

	DIN EN 61784-3 (VDE 0803-500)	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 35.160, 35.240.50 Ersatz für DIN EN 61784-3 (VDE 0803-500):2011-02 Siehe Anwendungsbeginn 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 Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions (IEC 61784-3:2016); German version EN 61784-3:2016 Réseaux de communication industriels – Profils – Partie 3: Bus de terrain de sécurité fonctionnelle – Règles générales et définitions de profils (IEC 61784-3:2016); Version allemande EN 61784-3:2016 Gesamtumfang 87 Seiten DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE		

Anwendungsbeginn

Anwendungsbeginn für die von CENELEC am 2016-06-17 angenommene Europäische Norm als DIN-Norm ist 2017-09-01.

Für **DIN EN 61784-3 (VDE 0803-500):2011-02** besteht eine Übergangsfrist bis 2019-06-17.

Nationales Vorwort

Vorausgegangener Norm-Entwurf: E DIN EN 61784-3 (VDE 0803-500):2014-04.

Für dieses Dokument ist das nationale Arbeitsgremium UK 914.1 „Profile für funktional sichere Kommunikationssysteme“ der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE (www.dke.de) zuständig.

Die enthaltene IEC-Publikation wurde vom SC 65C „Industrial networks“ erarbeitet.

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

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

Das Original-Dokument enthält Bilder in Farbe, die in der Papierversion in einer Graustufen-Darstellung wiedergegeben werden. Elektronische Versionen dieses Dokuments enthalten die Bilder in der originalen Farbdarstellung.

Änderungen

Gegenüber **DIN EN 61784-3 (VDE 0803-500):2011-02** wurden folgende Änderungen vorgenommen:

- a) Klärung und zusätzliche Erläuterung der Anforderungen, Verweisungen auf den neusten Stand gebracht;
- b) Streichung der technischen Übersichten der Profile (**Abschnitte 6 bis 13**) und dazugehörigen Unterabschnitte für Begriffe, Festlegungen, Symbole und Abkürzungen;
- c) Profile für die Kommunikationsprofilfamilien 8, 17 und 18 hinzugefügt (**Abschnitte 10, 14, 15**);
- d) Klärung der Modelle in **Anhang A**;
- e) **Anhang B** von informativ zu normativ geändert;
- f) Aufnahme eines neuen informativen **Anhangs E**, welcher Modelle für explizite und implizite FSCP-Mechanismen beschreibt;
- g) Aufnahme eines neuen informativen **Anhangs F**, welcher ein erweitertes Modell für die Abschätzung der Gesamtrestfehlerrate einführt;
- h) Aktualisierungen in CPF 1, CPF 2, CPF 3, CPF 8, CPF 13 (Details sind in den Teilen enthalten);
- i) Aufnahme eines neuen Teils für CPF 17.

Frühere Ausgaben

DIN EN 61784-3 (VDE 0803-500): 2008-11, 2011-02

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 (1 von 3)

Europäisches Dokument	Internationales Dokument	Deutsches Dokument	Klassifikation im VDE-Vorschriftenwerk
	IEC 60050 (alle Teile)	a	
	IEC 60050-191:1990	a	
EN 60204-1	IEC 60204-1	DIN EN 60204-1 (VDE 0113-1)	VDE 0113-1
EN 61000-1-2	IEC 61000-1-2	DIN EN 61000-1-2 (VDE 0839-1-2)	VDE 0839-1-2
EN 61000-6-7	IEC 61000-6-7	DIN EN 61000-6-7 (VDE 0839-6-7)	VDE 0839-6-7
EN 61010-2-201: 2013 + AC:2013	IEC 61010-2-201:2013	DIN EN 61010-2-201 (VDE 0411-2-201):2014-01	VDE 0411-2-201
EN 61131-2:2007	IEC 61131-2:2007	DIN EN 61131-2 (VDE 0411-500):2008-04 DIN EN 61131-2 Berichtigung 1 (VDE 0411-500 Berichtigung 1):2009-01	VDE 0411-500 VDE 0411-500 Berichtigung 1
EN 61131-6	IEC 61131-6	DIN EN 61131-6 (VDE 0411-506)	VDE 0411-506
EN 61158 (alle Teile)	IEC 61158 (alle Teile)	DIN EN 61158 (alle Teile)	–
EN 61326-3-1	IEC 61326-3-1	DIN EN 61326-3-1 (VDE 0843-20-3-1)	VDE 0843-20-3-1
EN 61326-2-3	IEC 61326-3-2	DIN EN 61326-2-3 (VDE 0843-20-2-3)	VDE 0843-20-2-3
EN 61496 (alle Teile)	IEC 61496 (alle Teile)	DIN EN 61496 (VDE 0113-2xx)	VDE 0113-2xx
EN 61496-1	IEC 61496-1	DIN EN 61496 (VDE 0113-201)	VDE 0113-201
EN 61508 (alle Teile)	IEC 61508 (alle Teile)	DIN EN 61508 (VDE 0803) (alle Teile)	VDE 0803

Tabelle NA.1 (2 von 3)

Europäisches Dokument	Internationales Dokument	Deutsches Dokument	Klassifikation im VDE-Vorschriftenwerk
EN 61508-1	IEC 61508-1:2010	DIN EN 61508-1 (VDE 0803-1):2011-02	VDE 0803-1
EN 61508-2	IEC 61508-2	DIN EN 61508-2 (VDE 0803-2)	VDE 0803-2
EN 61508-4:2010	IEC 61508-4:2010	DIN EN 61508-4 (VDE 0803-4):2011-02	VDE 0803-4
EN 61508-5:2010	IEC 61508-5:2010	DIN EN 61508-5 (VDE 0803-5):2011-02	VDE 0803-5
EN 61511 (alle Teile)	IEC 61511 (alle Teile)	DIN EN 61511 (VDE 0810) (alle Teile)	VDE 0810
EN 61784-1	IEC 61784-1	DIN EN 61784-1	–
EN 61784-2	IEC 61784-2	DIN EN 61784-2	–
EN 61784-3-1	IEC 61784-3-1	DIN EN 61784-3-1	–
EN 61784-3-2	IEC 61784-3-2	DIN EN 61784-3-2	–
EN 61784-3-3	IEC 61784-3-3	DIN EN 61784-3-3	–
EN 61784-3-6	IEC 61784-3-6	DIN EN 61784-3-6	–
EN 61784-3-8	IEC 61784-3-8	DIN EN 61784-3-8	–
EN 61784-3-12	IEC 61784-3-12	DIN EN 61784-3-12	–
EN 61784-3-13	IEC 61784-3-13	DIN EN 61784-3-13	–
EN 61784-3-14	IEC 61784-3-14	DIN EN 61784-3-14	–
–	IEC 61784-3-17	–	–
EN 61784-3-18	IEC 61784-3-18	DIN EN 61784-3-18	–
–	IEC 61784-4	–	–
EN 61784-5 (alle Teile)	IEC 61784-5 (alle Teile)	DIN EN 61784-5 (VDE 0800-500) (alle Teile)	VDE 0800-500
EN 61800-5-2	IEC 61800-5-2	DIN EN 61800-5-2 (VDE 0160-105-2)	VDE 0160-105-2
EN 61918:2013 + AC:2014	IEC 61918:2013, mod.	DIN EN 61918 (VDE 0800-500):2014-10	VDE 0800-500
–	IEC/TR 62059-11:2002	–	–
EN 62061:2005 + Cor.:2010 + A1:2013 + A2:2015	IEC 62061:2005 + A1:2012 + A2:2015	DIN EN 62061 (VDE 0113-50):2016-05	VDE 0113-50
–	IEC/TR 62210:2003	–	–
–	IEC 62280:2014	–	–
EN 62443 (alle Teile)	IEC 62443 (alle Teile)	DIN EN 62443 (VDE 0802) (alle Teile)	VDE 0802
CLC/TR 62685	IEC/TR 62685	DIN EN 61784-3 Beiblatt 1 (VDE 0803-500 Beiblatt 1)	VDE 0803-500 Beiblatt 1

Tabelle NA. 1 (3 von 3)

Europäisches Dokument	Internationales Dokument	Deutsches Dokument	Klassifikation im VDE-Vorschriftenwerk
EN ISO 10218-1	ISO 10218-1	DIN EN ISO 10218-1	–
EN ISO 12100	ISO 12100	DIN EN ISO 12100	–
EN ISO 13849 (alle Teile)	ISO 13849 (alle Teile)	DIN EN ISO 13849 (alle Teile)	–
EN ISO 13849-1:2015	ISO 13849-1:2015	DIN EN ISO 13849-1:2016-06	–
–	ISO/IEC 2382-16:1996 ersetzt durch: ISO/IEC 2382:2015-05	–	–
EN ISO/IEC 7498-1	ISO/IEC 7498-1	DIN EN ISO/IEC 7498-1	–
–	ISO/IEC Guide 51:2014	DIN 820-12:2014-06	–
^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 60204-1 (VDE 0113-1), *Sicherheit von Maschinen – Elektrische Ausrüstung von Maschinen – Teil 1: Allgemeine Anforderungen*

