroniken (d. h. zweikanalig), aber mit einem einkanaligen Sensor und einem einkanaligen Aktor.

3.3.2

Elektrisch/elektronisch/programmierbares elektronisches System

en: electrical/electronic/ programmable electronic system

E/E/PES

System zur Steuerung, zum Schutz oder zur Überwachung, basierend auf einem oder mehreren elektrischen/elektronischen/programmierbaren elektronischen (E/E/PE) Geräten, einschließlich aller Elemente des Systems wie z. B. Energieversorgung, Sensoren und anderen Eingabegeräten, Datenverbindungen und anderen Kommunikationswegen sowie Aktoren und anderen Ausgabeeinrichtungen (siehe Bild 3)

3.3.3

EUC-Leit- oder Steuerungssystem

en: EUC control system

System, das auf Eingangssignale des Prozesses und/oder eines Bedieners reagiert und Ausgangssignale erzeugt, welche die EUC in der gewünschten Art arbeiten lassen

ANMERKUNG Das EUC-Leit- oder Steuerungssystem schließt Eingabegeräte und Stellglieder ein.

3.3.4

Architektur

en: architecture

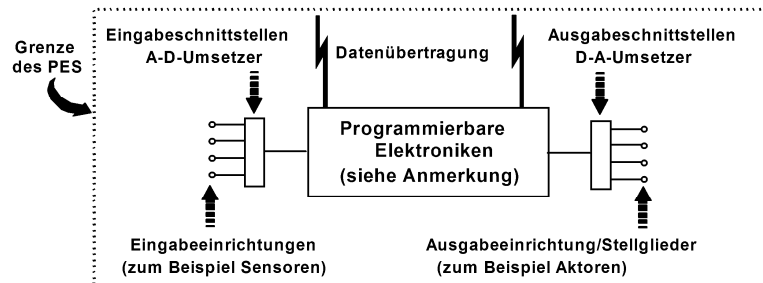
spezifische Konfiguration von Hardware- und Softwareelementen in einem System

3.3.5

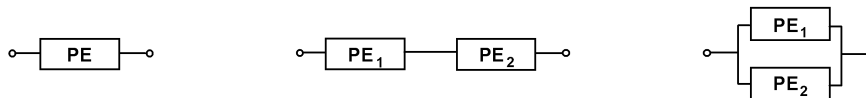
Softwaremodul

en: software module

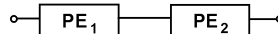
logische Einheit, die aus Unterprogrammen und/oder Datendeklarationen besteht und die mit anderen ebensolchen logischen Einheiten in Beziehung stehen kann



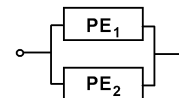
a) Basis-PES-Struktur



b) Ein PES mit einem programmierbaren elektronischen Gerät (d. h. ein PES bestehend aus einem Kanal der programmierbaren Elektroniken)



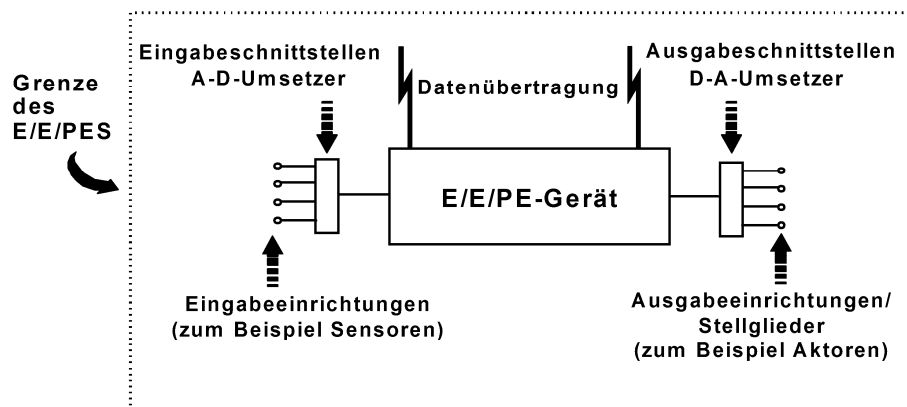
c) Ein PES mit zwei programmierbaren elektronischen Geräten seriell miteinander verbunden (zum Beispiel intelligente Sensoren und Speicherprogrammierbare Steuerungen)



d) Ein PES mit zwei programmierbaren elektronischen Geräten aber mit gemeinsamen Sensoren und Stellgliedern (d. h. ein PES bestehend aus zwei Kanälen programmierbarer Elektroniken)

ANMERKUNG Die programmierbaren Elektroniken werden zentral dargestellt, könnten sich aber auch in mehreren Teilen des PES befinden.

