

	DIN IEC 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 Einsprüche bis 2009-09-30 Entwurf Vorgesehen als Ersatz für DIN EN 61784-3 (VDE 0803-500):2008-11 Industrielle Kommunikationsnetze – Profile – Teil 3: Funktional sichere Übertragung bei Feldbussen (IEC 65C/500/CD:2008) Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses (IEC 65C/500/CD:2008) Anwendungswarnvermerk Dieser Norm-Entwurf mit Erscheinungsdatum 2009-07-20 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt. Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfes besonders zu vereinbaren. Stellungnahmen werden erbeten – vorzugsweise als Datei per E-Mail an dke@vde.com in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.dke.de/stellungnahme abgerufen werden – oder in Papierform an die DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE, Stresemannallee 15, 60596 Frankfurt am Main. Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevante Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen. Gesamtumfang 51 Seiten DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE		

Inhalt

	Seite
Einleitung	8
1 Anwendungsbereich	10
2 Normative Verweisungen	10
3 Begriffe, Symbole, Abkürzungen und Konventionen	11
3.1 Begriffe	11
3.2 Symbole und Abkürzungen	17
4 Konformität	19
5 Grundlagen von sicherheitsbezogenen Feldbussystemen	19
5.1 Struktur einer Sicherheitsfunktion	19
5.2 Kommunikationssystem	20
5.3 Kommunikationsfehler	22
5.4 Deterministische Abhilfemaßnahmen	24
5.5 Beziehungen zwischen Fehlern und Sicherheitsmaßnahmen	25
5.6 Betrachtungen zur Datenintegrität	26
5.7 Beziehungen zwischen funktionaler Sicherheit und Datensicherheit	28
5.8 Randbedingungen und Auflagen	29
5.9 Installationsleitfäden	29
5.10 Sicherheitshandbuch	29
5.11 Sicherheitsgrundsätze (Policy)	29
6 CPF 1 (FOUNDATION™ Fieldbus) – Profil für funktionale Sicherheit	30
6.1 FSCP 1/1 (FF-SIS™)	30
6.2 Technischer Überblick	30
7 CPF 2 (CIP™) – Profile für funktionale Sicherheit	31
7.1 FSCP 2/1 (CIP Safety™)	31
7.2 Technischer Überblick	31
8 CPF 3 (PROFIBUS™, PROFINET™) – Profil für funktionale Sicherheit	33
8.1 FSCP 3/1 (PROFIsafe™)	33
8.2 Technischer Überblick	33
9 CPF 6 (INTERBUS®) – Profil für funktionale Sicherheit	35
9.1 FSCP 6/7 (INTERBUS Safety™)	35
9.2 Technischer Überblick	36
10 CPF 8 (CC-Link™) – Profile für funktionale Sicherheit	37
10.1 FSCP 8/1 (CC-Link Safety™)	37
10.2 Technischer Überblick	37
11 CPF 12 (EtherCAT™) – Profile für funktionale Sicherheit	38
11.1 FSCP 12/1 (Safety-over-EtherCAT™)	38
11.2 Technischer Überblick	38
12 CPF 14 (EPA®) – Profile für funktionale Sicherheit	39