DIN EN 61000-1-2 (VDE 0839-1-2), *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*

DIN EN 61000-6-7 (VDE 0839-6-7), *Elektromagnetische Verträglichkeit (EMV) – Teil 6-7: Fachgrundnormen – Störfestigkeitsanforderungen an Geräte und Einrichtungen, die zur Durchführung von Funktionen in sicherheitsbezogenen Systemen (funktionale Sicherheit) an industriellen Standorten vorgesehen sind*

DIN EN 61010-2-201 (VDE 0411-2-201):2014-01, *Sicherheitsbestimmungen für elektrische Mess-, Steuer-, Regel- und Laborgeräte – Teil 2-201: Besondere Anforderungen für Steuer- und Regelgeräte (IEC 61010-2-201:2013); Deutsche Fassung EN 61010-2-201:2013 + AC:2013*

DIN EN 61131-2 (VDE 0411-500):2008-04, *Speicherprogrammierbare Steuerungen – Teil 2: Betriebsmittelanforderungen und Prüfungen (IEC 61131-2:2007); Deutsche Fassung EN 61131-2:2007*

DIN EN 61131-2 Berichtigung 1 (VDE 0411-500 Berichtigung 1):2009-01, *Speicherprogrammierbare Steuerungen – Teil 2: Betriebsmittelanforderungen und Prüfungen (IEC 61131-2:2007); Deutsche Fassung EN 61131-2:2007, Berichtigung zu DIN EN 61131-2 (VDE 0411-500):2008-04*

DIN EN 61131-6 (VDE 0411-506), *Speicherprogrammierbare Steuerungen – Teil 6: Funktionale Sicherheit*

DIN EN 61158 (alle Teile), *Industrielle Kommunikationsnetze – Feldbusse*

DIN EN 61326-3-1 (VDE 0843-20-3-1), Elektrische Mess-, Steuer-, Regel- und Laborgeräte – EMV-Anforderungen – Teil 3-1: Störfestigkeitsanforderungen für sicherheitsbezogene Systeme und für Geräte, die für sicherheitsbezogene Funktionen vorgesehen sind (Funktionale Sicherheit) – Allgemeine industrielle Anwendungen

DIN EN 61326-2-3 (VDE 0843-20-2-3), Elektrische Mess-, Steuer-, Regel- und Laborgeräte – EMV-Anforderungen – Teil 2-3: Besondere Anforderungen – Prüfanordnung, Betriebsbedingungen und Leistungsmerkmale für Messgrößenumformer mit integrierter oder abgesetzter Signalaufbereitung

DIN EN 61496 (VDE 0113-2xx), Sicherheit von Maschinen – Berührungslos wirkende Schutzeinrichtungen

DIN EN 61496 (VDE 0113-201), Sicherheit von Maschinen – Berührungslos wirkende Schutzeinrichtungen – Teil 1: Allgemeine Anforderungen und Prüfungen

DIN EN 61508 (VDE 0803) (alle Teile), Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme

DIN EN 61508-1 (VDE 0803-1):2011-02, Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 1: Allgemeine Anforderungen (IEC 61508-1:2010); Deutsche Fassung EN 61508-1:2010

DIN EN 61508-2 (VDE 0803-2), Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 2: Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme

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 61508-5 (VDE 0803-5):2011-02, Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 5: Beispiele zur Ermittlung der Stufe der Sicherheitsintegrität (safety integrity level) (IEC 61508-5:2010); Deutsche Fassung EN 61508-5:2010

DIN EN 61511 (VDE 0810) (alle Teile), Funktionale Sicherheit – Sicherheitstechnische Systeme für die Prozessindustrie

DIN EN 61784-1, Industrielle Kommunikationsnetze – Profile – Teil 1: Feldbusprofile (nur auf CD-ROM)

DIN EN 61784-2, Industrielle Kommunikationsnetze – Profile – Teil 2: Zusätzliche Feldbusprofile für Echtzeitnetzwerke basierend auf ISO/IEC 8802-3 (nur auf CD-ROM)

DIN EN 61784-3 Beiblatt 1 (VDE 0803-500 Beiblatt 1), Industrielle Kommunikationsnetze – Profile – Beurteilungsleitfaden für Sicherheitsgeräte, die funktional sichere Übertragung nach den Profilen der IEC 61784-3 verwenden

DIN EN 61784-3-1, Industrielle Kommunikationsnetze – Profile – Teil 3-1: Funktional sichere Übertragung bei Feldbussen – Zusätzliche Festlegungen für die Kommunikationsprofilfamilie 1

DIN EN 61784-3-2, Industrielle Kommunikationsnetze – Profile – Teil 3-2: Funktional sichere Übertragung bei Feldbussen – Zusätzliche Festlegungen für die Kommunikationsprofilfamilie 2

DIN EN 61784-3-3, Industrielle Kommunikationsnetze – Profile – Teil 3-3: Funktional sichere Übertragung bei Feldbussen – Zusätzliche Festlegungen für die Kommunikationsprofilfamilie 3

DIN EN 61784-3-6, Industrielle Kommunikationsnetze – Profile – Teil 3-6: Funktional sichere Übertragung bei Feldbussen – Zusätzliche Festlegungen für die Kommunikationsprofilfamilie 6

DIN EN 61784-3-8, Industrielle Kommunikationsnetze – Profile – Teil 3-8: Funktional sichere Übertragung bei Feldbussen – Zusätzliche Festlegungen für die Kommunikationsprofilfamilie 8

DIN EN 61784-3-12, *Industrielle Kommunikationsnetze – Profile – Teil 3-12: Funktional sichere Übertragung bei Feldbussen – Zusätzliche Festlegungen für die Kommunikationsprofilfamilie 12*

DIN EN 61784-3-13, *Industrielle Kommunikationsnetze – Profile – Teil 3-13: Funktional sichere Übertragung bei Feldbussen – Zusätzliche Festlegungen für die Kommunikationsprofilfamilie 13*

DIN EN 61784-3-14, *Industrielle Kommunikationsnetze – Profile – Teil 3-14: Funktional sichere Übertragung bei Feldbussen – Zusätzliche Festlegungen für die Kommunikationsprofilfamilie 14*

DIN EN 61784-3-18, *Industrielle Kommunikationsnetze – Profile – Teil 3-18: Funktional sichere Übertragung bei Feldbussen – Zusätzliche Festlegungen für die Kommunikationsprofilfamilie 18*

DIN EN 61784-5 (VDE 0800-500) (alle Teile), *Industrielle Kommunikationsnetze – Profile – Teil 5-x: Feldbus-installation*

DIN EN 61800-5-2 (VDE 0160-105-2), *Elektrische Leistungsantriebssysteme mit einstellbarer Drehzahl – Teil 5-2: Anforderungen an die Sicherheit – Funktionale Sicherheit*

DIN EN 61918 (VDE 0800-500):2014-10, *Industrielle Kommunikationsnetze – Installation von Kommunikationsnetzen in Industrieanlagen (IEC 61918:2013, modifiziert); Deutsche Fassung EN 61918:2013 + AC:2014*

DIN EN 62061 (VDE 0113-50):2016-05, *Sicherheit von Maschinen – Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und programmierbarer elektronischer Steuerungssysteme (IEC 62061:2005 + A1:2012 + A2:2015); Deutsche Fassung EN 62061:2005 + Cor.:2010 + A1:2013 + A2:2015*

DIN EN 62443 (VDE 0802) (alle Teile), *IT-Sicherheit für industrielle Automatisierungssysteme*

DIN EN ISO 10218-1, *Industrieroboter – Sicherheitsanforderungen – Teil 1: Roboter*

DIN EN ISO 12100, *Sicherheit von Maschinen – Allgemeine Gestaltungsleitsätze – Risikobeurteilung und Risikominderung*

DIN EN ISO 13849 (alle Teile), *Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen*

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

DIN EN ISO/IEC 7498-1, *Informationstechnik – Kommunikation Offener Systeme – Teil 1: Basis-Referenzmodell: Basismodell*

**Industrielle Kommunikationsnetze –
Profile –
Teil 3: Funktional sichere Übertragung bei Feldbussen –
Allgemeine Regeln und Festlegungen für Profile
(IEC 61784-3:2016)**

Industrial communication networks –
Profiles –
Part 3: Functional safety fieldbuses –
General rules and profile definitions
(IEC 61784-3:2016)

Réseaux de communication industriels –
Profils –
Partie 3: Bus de terrain de sécurité
fonctionnelle – Règles générales et
définitions de profils
(IEC 61784-3:2016)

Diese Europäische Norm wurde von CENELEC am 2016-06-17 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, 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: Avenue Marnix 17, B-1000 Brüssel

© 2016 CENELEC – Alle Rechte der Verwertung, gleich in welcher Form und in welchem Verfahren, sind weltweit den Mitgliedern von CENELEC vorbehalten.

