

DIN EN IEC 61784-3-100



ICS 35.160; 35.240.50

Einsprüche bis 2021-05-12
Ersatzvermerk
siehe unten**Entwurf****Industrielle Kommunikationsnetze –
Profile –****Teil 3-X: Funktional sichere Übertragung bei Feldbussen – Zusätzliche
Festlegungen für die Kommunikationsprofilfamilie X
(IEC 65C/996/CDV:2020);
Englische Fassung prEN IEC 61784-3-X:2020**Industrial communication networks –
Profiles –Part 3-X: Functional safety fieldbuses – Additional specifications for CPF X
(IEC 65C/996/CDV:2020);
English version prEN IEC 61784-3-X:2020Réseaux de communication industriels –
Profils –Partie 3-X: Bus de terrain de sécurité fonctionnelle – Spécifications supplémentaires pour
CPF X
(IEC 65C/996/CDV:2020);
Version anglaise prEN IEC 61784-3-X:2020**Anwendungswarnvermerk**Dieser Norm-Entwurf mit Erscheinungsdatum 2021-03-12 wird der Öffentlichkeit zur Prüfung und
Stellungnahme vorgelegt.Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses
Entwurfs besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal von DIN unter www.din.de/go/entwuerfe bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an dke@vde.com möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/go/stellungnahmen-norm-entwuerfe oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an die DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE oder Stresemannallee 15, 60596 Frankfurt am Main.

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten
Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.**Ersatzvermerk**Vorgesehen als Ersatz für DIN EN 61784-3-2:2018-09, DIN EN 61784-3-3:2018-09,
DIN EN 61784-3-8:2018-09 und DIN EN 61784-3-13:2018-09;
vorgesehen als Änderung von DIN EN 61784-3-18:2012-08

Gesamtumfang 798 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE

Nationales Vorwort

Die Englische Fassung des europäischen Dokuments prEN IEC 61784-3-X:2020 „Industrielle Kommunikationsnetze – Profile – Teil 3-X: Funktional sichere Übertragung bei Feldbussen – Zusätzliche Festlegungen für die Kommunikationsprofilfamilie X“ (Entwurf in der Umfrage) ist unverändert in diesen Norm-Entwurf übernommen worden.

Die Internationale Elektrotechnische Kommission (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. Dem entsprechend ist das internationale Dokument IEC 65C/996/CDV:2020 „Industrial communication networks – Profiles – Part 3-X: Functional safety fieldbuses – Additional specifications for CPF X“ unverändert in den Entwurf prEN IEC 61784-3-X:2020 übernommen worden.

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

Bei der Abstimmung zu dem Europäischen Schluss-Entwurf bei CENELEC und dem Internationalen Schluss-Entwurf bei IEC [Final Draft International Standard (FDIS)] sind jeweils nur „JA/NEIN“-Entscheidungen möglich, wobei „NEIN“-Entscheidungen fundiert begründet werden müssen. Dokumente, die bei CENELEC als Europäische Norm angenommen und ratifiziert werden, sind unverändert als Deutsche Normen zu übernehmen.

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.

Aktuelle Informationen zu diesem Dokument können über die Internetseiten von DKE (www.dke.de) und DIN (www.din.de) durch eine Suche nach der Dokumentennummer aufgerufen werden.

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 den vorliegenden Normentwurf erfüllt.

Da sich die Benutzer des vorliegenden Normentwurfs der englischen Sprache als Fachsprache bedienen, wird die englische Fassung der prEN IEC 61784-3-X:2020 veröffentlicht. Zu deren Einleitung und Abschnitt 1, der den Anwendungsbereich festlegt, und deren Abschnitt 3 (außer Unterabschnitt 3.3), der die Begriffe, Symbole und Abkürzungen festlegt, wurde eine Übersetzung angefertigt und als informativer Nationaler Anhang NA des vorliegenden Normentwurfs hinzugefügt. Für viele der verwendeten Begriffe existieren keine gebräuchlichen deutschen Benennungen, da sich die deutschen Anwender in der Regel ebenfalls der englischen Benennungen bedienen. Dieser Normentwurf steht nicht in unmittelbarem Zusammenhang mit Rechtsvorschriften und ist nicht als Sicherheitsnorm anzusehen.

Es ist vorgesehen, auch bei der entsprechenden zukünftigen Deutschen Norm auf die deutsche Sprachfassung zu verzichten und diese in der englischsprachigen Fassung zu veröffentlichen.

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.

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

Änderungen

Gegenüber DIN EN 61784-3-2:2018-09, DIN EN 61784-3-3:2018-09, DIN EN 61784-3-8:2018-09, DIN EN 61784-3-13:2018-09 und DIN EN 61784-3-18:2012-08 wurden folgende Änderungen vorgenommen:

- a) Hinzufügung von zwei neuen Safety Supervisor Objektzuständen in 6.6.5.5 (IEC 61784-3-2);
- b) Hinzufügung der Anforderung an das Verhalten der Net-LED für den vorschlagenden TUNID-Prozess in 6.6.8, 9.1.2 und 9.1.5 (IEC 61784-3-2);
- c) Hinzufügung der Unterstützung von Anwendungspfaden für Prozessvariablen in 6.3.9 und 6.3.10 (IEC 61784-3-2);
- d) Hinzufügung der Unterstützung von Mehrportgeräten in 6.6.4, 6.6.5, 6.6.7 und an verschiedenen Stellen (IEC 61784-3-2);
- e) Korrektur der Netzreaktionszeit 56 Gleichungen in 9.3.3 (IEC 61784-3-2);
- f) Ergänzung der SIL-Unterstützung bis SIL 3 in 7.6, 8.7, 8.9, 9.5 und diversen Stellen (IEC 61784-3-2);
- g) diverse kleinere Korrekturen seit der letzten Veröffentlichung (IEC 61784-3-2);
- h) Redaktionelle Änderungen bezüglich Aktualität, Umwandlung von Kommentaren in der Tabelle in Anweisungen (IEC 61784-3-3);
- i) Verwendung von Abkürzungen bei PROFINET (IEC 61784-3-3);
- j) Informationen zu Prüfungen und Sicherheitshandbuch für PROFIsafe-Adresse Typ 1 und 2 (IEC 61784-3-3) hinzugefügt;
- k) Informationen zu PFDavg hinzugefügt, Unterstützung des automatischen Tests, Diagnosemeldungen hinzufügen (IEC 61784-3-3);
- l) Erläuterung und Spezifikation der optionalen Statemachines 55 zur Reaktion auf Gerätefehler (IEC 61784-3-3);
- m) Neue optionale Variable "OAD_Nec_C" für optionale Eigenschaft "Reaktion auf Gerätefehler in F_Host" " (IEC 61784-3-3);
- n) Spezifikation des optionalen Merkmals F-Host für "Disable F-(Sub)Module" (IEC 61784-3-3);
- o) Spezifizierung der Anforderungen für FSCP 3/1 und PROFInergy (IEC 61784-3-3);
- p) Spezifizierung der Anforderung für mehrere F-Hosts, die mit einem einzigen F-(Sub)Modul kommunizieren (IEC 61784-3-3);
- q) Aktualisierung des Sicherheitshandbuchs (IEC 61784-3-3);
- r) Diverse Fehlerkorrekturen, Behebung von Tippfehlern und Aktualisierung der Referenzen (IEC 61784-3-3);
- s) Aktualisierte Bibliographie (IEC 61784-3-3);
- t) Strukturiert für die Übereinstimmung mit IEC 61784-3-0 Ed.4 (IEC 61784-3-8);
- u) Allgemeine redaktionelle Änderungen und Klarstellungen (IEC 61784-3-8);
- v) Sicherheitsmaßnahmen (11.5.3) (IEC 61784-3-8);
- w) Sicherheitstechnische Anwendungsdienstelemente (11.6.2) (IEC 61784-3-8);

E DIN EN IEC 61784-3-100:2021-04

- x) Sicherheits-PDU-Format (11.7.1) (IEC 61784-3-8);
- y) Einschränkungen für Berechnungen von System c 56 Charakteristika (11.9.5) (IEC 61784-3-8);
- z) Sicherheitsmaßnahmen (12.5.3) (IEC 61784-3-8);
- aa) Sicherheits-PDU-Format (12.7.1) (IEC 61784-3-8);
- bb) Verhaltensweisen (12.7.2) (IEC 61784-3-8);
- cc) Randbedingungen für Berechnungen von Systemeigenschaften (12.9.5) (IEC 61784-3-8);
- dd) Berechnungen der Hash-Funktion (Anhang A) (IEC 61784-3-8);
- ee) Entfernung von Block Up-/Download (IEC 61784-3-13);
- ff) Hinzufügen von SSDO mit Preload (IEC 61784-3-13);
- gg) Hinzufügen von SPDO-Feature-Sets (IEC 61784-3-13);
- hh) Ergänzung von SPDO mit 40-Bit-Zähler (IEC 61784-3-13);
- ii) Hinzufügung von SPDO mit dynamischem SCT (IEC 61784-3-13);
- jj) Hinzufügung von 56 zusätzlichen Parametersätzen (IEC 61784-3-13);
- kk) Korrekturen und redaktionelle Verbesserungen (IEC 61784-3-13);
- ll) Korrekturen und redaktionelle Verbesserungen (IEC 61784-3-18/A2).

Nationaler Anhang NA (informativ)

Auszugsweise Übersetzung

Reihenfolge und Inhalt der folgenden Abschnitte sind identisch mit denen in den jeweiligen Abschnitten der Englischen Fassung.