	Seite
12.1 FSCP 14/1 (EPASafety™)	39
12.2 Technischer Überblick	39
Anhang A (informativ) Beispiele für funktional sichere Kommunikationsmodelle	41
A.1 Allgemeines	41
A.2 Modell A	41
A.3 Modell B	41
A.4 Modell C	42
A.5 Modell D	42
Anhang B (informativ) Ein Kanalmodell für sichere Kommunikation unter Einsatz von CRC- basierten Fehlerprüfungen	44
B.1 Übersicht	44
B.2 Kanalmodell für Berechnungen	44
B.3 CRC-Prüfung	45
B.3.1 Allgemeines	45
B.3.2 Betrachtung der CRC-Polynome	47
Anhang C (informativ) Struktur der technologiespezifischen Teile	49
Bilder	
Bild 1 – Beziehungen der IEC 61784-3 mit anderen Normen (Fertigung)	8
Bild 2 – Beziehungen der IEC 61784-3 zu anderen Normen (Prozess)	9
Bild 3 – Sichere Kommunikation als Teil einer Sicherheitsfunktion	20
Bild 4 – Modellbeispiel für ein funktional sicheres Kommunikationssystem	21
Bild 5 – Beispiel für die Reaktionszeitkette einer Sicherheitsfunktion	22
Bild 6 – Anwendungsbeispiel	28
Bild 7 – Geltungsbereich des FSCP 1/1	31
Bild 8 – Beziehungen der Sicherheitsprüfer (Safety-Validator)	32
Bild 9 – Grundlegende Kommunikationsvoraussetzungen für FSCP 3/1	33
Bild 10 – Zusammensetzung einer FSCP 3/1-Sicherheits-PDU	34
Bild 11 – Betriebsarten der sicheren Kommunikation	35
Bild 12 – Kommunikationsvoraussetzungen für FSCP 6/7	36
Bild 13 – Basis-FSCP 12/1-System	39
Bild 14 – FSCP 14/1-Architektur der sicheren Kommunikation	40
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 Nachricht und CRC-Bits (redundanter Code)	46
Bild B.4 – Blockcodes zur Fehleraufdeckung	46
Bild B.5 – Propere und nicht propere CRC-Polynome	47

Tabellen

Tabelle 1 – Überblick über die Wirksamkeit von Maßnahmen gegen mögliche Fehler	26
Tabelle 2 – Definition der Größen für die Berechnung der Restfehlerrate.....	27
Tabelle 3 – Beziehungen zwischen Restfehlerrate und SIL.....	28
Tabelle 4 – Übersicht über Profilkennungen für FSCP 6/7	36
Tabelle B.1 – Beispiel für die Abhängigkeit von $d_{\min}$ und Blocklänge n	47
Tabelle C.1 – Gemeinsame Gliederung der technologiespezifischen Teile	49

Beginn der Gültigkeit

Diese Norm gilt ab ...

Nationales Vorwort

Das internationale Dokument IEC 65C/500/CD:2008 „Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses“ (CD, en: Committee Draft) ist unverändert in diesen Norm-Entwurf übernommen worden. Dieser Norm-Entwurf enthält eine autorisierte deutsche Übersetzung.

Das internationale Dokument wurde vom SC 65C „Industrial networks“ der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet und den nationalen Komitees zur Stellungnahme vorgelegt.

Die IEC und das Europäische Komitee für Elektrotechnische Normung (CENELEC) haben vereinbart, dass ein auf IEC-Ebene erarbeiteter Entwurf für eine Internationale Norm zeitgleich (parallel) bei IEC und CENELEC zur Umfrage (CDV-Stadium) und Abstimmung als FDIS (en: Final Draft International Standard) bzw. Schluss-Entwurf für eine Europäische Norm gestellt wird, um eine Beschleunigung und Straffung der Normungsarbeit zu erreichen. Dokumente, die bei CENELEC als Europäische Norm angenommen und ratifiziert werden, sind unverändert als Deutsche Normen zu übernehmen.

Da der Abstimmungszeitraum für einen FDIS bzw. Schluss-Entwurf prEN nur 2 Monate beträgt, und dann keine sachlichen Stellungnahmen mehr abgegeben werden können, sondern nur noch eine „JA/NEIN“-Entscheidung möglich ist, wobei eine „NEIN“-Entscheidung fundiert begründet werden muss, wird bereits der CD als DIN-Norm-Entwurf veröffentlicht, um die Stellungnahmen aus der Öffentlichkeit frühzeitig berücksichtigen zu können.

Für diesen Norm-Entwurf 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 DIN EN 61784-3 (VDE 0803-500-3):2008 erläutert die Grundsätze für funktional sichere Kommunikation, bezogen auf die Normen der Reihe DIN EN 61508 (VDE 0803).