Ref. Nr. EN 61784-3:2016 D

Europäisches Vorwort

Der Text des Dokuments 65C/840/FDIS, zukünftige 3. Ausgabe der IEC 61784-3, erarbeitet vom SC 65C „Industrial networks“ des IEC/TC 65 „Industrial-process measurement, control and automation“, wurde zur parallelen IEC-CENELEC-Abstimmung vorgelegt und von CENELEC als EN 61784-3:2016 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): 2017-03-17
- spätestes Datum, zu dem nationale Normen, die diesem Dokument entgegenstehen, zurückgezogen werden müssen (dow): 2019-06-17

Dieses Dokument ersetzt **EN 61784-3:2010**.

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

Anerkennungsnotiz

Der Text der Internationalen Norm IEC 61784-3:2016 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 60204-1	ANMERKUNG	Harmonisiert als EN 60204-1 .
IEC 61131-2:2007	ANMERKUNG	Harmonisiert als EN 61131-2:2007 (nicht modifiziert).
IEC 61131-6	ANMERKUNG	Harmonisiert als EN 61131-6 .
IEC 61496 (alle Teile)	ANMERKUNG	Harmonisiert in der Reihe EN 61496.
IEC 61496-1	ANMERKUNG	Harmonisiert als EN 61496-1 .
IEC 61508-4:2010	ANMERKUNG	Harmonisiert als EN 61508-4:2010 (nicht modifiziert).
IEC 61508-5:2010	ANMERKUNG	Harmonisiert als EN 61508-5:2010 (nicht modifiziert).
IEC 61511 (alle Teile)	ANMERKUNG	Harmonisiert in der Reihe EN 61511.
IEC 61800-5-2	ANMERKUNG	Harmonisiert als EN 61800-5-2 .
IEC 62061:2005	ANMERKUNG	Harmonisiert als EN 62061:2005 (nicht modifiziert).
IEC/TR 62685	ANMERKUNG	Harmonisiert als CLC/TR 62685 .
ISO 10218-1	ANMERKUNG	Harmonisiert als EN ISO 10218-1.
ISO 12100	ANMERKUNG	Harmonisiert als EN ISO 12100.
ISO 13849 (alle Teile)	ANMERKUNG	Harmonisiert in der Reihe EN ISO 13849.
ISO 13849-1:2015	ANMERKUNG	Harmonisiert als EN ISO 13849-1:2015 (nicht modifiziert).

Inhalt

Seite

Europäisches Vorwort	2
0 Einleitung.....	8
0.1 Allgemeines.....	8
0.2 Übergang von Ausgabe 2 zu erweiterten Bewertungsmethoden in Ausgabe 3	10
0.3 Patentangaben	11
1 Anwendungsbereich.....	12
2 Normative Verweisungen	12
3 Begriffe, Symbole, Abkürzungen und Konventionen	14
3.1 Begriffe	14
3.2 Symbole und Abkürzungen	22
4 Konformität.....	23
5 Grundlagen von sicherheitsbezogenen Feldbussystemen	23
5.1 Struktur einer Sicherheitsfunktion	23
5.2 Kommunikationssystem	24
5.2.1 Allgemeines.....	24
5.2.2 Feldbusse der IEC 61158	24
5.2.3 Kommunikationskanaltypen	25
5.2.4 Reaktionszeit einer Sicherheitsfunktion	25
5.3 Kommunikationsfehler.....	26
5.3.1 Allgemeines.....	26
5.3.2 Verfälschung	26
5.3.3 Unbeabsichtigte Wiederholung	26
5.3.4 Falsche Abfolge	27
5.3.5 Verlust	27
5.3.6 Inakzeptable Verzögerung	27
5.3.7 Einfügung	27
5.3.8 Maskerade	27
5.3.9 Adressierung	27
5.4 Deterministische Abhilfemaßnahmen	27
5.4.1 Allgemeines.....	27
5.4.2 Laufende Nummer	28
5.4.3 Zeitstempel.....	28
5.4.4 Zeiterwartung	28
5.4.5 Verbindungsauthentizität.....	28
5.4.6 Rückmeldung	28
5.4.7 Datensicherung	28
5.4.8 Redundanz mit Kreuzvergleich	29
5.4.9 Unterschiedliche Sicherungssysteme für die Datenintegrität	29

5.5	Typische Beziehungen zwischen Fehlern und Sicherheitsmaßnahmen.....	29
5.6	Kommunikationsphasen	30
5.7	FSCP-Implementierungsaspekte	31
5.8	Betrachtungen zur Datenintegrität.....	32
5.8.1	Berechnung der Restfehlerrate	32
5.8.2	Gesamtrestfehlerrate und SIL	33
5.9	Beziehungen zwischen funktionaler Sicherheit und IT-Sicherheit	34
5.10	Randbedingungen und Auflagen.....	35
5.10.1	Elektrische Sicherheit.....	35
5.10.2	Elektromagnetische Verträglichkeit (EMV).....	35
5.11	Installationsleitfäden	36
5.12	Sicherheitshandbuch	36
5.13	Sicherheitsgrundsätze (Policy).....	36
6	Kommunikationsprofilfamilie 1 (Foundation™ Fieldbus) – Profile für funktionale Sicherheit.....	37
7	Kommunikationsprofilfamilie 2 (CIP™) und Familie 16 (SERCOS®) – Profile für funktionale Sicherheit.....	37
8	Kommunikationsprofilfamilie 3 (PROFIBUS™, PROFINET™) – Profile für funktionale Sicherheit.....	37
9	Kommunikationsprofilfamilie 6 (INTERBUS®) – Profile für funktionale Sicherheit.....	38
10	Kommunikationsprofilfamilie 8 (CC-Link™) – Profile für funktionale Sicherheit	38
10.1	Funktional sicheres Kommunikationsprofil 8/1	38
10.2	Funktional sicheres Kommunikationsprofil 8/2	39
11	Kommunikationsprofilfamilie 12 (EtherCAT™) – Profile für funktionale Sicherheit.....	39
12	Kommunikationsprofilfamilie 13 (Ethernet POWERLINK™) – Profile für funktionale Sicherheit.....	39
13	Kommunikationsprofilfamilie 14 (EPA®) – Profile für funktionale Sicherheit	40
14	Kommunikationsprofilfamilie 17 (RAPIEnet™) – Profile für funktionale Sicherheit.....	40
15	Kommunikationsprofilfamilie 18 (SafetyNET p™) – Profile für funktionale Sicherheit.....	40
	Anhang A (informativ) Beispiele für funktional sichere Kommunikationsmodelle	41
A.1	Allgemeines	41
A.2	Modell A (Einzelnachricht, Kanal und FAL, redundante SCLs).....	41
A.3	Modell B (vollständige Redundanz).....	41
A.4	Modell C (redundante Nachrichten, FALs und SCLs, einkanalig).....	42
A.5	Modell D (redundante Nachrichten und SCLs, einkanalig und FAL)	42
	Anhang B (normativ) Kanalmodell für sichere Kommunikation unter Einsatz von CRC-basierten Fehlerprüfungen	44
B.1	Übersicht	44
B.2	Kanalmodell für Berechnungen	44
B.3	Bitfehlerwahrscheinlichkeit P_e	45
B.4	CRC-Prüfung	45

B.4.1	Allgemeines.....	45
B.4.2	Betrachtungen zu CRC-Polynomen.....	47
Anhang C (informativ) Struktur der technologiespezifischen Teile		49
Anhang D (informativ) Bewertungsleitfaden.....		51
D.1	Übersicht	51
D.2	Kanaltypen	51
D.2.1	Allgemeines.....	51
D.2.2	„Black Channel“.....	51
D.2.3	„White Channel“	51
D.3	Überlegungen zur Datensicherung bei „White Channel“-Ansätzen.....	52
D.3.1	Allgemeines.....	52
D.3.2	Modell B und Modell C	52
D.3.3	Modell A und Modell D	53
D.4	Verifikation der Sicherheitsmaßnahmen	54
D.4.1	Allgemeines.....	54
D.4.2	Implementierung.....	54
D.4.3	„Ruhestromprinzip“	54
D.4.4	Sicherer Zustand	54
D.4.5	Übertragungsfehler	54
D.4.6	Sicherheitsreaktions- und Antwortzeiten.....	54
D.4.7	Kombinierte Maßnahmen.....	55
D.4.8	Rückwirkungsfreiheit	55
D.4.9	Weitere Fehlerfälle („White Channel“)	55
D.4.10	Referenztestanlagen und Betriebsbedingungen.....	55
D.4.11	Konformitäts-Tester.....	55
Anhang E (informativ) Beispiele für implizite FSCP-Mechanismen		56
E.1	Allgemeines.....	56
E.2	Beispiel für Feldbus-Nachricht mit Sicherheits-PDUs.....	56
E.3	Modell mit ausschließlich expliziten Sicherungsmechanismen	56
E.4	Modell mit explizitem A-Code- und implizitem T-Code-Sicherungsmechanismus	57
E.5	Modell mit explizitem T-Code- und implizitem A-Code-Sicherungsmechanismus	57
E.6	Modell mit teilweise expliziten und teilweise impliziten Sicherungsmechanismen	58
E.7	Modell mit ausschließlich impliziten Sicherungsmechanismen	59
E.8	Ergänzung zu Anhang B – Einfluss der impliziten Daten auf die „Properness“.....	59
Anhang F (informativ) Erweiterte Modelle für die Abschätzung der gesamten Restfehlerrate		60
F.1	Geltungsbereich	60
F.2	Allgemeine Modelle für die „Black-Channel“-Kommunikation.....	60
F.3	Die Grund-Sicherheitseigenschaften	61
F.4	Annahmen für die Berechnung der Restfehler.....	61

