

	DIN EN 61511-1 (VDE 0810-1)	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 01.040.25; 01.040.35; 25.040.40; 35.240.50 Ersatz für DIN EN 61511-1 (VDE 0810-1):2005-05 Siehe Anwendungsbeginn Funktionale Sicherheit – PLT-Sicherheitseinrichtungen für die Prozessindustrie – Teil 1: Allgemeines, Begriffe, Anforderungen an Systeme, Hardware und Anwendungsprogrammierung (IEC 61511-1:2016 + COR1:2016 + A1:2017); Deutsche Fassung EN 61511-1:2017 + A1:2017 Functional safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and application programming Requirements (IEC 61511-1:2016 + COR1:2016 + A1:2017); German version EN 61511-1:2017 + A1:2017 Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur des industries de transformation – Partie 1: Cadre, définitions, exigences pour le système, le matériel et la programmation d'application (IEC 61511-1:2016 + COR1:2016 + A1:2017); Version allemande EN 61511-1:2017 + A1:2017 Gesamtumfang 100 Seiten DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE		

Anwendungsbeginn

Anwendungsbeginn für die von CENELEC am 2016-03-30 angenommene Europäische Norm und die am 2017-09-20 angenommene Änderung A1 als DIN-Norm ist 2019-02-01.

Für **DIN EN 61511-1 (VDE 0810-1):2005-05** besteht eine Übergangsfrist bis 2020-09-20.

Nationales Vorwort

Vorausgegangener Norm-Entwurf: E DIN EN 61511-1 (VDE 0810-1):2012-10 und E DIN EN 61511-1/A1 (VDE 0810-1/A1):2017-11.

Für dieses Dokument 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 in DIN und VDE (www.dke.de) zuständig.

Die enthaltene IEC-Publikation wurde vom SC 65A „System aspects“ erarbeitet.

Das IEC-Komitee hat entschieden, dass der Inhalt dieses Dokuments bis zu dem Datum (stability date) unverändert bleiben soll, das auf der IEC-Website unter „<http://webstore.iec.ch>“ zu diesem Dokument angegeben ist. Zu diesem Zeitpunkt wird entsprechend der Entscheidung des Komitees das Dokument

- bestätigt,
- zurückgezogen,
- durch eine Folgeausgabe ersetzt oder
- geändert.

A1 Die Änderung A1 wurde eingearbeitet und mit einer senkrechten Linie und A1 am linken Textrand gekennzeichnet.

Das IEC-Corrigendum 1 zu IEC 61511-1:2016 wurde in den Text eingearbeitet.

Änderungen

Gegenüber **DIN EN 61511-1 (VDE 0810-1):2005-05** wurden folgende Änderungen vorgenommen:

- a) Anforderungen an die Software ersetzt durch Anforderungen an die Anwendungsprogrammierung;
- b) Um das Management der funktionalen Sicherheit zu verbessern, wurden die Anforderungen an die Beurteilung der funktionalen Sicherheit weiter ausgeführt;
- c) Anforderungen an die Verfahren bei Modifikation hinzugefügt;
- d) Zur Gefährdungs- und Risikobeurteilung die Informationssicherheit hinzugefügt;
- e) Anforderungen an die Betriebseinrichtungen ausgeweitet, sofern sie als Schutzebene dienen;
- f) Anforderungen zur Hardwarefehlertoleranz wurden geändert. Anwender und Integratoren sollten sie sorgfältig durchsehen, um alle Möglichkeiten zu verstehen.

Frühere Ausgaben

DIN EN 61511-1 (VDE 0810-1): 2005-05

Nationaler Anhang NA (informativ)

Zusammenhang mit europäischen und internationalen Dokumenten

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

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

Eine Information über den Zusammenhang der zitierten Dokumente mit den entsprechenden deutschen Dokumenten ist nachstehend wiedergegeben.

Tabelle NA.1

Europäisches Dokument	Internationales Dokument	Deutsches Dokument	Klassifikation im VDE-Vorschriftenwerk
	IEC 60050 (alle Teile)	a	
–	ISO/IEC Guide 51:2014	DIN 820-12:2014-06	–
EN 60300-3-2:2005	IEC 60300-3-2:2004	DIN EN 60300-3-2:2005-08	–
–	IEC 60605-4:2001	DIN IEC 60605-4:2002-08	–
EN 60617-12:1998	IEC 60617-12:1997	DIN EN 60617-12:1999-04	–
EN 61000-1-2:2016	IEC/TS 61000-1-2:2008 <i>ersetzt durch</i> IEC 61000-1-2:2016	DIN EN 61000-1-2 (VDE 0839-1-2):2017-07	VDE 0839-1-2
EN 61025	IEC 61025	DIN EN 61025	–
EN 61131-3:2013	IEC 61131-3:2013	DIN EN 61131-3:2014-06	–
EN 61131-6:2012	IEC 61131-6:2012	DIN EN 61131-6 (VDE 0411-506):2013-10	VDE 0411-506
–	IEC 61506:1997	–	–
EN 61508-4:2010	IEC 61508-4:2010	DIN EN 61508-4 (VDE 0803-4):2011-02	VDE 0803-4
EN 61508-6:2010	IEC 61508-6:2010	DIN EN 61508-6 (VDE 0803-6):2011-02	VDE 0803-6
EN 61511-2:2017	IEC 61511-2:2016	DIN EN 61511-2 (VDE 0810-2):2019-02	VDE 0810-2
EN 61511-3:2017	IEC 61511-3:2016	DIN EN 61511-3 (VDE 0810-3):2019-02	VDE 0810-3
EN 61784-3:2010 <i>ersetzt durch</i>	IEC 61784-3:2010 <i>ersetzt durch</i>	DIN EN 61784-3 (VDE 0803-500):2011-02 <i>ersetzt durch</i>	VDE 0803-500
EN 61784-3:2016	IEC 61784-3:2016	DIN EN 61784-3 (VDE 0803-500):2017-09	VDE 0803-500
–	IEC 62443-2-1:2010	–	–

Europäisches Dokument	Internationales Dokument	Deutsches Dokument	Klassifikation im VDE-Vorschriftenwerk
EN 62682:2015	IEC 62682:2014	DIN EN 62682 (VDE 0810-682):2016-02	VDE 0810-682
–	ISO/IEC 2382:2006	–	–
EN ISO/IEC 27001:2017	ISO/IEC 27001:2013	DIN EN ISO/IEC 27001:2017-06	–
–	ISO/IEC 90003:2014	–	–
–	ISO 2382-1:1993	–	–
EN ISO 9000:2005 <i>ersetzt durch</i>	ISO 9000:2005 <i>ersetzt durch</i>	DIN EN ISO 9000:2005-12	–
EN ISO 9000:2015	ISO 9000:2015	DIN EN ISO 9000:2015-11	
EN ISO 9001:2008	ISO 9001:2008		
EN ISO 9001:2015	ISO 9001:2015	DIN EN ISO 9001:2015-11	
–	ISO/TR 12489:2013	–	–
EN ISO 13849-1:2006 <i>ersetzt durch</i>	ISO 13849-1:2006 <i>ersetzt durch</i>	DIN EN ISO 13849-1:2008-12 <i>ersetzt durch</i>	–
EN ISO 13849-1:2015	ISO 13849-1:2015	DIN EN ISO 13849-1:2016-06	
EN ISO 13849-2:2012	ISO 13849-2:2012	DIN EN ISO 13849-2:2013-02	–
EN ISO 14224:2006 <i>ersetzt durch</i>	ISO 14224:2006 <i>ersetzt durch</i>	DIN EN ISO 14224:2007-04 <i>ersetzt durch</i>	–
EN ISO 14224:2016	ISO 14224:2016	DIN EN ISO 14224:2017-04	–
^a „Internationales Elektrotechnisches Wörterbuch – Deutsche Ausgabe“, Online-Zugang: http://www.dke.de/dke-iev .			

Nationaler Anhang NB (informativ)

Literaturhinweise

DIN 820-12:2014-06, *Normungsarbeit – Teil 12: Leitfaden für die Aufnahme von Sicherheitsaspekten in Normen (ISO/IEC Guide 51:2014)*

DIN EN 60300-3-2:2005-08, *Zuverlässigkeitsmanagement – Teil 3-2: Anwendungsleitfaden – Erfassung von Zuverlässigkeitsdaten im Betrieb (IEC 60300-3-2:2004); Deutsche Fassung EN 60300-3-2:2005*

DIN IEC 60605-4:2002-08, *Prüfung der Zuverlässigkeit von Geräten – Teil 4: Statistische Verfahren für Exponentialverteilungen – Schätzwerte, Vertrauensbereiche, Vorhersageintervalle und Toleranzintervalle (IEC 60605-4:2001)*

DIN EN 60617-12:1999-04, *Graphische Symbole für Schaltpläne – Teil 12: Binäre Elemente (IEC 60617-12:1997); Deutsche Fassung EN 60617-12:1998*

DIN EN 61000-1-2 (VDE 0839-1-2):2017-07, *Elektromagnetische Verträglichkeit (EMV) – Teil 1-2: Allgemeines – Verfahren zum Erreichen der funktionalen Sicherheit von elektrischen und elektronischen Systemen einschließlich Geräten und Einrichtungen im Hinblick auf elektromagnetische Phänomene (IEC 61000-1-2:2016); Deutsche Fassung EN 61000-1-2:2016*

DIN EN 61025, Fehlzustandsbaumanalyse

DIN EN 61131-3:2014-06, Speicherprogrammierbare Steuerungen – Teil 3: Programmiersprachen (IEC 61131-3:2013); Deutsche Fassung EN 61131-3:2013

DIN EN 61131-6 (VDE 0411-506):2013-10, Speicherprogrammierbare Steuerungen – Teil 6: Funktionale Sicherheit (IEC 61131-6:2012); Deutsche Fassung EN 61131-6:2012

DIN EN 61508-4 (VDE 0803-4):2011-02, Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 4: Begriffe und Abkürzungen (IEC 61508-4:2010); Deutsche Fassung EN 61508-4:2010

DIN EN 61508-6 (VDE 0803-6):2011-02, Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 6: Anwendungsrichtlinie für IEC 61508-2 und IEC 61508-3 (IEC 61508-6:2010); Deutsche Fassung EN 61508-6:2010

DIN EN 61511-2 (VDE 0810-2):2019-02, Funktionale Sicherheit – Sicherheitstechnische Systeme für die Prozessindustrie – Teil 2: Anleitungen zur Anwendung des Teils 1

DIN EN 61511-3 (VDE 0810-3):2019-02, Funktionale Sicherheit – Sicherheitstechnische Systeme für die Prozessindustrie – Teil 3: Anleitung für die Bestimmung der erforderlichen Sicherheits-Integritätslevel

DIN EN 61784-3 (VDE 0803-500):2017-09, Industrielle Kommunikationsnetze – Profile – Teil 3: Funktional sichere Übertragung bei Feldbussen – Allgemeine Regeln und Festlegungen für Profile (IEC 61784-3:2016); Deutsche Fassung EN 61784-3:2016

DIN EN 62682 (VDE 0810-682):2016-02, Alarmmanagement in der Prozessindustrie (IEC 62682:2014); Deutsche Fassung EN 62682:2015

DIN EN ISO 9000:2015-11, Qualitätsmanagementsysteme – Grundlagen und Begriffe (ISO 9000:2015); Deutsche und Englische Fassung EN ISO 9000:2015

DIN EN ISO 9001:2015-11, Qualitätsmanagementsysteme – Anforderungen (ISO 9001:2015); Deutsche und Englische Fassung EN ISO 9001:2015

