

	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 Industrielle Kommunikationsnetze – Profile – Teil 3: Funktional sichere Übertragung bei Feldbussen – Allgemeine Regeln und Profilfestlegungen (IEC 61784-3:2007); Deutsche Fassung EN 61784-3:2008 Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions (IEC 61784-3:2007); German version EN 61784-3:2008 Réseaux de communication industriels – Profils – Partie 3: Bus de terrain de sécurité fonctionnelle – Règles générales et définitions des profils (CEI 61784-3:2007); Version allemande EN 61784-3:2008 Gesamtumfang 58 Seiten DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE		

Beginn der Gültigkeit

Die von CENELEC am 2008-05-01 angenommene EN 61784-3 gilt als DIN-Norm ab 2008-11-01.

Nationales Vorwort

Vorausgegangener Norm-Entwurf: E DIN IEC 61784-3 (VDE 0803-500):2005-07.

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

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

Die DIN EN 61784-3 (VDE 0803-500-3) erläutert die Grundsätze für funktional sichere Kommunikation, bezogen auf die Normen der Reihe DIN EN 61508 (VDE 0803). Für sie ist eine deutsche Sprachfassung verfügbar.

Die Normen der Reihe DIN EN 61784-3 legen mehrere Sicherheitskommunikationsschichten (Profile und entsprechende Protokolle) basierend auf den Kommunikationsprofilen und Protokollschichten der IEC 61784-1, IEC 61784-2 und der Reihe IEC 61158 fest. Für diese Kommunikationsnormen ist keine deutsche Sprachfassung verfügbar. Sie alleine sind nicht ausreichend zur Auslegung eines sicherheitsbezogenen Systems nach DIN EN 61508 (VDE 0803), stets ist die Beachtung der letztgenannten Normenreihe und der DIN EN 61784-3 erforderlich.

Die Kommunikationsnormen der Reihe DIN EN 61784-3 weisen alle die gleiche Gliederung auf, sie ist in der DIN EN 61784-3 (VDE 0803-500), [Anhang C](#) in deutscher und englischer Sprache wiedergegeben, so dass ein Bezug zwischen der deutschsprachigen DIN EN 61784-3 (VDE 0803-500) und den englischsprachigen DIN EN 61784-3-x jederzeit möglich ist. Darüber hinaus sind in ersterer alle Begriffe und Abkürzungen jeweils in Deutsch und in Englisch wiedergegeben.

Das IEC-Komitee hat entschieden, dass der Inhalt dieser Publikation bis zu dem Datum (maintenance result 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.

Nationaler Anhang NA (informativ)

Zusammenhang mit Europäischen und Internationalen Normen

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

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

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

Tabelle NA.1

Europäische Norm	Internationale Norm	Deutsche Norm	Klassifikation im VDE-Vorschriftenwerk
EN 61131-2	IEC 61131-2	DIN EN 61131-2 (VDE 0411-500)	VDE 0411-500
Normen der Reihe EN 61158	Normen der Reihe IEC 61158	Normen der Reihe DIN EN 61158	–
EN 61326-3-1	IEC 61326-3-1	DIN EN 61326-3-1 (VDE 0843-20-3-1)	VDE 0843-20-3-1
EN 61326-3-2	IEC 61326-3-2	DIN EN 61326-3-2 (VDE 0843-20-3-2)	VDE 0843-20-3-2
Normen der Reihe EN 61508	Normen der Reihe IEC 61508	Normen der Reihe DIN EN 61508 (VDE 0803)	Normen der Reihe VDE 0803
EN 61508-1	IEC 61508-1	DIN EN 61508-1 (VDE 0803-1)	VDE 0803-1
EN 61508-2	IEC 61508-2	DIN EN 61508-2 (VDE 0803-2)	VDE 0803-2
EN 61508-4	IEC 61508-4	DIN EN 61508-4 (VDE 0803-4)	VDE 0803-4
EN 61508-6	IEC 61508-6	DIN EN 61508-6 (VDE 0803-6)	VDE 0803-6
Normen der Reihe EN 61511	Normen der Reihe IEC 61511	Normen der Reihe DIN EN 61511 (VDE 0810-1)	Normen der Reihe VDE 0810-1
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	–
Normen der Reihe EN 61784-5	Normen der Reihe IEC 61784-5	Normen der Reihe DIN EN 61784-5 (VDE 0800-500)	Normen der Reihe VDE 0800-500
EN 61918	IEC 61918	DIN EN 61918 (VDE 0800-500)	VDE 0800-500
EN 50159-1:2001	–	DIN EN 50159-1 (VDE 0831-159-1):2001-11	VDE 0831-159-1