F.5	Restfehlerraten	62
F.5.1	Explizite und implizite Mechanismen.....	62
F.5.2	Berechnungen der Restfehlerraten	62
F.5.2.1	Allgemeines	62
F.5.2.2	Beitrag von Datenintegritätsfehlern (RR_I)	63
F.5.2.3	Beitrag von Authentizitätsfehlern (RR_A).....	63
F.5.2.4	Beitrag von Aktualitätsfehlern (RR_T)	63
F.5.2.5	Beitrag von Maskeradefehlern (RR_M)	64
F.6	Datenintegrität	64
F.6.1	Probabilistische Betrachtungen.....	64
F.6.2	Deterministische Betrachtungen	64
F.7	Authentizität.....	65
F.7.1	Allgemeines	65
F.7.2	Restfehlerrate für Authentizität (RR_A)	66
F.8	Aktualität (en: Timeliness)	67
F.8.1	Allgemeines	67
F.8.2	Restfehlerrate für Aktualität (RR_T)	69
F.9	Maskerade	70
F.9.1	Allgemeines	70
F.9.2	Restfehlerrate für die Abweisung von Maskerade (RR_M)	70
F.10	Berechnung der Gesamtrestfehlerrate für die SCL.....	70
F.10.1	Auf Basis der Summe der Restfehlerraten.....	70
F.10.2	Auf Basis anderer quantitativer Nachweise.....	71
F.11	Gesamtfehlerrate und SIL	72
F.12	Konfiguration und Parametrierung eines FSCP	72
F.12.1	Allgemeines	72
F.12.2	Änderungsrate der Konfiguration und Parametrierung	74
F.12.3	Restfehlerrate für die Konfiguration und Parametrierung.....	74
	Literaturhinweise.....	75
	Anhang ZA (normativ) Normative Verweisungen auf internationale Publikationen mit ihren entsprechenden europäischen Publikationen	78
Bilder		
	Bild 1 – Beziehungen der IEC 61784-3 zu anderen Normen (Fertigung).....	8
	Bild 2 – Beziehungen der IEC 61784-3 zu anderen Normen (Prozess).....	9
	Bild 3 – Übergang von den Bewertungsmethoden der Ausgabe 2 zu denen der Ausgabe 3	10
	Bild 4 – Sichere Kommunikation als Teil einer Sicherheitsfunktion.....	24
	Bild 5 – Modellbeispiel für ein funktional sicheres Kommunikationssystem.....	25
	Bild 6 – Beispiel für die Reaktionszeitkette einer Sicherheitsfunktion	26

Bild 7 – Konzeptionelles FSCP-Protokollmodell	31
Bild 8 – Implementierungsaspekte eines FSCP	31
Bild 9 – Anwendungsbeispiel 1 ($m = 4$).....	33
Bild 10 – Anwendungsbeispiel 2 ($m = 2$).....	33
Bild 11 – Zonen und Durchleitungskonzept für IT-Sicherheit nach IEC 62443.....	35
Bild A.1 – Modell A	41
Bild A.2 – Modell B	42
Bild A.3 – Modell C	42
Bild A.4 – Modell D	43
Bild B.1 – Kommunikationskanal mit Störungen	44
Bild B.2 – Binärsymmetrischer Kanal (BSC)	45
Bild B.3 – Beispiel eines Blocks mit Nachrichtteil und CRC-Signatur	46
Bild B.4 – Blockcodes zur Fehlerrückmeldung	47
Bild B.5 – Propere und nicht propere CRC-Polynome	48
Bild D.1 – Grundlegendes Markov-Modell.....	53
Bild E.1 – Beispiel von Sicherheits-PDUs in einer Feldbusnachricht.....	56
Bild E.2 – Modell mit ausschließlich expliziten Sicherungsmechanismen	56
Bild E.3 – Modell mit explizitem A-Code- und implizitem T-Code-Sicherungsmechanismus	57
Bild E.4 – Modell mit explizitem T-Code- und implizitem A-Code-Sicherungsmechanismus	58
Bild E.5 – Modell mit teilweise explizitem und teilweise implizitem Sicherungsmechanismus für die Aktualität und implizitem Sicherungsmechanismus für die Authentizität.....	58
Bild E.6 – Modell mit ausschließlich impliziten Sicherungsmechanismen	59
Bild F.1 – „Black Channel“ aus der Sicht des FSCP	60
Bild F.2 – Modell für die Authentizitäts-Betrachtung	65
Bild F.3 – Feldbus- und interne Adressfehler	66
Bild F.4 – Beispiel einer allmählich ansteigenden Nachrichten-Latenzzeit.....	68
Bild F.5 – Beispiel für das Versagen eines aktiven Netzwerkelements	69
Bild F.6 – Anwendungsbeispiel 1 ($m = 4$).....	71
Bild F.7 – Anwendungsbeispiel 2 ($m = 2$).....	71
Bild F.8 – Beispiel mit Konfigurier- und Parametervorgängen für FSCPs	73
Tabellen	
Tabelle 1 – Überblick über die Wirksamkeit von Maßnahmen gegen mögliche Fehler	30
Tabelle 2 – Definition der Größen für die Berechnung der Restfehlerraten.....	32
Tabelle 3 – Typische Beziehung zwischen Restfehlerrate und SIL	34
Tabelle 4 – Typische Beziehung zwischen Restfehler auf Anforderung und SIL	34
Tabelle 5 – Übersicht über Profilkennungen für FSCP 6/7	38
Tabelle B.1 – Beispiel für die Abhängigkeit von $d_{\min}$ und Blockbitlänge n	47
Tabelle C.1 – Gemeinsame Gliederung der technologiespezifischen Teile	49
Tabelle F.1 – Typische Beziehung zwischen Restfehlerrate und SIL.....	72
Tabelle F.2 – Typische Beziehung zwischen Restfehler auf Anforderung und SIL	72

