DEUTSCHE NORM Entwurf Juni 2009

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

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

Entwurf

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

Preisgr. 10 K
VDE-Vertr.-Nr. 1803009

Einzelverkauf und Abonnements durch VDE VERLAG GMBH, 10625 Berlin
Einzelverkauf auch durch Beuth Verlag GmbH, 10772 Berlin

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

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.

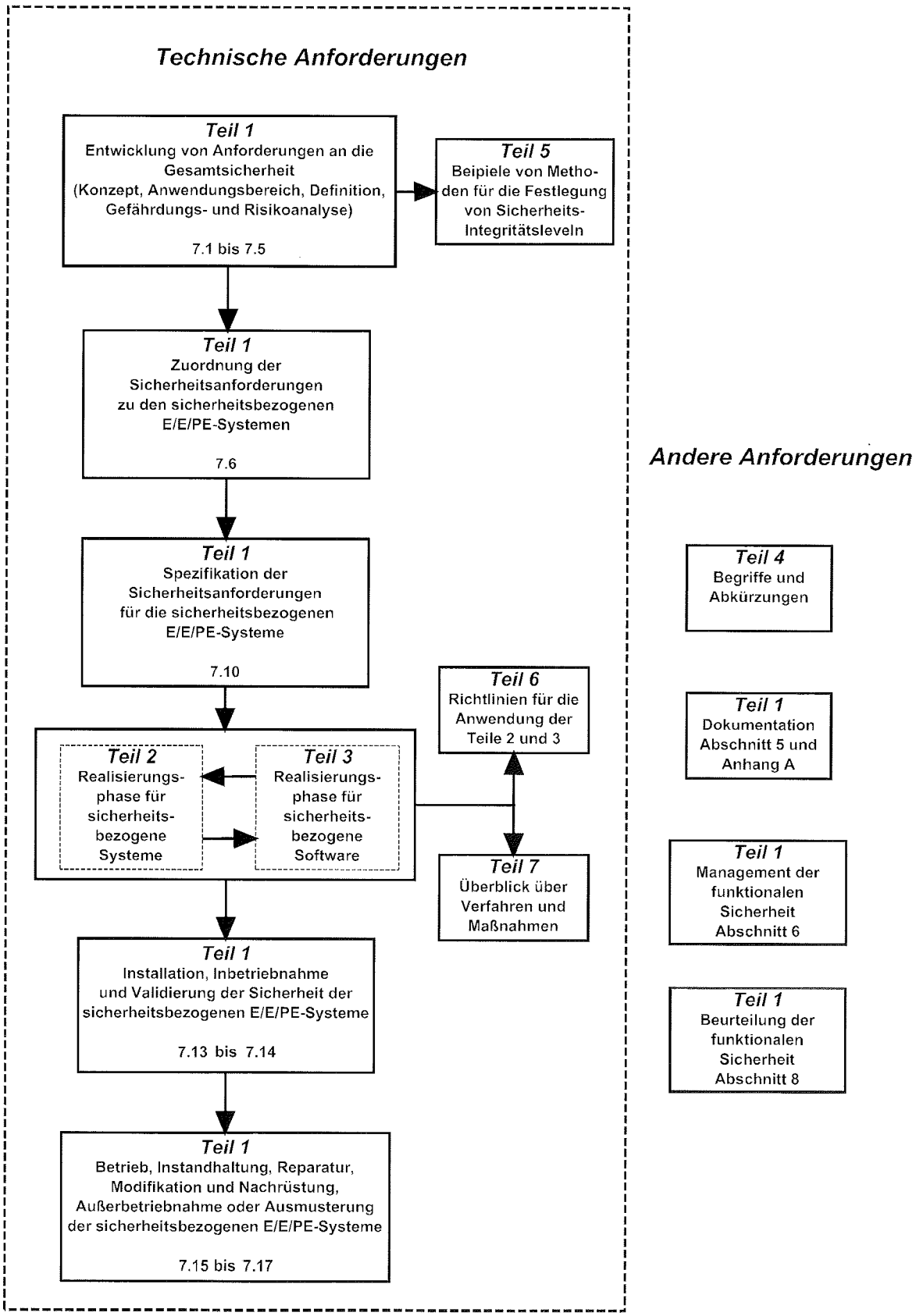


Bild 1 – Gesamtrahmen der IEC 61508

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) lösch- 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 lösch- und programmierbarer Festwertspeicher (en: electrically erasable and programmable read only memory)	
EPROM	lösch- 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 IEV 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 Ausgabeeinheiten 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 vorentworfene oder generierte 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 vorentworfene Makros.

  BEISPIEL 2 Eine Vielzahl ähnlicher Bauteile, wie in Beispiel 1 erwähnt, sind Beispiele für vorentworfene 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. Vorentworfene oder generierte Makros sind prozessspezifisch, können aber auf unterschiedliche Technologien übergetragen 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.

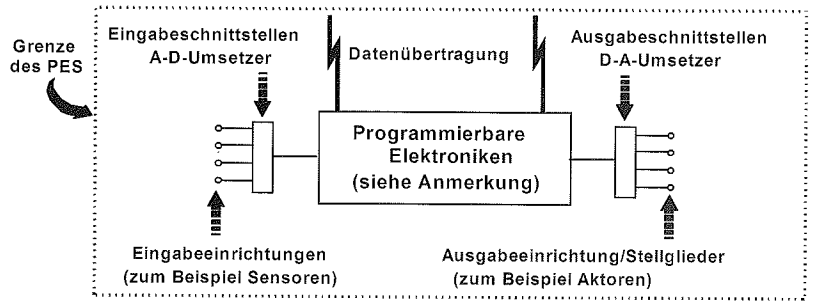
3.3.2
Elektrisch/elektronisch/programmierbares elektronisches System
en: electrical/electronic/ programmable electronic system
E/E/PES
System zur Steuerung, zum Schutz oder zur Überwachung, basierend auf einem oder mehreren elektrischen/elektronischen/programmierbaren elektronischen (E/E/PE) Geräten, 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

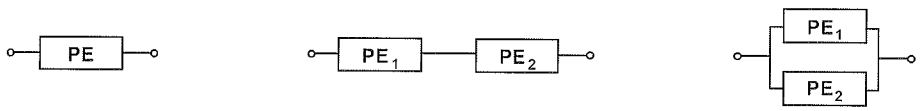
ANMERKUNG Das EUC-Leit- oder Steuerungssystem schließt Eingabegeräte und Stellglieder ein.

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



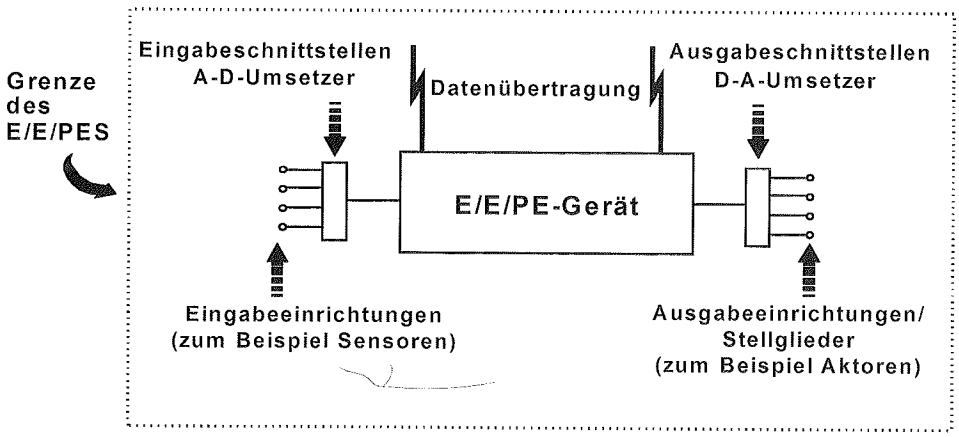
b) Ein PES mit einem programmierbaren elektronischen Gerät (d. h. ein PES bestehend aus einem Kanal der programmierbaren Elektroniken)

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

Moment) zu verbessern. Sie darf auch verwendet werden, um Fehlauslösungen durch Architekturen wie zum Beispiel 2oo3 zu minimieren.

ANMERKUNG 2 Die Definition in IEV 191-15-01 ist weniger vollständig.

ANMERKUNG 3 Redundanz darf „heiß" oder „aktiv" (alle redundanten Einheiten werden zur gleichen Zeit betrieben), „kalt" oder „in Bereitschaft" (nur eine der redundanten Einheiten wird zur gleichen Zeit betrieben) oder „gemischt" (eine oder mehrere Einheiten werden zur gleichen Zeit betrieben und eine oder mehrere Einheiten sind zur gleichen Zeit in Bereitschaft) sein.

3.5 Sicherheitsfunktionen und Sicherheitsintegrität

3.5.1
Sicherheitsfunktion
en: safety function
Funktion, die von einem sicherheitsbezogenen E/E/PE-System oder anderen risikomindernden Maßnahmen ausgeführt wird, und dazu vorgesehen ist, unter Berücksichtigung eines festgelegten gefährlichen Vorfalls (siehe 3.4.1) einen sicheren Zustand für die EUC zu erreichen oder aufrechtzuerhalten

BEISPIEL Beispiele von Sicherheitsfunktionen sind:

- Funktionen, die erforderlich sind, als positive Handlungen durchgeführt zu werden, um die Gefährdungssituationen zu vermeiden (zum Beispiel Ausschalten eines Motors); und
- Funktionen, die verhindern, dass Handlungen ausgeführt werden (zum Beispiel Verhinderung des Anlaufens eines Motors).

3.5.2
Gesamt-Sicherheitsfunktion
en: overall safety function
Mittel zum Erreichen oder Aufrechthalten eines sicheren Zustands der EUC unter Berücksichtigung eines festgelegten gefährlichen Vorfalls

3.5.3
Sicherheitsfunktion des Elements
en: element safety function
Funktion eines Elements, das zur Unterstützung einer Sicherheitsfunktion vorgesehen ist

ANMERKUNG Eine Sicherheitsfunktion des Elements kann eine festgelegte systematische Eignung (siehe 3.5.9) haben.

3.5.4
Sicherheitsintegrität
en: safety integrity
Wahrscheinlichkeit, dass ein sicherheitsbezogenes E/E/PE-System die festgelegten Sicherheitsfunktionen unter allen festgelegten Bedingungen innerhalb eines festgelegten Zeitraumes anforderungsgemäß ausführt

ANMERKUNG 1 Je höher der Sicherheits-Integritätslevel, umso geringer ist die Wahrscheinlichkeit, dass das sicherheitsbezogene System bei Vorliegen einer Anforderung die festgelegten Sicherheitsfunktionen nicht ausführen oder einen festgelegten Zustand nicht annehmen wird.

ANMERKUNG 2 Es gibt vier Stufen der Sicherheitsintegrität (siehe 3.5.8).

ANMERKUNG 3 Für die Bestimmung der Sicherheitsintegrität sollten alle Ursachen von Ausfällen (sowohl zufällige Hardwareausfälle als auch systematische Ausfälle), die zu einem nicht sicheren Zustand führen können, berücksichtigt werden, zum Beispiel Hardwareausfälle, Ausfälle durch Software und Ausfälle infolge elektrischer Störbeeinflussung. Einige dieser Ausfallarten, insbesondere zufällige Hardwareausfälle, können z. B. unter Verwendung der mittleren Häufigkeit von Ausfällen mit gefahrbringender Ausfallart oder der Ausfallwahrscheinlichkeit eines sicherheitsbezogenen Schutzsystems bei Anforderung quantifiziert werden. Die Sicherheitsintegrität hängt jedoch auch von vielen Faktoren ab, die nicht genau quantifiziert, sondern nur qualitativ betrachtet werden können.

ANMERKUNG 4 Die Sicherheitsintegrität beinhaltet die Sicherheitsintegrität der Hardware (siehe 3.5.7) und die systematische Sicherheitsintegrität (siehe 3.5.6).

ANMERKUNG 5 Diese Definition bezieht sich auf die Zuverlässigkeit der sicherheitsbezogenen Systeme, die Sicherheitsfunktionen auszuführen (siehe Definition der Zuverlässigkeit IEV 191-12-01).

3.5.5
Sicherheitsintegrität der Software
en: software safety integrity
Teil der Sicherheitsintegrität eines sicherheitsbezogenen Systems, der sich auf systematisches Versagen mit gefahrbringender Versagensart, die der Software zuordenbar ist, bezieht

3.5.6
systematische Sicherheitsintegrität
en: systematic safety integrity
Teil der Sicherheitsintegrität eines sicherheitsbezogenen Systems, der sich auf systematische Ausfälle mit gefahrbringender Ausfallart bezieht

ANMERKUNG Die systematische Sicherheitsintegrität kann üblicherweise nicht quantifiziert werden (zum Unterschied zur Sicherheitsintegrität der Hardware, bei der dies üblicherweise möglich ist).

3.5.7
Sicherheitsintegrität der Hardware
en: hardware safety integrity
Teil der Sicherheitsintegrität eines sicherheitsbezogenen Systems, der sich auf zufällige Hardwareausfälle mit gefahrbringender Ausfallart bezieht

ANMERKUNG Der Begriff bezieht sich auf Ausfälle mit gefahrbringender Ausfallart. Dieses sind die Ausfälle eines sicherheitsbezogenen Systems, welche die Sicherheitsintegrität beeinträchtigen können. Die in diesem Zusammenhang relevanten zwei Parameter sind die mittlere Häufigkeit von gefahrbringenden Ausfällen und die Wahrscheinlichkeit eines Ausfalls im Anforderungsfall. Der erste Zuverlässigkeitsparameter wird verwendet, wenn es notwendig ist, eine kontinuierliche Steuerung aufrechtzuerhalten, um Sicherheit zu erreichen, der zweite Zuverlässigkeitsparameter wird im Zusammenhang mit sicherheitsbezogenen Schutzsystemen verwendet.

3.5.8
Sicherheits-Integritätslevel
en: safety integrity level
SIL
eine von vier diskreten Stufen, die einem Wertebereich der Sicherheitsintegrität entsprechen, wobei der Sicherheits-Integritätslevel 4 die höchste Stufe der Sicherheitsintegrität und der Sicherheits-Integritätslevel 1 die niedrigste darstellt

ANMERKUNG 1 Die Ausfallgrenzwerte (siehe 3.5.15) für die vier Sicherheits-Integritätslevel sind in den Tabellen 2 und 3 der IEC 61508-1 festgelegt.

ANMERKUNG 2 Sicherheits-Integritätslevel werden zur Festlegung der Anforderungen zur Sicherheitsintegrität der Sicherheitsfunktionen, die dem sicherheitsbezogenen E/E/PE-System zugeordnet werden, verwendet.

ANMERKUNG 3 Ein Sicherheits-Integritätslevel (SIL) ist keine Eigenschaft eines Systems, Teilsystems, Elements oder Bauteils. Die korrekte Deutung der Redensart "sicherheitsbezogenes System mit SILn" (wobei n 1, 2, 3 oder 4 ist) ist, dass das System möglicherweise fähig ist, Sicherheitsfunktionen mit einem Sicherheits-Integritätslevel bis zu n zu unterstützen.