Nationaler Anhang NB (informativ)

Literaturhinweise

DIN EN 61131-2 (VDE 0411-500), *Speicherprogrammierbare Steuerungen – Teil 2: Betriebsmittelanforderungen und Prüfungen*

Normen der Reihe

DIN EN 61158, *Digitale Datenkommunikation in der Leittechnik – Feldbus für industrielle Leitsysteme*

IEC 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*

IEC 61326-3-2 (VDE 0843-20-3-2), *Elektrische Mess-, Steuer-, Regel- und Laborgeräte – EMV-Anforderungen – Teil 3-2: Störfestigkeitsanforderungen für Geräte, die sicherheitsbezogene Funktionen ausführen oder für sicherheitsbezogene Funktionen eingesetzt werden (Funktionale Sicherheit) – Anwendungen in Industriebereichen mit besonderer elektromagnetischer Umgebung*

Normen der Reihe

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

DIN EN 61508-1 (VDE 0803-1), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 1: Allgemeine Anforderungen*

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

DIN EN 61508-6 (VDE 0803-6), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 6: Anwendungsrichtlinie für IEC 61508-2 und IEC 61508-3*

Normen der Reihe

DIN EN 61511 (VDE 0810-1), *Funktionale Sicherheit - Sicherheitstechnische Systeme für die Prozessindustrie*

DIN EN 61784-1, *Industrielle Kommunikationsnetze – Profile – Teil 1: Feldbusprofile*

DIN EN 61784-2, *Industrielle Kommunikationsnetze – Profile – Teil 2: Zusätzliche Feldbusprofile für Echtzeitnetzwerke basierend auf ISO/IEC 8802-3*

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*

Normen der Reihe

DIN EN 61784-5 (VDE 0800-500), *Digitale Datenkommunikation in der Leittechnik – Teil 5: Installationsprofile für Kommunikationsnetzwerke in industriellen Leitsystemen*

DIN EN 61918 (VDE 0800-500), *Industrielle Kommunikationsnetze – Installation von Kommunikationsnetzen in Industrieanlagen*

DIN EN 50159-1 (VDE 0831-159-1), *Bahnanwendungen – Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme – Teil 1: Sicherheitsrelevante Kommunikation in geschlossenen Übertragungssystemen; Deutsche Fassung EN 50159-1:2001*

– Leerseite –

Industrielle Kommunikationsnetze –
Profile –
Teil 3: Funktional sichere Übertragung bei Feldbussen – Allgemeine Regeln
und Profilfestlegungen
(IEC 61784-3:2007)

Industrial communication networks –
Profiles –
Part 3: Functional safety fieldbuses – General
rules and profile definitions
(IEC 61784-3:2007)

Réseaux de communication industriels –
Profils –
Partie 3: Bus de terrain de sécurité fonctionnelle
– Règles générales et définitions des profils
(CEI 61784-3:2007)

Diese Europäische Norm wurde von CENELEC am 2008-05-01 angenommen. Die 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 Zentralsekretariat 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 Zentralsekretariat mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

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

CENELEC

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

Zentralsekretariat: rue de Stassart 35, B-1050 Brüssel

© 2008 CENELEC – Alle Rechte der Verwertung, gleich in welcher Form und in welchem Verfahren, sind weltweit den Mitgliedern von CENELEC vorbehalten.

Ref. Nr. EN 61784-3:2008 D

Vorwort

Der Text des Schriftstücks 65C/470/FDIS, zukünftige 1. Ausgabe von IEC 61784-3, ausgearbeitet von dem SC 65C „Industrial networks“ des IEC TC 65 „Industrial-process measurement, control and automation“, wurde der IEC-CENELEC Parallelen Abstimmung unterworfen und von CENELEC am 2008-05-01 als EN 61784-3 angenommen.