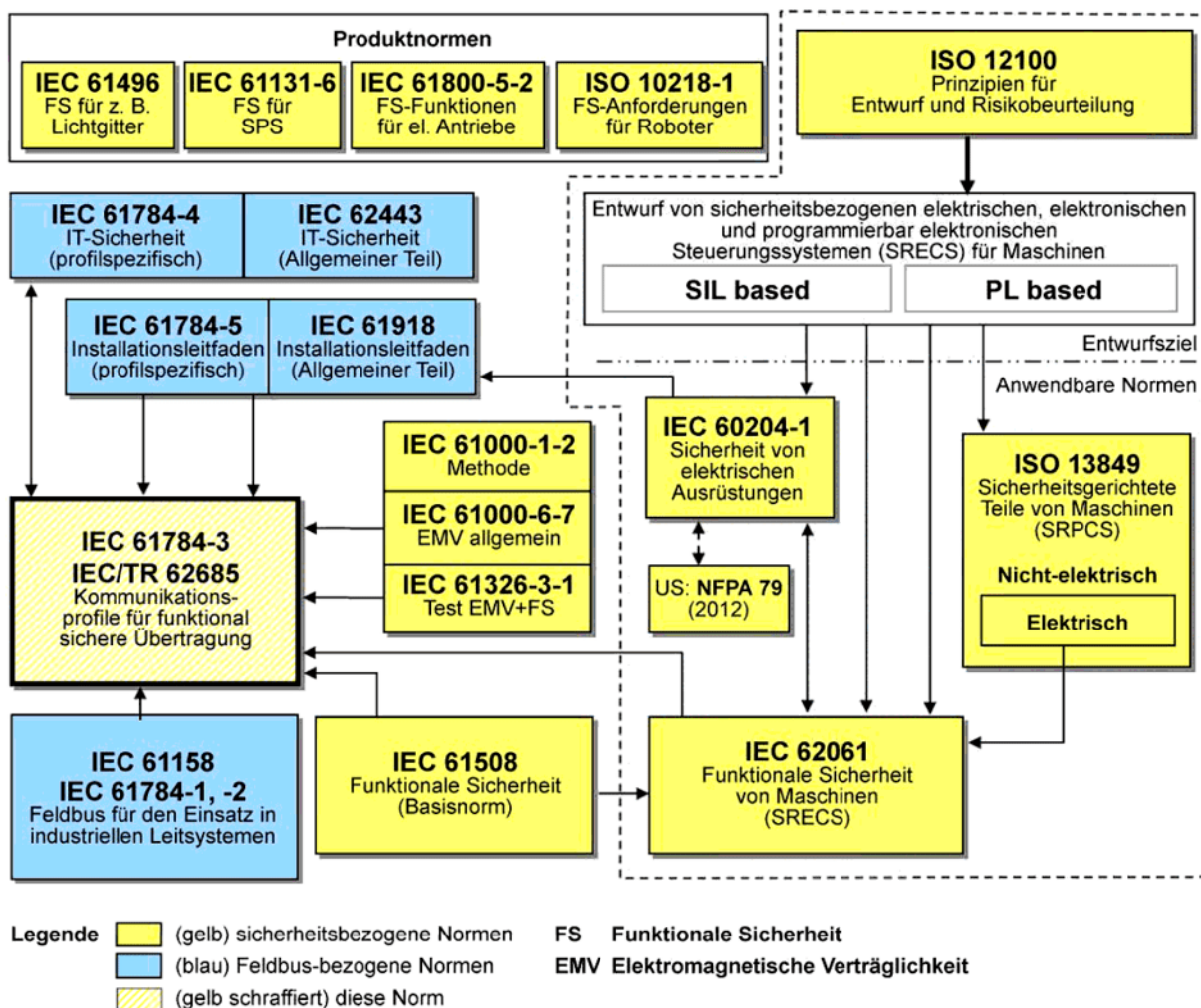
0 Einleitung

0.1 Allgemeines

Die IEC 61158-Feldbusnormen und ihre Begleitnormen IEC 61784-1 bzw. IEC 61784-2 spezifizieren zusammen mehrere Kommunikationsprotokolle, die die dezentrale Automatisierung von Applikationen ermöglichen. Die Feldbustechnologie hat sich inzwischen in der Praxis bewährt und ist in hohem Maße akzeptiert. So treten nun Feldbuserweiterungen in Erscheinung, die auf Anwendungen für Bereiche wie Echtzeit, funktionale Sicherheit und Informationssicherheit abzielen.

Diese Norm erläutert die relevanten Prinzipien für funktional sichere Kommunikation bezogen auf Normen der Reihe IEC 61508. Sie spezifiziert mehrere Sicherheitskommunikationsschichten (Profile und entsprechende Protokolle) basierend auf den Kommunikationsprofilen und Protokollschichten in der IEC 61784-1, IEC 61784-2 und der Reihe IEC 61158. Sie deckt Aspekte der elektrischen Sicherheit und der Eigensicherheit nicht ab.

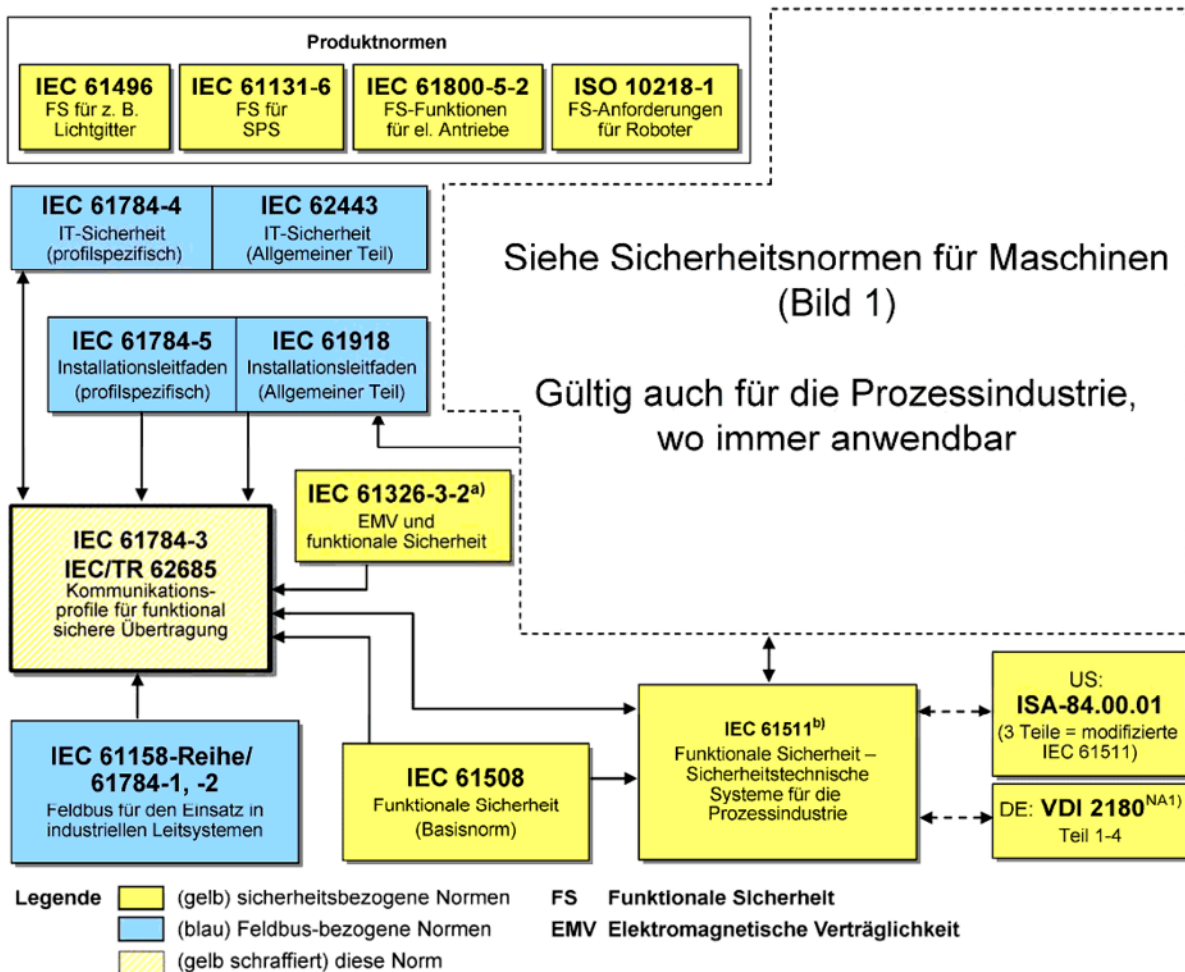
Bild 1 zeigt die Beziehungen dieser Norm zu für die Fertigungsautomatisierung relevanten Sicherheits- und Feldbusnormen.



ANMERKUNG: Unterabschnitte 6.7.6.4 (hohe Komplexität) und 6.7.8.1.6 (niedrige Komplexität) der IEC 62061 beschreiben das Verhältnis zwischen PL (Kategorie) und SIL.

Bild 1 – Beziehungen der IEC 61784-3 zu anderen Normen (Fertigung)

Bild 2 zeigt die Beziehungen dieser Norm zu für die Prozessautomatisierung relevanten Sicherheits- und Feldbusnormen.



- a) In spezifizierten elektromagnetischen Umgebungen, ansonsten IEC 61326-3-1 oder IEC 61000-6-7.
- b) Als EN ratifiziert.
- NA1) Gemeint ist VDI/VDE 2180 Blatt 1 bis Blatt 5.

Bild 2 – Beziehungen der IEC 61784-3 zu anderen Normen (Prozess)

Die als Bestandteile eines sicherheitsgerichteten Systems nach Reihe IEC 61508 implementierten Sicherheitskommunikationsschichten gewährleisten das notwendige Vertrauen in den Transport von Nachrichten (Informationen) zwischen zwei oder mehr Feldbusteilnehmern in einem sicherheitsbezogenen System bzw. ausreichendes Vertrauen in das Sicherheitsverhalten beim Auftreten von Feldbusfehlern oder -ausfällen.

Die in dieser Norm spezifizierten Sicherheitskommunikationsschichten tun dies dergestalt, dass ein Feldbus in Anwendungen mit funktionaler Sicherheit bis zu einer Sicherheitsstufe (SIL) eingesetzt werden kann, wie sie im jeweiligen Kommunikationsprofil für funktional sichere Übertragung festgelegt ist.

Der resultierende SIL-Anspruch eines Systems hängt von der Implementierung des gewählten Kommunikationsprofils für funktional sichere Übertragung (FSCP) in diesem System ab – eine Implementierung eines funktional sicheren Kommunikationsprofils in einem Standardgerät reicht nicht aus, um es als Sicherheitsgerät zu qualifizieren.

Diese Norm beschreibt:

- grundlegende Prinzipien für die Erfüllung der Anforderungen der Reihe IEC 61508 für die funktional sichere Kommunikation, einschließlich möglicher Übertragungsfehler, deren Abhilfemaßnahmen und Betrachtungen zur Datenintegrität;
- funktional sichere Kommunikationsprofile für mehrere Kommunikationsprofilfamilien der IEC 61784-1 und IEC 61784-2, welche Ergänzungen der Kommunikationsdienst- und -protokollabschnitte der Reihe IEC 61158 um eine Sicherheitsschicht enthalten.

