

DIN EN 61784-3-3

ICS 35.160; 35.240.50

Ersatz für
DIN EN 61784-3-3:2012-03
Siehe Anwendungsbeginn

**Industrielle Kommunikationsnetze –
Profile –
Teil 3-3: Funktional sichere Übertragung bei Feldbussen –
Zusätzliche Festlegungen für die Kommunikationsprofilfamilie 3
(IEC 61784-3-3:2016);
Englische Fassung EN 61784-3-3:2017**

Industrial communication networks –
Profiles –
Part 3-3: Functional safety fieldbuses –
Additional specifications for CPF 3
(IEC 61784-3-3:2016);
English version EN 61784-3-3:2017

Réseaux de communication industriels –
Profils –
Partie 3-3: Bus de terrain de sécurité fonctionnelle –
Spécifications supplémentaires pour CPF 3
(IEC 61784-3-3:2016);
Version anglaise EN 61784-3-3:2017

Gesamtumfang 163 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE



Anwendungsbeginn

Anwendungsbeginn für die von CENELEC am 2016-08-16 angenommene Europäische Norm als DIN-Norm ist 2018-09-01.

Für DIN EN 61784-3-3:2012-03 besteht eine Übergangsfrist bis 2020-11-10.

Nationales Vorwort

Vorausgegangener Norm-Entwurf: E DIN EN 61784-3-100:2014-12.

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.

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.

Der Zusammenhang der zitierten Dokumente mit den entsprechenden deutschen Dokumenten ergibt sich, soweit ein Zusammenhang besteht, grundsätzlich über die Nummer der entsprechenden IEC-Publikation. Beispiel: IEC 60068 ist als EN 60068 als Europäische Norm durch CENELEC übernommen und als DIN EN 60068 ins Deutsche Normenwerk aufgenommen.

Das Präsidium des DIN hat mit Präsidialbeschluss 1/2004 festgelegt, dass DIN-Normen, deren Inhalt sich auf internationale Arbeitsergebnisse der Informationsverarbeitung gründet, unter bestimmten Bedingungen allein in englischer Sprache veröffentlicht werden dürfen. Diese Bedingungen sind für die vorliegende Norm erfüllt.

Da sich die Benutzer der vorliegenden Norm der englischen Sprache als Fachsprache bedienen, wird die Englische Fassung der EN 61784-3-3 veröffentlicht. Zu deren Abschnitt 0, der die Einleitung festlegt, Abschnitt 1, der den Anwendungsbereich festlegt, und Abschnitt 3, der die Begriffe, Abkürzungen und Konventionen festlegt, wurde eine Übersetzung angefertigt und als informativer Nationaler Anhang NA der vorliegenden Norm hinzugefügt. Für die meisten der verwendeten Begriffe existieren keine gebräuchlichen deutschen Benennungen, da sich die deutschen Anwender in der Regel ebenfalls der englischen Benennungen bedienen. Diese Norm steht nicht in unmittelbarem Zusammenhang mit Rechtsvorschriften und ist nicht als Sicherheitsnorm anzusehen.

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 61784-3-3:2012-03 wurden folgende Änderungen vorgenommen:

- a) Der Legacy V1-Modus wurde von dieser Protokolledition entfernt;
- b) Protokollerweiterungen zum Schutz gegen mögliche "Loopbacks" (LP- Erweiterungen);

- c) Protokollerweiterungen zur Beibehaltung von SIL3 für sichere Netzwerke mit hoher Anzahl an Teilnehmern (XP-Erweiterungen) und demzufolge neue F-Parameter "F_CRC_Seed";
- d) Einführung eines zufälligen und disjunkten Codenamens, basierend auf MonitoringNumbers (MNR) neben den vorherigen fortlaufenden Nummern;
- e) Bestimmungen für die granulare Passivierung von Kanälen und demzufolge neuer F-Parameter "F_Passivation";
- f) GSD-Erweiterungen aufgrund neuer F-Parameter;
- g) Bezeichnung gemäß der CP 3-Familie in IEC 61158 (z. B. IO Controller);
- h) zusätzliche Diagnose-Nachrichtentypen;
- i) verschiedene Fehlerbehebungen und Aktualisierung von Dokumenten in den Literaturhinweisen.