3.5.9
systematische Eignung
en: systematic capability
Maß des Vertrauens (ausgedrückt auf einer Skala von SIL 1 bis SIL 4), dass die systematische Sicherheitsintegrität eines Elements den Anforderungen des festgelegten SILs hinsichtlich der festgelegten Sicherheitsfunktion des Elements entspricht, wenn das Element in Übereinstimmung mit den in dem Sicherheitshandbuch des konformen Elements festgelegten Anweisungen angewendet wird

ANMERKUNG 1 Die systematische Eignung wird mit Bezug auf die Anforderungen zur Vermeidung und Beherrschung von systematischen Fehlern bestimmt (siehe IEC 61508-2 und IEC 61508-3).

ANMERKUNG 2 Es wird von der Natur des Elements abhängen, was ein relevanter systematischer Ausfallmechanismus ist. Für ein Element, das nur Software enthält, müssen zum Beispiel nur Mechanismen zum Softwareversagen betrachtet werden. Für ein Element, das Hardware und Software enthält, wird es notwendig sein, Mechanismen zum systematischen Hardwareausfall und zum Softwareversagen zu betrachten.

ANMERKUNG 3 Eine systematische Eignung eines Elements für SIL X hinsichtlich der festgelegten Sicherheitsfunktion des Elements bedeutet, dass die systematische Sicherheitsintegrität für SIL X erreicht ist, wenn das Element in Übereinstimmung mit den in dem Sicherheitshandbuch des konformen Elements festgelegten Anweisungen angewendet wird.

3.5.10
Software-Sicherheits-Integritätslevel
en: software safety integrity level
systematische Eignung eines Software-Elements, dass Teil eines Teilsystems eines sicherheitsbezogenen Systems darstellt

ANMERKUNG SIL kennzeichnet die Gesamt-Sicherheitsfunktion, aber nicht irgendeine der verschiedenen Teilsysteme oder Elemente, die diese Sicherheitsfunktion unterstützen. Daher hat Software gemeinsam mit irgendeinem Element keinen eigenständigen SIL. Jedoch ist es zweckmäßig, über "SIL X Software" zu sprechen, mit der Bedeutung "Software, in die Vertrauen gerechtfertigt ist (ausgedrückt auf einer Skala von 1 bis 4), dass die Sicherheitsfunktion des (Software-) Elements nicht wegen relevanter systematischer Versagensmechanismen versagen wird, wenn das (Software-) Element in Übereinstimmung mit den in dem Sicherheitshandbuch des konformen Elements festgelegten Anweisungen angewendet wird".

3.5.11
Spezifikation der Anforderungen zu den E/E/PE-Sicherheitsfunktionen
en: E/E/PE safety functions requirements specification
Spezifikation der Anforderungen an die Sicherheitsfunktionen, die vom sicherheitsbezogenen System ausgeführt werden müssen

ANMERKUNG 1 Diese Spezifikation ist ein Teil (der Sicherheitsfunktions-Teil) der Spezifikation der E/E/PE-Sicherheitsanforderungen (siehe IEC 61508-1, 7.10 und 7.10.2.6) und enthält die genauen Einzelheiten der Sicherheitsfunktionen, die vom sicherheitsbezogenen System auszuführen sind.

ANMERKUNG 2 Spezifikationen dürfen in Text, Flussdiagrammen, Matrizen, Logikdiagrammen usw. vorliegen, vorausgesetzt, die Sicherheitsfunktionen sind eindeutig dargestellt.

3.5.12
Spezifikation der Anforderungen zur Sicherheitsintegrität des E/E/PE-Systems
en: E/E/PE system safety integrity requirements specification
Spezifikation der Anforderungen zur Sicherheitsintegrität der Sicherheitsfunktionen, die vom sicherheitsbezogenen System ausgeführt werden müssen

ANMERKUNG Diese Spezifikation ist ein Teil (der Sicherheitsintegritäts-Teil) der Spezifikation der Sicherheitsanforderungen des E/E/PE-Systems (siehe IEC 61508-1, 7.10 und 7.10.2.7).

3.5.13
sicherheitsbezogene Software
en: safety-related software
Software, die zur Durchführung von Sicherheitsfunktionen in einem sicherheitsbezogenen System verwendet wird

3.5.14
Betriebsart
en: mode of operation
Art der Verwendung einer Sicherheitsfunktion, welche entweder sein kann:

- **Betriebsart mit niedriger Anforderungsrate (en: low demand mode):** wobei die Sicherheitsfunktion nur auf Anforderung ausgeführt wird, um die EUC in einen festgelegten sicheren Zustand zu überführen und wobei die Häufigkeit von Anforderungen nicht mehr als einmal pro Jahr beträgt; oder

ANMERKUNG Das sicherheitsbezogene E/E/PE-System, das die Sicherheitsfunktion ausführt, hat normalerweise keinen Einfluss auf die EUC oder das EUC-Leit- oder Steuerungssystem, bis eine Anforderung auftritt. Wenn das sicherheitsbezogene E/E/PE-System ausfällt, so dass es nicht die Sicherheitsfunktion ausführen kann, dann kann es jedoch die EUC veranlassen, in einen sicheren Zustand zu wechseln (siehe IEC 61508-2, 7.4.6).

- **Betriebsart mit hoher Anforderungsrate (en: high demand mode):** wobei die Sicherheitsfunktion nur auf Anforderung ausgeführt wird, um die EUC in einen festgelegten sicheren Zustand zu überführen und wobei die Häufigkeit von Anforderungen mehr als einmal pro Jahr beträgt; oder
- **Betriebsart mit kontinuierlicher Anforderung (en: continuous mode):** wobei die Sicherheitsfunktion die EUC in einem sicheren Zustand als Teil des normalen Betriebs hält.

3.5.15
Ausfallgrenzwert
en: target failure measure
zu unterschreitender Grenzwert der Wahrscheinlichkeit gefahrbringender Ausfallarten, der aufgrund der Anforderungen zur Sicherheitsintegrität festgelegt wird als:

- mittlere Wahrscheinlichkeit eines gefahrbringenden Ausfalls der Sicherheitsfunktion bei Anforderung (in der Betriebsart mit niedriger Anforderungsrate);
- mittlere Häufigkeit gefahrbringender Ausfällen [h-1] (in der Betriebsart mit hoher Anforderungsrate oder in der Betriebsart mit kontinuierlicher Anforderung)

ANMERKUNG Die Zahlenwerte für die Ausfallgrenzwerte werden in den Tabellen 2 und 3 der IEC 61508-1 angegeben.

3.5.16
notwendige Risikominderung
en: necessary risk reduction
zu erreichende Risikominderung durch die sicherheitsbezogenen E/E/PE-Systeme und/oder andere risikomindernde Maßnahmen, um sicherzustellen, dass das tolerierbare Risiko nicht überschritten wird

3.6 Fehler, Ausfall und Abweichung

3.6.1
Fehler
en: fault
nicht normale Bedingung, die eine Verminderung oder den Verlust der Fähigkeit einer Funktionseinheit verursachen kann, eine geforderte Funktion auszuführen

[ISO/IEC 2382-14-01-10]

ANMERKUNG IEV 191-05-01 definiert "Fehlzustand" als den Zustand einer Einheit, in dem sie unfähig ist, eine geforderte Funktion zu erfüllen, wobei die durch Instandhaltung oder andere geplante Handlungen bzw. durch das Fehlen äußerer Mittel verursachte Funktionsfähigkeit ausgeschlossen ist. Siehe Bild 4 für eine Darstellung dieser zwei Standpunkte.

3.6.2
Fehlervermeidung
en: fault avoidance
Verwendung von Techniken und Verfahren mit dem Ziel, die Entstehung von Fehlern während jeder Phase des Sicherheitslebenszyklus des sicherheitsbezogenen Systems zu vermeiden

3.6.3
Fehlertoleranz
en: fault tolerance
Fähigkeit einer Funktionseinheit, eine geforderte Funktion bei Bestehen von Fehlern oder Abweichungen weiter auszuführen

[ISO/IEC 2382-14-04-06]

ANMERKUNG Die Definition in IEV 191-15-05 bezieht sich nur auf die Teilmenge der Fehler in Untereinheiten. Siehe die Anmerkung zum Begriff Fehler in 3.6.1.

3.6.4
Ausfall
en: failure
Versagen
Beendigung der Fähigkeit einer Funktionseinheit, eine geforderte Funktion bereitzustellen oder Betrieb einer Funktionseinheit in irgendeiner Art anders als gefordert

ANMERKUNG 1 Dies basiert auf IEV 191-04-01 mit Änderungen, um systematische Ausfälle durch zum Beispiel Unzulänglichkeiten in der Spezifikation oder Software zu berücksichtigen.

ANMERKUNG 2 Für die Beziehung zwischen Fehlern und Ausfällen, sowohl in IEC 61508 als auch IEV 60050(191) siehe Bild 4.

ANMERKUNG 3 Die Ausführung geforderter Funktionen schließt notwendigerweise bestimmte Verhalten aus, und einige Funktionen dürfen derart spezifiziert werden, dass sie ein bestimmtes Verhalten vermeiden. Das Eintreten solch eines Verhaltens ist dann ein Ausfall.

ANMERKUNG 4 Ausfälle sind entweder zufällig (in Hardware) oder systematisch (in Hardware oder Software), siehe 3.6.5 und 3.6.6.

3.6.5
zufälliger Hardwareausfall
en: random hardware failure
Ausfall, der zu einem zufälligen Zeitpunkt auftritt und der aus einem oder mehreren möglichen Mechanismen in der Hardware resultiert, die zu einer Verschlechterung der Eigenschaften der Bauteile führen

ANMERKUNG 1 Es gibt viele Mechanismen der Verschlechterung, die mit unterschiedlicher Häufigkeit in verschiedenen Bauteilen auftreten. In ihrer Folge treten Bauteilausfälle aufgrund von Fertigungstoleranzen nach unterschiedlichen Betriebszeiten auf. Ausfälle von Einrichtungen, die viele Bauteile enthalten, treten in vorhersagbaren Häufigkeiten, aber zu unbestimmten (d. h. zufälligen) Zeiten auf.

ANMERKUNG 2 Ein wichtiges Unterscheidungsmerkmal zwischen zufälligen Hardwareausfällen und systematischen Ausfällen (siehe 3.6.6) ist, dass Systemausfallraten (oder andere angemessene Kenngrößen), die aus zufälligen Hardwareausfällen herrühren, mit vernünftiger Genauigkeit vorausgesagt werden können, systematische Ausfälle aber schon von Natur aus nicht genau vorausgesagt werden können. Das heißt, dass Systemausfallraten, die aus zufälligen Hardwareausfällen herrühren, mit vernünftiger Genauigkeit quantifiziert werden können, aber diejenige, die durch systematische Ausfälle entstehen, statistisch nicht genau quantifiziert werden können, weil die Ereignisse, die zu diesen führen, nicht leicht vorausgesagt werden können.

3.6.6
Versagen
systematischer Ausfall
en: systematic failure
Systematisches Versagen[NA1)]/Ausfall, bei dem eindeutig auf eine Ursache geschlossen werden kann, die nur durch eine Modifikation des Entwurfs oder des Fertigungsprozesses, der Art und Weise des Betreibens, der Bedienungsanleitung oder anderer Einflussfaktoren beseitigt werden kann

[IEV 191-04-19]

ANMERKUNG 1 Eine Instandsetzung ohne derartige Modifikation beseitigt in der Regel nicht die Ausfallursache.

ANMERKUNG 2 Ein systematischer Ausfall kann gezielt durch Simulation der Ausfallursache ausgelöst werden.

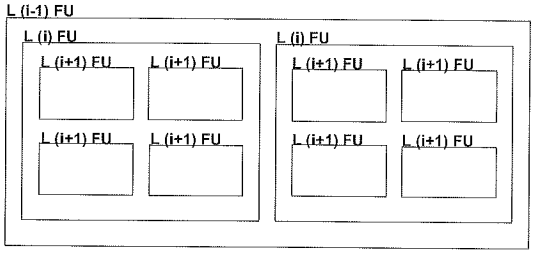
ANMERKUNG 3 Beispiele von Ursachen für systematische Ausfälle schließen menschliches Versagen ein in:

- der Spezifikation der Sicherheitsanforderungen;
- dem Entwurf, der Herstellung, dem Einbau, dem Betrieb der Hardware;
- dem Entwurf, der Implementierung der Software usw.

ANMERKUNG 4 In dieser Norm werden Ausfälle in einem sicherheitsbezogenen System in zufällige Hardwareausfälle eingeteilt oder

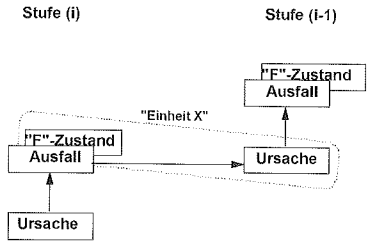
---

NA1) Nationale Fußnote: Bei systematischem Versagen, beispielsweise in Zusammenhang mit Software, steht in den Normen der Reihe DIN EN 61508 (VDE 0803) vorzugsweise „Versagen" statt „Ausfall".

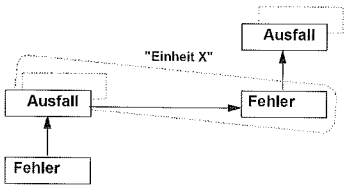


(L = Stufe; i = 1, 2, 3 usw.; FU = funktionale Einheit)

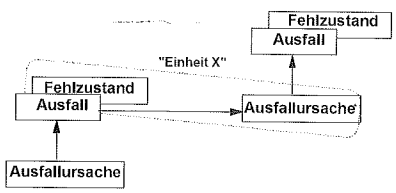
a) Konfiguration einer funktionalen Einheit



b) Allgemeine Ansicht



c) Ansicht nach IEC 61508 und ISO/IEC 2382-14



d) Ansicht nach IEC 60050-191

ANMERKUNG 1 Wie in a) gezeigt, kann eine Funktionseinheit als eine hierarchische Zusammenstellung verschiedener Ebenen betrachtet werden. Jede hiervon kann wiederum eine Funktionseinheit genannt werden. In Ebene (i) kann sich eine "Ursache" als eine Abweichung (vom korrekten Wert oder Zustand) innerhalb dieser Funktionseinheit der Ebene (i) offenbaren und, falls sie nicht berichtigt oder umgangen wird, einen Ausfall dieser Funktionseinheit verursachen. Daraufhin fällt diese in den Zustand "F", wo sie nicht länger fähig ist, eine geforderte Funktion (siehe b)) auszuführen. Dieser "F"-Zustand der Funktionseinheit der Ebene (i) kann sich wiederum als eine Abweichung in der Funktionseinheit der Stufe (i-1) offenbaren und, falls sie nicht berichtigt oder umgangen wird, einen Ausfall dieser Funktionseinheit der Ebene (i-1) verursachen.

ANMERKUNG 2 In dieser Ursachen- und Wirkungskette kann die gleiche Einheit ("Einheit X") als ein Zustand ("F"-Zustand) der Funktionseinheit der Ebene (i) betrachtet werden, in den sie als Ergebnis ihres Ausfalls gefallen ist und auch als Ursache eines Ausfalls der Funktionseinheit der Ebene (i-1). Diese "Einheit X" kombiniert die Konzepte der "Fehler" nach IEC 61508 und ISO/IEC 2382-14, welche den Ursachenaspekt betonen, wie in c) dargestellt, und den Aspekt des "Fehlzustands" nach IEC 60050(191), wo die Zustandsaspekte betont sind, wie in d) dargestellt. Der "F"-Zustand wird nach IEC 60050(191) Fehlzustand genannt, während er nach IEC 61508 und ISO/IEC 2382-14 nicht definiert ist.