Nachstehende Daten wurden festgelegt:

- spätestes Datum, zu dem die EN auf nationaler Ebene durch Veröffentlichung einer identischen nationalen Norm oder durch Anerkennung übernommen werden muss (dop): 2009-02-01
- spätestes Datum, zu dem nationale Normen, die der EN entgegenstehen, zurückgezogen werden müssen (dow): 2011-05-01

Die Internationale Elektrotechnische Kommission (IEC) und CENELEC weisen darauf hin, dass die Übereinstimmung mit dieser Norm die Verwendung von Patenten hinsichtlich der in EN 61784-3-1, EN 61784-3-2, EN 61784-3-3 und EN 61784-3-6 angegebenen Kommunikationsprofile für funktional sichere Übertragung für die Kommunikationsprofilfamilien 1, 2, 3 und 6 bedeuten kann.

Die IEC und CENELEC nehmen keine Stellung zur Rechtmäßigkeit, zur Gültigkeit und zum Anwendungsbereich dieser Patentrechte.

Die Halter dieser Patentrechte haben IEC zugesichert, dass sie bereit sind, über Lizenzen zu vernünftigen und nicht diskriminierenden Geschäftsbedingungen mit Antragstellern in der ganzen Welt zu verhandeln. In diesem Zusammenhang sind die Erklärungen der Halter dieser Patentrechte bei IEC registriert.

ANMERKUNG Detaillierte Angaben bezüglich dieser Patente und Kontaktinformationen sind in EN 61784-3-1, EN 61784-3-2, EN 61784-3-3 und EN 61784-3-6 erhalten.

Der Anhang ZA wurde von CENELEC hinzugefügt.

Anerkennungsnotiz

Der Text der Internationalen Norm IEC 61784-3:2007 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 60204-1:2006 (nicht modifiziert).
IEC 61496	ANMERKUNG	Harmonisiert als EN 61496-1:2004 (modifiziert) und als CLC/TS 61496-2:2006 (nicht modifiziert) und CLC/TC 61496-3:2008 (nicht modifiziert)
IEC 61508-4	ANMERKUNG	Harmonisiert als EN 61508-4:2001 (nicht modifiziert).
IEC 61508-6	ANMERKUNG	Harmonisiert als EN 61508-6:2001 (nicht modifiziert).
IEC 61511	ANMERKUNG	Harmonisiert in der Reihe EN 61511 (nicht modifiziert).
IEC 61800-5-2	ANMERKUNG	Harmonisiert als EN 61800-5-2:2007 (nicht modifiziert).
IEC 62061	ANMERKUNG	Harmonisiert als EN 62061:2005 (nicht modifiziert).
ISO 12100-1	ANMERKUNG	Harmonisiert als EN ISO 12100-1:2003 (nicht modifiziert).
ISO 13849-1	ANMERKUNG	Harmonisiert als EN ISO 13849-1:2006 (nicht modifiziert).
ISO 13849-2	ANMERKUNG	Harmonisiert als EN ISO 13849-2:2003 (nicht modifiziert).

Inhalt

	Seite
Vorwort	2
Einleitung.....	6
1 Anwendungsbereich	9
2 Normative Verweisungen.....	9
3 Begriffe, Symbole, Abkürzungen und Konventionen	10
3.1 Begriffe.....	10
3.1.1 Allgemeine Begriffe.....	10
3.1.2 CPF 1: Zusätzliche Begriffe und Definitionen	16
3.1.3 CPF 2: Zusätzliche Begriffe und Definitionen	16
3.1.4 CPF 3: Zusätzliche Begriffe und Definitionen	16
3.1.5 CPF 6: Zusätzliche Begriffe und Definitionen	16
3.2 Symbole und Abkürzungen.....	16
3.2.1 Allgemeine Symbole und Abkürzungen.....	16
3.2.2 CPF 1: Zusätzliche Symbole und Abkürzungen	17
3.2.3 CPF 2: Zusätzliche Symbole und Abkürzungen	17
3.2.4 CPF 3: Zusätzliche Symbole und Abkürzungen	17
3.2.5 CPF 6: Zusätzliche Symbole und abgekürzte Begriffe	17
4 Konformität.....	17
5 Grundlagen von sicherheitsbezogenen Feldbussystemen.....	18
5.1 Struktur einer Sicherheitsfunktion	18
5.2 Kommunikationssystem	18
5.2.1 Allgemein	18
5.2.2 Feldbusse der IEC 61158	19
5.2.3 Kommunikationskanaltypen	19
5.2.4 Reaktionszeit einer Sicherheitsfunktion.....	19
5.3 Kommunikationsfehler	20
5.3.1 Allgemein	20
5.3.2 Verfälschung	20
5.3.3 Unbeabsichtigte Wiederholung.....	20
5.3.4 Falsche Abfolge	21
5.3.5 Verlust.....	21
5.3.6 Inakzeptable Verzögerung.....	21
5.3.7 Einfügung.....	21
5.3.8 Maskerade	22
5.3.9 Adressierung.....	22
5.4 Deterministische Abhilfemaßnahmen	22
5.4.1 Allgemein	22
5.4.2 Laufende Nummer	22