Frühere Ausgaben

DIN EN 61784-3-3: 2008-11, 2012-03

Nationaler Anhang NA (informativ)

Auszugsweise Übersetzung^{N1}

0 Einleitung

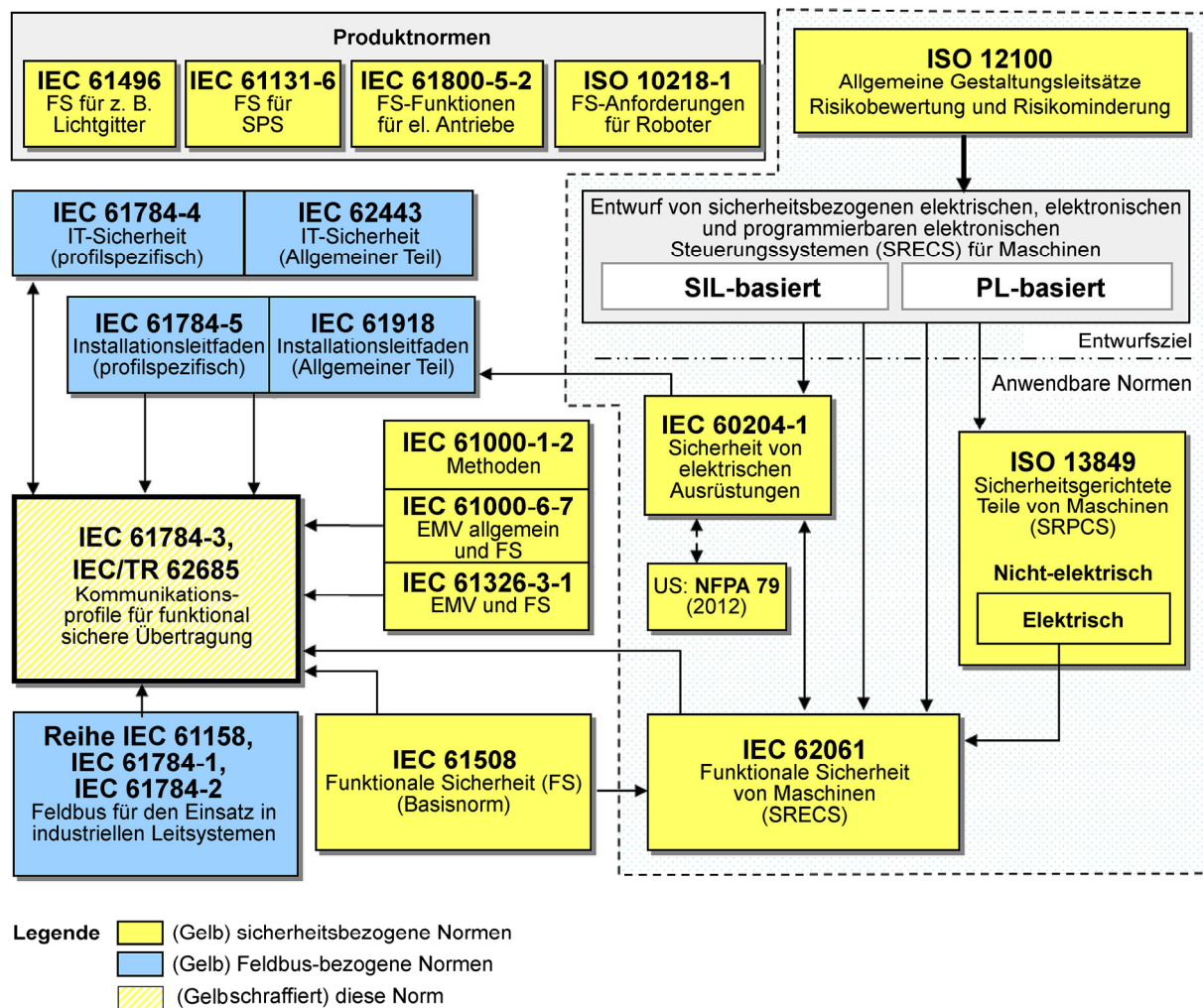
0.1 Allgemeines

Die IEC 61158-Feldbusnorm(en) und ihre Begleitnormen IEC 61784-1 und 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 z. B. Echtzeit, funktionale Sicherheit und Informationssicherheit abzielen.