ANMERKUNG 3 In einigen Fällen kann ein Ausfall oder eine Abweichung durch ein externes Ereignis, wie z. B. Blitz oder elektrostatischer Entladung, statt durch einen internen Fehler verursacht werden. Ebenso kann ein Fehler (nach der vorliegenden Norm) oder ein Fehlzustand (nach IEC 60050(191)) ohne einen vorherigen Ausfall bestehen. Ein Beispiel hierfür ist ein Entwurfsfehler.

Bild 4 – Ausfallmodell

3.6.7
gefahrbringender Ausfall
en: dangerous failure

Ausfall eines Elements und/oder Teilsystems und/oder Systems, das Anteil an der Ausführung der Sicherheitsfunktion hat, der

a) verhindert, dass eine Sicherheitsfunktion bei Anforderung ausgeführt wird (Anforderungs-Betriebsart) oder den Ausfall einer Sicherheitsfunktion verursacht (Betriebsart mit kontinuierlicher Anforderung), so dass die EUC in einen gefährlichen oder möglicherweise gefährlichen Zustand gebracht wird; oder,

b) die Wahrscheinlichkeit vermindert, die Sicherheitsfunktion bei Anforderung ordnungsgemäß auszuführen.

3.6.8
ungefährlicher Ausfall
en: safe failure
Ausfall eines Elements und/oder Teilsystems und/oder Systems, das Anteil an der Ausführung der Sicherheitsfunktion hat, der

a) zu einem fehlerhaften Betrieb der Sicherheitsfunktion führt, die EUC (oder Teile davon) in einen sicheren Zustand zu bringen oder den sicheren Zustand aufrechtzuerhalten; oder
b) die Wahrscheinlichkeit des fehlerhaften Betriebs der Sicherheitsfunktion erhöht, die EUC (oder Teile davon) in einen sicheren Zustand zu bringen oder den sicheren Zustand aufrechtzuerhalten.

3.6.9
abhängiger Ausfall
en: dependent failure
Ausfall, dessen Wahrscheinlichkeit nicht als das einfache Produkt der Wahrscheinlichkeiten der individuellen Ereignisse, die ihn verursachten, ausgedrückt werden kann

ANMERKUNG Zwei Ereignisse A und B sind nur dann abhängig, wenn gilt: $P(A \text{ und } B) > P(A) \times P(B)$.

3.6.10
Ausfall infolge gemeinsamer Ursache
en: common cause failure
Ausfall, der das Ergebnis eines oder mehrerer Ereignisse ist, die gleichzeitige Ausfälle von zwei oder mehreren getrennten Kanälen in einem mehrkanaligen System verursachen und zu einem Systemausfall führen

3.6.11
Abweichung
en: error
Nichtübereinstimmung zwischen Rechenergebnissen, beobachteten oder gemessenen Werten oder Beschaffenheiten und den betreffenden wahren, spezifizierten oder theoretisch richtigen Werten oder Beschaffenheiten

ANMERKUNG Aus IEV 191-05-24 mit Ausnahme der Anmerkungen.

3.6.12
Soft-Error
en: soft-error
fehlerhafte Veränderungen von Dateninhalten, jedoch keine Veränderungen des physikalischen Schaltkreises selbst

ANMERKUNG 1 Wenn sich ein Soft-Error ereignet hat und die Daten neu geschrieben werden, wird der Schaltkreis in seinen ursprünglichen Zustand zurückgesetzt.

ANMERKUNG 2 Soft-Errors können im Speicher, digitaler Logik, analogen Schaltkreisen und auf Übertragungsleitungen usw. auftreten. Sie sind vorherrschend in Halbleiter-Speicher einschließlich Registern und Latches.

ANMERKUNG 3 Soft-Errors sind transient und sollten nicht mit Programmierfehlern in der Software verwechselt werden.

3.6.13
Ausfall eines unbeteiligten Bauteils
en: no part failure
Ausfall eines Bauteils, das keinen Anteil an der Ausführung der Sicherheitsfunktion hat

ANMERKUNG Der Ausfall eines unbeteiligten Bauteils wird in der Berechnung der SFF nicht berücksichtigt.

3.6.14
Ausfall ohne Auswirkung
en: no effect failure
Ausfall eines Elements, das einen Anteil an der Ausführung der Sicherheitsfunktion hat und keine direkte Auswirkung auf die Sicherheitsfunktion hat

ANMERKUNG 1 Der Ausfall ohne Auswirkung hat definitionsgemäß keine Auswirkung auf die Sicherheitsfunktion, er kann also nicht zur Ausfallrate der Sicherheitsfunktion beitragen.

ANMERKUNG 2 Der Ausfall ohne Auswirkung wird in der Berechnung der SFF nicht berücksichtigt.

3.6.15
Anteil sicherer Ausfälle
en: safe failure fraction
SFF
Eigenschaft eines sicherheitsbezogenen Elements, die durch das Verhältnis der mittleren Ausfallrate ungefährlicher plus gefahrbringender erkannter Ausfälle und ungefährlicher plus gefahrbringender Ausfälle definiert wird. Dieses Verhältnis wird durch die folgende Gleichung dargestellt:

$SFF = (\Sigma\lambda_{S\,avg} + \Sigma\lambda_{Dd\,avg})/(\Sigma\lambda_{S\,avg} + \Sigma\lambda_{Dd\,avg} + \Sigma\lambda_{Du\,avg})$

wenn die Ausfallraten auf konstanten Ausfallraten basieren, kann die Gleichung vereinfacht werden zu:

$SFF = (\Sigma\lambda_S + \Sigma\lambda_{Dd})/(\Sigma\lambda_S + \Sigma\lambda_{Dd} + \Sigma\lambda_{Du})$

3.6.16
Ausfallrate
en: failure rate
Zuverlässigkeitsparameter ($\lambda(t)$) einer Einheit (einzelne Bauteile oder Systeme) derart, dass $\lambda(t).dt$ die Ausfallwahrscheinlichkeit dieser Einheit innerhalb [t, t+dt] ist, vorausgesetzt, dass sie während [0, t] nicht ausgefallen ist

ANMERKUNG 1 Mathematisch ist □(t) die bedingte Ausfallwahrscheinlichkeit pro Zeiteinheit über [t, t+dt]. Sie steht in starker Beziehung mit der Zuverlässigkeitsfunktion (d. h. Wahrscheinlichkeit keines Ausfalls von 0 bis t) durch die allgemeine Formel: $R(t) = \exp(-\int_0^t \lambda(\tau)d\tau$. Umgekehrt wird sie durch die Zuverlässigkeitsfunktion definiert mit: $\lambda(t) = -\frac{dR(t)}{dt}\frac{1}{R(t)}$.

ANMERKUNG 2 Ausfallraten und ihre Unsicherheiten können aus Rückläufern aus dem Feld unter Anwendung herkömmlicher Statistiken abgeschätzt werden. Während der „Gebrauchsdauer" (d.h. nach den Früh- und vor den Spätausfällen) ist die Ausfallrate eines einfachen Objekts mehr oder weniger konstant: □(t) ≡ □.

ANMERKUNG 3 Das Mittel von $\lambda(t)$ über eine gegebene Zeitdauer [0, T]: $\lambda_{avg}(T) = (\int_0^T \lambda(\tau)d\tau)/T$ ist keine Ausfallrate, weil es nicht zur Berechnung von R(t), wie in Anmerkung 1 gezeigt, verwendet werden kann. Es darf jedenfalls als mittlere Häufigkeit von Ausfällen über diese Zeitdauer (d.h. als PFH, siehe Teil 6 Anhang B) interpretiert werden.

ANMERKUNG 4 Die Ausfallrate von einer Serie von Objekten ist die Summe der Ausfallraten von jedem Objekt.

ANMERKUNG 5 Die Ausfallrate von redundanten Systemen ist üblicherweise nicht konstant. Wenn alle Ausfälle schnell erkannt werden, unabhängig und schnell repariert werden, nähert sich $\lambda(t)$ trotzdem schnell einem asymptotischen Wert λ_{as} an, der die äquivalente Ausfallrate des Systems ist. Sie sollte nicht mit der mittleren Ausfallrate, wie in Anmerkung 3 beschrieben, verwechselt werden, welche sich notwendigerweise nicht einem asymptotischen Wert nähert.

3.6.17
Wahrscheinlichkeit eines gefahrbringenden Ausfalls bei Anforderung
en: probability of dangerous failure on demand
PFD
sicherheitsbezogene Nichtverfügbarkeit (siehe IEC 60050-191) eines sicherheitsbezogenen E/E/PE-Systems, die festgelegte Sicherheitsfunktion auszuführen, wenn von der EUC oder dem EUC-Leit- oder Steuerungssystem eine Anforderung erfolgt

ANMERKUNG 1 Die [momentane] Nichtverfügbarkeit ist (laut IEC 60050-191) die Wahrscheinlichkeit, dass ein Objekt nicht in der Lage ist, eine erforderliche Funktion unter gegebenen Bedingungen zu einem gegebenen Moment auszuführen, in der Annahme, dass die erforderlichen externen Betriebsmittel zur Verfügung stehen. Sie ist allgemein bekannt durch U(t).

ANMERKUNG 2 Die [momentane] Verfügbarkeit ist nicht abhängig vom Zustand (laufend oder ausgefallen) des Objekts vor t. Sie charakterisiert ein Objekt, das nur arbeitsfähig sein muss, wenn dies erforderlich ist, zum Beispiel ein sicherheitsbezogenes E/E/PE-System betrieben in der Betriebsart mit niedriger Anforderungsrate.

ANMERKUNG 3 Wenn periodisch getestet, wird die PFD eines sicherheitsbezogenen E/E/PE-Systems hinsichtlich der festgelegten Sicherheitsfunktion mit einer Sägezahnkurve mit einem weiten Bereich von Wahrscheinlichkeiten im Intervall von niedrig, kurz nach einem Test, zu einem Maximum, kurz vor einem Test, dargestellt.

3.6.18
Mittlere Wahrscheinlichkeit eines gefahrbringenden Ausfalls bei Anforderung
en: average probability of dangerous failure on demand
PFDavg
mittlere Nichtverfügbarkeit (siehe IEC 60050-191) eines sicherheitsbezogenen E/E/PE-Systems, die festgelegte Sicherheitsfunktion auszuführen, wenn von der EUC oder dem EUC-Leit- oder Steuerungssystem eine Anforderung erfolgt

ANMERKUNG 1 Die mittlere Nichtverfügbarkeit über ein gegebenes Zeitintervall [t1, t2] ist allgemein bekannt durch U(t1, t2).

ANMERKUNG 2 Zwei Arten von Ausfällen tragen zur PFD und PFDavg bei: die gefahrbringenden unerkannten Ausfälle, die seit der letzten Wiederholungsprüfung aufgetreten sind, und die echten Ausfälle bei Anforderung selbst, verursacht durch die Anforderungen (Wiederholungsprüfungen und Sicherheitsanforderungen). Die erste ist zeitabhängig und durch ihre Rate gefahrbringender Ausfälle □DU(t) charakterisiert, während die zweite nur von der Anzahl der Anforderungen abhängig ist und durch eine Wahrscheinlichkeit eines Ausfalls pro Anforderung (bezeichnet mit □) charakterisiert wird.

ANMERKUNG 3 Weil echte Ausfälle „bei Anforderung" nicht durch Tests erkannt werden können, ist es notwendig, sie zu identifizieren und sie bei der Berechnung der Ausfallgrenzwerte zu berücksichtigen.

3.6.19
Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde
en: probability of dangerous failure per hour
PFH
mittlere Häufigkeit eines gefahrbringenden Ausfalls über einen gegebenen Zeitraum eines sicherheitsbezogenen E/E/PE-Systems, die festgelegte Sicherheitsfunktion auszuführen

ANMERKUNG 1 Der Begriff „Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde" wird in dieser Norm nicht verwendet, aber die Abkürzung PFH wurde beibehalten. Wenn sie verwendet wird, bedeutet sie „mittlere Häufigkeit eines gefahrbringenden Ausfalls [h-1]".

ANMERKUNG 2 Theoretisch ist die PFH der Mittelwert der unbedingten Ausfalldichte auch Ausfall-Häufigkeit genannt und wird allgemein mit w(t) bezeichnet. Sie sollte nicht mit der Ausfallrate verwechselt werden (siehe Teil 6 Anhang B).

ANMERKUNG 3 Wenn das sicherheitsbezogene E/E/PE-System die höchste Sicherheitsschicht ist, sollte die PFH aus ihrer Unzuverlässigkeit F(T)=1-R(T) berechnet werden (siehe Ausfallrate oben). Wenn es nicht das höchste sicherheitsbezogene System ist, muss seine PFH aus seiner Nichtverfügbarkeit U(t) (siehe PFH oben) berechnet werden. Näherungswerte für PFH werden durch F(T)/T und 1/MTTF im ersten Fall und 1/MTBF im zweiten Fall gegeben.

ANMERKUNG 4 Wenn das sicherheitsbezogene E/E/PE-System nur schnell erkannte und reparierte Ausfälle beinhaltet, dann wird eine asymptotische Ausfallrate □as schnell erreicht. Sie liefert eine Abschätzung der PFH.

3.6.20
Diagnose-Testintervall
en: diagnostic test interval
Zeitraum zwischen Online-Prüfungen, um Fehler in einem sicherheitsbezogenen System mit spezifiziertem Diagnosedeckungsgrad zu entdecken

3.6.21
Prozess-Sicherheitszeit
en: process safety time
Zeitspanne zwischen dem Auftreten eines Ausfalls der EUC oder des EUC-Leit- oder Steuerungssystems mit dem Potential, einen gefährlichen Vorfall zu verursachen, und dem Zeitpunkt, bei dem die Handlung in der EUC abgeschlossen sein muss, um das Auftreten des gefährlichen Vorfalls zu verhindern

3.7 Lebenszyklustätigkeiten

3.7.1
Sicherheitslebenszyklus
en: safety lifecycle
notwendige Tätigkeiten im Rahmen der Realisierung von sicherheitsbezogenen Systemen während eines Zeitraumes, der mit der Konzeptphase eines Projektes beginnt und endet, wenn alle sicherheitsbezogene E/E/PE-Systeme und andere risikomindernde Maßnahmen nicht mehr für die Verwendung verfügbar sind

ANMERKUNG 1 Der Begriff "funktionaler Sicherheitslebenszyklus" ist genauer, aber das Adjektiv "funktional" wird in diesem Fall im Zusammenhang mit dieser Norm als nicht notwendig betrachtet.

ANMERKUNG 2 Die Modelle des Sicherheitslebenszyklus, die in dieser Norm verwendet werden, werden in den Bildern 2, 3 und 4 der IEC 61508-1 spezifiziert.