DIN EN ISO/IEC 27001:2017-06, Informationstechnik – Sicherheitsverfahren – Informationssicherheitsmanagementsysteme – Anforderungen (ISO/IEC 27001:2013 einschließlich Cor 1:2014 und Cor 2:2015); Deutsche Fassung EN ISO/IEC 27001:2017

DIN EN ISO 13849-1:2016-06, Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Teil 1: Allgemeine Gestaltungsgrundsätze (ISO 13849-1:2015); Deutsche Fassung EN ISO 13849-1:2015

DIN EN ISO 13849-2:2013-02, Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Teil 2: Validierung (ISO 13849-2:2012); Deutsche Fassung EN ISO 13849-2:2012

DIN EN ISO 14224:2017-04, Erdöl-, petrochemische und Erdgasindustrie – Sammlung und Austausch von Zuverlässigkeits- und Wartungsdaten für Ausrüstungen (ISO 14224:2016, korrigierte Fassung 2016-10-01); Englische Fassung EN ISO 14224:2016, nur auf CD-ROM

**Funktionale Sicherheit –
PLT-Sicherheitseinrichtungen für die Prozessindustrie –
Teil 1: Allgemeines, Begriffe, Anforderungen an Systeme, Hardware und
Anwendungsprogrammierung
(IEC 61511-1:2016 + COR1:2016 + A1:2017)**

Functional safety –
Safety instrumented systems for the process
industry sector –
Part 1: Framework, definitions, system, hardware
and application programming Requirements
(IEC 61511-1:2016 + COR1:2016 + A1:2017)

Sécurité fonctionnelle –
Systèmes instrumentés de sécurité pour le
secteur des industries de transformation –
Partie 1: Cadre, définitions, exigences pour le
système, le matériel et la programmation
d'application
(IEC 61511-1:2016 + COR1:2016 + A1:2017)

Diese Europäische Norm wurde von CENELEC am 2016-03-30 und die A1 am 2017-09-20 angenommen. CENELEC-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist.

Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim CEN-CENELEC Management Centre oder bei jedem CENELEC-Mitglied auf Anfrage erhältlich.

Diese Europäische Norm besteht in drei offiziellen Fassungen (Deutsch, Englisch, Französisch). Eine Fassung in einer anderen Sprache, die von einem CENELEC-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem CEN-CENELEC Management Centre mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CENELEC-Mitglieder sind die nationalen elektrotechnischen Komitees von Belgien, Bulgarien, Dänemark, Deutschland, der ehemaligen jugoslawischen Republik Mazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, der Schweiz, Serbien, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, der Türkei, Ungarn, dem Vereinigten Königreich und Zypern.



Europäisches Komitee für Elektrotechnische Normung
European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

© 2017 CENELEC – Alle Rechte der Verwertung, gleich in welcher Form und in welchem Verfahren, sind weltweit den Mitgliedern von CENELEC vorbehalten.

Ref. Nr. EN 61511-1:2017 + A1:2017 D

Europäisches Vorwort

Der Text des Dokuments 65A/777/FDIS, zukünftige 2. Ausgabe der IEC 61511-1, erarbeitet vom SC 65A „System aspects“ of IEC/TC 65 „Industrial-process measurement, control and automation“, wurde zur parallelen IEC-CENELEC-Abstimmung vorgelegt und von CENELEC als EN 61511-1:2017 angenommen.

Nachstehende Daten wurden festgelegt:

- spätestes Datum, zu dem dieses Dokument auf nationaler Ebene durch Veröffentlichung einer identischen nationalen Norm oder durch Anerkennung übernommen werden muss (dop): 2017-10-21
- spätestes Datum, zu dem nationale Normen, die diesem Dokument entgegenstehen, zurückgezogen werden müssen (dow): 2020-04-21

Dieses Dokument ersetzt **EN 61511-1:2004**.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. CENELEC [und/oder CEN] ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Anerkennungsnotiz

Der Text der Internationalen Norm IEC 61511-1:2016 + COR1:2016 wurde von CENELEC ohne irgendeine Abänderung als Europäische Norm angenommen.

In der offiziellen Fassung sind unter „Literaturhinweise“ zu den aufgelisteten Normen die nachstehenden ANMERKUNGEN einzutragen:

IEC 60300-3-2:2004	ANMERKUNG	Harmonisiert als EN 60300-3-2:2005 (nicht modifiziert).
IEC 61025	ANMERKUNG	Harmonisiert als EN 61025.
IEC 61131-3:2013	ANMERKUNG	Harmonisiert als EN 61131-3:2013 (nicht modifiziert).
IEC 61131-6:2012	ANMERKUNG	Harmonisiert als EN 61131-6:2012 (nicht modifiziert).
IEC 61508-4:2010	ANMERKUNG	Harmonisiert als EN 61508-4:2010 (nicht modifiziert).
IEC 61508-6:2010	ANMERKUNG	Harmonisiert als EN 61508-6:2010 (nicht modifiziert).
IEC 61511-2	ANMERKUNG	Harmonisiert als EN 61511-2 .
IEC 61511-3	ANMERKUNG	Harmonisiert als EN 61511-3 .
IEC 61784-3:2010	ANMERKUNG	Harmonisiert als EN 61784-3:2010 (nicht modifiziert).
IEC 62682:2014	ANMERKUNG	Harmonisiert als EN 62682:2015 (nicht modifiziert).
ISO 9000:2005	ANMERKUNG	Harmonisiert als EN ISO 9000:2005 ^{Z1} (nicht modifiziert).
ISO 9001:2008	ANMERKUNG	Harmonisiert als EN ISO 9001:2008 ^{Z2} (nicht modifiziert).
ISO 13849-1:2006	ANMERKUNG	Harmonisiert als EN ISO 13849-1:2006 ^{Z3} (nicht modifiziert).
ISO 13849-2:2012	ANMERKUNG	Harmonisiert als EN ISO 13849-2:2012 (nicht modifiziert).
ISO 14224:2006	ANMERKUNG	Harmonisiert als EN ISO 14224:2006 (nicht modifiziert).

^{Z1} Wurde ersetzt durch EN ISO 9000:2015 (ISO 9000:2015).

^{Z2} Wurde ersetzt durch EN ISO 9001:2015 (ISO 9001:2015).

^{Z3} Wurde ersetzt durch EN ISO 13849-1:2015 (ISO 13849-1:2015).

Europäisches Vorwort zur Änderung A1

Der Text des Dokuments 65A/777/FDIS, zukünftige 1. Ausgabe der IEC 61511-1:2016/A1:2017, erarbeitet vom IEC/SC 65A „System aspects“, des IEC/TC 65 „Industrial-process measurement, control and automation“, wurde zur parallelen IEC-CENELEC-Abstimmung vorgelegt und von CENELEC als EN 61511-1:2017/A1:2017 angenommen.

Nachstehende Daten wurden festgelegt:

- spätestes Datum, zu dem dieses Dokument auf nationaler Ebene durch Veröffentlichung einer identischen nationalen Norm oder durch Anerkennung übernommen werden muss (dop): 2018-06-20
- spätestes Datum, zu dem nationale Normen, die diesem Dokument entgegenstehen, zurückgezogen werden müssen (dow): 2020-09-20

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. CENELEC ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Anerkennungsnotiz

Der Text der Internationalen Norm IEC 61511-1:2016/A1:2017 wurde von CENELEC ohne irgendeine Abänderung als Europäische Norm angenommen.

Ersetze die folgenden Verweisungen in den Literaturhinweisen der EN 61511-1:2017:

IEC 61511-2:2016	ANMERKUNG	Harmonisiert als EN 61511-2:2017 .
IEC 61511-3:2016	ANMERKUNG	Harmonisiert als EN 61511-3:2017 .

Anhang ZA (normativ)

Normative Verweisungen auf internationale Publikationen mit ihren entsprechenden europäischen Publikationen

Die folgenden Dokumente, die in diesem Dokument teilweise oder als Ganzes zitiert werden, 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).

ANMERKUNG 1 Ist eine internationale Publikation durch gemeinsame Abänderungen modifiziert worden, gekennzeichnet durch (mod.), dann gilt die entsprechende EN oder das HD.

ANMERKUNG 2 Aktualisierte Informationen über die in diesem Anhang aufgeführten aktuellen Fassungen der Europäischen Normen sind hier verfügbar: www.cenelec.eu.

<u>Publikation</u>	<u>Jahr</u>	<u>Titel</u>	<u>EN/HD</u>	<u>Jahr</u>
IEC 61508-1	2010	Functional safety of electrical/electronic/programmable electronic safety- related systems – Part 1: General requirements	EN 61508-1	2010
IEC 61508-2	2010	Functional safety of electrical/electronic/programmable electronic safety- related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety- related systems	EN 61508-2	2010
IEC 61508-3	2010	Functional safety of electrical/electronic/programmable electronic safety- related systems – Part 3: Software requirements	EN 61508-3	2010

Inhalt

Seite

Europäisches Vorwort	2
Europäisches Vorwort zur Änderung A1	3
Anhang ZA (normativ) Normative Verweisungen auf internationale Publikationen mit ihren entsprechenden europäischen Publikationen	4
Einleitung	8
1 Anwendungsbereich	10
2 Normative Verweisungen	13
3 Begriffe und Abkürzungen	13
3.1 Begriffe	13
3.2 Begriffe	14
3.3 Abkürzungen	37
4 Übereinstimmung mit der IEC 61511-1:2016	38
5 Management der funktionalen Sicherheit	39
5.1 Ziel	39
5.2 Anforderungen	39
6 Anforderungen an den Sicherheitslebenszyklus	44
6.1 Ziele	44
6.2 Anforderungen	46
6.3 Anforderungen an den Sicherheitslebenszyklus des Anwendungsprogramms	48
7 Verifikation	50
7.1 Ziel	50
7.2 Anforderungen	50
8 Gefährdungs- und Risikobeurteilung des Prozesses	52
8.1 Ziele	52
8.2 Anforderungen	52
9 Zuordnung der Sicherheitsfunktionen zu den Schutzebenen	54
9.1 Ziele	54
9.2 Anforderungen an den Prozess der Zuordnung	54
9.3 Anforderungen an PLT-Betriebseinrichtungen als Schutzebene	57
9.4 Anforderungen zur Vermeidung von Ausfällen infolge gemeinsamer Ursache, gleichartigen Ausfällen und abhängigen Ausfällen	58
10 Spezifikation der Sicherheitsanforderungen an die PLT-Sicherheitseinrichtung (SRS)	59
10.1 Ziel	59
10.2 Allgemeine Anforderungen	59
10.3 Sicherheitsanforderungen an die PLT-Sicherheitseinrichtung	59
11 Entwurf und Planung der PLT-Sicherheitseinrichtung (SIS)	62
11.1 Ziel	62
11.2 Allgemeine Anforderungen	62
11.3 Anforderungen an das Systemverhalten bei Entdeckung eines Fehlers	64