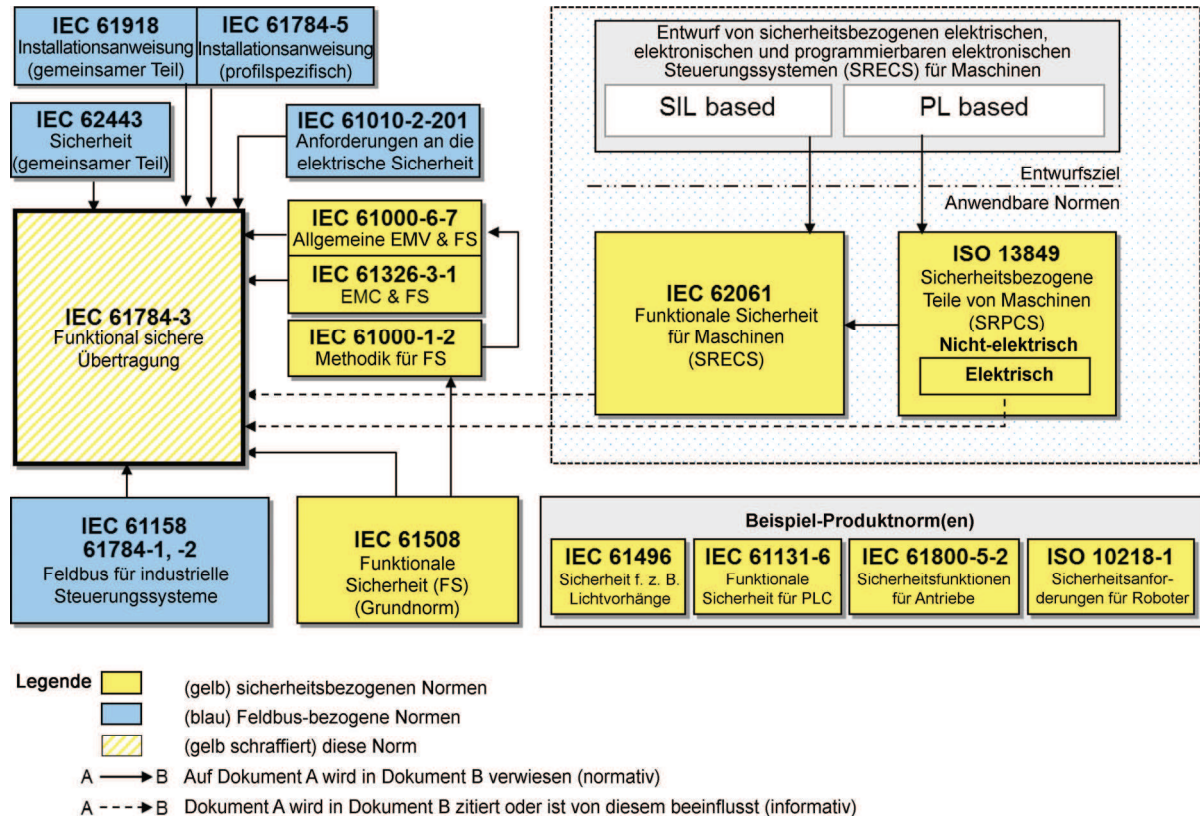
0 Einleitung zu E DIN EN IEC 61784-3-2, E DIN EN IEC 61784-3-3, E DIN EN IEC 61784-3-8, E DIN EN IEC 61784-3-13

0.1 Allgemeines

Die Feldbusnorm IEC 61158 (alle Teile) 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 Echtzeit und sicherheitsbezogene Anwendungen abzielen.

IEC 61784-3 (alle Teile) erläutert die relevanten Prinzipien für funktional sichere Kommunikation bezogen auf IEC 61508 (alle Teile) und spezifiziert mehrere Sicherheitskommunikationsschichten (Profile und entsprechende Protokolle) basierend auf den Kommunikationsprofilen und Protokollschichten in IEC 61784-1, IEC 61784-2 und IEC 61158 (alle Teile). Sie deckt Aspekte der elektrischen Sicherheit und der Eigensicherheit nicht ab. Sie behandelt jedoch weder Sicherheitsaspekte noch stellt sie Anforderungen an die IT-Sicherheit.

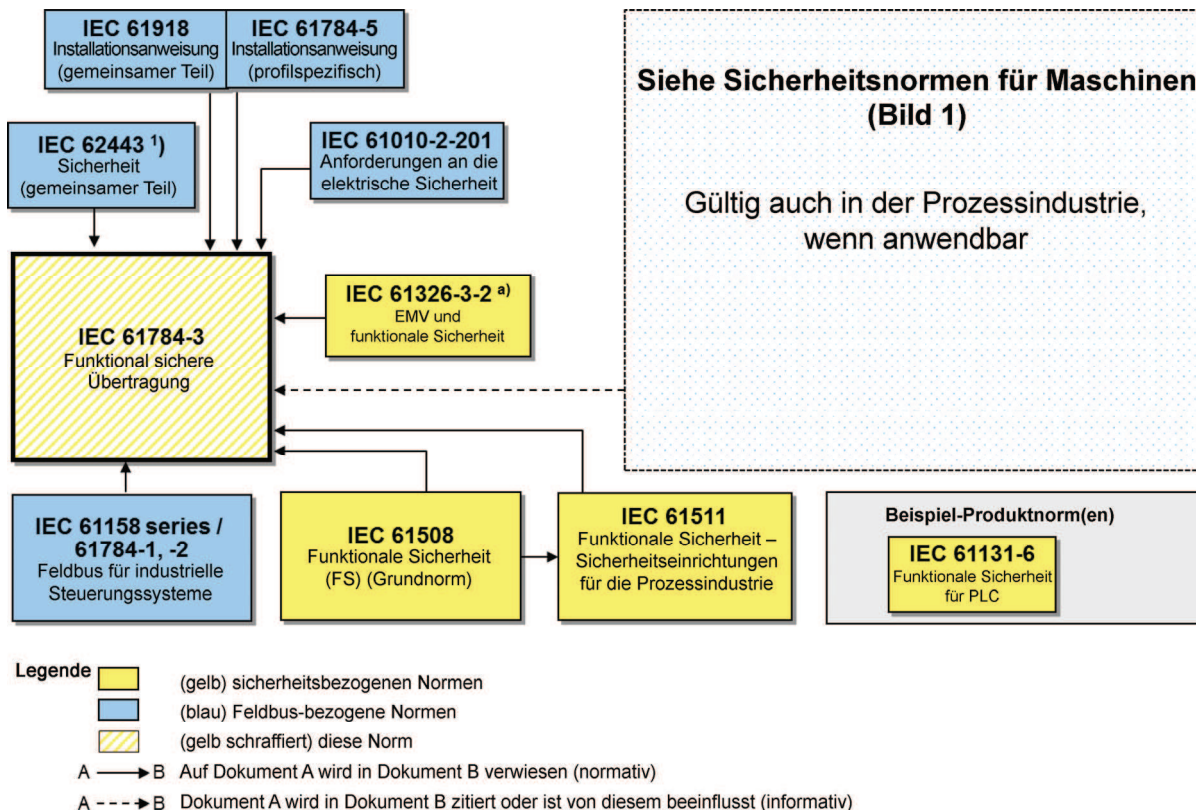
Bild 1 zeigt die Beziehungen zwischen IEC 61784-3 (alle Teile) und den für die Fertigungsautomatisierung relevanten Sicherheits- und Feldbusnormen.