	Seite
5.4.3 Zeitstempel.....	22
5.4.4 Zeiterwartung	22
5.4.5 Verbindungsauthentizität.....	23
5.4.6 Rückmeldung	23
5.4.7 Datensicherung	23
5.4.8 Redundanz mit Kreuzvergleich	23
5.4.9 Unterschiedliche Sicherungssysteme für die Datenintegrität	23
5.5 Beziehungen zwischen Fehlern und Sicherheitsmaßnahmen	24
5.6 Betrachtungen zur Datenintegrität	25
5.6.1 Berechnung der Restfehlerrate	25
5.6.2 Restfehlerrate und SIL	27
5.7 Beziehungen zwischen funktionaler Sicherheit und Datensicherheit	27
5.8 Randbedingungen und Auflagen.....	28
5.8.1 Elektrische Sicherheit.....	28
5.8.2 Elektromagnetische Verträglichkeit (EMV)	28
5.9 Installationsleitfäden.....	28
5.10 Sicherheitshandbuch.....	28
5.11 Sicherheitsgrundsätze (Policy).....	28
6 CPF 1 (FOUNDATION™ Fieldbus) – Profil für funktionale Sicherheit.....	29
6.1 FSCP 1/1 (FF-SIS™)	29
6.2 Technischer Überblick.....	29
7 CPF 2 (CIP™) – Profile für funktionale Sicherheit.....	30
7.1 FSCP 2/1 (CIP Safety™)	30
7.2 Technischer Überblick.....	30
8 CPF 3 (PROFIBUS™, PROFINET™) – Profil für funktionale Sicherheit.....	32
8.1 FSCP 3/1 (PROFIsafe™).....	32
8.2 Technischer Überblick.....	32
9 CPF 6 (INTERBUS®) – Profil für funktionale Sicherheit.....	34
9.1 FSCP 6/7 (INTERBUS Safety™)	34
9.2 Technischer Überblick.....	35
Anhang A (informativ) Beispiele für funktional sichere Kommunikationsmodelle	37
A.1 Allgemeines	37
A.2 Modell A	37
A.3 Modell B	37
A.4 Modell C	38
A.5 Modell D	38
Anhang B (informativ) Ein Kanalmodell für sichere Kommunikation unter Einsatz von CRC- basierten Fehlerprüfungen	40
B.1 Übersicht	40