3.7.2
Software-Lebenszyklus
en: software lifecycle
Tätigkeiten während eines Zeitraumes, der mit der Softwareentwicklung beginnt und endet, wenn die Software dauerhaft außer Betrieb genommen wird

ANMERKUNG 1 Ein Software-Lebenszyklus schließt typischerweise die Anforderungsphase, Entwicklungsphase, Erprobungsphase, Integrationsphase, Installationsphase und die Modifikationsphase ein.

ANMERKUNG 2 Software lässt sich nicht instand halten, sondern wird modifiziert.

3.7.3
Konfigurationsmanagement
en: configuration management
Verfahren zur Identifikation der Einheit eines zu entwickelnden Systems zum Zweck der Lenkung von Veränderungen an diesen Bauteilen und zur Aufrechterhaltung von Kontinuität und Rückverfolgbarkeit während des Lebenszyklus

ANMERKUNG Für Details zum Software-Konfigurationsmanagement siehe IEC 61508-7.

3.7.4
Basiskonfiguration
en: configuration baseline
die Informationen, die es ermöglichen, die Softwareausgabe in einer auditierbaren und systematischen Art zu erstellen, einschließlich: gesamter Quelltext, Daten, Laufzeitdateien, Dokumentation, Konfigurationsdateien und Installationsanweisungen, die eine Softwareausgabe beinhaltet; Informationen über Compiler, Betriebssysteme und Entwicklungswerkzeuge, die verwendet werden, um eine Softwareausgabe zu erstellen

3.7.5
Einflussanalyse
en: impact analysis
Tätigkeit zur Bestimmung des Einflusses, den eine Änderung einer Funktion oder eines Bauteils des Systems auf andere Funktionen oder Bauteile im System oder auf andere Systeme haben kann

ANMERKUNG Im Zusammenhang mit Software siehe C.5.23 der IEC 61508-7.

3.8 Bestätigung von Sicherheitsmaßnahmen

3.8.1
Verifikation
en: verification
Bestätigen aufgrund einer Untersuchung und durch Bereitstellung eines Nachweises, dass die Anforderungen erfüllt worden sind

ANMERKUNG 1 Aus ISO 8402, angepasst durch Weglassen der Anmerkungen.

ANMERKUNG 2 In Zusammenhang mit dieser Norm ist Verifikation die Tätigkeit, die in jeder Phase des relevanten Sicherheitslebenszyklus (Gesamt, E/E/PES und Software) durch Analyse, mathematische Schlussfolgerung und/oder Prüfung darlegt, dass für die speziellen Eingaben die Ergebnisse in jeder Hinsicht die Ziele und Anforderungen erfüllen, die für diese Phase festgelegt wurden.

BEISPIEL Zu den Tätigkeiten der Verifikation gehören:

- die Überprüfungen der Ergebnisse (Dokumente aus allen Phasen des Sicherheitslebenszyklus), um unter Berücksichtigung der jeweiligen Eingaben der Phase die Übereinstimmung mit den Zielen und Anforderungen der Phase sicherzustellen;
- Entwurfsüberprüfungen;
- ausgeführte Prüfungen an entwickelten Produkten, um sicherzustellen, dass sie gemäß ihrer Spezifikation arbeiten;
- Ausführung von Integrationsprüfungen, wobei unterschiedliche Teile eines Systems Schritt für Schritt zusammengesetzt und Prüfungen unter Umgebungsbedingungen durchgeführt werden, um sicherzustellen, dass alle Teile in der spezifizierten Art zusammenarbeiten.

3.8.2
Validierung
en: validation
Bestätigen aufgrund einer Untersuchung und durch Bereitstellung eines Nachweises, dass die besonderen Anforderungen für eine spezielle beabsichtigte Verwendung erfüllt worden sind

ANMERKUNG 1 Aus ISO 8402, angepasst durch Weglassen der Anmerkungen.

ANMERKUNG 2 In dieser Norm gibt es drei Validierungsphasen:

- Gesamtvalidierung der Sicherheit (siehe Bild 2 der IEC 61508-1);
- Validierung des E/E/PES (siehe Bild 3 der IEC 61508-1);
- Validierung der Software (siehe Bild 4 der IEC 61508-1).

ANMERKUNG 3 Die Validierung ist die Tätigkeit, die darlegt, dass das betrachtete sicherheitsbezogene System vor und nach der Installation in jeder Hinsicht der Spezifikation der Sicherheitsanforderungen des sicherheitsbezogenen Systems entspricht. Deshalb bedeutet zum Beispiel Validierung der Software die Bestätigung durch Untersuchung und Bereitstellung eines Nachweises, dass die Software die Spezifikation der Sicherheitsanforderungen der Software erfüllt.

3.8.3
Beurteilung der funktionalen Sicherheit
en: functional safety assessment
auf Nachweise gestützte Untersuchung, welche die funktionale Sicherheit beurteilt, die durch ein oder mehrere sicherheitsbezogene E/E/PE-Systeme und/oder andere risikomindernde Maßnahmen erreicht wird

3.8.4
Audit der funktionalen Sicherheit
en: functional safety audit
systematische und unabhängige Untersuchung, die bestimmt, ob die Verfahren zur Festlegung der Anforderungen an die funktionale Sicherheit mit den geplanten Vereinbarungen übereinstimmen, wirksam durchgeführt wurden und angemessen sind, die spezifizierten Ziele zu erreichen

ANMERKUNG Ein Audit zur funktionalen Sicherheit kann im Rahmen der Beurteilung der funktionalen Sicherheit ausgeführt werden.

3.8.5
Wiederholungsprüfung
en: proof test
wiederkehrende Prüfung zur Aufdeckung von versteckten gefahrbringenden Ausfällen in einem sicherheitsbezogenen System, so dass nötigenfalls eine Reparatur das System in einen "Wie-Neu"-Zustand bringen oder so nah wie unter praktischen Gesichtspunkten möglich an diesen Zustand heranbringen kann

ANMERKUNG 1 In dieser Norm wird der Begriff „Wiederholungsprüfung" verwendet, aber es ist anerkannt, dass der Begriff „periodische Prüfung" gleichbedeutend ist.

ANMERKUNG 2 Die Wirksamkeit der Wiederholungsprüfung wird von der Abdeckung der Ausfälle und der Wirksamkeit der Reparatur abhängig sein. In der Praxis wird eine vollständige Erkennung der versteckten gefahrbringenden Ausfälle

für nicht einfache sicherheitsbezogene E/E/PE-Systeme nicht leicht erreicht. Dies sollte aber das Ziel sein. Mindestens alle ausgeführten Sicherheitsfunktionen werden gemäß der Spezifikation der Sicherheitsanforderungen des E/E/PE-Systems geprüft. Falls separate Kanäle verwendet werden, werden diese Prüfungen für jeden Kanal getrennt ausgeführt. Für komplexe Elemente kann eine Analyse durchgeführt werden müssen, um nachzuweisen, dass die Wahrscheinlichkeit von durch Wiederholungsprüfungen nicht erkannten versteckten gefahrbringenden Ausfällen über die gesamte Lebensdauer des sicherheitsbezogenen E/E/PE-Systems vernachlässigbar ist.

ANMERKUNG 3 Eine Wiederholungsprüfung braucht Zeit zur Ausführung. Während dieser Zeit darf das sicherheitsbezogene E/E/PE-System teilweise oder vollständig blockiert werden. Die Dauer der Wiederholungsprüfung kann nur vernachlässigt werden, wenn der zu prüfende Teil des sicherheitsbezogenen E/E/PE-Systems im Falle einer Anforderung der Ausführung verfügbar bleibt, oder wenn die EUC während des Tests abgeschaltet wird.

ANMERKUNG 4 Während einer Wiederholungsprüfung darf das sicherheitsbezogene E/E/PE-System teilweise oder vollständig nicht in der Lage sein, auf Anforderungen der Ausführung zu reagieren. Die MTTR (mittlere Zeit bis zur Wiederherstellung) darf zur Berechnung des SIL nur vernachlässigt werden, wenn die EUC während der Reparatur abgeschaltet wird oder wenn andere Risikomaßnahmen mit vergleichbarer Wirksamkeit angewendet werden.

3.8.6
Diagnosedeckungsgrad
en: diagnostic coverage
DC
der Anteil der gefahrbringenden Ausfälle, die durch automatische diagnostische Online-Prüfungen erkannt werden. Der Anteil der gefahrbringenden Ausfälle wird mittels der Raten gefahrbringender Ausfälle zugehörig zu den erkannten gefahrbringenden Ausfällen geteilt durch die Gesamtrate der gefahrbringenden Ausfälle berechnet

ANMERKUNG 1 Der Diagnosedeckungsgrad gefahrbringender Ausfälle wird mittels der folgenden Gleichung berechnet, wobei DC der Diagnosedeckungsgrad ist, λDD die Rate erkannter gefahrbringender Ausfälle und λD total die Rate aller gefahrbringenden Ausfälle ist:

$$DC = \frac{\sum \lambda_{DD}}{\sum \lambda_{Dtotal}}$$

ANMERKUNG 2 Diese Definition ist anwendbar vorausgesetzt, dass die einzelnen Bauteile konstante Ausfallraten haben.

3.8.7
Diagnose-Testintervall
en: diagnostic test interval
Zeitraum zwischen Online-Prüfungen, um Fehler in einem sicherheitsbezogenen System mit spezifiziertem Diagnosedeckungsgrad zu entdecken

3.8.8
erkannt
en: detected, overt, revealed
offenkundig
in Verbindung mit Hardware erkannt durch diagnostische Prüfungen, Wiederholungsprüfungen, Bedienereingriff (zum Beispiel durch Inspektion und manuelle Prüfungen) oder während des üblichen Betriebes

BEISPIEL Diese Adjektive werden bei erkanntem Fehler und erkanntem Ausfall verwendet.

ANMERKUNG Ein durch Diagnoseprüfungen erkannter gefahrbringender Ausfall verhält sich wie ein erkannter Ausfall. Er verhält sich nur wie ein ungefährlicher Ausfall, wenn automatische oder manuelle Maßnahmen ergriffen werden, um so zu handeln.

3.8.9
unerkannt
en: undetected, covert, unrevealed
verdeckt
in Verbindung mit Hardware unerkannt durch diagnostische Prüfungen, Wiederholungsprüfungen, Bedienereingriff (zum Beispiel durch Inspektion und manuelle Prüfungen) oder während des üblichen Betriebes

BEISPIEL Diese Adjektive werden bei unerkanntem Fehler und unerkanntem Ausfall verwendet.

3.8.10
beurteilende Person
en: assessor
Person, Personen oder Organisation, welche die Beurteilung der funktionalen Sicherheit ausführt, um zu einer Beurteilung zu gelangen, ob die funktionale Sicherheit durch die sicherheitsbezogenen E/E/PE-Systeme und anderen risikomindernden Maßnahmen erreicht worden ist

ANMERKUNG Siehe auch IEC 61508-1, Abschnitt 8.

3.8.11
unabhängige Person
en: independent person
Person, die getrennt und nicht eingebunden ist in die Tätigkeiten, die während einer speziellen Phase des Gesamt-Sicherheitslebenszyklus, des E/E/PES-Sicherheitslebenszyklus oder des Software-Sicherheitslebenszyklus, der Gegenstand der Beurteilung der funktionalen Sicherheit oder Validierung ist, stattfinden und die keine direkte Verantwortung für diese Tätigkeiten trägt

3.8.12
unabhängige Abteilung
en: independent department
Abteilung, die getrennt und nicht in Verbindung mit den Abteilungen steht, die verantwortlich für die Tätigkeiten sind, die während einer speziellen Phase des Gesamt-Sicherheitslebenszyklus, des E/E/PES-Sicherheitslebenszyklus oder des Software-Sicherheitslebenszyklus, der Gegenstand der Beurteilung der funktionalen Sicherheit oder Validierung ist, stattfinden

3.8.13
unabhängige Organisation
en: independent organisation
Organisation, die aufgrund ihres Managements und ihrer anderen Mittel getrennt ist und nicht in Verbindung mit den Organisationen steht, die für die Tätigkeiten verantwortlich sind, die während einer speziellen Phase des Gesamt-Sicherheitslebenszyklus, des E/E/PES-Sicherheitslebenszyklus oder des Software-Sicherheitslebenszyklus, der Gegenstand der Beurteilung der funktionalen Sicherheit oder Validierung ist, stattfinden

3.8.14
Animation
en: animation
simulierter Betrieb des Softwaresystems (oder eines wichtigen Teils des Systems), um wichtige Aspekte des Verhaltens des Systems darzustellen, angewendet zum Beispiel auf eine Anforderungsspezifikation in einer angemessenen Art oder auf einem angemessenen hohen Niveau der Darstellung des Systementwurfs

ANMERKUNG Die Animation kann zusätzliches Vertrauen schaffen, dass das System die realen Anforderungen erfüllt, weil sie die Erkennbarkeit des spezifizierten Verhaltens für den Menschen verbessert.

3.8.15
dynamisches Testen
en: dynamic testing
überwachter und systematischer Einsatz von Software und/oder Betrieb der Hardware, um das geforderte Verhalten und das Nichtvorhandensein von unerwünschtem Verhalten darzulegen

ANMERKUNG Dynamisches Testen steht im Gegensatz zu statischer Analyse, bei der die Software nicht ausgeführt werden muss oder die Hardware in Betrieb sein muss.

3.8.16
Prüfeinrichtung
en: test harness
Einrichtung, die in der Lage ist (bis zu einem sinnvollen Grad), die Betriebsumgebung der Software oder Hardware während der Entwicklung durch Anwendung von Testfällen auf die Software und Aufzeichnung der Antwort zu simulieren

ANMERKUNG Die Prüfeinrichtung darf auch Testfallgeneratoren und Einrichtungen enthalten, um die Testergebnisse nachzuprüfen (entweder automatisch gegen Werte, die als korrekt angenommen werden, oder durch manuelle Analyse).

3.8.17
Sicherheitshandbuch eines konformen Objekts
en: compliant item safety manual
Dokument, das alle Informationen in Bezug auf die funktionale Sicherheit eines Elements hinsichtlich der festgelegten Sicherheitsfunktionen des Elements bereitstellt, das erforderlich ist, um sicherzustellen, dass das System die Anforderungen der IEC 61508 erfüllt

3.8.18
betriebsbewährt
en: proven in use
Nachweis, basierend auf einer Analyse der betrieblichen Erfahrung für eine spezielle Konfiguration eines Elements, dass die Wahrscheinlichkeit eines gefahrbringenden systematischen Fehlers niedrig genug ist, damit jede Sicherheitsfunktion, die das Element verwendet, ihren erforderlichen Sicherheits-Integritätslevel erreicht

Literaturhinweise

[1] IEC 61511 (alle Teile), *Functional safety – Safety instrumented systems for the process industry sector*

[2] IEC 62061, *Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems*

[3] IEC TR 61508-0:2005, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 0: Functional safety and IEC 61508*

[4] IEC 61508-5:—, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 5: Examples of methods for the determination of safety integrity levels*

[5] IEC 61508-6:—, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3*

[6] IEC 61508-7:—, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 7: Overview of techniques and* measures

[7] ISO/IEC 2382-1:1993, *Information technology – Vocabulary – Part 1: Fundamental terms*

[8] IEC 61131-3:2003, *Programmable controllers – Part 3: Programming languages*

CONTENTS

Figures

Tables

INTERNATIONAL ELECTROTECHNICAL COMMISSION

FUNCTIONAL SAFETY OF ELECTRICAL/ELECTRONIC/PROGRAMMABLE ELECTRONIC SAFETY-RELATED SYSTEMS –

Part 4: Definitions and abbreviations

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with an IEC Publication.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 61508-4 has been prepared by subcommittee 65A: System aspects, of IEC technical committee 65: Industrial-process measurement and control. This second edition cancels and replaces IEC 61508-4: 1998.