ANMERKUNG IEC 62061 beschreibt das Verhältnis zwischen PL (Kategorie) und SIL.

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

Bild 2 zeigt die Beziehungen zwischen IEC 61784-3 (alle Teile) und den für die Fertigungsautomatisierung relevanten Sicherheits- und Feldbusnormen.



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

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

Die als Bestandteile eines sicherheitsbezogenen Systems nach IEC 61508 (alle Teile) 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 IEC 61784-3 (alle Teile) spezifizierten Sicherheitskommunikationsschichten tun dies dergestalt, dass ein Feldbus in Anwendungen mit funktionaler Sicherheit bis zu dem Sicherheits-Integritätslevel (SIL) eingesetzt werden kann, der 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.

IEC 61784-3 (alle Teile) beschreibt:

- grundlegende Prinzipien für die Erfüllung der Anforderungen von IEC 61508 (alle Teile) 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 von IEC 61158 (alle Teile) um eine Sicherheitsschicht enthalten.

E DIN EN IEC 61784-3-2

0.2 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 Familie 2, bei denen die Bezeichnung [xx] den Halter der Patentrechte angibt:

(6.631.476)	[RA]	Sicherheitsnetzwerk für Industriesteuerungen mit redundanten Verbindungen auf einzelnen Medien
(6.701.198)	[RA]	Sicherheitsnetzwerk für Industriesteuerungen, das die Initialisierung auf Standardnetzwerken erlaubt
(6.721.900)	[RA]	Sicherheitsnetzwerk für Industriesteuerungen mit verringerten Bandbreiteneanforderungen
(6.891.850)	[RA]	Netzwerkunabhängiges Sicherheitsprotokoll für Industriesteuerungen
(6.915.444)	[RA]	Netzwerkunabhängiges Sicherheitsprotokoll für Industriesteuerungen unter Verwendung von Datenmanipulationstechniken

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

Der Halter dieser Patentrechte hat ISO [und/oder] IEC zugesichert, dass er bereit ist, entweder kostenfrei oder über Lizenzen zu vernünftigen und nicht diskriminierenden Geschäftsbedingungen mit Antragstellern in der ganzen Welt zu verhandeln. In diesem Zusammenhang ist die Erklärung des Halters dieser Patentrechte bei ISO [und/oder] IEC registriert.

Informationen sind erhältlich bei:

[RA] Rockwell Automation, Inc.
1201 S. Second Street
Milwaukee, WI 53204
USA
Achtung: Abteilung Geistiges Eigentum

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

CEN (<http://www.cen.eu/cen/WorkArea/IPR/Pages/default.aspx>) und CENELEC (<http://www.cenelec.eu/membersandexperts/toolsandapplications/index.html>) stellen online eine aktuelle Liste mit den für ihre Normen relevanten Patenten bereit. Anwender werden ermutigt, sich diese Liste anzusehen, um die aktuellsten Informationen hinsichtlich Patenten zu erhalten.

1 Anwendungsbereich

Dieser Teil von IEC 61784-3 (alle Teile) legt eine Sicherheitskommunikationsschicht (Dienste und Protokoll) auf der Basis von CPF 2 in IEC 61784-1, IEC 61784-2 und IEC 61158 Typ 2 fest. Sie stellt die Grundsätze der funktional sicheren Kommunikation nach IEC 61784-3 fest, die für diese Sicherheitskommunikationsschicht wichtig sind. Diese Sicherheitskommunikationsschicht ist für die ausschließliche Implementierung in Sicherheitsgeräten vorgesehen.

ANMERKUNG 1 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.

Dieses Dokument legt Mechanismen fest für die Übertragung von sicherheitsrelevanten Nachrichten zwischen Teilnehmern in einem verteilten Netzwerk unter Verwendung von Feldbus-Technologie in Übereinstimmung mit IEC 61508 (alle Teile)¹⁾ für funktionale Sicherheit. Diese Mechanismen dürfen in verschiedenen Industrieanwendungen verwendet werden, wie Prozesssteuerung, Fertigungsautomatisierung und Maschinen.

Dieses Dokument enthält Leitlinien sowohl für Entwickler als auch Gutachter von entsprechenden 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 diesem Dokument 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 Begriffe nach IEC 61784-3 und die folgenden Begriffe.

ISO und IEC stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

- IEC Electropedia: verfügbar unter <http://www.electropedia.org/>
- ISO-Online-Rechercheplattform: verfügbar unter <http://www.iso.org/obp>

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

3.1.1 Allgemeine Begriffe

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

3.1.1.1

Verfügbarkeit

(en: availability)

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

¹⁾ In den nachfolgenden Seiten dieser Norm bedeutet „IEC 61508“ stets „IEC 61508 (alle Teile)“.

3.1.1.2

Bitfehlerwahrscheinlichkeit

(en: bit error probability)

P_e

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

3.1.1.3

Black Channel

(en: 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.