	Seite
B.2 Kanalmodell für Berechnungen	40
B.3 CRC-Prüfung	41
B.3.1 Allgemeines	41
B.3.2 Betrachtung der CRC-Polynome	43
Anhang C (informativ) Struktur der technologiespezifischen Teile	45
Literaturhinweise	48
Anhang ZA (normativ) Normative Verweisungen auf internationale Publikationen mit ihren entsprechenden europäischen Publikationen.....	51
<u>Tabellen</u>	
Tabelle 1 – Überblick über die Wirksamkeit von Maßnahmen gegen mögliche Fehler.....	25
Tabelle 2– Definition der Größen für die Berechnung der Restfehlerrate	26
Tabelle 3 – Beziehungen zwischen Restfehlerrate und SIL	27
Tabelle 4 – Übersicht über Profilkennungen für FSCP 6/7	35
Tabelle B.1 – Beispiel für die Abhängigkeit von d_{min} und Blocklänge n.....	43
Tabelle C.1 – Gemeinsame Gliederung der technologiespezifischen Teile	45
<u>Bilder</u>	
Bild 1 – Beziehungen der IEC 61784-3 mit anderen Normen (Fertigung)	6
Bild 2 – Beziehungen der IEC 61784-3 mit anderen Normen (Prozess)	7
Bild 3 – Sichere Kommunikation als Teil einer Sicherheitsfunktion	18
Bild 4 – Modellbeispiel für ein funktional sicheres Kommunikationssystem	19
Bild 5 – Beispiel für die Reaktionszeitkette einer Sicherheitsfunktion	20
Bild 6 – Anwendungsbeispiel	27
Bild 7 – Geltungsbereich des FSCP 1/1	30
Bild 8 – Beziehungen der Sicherheitsprüfer (Safety-Validator)	31
Bild 9 – Grundlegende Kommunikationsvoraussetzungen für FSCP 3/1	33
Bild 10 – Zusammensetzung einer FSCP 3/1-Sicherheits-PDU	33
Bild 11 – Betriebsarten der sicheren Kommunikation.....	34
Bild 12 – Kommunikationsvoraussetzungen für FSCP 6/7	35
Bild A.1 – Modell A.....	37
Bild A.2 – Modell B.....	38
Bild A.3 – Modell C.....	38
Bild A.4 – Modell D.....	39
Bild B.1 – Kommunikationskanal mit Störungen	40
Bild B.2 – Binärsymmetrischer Kanal (BSC).....	41
Bild B.3 – Beispiel eines Blocks mit Nachricht und CRC-Bits (redundanter Code)	42
Bild B.4 – Blockcodes zur Fehleraufdeckung	42
Bild B.5 – Propere und nicht propere CRC-Polynome.....	43

Einleitung

Die Reihe der 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. Zahlreiche Feldbuserweiterungen treten daher in Erscheinung, die auf bisher noch nicht genormte Bereiche wie Echtzeit, funktionale Sicherheit und Informationssicherheit abzielen.

Diese Norm erläutert die relevanten Prinzipien für funktional sichere Kommunikation bezogen auf die 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 IEC 61158-Reihe. 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.