Diese Norm erläutert die relevanten Prinzipien für funktional sichere Kommunikation bezogen auf Normen der Reihe IEC 61508 und spezifiziert mehrere Sicherheitskommunikationsschichten (Profile und entsprechende Protokolle) basierend auf den Kommunikationsprofilen und Protokollschichten in 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.

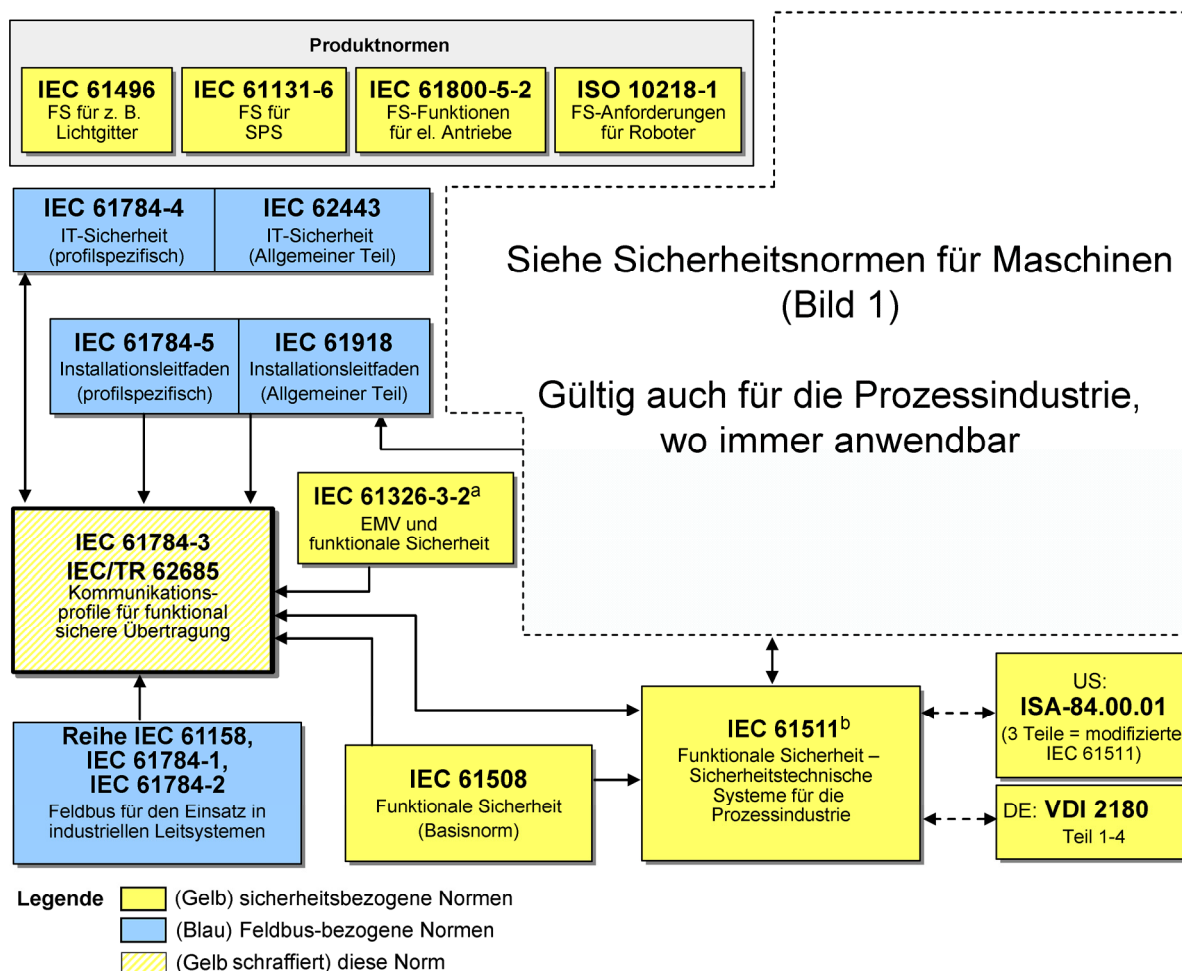
^{N1} Nationale Fußnote: Die Nummerierung aus IEC 61784-3-3:2016-07 wurde beibehalten.



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

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

Bild 2 zeigt die Beziehungen zwischen dieser Norm und einem Prozessumfeld in relevanten Sicherheits- und Feldbusnormen.



^a In spezifizierten elektromagnetischen Umgebungen, ansonsten IEC 61326-3-1 oder IEC 61000-6-7.