3.1.1.4

Bridge

abstraktes Gerät, welches auf der Ebene der Sicherungsschicht mehrere Netzwerksegmente verbindet

3.1.1.5

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 62280:2014, 3.1.6, modifiziert – Übertragung ersetzt durch Kommunikation]

3.1.1.6

Kommunikationskanal

(en: communication channel)

logische *Verbindung* zwischen zwei Endpunkten in einem *Kommunikationssystem*

3.1.1.7

Kommunikationssystem

(en: communication system)

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

3.1.1.8

Verbindung

(en: connection)

logische Verbindung zwischen zwei Anwendungsobjekten in demselben oder in unterschiedlichen Geräten

3.1.1.9

zyklische Redundanzprüfung

(en: Cyclic Redundancy Check)

CRC

<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 diesem Dokument verwendet sein, um redundante Daten zu kennzeichnen.

Anmerkung 2 zum Begriff: Siehe auch [25], [26]².

²) Die Zahlen in eckigen Klammern verweisen auf die Literaturhinweise.

3.1.1.10

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

3.1.1.11

Gerät

mit dem Feldbus verbundene physikalische Einheit, die aus einem Kommunikationselement und möglicherweise anderen Funktionselementen besteht

[QUELLE: IEC 61158-2:2014, 3.1.13, modifiziert – Anmerkung zum Begriff und einige Einzelheiten wurden gestrichen.]

3.1.1.12

Fehler

(en: error)

Nichtübereinstimmung zwischen Rechenergebnissen, beobachteten oder gemessenen Werten oder Beschaffenheiten und den betreffenden wahren, spezifizierten oder theoretisch richtigen Werten oder Beschaffenheiten

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]

3.1.1.13

Ausfall

(en: failure)

Beendigung der Fähigkeit einer Funktionseinheit, eine geforderte Funktion auszuführen, oder 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]

3.1.1.14

Fehler

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 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]

3.1.1.15

Feldbus

(en: fieldbus)

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

3.1.1.16

DLPDU

(en: Data Link Protocol Data Unit)

ABGELEHNT: frame

Data Link Protocol Data Unit

3.1.1.17

funktional sicheres Kommunikationsprofil

FSCP

Technikspezifikation für die Implementierung eines SCL

3.1.1.18

Hash-Funktion

(en: hash function)

(mathematische) Funktion, die Werte aus einem (möglicherweise sehr) großen Wertebereich in einem (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.

3.1.1.19

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

3.1.1.20

Master

aktive Kommunikationseinheit, die Kommunikationsaktivitäten anderer Stationen, seien es Master oder Slaves, einleiten und planen kann

3.1.1.21

Nachricht

(en: message)

<Informationstheorie und Kommunikationstheorie> geordnete Zeichenfolge (in der Regel Oktetts), die zur Beförderung von Informationen vorgesehen ist

[QUELLE: ISO/IEC 2382:2015, 2123205, modifiziert – „(in der Regel Oktetts)“ eingefügt, Anmerkungen und Quelle gestrichen]

3.1.1.22

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.

3.1.1.23

Performance Level

PL

diskreter Level, der die Fähigkeit von sicherheitsbezogenen Teilen einer Steuerung spezifiziert, eine *Sicherheitsfunktion* unter vorhersehbaren Bedingungen auszuführen

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

3.1.1.24

Redundanz

(en: redundancy)

Vorhandensein von mehr als einem Mittel zum Ausführen einer geforderten Funktion oder zur Darstellung von Informationen

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

3.1.1.25

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, zwei Anmerkungen hinzugefügt]

3.1.1.26

Restfehlerrate

(en: residual error rate)

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

3.1.1.27

Risiko

(en: risk)

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

Anmerkung 1 zum Begriff: Für die 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]

3.1.1.28

Sicherheitskommunikationskanal

(en: safety communication channel)

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.

3.1.1.29

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

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 1 zum Begriff: 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

Sicherheitsfunktion

(en: safety function)

Funktion, die von einem sicherheitsbezogenen E/E/PE-System oder anderen risikomindernden Maßnahmen ausgeführt wird und dazu vorgesehen ist, unter Berücksichtigung eines festgelegten gefährlichen Vorfalles einen sicheren Zustand für die EUC zu erreichen oder aufrechtzuerhalten

[QUELLE: IEC 61508-4:2010, 3.5.1, modifiziert – Verweisungen und Beispiel entfernt]

3.1.1.34

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 Sicherheitsaktors erreicht wurde unter Berücksichtigung von gleichzeitig auftretenden *Fehlern* und *Ausfällen* in der *Sicherheitsfunktion*

Anmerkung 1 zum Begriff: Dieses Konzept wird in IEC 61784-3:—, 5.2.4 eingeführt und von den in diesem Dokument aufgeführten Kommunikationsprofilen für funktional sichere Übertragung verwendet.

3.1.1.35

Sicherheits-Integritätslevel

(en: safety integrity level)

SIL

eine von vier diskreten Stufen, die einem Wertebereich der Sicherheitsintegrität entsprechen, wobei der Sicherheits-Integritätslevel 4 die höchste Stufe der Sicherheitsintegrität und der Sicherheits-Integritätslevel 1 die niedrigste darstellt

Anmerkung 1 zum Begriff: Die *Ausfallgrenzen* (siehe IEC 61508-4:2010, 3.5.17) für die vier Sicherheits-Integritätslevel sind in IEC 61508-1:2010, Tabellen 2 und 3, festgelegt.