Das internationale Schriftstück IEC 65C/500/CD:2008 enthält auch die Festlegungen für mehrere Sicherheitskommunikationsschichten (Profile und entsprechende Protokolle) basierend auf den Kommunikationsprofilen und Protokollschichten der IEC 61784-1, IEC 61784-2 und der Reihe IEC 61158. Sie sind in dem vorliegenden Norm-Entwurf nicht wiedergegeben.

Änderungen

Gegenüber DIN EN 61784-3 (VDE 0803-500):2008-11 wurden folgende Änderungen vorgenommen:

- a) Beschreibung zusätzlicher Profile aus den Kommunikationsprofilfamilien 8, 12, 13 und 14 nach DIN EN 61784-1 und DIN EN 61784-2 (CC-Link, EtherCAT, EPL und EPA);
- b) Forderungen nach Zertifizierung durch Empfehlungen für Konformitätsbewertungen gemäß den Regeln der für die Profile verantwortlichen Konsortien ersetzt;
- c) textliche Klarstellungen.

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 61131-2:2007	IEC 61131-2:2007	DIN EN 61131-2 (VDE 0411-500):2008-04	VDE 0411-500
Normen der Reihe EN 61158:2008	Normen der Reihe IEC 61158:2007	Normen der Reihe DIN EN 61158:2008-09	–
–	IEC 61326-3-1	–	–
–	IEC 65A/472/CD:2006	E DIN IEC 61326-3-2 (VDE 0843-20-32):2006-06	VDE 0843-20-32
–	Normen der Reihe IEC 61508	Normen der Reihe DIN EN 61508 (in Vorbereitung)	–
EN 61508-1:2001	IEC 61508-1:1998 + Corrigendum 1999	DIN EN 61508-1 (VDE 0803-1):2002-11	VDE 0803-1
–	IEC 65A/468A/CD:2005	E DIN IEC 61508-2 (VDE 0803-2):2006-07	VDE 0803-2
–	IEC 65C/430/CDV:2006	E DIN EN 61784-1:2006-11	–
–	IEC 65C/350/CD:2004	E DIN IEC 61784-2:2005-09	–
EN 61784-3-1:2008	IEC 61784-3-1:2007	DIN EN 61784-3-1:2008-11	–
EN 61784-3-2:2008	IEC 61784-3-2:2007	DIN EN 61784-3-2:2008-11	–
EN 61784-3-3:2008	IEC 61784-3-3:2007	DIN EN 61784-3-3:2008-11	–
EN 61784-3-6:2008	IEC 61784-3-6:2007	DIN EN 61784-3-6:2008-11	–
–	IEC 61784-3-8	–	–
–	IEC 61784-3-12	–	–
–	IEC 61784-3-14	–	–
Normen der Reihe EN 61784-5:2008	Normen der Reihe IEC 61784-5	Normen der Reihe DIN EN 61784-5 (VDE 0800-500):2009-01	Normen der Reihe VDE 0800-500
EN 61918:2008	IEC 61918:2007	DIN EN 61918 (VDE 0800-500):2009-01	VDE 0800-500
–	IEC 62280-1:2002	–	–

Nationaler Anhang NB (informativ)

Literaturhinweise

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

DIN EN 61158:2008-09 (alle Teile), *Industrielle Kommunikationsnetze – Feldbusse*

E DIN IEC 61326-3-2 (VDE 0843-20-32), *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*

DIN EN 61508 (alle Teile), *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*

E DIN IEC 61508-2 (VDE 0803-2), *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*

E DIN EN 61784-1, *Digitale Datenkommunikationen in der Leittechnik – Teil 1: Feldbus-Kommunikationsprofile für die prozess- und fertigungstechnische Automatisierung, Text in Englisch, nur auf CD-ROM*

E DIN IEC 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 – Feldbusse für funktionale Sicherheit – Teil 3-2: Allgemeine Regeln und Profilstellungen*

DIN EN 61784-3-3, *Industrielle Kommunikationsnetze – Profile – Feldbusse für funktionale Sicherheit – Teil 3-3: Allgemeine Regeln und Profilstellungen*

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

Reihe DIN EN 61784-5 (VDE 0800-500), *Industrielle Kommunikationsnetze – Profile*

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

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 mit 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 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 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.