^b Als EN ratifiziert.

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

Die als Bestandteile eines sicherheitsbezogenen Systems nach der 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 einem Sicherheits-Integritätslevel (SIL) eingesetzt werden kann, wie es 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 der IEC 61784-2, welche Ergänzungen der Kommunikationsdienst- und -protokollabschnitte der Reihe IEC 61158 um eine Sicherheitsschicht enthalten.

0.2 Patentangaben

Die Internationale Elektrotechnische Kommission (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 Familie 3. Die Patente sind nachfolgend aufgeführt, dabei kennzeichnet die Bezeichnung [xx] den Inhaber der Patentrechte:

US 6907542	[SI]	System, device and method for determining the reliability of data carriers in a failsafe system network
US 6725419 DE 59910661.1 EP 1064590	[SI]	Automation system and method for operating an automation system
US 7808917 DE 50 2005 001 819.2 EP 1686732	[SI]	Method and system for transmitting telegrams
US 7640480 DE 50 2005 004 305.7 EP 1802019	[SI]	Detection of errors in the communication of data
EP 1921525	[SI]	Security-related system component e.g. guard door, for automation system of production system, has comparing unit comparing signatures for identity, where component supports security-related operation during sameness of signatures
EP 13172092.2	[SI]	Method and System for Detecting Errors when Transmitting Data from a Transmitter to at Least One Receive

IEC übernimmt keine Verantwortung hinsichtlich Nachweis(en), Gültigkeit und Anwendungsbereich von Patentrechten.

Der Halter der Patentrechte hat der IEC gegenüber versichert, dass er bereit ist, Anwendern weltweit Nutzungsrechte unentgeltlich oder zu angemessenen und nicht diskriminierenden Bedingungen einzuräumen. Diesbezügliche Aussagen des Halters dieser Patentrechte sind bei der IEC hinterlegt.

Informationen sind erhältlich bei:

[SI] Siemens Aktiengesellschaft
CT IP M&A
Otto-Hahn-Ring 6
81739 München
GERMANY

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. IEC ist 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 Normen 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 legt eine Sicherheitskommunikationsschicht (Dienste und Protokoll) auf der Basis von CPF 3 in IEC 61784-1, IEC 61784-2 (CP 3/1, CP 3/2, CP 3/4, CP 3/5 und CP 3/6) und IEC 61158, Typ 3 und Typ 10 fest. Er erläutert die Prinzipien für eine funktional sichere Kommunikation nach den Festlegungen in IEC 61784-3, die für diese Sicherheitskommunikationsschicht zutreffen. Diese Sicherheitskommunikationsschicht ist nur für die Implementierung in Sicherheitsgeräten zutreffend.

ANMERKUNG 1 Er deckt Aspekte der elektrischen Sicherheit und der Eigensicherheit nicht ab. Elektrische Sicherheit bezieht sich auf Gefährdungen wie z. B. elektrischer Schlag. Eigensicherheit bezieht sich auf Gefährdungen, wie sie durch explosionsfähige Gasgemische gegeben sind.

Dieser Teil¹ definiert Mechanismen für die Übertragung sicherheitsbezogener Nachrichten unter Teilnehmern innerhalb eines verteilten Netzwerks unter Anwendung der Feldbustechnologie nach den Anforderungen der Reihe IEC 61508² für funktionale Sicherheit. Diese Mechanismen dürfen in verschiedenen industriellen Anwendungen wie z. B. Prozessleitsystemen, Fertigungsautomatisierung und Maschinenanlagen verwendet werden.

Dieser Teil enthält Leitfäden sowohl für Entwickler als auch für Gutachter von konformen Geräten und Systemen.

ANMERKUNG 2 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 nach der vorliegenden Norm in einem Standardgerät reicht nicht aus, um es als Sicherheitsgerät zu qualifizieren.

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 in 3.1 definiert sind.

3.1.1 Allgemeine Begriffe

ANMERKUNG Diese allgemeinen Begriffe wurden aus IEC 61784-3 übernommen.

3.1.1.1

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]

3.1.1.2

Verfügbarkeit

(en: availability)

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

¹ Auf den folgenden Seiten dieser Norm wird „dieser Teil“ für „diesen Teil der Reihe IEC 61784-3“ verwendet.