Anmerkung 2 zum Begriff: Sicherheits-Integritätslevel werden eingesetzt zur Festlegung der Anforderungen an die Sicherheitsintegrität von Sicherheitsfunktionen von *E/E/PE-sicherheitsbezogenen Systemen*.

Anmerkung 3 zum Begriff: Ein Sicherheits-Integritätslevel (SIL) ist nicht Attribut eines Systems, Subsystems, Elements oder einer Komponente. Die richtige Interpretation der Aussage „SIL *n* sicherheitsbezogenes System“ (wobei *n* 1, 2, 3 oder 4 sein kann) ist die, dass das System potenziell in der Lage ist, *Sicherheitsfunktionen* mit einem Sicherheits-Integritätslevel bis *n* zu unterstützen.

[QUELLE: IEC 61508-4:2010, 3.5.8]

3.1.1.36

Sicherheitsmaßnahme

(en: safety measure)

Mittel zur Beherrschung möglicher *Kommunikationsfehler*, welches in Übereinstimmung mit den Anforderungen der IEC 61508 entworfen und ausgeführt wurde

Anmerkung 1 zum Begriff: In der Praxis werden mehrere Sicherheitsmaßnahmen kombiniert, um den geforderten *Sicherheits-Integritätslevel* zu erzielen.

Anmerkung 2 zum Begriff: *Kommunikationsfehler* und zugehörige Sicherheitsmaßnahmen sind ausführlich in IEC 61784-3:—, 5.3 und 5.4 beschrieben.

3.1.1.37

Sicherheits-PDU

(en: safety PDU)

SPDU

durch einen Sicherheitskommunikationskanal übertragene PDU

Anmerkung 1 zum Begriff: Die SPDU kann mehr als eine Kopie der *sicheren Daten* unter Nutzung unterschiedlicher Codierungsstrukturen und *Hash-Funktionen*, zusammen mit eindeutigen Teilen zusätzlichen Schutzes wie Schlüssel, fortlaufenden Nummern oder einem *Zeitstempel*, beinhalten.

Anmerkung 2 zum Begriff: Redundante SCLs können zwei unterschiedliche Versionen der SPDU in getrennten Feldern der *Feldbus-DLPDU* vorsehen.

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

3.1.1.38

sicherheitsbezogene Anwendung

(en: safety-related application)

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

3.1.1.39

sicherheitsbezogenes System

System, welches *Sicherheitsfunktionen* nach IEC 61508 ausführt

3.1.1.40

Slave

(en: slave)

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

3.1.1.41

unberechtigte Auslösung

(en: spurious trip)

Auslösung in einem Sicherheitssystem ohne Prozessanforderung

3.1.1.42

Zeitstempel

(en: time stamp)

Zeitinformation in einer *Nachricht*

3.1.2 CPF 2: Zusätzliche Begriffe

3.1.2.1

Basisformat

(en: base format)

Format, das für Verbindungs-RPIs von kleiner als 100 ms oder für Anwendungen, bei denen unterbrochene Verbindungen toleriert werden, verwendet wird

3.1.2.2

erweitertes Format

(en: extended format)

Format, das für Verbindungs-RPIs von größer als 100 ms oder für Anwendungen, bei denen unterbrochene Verbindungen dringend vermieden werden müssen, verwendet wird

3.1.2.3

Ping

(en: ping)

Anforderung an den Verbraucher, den Empfang einer Nachricht zu bestätigen

3.1.2.4

Ping-Antwort

(en: ping response)

Antwort auf einen Ping

3.1.2.5

Urheber

(en: originator)

Knoten, der die Herstellung einer Verbindung anfordert

3.1.2.6

Signatur

(en: signature)

Verfahren zur eindeutigen Identifizierung einer Datenmenge

Anmerkung 1 zum Begriff: Dies könnte durch Verfahren wie Änderung, Quersumme, oder andere Verfahren, die von den versendenden und Zielgeräten vereinbart wurden, umgesetzt werden.

3.1.2.7

Gerät mit individuellem Sicherheitsanschluss

(en: single safety port device)

Urheber-, Ziel- oder gemischtes Urheber-/Zielgerät, das Sicherheitskommunikation über einen einzigen Sicherheitsanschluss durchführt

3.1.2.8

systematische Eignung

(en: systematic capability)

Maß des Vertrauens (ausgedrückt auf einer Skala von SC 1 bis SC 4), dass die systematische Sicherheitsintegrität eines Elements den Anforderungen des festgelegten SIL hinsichtlich der festgelegten Element-Sicherheitsfunktion entspricht, wenn das Element in Übereinstimmung mit den im Sicherheitshandbuch für konforme Objekte für das Element festgelegten Anweisungen angewendet wird

[QUELLE: IEC 61508-4:2010, 3.5.9, modifiziert – Anmerkungen wurden entfernt]

3.1.2.9

systematische Sicherheitsintegrität

(en: systematic safety integrity)

Teil der Sicherheitsintegrität eines sicherheitsbezogenen Systems, der sich auf systematische Ausfälle mit gefahrbringender Ausfallart bezieht

[QUELLE: IEC 61508-4:2010, 3.5.6, modifiziert – Anmerkung entfernt]

3.1.2.10

Ziel

(en: target)