11.4	Hardware-Fehlertoleranz.....	64
11.5	Anforderungen an die Geräteauswahl.....	65
11.6	Feldgeräte	69
11.7	Schnittstellen	69
11.8	Anforderungen an Instandhaltungs- oder Testeinrichtungen	71
11.9	Quantifizierung zufälliger Ausfälle	72
12	Anforderungen an die Entwicklung des Anwendungsprogramms der PLT-Sicherheitseinrichtung	74
12.1	Ziel	74
12.2	Allgemeine Anforderungen	74
12.3	Entwurf des Anwendungsprogramms	75
12.4	Implementierung des Anwendungsprogramms.....	76
12.5	Anforderungen an die Verifikation des Anwendungsprogramms (Review und Test)	77
12.6	Anforderungen hinsichtlich Methodik des Anwendungsprogramms und Werkzeugen	78
13	Werksendprüfungen (FAT) (en: Factory Acceptance Tests).....	79
13.1	Ziele	79
13.2	Empfehlungen	79
14	Montage und Inbetriebnahme der PLT-Sicherheitseinrichtung.....	81
14.1	Ziele	81
14.2	Anforderungen	81
15	Sicherheits-Validierung der PLT-Sicherheitseinrichtung.....	82
15.1	Ziel	82
15.2	Anforderungen	82
16	Betrieb und Instandhaltung der PLT-Sicherheitseinrichtung.....	85
16.1	Ziele	85
16.2	Anforderungen	85
16.3	Funktionsprüfungen und Inspektionen	88
17	Modifikationen der PLT-Sicherheitseinrichtung.....	89
17.1	Ziele	89
17.2	Anforderungen	89
18	Außerbetriebnahme der PLT-Sicherheitseinrichtung	90
18.1	Ziele	90
18.2	Anforderungen	90
19	Anforderungen an die Information und Dokumentation	91
19.1	Ziele	91
19.2	Anforderungen	91
	Literaturhinweise.....	93

Bilder

Bild 1 – Gesamtrahmen der IEC 61511-Reihe	9
Bild 2 – Beziehung zwischen IEC 61508 und IEC 61511	11
Bild 3 – Detaillierte Beziehung zwischen IEC 61508 und IEC 61511	12
Bild 4 – Zusammenhang zwischen PLT-Sicherheitsfunktionen und anderen Funktionen	13
Bild 5 – Programmierbares elektronisches System (PES), Struktur und Begriffe	28
Bild 6 – Beispiel einer Architektur einer PLT-Sicherheitseinrichtung mit drei Teilsystemen	31
Bild 7 – Phasen des Sicherheitslebenszyklus einer PLT-Sicherheitseinrichtung und Stufen der Beurteilung der funktionalen Sicherheit	45
Bild 8 – Sicherheitslebenszyklus des Anwendungsprogramms und Verhältnis zum Lebenszyklus der PLT-Sicherheitseinrichtung	48
Bild 9 – Typische Schutzebenen und Maßnahmen zur Risikominderung	57

Tabellen

Tabelle 1 – In der IEC 61511 verwendete Abkürzungen	37
Tabelle 2 – Übersicht über den Sicherheitslebenszyklus einer PLT-Sicherheitseinrichtung	46
Tabelle 3 – Sicherheitslebenszyklus des Anwendungsprogramms: Übersicht	49
Tabelle 4 – Anforderungen bezüglich der Sicherheits-Integritäts: PFD_{avg}	54
Tabelle 5 – Anforderungen bezüglich der Sicherheits-Integritäts: durchschnittliche Häufigkeit gefährlicher Ausfälle einer PLT-Sicherheitsfunktion	55
Tabelle 6 – Mindest-Hardware-Fehlertoleranz in Abhängigkeit vom SIL	65

Einleitung

PLT-Sicherheitseinrichtungen (Sicherheitstechnische Systeme, SIS) sind seit vielen Jahren für PLT-Sicherheitsfunktionen (SIF) in der Prozessindustrie im Einsatz. Wenn der Einsatz der Prozessleittechnik für PLT-Sicherheitsfunktionen effizient sein soll, dann muss sie bestimmten Mindestanforderungen entsprechen.

Die IEC 61511-Reihe behandelt die Anwendung von PLT-Sicherheitseinrichtungen in der Prozessindustrie. Sie behandelt außerdem die Gefährdungs- und Risikoanalyse des Prozesses, die durchzuführen ist, um die Spezifikation der PLT-Sicherheitseinrichtungen daraus abzuleiten. Die Beiträge anderer Sicherheitseinrichtungen werden nur im Hinblick auf die Anforderungen an die PLT-Sicherheitseinrichtung betrachtet. Dieses umfasst dabei alle zur Ausführung einer PLT-Sicherheitsfunktion erforderlichen Geräte vom Sensor bis zum Aktor.

Der „Sicherheitslebenszyklus einer PLT-Sicherheitseinrichtung“ und der „Sicherheits-Integritätslevel“ (SIL) bilden die Grundlage für die Anwendung dieser Internationalen Norm..

Die in der IEC 61511-Reihe betrachteten PLT-Sicherheitseinrichtungen beruhen auf elektrischer/elektronischer/programmierbarer elektronischer Technologie. Wenn andere Technologien für Logiksysteme (Steuerungen) verwendet werden, können die grundlegenden Prinzipien dieser Norm in entsprechender Weise angewendet werden, um sicherzustellen, dass die Anforderungen an die funktionale Sicherheit erfüllt werden. In der IEC 61511-Reihe werden auch die Sensoren und Aktoren von PLT-Sicherheitseinrichtungen betrachtet, unabhängig von der Technologie, in der sie ausgeführt sind. Die IEC 61511-Reihe wurde als sektorspezifische Ausprägung der IEC 61508-Reihe entwickelt. Die IEC 61511-Reihe ist innerhalb des Rahmens der IEC 61508 zugeschnitten auf die Prozessindustrie.

Die IEC 61511-Reihe beschreibt die notwendigen Tätigkeiten im Sicherheits-Lebenszyklus, damit die oben genannten Mindestanforderungen erfüllt werden können. Dieser Ansatz wurde gewählt, damit eine überlegte und einheitliche technische Vorgehensweise zustande kommt.

In den meisten Fällen lässt sich die Sicherheit am besten durch den Entwurf eines sicheren Prozesses gewährleisten. Dies ist jedoch in manchen Fällen nicht möglich oder umsetzbar. Wenn erforderlich kann dies mit einem oder mehreren Schutzsystemen im Hinblick auf jegliche identifizierte Restrisiken verbunden werden. Schutzsysteme können auf unterschiedlichen Technologien (chemische, mechanische, hydraulische, pneumatische, elektrische, elektronische, programmierbar elektronische) beruhen. Um diesen Ansatz zu erleichtern,

- spricht die IEC 61511-Reihe die Durchführung einer Gefährdungs- und Risiko-Beurteilung an, um die übergreifenden Sicherheitsanforderungen festzulegen;
- hebt die IEC 61511-Reihe auf die Zuordnung der Sicherheitsanforderungen zu den PLT-Sicherheitseinrichtungen ab;
- arbeitet die IEC 61511-Reihe innerhalb eines Betrachtungsrahmens, der alle sicherheitstechnischen Methoden zur Erlangung funktionaler Sicherheit umfasst;
- führt die IEC 61511-Reihe die Ausführung bestimmter Tätigkeiten, die sich auf alle Methoden zur Erlangung der funktionalen Sicherheit anwenden lassen, wie z. B. Sicherheits-Management, im einzelnen aus..

Die IEC 61511-Reihe zum Thema PLT-Sicherheitseinrichtungen für die Prozessindustrie

- behandelt alle Phasen innerhalb des Sicherheits-Lebenszyklus vom anfänglichen Konzept, Entwurf, Ausführung, Betrieb und Instandhaltung bis hin zur Außerbetriebnahme;
- erlaubt es, bereits bestehende oder neue landesspezifische Normen für die Prozessindustrie mit dieser Norm zu harmonisieren.

Die IEC 61511-Reihe strebt nach einer hohen Übereinstimmung (beispielsweise bezüglich zugrundeliegender Prinzipien, Terminologie, Dokumentation) innerhalb der Prozessindustrie. Dies sollte sowohl Vorteile für die Sicherheit als auch ökonomische Vorteile bringen. [Bild 1](#) zeigt den Gesamtrahmen der IEC 61511-Reihe.

In Staaten, in denen von Seiten des Gesetzgebers (beispielsweise durch Bund, Länder oder Gemeinden) Vorschriften bezüglich Prozessentwurf, Prozesssicherheitsmanagement oder andere Regeln erlassen wurden, haben diese Vorrang gegenüber den Anforderungen dieser Norm.

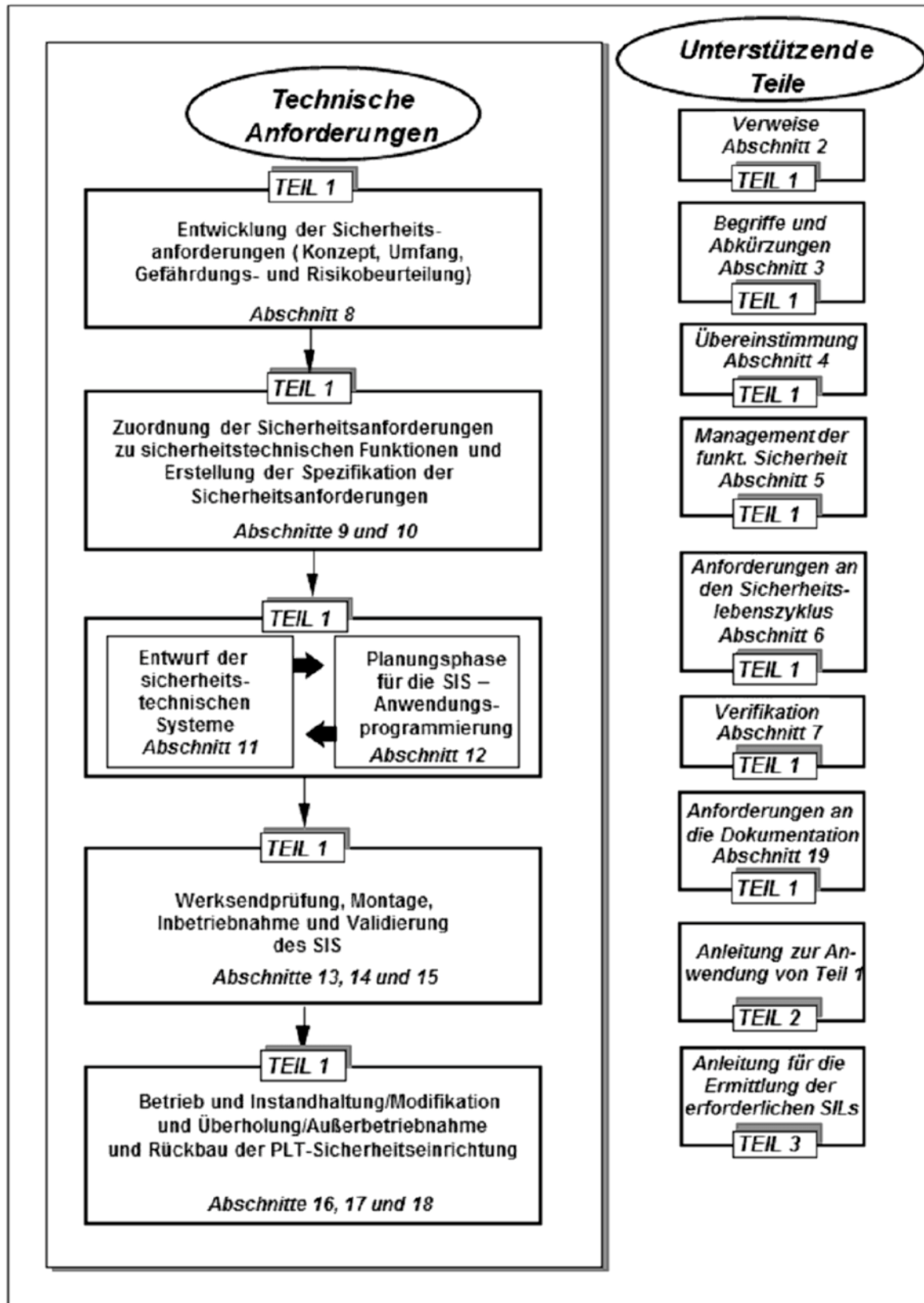


Bild 1 – Gesamtrahmen der IEC 61511-Reihe

1 Anwendungsbereich

Dieser Teil der IEC 61511 stellt Anforderungen an die Spezifikation, den Entwurf, die Installation, den Betrieb und die Instandhaltung einer PLT-Sicherheitseinrichtung (SIS) auf, so dass dieses den Prozess in einen sicheren Zustand versetzen oder in einem sicheren Zustand halten kann. IEC 61511-1 wurde als Umsetzung der Internationalen Norm IEC 61508:2010 für die Prozessindustrie erstellt.