It has the status of a basic safety publication according to IEC Guide 104.

The text of this standard is based on the following documents:

FDIS	Report on voting
XX/XX/FDIS	XX/XX/RVD

Full information on the voting for the approval of this standard can be found in the report on voting indicated in the above table.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

IEC 61508 consists of the following parts, under the general title Functional safety of electrical/electronic/programmable electronic safety-related systems:

- Part 0: Functional safety and IEC 61508
- Part 1: General requirements
- Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems
- Part 3: Software requirements
- Part 4: Definitions and abbreviations
- Part 5: Examples of methods for the determination of safety integrity levels
- Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3
- Part 7: Overview of techniques and measures

The committee has decided that the contents of this publication will remain unchanged until the maintenance result date[1)] indicated on the IEC web site under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

1) The National Committees are requested to note that for this publication the maintenance result date is 2014

INTRODUCTION

Systems comprised of electrical and/or electronic elements have been used for many years to perform safety functions in most application sectors. Computer-based systems (generically referred to as programmable electronic systems) are being used in all application sectors to perform non-safety functions and, increasingly, to perform safety functions. If computer system technology is to be effectively and safely exploited, it is essential that those responsible for making decisions have sufficient guidance on the safety aspects on which to make these decisions.

This International Standard sets out a generic approach for all safety lifecycle activities for systems comprised of electrical and/or electronic and/or programmable electronic (E/E/PE) elements that are used to perform safety functions. This unified approach has been adopted in order that a rational and consistent technical policy be developed for all electrically-based safety-related systems. A major objective is to facilitate the development of application sector standards.

In most situations, safety is achieved by a number of systems which rely on many technologies (for example mechanical, hydraulic, pneumatic, electrical, electronic, programmable electronic). Any safety strategy must therefore consider not only all the elements within an individual system (for example sensors, controlling devices and actuators) but also all the safety-related systems making up the total combination of safety-related systems. Therefore, while this International Standard is concerned with E/E/PE safety-related systems, it may also provide a framework within which safety-related systems based on other technologies may be considered.

It is recognized that there is a great variety of applications using E/E/PE safety-related systems in a variety of application sectors and covering a wide range of complexity, hazard and risk potentials. In any particular application, the required safety measures will be dependent on many factors specific to the application. This International Standard, by being generic, will enable such measures to be formulated in future application sector international standards and in revisions of those that already exist.

This International Standard

- considers all relevant overall, E/E/PE system and software safety lifecycle phases (for example, from initial concept, through design, implementation, operation and maintenance to decommissioning) when E/E/PE systems are used to perform safety functions;
- has been conceived with a rapidly developing technology in mind; the framework is sufficiently robust and comprehensive to cater for future developments;
- enables application sector international standards, dealing with E/E/PE safety-related systems, to be developed; the development of application sector international standards, within the framework of this standard, should lead to a high level of consistency (for example, of underlying principles, terminology etc.) both within application sectors and across application sectors; this will have both safety and economic benefits;

NOTE 1 References [1] and [2] in the bibliography are application sector international standards.

- provides a method for the development of the safety requirements specification necessary to achieve the required functional safety for E/E/PE safety-related systems;
- adopts a risk-based approach by which the safety integrity level requirements can be determined;
- introduces safety integrity levels for specifying the target level of safety integrity for the safety functions to be implemented by the E/E/PE safety-related systems;

NOTE 2 The standard does not specify the safety integrity requirements for any safety function, nor does it mandate how the safety integrity level is determined. Instead it provides a risk-based conceptual framework and example techniques.

- sets target failure measures for safety functions carried out by E/E/PE safety-related systems, which are linked to the safety integrity levels;
- sets a lower limit on the target failure measures for a safety function carried out by a single E/E/PE safety-related system. For E/E/PE safety-related systems operating in
  - a low demand mode of operation, the lower limit is set at an average probability of dangerous failure on demand of 10^{-5},
  - a high demand or a continuous mode of operation, the lower limit is set at an average frequency of dangerous failure of 10^{-9} [h^{-1}];

NOTE 3 A single E/E/PE safety-related system does not necessarily mean a single-channel architecture.

NOTE 4 It may be possible to achieve designs of safety-related systems with lower values for the target safety integrity for non-complex systems, but these limits are considered to represent what can be achieved for relatively complex systems (for example programmable electronic safety-related systems) at the present time.

- sets requirements for the avoidance and control of systematic faults, which are based on experience and judgement gained from practical experience gained in industry. Even though the probability of occurrence of systematic failures cannot in general be quantified the standard does, however, allow a claim to be made, for a specified safety function, that the target failure measure associated with the safety function can be considered to be achieved if all the requirements in the standard have been met.
- adopts a broad range of principles, techniques and measures to achieve functional safety for E/E/PE safety-related systems, but does not use the concept of fail safe which may be of value when the failure modes are well defined and the level of complexity is relatively low. The concept of fail safe was considered inappropriate because of the full range of complexity of E/E/PE safety-related systems that are within the scope of the standard.

FUNCTIONAL SAFETY OF ELECTRICAL/ELECTRONIC/PROGRAMMABLE ELECTRONIC SAFETY-RELATED SYSTEMS –

Part 4: Definitions and abbreviations

1 Scope

1.1 This part of IEC 61508 contains the definitions and explanation of terms that are used in parts 1 to 7 of this standard.

1.2 The definitions are grouped under general headings so that related terms can be understood within the context of each other. However, it should be noted that these headings are not intended to add meaning to the definitions.

1.3 Parts 1, 2, 3 and 4 of this standard are basic safety publications, although this status does not apply in the context of low complexity E/E/PE safety-related systems (see 3.4.4 of part 4). As basic safety publications, they are intended for use by technical committees in the preparation of standards in accordance with the principles contained in *IEC Guide 104* and *ISO/IEC Guide 51*. Parts 1, 2, 3, and 4 are also intended for use as stand-alone publications. The horizontal safety function of this international standard does not apply to medical equipment in compliance with the IEC 60601 series.

One of the responsibilities of a technical committee is, wherever applicable, to make use of basic safety publications in the preparation of its publications. In this context, the requirements, test methods or test conditions of this basic safety publication will not apply unless specifically referred to or included in the publications prepared by those technical committees.

1.4 Figure 1 shows the overall framework for parts 1 to 7 of IEC 61508 and indicates the role that IEC 61508-4 plays in the achievement of functional safety for E/E/PE safety-related systems.

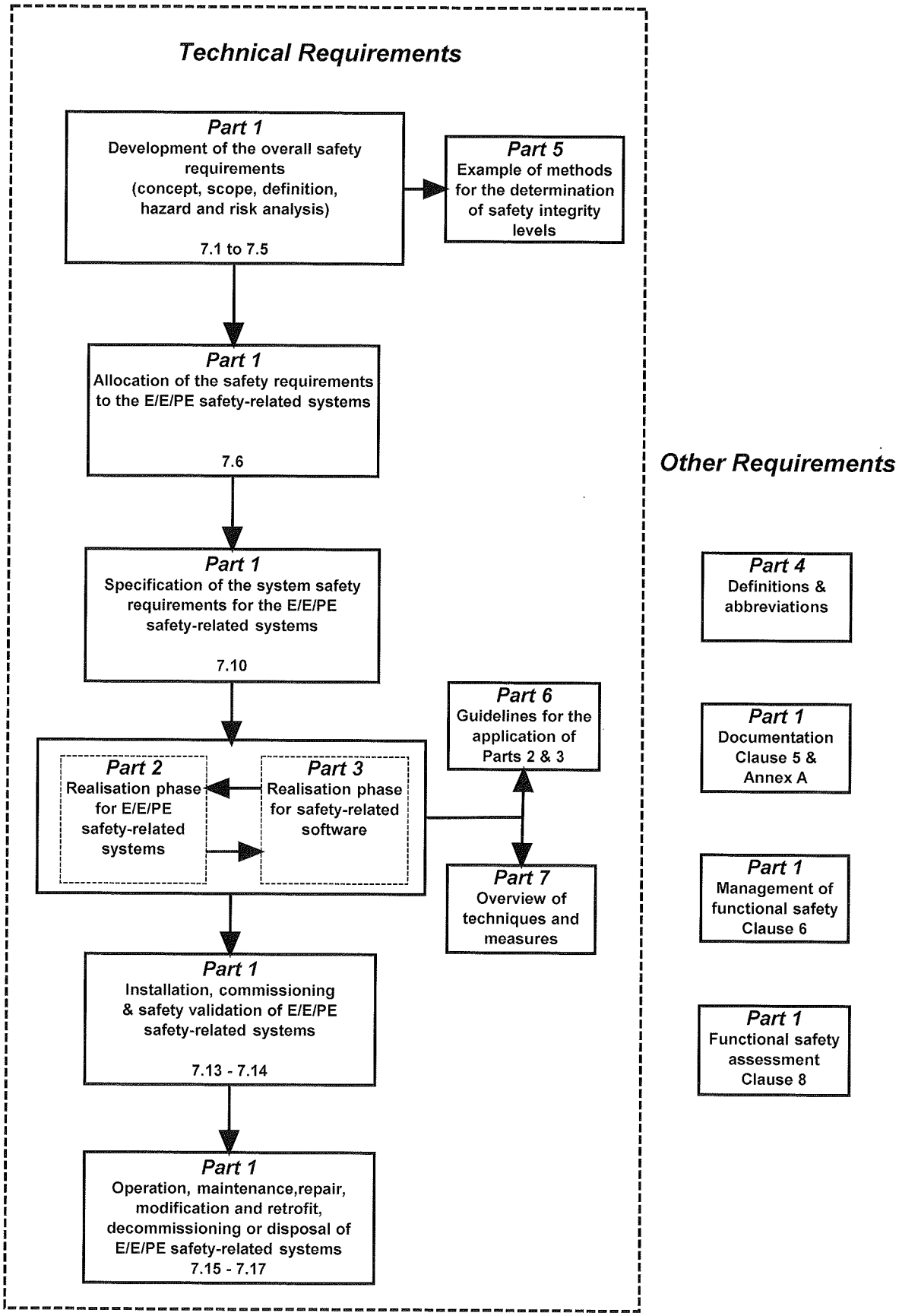


Figure 1 — Overall framework of IEC 61508

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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* [2)]

IEC 61508-2:—, *Functional safety of electrical/electronical/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* [2)]

NOTE For an introduction to the IEC 61508 series of standards, see the bibliography reference [3]. For guidance on applying normative Parts 1 to 4 of IEC 61508, see references [4], [5] and [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 Definitions and abbreviations

For the purposes of this International Standard, the following definitions and the abbreviations given in table 1 apply.

Table 1 — Abbreviations used in this standard

Abbreviation	Full expression	Definition and/or explanation of term
ALARP	As Low As Reasonably Practicable	IEC 61508-5, Annex B
ASIC	Application Specific Integrated Circuit	3.2.15
CPLD	Complex Programmable Logic Device	
DC	Diagnostic Coverage	3.8.6
(E)EPLD	(Electrically) Erasable Programmable Logic Device	
E/E/PE	Electrical/Electronic/Programmable Electronic	3.2.13, example: E/E/PE safety-related system
E/E/PES	Electrical/Electronic/Programmable Electronic System	3.3.3
EEPROM	Electrically Erasable Programmable Read-Only Memory	
EPROM	Erasable Programmable Read-Only Memory	
EUC	Equipment Under Control	3.2.1
FPGA	Field Programmable Gate Array	
GAL	Generic Array Logic	
HFT	Hardware Fault Tolerance	IEC 61508-2, 7.4.4
MooN	M out of N channel architecture (for example 1oo2 is 1 out of 2 architecture, where either of the two channels can perform the safety function)	IEC 61508-6, Annex B
MooND	M out of N channel architecture with Diagnostics	IEC 61508-6, Annex B
PAL	Programmable Array Logic	
PE	Programmable Electronic	3.2.12
PES	Programmable Electronic System	3.3.1
PFD	Probability of dangerous Dailure on Demand	3.6.17
PFDavg	Average Probability of dangerous Failure on Demand	3.6.18
PFH	Average frequency of dangerous failure [h^{-1}] per Hour	3.6.19
PLA	Programmable Logic Array	
PLC	Programmable Logic Controller	IEC 61508-6, Annex E
PLD	Programmable Logic Device	
PLS	Programmable Logic Sequenzer	
PML	Programmable. Macro Logic	
RAM	Random Access Memory	
ROM	Read-Only Memory	
SFF	Safe Failure Fraction	3.6.15
SIL	Safety Integrity Level	3.5.8
VHDL	Verilog Hardware Description Language	IEC 61508-2, Annex F, Note 2

3.1 Safety terms

3.1.1
harm
physical injury or damage to the health of people or damage to property or the environment [ISO/IEC Guide 51:1999, definition 3.3]

3.1.2
hazard
potential source of harm
[ISO/IEC Guide 51:1999, definition 3.5]

NOTE The term includes danger to persons arising within a short time scale (for example, fire and explosion) and also those that have a long-term effect on a person's health (for example, release of a toxic substance).

3.1.3
hazardous situation
circumstance in which people, property or the environment are exposed to one or more hazards or hazardous events [ISO/IEC Guide 51:1999, definition 3.6, modified]

3.1.4
hazardous event
event that may result in harm

NOTE Whether or not a hazardous event results in harm depends on whether people, property or the environment are exposed to the consequence of the hazardous event and, in the case of harm to people, whether any such exposed people can escape the consequences of the event after it has occurred.

3.1.5
harmful event
occurrence in which a hazardous situation results in harm, or hazardous event that results in harm

NOTE Adapted from ISO/IEC Guide 51, definition 3.4, to allow for a hazardous event.

3.1.6
risk
combination of the probability of occurrence of harm and the severity of that harm [ISO/IEC Guide 51:1999, definition 3.2]

NOTE For more discussion on this concept see annex A of IEC 61508-5.

3.1.7
tolerable risk
risk which is accepted in a given context based on the current values of society
[ISO/IEC Guide 51:1999, definition 3.7]

NOTE See annex B of IEC 61508-5.

3.1.8
residual risk
risk remaining after protective measures have been taken
[ISO/IEC Guide 51:1999, definition 3.9]

3.1.9
EUC risk
risk arising from the EUC or its interaction with the EUC control system

NOTE 1 The risk in this context is that associated with the specific harmful event in which E/E/PE safety-related systems and other risk reduction measures are to be used to provide the necessary risk reduction, (i.e. the risk associated with functional safety).

NOTE 2 The EUC risk is indicated in Figure A.1 of IEC 61508-5. The main purpose of determining the EUC risk is to establish a reference point for the risk without taking into account E/E/PE safety-related systems and other risk reduction measures.

NOTE 3 Assessment of this risk will include associated human factor issues.