INDUSTRIELLE KOMMUNIKATIONSNETZE – PROFILE

Teil 3: Funktional sichere Übertragung bei Feldbussen – Allgemeine Regeln und Profilstellungen

1 Anwendungsbereich

Dieser Teil der Normen 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 IEC 61508-Reihe 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 Feldbus-technologien in der IEC 61784-1, IEC 61784-2 und der IEC 61158-Reihe.

ANMERKUNG 1 Es kann andere sicherheitsrelevante 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 Lebenszyklusses unautorisierten Zugriffen ausgesetzt. Zusätzliche Maßnahmen sind daher in jeder sicherheitsrelevanten Anwendung einzuplanen, um Feldbus-systeme 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 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 der IEC 61508-Reihe 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 (alle Teile), *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 (alle Teile), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

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

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

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

IEC 61784-5 (alle Teile), *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 IEC 61508-Reihe

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 [28], [29]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 anderen Effekten.

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 [28], [29].

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

3.1.1.19

Master

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

3.1.1.20

Nachricht

en: message

geordnete Folge von Octets bestimmt für die Übermittlung von Information

[ISO/IEC 2382-16.02.01, modifiziert]

3.1.1.21

Nachrichtensenke

en: message sink

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

[ISO/IEC 2382-16.02.03]

3.1.1.22

Nachrichtenquelle

en: message source

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

[ISO/IEC 2382-16.02.02]

3.1.1.23

Fehlauslösung

en: nuisance trip

unberechtigte Auslösung ohne schädliche Wirkung

ANMERKUNG Interne außergewöhnliche Fehler können zum Beispiel in Kommunikationssystemen wie Funkübertragung durch zu viele Wiederholungen unter Störeinfluss auftreten.

3.1.1.24

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 Ein PELV-Stromkreis ist wie ein SELV-Stromkreis, der mit Schutz Erde verbunden ist.

[IEC 61131-2]

3.1.1.25

Redundanz

en: redundancy

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

BEISPIEL Zweifache Ausführung der funktionellen Komponenten und das Hinzufügen von Prüfbits (Paritätsbits) sind beides Beispiele für Redundanz.

ANMERKUNG 1 Redundanz dient hauptsächlich der Verbesserung von Zuverlässigkeit oder Verfügbarkeit.

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

[IEC 61508-4:1998], [ISO/IEC 2382-14.01.12]

3.1.1.26

relativer Zeitstempel

en: relative time stamp

Zeitstempel, der sich auf die lokale Zeit einer Einheit bezieht

ANMERKUNG Im Allgemeinen gibt es keine Beziehungen zu den Uhren in anderen Einheiten.

[IEC 62280-2, modified]

3.1.1.27

Unverlässigkeit

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 Es wird allgemein angenommen, dass das automatisierte System sich am Anfang des Zeitintervalls in einem Zustand befindet, um die geforderte Funktion auszuführen.

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

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

ANMERKUNG 4 Zuverlässigkeit unterscheidet sich von Verfügbarkeit.

[IEC 62059-11, modifiziert]

3.1.1.28

Risiko

en: risk

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

[IEC 61508-4:1998]

3.1.1.29

Sicherheitskommunikationsschicht

en: safety communication layer (SCL)

Kommunikationsschicht, die sämtliche notwendigen Mittel beinhaltet, um die sichere Übertragung von Daten entsprechend den Anforderungen der IEC 61508 zu gewährleisten

3.1.1.30

sichere Verbindung

en: safety connection

Verbindung, welche das Sicherheitsprotokoll für Kommunikationstätigkeiten nutzt

3.1.1.31

Sicherheitsdaten

en: safety data

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

ANMERKUNG Die Sicherheitskommunikationsschicht garantiert nicht sichere Daten an sich, sondern nur den gesicherten Transport.