Insbesondere, die IEC 61511-1

- a) stellt Anforderungen zur Erreichung der funktionalen Sicherheit auf, legt jedoch nicht fest, wer für die Erfüllung dieser Anforderungen verantwortlich ist (beispielsweise Planer, Lieferanten, Eigentümer/Betreiber, Kontraktoren). Diese Verantwortlichkeit wird den Beteiligten im Rahmen der Sicherheitsplanung, der Projektplanung, des Projektmanagements oder nationaler Vorschriften zugewiesen;
- b) ist anwendbar, wenn Geräte, die den Anforderungen der IEC 61508 Serie 2010 oder IEC 61511-1:2016 [11.5] entsprechen, in ein Gesamtsystem integriert werden, das in der Prozessindustrie eingesetzt werden soll. Sie ist nicht anwendbar, wenn Hersteller die Eignung von Geräten als PLT-Sicherheitseinrichtungen in der Prozessindustrie erklären wollen (siehe IEC 61508-2:2010 und IEC 61508-3:2010);
- c) beschreibt den Zusammenhang zwischen der IEC 61511 und der IEC 61508 (siehe Bild 2 und Bild 3);
- d) ist anwendbar, wenn Anwendungsprogramme für Systeme mit Sprachen eingeschränkten Sprachumfangs oder Geräte mit festen Programmen erstellt werden; sie trifft jedoch nicht zu für Hersteller, Planer von PLT-Sicherheitseinrichtungen, Systemerrichter und Anwender, die Embedded-Software entwickeln oder Sprachen mit nicht eingeschränktem Sprachumfang benutzen (siehe IEC 61508-3:2010);
- e) gilt für einen weiten Bereich von Industrien innerhalb der Prozessindustrie, beispielsweise Chemie, Öl- und Gasindustrie, Papierherstellung, Pharma-, Nahrungs- und Getränkeindustrie und nicht-nukleare Stromerzeugung;

ANMERKUNG 1 Innerhalb der Prozessindustrie können für einzelne Anwendungen zusätzliche Anforderungen gelten, die beachtet werden müssen.

- f) zeigt den Zusammenhang zwischen PLT-Sicherheitsfunktionen und anderen PLT-Funktionen (siehe Bild 4);
- g) führt zu einer Aufstellung der funktionalen Anforderungen und der Anforderungen an die Sicherheitsintegrität der PLT-Sicherheitsfunktionen unter Berücksichtigung der mit anderen Methoden erreichten Risikominderung;
- h) legt Anforderungen an den Lebenszyklus bezüglich Systemarchitektur, Hardwarekonfiguration, Anwendungsprogramme und die Systemintegration fest;
- i) legt Anforderungen an die Anwendungsprogrammierung für Anwender und Systemerrichter von PLT-Sicherheitseinrichtungen fest.
- j) gilt dann, wenn die funktionale Sicherheit mit einer oder mehreren PLT-Sicherheitsfunktionen zum Schutz der Mitarbeiter, der Öffentlichkeit oder der Umwelt erreicht wird;
- k) kann auch in Nicht-Sicherheitsanwendungen, beispielsweise zum Schutz eines Wirtschaftsguts angewendet werden;
- l) legt Anforderungen fest, nach denen PLT-Sicherheitsfunktion als Teil einer Gesamt-Methode zum Erlangen der funktionalen Sicherheit ausgeführt werden müssen;
- m) verwendet einen Sicherheitslebenszyklus für PLT-Sicherheitseinrichtungen (siehe Bild 7) und legt eine Reihe von Tätigkeiten fest, die notwendig sind, um die funktionalen Anforderungen und die erforderliche Sicherheitsintegrität für PLT-Sicherheitseinrichtungen festzulegen;
- n) fordert eine Gefährdungs- und Risikobeurteilung, in der die Anforderungen an die funktionale Sicherheit und an den Sicherheits-Integritätslevel (SIL) für jede einzelne PLT-Sicherheitsfunktion festgelegt werden;

ANMERKUNG 2 Bild 9 zeigt eine Übersicht über Methoden zur Risikominderung.

- o) definiert Zielwerte für die mittlere Ausfallwahrscheinlichkeit bei Anforderung (in der Anforderungsbetriebsart) und die mittlere Häufigkeit gefährlicher Ausfälle (in der Betriebsart mit hoher Anforderungsrate oder der kontinuierlichen Betriebsart) für die verschiedenen Sicherheits-Integritätslevel;

- p) stellt Mindestanforderungen an die Fehlertoleranz der Hardware (HFT);
- q) schreibt die zum Erreichen der geforderten SIL notwendigen Vorgehensweisen und Maßnahmen vor;
- r) definiert einen höchsten Sicherheits-Integritätslevel (SIL 4), welchen eine nach der IEC 61511-1 ausgelegte PLT-Sicherheitsfunktion erreichen kann;
- s) definiert einen niedrigsten Sicherheits-Integritätslevel (SIL 1), unterhalb dessen die IEC 61511-1 nicht mehr gültig ist;
- t) gibt einen Rahmen zur Festlegung von Sicherheits-Integritätsleveln vor, ohne jedoch festzulegen, welche Sicherheits-Integritätslevel in bestimmten Anwendungen benötigt werden (dies sollte aufgrund von Erfahrungen mit der jeweiligen Anwendung und mit Blick auf die beabsichtigte Gesamt-Risikominderung erfolgen);
- u) schreibt Anforderungen an alle Teile einer PLT-Sicherheitseinrichtung von den Sensoren bis zu den Aktoren vor;
- v) legt fest, welche Informationen während des Sicherheitslebenszyklus der PLT-Sicherheitseinrichtung benötigt wird;
- w) fordert, dass der Entwurf der PLT-Sicherheitseinrichtungen menschliche Verhaltensweisen berücksichtigt;
- x) stellt keinerlei direkte Anforderungen an den einzelnen Anlagenfahrer oder an Mitarbeiter der Instandhaltung.

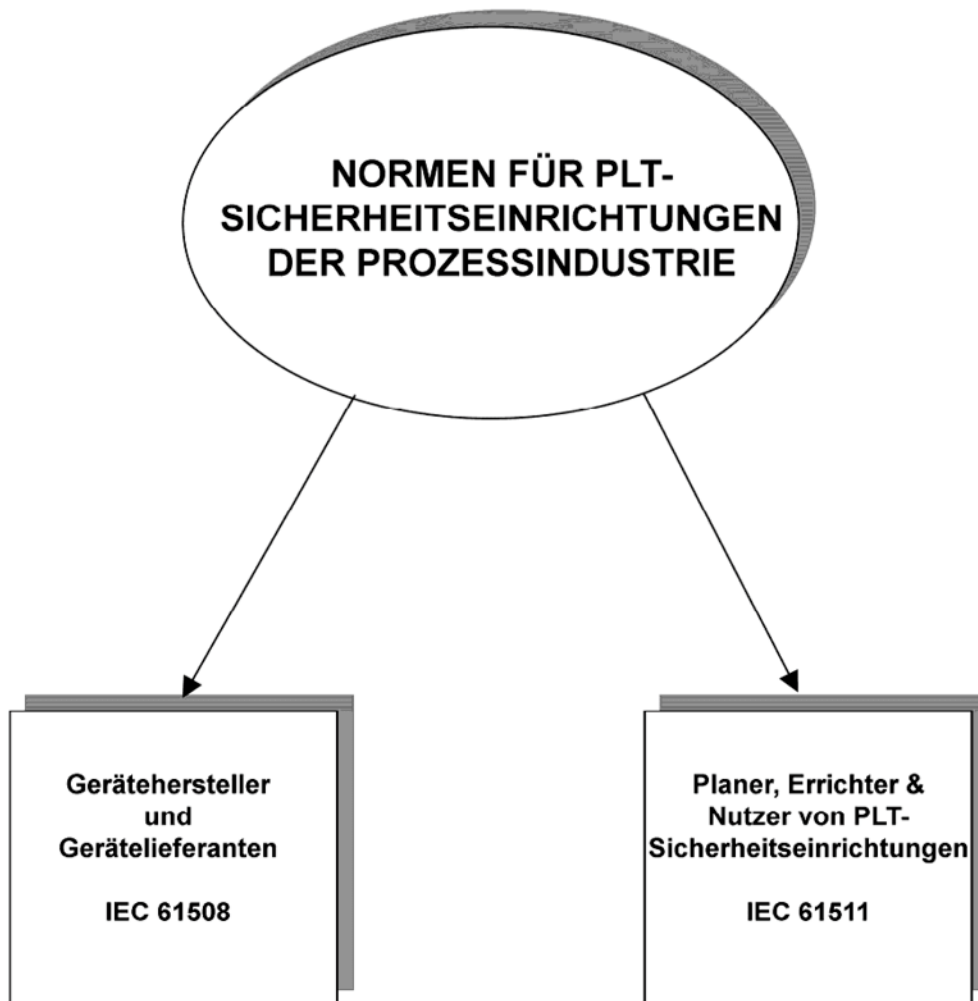


Bild 2 – Beziehung zwischen IEC 61508 und IEC 61511

ANMERKUNG 3 Wo es die IEC 61511 anweist, wird die IEC 61508 auch von Konstrukteuren von PLT-Sicherheitsgeräten, Errichtern und Anwendern verwendet.