3.1.10
target risk
risk that is intended to be reached for a specific hazard taking into account the EUC risk together with the E/E/PE safety-related systems and the other risk reduction measures

3.1.11
safety
freedom from unacceptable risk
[ISO/IEC Guide 51:1999, definition 3.1]

3.1.12
functional safety
part of the overall safety relating to the EUC and the EUC control system that depends on the correct functioning of the E/E/PE safety-related systems and other risk reduction measures

3.1.13
safe state
state of the EUC when safety is achieved

NOTE In going from a potentially hazardous condition to the final safe state, the EUC may have to go through a number of intermediate safe states. For some situations a safe state exists only so long as the EUC is continuously controlled. Such continuous control may be for a short or an indefinite period of time.

3.1.14
reasonably foreseeable misuse
use of a product, process or service in a way not intended by the supplier, but which may result from readily predictable human behaviour
[ISO/IEC Guide 51:1999, definition 3.14]

3.2 Equipment and devices

3.2.1
equipment under control
EUC
equipment, machinery, apparatus or plant used for manufacturing, process, transportation, medical or other activities

NOTE The EUC control system is separate and distinct from the EUC.

3.2.2
environment
all relevant parameters that can affect the achievement of functional safety in the specific application under consideration and in any safety lifecycle phase

NOTE This would include, for example, physical environment, operating environment, legal environment and maintenance environment.

3.2.3
functional unit
entity of hardware or software, or both, capable of accomplishing a specified purpose
[ISO/IEC 2382-14-01-01]

NOTE In IEV 191-01-01 the more general term "item" is used in place of functional unit. An item may sometimes include people.

3.2.4
application
Task related to the EUC rather than to the E/E/PE system

3.2.5
software
intellectual creation comprising the programs, procedures, data, rules and any associated documentation pertaining to the operation of a data processing system

NOTE 1 Software is independent of the medium on which it is recorded.

NOTE 2 This definition without Note 1 differs from ISO 2382-1 (reference [7] in the bibliography) by the addition of the word data.

3.2.6
system software
part of the software of a PE system that relates to the functioning of, and services provided by, the programmable device itself, as opposed to the application software that specifies the functions that perform a task related to the EUC

NOTE Refer to IEC 61508-7 for examples.

3.2.7
application software
application data
configuration data
that part of the software of a programmable electronic system that specifies the functions that perform a task related to the EUC rather than the functioning of, and services provided by the programmable device itself

3.2.8
pre-existing software
a software element which already exists and is not developed specifically for the current project or SRS

NOTE The software could be a commercially available product, or it could have been developed by some organisation for a previous product or system. Pre-existing software may or may not have been developed in accordance with the requirements of this standard.

3.2.9
data
information represented in a manner suitable for communication, interpretation, or processing by computers.

NOTE 1 Data may take the form of static information (for example configuration of a set point or a representation of geographical information) or it may take the form of instructions to specify a sequence of pre-existing functions.

NOTE 2 Refer to IEC 61508-7 for examples.

3.2.10
software on-line support tool
a software tool that can directly influence the SRS during its run time

3.2.11
software off-line support tool
a software tool that supports a phase of the software development lifecycle and that cannot directly influence the SRS during its run time. Software off-line tools may be divided into the following classes:

- **T1**
  generates no outputs which can directly or indirectly contribute to the executable code (including data) of the safety related system;

NOTE T1 examples include: a text editor or a requirements or design support tool with no automatic code generation capabilities; configuration control tools.

- **T2**
  supports the test or verification of the design or executable code, where errors in the tool can fail to reveal defects but cannot directly create errors in the executable software;

NOTE T2 examples include: a test harness generator; a test coverage measurement tool; a static analysis tool.

- **T3**
  generates outputs which can directly or indirectly contribute to the executable code of the safety related system.

NOTE T3 examples include: a tool to change set-points during system operation; an optimising compiler where the relationship between the source code program and the generated object code is not obvious; a compiler that incorporates an executable run-time package into the executable code.

3.2.12
programmable electronic
PE

based on computer technology which may be comprised of hardware, software, and of input and/or output units

NOTE This term covers microelectronic devices based on one or more central processing units (CPUs) together with associated memories, etc.

EXAMPLE The following are all programmable electronic devices:

- microprocessors;
- micro-controllers;
- programmable controllers;
- application specific integrated circuits (ASICs);
- programmable logic controllers (PLCs);
- other computer-based devices (for example smart sensors, transmitters, actuators).

3.2.13
electrical/electronic/programmable electronic
E/E/PE

based on electrical (E) and/or electronic (E) and/or programmable electronic (PE) technology

NOTE The term is intended to cover any and all devices or systems operating on electrical principles.

EXAMPLE Electrical/electronic/programmable electronic devices include

- electro-mechanical devices (electrical);
- solid-state non-programmable electronic devices (electronic);
- electronic devices based on computer technology (programmable electronic); see 3.2.5.

3.2.14
limited variability language

software programming language, whose notation is textual or graphical or has characteristics of both, for commercial and industrial programmable electronic controllers with a range of capabilities limited to their application

EXAMPLE The following are limited variability languages, from IEC 61131-3 (reference [8] in the bibliography) and other sources, which are used to represent the application program for a PLC system:

- ladder diagram: a graphical language consisting of a series of input symbols (representing behaviour similar to devices such as normally open and normally closed contacts) interconnected by lines (to indicate the flow of current) to output symbols (representing behaviour similar to relays);
- Boolean algebra: a low-level language based on Boolean operators such as AND, OR and NOT with the ability to add some mnemonic instructions;
- function block diagram: in addition to Boolean operators, allows the use of more complex functions such as data transfer file, block transfer read/write, shift register and sequencer instructions;
- sequential function chart: a graphical representation of a sequential program consisting of interconnected steps, actions and directed links with transition conditions.

3.2.15
application specific integrated circuit
ASIC

integrated circuit designed and manufactured for specific function, where this functionality is defined by the product developer

NOTE The term ASIC as a stand-alone covers all types of the following integrated circuits

- full custom ASIC: ASIC where design and production is similar to a standard integrated circuit (see Note), with the functionality defined by the product developer

  A standard integrated circuit is manufactured in large quantities and can be used for different applications. Functionality, validation, production and production test are solely in the hand of the semiconductor vendor. Manual manipulations and optimisations at layout level are frequently used to reduce required area. They are not designed for safety-related systems. Frequent changes in production process, process technology and layout are likely for cost and yield optimisation. The number of components manufactured using a certain process or mask revision are not publicly known.
- core based ASIC: ASIC based on pre-layouted, designed or generated macro cores, supported by additional logic

  EXAMPLE 1 Examples for pre-layouted macros are standard microprocessor cores, peripheral components, communication interfaces, analogue blocks, special function I/O cells.

  EXAMPLE 2 Examples for pre-designed macros known as Intellectual Property (IP) are variety of similar components as mentioned in Example 1, with the difference that the design data consists of a high level hardware description language (VHDL, Verilog) as described for cell based ASIC.

  EXAMPLE 3 Examples for generated macros include embedded RAM, ROM, EEPROM or FLASH. Generated blocks are assumed to be correct by construction, based on design rules. Pre-layouted or generated macros are process specific but may be ported to different technologies. In most cases, the macro cores are not identical to the original discrete off-the-shelf components (different process, provided by a third party).
- cell based ASIC: ASIC based on logic primitives (like AND, OR, Flip-Flop, Latch) taken from a cell library

  The gate-level netlist containing the logic primitives and the interconnections is usually created from a high level hardware description language (VHDL, Verilog) using synthesis tools. The functional and timing characteristics of the logic primitives is characterised in the cell library; these parameters are used to drive the synthesis tool and are also used for simulation. In addition, layout tools are used to place the cells and to route the interconnects.
- gate array: pre-manufactured silicon masters with a fixed number of cells that provide a common starting point for different components

  The functionality is defined by the interconnection matrix (metal layer) between the pre-manufactured cells. The design process is very similar to that of a cell based ASIC, while the layout step is replaced by a routing step to connect the already existing cells.
- field programmable gate array (FPGA): standard integrated circuit, using one-time programmable or re-programmable elements to define the connection between functional blocks and to configure the functionality of the individual blocks

  It is not possible to test one-time programmable FPGAs completely during production due to the nature of the programmable element.
- programmable logic device (PLD): standard integrated circuit, with low to medium complexity, using one-time programmable or electrical erasable elements (fuses) to define combinatorial logic – typically based on AND or OR product terms – and configurable storage elements

  PLDs provide predictable timing and guaranteed maximum operating frequency in synchronous design due to their regular structure.

  Type of PLD are for example PAL, GAL, PML, (E)EPLD, PLA, PLS.
- complex programmable logic device (CPLD): multiple PLD-like blocks on a single chip, connected by a programmable interconnection matrix (crossbar)

  The programmable logic element is re-programmable (EPROM or EEPROM) in most cases.

3.3 Systems: general aspects

3.3.1
programmable electronic system
PES

system for control, protection or monitoring based on one or more programmable electronic devices, including all elements of the system such as power supplies, sensors and other input devices, data highways and other communication paths, and actuators and other output devices (see Figure 2)

NOTE The structure of a PES is shown in Figure 2 a). Figure 2 b) illustrates the way in which a PES is represented in this International Standard, with the programmable electronics shown as a unit distinct from sensors and actuators on the EUC and their interfaces, but the programmable electronics could exist at several places in the PES. Figure 2 c) illustrates a PES with two discrete units of programmable electronics. Figure 2 d) illustrates a PES with dual programmable electronics (i.e. two-channel), but with a single sensor and a single actuator.

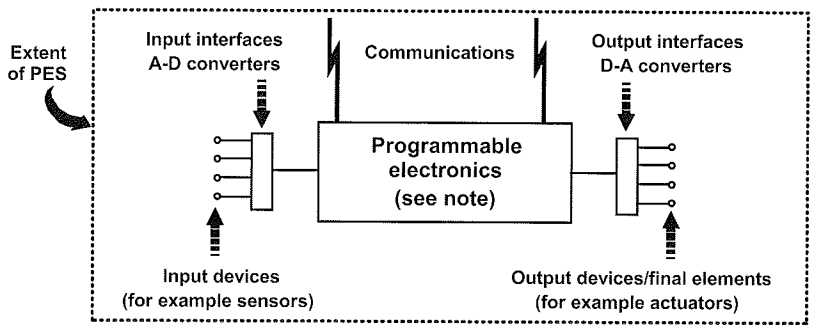
3.3.2
electrical/electronic/programmable electronic system
E/E/PES
system for control, protection or monitoring based on one or more electrical/electronic programmable electronic (E/E/PE) devices, including all elements of the system such as power supplies, sensors and other input devices, data highways and other communication paths, and actuators and other output devices (see Figure 3)

3.3.3
EUC control system
system that responds to input signals from the process and/or from an operator and generates output signals causing the EUC to operate in the desired manner

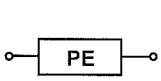
NOTE The EUC control system includes input devices and final elements.

3.3.4
architecture
specific configuration of hardware and software elements in a system

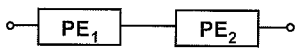
3.3.5
software module
construct that consists of procedures and/or data declarations and that can also interact with other such constructs



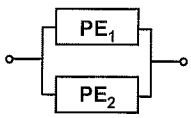
a) Basic PES structure



b) Single PES with single programmable electronic device (i.e. one PES comprised of a single channel of programmable electronics)



c) Single PES with dual programmable electronic devices linked in a serial manner (for example intelligent sensor and programmable controller)

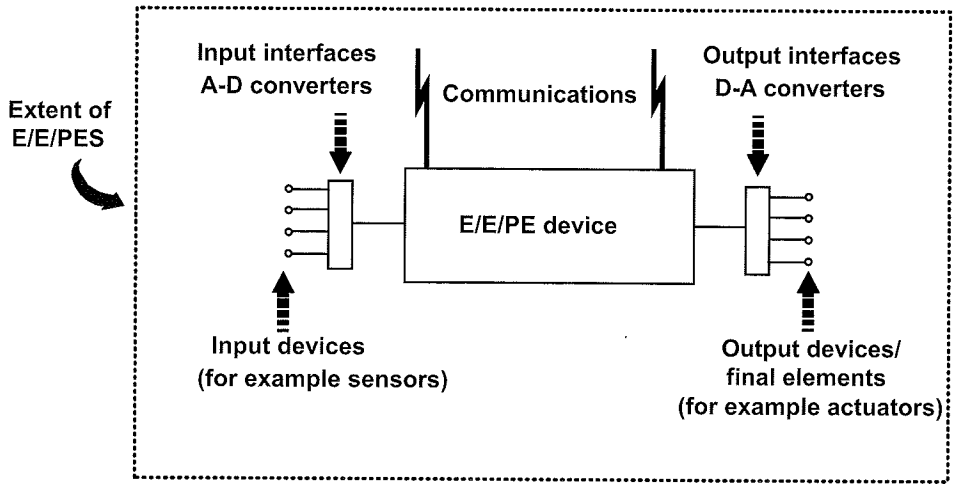


d) Single PES with dual programmable electronic devices but with shared sensors and final elements (i.e. one PES comprised of two channels of programmable electronics)

IEC 1 657/98

NOTE The programmable electronics are shown centrally located but could exist at several places in the PES.

Figure 2 — Programmable electronic system (PES): structure and terminology



NOTE THE E/E/PE device is shown centrally located but such device(s) could exist at several places in the E/E/PES.

Figure 3 — Electrical/electronic/programmable electronic system (E/E/PES): structure and terminology

3.3.6
channel
element or group of elements that independently perform(s) a function

EXAMPLE A two-channel (or dual-channel) configuration is one with two channels that independently perform the same function.

NOTE 1 The elements within a channel could include input/output modules, a logic system (see 3.4.5), sensors and final elements.

NOTE 2 The term can be used to describe a complete system, or a portion of a system (for example, sensors or final elements).

3.3.7
diversity
different means of performing a required function

NOTE Diversity may be achieved by different physical methods or different design approaches.

3.4 Systems: safety-related aspects

3.4.1
safety-related system
designated system that both

- implements the required safety functions necessary to achieve or maintain a safe state for the EUC; and
- is intended to achieve, on its own or with other E/E/PE safety-related systems and other risk reduction measures, the necessary safety integrity for the required safety functions

NOTE 1 The term refers to those systems, designated as safety-related systems, that are intended to achieve, together with the other risk reduction measures (see 3.4.3), the necessary risk reduction in order to meet the required tolerable risk (see 3.1.7). See also annex A of IEC 61508-5.

NOTE 2 Safety-related systems are designed to prevent the EUC from going into a dangerous state by taking appropriate action on receipt of commands. The failure of a safety-related system would be included in the events leading to the determined hazard or hazards. Although there may be other systems having safety functions, it is the safety-related systems that have been designated to achieve, in their own right, the required tolerable risk. Safety-related systems can broadly be divided into safety-related control systems and safety-related protection systems.

NOTE 3 Safety-related systems may be an integral part of the EUC control system or may interface with the EUC by sensors and/or actuators. That is, the required safety integrity level may be achieved by implementing the safety functions in the EUC control system (and possibly by additional separate and independent systems as well) or the safety functions may be implemented by separate and independent systems dedicated to safety.

NOTE 4 A safety-related system may

a) be designed to prevent the harmful event (i.e. if the safety-related systems perform their safety functions then no harmful event arises);

b) be designed to mitigate the effects of the harmful event, thereby reducing the risk by reducing the consequences;

c) be designed to achieve a combination of a) and b).