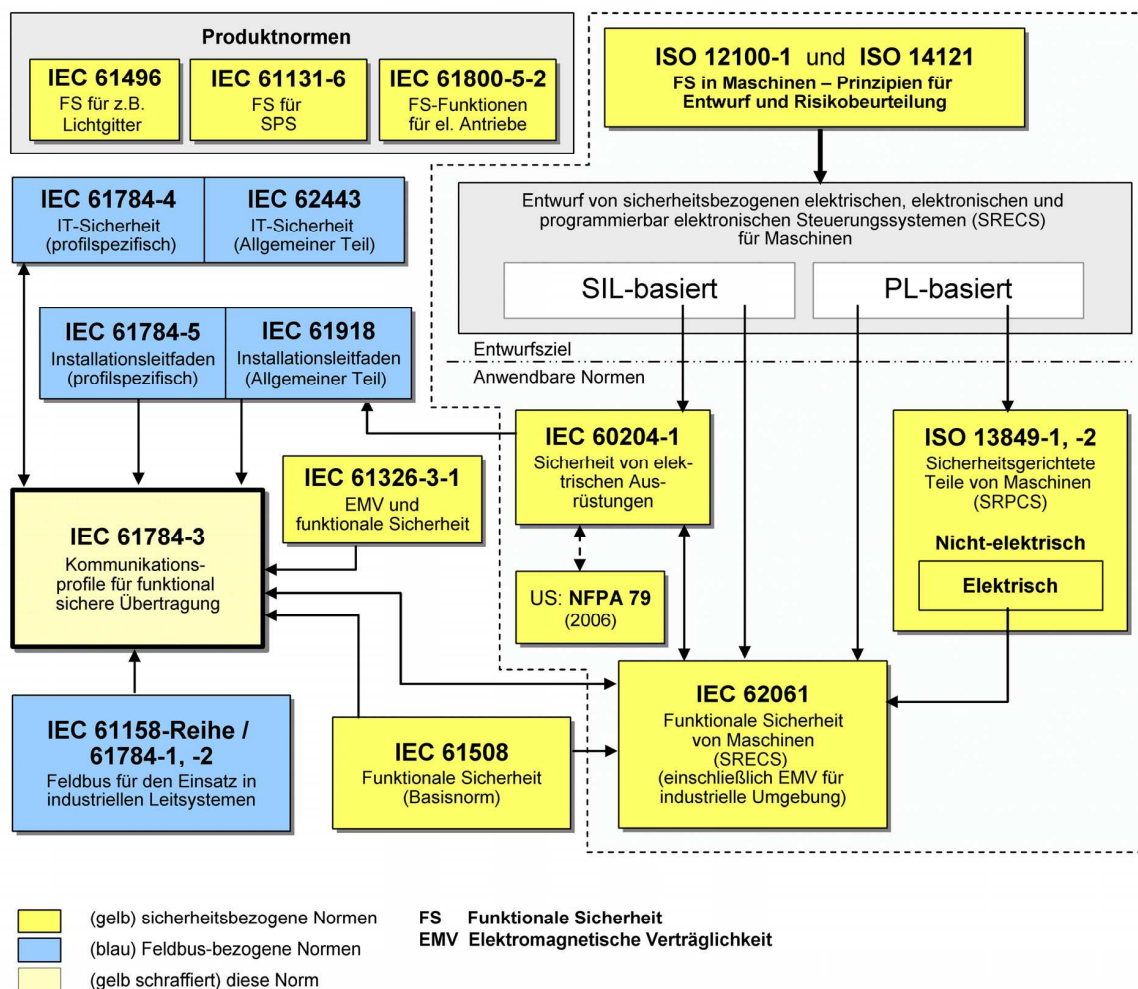
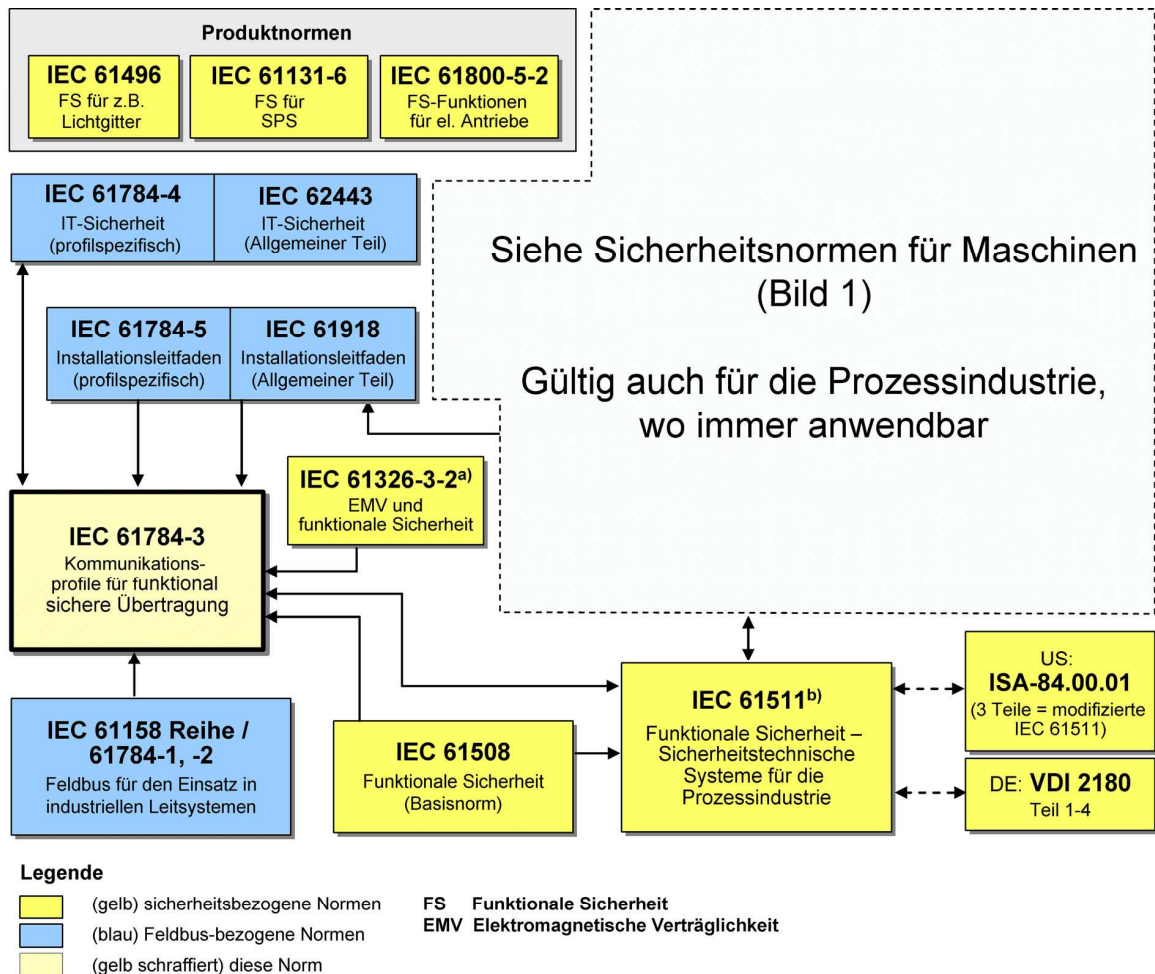