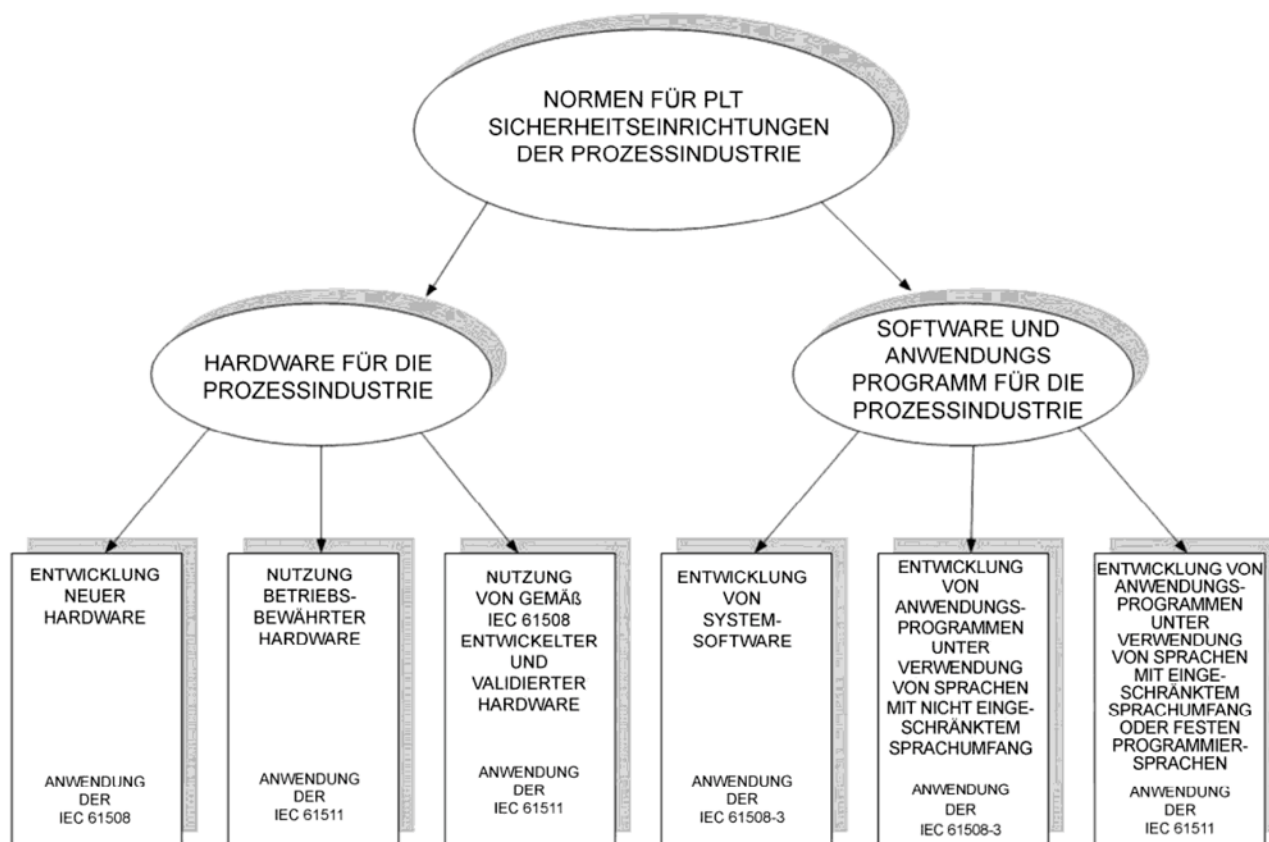
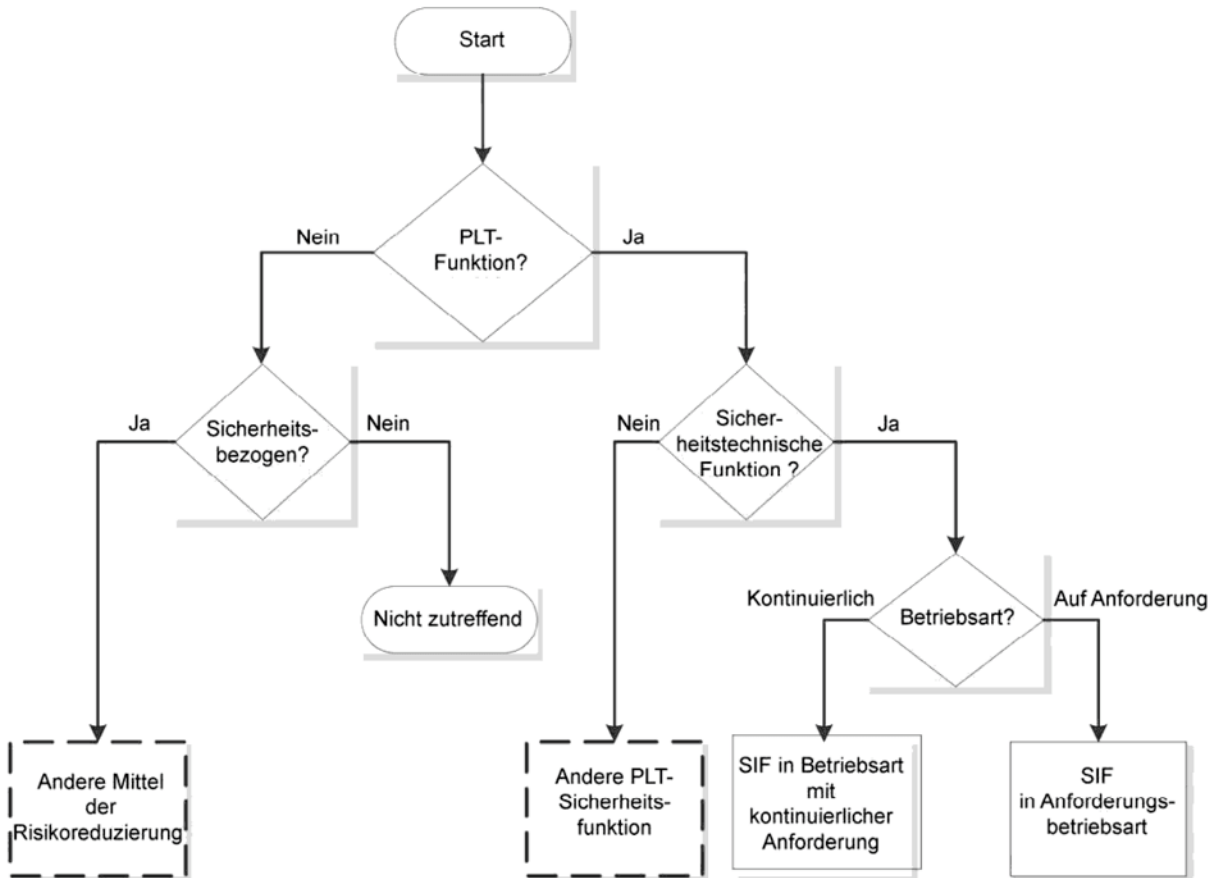


Bild 3 – Detaillierte Beziehung zwischen IEC 61508 und IEC 61511

A1 ANMERKUNG 4 IEC 61511-1:2016, 7.2.2 und IEC 61511-2:2016, A.7.2.2 zeigen, wie Subsysteme integriert werden können, die anderen Normen entsprechen (z. B. Maschinen, Brenner usw.).



 bedeutet: die Norm schreibt durchzuführende Tätigkeiten vor, ohne detaillierte Anforderungen vorzugeben

Bild 4 – Zusammenhang zwischen PLT-Sicherheitsfunktionen und anderen Funktionen

2 Normative Verweisungen

Die folgenden Dokumente, die in diesem Dokument teilweise oder als Ganzes zitiert werden, 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 61508-1:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems, Part 1: General Requirements*

IEC 61508-2:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems, Part 2: Requirements for electrical electronic/programmable electronic safety-related systems*

IEC 61508-3:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems, Part 3: Software requirements*

3 Begriffe und Abkürzungen

3.1 Begriffe

Die Begriffe sind in 3.2 alphabetisch aufgeführt.

3.2 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

In einigen Fällen weichen die Definitionen von denen der gleichen Begriffe in IEC 61508-4:2010 ab. In einigen Fällen liegt das an der in der Prozessindustrie verwendeten Terminologie. In anderen Fällen wurden die Definitionen an andere wichtige Quellen angepasst (z. B. an das internationale elektrotechnische Wörterbuch in IEC 60050 oder an den ISO/IEC Guide 51:2013). Es besteht jedoch, sofern nicht anders vermerkt, zwischen diesen Definitionen und den entsprechenden in der IEC 61508-4:2010 kein Unterschied in der technischen Bedeutung.

3.2.1

Architektur

(en: architecture)

spezifische Anordnung von Bestandteilen aus Hardware oder Software zu einem System

Anmerkung 1 zum Begriff: In der IEC 61511-Reihe kann dies beispielsweise die Zusammenstellung von Teilsystemen einer PLT-Sicherheitseinrichtung, die innere Struktur eines Teilsystems einer PLT-Sicherheitseinrichtung oder die interne Anordnung von Anwendungsprogrammen einer PLT-Sicherheitseinrichtung betreffen.

3.2.2

Schutz vor Sachschäden

(en: asset protection)

eine einem System zugeordnete Funktion zum Zwecke der Verhinderung von Sachschäden

3.2.3

PLT-Betriebseinrichtung

BPCS

(en: basic process control system)

System, das auf Eingangssignale des Prozesses, seiner zugehörigen technischen Einrichtungen, anderer programmierbarer Systeme und/oder von Bedienern anspricht und Ausgangssignale erzeugt, die den Prozess und seine zugehörigen technischen Einrichtungen in der gewünschten Weise steuern. Eine PLT-Betriebseinrichtung führt jedoch keine PLT-Sicherheitsfunktionen aus.

Anmerkung 1 zum Begriff: Eine PLT-Betriebseinrichtung umfasst alle notwendigen Geräte, damit der Prozess in der gewünschten Art und Weise arbeitet.

Anmerkung 2 zum Begriff: Eine PLT-Betriebseinrichtung kann die unterschiedlichsten Funktionen ausführen, beispielsweise Regelungsfunktionen, Überwachungsfunktionen, Alarmierungen oder andere Nicht-Sicherheitsfunktionen.

3.2.4

Überbrückung

(en: bypass)

Tätigkeit oder Einrichtung, um die Ausführung der gesamten oder von Teilen einer PLT-Sicherheitsfunktionalität zu verhindern

Anmerkung 1 zum Begriff: Beispiele für Überbrückungen sind:

- Ein Eingangssignal wird von der Abschaltlogik getrennt, während die Eingangsgrößen und ein Alarm dem Bedienungspersonal weiterhin angezeigt werden;
- das Ausgangssignal der Abschaltlogik zum Aktor wird im Normalzustand gehalten, um eine Aktion des Aktors zu verhindern;
- eine um einen Aktor herumführende Umgehungsrohrleitung ist vorhanden;
- ein ausgewählter Status (z. B. ein oder aus) eines oder mehrerer Eingangswerte wird über ein Engineering-Werkzeug auf einen bestimmten Wert gesetzt (z. B. im Anwendungsprogramm).

Anmerkung 2 zum Begriff: Für den Begriff Überbrückung gibt es eine Reihe weiterer Benennungen wie „Muting“.

3.2.5

Kanal

(en: channel)

Gerät oder Gruppe von Geräten, die eine bestimmte Funktion unabhängig ausführen

Anmerkung 1 zum Begriff: Die Geräte innerhalb eines Kanals können Eingabe-/Ausgabebaugruppen, Logiksysteme, Sensoren und Aktoren beinhalten.

Anmerkung 2 zum Begriff: Eine zweikanalige Konfiguration ist eine Konfiguration mit zwei Kanälen, die die gleiche Funktion unabhängig voneinander ausführen. Die Kanäle können gleich- oder verschiedenartig sein.

Anmerkung 3 zum Begriff: Die Benennung kann verwendet werden, um ein vollständiges System oder ein Teil eines Systems (z. B. Sensoren oder Aktoren) zu beschreiben.

Anmerkung 4 zum Begriff: Ein Kanal wird zur Beschreibung einer Architektureigenschaft der Hardware einer PLT-Sicherheitseinrichtung verwendet, die oft der Erfüllung der Anforderungen an die Fehlertoleranz der Hardware dient.

3.2.6

gemeinsame Ursache

(en: common cause)

3.2.6.1

Ausfälle infolge gemeinsamer Ursache

(en: common cause failures)

gleichzeitige Ausfälle verschiedener Geräte durch ein einzelnes Ereignis, wobei diese Ausfälle nicht aufeinander zurückzuführen sind

Anmerkung 1 zum Begriff: Ausfälle infolge einer gemeinsamen Ursache ereignen sich nicht notwendigerweise alle zum gleichen Zeitpunkt, somit kann Zeit zur Erkennung des Ausfalls gemeinsamer Ursache zur Verfügung stehen, bevor eine PLT-Sicherheitsfunktion tatsächlich ausfällt.