Bild 2 – Programmierbares elektronisches System (PES): Struktur und Begriffe



ANMERKUNG Das E/E/PE-Gerät ist zentral dargestellt, solche Geräte könnten sich aber auch in mehreren Teilen des E/E/PES befinden.

Bild 3 – Elektrisch/elektronisch/programmierbares elektronisches System (E/E/PES): Struktur und Begriffe

3.3.6

Kanal

en: channel

Element oder Gruppe von Elementen, die eine Funktion unabhängig ausführen

BEISPIEL Eine zweikanalige Konfiguration (oder doppelter Kanal) ist eine Konfiguration mit zwei Kanälen, welche die gleiche Funktion unabhängig voneinander ausführen.

ANMERKUNG 1 Die Elemente innerhalb eines Kanals können Eingabe-/Ausgabebaugruppen, ein Logiksystem (siehe 3.4.5), Sensoren und Aktoren beinhalten.

ANMERKUNG 2 Die Benennung kann verwendet werden, um ein vollständiges System oder ein Teil eines Systems (zum Beispiel Sensoren oder Aktoren) zu beschreiben.

3.3.7

Diversität

en: diversity

ungleichartige Mittel zur Ausführung einer geforderten Funktion

ANMERKUNG Diversität kann durch unterschiedliche physikalische Methoden oder unterschiedliche Lösungen für die gleiche Aufgabenstellung erreicht werden.

3.4 Systeme: sicherheitsbezogene Aspekte

3.4.1

sicherheitsbezogenes System

en: safety-related system

System, das sowohl

- die erforderlichen Sicherheitsfunktionen ausführt, die notwendig sind, um einen sicheren Zustand für die EUC zu erreichen oder aufrechtzuerhalten, als auch
- dazu vorgesehen ist, selbst oder mit anderen sicherheitsbezogenen E/E/PE-Systemen und anderen risikomindernden Maßnahmen die notwendige Sicherheitsintegrität für die geforderten Sicherheitsfunktionen zu erreichen

ANMERKUNG 1 Der Begriff bezieht sich auf jene Systeme, die als sicherheitsbezogene Systeme bezeichnet werden und die zusammen mit den anderen risikomindernden Maßnahmen (siehe 3.4.2) dazu vorgesehen sind, die notwendige Risikominderung zu erreichen, um das geforderte tolerierbare Risiko zu erreichen (siehe 3.1.7). Siehe auch Anhang A der IEC 61508-5.

ANMERKUNG 2 Sicherheitsbezogene Systeme werden entworfen, um die EUC am Übergang in einen gefahrbringenden Zustand zu hindern, indem in Abhängigkeit von Eingangsbefehlen eine angemessene Aktion eingeleitet wird. Der Ausfall des sicherheitsbezogenen Systems wird demnach zu den Ereignissen hinzugerechnet werden, die zu den festgestellten Gefährdungen führen. Obwohl es andere Systeme mit Sicherheitsfunktionen geben darf, sind es die sicherheitsbezogenen Systeme, die dazu bestimmt wurden, das geforderte tolerierbare Risiko zu erreichen. Sicherheitsbezogene Systeme können allgemein in sicherheitsbezogene Leit- oder Steuerungssysteme und sicherheitsbezogene Schutzsysteme eingeteilt werden.

ANMERKUNG 3 Sicherheitsbezogene Systeme dürfen Bestandteil des EUC-Leit- oder Steuerungssystems oder durch Sensoren und/oder Aktoren mit der EUC verbunden sein. Das heißt, der erforderliche Sicherheits-Integritätslevel darf durch in dem EUC-Leit- oder Steuerungssystem realisierte Sicherheitsfunktionen (und möglicherweise auch durch zusätzliche getrennte und unabhängige Systeme) erreicht werden, oder die Sicherheitsfunktionen dürfen von getrennten und unabhängigen Systemen durchgeführt werden, die der Sicherheit zugeordnet sind.