Bild 1 – Beziehungen der IEC 61784-3 zu anderen Normen (Fertigung)

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



- a Für bestimmte elektromagnetische Umgebungen; sonst IEC 61326-3-1.
- b EN ratifiziert.

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

Die als Bestandteile eines sicherheitsgerichteten Systems nach IEC 61508 implementierten Sicherheitskommunikationsschichten gewährleisten das notwendige Vertrauen in den Transport von Nachrichten (Informationen) zwischen zwei oder mehr Feldbusteilnehmern in einem sicherheitsgerichteten 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 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 IEC 61508 für die funktional sichere Kommunikation, einschließlich möglicher Übertragungsfehler, deren Abhilfemaßnahmen und Betrachtungen zur Datenintegrität;
- individuelle Beschreibung der Kommunikationsprofile für funktional sichere Übertragung für mehrere Kommunikationsprofilfamilien der IEC 61784-1 und IEC 61784-2;
- Ergänzung der Kommunikationsdienst- und -protokollabschnitte der IEC 61158-Reihe um eine Sicherheitsschicht.

1 Anwendungsbereich

Dieser Teil der Reihe IEC 61784-3 erläutert einige allgemeine Prinzipien, die bei der Übertragung von sicherheitsrelevanten Nachrichten zwischen Teilnehmern eines verteilten Netzwerks mit Feldbustechnologie zum Einsatz kommen können und die den Anforderungen der Reihe IEC 61508 entsprechen. Diese Prinzipien können in zahlreichen industriellen Anwendungen wie Prozess- oder Fertigungsautomatisierung und Maschinenanlagen genutzt werden.

Dieser Normteil¹⁾ und die IEC 61784-3-x-Normteile spezifizieren mehrere Kommunikationsprofile für funktional sichere Übertragung basierend auf den Kommunikationsprofilen und Protokollschichten der Feldbustechnologien in der IEC 61784-1, IEC 61784-2 und der Reihe IEC 61158.

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

ANMERKUNG 2 Aspekte der elektrischen Sicherheit und Eigensicherheit werden nicht abgedeckt. 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 sicherheitsrelevanten Anwendung einzuplanen, um Feldbussysteme gegen unautorisierte Zugriffe zu schützen. Die IEC 62443 wird viele diesbezügliche Punkte betrachten; die Beziehung zur IEC 62443 ist in einem eigenen Unterabschnitt in diesem Normteil weiter ausgeführt.

ANMERKUNG 3 In einer künftigen IEC 61784-4 können zusätzlich profilspezifische Anforderungen an die IT-Sicherheit 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 der Reihe IEC 61508 zu qualifizieren.

ANMERKUNG 5 Der resultierende SIL-Anspruch eines Systems hängt vom gewählten Kommunikationsprofil für funktional sichere Übertragung innerhalb dieses Systems ab.

2 Normative Verweisungen

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

IEC 61131-2, *Programmable controllers – Part 2: Equipment requirements and tests*

IEC 61158 (all parts), *Industrial communication networks – Fieldbus specifications*

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 (all parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

¹⁾ Auf den nachfolgenden Seiten dieser Norm bedeutet „dieser Normteil“ stets „dieser Teil der Reihe IEC 61784-3“.