Anmerkung 2 zum Begriff: Ausfälle gemeinsamer Ursache können auch zu Ausfällen gleicher Ausfallart führen.

Anmerkung 3 zum Begriff: Potentielle Ausfälle gemeinsamer Ursache vermindern die Wirkung der Systemredundanz oder der Fehlertoleranz (beispielsweise erhöht sich die Ausfallwahrscheinlichkeit von zwei oder mehr Kanälen in einem mehrkanaligen System).

Anmerkung 4 zum Begriff: Ausfälle gemeinsamer Ursache sind abhängige Ausfälle. Sie können aufgrund äußerer Ereignisse (z. B. Temperatur, Feuchtigkeit, Überspannung, Feuer und Korrosion), systematischer Fehler (z. B. Auslegung, Fehler bei Zusammenbau oder Einbau, Software-Fehler), menschliches Versagen (z. B. falsche Verwendung), usw. entstehen.

Anmerkung 5 zum Begriff: ein Ausfall gemeinsamer Ursache (im Singular) gehört zu einer Reihe zugehöriger Ausfälle (Plural) entsprechend der Definition in 3.2.6.1.

3.2.6.2

Ausfälle mit gemeinsamen Ausfallart

(en: common mode failure)

gleichzeitige Ausfälle verschiedener Geräte, die durch die gleiche Ausfallart gekennzeichnet sind (d. h. durch identische Fehler)

Anmerkung 1 zum Begriff: Ausfälle mit gemeinsamen Ausfallart können das Ergebnis von Ausfällen gemeinsamer Ursache sein.

Anmerkung 2 zum Begriff: Ausfälle mit gemeinsamen Ausfallart können auch Ausfälle gemeinsamer Ursache sein (3.2.6.2).

Anmerkung 3 zum Begriff: Potentielle Ausfälle mit gemeinsamen Ausfallart vermindern den Effekt der Systemredundanz oder der Fehlertoleranz (beispielsweise Ausfall von zwei oder mehr Kanälen in einem mehrkanaligen System verursachen das gleiche falsche Ergebnis).

Anmerkung 4 zum Begriff: Im weiteren Sinne ist ein Ausfall gemeinsamer Ausfallart ein Ausfall, der zu einer Menge gleichzeitiger Ausfälle entsprechend der Definition in 3.2.6.1. gehört.

3.2.7

Ersatzmaßnahme

(en: compensating measure)

zeitlich begrenzte, geplante und dokumentierte Methoden zur Risikobeherrschung während eines Zeitraums der Instandhaltung oder des Anlagenbetriebs, für den bekannt ist, dass die Leistungsfähigkeit der PLT-Sicherheitseinrichtung vermindert ist.

3.2.8

Komponente

(en: component)

Teil eines Systems, Teilsystem einer PLT-Sicherheitseinrichtung oder ein Gerät, das eine bestimmte Funktion ausführt.

Anmerkung 1 zum Begriff: Eine Komponente kann auch Software beinhalten.

3.2.9

Konfigurationsmanagement

(en: configuration management)

Verfahren zur Identifikation der Komponenten und ihrer Zusammenstellung eines sich in der Entwicklung befindenden Systems zum Zwecke der Kontrolle von Veränderungen an diesen Komponenten und der Aufrechterhaltung der Kontinuität des Systems und der Zurückverfolgbarkeit aller Änderungen während des Lebenszyklus.

3.2.9.1

konservativer Ansatz

(en: conservative approach)

Zurückhaltendes Vorgehen bei der Durchführung von Analysen und Berechnungen.

Anmerkung 1 zum Begriff: Im Bereich der Sicherheit kann dieser Ansatz immer dann angewendet werden, wenn Analysen, Annahmen oder Berechnungen durchgeführt werden (im Zusammenhang mit Modellen, Eingangswerten, Berechnungsformeln usw.), um sicher pessimistische Ergebnisse zu erhalten.

3.2.10

Regelsystem

(en: control system)

System, das auf Eingangssignale des Prozesses und/oder des Bedieners reagiert und Ausgangssignale erzeugt, die den Prozess (verfahrenstechnische Anlage) veranlassen, in der gewünschten Weise zu arbeiten

Anmerkung 1 zum Begriff: Das Regelsystem schließt die Sensoren und Aktoren ein und kann entweder eine PLT-Betriebseinrichtung (BPCS) oder eine PLT-Sicherheitseinrichtung (SIS) oder eine Kombination von beiden sein.

3.2.11

gefährlicher Ausfall

(en: dangerous failure)

Ausfall, der eine bestimmte Sicherheitsmaßnahme behindert oder unterbindet.

Anmerkung 1 zum Begriff: Ein Ausfall ist nur im Hinblick auf eine gegebene PLT-Sicherheitsfunktion „gefährlich“.

Anmerkung 2 zum Begriff: Wenn Fehlertoleranz vorhanden ist, kann ein gefährlicher Ausfall entweder

- zu einer eingeschränkten PLT-Sicherheitsfunktion führen, indem die Sicherheitsmaßnahme zwar verfügbar ist, jedoch mit einer höheren PFD oder PFH oder
- zu einer nicht einsatzfähigen PLT-Sicherheitsfunktion führen, indem die Sicherheitsmaßnahme vollständig fehlt oder das gefährliche Ereignis herbeigeführt worden ist.

Anmerkung 3 zum Begriff: Ist keine Fehlertoleranz vorhanden, so setzen alle gefährlichen Ausfälle die PLT-Sicherheitsfunktion außer Funktion.

3.2.12

abhängiger Ausfall

(en: dependent failure)

Ausfall, dessen Wahrscheinlichkeit nicht als das einfache Produkt der Wahrscheinlichkeiten der individuellen Ereignisse, die ihn verursacht haben, ausgedrückt werden kann

Anmerkung 1 zum Begriff: Zwei Ereignisse A und B sind dann abhängig, wenn die Wahrscheinlichkeit des Auftretens von A und B, $P(A \text{ und } B)$, größer ist als $P(A) \times P(B)$.

Anmerkung 2 zum Begriff: Siehe 9.4.2 und IEC 61511-3:2016, Anhang J zur Berücksichtigung abhängiger Ausfälle zwischen Schutzebenen.

Anmerkung 3 zum Begriff: Zu den abhängigen Ausfällen gehören auch die Ausfälle infolge gemeinsamer Ursache.

3.2.13

erkannt, offenkundig

(en: detected, revealed, overt)

in Bezug auf Hard- und Software Ausfälle oder Fehler, die nicht versteckt sind, weil sie sich selbst melden oder im Normalbetrieb entdeckt werden oder mit Hilfe spezieller Detektionsmechanismen entdeckt werden

Anmerkung 1 zum Begriff: Die genannten Begriffe werden unterschiedlich verwendet:

- Offenkundig wird für Ausfälle oder Fehlzustände verwendet, die sich bei ihrem Auftreten selbst zeigen (z. B. durch eine Zustandsänderung). Die Behebung solcher Ausfälle kann beginnen, sobald sie aufgetreten sind.
- Erkannt wird für Ausfälle oder Fehler verwendet, die sich bei ihrem Auftreten nicht selbst zeigen und versteckt bleiben, bis sie erkannt werden, beispielsweise durch Diagnosetest, Funktionsprüfungen, Bedienereingriff wie Sichtprüfung oder händische Prüfung. Die Behebung solcher Ausfälle kann erst beginnen, wenn sie aufgedeckt worden sind. Siehe Anmerkung 2 zur Verwendung dieses Begriffs in IEC 61511.
- aufgedeckt wird für Fehlzustände und Ausfälle verwendet, die offenkundig sind oder erkannt worden sind.

Anmerkung 2 zum Begriff: Falls aus dem Zusammenhang nichts anderes hervorgeht, handelt es sich bei „gefährlichen erkannten Ausfällen oder Fehlern“ in IEC 61511 um solche, die durch Diagnosetests erkannt worden sind.

Anmerkung 3 zum Begriff: Verläuft die Erkennung sehr schnell (z. B. durch Diagnosetests), können die erkannten Fehler oder Ausfälle als offenkundig aufgefasst werden. Wenn die Erkennung nicht sehr schnell verläuft (z. B. bei Funktionsprüfungen), kann der erkannte Ausfall oder Fehler bezüglich einer SIL-Zuweisung nicht als offenkundig aufgefasst werden.

Anmerkung 4 zum Begriff: Ein aufgedeckter gefährlicher Ausfall kann nur dann als ungefährlich betrachtet werden, wenn wirksame Maßnahmen automatischer oder händischer Art in einer genügend kurzer Zeit getroffen werden, so dass die Prozesssicherheit erhalten bleibt.

3.2.14

Gerät

(en: device)

Hardware, mit oder ohne Software, die eine bestimmte Funktion ausführen kann

Anmerkung 1 zum Begriff: Beispiele sind Sensoren, Logiksysteme, Aktoren, Bedienerschnittstellen und Feldverdrahtung.

3.2.14.1

Feldgerät

(en: field device)

Gerät der PLT-Sicherheitseinrichtung (SIS) oder PLT-Betriebseinrichtung (BPCS) mit direktem Prozessanschluss oder in unmittelbarer Nähe zum Prozess

Anmerkung 1 zum Begriff: Beispiele sind Sensoren, Aktoren und handbetätigte Schalter.

3.2.15

Diagnose

(en: diagnostics)

Häufiger (im Vergleich zur Prozessfehlertoleranzzeit) automatischer Test zur Aufdeckung von Fehlern.

3.2.15.1

Diagnosedeckungsgrad

DC

(en: diagnostic coverage)

Anteil der durch Diagnosetests erkannten gefährlichen Ausfälle. Der Diagnosedeckungsgrad beinhaltet keine bei Funktionsprüfungen festgestellten Fehler

Anmerkung 1 zum Begriff: Der Diagnosedeckungsgrad wird üblicherweise für Geräte in PLT-Sicherheitseinrichtungen oder Teilsysteme von PLT-Sicherheitseinrichtungen angewendet, beispielsweise wird er für Sensoren, Stellglieder oder Logiksysteme bestimmt.

Anmerkung 2 zum Begriff: Für Sicherheitsanwendungen wird der Diagnosedeckungsgrad typischerweise auf gefährliche Ausfälle von Geräten in PLT-Sicherheitseinrichtungen oder Teilsystemen von PLT-Sicherheitseinrichtungen angewendet. Beispielsweise kann der Diagnosedeckungsgrad für gefährliche Ausfälle bei einem Gerät $DC = \lambda_{DD} / \lambda_{DT}$ betragen, wobei λ_{DD} die Rate erkannter gefährlicher Ausfälle und λ_{DT} die Gesamtfallrate für gefährliche Ausfälle ist. Für ein Teilsystem einer PLT-Sicherheitseinrichtung mit interner Redundanz ist DC zeitabhängig: $DC(t) = \lambda_{DD}(t) / \lambda_{DT}(t)$.

Anmerkung 3 zum Begriff: Wenn der Diagnosedeckungsgrad (DC) und die Gesamtausfallrate (λ_{DT}) gegeben sind, können die Rate erkannter (λ_{dd}) und die Rate unerkannter Ausfälle (λ_{du}) folgendermaßen berechnet werden:

$$\lambda_{DD} = DC \times \lambda_{DT} \text{ und } \lambda_{DU} = (1-DC) \times \lambda_{DT}.$$

3.2.16

Diversität

(en: diversity)

unterschiedliche Mittel zur Ausführung einer geforderten Funktion

Anmerkung 1 zum Begriff: Diversität kann durch unterschiedliche physikalische Mittel, unterschiedliche Programmiermethoden oder unterschiedliche Entwurfsansätze erreicht werden.