3.1.1.32

Sicherheitsgerät

en: safety device

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

3.1.1.33

Sicherheitskleinspannung

en: safety extra-low-voltage (SELV)

Stromkreis, in der die Spannung AC 30 V, 42,4 V Scheitelwert oder DC 60 V unter Normalbedingungen oder den Bedingungen eines Einzelfehlers nicht überschreitet, einschließlich Erdungsfehler in anderen Stromkreisen

ANMERKUNG Ein SELV-Stromkreis ist nicht mit Schutz Erde verbunden.

[IEC 61131-2]

3.1.1.34

Sicherheitsfunktion

en: safety function

Funktion, die von einem E/E/PE-sicherheitsbezogenen System, einem sicherheitsbezogenen System anderer Technologie oder externen Einrichtungen zur Risikominderung ausgeführt wird mit dem Ziel, unter Berücksichtigung eines festgelegten gefährlichen Vorfalls einen sicheren Zustand für die EUC zu erreichen oder aufrechtzuerhalten

[IEC 61508-4:1998]

3.1.1.35

Reaktionszeit einer Sicherheitsfunktion

en: safety function response time

im ungünstigsten Fall benötigte Zeit, nach Aktivierung eines am Feldbus angeschlossenen Sicherheitssensors, bis der zugehörige sichere Zustand des Sicherheitsaktuators erreicht wurde, unter Berücksichtigung von gleichzeitig auftretenden Fehlern und Ausfällen im Übertragungskanal der Sicherheitsfunktion

ANMERKUNG Dieses Konzept wird in 0 eingeführt und von den in diesem Normteil aufgeführten Kommunikationsprofilen für funktional sichere Übertragung verwendet.

3.1.1.36

Sicherheits-Integritätslevel

en: safety integrity level (SIL)

eine von vier diskreten Stufen zur Spezifizierung der Anforderung für die Sicherheitsintegrität der *Sicherheitsfunktionen*, die dem E/E/PE-sicherheitsrelevanten System zugeordnet werden, wobei der Sicherheits-Integritätslevel 4 die höchste Stufe der Sicherheitsintegrität und der Sicherheits-Integritätslevel 1 die niedrigste darstellt

ANMERKUNG Die Ausfallgrenze für die vier Sicherheits-Integritätslevel sind in den Tabellen 2 und 3 der IEC 61508-1 festgelegt.

[IEC 61508-4:1998]

3.1.1.37

Sicherheitsmaßnahme

en: safety measure

<diese Norm> Mittel zur Beherrschung möglicher Kommunikationsfehler, welches in Übereinstimmung mit den Anforderungen der IEC 61508 entworfen und ausgeführt wurde

ANMERKUNG 1 In der Praxis werden mehrere Sicherheitsmaßnahmen kombiniert, um den geforderten Sicherheits-Integritätslevel zu erzielen.

ANMERKUNG 2 Kommunikationsfehler und zugehörige Sicherheitsmaßnahmen sind ausführlich in 0 und 0 beschrieben.

3.1.1.38

sicherheitsbezogene Anwendung

en: safety-related application

Programme, welche in Übereinstimmung mit den Anforderungen der IEC 61508 ausgeführt sind, um die SIL-Anforderungen einer Anwendung einzuhalten

3.1.1.39

sicherheitsbezogenes System

en: safety-related system

System, welches *Sicherheitsfunktionen* nach IEC 61508 ausführt

3.1.1.40

Slave

passive Kommunikationseinheit, die Nachrichten empfangen kann und sie als Antwort an andere Kommunikationseinheiten sendet, die Master oder Slave sein können

3.1.1.41

unberechtigte Auslösung

en: spurious trip

Auslösung in einem Sicherheitssystem ohne Prozessanforderung