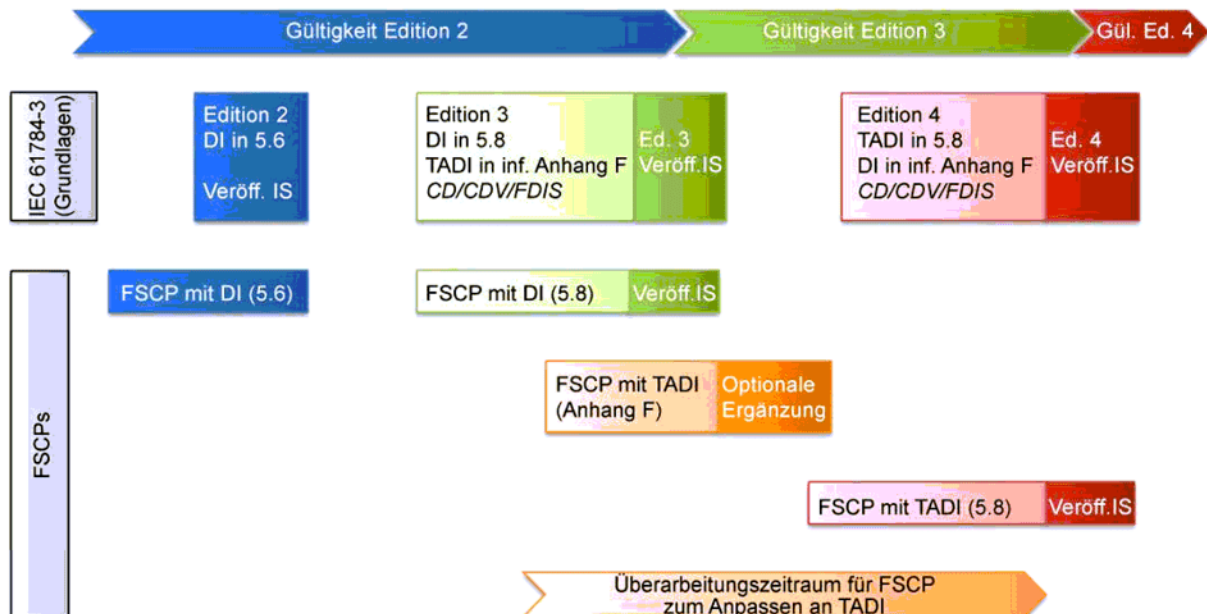
0.2 Übergang von Ausgabe 2 zu erweiterten Bewertungsmethoden in Ausgabe 3

Diese Ausgabe des allgemeinen Teils der Norm enthält zusätzliche erweiterte Modelle zur künftigen Anwendung beim Abschätzen der gesamten Restfehlerrate eines FSCP. Dieser Wert kann zur Überprüfung dienen, ob das FSCP bestimmte SIL-Anforderungen funktional sicherer Applikationen erfüllt. Diese erweiterten Modelle zur qualitativen und quantitativen Bestimmung funktionaler Sicherheit sind in [Anhang E](#) und [Anhang F](#) detailliert beschrieben.

Bedingt durch die in der Regel zeitaufwändigen Bewertungsprozesse können die vor oder in dieser Norm erschienenen FSCPs nur nach den Methoden vorhergehender Ausgaben abgenommen werden, die auf Datenintegritäts-Betrachtungen in [5.8](#) beruhen.

Das Gültigkeitsschema in Bild 3 zeigt, wie der Übergang von den ursprünglichen Bewertungsmethoden der Ausgabe 2 (spezifiziert in [5.8](#)) zu den erweiterten Bewertungsmethoden der Ausgabe 3 (zurzeit spezifiziert in [Anhang F](#)) gehandhabt werden soll. Gemäß diesem Schema sind die FSCPs von einer neuerlichen Bewertung in Übereinstimmung mit [Anhang F](#) befreit bis zur Ausgabe 4, in der die Inhalte des jetzigen Anhangs F die des [5.8](#) ersetzen werden.

ANMERKUNG: Ein bestimmtes FSCP kann jedoch eine frühere Bewertung vornehmen und eine entsprechende Änderung veröffentlichen.



Legende

DI Datenintegrität

TADI Timeliness (Aktualität), Authenticity (Authentizität), Datenintegrität

Bild 3 – Übergang von den Bewertungsmethoden der Ausgabe 2 zu denen der Ausgabe 3

0.3 Patentangaben

Die Organisation International Electrotechnical Commission (IEC) weist auf Ansprüche hin, die es für eine Übereinstimmung mit diesem Dokument notwendig machen, von Patenten Gebrauch zu machen. Dies betrifft funktional sichere Kommunikationsprofile für die Familien 1, 2, 3, 6, 8, 12, 13, 14, 17 und 18 in IEC 61784-3-1, IEC 61784-3-2, IEC 61784-3-3, IEC 61784-3-6, IEC 61784-3-8, IEC 61784-3-12, IEC 61784-3-13, IEC 61784-3-14, IEC 61784-3-17 und IEC 61784-3-18.

IEC übernimmt keine Verantwortung hinsichtlich Nachweisen, Gültigkeit und Anwendungsbereich von Patentrechten.

Die Halter der Patentrechte haben der IEC gegenüber versichert, dass sie bereit sind, Anwendern weltweit Nutzungsrechte unentgeltlich oder zu angemessenen und nicht diskriminierenden Bedingungen einzuräumen. Diesbezügliche Aussagen der Halter von solchen Patentrechten sind bei der IEC hinterlegt.

ANMERKUNG Details und Kontaktinformationen zu den Patenten sind verfügbar in IEC 61784-3-1, IEC 61784-3-2, IEC 61784-3-3, IEC 61784-3-6, IEC 61784-3-8, IEC 61784-3-12, IEC 61784-3-13, IEC 61784-3-14, IEC 61784-3-17 und IEC 61784-3-18.

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

ISO (www.iso.org/patents) und IEC (<http://patents.iec.ch>) unterhalten Online-Datenbanken mit Patenten, die für ihre jeweiligen Standards relevant sind. Den Anwendern wird geraten, diese Datenbanken zu nutzen, um aktuellste Informationen über Patente zu erlangen.

1 Anwendungsbereich

Dieser Teil der Reihe IEC 61784-3 erläutert einige allgemeine Prinzipien, die bei der Übertragung von sicherheitsbezogenen Nachrichten zwischen Teilnehmern eines verteilten Netzwerks mit Feldbustechnologie zum Einsatz kommen können und die den Anforderungen der Reihe IEC 61508¹⁾ entsprechen. Diese Prinzipien basieren auf dem Black-Channel-Ansatz. Sie können in zahlreichen industriellen Anwendungen wie Prozess- oder Fertigungsautomatisierung und Maschinenanlagen genutzt werden.

Dieser Normteil²⁾ und die IEC 61784-3-x-Normteile spezifizieren mehrere Kommunikationsprofile für funktional sichere Übertragung basierend auf den Kommunikationsprofilen und Protokollschichten der Feldbustechnologien in IEC 61784-1, IEC 61784-2 und der Reihe IEC 61158. Diese funktional sicheren Kommunikationsprofile nutzen den Black-Channel-Ansatz, wie er in IEC 61508 definiert ist. Sie sind ausnahmslos für eine Implementierung in sicherheitsgerichteten Geräten gedacht.

ANMERKUNG 1 Es kann andere sicherheitsbezogene Kommunikationssysteme geben, die den Anforderungen der IEC 61508 entsprechen, jedoch in dieser Norm nicht enthalten sind.

ANMERKUNG 2 Sie deckt Aspekte der elektrischen Sicherheit und Eigensicherheit nicht ab. Elektrische Sicherheit bezieht sich auf Gefährdungen wie elektrischer Schlag. Eigensicherheit bezieht sich auf Gefährdungen, wie sie durch explosionsfähige Gasgemische gegeben sind.

Alle Systeme sind irgendwann im Laufe ihres Lebenszyklus unautorisierten Zugriffen ausgesetzt. Zusätzliche Maßnahmen sind daher in jeder sicherheitsbezogenen Anwendung einzuplanen, um Feldbussysteme gegen unautorisierte Zugriffe zu schützen. Die Reihe IEC 62443 wird viele diesbezügliche Punkte betrachten; die Beziehung zur IEC 62443 ist in einem eigenen Unterabschnitt dieses Normteils weiter ausgeführt.

ANMERKUNG 3 In einer künftigen IEC 61784-4³⁾ können zusätzlich profilspezifische Anforderungen an die Datensicherheit definiert werden.

ANMERKUNG 4 Die Implementation eines Kommunikationsprofils für funktional sichere Übertragung nach diesem Normteil in einem Gerät reicht nicht aus, um es zum Sicherheitsgerät nach Reihe IEC 61508 zu qualifizieren.

ANMERKUNG 5 Der resultierende SIL-Anspruch eines Systems hängt von der Implementierung eines ausgewählten Kommunikationsprofils für funktional sichere Übertragung innerhalb dieses Systems ab.

2 Normative Verweisungen

Die folgenden Dokumente, die in diesem Dokument teilweise oder als Ganzes normativ 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 61000-6-7, *Electromagnetic compatibility (EMC) – Part 6-7: Generic standards – Immunity requirements for equipment intended to perform functions in a safety-related system (functional safety) in industrial locations*

IEC 61010-2-201:2013, *Safety requirements for electrical equipment for measurement, control and laboratory use – Part 2-201: Particular requirements for control equipment*

IEC 61158 (alle Teile), *Industrial communication networks – Fieldbus specifications*

¹⁾ In den nachfolgenden Seiten dieser Norm bedeutet „IEC 61508“ stets „Reihe IEC 61508“.

²⁾ In den nachfolgenden Seiten dieser Norm bedeutet „dieser Normteil“ stets „dieser Teil der Reihe IEC 61784-3“.