3.2.17

Abweichung

(en: error)

Nichtübereinstimmung zwischen einem berechneten, beobachteten oder gemessenen Wert oder einer Beschaffenheit und dem wahren, festgelegten oder theoretisch richtigen Wert oder der wahren Beschaffenheit

[QUELLE: IEC60050-192:2015, 192-03-02^{N1}]

3.2.18

Ausfall

(en: failure)

Verlust der Fähigkeit, wie gefordert zu funktionieren

Anmerkung 1 zum Begriff: Der Ausfall eines Gerätes ist ein Ereignis das zu einem Fehlzustand desselben führt.

Anmerkung 2 zum Begriff: Wenn der Verlust dieser Fähigkeit durch einen latent vorhandenen Fehler verursacht wird, geschieht der Ausfall dann, wenn eine bestimmte Reihe von Umständen eintritt.

^{N1} Nationale Fußnote: In der deutschen Ausgabe des IEV (DAIEV) stehen hier die Benennungen „Fehlaussage“ und „Irrtum“. Weiterhin sind die Anmerkungen 1 und 2 aus dem DAIEV nicht übernommen.

Anmerkung 3 zum Begriff: Die Durchführung geforderter Funktionen schließt notwendigerweise bestimmte Verhaltensweisen aus, und manche Funktionen können derart spezifiziert werden, dass sie ein bestimmtes Verhalten vermeiden. Das Eintreten solch eines Verhaltens ist dann ein Ausfall.

A1 | Anmerkung 4 zum Begriff: Ausfälle sind entweder zufällig oder systematisch (siehe 3.2.59 und 3.2.81)

[QUELLE: IEC 60050-192:2015, 192-03-01, die Anmerkungen wurden geändert]

3.2.18.1

Ausfallart

(en: failure mode)

Art und Weise, wie sich ein Ausfall ereignet

Anmerkung 1 zum Begriff: Eine Ausfallart kann durch die verlorene Funktion oder durch den eingetretenen Zustandsübergang definiert werden.

[QUELLE: IEC 60050-192:2015, 192-03-17]

3.2.19

Fehler

(en: fault)

Unfähigkeit aufgrund eines internen Zustands, wie gefordert zu funktionieren

Anmerkung 1 zum Begriff: Ein Fehler einer Betrachtungseinheit resultiert aus einem Ausfall der Betrachtungseinheit selbst oder aus einem Mangel zu einem früheren Zeitpunkt im Lebenszyklus, z. B. während der Spezifikation, des Entwurfs, der Fertigung oder der Instandhaltung.

Anmerkung 2 zum Begriff: Ein Gerätefehler hat einen Ausfall zur Folge, wenn eine bestimmte Reihe von Umständen eintrifft.

[QUELLE: IEC 60050-192:2015, 192-04-01], modifiziert – einige Anmerkungen wurden verändert, andere wurden entfernt^{N2}.

3.2.20

Fehlervermeidung

(en: fault avoidance)

Verwendung von Techniken und Verfahren mit dem Ziel, die Entstehung von Fehlern während jeder Phase des Sicherheitslebenszyklus der PLT-Sicherheitseinrichtung zu vermeiden

3.2.20.1

Fehlerausschluss

(en: fault exclusion)

Ausschluss von Fehlern für die weitere Betrachtung wegen unwahrscheinlicher Ausfallarten.

Anmerkung 1 zum Begriff: Weitere Informationen über Fehlerausschlüsse sind in ISO 13849-1 und ISO 13849-2 zu finden. Gemäß dieser Normen kann ein Fehlerausschluss beruhen auf

- der technischen Unwahrscheinlichkeit für das Auftreten bestimmter Fehler,
- allgemein anerkannten Erfahrungen unabhängig von der betrachteten Anwendung,
- technischen Anforderungen für eine bestimmte Anwendung und die spezifische Gefährdung.

^{N2} Nationale Fußnote: In der deutschen Ausgabe des IECV (DAIEV) steht hier die Benennung „Fehlzustand“.

Anmerkung 2 zum Begriff: Erkannte Ausfallarten in den Geräten, die die Sicherheitsfunktion ausführen, können ausgeschlossen werden, weil ihre zugeordnete gefährliche Ausfallrate(n) sehr klein verglichen mit der Ziel-Ausfallrate der betrachteten Sicherheitsfunktion ist. Das bedeutet, die Summe der gefährlichen Ausfallraten aller hintereinandergeschalteten Geräte, auf die der Fehlerausschluss angewendet wird, kann grundsätzlich nicht größer als 1 % der Ziel-Ausfallrate sein.

3.2.21

Fehlertoleranz

(en: fault tolerance)

Fähigkeit einer Funktionseinheit, eine geforderte Funktion bei Vorhandensein von Fehlern oder Abweichungen weiter auszuführen

3.2.22

Aktor

(en: final element)

Teil einer PLT-Betriebs- oder PLT-Sicherheitseinrichtung, der die Eingriffe in den Prozess ausführt, um einen sicheren Zustand zu erreichen oder zu erhalten

Anmerkung 1 zum Begriff: Beispiele sind Ventile, Schalter und Motoren einschließlich ihrer Hilfsaggregate (wie ein Magnetventil und der Antrieb, welche zum Betreiben eines Ventils verwendet werden).

3.2.23

funktionale Sicherheit

(en: functional safety)

Teil der Gesamtsicherheit, der sich auf den Prozess und die PLT-Betriebseinrichtungen bezieht und der von der korrekten Funktion der PLT-Sicherheitseinrichtung(en) und anderer Schutzebenen abhängt.

3.2.24

Beurteilung der funktionalen Sicherheit

(en: functional safety assessment, FSA)

auf Nachweise gestützte Untersuchung, die die funktionale Sicherheit beurteilt, die durch eine oder mehrere PLT-Sicherheitseinrichtungen und/oder andere Schutzebenen erreicht wird

3.2.25

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 Vorgehensweisen übereinstimmen, wirksam durchgeführt werden und angemessen sind, die spezifizierten Ziele zu erreichen

Anmerkung 1 zum Begriff: Ein Audit der funktionalen Sicherheit kann im Rahmen der Beurteilung der funktionalen Sicherheit ausgeführt werden.

3.2.26

Sicherheitsintegrität der Hardware

(en: hardware safety integrity)

Teil der Sicherheitsintegrität der PLT-Sicherheitseinrichtung, der sich auf zufällige Hardware-Ausfälle mit gefährlicher Ausfallart bezieht

A1 | Anmerkung 1 zum Begriff: Die in diesem Zusammenhang relevanten Maßstäbe für einen Ausfall sind die mittlere Häufigkeit eines gefährlichen Ausfalls und die mittlere Wahrscheinlichkeit eines Versagens bei Anforderung.

Anmerkung 2 zum Begriff: Siehe [3.2.82](#).

Anmerkung 3 zum Begriff: Diese Definition weicht wegen in der Prozessindustrie vorhandener Unterschiede in der Terminologie von der Definition in [IEC 61508-4:2010](#) ab.

3.2.27

Schaden

(en: harm)

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

[QUELLE: ISO/IEC Guide 51:2014, 3.1]

3.2.27.1

Schadensereignis

(en: harmful event)

Gefährliches Ereignis, das einen Schaden verursacht hat.

Anmerkung 1 zum Begriff: Ob ein gefährlicher Vorfall einen Schaden hervorruft, hängt davon ab, ob Menschen, Eigentum oder die Umwelt der gefährlichen Situation ausgesetzt sind und im Falle von Menschen, ob solchermaßen ausgesetzte Menschen den Auswirkungen des Ereignisses entkommen können, wenn es sich ereignet hat. Ein gefährlicher Vorfall, der einen Schaden verursacht hat, wird als Schadensereignis bezeichnet.

3.2.28

Gefährdung

(en: hazard)

potentielle Schadensquelle

Anmerkung 1 zum Begriff: Der Begriff schließt die Gefährdungen von Personen ein, die innerhalb einer kurzen Zeitspanne entstehen (z. B. durch Feuer und Explosion) und auch die, die eine langfristige Wirkung auf die Gesundheit einer Person haben (z. B. durch Freisetzung einer giftigen Substanz oder Radioaktivität).

[QUELLE: ISO/IEC Guide 51:2014, 3.2, modifiziert – Anmerkung 1 zum Begriff wurde eingefügt]

3.2.28.1

gefährlicher Vorfall

(en: hazardous event)

Ereignis, das Schaden verursachen kann

Anmerkung 1 zum Begriff: Ob ein gefährlicher Vorfall einen Schaden hervorruft, hängt davon ab, ob Menschen, Eigentum oder die Umwelt der gefährlichen Situation ausgesetzt sind und im Falle von Menschen, ob solchermaßen ausgesetzte Menschen den Auswirkungen des Ereignisses entkommen können, wenn es sich ereignet hat.

[QUELLE: ISO/IEC Guide 51:2014, 3.3, modifiziert – siehe Anmerkung 1]

3.2.28.2

gefährliche Situation

(en: hazardous situation)

Umstand, in dem Menschen, Güter oder die Umwelt einer oder mehreren Gefährdungen ausgesetzt sind

[QUELLE: ISO/IEC Guide 51:2014, 3.4]

3.2.29

menschliches Versagen

(en: human error)

beabsichtigte oder unbeabsichtigte Handlung oder Unterlassung eines Menschen, die zu einem ungünstigen Ergebnis führt

Anmerkung 1 zum Begriff: Ein Irrtum oder Lapsus ist ein Beispiel hierfür.

Anmerkung 2 zum Begriff: Diese Definition schließt böswillige Aktionen aus.

3.2.30

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 in anderen Systemen haben kann

3.2.31

unabhängige Organisation

(en: independent organization)

Organisation, die aufgrund ihres Managements und anderer Ressourcen eindeutig getrennt ist und nicht in Verbindung mit den Organisationen steht, die für die Tätigkeiten verantwortlich sind, die während einer speziellen Phase des Sicherheitslebenszyklus, der Gegenstand der Beurteilung der funktionalen Sicherheit oder Validierung ist, stattfinden

3.2.32

unabhängige Person

(en: independent person)

Person, die getrennt und nicht eingebunden ist in die Tätigkeiten, die während einer speziellen Phase des Sicherheitslebenszyklus stattfinden, die Gegenstand der Beurteilung der funktionalen Sicherheit oder Validierung ist, und die keine direkte Verantwortung für diese Tätigkeiten trägt

3.2.33

Eingangsfunktion

(en: input function)

Funktion, die den Prozess und seine zugehörigen technischen Einrichtungen überwacht und diese Information einer Logikfunktion zur Verfügung stellt

Anmerkung 1 zum Begriff: Eine Eingangsfunktion kann auch eine manuelle Funktion sein.

3.2.34

Instrument

(en: instrument)

Gerät, das zur Ausführung einer Aktion verwendet wird (typischerweise in prozessleittechnischen Systemen)

3.2.34.1

PLT-Einrichtung

(en: instrumented system)

PLT-Einrichtung, aufgebaut aus Sensoren (beispielsweise Druck-, Durchfluss-, Temperaturmessumformer), Logiksystemen (beispielsweise SPSen, verteilte Leitsysteme, diskrete Regler) und Aktoren (beispielsweise Stellventile, Motorstromkreise).

Anmerkung 1 zum Begriff: PLT-Einrichtungen führen PLT-Funktionen aus, darunter Regel-, Überwachungs-, Alarm- und Schutzfunktionen. PLT-Einrichtungen können PLT-Sicherheitseinrichtungen (siehe 3.2.67) oder PLT-Betriebseinrichtungen (siehe 3.2.3) sein.