² Auf den folgenden Seiten dieser Norm wird „IEC 61508“ für „Reihe IEC 61508“ verwendet.

3.1.1.3

Bitfehlerwahrscheinlichkeit

Pe

(en: bit error probability)

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

3.1.1.4

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.

3.1.1.5

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 7498-1-Anwendungsschicht) von einer Anwendung zur anderen

3.1.1.7

Verbindung

(en: connection)

logische Verbindung zwischen zwei Anwendungsobjekten in demselben oder in unterschiedlichen Geräten

3.1.1.8

CRC-Prüfung

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 z. B. CRC1, CRC2 können ebenfalls in dieser Norm verwendet sein, um redundante Daten zu kennzeichnen.

Anmerkung 2 zum Begriff: Siehe auch [33], [34]⁴.

3.1.1.9

festgelegtes Kommunikationssystem

(en: defined communication system;

defined channel)

festgelegte Anzahl oder festgelegte maximale Anzahl von Teilnehmern, die über ein auf einem *Feldbus* basierenden *Kommunikationssystem* verbunden sind, mit wohldefinierten und festgelegten Eigenschaften wie z. B. 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

3.1.1.10

Fehler

(en: error)

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

⁴ Zahlen in rechteckigen Klammern beziehen sich auf die Literaturhinweise.

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

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]

3.1.1.11

Ausfall

(en: failure)

Beendigung der Fähigkeit einer Funktionseinheit, eine geforderte Funktion auszuführen oder Betrieb einer Funktionseinheit in irgendeiner Art 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]

3.1.1.12

Fehlzustand

(en: fault)

nicht normale Bedingung, die eine Verminderung oder den Verlust der Fähigkeit einer Funktionseinheit verursachen 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 durch dieses Unvermögen während vorbeugender Instandhaltung, anderer geplanter Aktionen oder auf Grund fehlender externer Betriebsmittel.

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

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 Protokolldateneinheit der Sicherungsschicht (en: data link protocol data unit (DLPDU))

3.1.1.16

Blockprüfzeichenfolge

FCS

(en: Frame Check Sequence)

redundante Daten, mittels Hash-Funktion aus einem Block von Daten in einer DLPDU abgeleitet und mit diesem Block von Daten 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 [33], [34].

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 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]

3.1.1.18

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

3.1.1.19

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

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

3.1.1.21

Fehlauslösung

(en: nuisance trip)

unberechtigte Auslösung ohne schädliche Wirkung

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

3.1.1.22

Wiederholungsprüfung

(en: proof test)

wiederkehrende Prüfung zur Aufdeckung von versteckten gefahrbringenden Ausfällen in einem *sicherheitsbezogenen System*, so dass nötigenfalls eine Reparatur das System in einen „Wie-Neu“-Zustand zurückbringen oder so nah wie unter praktischen Gesichtspunkten möglich an diesen Zustand heranbringen kann

Anmerkung 1 zum Begriff: Eine Wiederholungsprüfung ist zur Bestätigung vorgesehen, dass sich das sicherheitsbezogene System in einem Zustand befindet, der die festgelegte Sicherheitsintegrität garantiert.

[QUELLE: IEC 61508-4:2010, 3.8.5, modifiziert – Ersatz der vier Anmerkungen durch eine andere Anmerkung]

3.1.1.23

Performance Level

PL

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

[QUELLE: ISO 13849-1:2006, 3.1.23]

3.1.1.24

Schutzkleinspannung

PELV

(en: protective extra-low-voltage)

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 ähnelt einem SELV-Stromkreis, der mit Schutzerde verbunden ist.

[QUELLE: IEC 61131-2:2007, 3.54]

3.1.1.25**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]

3.1.1.26**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 (en: 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, anstelle von „Benennung“ und zwei Anmerkungen hinzugefügt]

3.1.1.27**Restfehlerwahrscheinlichkeit****RP**

(en: residual error probability)

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

3.1.1.28**Restfehlerrate**

(en: residual error rate)

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

3.1.1.29**Risiko**

(en: risk)

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

Anmerkung 1 zum Begriff: Für weitere Diskussion dieses Begriffs 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]

3.1.1.30**Sicherheitskommunikationskanal**

(en: safety communication channel)

Kommunikationskanal, beginnend am oberen Rand des 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.

3.1.1.31**Sicherheitskommunikationsschicht****SCL**

(en: safety communication layer)

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