NOTE 5 A person can be part of a safety-related system (see 3.4.1). For example, a person could receive information from a programmable electronic device and perform a safety action based on this information, or perform a safety action through a programmable electronic device.

NOTE 6 A safety-related system includes all the hardware, software and supporting services (for example, power supplies) necessary to carry out the specified safety function (sensors, other input devices, final elements (actuators) and other output devices are therefore included in the safety-related system).

NOTE 7 A safety-related system may be based on a wide range of technologies including electrical, electronic, programmable electronic, hydraulic and pneumatic.

3.4.2
other risk reduction measure
measure to reduce or mitigate risk that is separate and distinct from, and does not use, E/E/PE safety-related systems

EXAMPLE A relief valve is an other risk reduction measure.

3.4.3
low complexity E/E/PE safety-related system
E/E/PE safety-related system (see 3.2.6 and 3.4.1), in which

- the failure modes of each individual component are well defined;
- the behaviour of the system under fault conditions can be completely determined.

NOTE Behaviour of the system under fault conditions may be determined by analytical and/or test methods.

EXAMPLE A system comprising one or more limit switches, operating, possibly via interposing electro-mechanical relays, one or more contactors to de-energise an electric motor is a low-complexity E/E/PE safety-related system.

3.4.4
subsystem
entity of the top-level architectural design of a safety-related system where a dangerous failure according to 3.6.7 (a) of the subsystem results in dangerous failure of a safety function according to 3.6.7 (a).

3.4.5
element
part of a subsystem comprising a single component or any group of components that performs one or more element safety functions.

[IEC 62061, definition 3.2.6, modified]

NOTE An element may comprise hardware and/or software.

3.4.6
redundancy
existence of means, in addition to the means which would be sufficient for a functional unit to perform a required function or for data to represent information

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

EXAMPLE Duplicated functional components and the addition of parity bits are both instances of redundancy.

NOTE 1 Redundancy is used primarily to improve reliability (probability of functioning properly over a given period of time) or availability (probability of functioning at given instant). It may also be used in order to minimize spurious actions through architectures such as 2oo3.

NOTE 2 The definition in IEV 191-15-01 is less complete.

NOTE 3 Redundancy may be "hot" or "active" (all redundant item running at the same time), "cold" or "stand-by" (only one of the redundant item working at the same time), "mixed" (one or several items running and one or several items in stand-by at the same time).

3.5 Safety functions and safety integrity

3.5.1
safety function
function to be implemented by an E/E/PE safety-related system or other risk reduction measures, that is intended to achieve or maintain a safe state for the EUC, in respect of a specific hazardous event (see 3.4.1)

EXAMPLE Examples of safety functions include

- functions that are required to be carried out as positive actions to avoid hazardous situations (for example switching off a motor); and
- functions that prevent actions being taken (for example preventing a motor starting).

3.5.2
overall safety function
means of achieving or maintaining a safe state for the EUC, in respect of a specific hazardous event

3.5.3
element safety function
function of an element that is intended for application in support of a safety function

NOTE An element safety function can have a specified systematic capability (see 3.5.9).

3.5.4
safety integrity
probability of an E/E/PE safety-related system satisfactorily performing the specified safety functions under all the stated conditions within a stated period of time

NOTE 1 The higher the level of safety integrity, the lower the probability that the safety-related system will fail to carry out the specified safety functions or will fail to adopt a specified state when required.

NOTE 2 There are four levels of safety integrity (see 3.5.8).

NOTE 3 In determining safety integrity, all causes of failures (both random hardware failures and systematic failures) that lead to an unsafe state should be included, for example hardware failures, software induced failures and failures due to electrical interference. Some of these types of failure, in particular random hardware failures, may be quantified using such measures as the average frequency of failure in the dangerous mode of failure or the probability of a safety-related protection system failing to operate on demand. However, safety integrity also depends on many factors that cannot be accurately quantified but can only be considered qualitatively.

NOTE 4 Safety integrity comprises hardware safety integrity (see 3.5.7) and systematic safety integrity (see 3.5.6).

NOTE 5 This definition focuses on the reliability of the safety-related systems to perform the safety functions (see IEV 191-12-01 for a definition of reliability).

3.5.5
software safety integrity
part of the safety integrity of a safety-related system relating to systematic failures in a dangerous mode of failure that are attributable to software

3.5.6
systematic safety integrity
part of the safety integrity of a safety-related system relating to systematic failures in a dangerous mode of failure

NOTE Systematic safety integrity cannot usually be quantified (as distinct from hardware safety integrity which usually can).

3.5.7
hardware safety integrity
part of the safety integrity of a safety-related system relating to random hardware failures in a dangerous mode of failure

NOTE The term relates to failures in a dangerous mode, that is, those failures of a safety-related system that would impair its safety integrity. The two parameters that are relevant in this context are the average frequency of dangerous failure and the probability of failure to operate on demand. The former reliability parameter is used when it is necessary to maintain continuous control in order to maintain safety, the latter reliability parameter is used in the context of safety-related protection systems.

3.5.8
safety integrity level
SIL
discrete level (one out of a possible four), corresponding to a range of safety integrity values, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest

NOTE 1 The target failure measures (see 3.5.15) for the four safety integrity levels are specified in tables 2 and 3 of IEC 61508-1.

NOTE 2 Safety integrity levels are used for specifying the safety integrity requirements of the safety functions to be allocated to the E/E/PE safety-related systems.

NOTE 3 A safety integrity level (SIL) is not a property of a system, subsystem, element or component. The correct interpretation of the phrase "SILn safety-related system" (where n is 1, 2, 3 or 4) is that the system is potentially capable of supporting safety functions with a safety integrity level up to n.

3.5.9
systematic capability
measure (expressed on a scale of SIL 1 to SIL 4) of the confidence that the systematic safety integrity of an element meets the requirements of the specified SIL, in respect of the specified element safety function, when the element is applied in accordance with the instructions specified in the compliant item safety manual for the element.

NOTE 1 Systematic capability is determined with reference to the requirements for the avoidance and control of systematic faults (see IEC 61508-2 and IEC 61508-3).

NOTE 2 What is a relevant systematic failure mechanism will depend on the nature of the element. For example, for an element comprising solely software, only software failure mechanisms will need to be considered. For an element comprising hardware and software it will be necessary to consider both systematic hardware and software failure mechanisms.

NOTE 3 A Systematic Capability of SIL X for an element, in respect of the specified element safety function, means that the systematic safety integrity of SIL X has been met when the element is applied in accordance with the instructions specified in the compliant item safety manual for the element.

3.5.10
software safety integrity level
systematic capability of a software element that forms part of a subsystem of a safety-related system

NOTE SIL characterises the overall safety function, but not any of the distinct subsystems or elements that support that safety function. In common with any "element", software therefore has no SIL in its own right. However, it is convenient to talk about "SIL X software" meaning "software in which confidence is justified (expressed on a scale of 1 to 4) that the (software) element safety function will not fail due to relevant systematic failure mechanisms when the (software) element is applied in accordance with the instructions specified in the compliant item safety manual for the element".

3.5.11
E/E/PE safety functions requirements specification
specification containing the requirements for the safety functions that have to be performed by the safety-related systems

NOTE 1 This specification is one part (the safety functions part) of the E/E/PE safety requirements specification (see see IEC 61508-1; 7.10 and 7.10.2.6) and contains the precise details of the safety functions that have to be performed by the safety-related systems.

NOTE 2 Specifications may be documented in text, flow diagrams, matrices, logic diagrams, etc., providing that the safety functions are clearly conveyed.

3.5.12
E/E/PE system safety integrity requirements specification
specification containing the safety integrity requirements of the safety functions that have to be performed by the safety-related systems

NOTE This specification is one part (the safety integrity part) of the E/E/PE system safety requirements specification (see IEC 61508-1; 7.10 and 7.10.2.7)

3.5.13
safety-related software
software that is used to implement safety functions in a safety-related system

3.5.14
mode of operation
way in which a safety function operates, which may be either

- **low demand mode:** where the safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is no greater than one per year; or

NOTE The E/E/PE safety-related system that performs the safety function normally has no influence on the EUC or EUC control system until a demand arises. However, if the E/E/PE safety-related system fails in such a way that it is unable to carry out the safety function then it may cause the EUC to move to a safe state (see IEC 61508-2, 7.4.6).

- **high demand mode:** where the safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is greater than one per year; or
- **continuous mode:** where the safety function retains the EUC in a safe state as part of normal operation.

3.5.15
target failure measure
target probability of dangerous mode failures to be achieved in respect of the safety integrity requirements, specified in terms of either

- the average probability of dangerous failure of the safety function on demand (for a low demand mode of operation);
- the average frequency of dangerous failure [h^{-1}](for a high demand mode of operation or a continuous mode of operation)

NOTE – The numerical values for the target failure measures are given in tables 2 and 3 of IEC 61508-1.

3.5.16
necessary risk reduction
risk reduction to be achieved by the E/E/PE safety-related systems and/or other risk reduction measures in order to ensure that the tolerable risk is not exceeded

3.6 Fault, failure and error

3.6.1
fault
abnormal condition that may cause a reduction in, or loss of, the capability of a functional unit to perform a required function

[ISO/IEC 2382-14-01-10]

NOTE IEV 191-05-01 defines "fault" as a state characterised by the inability to perform a required function, excluding the inability during preventative maintenance or other planned actions, or due to lack of external resources. See Figure 4 for an illustration of these two points of view.

3.6.2
fault avoidance
use of techniques and procedures that aim to avoid the introduction of faults during any phase of the safety lifecycle of the safety-related system

3.6.3
fault tolerance
ability of a functional unit to continue to perform a required function in the presence of faults or errors

[ISO/IEC 2382-14-04-06]

NOTE The definition in IEV 191-15-05 refers only to sub-item faults. See the note for the term fault in 3.6.1.

3.6.4
failure
termination of the ability of a functional unit to provide a required function or operation of a functional unit in any way other than as required

NOTE 1 This is based on IEV 191-04-01 with changes to include systematic failures due to, for example, deficiencies in specification or software.

NOTE 2 See Figure 4 for the relationship between faults and failures, both in IEC 61508 and IEV 60050(191).

NOTE 3 Performance of required functions necessarily excludes certain behaviour, and some functions may be specified in terms of behaviour to be avoided. The occurrence of such behaviour is a failure.

NOTE 4 Failures are either random (in hardware) or systematic (in hardware or software), see 3.6.5 and 3.6.6.

3.6.5
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

NOTE 1 There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

NOTE 2 A major distinguishing feature between random hardware failures and systematic failures (see 3.6.6), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

3.6.6
systematic failure
failure, related in a deterministic way to a certain cause, that can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors

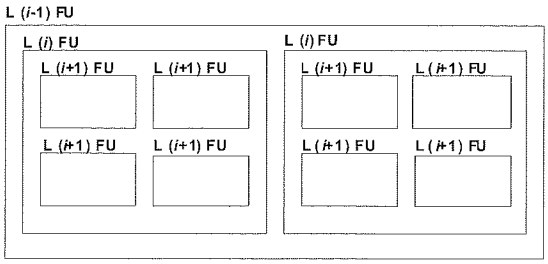
[IEV 191-04-19]

NOTE 1 Corrective maintenance without modification will usually not eliminate the failure cause.

NOTE 2 A systematic failure can be induced by simulating the failure cause.

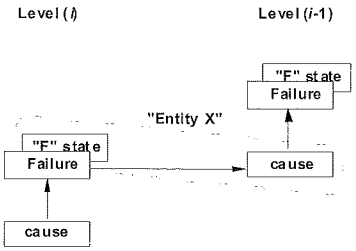
NOTE 3 Examples of causes of systematic failures include human error in
- the safety requirements specification;
- the design, manufacture, installation, operation of the hardware;
- the design, implementation, etc. of the software.

NOTE 4 In this standard, failures in a safety-related system are categorized as random hardware failures or

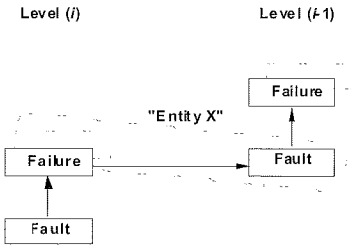


(L = level; i = 1, 2, 3 etc.; FU = functional unit)

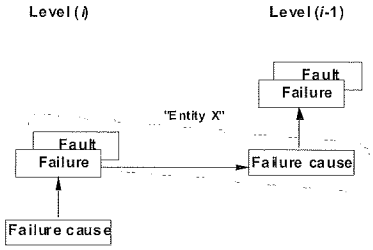
a) Configuration of a functional unit



b) Generalised view



c) From the point of view of IEC 61508 and ISO/IEC 2382-14



d) From the point of view of IEC 60050(191)

IEC 1 659/98

NOTE 1 As shown in a), a functional unit can be viewed as a hierarchical composition of multiple levels, each of which can in turn be called a functional unit. In level (i), a "cause" may manifest itself as an error (a deviation from the correct value or state) within this level (i) functional unit, and, if not corrected or circumvented, may cause a failure of this functional unit, as a result of which it falls into an "F" state where it is no longer able to perform a required function (see b)). This "F" state of the level (i) functional unit may in turn manifest itself as an error in the level (i-1) functional unit and, if not corrected or circumvented, may cause a failure of this level (i-1) functional unit.

NOTE 2 In this cause and effect chain, the same thing ("Entity X") can be viewed as a state ("F" state) of the level (i) functional unit into which it has fallen as a result of its failure, and also as the cause of the failure of the level (i-1) functional unit. This "Entity X" combines the concept of "fault" in IEC 61508 and ISO/IEC 2382-14, which emphasizes its cause aspect as illustrated in c), and that of "fault" in IEC 60050(191), which emphasizes its state aspect as illustrated in d). The "F" state is called fault in IEC 60050(191), whereas it is not defined in IEC 61508 and ISO/IEC 2382-14.

NOTE 3 In some cases, a failure or an error may be caused by an external event such as lightning or electrostatic noise, rather than by an internal fault. Likewise, a fault (in both vocabularies) may exist without a prior failure. An example of such a fault is a design fault.

Figure 4 — Failure model

3.6.7
dangerous failure

failure of an element and/or subsystem and/or system that plays a part in implementing the safety function that:

a) prevents a safety function from operating when required (demand mode) or causes a safety function to fail (continuous mode) such that the EUC is put into a hazardous or potentially hazardous state; or,

b) decreases the probability that the safety function operates correctly when required.

3.6.8
safe failure
failure of an element and/or subsystem and/or system that plays a part in implementing the safety function that:

a) results in the spurious operation of the safety function to put the EUC (or part thereof) into a safe state or maintain a safe state; or,

b) increases the probability of the spurious operation of the safety function to put the EUC (or part thereof) into a safe state or maintain a safe state.

3.6.9
dependent failure
failure whose probability cannot be expressed as the simple product of the unconditional probabilities of the individual events that caused it

NOTE Two events A and B are dependent, only if: $P(\text{A and B}) > P(\text{A}) \times P(\text{B})$

3.6.10
common cause failure
failure, that is the result of one or more events, causing coincident failures of two or more separate channels in a multiple channel system, leading to system failure

3.6.11
error
discrepancy between a computed, observed or measured value or condition and the true, specified or theoretically correct value or condition

NOTE Adapted from IEV 191-05-24 by excluding the notes

3.6.12
soft-error
erroneous changes to data content but not changes to the physical circuit itself.
NOTE 1 When a soft error has occurred and the data is rewritten, the circuit will be restored to its original state.