3.2.35

Logikfunktion

(en: logic function)

Funktion, die die Umwandlung der Eingangsinformation (bereitgestellt durch eine oder mehrere Eingangsfunktionen) zur Ausgangsinformation (verwendet durch eine oder mehrere Ausgangsfunktionen) durchführt

Anmerkung 1 zum Begriff: Logikfunktionen transformieren eine oder mehrere Eingangsfunktionen in eine oder mehrere Ausgangsfunktionen.

Anmerkung 2 zum Begriff: Weitere Hinweise finden sich in IEC 61131-3:2012 und IEC 60617-12:1997.

3.2.36

Logiksystem

(en: logic solver)

Teil einer PLT-Betriebseinrichtung oder einer PLT-Sicherheitseinrichtung, der eine oder mehrere Logikfunktionen ausführt

Anmerkung 1 zum Begriff: In der IEC 61511 werden folgende Begriffe für Logiksysteme verwendet:

- elektrische Logiksysteme für Logiksysteme in elektromechanischer Technologie;
- elektronische Logiksysteme für Logiksysteme in elektronischer Technologie;

- programmierbare elektronische Systeme (PE-Logiksysteme) für Logiksysteme mit programmierbarer Elektronik.

Anmerkung 2 zum Begriff: Beispiele sind: elektrische Systeme, elektronische Systeme, programmierbare elektronische Systeme, pneumatische Systeme und hydraulische Systeme. Sensoren und Aktoren sind nicht Bestandteil des Logiksystems.

3.2.36.1

sicherheitskonfiguriertes PE-Logiksystem

(en: safety configured PE-logic solver)

Standard-Industrie-PE-Logiksystem, das speziell für den Einsatz in Sicherheitsanwendungen konfiguriert wurde.

Anmerkung 1 zum Begriff: Weitere Hinweise siehe 11.5.

3.2.37

Instandhaltungs- oder Engineering-Schnittstelle

(en: maintenance/engineering interface)

zur Instandhaltung oder Modifikation einer PLT-Sicherheitseinrichtung vorgesehene Hardware und Software.

Anmerkung 1 zum Begriff: Die Instandhaltungs- und Engineering-Schnittstelle kann auch Anweisungen oder Diagnosemittel einschließen, welche in Software, Programmiergeräten mit zugehörigen Kommunikationsprotokollen, Diagnosewerkzeugen, Anzeigen, Überbrückungseinrichtungen, Prüf- und Kalibriergeräten zu finden sind.

3.2.37.1

Mittlere Reparaturzeit

MRT

(en: mean repair time)

erwartete Gesamt-Reparaturdauer

Anmerkung 1 zum Begriff: Die MRT umfasst die Zeiten (b), (c) und (d) der MTTR (siehe 3.2.37.2).

3.2.37.2

Mittlere Zeit bis zur Wiederherstellung

MTTR

(en: Mean Time To Restoration)

erwartete Zeit bis zur Wiederherstellung

Anmerkung 1 zum Begriff: Die MTTR umfasst

- die Zeit bis zur Fehlerentdeckung (a),
- die Zeit bis zum Beginn der Reparatur (b),
- die tatsächliche Reparaturzeit (c),
- die Zeit bis zur Wiederinbetriebnahme der Komponente (d).

Startpunkt für (b) ist das Ende von (a), Startpunkt für (c) ist das Ende von (b), Startpunkt für (d) ist das Ende von (c),

3.2.37.3

Maximal zulässige Reparaturzeit

MPRT

(en: maximum permitted repair time)

Maximal zulässige Zeit für die Reparatur eines Fehlers nach seiner Aufdeckung.

Anmerkung 1 zum Begriff: Die MRT kann als MPRT verwendet werden, aber die MPRT kann ohne Berücksichtigung der MRT festgelegt werden:

- Eine MPRT kleiner als MRT kann gewählt werden, um die Wahrscheinlichkeit eines gefährlichen Vorfalls zu vermindern.
- Eine MPRT größer als die MRT kann gewählt werden, wenn die Wahrscheinlichkeit eines gefährlichen Vorfalls verringert werden kann.

Anmerkung 2 zum Begriff: Wenn eine MPRT festgelegt wurde, kann diese anstelle der MRT für die Berechnung zufälliger Hardware-Ausfälle verwendet werden.

3.2.38

Schadensbegrenzungsmaßnahme

(en: mitigation)

Maßnahme zur Verringerung der Auswirkung(en) eines gefährlichen Ereignisses

Anmerkung 1 zum Begriff: Beispiele für Schadensbegrenzungsmaßnahmen sind Notentspannungssysteme oder Schließen von Lüftungskappen bei Entdeckung oder Bestätigung eines Brand- oder Leckagefalls oder Auslösung einer Sprühwasserlöschanlage im Brandfall.

3.2.39

Betriebsart (einer PLT-Sicherheitsfunktion)

(en: mode of operation (of a SIF))

Art, in der eine PLT-Sicherheitsfunktion betrieben wird. Mögliche Betriebsarten sind Betriebsart mit niedriger Anforderungsrate, mit hoher Anforderungsrate und mit kontinuierlicher Anforderung:

- a) **Betriebsart mit niedriger Anforderungsrate:** Betriebsart, in der die PLT-Sicherheitsfunktion nur auf Anforderung ausgeführt wird, um den Prozess in einem sicheren Zustand zu führen, und die Häufigkeit von Anforderungen nicht mehr als einmal pro Jahr beträgt
- b) **Betriebsart mit hoher Anforderungsrate:** Betriebsart, in der die PLT-Sicherheitsfunktion nur auf Anforderung ausgeführt wird, um den Prozess in einem sicheren Zustand zu führen, und die Häufigkeit von Anforderungen mehr als einmal pro Jahr beträgt
- c) **Betriebsart mit kontinuierlicher Anforderung:** Betriebsart, in der die PLT-Sicherheitsfunktion als Teil des normalen Betriebes einen sicheren Zustand des Prozesses aufrecht erhält

3.2.39.1

PLT-Sicherheitsfunktion in der Anforderungsbetriebsart

(en: demand mode safety instrumented function)

PLT-Sicherheitsfunktion, arbeitet entweder in der Betriebsart mit niedriger (3.2.39, a)) oder mit hoher Anforderungsrate (3.2.39, b)).

Anmerkung 1 zum Begriff: Im Falle eines gefährlichen Ausfalls der PLT-Sicherheitsfunktion kann ein gefährlicher Vorfall nur dann auftreten, wenn

- der Ausfall unerkannt ist und eine Anforderung vor dem nächsten Funktionstest erfolgt
- der Ausfall durch Diagnosetests erkannt wurde, jedoch der zugeordnete Prozess und seine zugehörigen technischen Einrichtungen noch nicht in einen sicheren Zustand gebracht wurden, bevor eine Anforderung erfolgt.

Anmerkung 2 zum Begriff: In Betriebsart mit hoher Anforderungsrate ist die Verwendung der Kriterien für die Betriebsart mit kontinuierlicher Anforderung im Normalfall geeigneter.

Anmerkung 3 zum Begriff: Die Sicherheits-Integritätslevel für PLT-Sicherheitsfunktionen in der Anforderungsbetriebsart sind in [Tabelle 4](#) und [Tabelle 5](#) vorgegeben.

3.2.39.2

PLT-Sicherheitsfunktion in der Betriebsart mit kontinuierlicher Anforderung

(en: continuous mode safety instrumented function)

PLT-Sicherheitsfunktion, arbeitet in der Betriebsart mit kontinuierlicher Anforderung

Anmerkung 1 zum Begriff: bei einem gefährlichen Ausfall der PLT-Sicherheitsfunktion tritt ein gefährlicher Vorfall ohne einen weiteren Ausfall ein, wenn innerhalb der Prozessfehlertoleranzzeit keine Maßnahme zu seiner Verhinderung ergriffen wird

Anmerkung 2 zum Begriff: Die Betriebsart mit kontinuierlicher Anforderung deckt diejenigen PLT-Sicherheitsfunktionen ab, die Regelungen zur Aufrechterhaltung der funktionalen Sicherheit beinhalten.

Anmerkung 3 zum Begriff: Die Sicherheits-Integritätslevel für PLT-Sicherheitsfunktionen in kontinuierlicher Betriebsart sind in [Tabelle 5](#) vorgegeben.

3.2.40

Modul

(en: module)

in sich abgeschlossener Teil eines Anwendungsprogramms einer PLT-Sicherheitseinrichtung (innerhalb eines einzelnen Programms oder einer Reihe von Programmen), der eine bestimmte Funktion ausführt.(z. B. Start/Stop/Test-Sequenz für einen Aktor, anwendungsspezifischer Ablauf innerhalb einer PLT-Schutzfunktion)

Anmerkung 1 zum Begriff: Eine Funktion oder ein Funktionsbaustein in der IEC 61131-3:2012 ist ein Software-Modul.

Anmerkung 2 zum Begriff: Die meisten Module werden innerhalb eines Anwendungsprogramms mehrfach verwendet.

3.2.41

MooN-System

(en: MooN, M out of N)

PLT-Sicherheitseinrichtung oder Teil davon, das aus „N“ unabhängigen Kanälen besteht, die derart miteinander verbunden sind, dass jeweils „M“ Kanäle genügen, um die PLT-Sicherheitsfunktion auszuführen

3.2.42

notwendige Risikominderung

(en: necessary risk reduction)

Durch die PLT-Sicherheitseinrichtung(en) und/oder andere Schutzebenen zu erreichende Risikominderung, um sicherzustellen, dass das vertretbare Risiko (Grenzrisiko) nicht überschritten wird

3.2.43

nicht programmierbares (NP) System

(en: non-programmable (NP) system)

ein nicht auf Computertechnologie basierendes System (d. h. ein nicht auf programmierbarer Elektronik [PE] oder Software basierendes System)

Anmerkung 1 zum Begriff: Beispiele sind festverdrahtete elektrische oder elektronische Systeme, mechanische, hydraulische oder pneumatische Systeme.

3.2.44

Betriebsbedingungen

(en: operating environment)

Einbaubedingungen eines Geräts, die seine Funktion und die Sicherheitsintegrität beeinflussen können, beispielsweise:

- Umgebungsbedingungen, beispielsweise winterliche Erfordernisse, Ex-Zone;
- Prozess-Betriebsbedingungen, beispielsweise Extremwerte für Temperatur, Druck, Vibration;
- Prozess-Zusammensetzung, beispielsweise Feststoffe, Salze oder korrosive Stoffe;
- Prozessanschlüsse;
- Einbindung in die für die Anlage geltenden Management-Systeme für Instandhaltung und Betrieb;
- Kommunikationsdurchsatz, z. B. elektromagnetische Beeinflussungen;
- Qualität der Hilfsenergieversorgung, beispielsweise elektrische Energie, Luft, Hydraulik

Anmerkung 1 zum Begriff: Einige Prozess-Anwendungen können besondere Betriebsbedingungen erfordern, um ein größeres Unfallereignis zu überstehen. Beispielsweise benötigen manche Geräte spezielle Gehäuse, Spüleinrichtungen oder Brandschutz.

3.2.45

Betriebsart

Prozess-Betriebsart

(en: process operating, process operating mode)

jegliche geplante Prozess-Betriebsart, wie Wiederanfahren nach einer Not-Abschaltung, normales Anfahren, Normalbetrieb und Abfahren, zeitlich begrenzter Betrieb und Notbetrieb und Not-Abschaltung