Knoten, der eine Anforderung zur Herstellung einer Verbindung empfängt

3.2 Symbole und Abkürzungen

3.2.1 Allgemeine Symbole und Abkürzungen

CP	Kommunikationsprofil (en: Communication Profile)	[IEC 61784-1]
CPF	Kommunikationsprofilfamilie (en: Communication Profile Family)	[IEC 61784-1]
CRC	zyklische Redundanzprüfung (en: Cyclic Redundancy Check)	
DLL	Sicherungsschicht (en: Data Link Layer)	[ISO/IEC 7498-1]
DLPDU	Protokolldateneinheit der Sicherungsschicht (en: Data Link Protocol Data Unit)	
EMC	elektromagnetische Verträglichkeit	
EUC	Prüfling (en: equipment under control)	[IEC 61508-4:2010]
E/E/PE	elektrisch/elektronisch/programmierbar elektronisch (en: Electrical/Electronic/Programmable Electronic)	[IEC 61508-4:2010]
FAL	Feldbusanwendungsschicht (en: Fieldbus Application Layer)	[IEC 61158-5]
FS	funktionale Sicherheit (en: Functional Safety)	
FSCP	funktional sicheres Kommunikationsprofil (en: Functional Safety Communication Profile)	
MTBF	mittlere Zeit zwischen Ausfällen (en: Mean Time Between Failures)	
MTTF	mittlere Zeit bis zu einem Ausfall (en: Mean Time To Failure)	
PDU	Protokolldateneinheit (en: Protocol Data Unit)	[ISO/IEC 7498-1]
PFD	mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung (en: Probability of dangerous Failure on Demand)	[IEC 61508-4:2010]
PFH	mittlere Häufigkeit eines gefahrbringenden Ausfalls je Stunde [h^{-1}]	[IEC 61508-4:2010]
PhL	Bitübertragungsschicht (en: Physical Layer)	[ISO/IEC 7498-1]
PL	Performance Level	[ISO 13849-1]
PLC	speicherprogrammierbare Steuerung (en: Programmable Logic Controller)	
SCL	Sicherheitskommunikationsschicht (en: Safety Communication Layer)	
SIL	Sicherheits-Integritätslevel (en: safety integrity level)	[IEC 61508-4:2010]

3.2.2 CPF 2: Zusätzliche Symbole und Abkürzungen

AIRS	Bereits im angeforderten Modus/Zustand (en: already in requested mode/state)
BER	Bitfehlerquote (en: bit error rate)
BF	Basisformat (en: base format)
CCO	Verbindungskonfigurationsobjekt (en: connection configuration object)
CFUNID	Konfigurations-UNID (en: configuration UNID)
CNP	Verbindungspunkt (en: connection point)
CID	Verbraucher-ID (en: consumer ID)
CIP™ ³⁾	Common Industrial Protocol (Anwendungs-Framework, das von den CPF-2-Kommunikationsprofilen gemeinsam genutzt wird)
CPCRC	Verbindungsparameter-CRC
CTM	Multiplikator der Verbindungszeitüberschreitung (en: connection timeout multiplier)
EDS	elektronisches Datenblatt (en: electronic data sheet)
EF	erweitertes Format (en: extended format)
EPI	erwartetes Paketintervall (en: expected packet interval)
LED	lichtemittierende Diode
MACID	Physikalische Adresse des Geräts (CP 2/3)
MOD	Modul
NodeID	Für CP 2/3-Sicherheitsgeräte ist dies die MACID des Geräts im Netzwerk. Für CP 2/2-Sicherheitsgeräte ist dies die IP-Adresse des Geräts im Netzwerk. Für CP 16/3-Sicherheitsgeräte ist dies die SDID des Geräts im Netzwerk.
NV	nichtflüchtig (en: non-volatile)
NVS	nichtflüchtiger Speicher (en: non-volatile storage)

³⁾ Zur Angabe von Handelsnamen siehe Abschnitt 4.

E DIN EN IEC 61784-3-100:2021-04

OCPUNID	Eigner-UNID der Ausgangsverbindung (output connection owner UNID)	
OSC	Objektstatuskonflikt (en: object status conflict)	
O-to-T	Urheber-zu-Ziel (en: originator to target)	
OUNID	Urheber-UNID (en: originator UNID)	
PID	Erzeugerkennung (en: producer identifier)	
PS	Energieversorgung (en: power supply)	
Res.	reserviert (en: reserved)	
RPI	angefordertes Paketintervall (en: requested packet interval)	
SCCRC	Sicherheitskonfigurationsdaten-CRC (en: safety configuration data CRC)	
SCID	Identifizierte Sicherheitskonfiguration (en: safety configuration identified)	
SCTS	Zeitstempel der Sicherheitskonfiguration (en: safety configuration time stamp)	
SNCT	Sicherheitsnetzwerkkonfigurationswerkzeug (en: safety network configuration tool)	
SNN	Sicherheitsnetzwerknummer (en: safety network number)	
T-to-O	Ziel-zu-Urheber (en: target-to-originator)	
TBD	festzulegen (en: to be defined)	
TNS	TUNID nicht gesetzt (en: TUNID not set)	
TUNID	Ziel-UNID (en: target TUNID)	
UML	Universal Modeling Language	[ISO/IEC 19501]
UNID	eindeutige Netzwerkkennung (en: unique network identifier)	

E DIN EN IEC 61784-3-3

0.2 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 Familie 3, bei denen die Bezeichnung [xx] den Halter der Patentrechte angibt:

(6.907.542)	[SI]	System, Gerät und Verfahren zur Bestimmung der Zuverlässigkeit von Datenträgern in einem ausfallsicheren Systemnetzwerk
(6.725.419)	[SI]	Automationssystem und Verfahren zum Betrieb eines Automationssystems
US 7,808,917	[SI]	Verfahren und System zur Übertragung von Telegrammen
EP 1686732 (DE, FR, GB, IT)		
US 7,640,480	[SI]	Erkennung von Fehlern in der Datenkommunikation
EP 1802019 (DE, FR, GB, IT)		
EP 1921525 (DE, FR, IT)	[SI]	Sicherheitsbezogene Systemkomponente, z. B. Schutztür, für das Automatisierungssystem eines Produktionssystems, hat eine Vergleichseinheit, die Signaturen auf Identität vergleicht, wobei die Komponente den sicherheitsbezogenen Betrieb bei Gleichheit der Signaturen unterstützt
EP 2814193 (DE, FR, IT)	[SI]	Verfahren und System zur Erkennung von Fehlern bei der Übertragung von Daten von einem Sender zu mindestens einem Empfänger
US 9,411,677		
CN 104243093		

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.