NOTE 2 Soft errors can occur in memory, digital logic, analogue circuits, and on transmission lines, etc and are dominant in semiconductor memory, including registers and latches.

NOTE 3 Soft errors are transient and should not be confused with software programming errors.

3.6.13
no part failure
failure of a component that plays no part in implementing the safety function

NOTE The no part failure is not used for SFF calculations

3.6.14
no effect failure
failure of an element that plays a part in implementing the safety function has no direct effect on the safety function

NOTE 1 The no effect failure has by definition no effect on the safety function so it cannot contribute to the failure rate of the safety function.))

NOTE 2 The no effect failure is not used for SFF calculations

3.6.15
safe failure fraction
SFF

property of a safety related element that is defined by the ratio of the average failure rates of safe plus dangerous detected failures and safe plus dangerous failures. This ratio is represented by the following equation:

$$SFF = (\Sigma\lambda_{S\ avg} + \Sigma\lambda_{Dd\ avg})/(\Sigma\lambda_{S\ avg} + \Sigma\lambda_{Dd\ avg} + \Sigma\lambda_{Du\ avg})$$

when the failure rates are based on constant failure rates the equation can be simplified to:

$$SFF = (\Sigma\lambda_S + \Sigma\lambda_{Dd})/(\Sigma\lambda_S + \Sigma\lambda_{Dd} + \Sigma\lambda_{Du})$$

3.6.16
failure rate

reliability parameter ($\lambda(t)$) of an entity (single components or systems) such that $\lambda(t).dt$ is the probability of failure of this entity within [t, t+dt] provided that it has not failed during [0, t]

NOTE 1 Mathematically, $\lambda(t)$ is the conditional probability of failure per unit of time over [t, t+dt]. It is in strong relationship with the reliability function (i.e. probability of no failure from 0 to t) by the general formula $R(t) = \exp(-\int_0^t \lambda(\tau)d\tau$. Reversely it is defined from the reliability function by $\lambda(t) = -\frac{dR(t)}{dt}\frac{1}{R(t)}$.

NOTE 2 Failure rates and their uncertainties can be estimated from field feedback by using conventional statistics. During the "useful life" (i.e. after burn-in and before wear-out), the failure rate of a simple items is more or less constant, $\lambda(t) \equiv \lambda$.

NOTE 3 The average of $\lambda(t)$ over a given period [0, T], $\lambda_{avg}(T) = (\int_0^T \lambda(\tau)d\tau)/T$, is not a failure rate because it cannot be used for calculating R(t) as shown in NOTE 1. Anyway it may be interpreted as the *average frequency* of failure over this period (i.e. the PFH, see part 6 annex B)).

NOTE 4 The failure rate of a series of items is the sum of the failure rates of each items.

NOTE 5 The failure rate of redundant systems is generally non constant. Nevertheless when all failures are quickly revealed, independent and quickly repaired, $\lambda(t)$ converges quickly to an asymptotic value λ_{as} which is the *equivalent failure rate* of the systems. It should not be confused with the average failure rate described in note 3 which doesn't necessarily converge to an asymptotic value.

3.6.17
probability of dangerous failure on demand
PFD

safety unavailability (see IEC 60050-191) of an E/E/PE safety-related system to perform the specified safety function when a demand occurs from the EUC or EUC control system

NOTE 1 The [instantaneous] unavailability (as per IEC 60050-191) is the probability that an item is not in state to perform a required function under given conditions at a given instant of time, assuming that the required external resources are provided. It is generally noted by U (t).

NOTE 2 The [instantaneous] availability does not depend on the states (running or failed) experienced by the item before t. It characterizes an item which only has to be able to work when it is required to do so, for example, an E/E/EP safety related system working in low demand mode

NOTE 3 If periodically tested, the PFD of an E/E/PE safety-related system is, in respect of the specified safety function, represented by a saw tooth curve with a large range of probabilities ranging from low, just after a test, to a maximum just before a test.

3.6.18
average probability of dangerous failure on demand
PFDavg
mean unavailability (see IEC 60050-191) of an E/E/PE safety-related system to perform the specified safety function when a demand occurs from the EUC or EUC control system

NOTE 1 The mean unavailability over a given time interval [t1, t2] is generally noted by U (t1, t2).

NOTE 2 Two kind of failures contribute to **PFD** and $\mathbf{PFD_{avg}}$: the *dangerous undetected failures* occurred since the last proof test and genuine *on demand failures* caused by the demands (proof tests and safety demands) themselves. The first one is *time dependent* and characterized by their dangerous failure rate $\lambda_{DU}(t)$ whilst the second one is dependent only on the number of demands and is characterized by a *probability of failure per demand* (denoted by γ).

NOTE 3 As genuine "on demand" failures cannot be detected by tests, it is necessary to identify them and take them into consideration when calculating the target failure measures.

3.6.19
probability of dangerous failure per hour
PFH
average frequency of a dangerous failure over a given period of time of an E/E/PE safety-related system to perform the specified safety function

NOTE 1 The term probability of dangerous failure per hour" is not used in the standard but the acronym PFH has been retained but when it is used it means "average frequency of dangerous failure [h-1].

NOTE 2 From a theoretical point of view, the PFH is the average of the *unconditional failure intensity,*also called *failure frequency,* and which is generally designated w(t). It should not be confused with a failure rate (see part 6 annex B).

NOTE 3 When the E/E/PE safety-related system is the ultimate safety layer, the PFH should be calculated from its *unreliability* F(T)=1-R(t) (see failure rate above). When it is not the ultimate safety-related system its PFH shall be calculated from its *unavailability* U(t) (see PFD above). PFH approximations are given by F(T)/T and 1/MTTF in the first case and 1/MTBF in the second case.

NOTE 4 when the E/E/PE safety-related system implies only quickly repaired revealed failures then an asymptotic failure rate λ_{as} is quickly reached. It provides an estimate of the PFH.

3.6.20
diagnostic test interval
interval between on-line tests to detect faults in a safety-related system that has a specified diagnostic coverage

3.6.21
process safety time
period of time between a failure, that has the potential to give rise to a hazardous event, occurring in the EUC or EUC control system and the time by which action has to be completed in the EUC to prevent the hazardous event occurring

3.7 Lifecycle activities

3.7.1
safety lifecycle
necessary activities involved in the implementation of safety-related systems, occurring during a period of time that starts at the concept phase of a project and finishes when all of the E/E/PE safety-related systems and other risk reduction measures are no longer available for use

NOTE 1 The term "functional safety lifecycle" is more accurate, but the adjective "functional" is not considered necessary in this case within the context of this standard.

NOTE 2 The safety lifecycle models used in this standard are specified in Figures 2, 3 and 4 of IEC 61508-1.

3.7.2
software lifecycle
activities occurring during a period of time that starts when software is conceived and ends when the software is permanently decommissioned

NOTE 1 A software lifecycle typically includes a requirements phase, development phase, test phase, integration phase, installation phase and a modification phase.

NOTE 2 Software is not capable of being maintained; rather, it is modified.

3.7.3
configuration management
discipline of identifying the components of an evolving system for the purposes of controlling changes to those components and maintaining continuity and traceability throughout the lifecycle

NOTE For details on software configuration management see IEC 61508-7.

3.7.4
configuration baseline
the information that allows the software release to be recreated in an auditable and systematic way, including: all source code, data, run time files, documentation, configuration files, and installation scripts that comprise a software release; information about compilers, operating systems, and development tools used to create the software release

3.7.5
impact analysis
activity of determining the effect that a change to a function or component in a system will have to other functions or components in that system as well as to other systems

NOTE In the context of software, see C.5.23 of IEC 61508-7.

3.8 Confirmation of safety measures

3.8.1
verification
confirmation by examination and provision of objective evidence that the requirements have been fulfilled

NOTE 1 Adapted from ISO 8402 by excluding the notes.

NOTE 2 In the context of this standard, verification is the activity of demonstrating for each phase of the relevant safety lifecycle (overall, E/E/PES and software), by analysis, mathematical reasoning and/or tests, that, for the specific inputs, the outputs meet in all respects the objectives and requirements set for the specific phase.

EXAMPLE Verification activities include

– reviews on outputs (documents from all phases of the safety lifecycle) to ensure compliance with the objectives and requirements of the phase, taking into account the specific inputs to that phase;

– design reviews;

– tests performed on the designed products to ensure that they perform according to their specification;

– integration tests performed where different parts of a system are put together in a step-by-step manner and by the performance of environmental tests to ensure that all the parts work together in the specified manner.

3.8.2
validation
confirmation by examination and provision of objective evidence that the particular requirements for a specific intended use are fulfilled

NOTE 1 Adapted from ISO 8402 by excluding the notes.

NOTE 2 In this standard there are three validation phases:

– overall safety validation (see Figure 2 of IEC 61508-1);
– E/E/PES validation (see Figure 3 of IEC 61508-1);
– software validation (see Figure 4 of IEC 61508-1).

NOTE 3 Validation is the activity of demonstrating that the safety-related system under consideration, before or after installation, meets in all respects the safety requirements specification for that safety-related system. Therefore, for example, software validation means confirming by examination and provision of objective evidence that the software satisfies the software safety requirements specification.

3.8.3
functional safety assessment
investigation, based on evidence, to judge the functional safety achieved by one or more E/E/PE safety-related systems and/or other risk reduction measures

3.8.4
functional safety audit
systematic and independent examination to determine whether the procedures specific to the functional safety requirements to comply with the planned arrangements are implemented effectively and are suitable to achieve the specified objectives

NOTE A functional safety audit may be carried out as part of a functional safety assessment.

3.8.5
proof test
periodic test performed to detect dangerous hidden failures in a safety-related system so that, if necessary, a repair can restore the system to an "as new" condition or as close as practical to this condition

NOTE 1 in this standard the term "proof test" is used but it is recognised that a synonymous term is "periodical test".

NOTE 2 The effectiveness of the proof test will be dependent both on failure coverage and repair effectiveness. In practice detecting 100 % of the hidden dangerous failures is not easily achieved for other than low-complexity E/E/PE safety-related systems. This should be the target. As a minimum, all the safety functions which are executed are checked according to the E/E/PES safety requirements specification. If separate channels are used, these tests are done for each channel separately. For complex elements an analysis may need to be performed in order to demonstrate that the probability of hidden dangerous failure not detected by proof tests is negligible over the whole life duration of the E/E/EP safety related system.

NOTE 3 A proof test needs some time to be achieved. During this time the E/E/EP safety related system may be inhibited partially or completely. The proof test duration can be neglected only if the part of the E/E/EP safety related system under test remains available in case of a demand for operation or if the EUC is shut down during the test.

NOTE 4 During a proof test, the E/E/EP safety related system may be partly or completely unavailable to respond to a demand for operation. The MTTR (Mean Time To Repair) can be neglected for SIL calculations only if the EUC is shut down during repair or if other risk measures are put in place with equivalent effectiveness.

3.8.6
diagnostic coverage
DC
the fraction of dangerous failures detected by automatic on-line diagnostic tests. The fraction of dangerous failures is computed by using the dangerous failure rates associated with the detected dangerous failures divided by the total rate of dangerous failures

NOTE 1 The dangerous failure diagnostic coverage is computed using the following equation, where *DC* is the diagnostic coverage, λ_{DD} is the detected dangerous failure rate and $\lambda_{D\ total}$ is the total dangerous failure rate:

$$DC = \frac{\sum \lambda_{DD}}{\sum \lambda_{Dtotal}}$$

NOTE 2 This definition is applicable providing the individual components have constant failure rates.

3.8.7
diagnostic test interval
interval between on-line tests to detect faults in a safety-related system that has a specified diagnostic coverage

3.8.8
detected
revealed
overt
in relation to hardware, detected by the diagnostic tests, proof tests, operator intervention (for example physical inspection and manual tests), or through normal operation

EXAMPLE These adjectives are used in detected fault and detected failure.

NOTE A dangerous failure detected by diagnostic test behaves like a revealed failure. It behaves like a safe failure only if measures, automatic of manual, are taken to do so.

3.8.9
undetected
unrevealed
covert
in relation to hardware, undetected by the diagnostic tests, proof tests, operator intervention (for example physical inspection and manual tests), or through normal operation

EXAMPLE These adjectives are used in undetected fault and undetected failure.

3.8.10
assessor
person, persons or organization that performs the functional safety assessment in order to arrive at a judgement on the functional safety achieved by the E/E/PE safety-related systems and other risk reduction measures

NOTE See also IEC 61508-1, Clause 8.

3.8.11
independent person
person who is separate and distinct from the activities that take place during the specific phase of the overall, E/E/PES or software safety lifecycle that is subject to the functional safety assessment or validation, and does not have direct responsibility for those activities

3.8.12
independent department
department that is separate and distinct from the departments responsible for the activities that take place during the specific phase of the overall, E/E/PES or software safety lifecycle that is subject to the functional safety assessment or validation

3.8.13
independent organisation
organisation that is separate and distinct, by management and other resources, from the organisations responsible for the activities that take place during the specific phase of the overall, E/E/PES or software safety lifecycle that is subject to the functional safety assessment or validation

3.8.14
animation
simulated operation of the software system (or of some significant portion of the system) to display significant aspects of the behaviour of the system, for instance applied to a requirements specification in an appropriate format or an appropriate high-level representation of the system design

NOTE Animation can give extra confidence that the system meets the real requirements because it improves human recognition of the specified behaviour.

3.8.15
dynamic testing
executing software and/or operating hardware in a controlled and systematic way, so as to demonstrate the presence of the required behaviour and the absence of unwanted behaviour

NOTE Dynamic testing contrasts with static analysis, which does not require the software to be executed or hardware to be in operation.

3.8.16
test harness
facility that is capable of simulating (to some useful degree) the operating environment of software or hardware under development, by applying test cases to the software and recording the response

NOTE The test harness may also include test case generators and facilities to verify the test results (either automatically against values that are accepted as correct or by manual analysis).

3.8.17
compliant item safety manual
document that provides all the information relating to the functional safety of an element, in respect of specified element safety functions, that is required to ensure that the system meets the requirements of IEC 61508

3.8.18
proven in use
demonstration, based on an analysis of operational experience for a specific configuration of an element, that the likelihood of an dangerous systematic faults is low enough so that every safety function that uses the element achieves its required safety integrity level

Bibliography

[1] IEC 61511 (all parts), *Functional safety – Safety instrumented systems for the process industry sector*

[2] IEC 62061, *Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems*

[3] IEC TR 61508-0:2005, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 0: Functional safety and IEC 61508*

[4] IEC 61508-5:—, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 5: Examples of methods for the determination of safety integrity levels* [3)]

[5] IEC 61508-6:—, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3* [3)]

[6] IEC 61508-7:—, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 7: Overview of techniques and* measures [3)]

[7] ISO/IEC 2382-1:1993, *Information technology – Vocabulary – Part 1: Fundamental terms*

[8] IEC 61131-3:2003, *Programmable controllers – Part 3: Programming languages*

INDEX