³⁾ Vorgeschlagenes Normungsprojekt wird derzeit geprüft.

IEC 61326-3-1, *Electrical equipment for measurement, control and laboratory use – EMC requirements – Part 3-1: Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety) – General industrial applications*

IEC 61326-3-2, *Electrical equipment for measurement, control and laboratory use – EMC requirements – Part 3-2: Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety) – Industrial applications with specified EM environment*

IEC 61508 (alle Teile), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

IEC 61508-1:2010, *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 61784-1, *Industrial communication networks – Profiles – Part 1: Fieldbus profiles*

IEC 61784-2, *Industrial communication networks – Profiles – Part 2: Additional fieldbus profiles for real-time networks based on ISO/IEC 8802-3*

IEC 61784-3-1, *Industrial communication networks – Profiles – Part 3-1: Functional safety fieldbuses – Additional specifications for CPF 1*

IEC 61784-3-2, *Industrial communication networks – Profiles – Part 3-2: Functional safety fieldbuses – Additional specifications for CPF 2*

IEC 61784-3-3, *Industrial communication networks – Profiles – Part 3-3: Functional safety fieldbuses – Additional specifications for CPF 3*

IEC 61784-3-6, *Industrial communication networks – Profiles – Part 3-6: Functional safety fieldbuses – Additional specifications for CPF 6*

IEC 61784-3-8, *Industrial communication networks – Profiles – Part 3-8: Functional safety fieldbuses – Additional specifications for CPF 8*

IEC 61784-3-12, *Industrial communication networks – Profiles – Part 3-12: Functional safety fieldbuses – Additional specifications for CPF 12*

IEC 61784-3-13, *Industrial communications networks – Profiles – Part 3-13: Functional safety fieldbuses – Additional specifications for CPF 13*

IEC 61784-3-14, *Industrial communication networks – Profiles – Part 3-14: Functional safety fieldbuses – Additional specifications for CPF 14*

IEC 61784-3-17⁴⁾, *Industrial communication networks – Profiles – Part 3-17: Functional safety fieldbuses – Additional specifications for CPF 17*

IEC 61784-3-18, *Industrial communication networks – Profiles – Part 3-18: Functional safety fieldbuses – Additional specifications for CPF 18*

IEC 61784-5 (alle Teile), *Industrial communication networks – Profiles – Part 5: Installation of fieldbuses*

IEC 61918:2013, *Industrial communication networks – Installation of communication networks in industrial premises*

IEC 62443 (alle Teile), *Industrial communication networks – Network and system security*

⁴⁾ Noch zu veröffentlichen.

3 Begriffe, Symbole, Abkürzungen und Konventionen

3.1 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

ANMERKUNG: Kursive Schrift wird in den Definitionen verwendet, um Begriffe zu markieren, die selbst in 3.1 definiert sind.

3.1.1

absoluter Zeitstempel

(en: **absolute time stamp**)

Zeitstempel, der sich auf eine zentrale Zeit bezieht, welche für eine Gruppe von Geräten an einem Feldbus gleich ist

[QUELLE: IEC 62280:2014, 3.1.1, modifiziert – Geräte und Feldbus verwendet]

3.1.2

aktives Netzwerkelement

(en: **active network element**)

Netzwerkelement mit elektrischen und/oder optischen aktiven Bauteilen, die eine Erweiterung des Netzwerkes ermöglichen

Anmerkung 1 zum Begriff: Beispiele für aktive Netzwerkelemente sind Signalverstärker und Switches

[QUELLE: IEC 61918:2013, 3.1.2]

3.1.3

Verfügbarkeit

(en: **availability**)

Wahrscheinlichkeit eines automatisierten Systems, dass innerhalb einer bestimmten Zeitdauer keine unzureichenden Systembedingungen wie Produktionsausfall auftreten

3.1.4

Bitfehlerwahrscheinlichkeit

(en: **bit error probability**)

P_e

Wahrscheinlichkeit, dass für ein gegebenes Bit der falsche Wert empfangen wird.

3.1.5

Black Channel

festgelegtes Kommunikationssystem, bestehend aus einem oder mehreren Elementen ohne Nachweis des Entwurfs oder der Validierung nach IEC 61508

Anmerkung 1 zum Begriff: Diese Definition erweitert die übliche Definition eines Kommunikationskanals um das System, welches den Kanal enthält.

3.1.6

Bridge

abstraktes (Kommunikations-)Element, welches auf der Ebene des Data Link Layer mehrere Netzwerksegmente verbindet

3.1.7

geschlossenes Kommunikationssystem

(en: **closed communication system**)

festgelegte Anzahl oder festgelegte maximale Anzahl von Teilnehmern, die über ein Kommunikationssystem verbunden sind, mit wohldefinierten und festgelegten Eigenschaften und wo das Risiko eines unerlaubten Zugriffs als vernachlässigbar betrachtet wird

[QUELLE: IEC 62280-1:2002, 3.2, modifiziert – Übertragung ersetzt durch Kommunikation]

3.1.8

Kommunikationskanal

(en: communication channel)

logische Verbindung zwischen zwei Endpunkten in einem *Kommunikationssystem*

3.1.9

Kommunikationssystem

(en: communication system)

Anordnung von Hardware, Software und Ausbreitungsmedien zur Übertragung von Nachrichten (ISO/IEC 7498-1-Anwendungsschicht) von einer Anwendung zur anderen

3.1.10

Verbindung

(en: connection)

logische Verbindung zwischen zwei Anwendungsobjekten in demselben oder in unterschiedlichen Geräten

3.1.11

CRC

(en: Cyclic Redundancy Check)

<Wert> redundante Daten, abgeleitet von einem Block von Daten und mit diesen zusammen gespeichert oder übertragen zur Aufdeckung von Datenverfälschungen

<Methode> Prozedur zur Berechnung der redundanten Daten

Anmerkung 1 zum Begriff: Begriffe wie „CRC-Code“ und „CRC-Signatur“ und Bezeichnungen wie CRC1, CRC2 können ebenfalls in dieser Norm verwendet sein, um redundante Daten zu kennzeichnen.

Anmerkung 2 zum Begriff: Siehe auch [28], [29]⁵⁾.

3.1.12

festgelegtes Kommunikationssystem

(en: defined communication system (defined channel))

Festgelegte Anzahl oder festgelegte maximale Anzahl von Teilnehmern, die über ein Kommunikationssystem verbunden sind, mit wohldefinierten und festgelegten Eigenschaften wie beispielsweise Aufbaubedingungen, elektromagnetische Störfestigkeit, industrielle (aktive) Netzwerkkomponenten und wo das Risiko eines unerlaubten Zugriffs gemäß Lebenszyklusmodell der IEC 62443 auf ein toleriertes Maß reduziert ist durch zum Beispiel Zonen und Durchleitungen

3.1.13

Diversität

(en: diversity)

ungleichartige Mittel zur Ausführung einer geforderten Funktion

Anmerkung 1 zum Begriff: Diversität kann durch unterschiedliche physikalische Methoden oder unterschiedliche Lösungen für dieselbe Aufgabenstellung erreicht werden.

[QUELLE: IEC 61508-4:2010, 3.3.7]

3.1.14

Fehler

(en: error)

Unterschied zwischen einem berechneten, beobachteten bzw. gemessenen Wert oder Zustand und dem wahren, spezifizierten bzw. theoretisch korrekten Wert oder Zustand

Anmerkung 1 zum Begriff: Fehler können auf einem Entwurfsirrtum bei Hardware/Software beruhen und/oder auf verfälschten Informationen durch elektromagnetische Einflüsse und/oder anderen Effekten.

Anmerkung 2 zum Begriff: Fehler führen nicht notwendigerweise zu einem *Ausfall* oder einem *Fehlzustand*.

[QUELLE: IEC 61508-4:2010, 3.6.11, modifiziert – Anmerkungen hinzugefügt]

⁵⁾ Zahlen in rechteckigen Klammern beziehen sich auf die Literaturhinweise.

3.1.15

expliziter Code

(en: **explicit code**)

Sicherheits-Code, der in der SPDU tatsächlich transportiert wird, und sowohl Sender als auch Empfänger bekannt ist

3.1.16

Ausfall

(en: **failure**)

Beendigung der Fähigkeit einer Funktionseinheit, eine geforderte Funktion auszuführen, oder der Betrieb einer Funktionseinheit anders als gefordert

Anmerkung 1 zum Begriff: Ein Ausfall kann auf einen *Fehler* zurückzuführen sein (z. B. ein Problem des Hardware/Softwareentwurfs oder eine Nachrichtenstörung).

[QUELLE: IEC 61508-4:2010, 3.6.4, modifiziert – Anmerkungen und Bilder entfernt]

3.1.17

Fehlzustand

(en: **fault**)

nicht normale Bedingung, die eine Verringerung oder den Verlust der Fähigkeit einer Funktionseinheit auslösen kann, eine geforderte Funktion auszuführen

Anmerkung 1 zum Begriff: IEC 60050-191:1990, 191-05-01 definiert „fault“ als einen Zustand, der durch das Unvermögen gekennzeichnet ist, eine geforderte Funktion auszuführen, jedoch nicht ein Unvermögen während vorbeugender Instandhaltung, anderer geplanter Aktionen oder auf Grund fehlender externer Betriebsmittel.