ANMERKUNG 4 Ein sicherheitsbezogenes System darf:

- a) dazu entworfen sein, um das Schadensereignis zu vermeiden (d. h., falls das sicherheitsbezogene System seine Sicherheitsfunktionen ausführt, entsteht kein Schadensereignis);
- b) dazu entworfen sein, um die Auswirkungen des Schadensereignisses zu mildern, so dass durch Reduzierung der Auswirkungen das Risiko reduziert wird;
- c) dazu entworfen sein, um eine Kombination von a) und b) zu erreichen.

ANMERKUNG 5 Eine Person kann Teil eines sicherheitsbezogenen Systems sein (siehe 3.4.1). Zum Beispiel könnte eine Person eine Information von einem programmierbaren elektronischen Gerät erhalten und aufgrund dieser eine Sicherheitshandlung oder eine Sicherheitshandlung über ein programmierbares elektronisches Gerät ausführen.

ANMERKUNG 6 Ein sicherheitsbezogenes System schließt alle Hardware-, Software- und Versorgungseinrichtungen (zum Beispiel Stromversorgung) ein, die notwendig sind, die angegebene Sicherheitsfunktion auszuführen (Sensoren, andere Eingabeeinrichtungen, Stellglieder (Aktoren). Andere Ausgabeeinrichtungen sind deshalb im sicherheitsbezogenen System eingeschlossen).

ANMERKUNG 7 Ein sicherheitsbezogenes System darf auf einem breiten Bereich von Technologien, einschließlich elektrisch, elektronisch, programmierbar elektronisch, hydraulisch und pneumatisch basieren.

3.4.2

andere risikomindernde Maßnahme

en: other risk reduction measure

Maßnahme, um das Risiko zu reduzieren oder zu mildern, das getrennt und verschieden von sicherheitsbezogenen E/E/PE-Systemen ist und diese nicht verwendet

BEISPIEL Ein Überdruckventil ist eine andere risikomindernde Maßnahme.

3.4.3

einfaches sicherheitsbezogenes E/E/PE-System

en: low complexity E/E/PE safety-related system

sicherheitsbezogenes E/E/PE-System (siehe 3.2.6 und 3.4.1), in dem:

- die Ausfallarten jedes einzelnen Bauteiles bekannt sind;
- das Verhalten des Systems unter Fehlerbedingungen vollständig bestimmt werden kann.

ANMERKUNG Das Verhalten des Systems unter Fehlerbedingungen kann durch analytische und/oder Prüfungsmethoden bestimmt werden.

BEISPIEL Ein System, das einen oder mehrere Grenztaster beinhaltet und möglicherweise über zwischengeschaltete elektromechanische Relais mit einem oder mehreren Kontakten einen elektrischen Motor spannungsfrei schaltet, ist ein einfaches sicherheitsbezogenes E/E/PE-System.

3.4.4

Teilsystem

en: subsystem

Einheit des Architekturentwurfs eines sicherheitsbezogenen Systems auf oberster Ebene, wobei ein gefahrbringender Ausfall des Teilsystems gemäß 3.6.7 (a) zu einem gefahrbringenden Ausfall der Sicherheitsfunktion gemäß 3.6.7 (a) führt

3.4.5

Element

en: element

Teil eines Teilsystems, das ein einzelnes Bauteil oder irgendeine Gruppe von Bauteilen umfasst, das eine oder mehrere Sicherheitsfunktionen des Elements ausführt

[IEC 62061, Definition 3.2.6, modifiziert]

ANMERKUNG Ein Element kann Hardware und/oder Software umfassen.

3.4.6

Redundanz

en: redundancy

Vorhandensein von mehr als den notwendigen Mitteln, damit eine Funktionseinheit eine geforderte Funktion ausführt oder damit Daten eine Information darstellen können

[ISO/IEC 2382-14-01-12]

BEISPIEL Verdoppelte Bauteile für eine Funktion und das Hinzufügen von Prüfbits (Paritätsbits) sind beides Beispiele für Redundanz.

ANMERKUNG 1 Redundanz wird hauptsächlich verwendet, um die Zuverlässigkeit (Wahrscheinlichkeit der richtigen Funktion über einen gegebenen Zeitraum) oder Verfügbarkeit (Wahrscheinlichkeit der Funktion zu einem gegebenen