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

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

IEC 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 61784-5 (all parts), *Industrial communication networks – Profiles – Part 5: Installation of fieldbuses – Installation profiles for CPF x*

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

IEC 62280-1:2002, *Railway applications – Communication, signalling and processing systems – Part 1: Safety-related communication in closed transmission systems*

3 Begriffe, Symbole, Abkürzungen und Konventionen

3.1 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

3.1.1 Allgemeine Begriffe

3.1.1.1

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

[IEC 62280-2, modifiziert]

3.1.1.2

Verfügbarkeit (en: availability)

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

ANMERKUNG Verfügbarkeit hängt ab von der MTBF (mean time between failure) und MDT (mean down time):

Verfügbarkeit = $MTBF / (MTBF + MDT)$.

3.1.1.3

Black Channel

Kommunikationskanal ohne verfügbaren Nachweis des Entwurfs oder der Validierung nach der Reihe IEC 61508

3.1.1.4

Bridge

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

3.1.1.5

Kommunikationskanal (en: communication channel)

logische Verbindung zwischen zwei Endpunkten in einem *Kommunikationssystem*

3.1.1.6

Kommunikationssystem (en: communication system)

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

3.1.1.7

Verbindung (en: connection)

logische Bindung zwischen zwei Anwendungsobjekten in demselben oder unterschiedlichen Geräten

3.1.1.8

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 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 Siehe auch [26], [27]²⁾.

3.1.1.9

Diversität (en: diversity)

ungleichartige Mittel zur Ausführung einer geforderten Funktion

BEISPIEL Diversität kann durch unterschiedliche physikalische Methoden oder unterschiedliche Lösungen für dieselbe Aufgabenstellung erreicht werden.

[IEC 61508-4:1998]

3.1.1.10

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 Ein Fehler kann durch eine schadhafte betrachtete Einheit verursacht werden, z. B. ein Berechnungsfehler durch ein schadhaftes Rechnerbauelement.

[IEV 191-05-24], [IEC 61508-4:1998], [IEC 61158]

ANMERKUNG 2 Fehler können auf einem Entwurfsirrtum bei Hardware/Software beruhen und/oder auf verfälschten Informationen durch elektromagnetische Einflüsse und/oder durch andere Effekte.

ANMERKUNG 3 Fehler führen nicht notwendigerweise zu einem *Ausfall* oder einem *Fehlzustand*.

²⁾ Zahlen in rechteckigen Klammern beziehen sich auf die Literaturhinweise.

3.1.1.11

Ausfall (en: failure)

Beendigung der Fähigkeit einer Funktionseinheit, eine geforderte Funktion auszuführen

ANMERKUNG 1 Die Definition IEC 191-04-01 ist die gleiche, jedoch mit zusätzlichen Anmerkungen.

[IEC 61508-4:1998], [ISO/IEC 2382-14.01.11]

ANMERKUNG 2 Ein Ausfall kann auf einen *Fehler* zurückzuführen sein (zum Beispiel ein Problem des Hardware/Softwareentwurfs oder eine Nachrichtenstörung)

3.1.1.12

Fehlzustand (en: fault)

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

ANMERKUNG IEC 191-05-01 definiert „fault“ als ein 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.

[IEC 61508-4:1998], [ISO/IEC 2382-14.01.10]

3.1.1.13

Feldbus (en: fieldbus)

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

3.1.1.14

Feldbussystem (en: fieldbus system)

System mit einem *Feldbus* und angeschlossenen Geräten

3.1.1.15

Telegrammrahmen (en: frame)

veraltetes Synonym für DLPDU

3.1.1.16

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 Eine FCS kann zum Beispiel mittels einer CRC oder einer anderen Hash-Funktion abgeleitet werden.

ANMERKUNG 2 Siehe auch [26], [27].

3.1.1.17

Hash-Funktion (en: hash function)

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

ANMERKUNG 1 Hash-Funktionen können zur Aufdeckung von Datenverfälschung eingesetzt werden.

ANMERKUNG 2 Gebräuchliche Hash-Funktionen sind Parity-Bit, Quersummen oder CRC.

[IEC 62210, modifiziert]

3.1.1.18

Gefährdung (en: hazard)

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