[QUELLE: IEC 61508-4:2010, 3.6.1, modifiziert – Referenz auf Bild entfernt]

3.1.18

Feldbus

(en: **fieldbus**)

Kommunikationssystem basierend auf serieller Datenübertragung und eingesetzt in der industriellen Automatisierung oder in Prozessleitsystemen

3.1.19

Feldbussystem

(en: **fieldbus system**)

System mit einem *Feldbus* und angeschlossenen Geräten

3.1.20

DLPDU

DEPRECATED: frame

Data Link Protocol Data Unit

3.1.21

Blockprüfzeichenfolge

(en: **Frame Check Sequence**)

FCS

redundante Daten, mittels Hash-Funktion aus einem Block von Daten in einer DLPDU (Telegrammrahmen) abgeleitet und mit diesen zusammen zur Aufdeckung von Datenverfälschungen gespeichert oder übertragen

Anmerkung 1 zum Begriff: Eine FCS kann z. B. mittels einer CRC oder einer anderen Hash-Funktion abgeleitet werden.

Anmerkung 2 zum Begriff: Siehe auch [28], [29].

Anmerkung 3 zum Begriff: Diese Anmerkung ist nur für die französischsprachige Fassung relevant.

3.1.22

Hash-Funktion

(en: hash function)

(mathematische) Funktion, die Werte aus einem (möglicherweise sehr) großen Wertebereich in einen (üblicherweise) kleineren Wertebereich abbildet

Anmerkung 1 zum Begriff: Hash-Funktionen können zur Aufdeckung von Datenverfälschung eingesetzt werden.

Anmerkung 2 zum Begriff: Gebräuchliche Hash-Funktionen schließen Parity-Bit, Quersummen oder CRC mit ein.

[QUELLE: IEC/TR 62210:2003, 4.1.12, modifiziert – „üblicherweise“ und Anmerkungen hinzugefügt]

3.1.23

Gefährdung

(en: hazard)

Zustand oder Umstände in einem System, der/die zusammen mit weiteren Bedingungen zwangsläufig zu einem Schaden an Personen, Eigentum oder der Umwelt führt/führen

3.1.24

Impliziter Code

(en: implicit code)

Sicherheits-Code, der nicht in der SPDU transportiert wird, aber sowohl Sender als auch Empfänger bekannt ist

3.1.25

Master

aktive Kommunikationseinheit, die Kommunikationsaktivitäten anderer Stationen, seien es Master oder Slaves, einrichten und festlegen kann

3.1.26

Nachricht

(en: message)

geordnete Folge von Octets, bestimmt für die Übermittlung von Information

[QUELLE: ISO/IEC 2382-16:1996, 16.02.01, modifiziert – Zeichen durch Octet ersetzt]

3.1.27

Nachrichtensenke

(en: message sink)

Teil eines Kommunikationssystems, der für den Empfang von Nachrichten gedacht ist

[QUELLE: ISO/IEC 2382-16:1996, 16.02.03]

3.1.28

Nachrichtenquelle

(en: message source)

Teil eines Kommunikationssystems, der für den Versand von Nachrichten gedacht ist

[QUELLE: ISO/IEC 2382-16:1996, 16.02.02]

3.1.29

Fehlauslösung

(en: nuisance trip)

unberechtigte Auslösung ohne schädliche Wirkung

Anmerkung 1 zum Begriff: Interne außergewöhnliche Fehler können z. B. in Kommunikationssystemen wie Funkübertragung durch zu viele Wiederholungen unter Störeinfluss auftreten.

3.1.30

Performance Level

PL

diskrete Stufen zur Bestimmung der Fähigkeit eines sicherheitsbezogenen Teils eines Steuerungssystems, um eine Sicherheitsfunktion unter vorhersehbaren Bedingungen auszuführen

[QUELLE: ISO 13849-1:2015, 3.1.23]

3.1.31

Schutzkleinspannung

(en: protective extra-low-voltage)

PELV

Stromkreis, in dem unter Normalbedingungen oder unter den Bedingungen eines Einzelfehlers die Spannung AC 30 V, 42,4 V Scheitelwert oder DC 60 V nicht überschritten wird, ausgenommen durch Erdungsfehler in anderen Stromkreisen

Anmerkung 1 zum Begriff: Ein PELV-Stromkreis enthält eine Verbindung zur Schutzterde, verbunden ist. Ohne Verbindung zur Schutzterde oder bei fehlerhafter Verbindung zur Schutzterde werden die Spannungen des Stromkreises nicht kontrolliert.

[QUELLE: IEC 61010-2-201:2013: 3.109, modifiziert – Entfernung des Begriffs „Circuit“ aus dem Term, und Entfernung der zweiten Anmerkung]

3.1.32

Redundanz

(en: redundancy)

Vorhandensein von mehr als einem Mittel, um eine geforderte Funktion auszuführen oder eine Information darzustellen

[QUELLE: IEC 61508-4:2010, 3.4.6 modifiziert – Beispiel und Anmerkungen entfernt]

3.1.33

relativer Zeitstempel

(en: relative time stamp)

Zeitstempel, der sich auf die lokale Zeit einer Einheit bezieht

Anmerkung 1 zum Begriff: Im Allgemeinen gibt es keine Beziehungen zu den Zeitgebern in anderen Einheiten.

[QUELLE: IEC 62280:2014 3.1.43]

3.1.34

Zuverlässigkeit

(en: reliability)

Wahrscheinlichkeit, dass ein automatisiertes System eine geforderte Funktion unter bestimmten Voraussetzungen in einem bestimmten Zeitintervall (t_1 , t_2) ausführen kann

Anmerkung 1 zum Begriff: Es wird allgemein angenommen, dass das automatisierte System sich am Anfang des Zeitintervalls in einem Zustand befindet, um die geforderte Funktion ausführen zu können.

Anmerkung 2 zum Begriff: Der Begriff Zuverlässigkeit wird ebenfalls zur Kennzeichnung der Überlebenswahrscheinlichkeit (reliability performance) genutzt und durch die Wahrscheinlichkeit bemessen.

Anmerkung 3 zum Begriff: Innerhalb der MTBF- oder MTTF-Zeitspanne nimmt die Wahrscheinlichkeit ab, dass ein automatisiertes System eine geforderte Funktion unter bestimmten Bedingungen ausführen kann.

Anmerkung 4 zum Begriff: Zuverlässigkeit unterscheidet sich von Verfügbarkeit.

[QUELLE: IEC/TR 62059-11:2002, 3.17, modifiziert – „automatisiertes System“ verwendet, zwei Anmerkungen hinzugefügt]

3.1.35

Restfehlerwahrscheinlichkeit (en: residual error probability) **RP**

Wahrscheinlichkeit eines Fehlers, dass er durch die Sicherheitsmaßnahmen im SCL nicht aufgedeckt wird

Anmerkung 1 zum Begriff: Diese Anmerkung ist nur für die französischsprachige Fassung relevant.

3.1.36

Restfehlerrate (en: residual error rate)

statistische Rate, mit der die Sicherheitsmaßnahmen im SCL Fehler nicht aufdecken

3.1.37

Risiko (en: risk)

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

Anmerkung 1 zum Begriff: Siehe IEC 61508-5:2010, Anhang A.

[QUELLE: IEC 61508-4:2010, 3.1.6 und ISO/IEC Guide 51:2014, Definition 3.9, modifiziert – andere Anmerkung]

3.1.38

Sicherheitskommunikationskanal (en: safety communication channel) **SC**

Kommunikationskanal beginnend auf dem SCL der *Nachrichtenquelle* und endend auf dem SCL der *Nachrichtensenke*

Anmerkung 1 zum Begriff: Er kann als zwei SCLs modelliert werden, die über einen „Black Channel“, ein *festgelegtes Kommunikationssystem* oder einen *festgelegten Kanal* verbunden sind.

3.1.39

Sicherheitskommunikationsschicht (en: safety communication layer) **SCL**

Kommunikationsschicht über dem FAL, die die notwendigen zusätzlichen Mittel beinhaltet, um die sichere Übertragung von Daten entsprechend den Anforderungen der IEC 61508 zu gewährleisten

Anmerkung 1 zum Begriff: Diese Anmerkung ist nur für die französischsprachige Fassung relevant.

3.1.40

sichere Verbindung (en: safety connection)

Verbindung, welche das Sicherheitsprotokoll für Kommunikationstätigkeiten nutzt

3.1.41

Sicherheitsdaten (en: safety data)

Daten, die in einem Sicherheitsnetzwerk unter Nutzung eines Sicherheitsprotokolls übertragen wurden

Anmerkung 1 zum Begriff: Die Sicherheitskommunikationsschicht garantiert nicht sichere Daten an sich, sondern nur den gesicherten Transport.

3.1.42

Sicherheitsgerät (en: safety device)

Gerät, welches nach IEC 61508 ausgeführt wurde und das funktional sichere Kommunikationsprofil zur Anwendung bringt