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, ohne dass diese vorstehend identifiziert wurden. IEC [und/oder ISO] sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

CEN (<http://www.cen.eu/cen/WorkArea/IPR/Pages/default.aspx>) und CENELEC (<http://www.cenelec.eu/membersandexperts/toolsandapplications/index.html>) stellen online eine aktuelle Liste mit den für ihre Normen relevanten Patenten bereit. Anwender werden ermutigt, sich diese Liste anzusehen, um die aktuellsten Informationen hinsichtlich Patenten zu erhalten.

1 Anwendungsbereich

Dieser Teil von IEC 61784-3 (alle Teile) 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. Sie stellt die Grundsätze der funktional sicheren Kommunikation nach IEC 61784-3 fest, die für diese Sicherheitskommunikationsschicht wichtig sind. Diese Sicherheitskommunikationsschicht ist für die ausschließliche Implementierung in Sicherheitsgeräten vorgesehen.

ANMERKUNG 1 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.

Dieses Dokument legt Mechanismen fest für die Übertragung von sicherheitsrelevanten Nachrichten zwischen Teilnehmern in einem verteilten Netzwerk unter Verwendung von Feldbus-Technologie in Übereinstimmung mit IEC 61508 (alle Teile)⁴⁾ für funktionale Sicherheit. Diese Mechanismen dürfen in verschiedenen Industrieanwendungen verwendet werden, wie Prozesssteuerung, Fertigungsautomatisierung und Maschinen.

Dieses Dokument enthält Leitlinien sowohl für Entwickler als auch Gutachter von entsprechenden 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 diesem Dokument in einem Standardgerät reicht nicht aus, um es als Sicherheitsgerät zu qualifizieren.

3 Begriffe, Symbole, Abkürzungen und Konventionen

3.2 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach IEC 61784-3 und die folgenden Begriffe.

ISO und IEC stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

- IEC Electropedia: verfügbar unter <http://www.electropedia.org/>
- ISO-Online-Rechercheplattform: verfügbar unter <http://www.iso.org/obp>

ANMERKUNG Kursive Schrift wird in den Definitionen verwendet, um Begriffe zu markieren, die selbst 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 Netzelemente sind Repeater und Switches

⁴⁾ In den nachfolgenden Seiten dieser Norm bedeutet „IEC 61508“ stets „IEC 61508 (alle Teile)“.

[QUELLE: IEC 61918:2018, 3.1.2]

3.1.1.2

Verfügbarkeit

(en: availability)

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

3.1.1.3

Bitfehlerwahrscheinlichkeit

(en: bit error probability)

Pe

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

3.1.1.4

Black Channel

(en: 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

zyklische Redundanzprüfung

(en: Cyclic Redundancy Check)

CRC

<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 [29],[30]⁵⁾.

⁵⁾ Die Zahlen in eckigen Klammern verweisen auf die Literaturhinweise.

3.1.1.9

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

3.1.1.10

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 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]

3.1.1.11

expliziter Code

(en: explicit code)

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

3.1.1.12

explizite Daten

(en: explicit data)

übertragene Daten

Anmerkung 1 zum Begriff: Explizite Daten werden als Gegensatz zu impliziten Daten definiert.

3.1.1.13

Ausfall

Versagen

(en: failure)

Beendigung der Fähigkeit einer Funktionseinheit, eine geforderte Funktion bereitzustellen 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]

3.1.1.14

Fehler

(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 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]

3.1.1.15

Feldbus

(en: fieldbus)

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

3.1.1.16

Feldbussystem

(en: fieldbus system)

System mit einem *Feldbus* und angeschlossenen Geräten

3.1.1.17

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: [29][30]

3.1.1.18

funktional sicheres Kommunikationsprofil

(en: functional safety communication profile)

FSCP

Technikspezifikation für die Implementierung eines SCL

3.1.1.19

Hash-Funktion

(en: hash function)

(mathematische) Funktion, die Werte aus einem (möglicherweise sehr) großen Wertebereich in einem (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.

3.1.1.20

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

3.1.1.21

impliziter Code

(en: implicit code)

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

3.1.1.22

implizite Daten

(en: implicit data)

zusätzliche Daten, die nicht übertragen werden, dem Sender und dem Empfänger aber bekannt sind und zur Codierung und Decodierung der Nachricht/SPDU verwendet werden

Anmerkung 1 zum Begriff: Implizite Daten werden als Gegensatz zu expliziten Daten definiert.

[QUELLE: IEC 62280:2014, 3.1.25, modifiziert – Ergänzung von „und zur Codierung und Decodierung der Nachricht/SPDU verwendet werden“]

3.1.1.23

Master

(en: master)

aktive Kommunikationseinheit, die Kommunikationsaktivitäten anderer Stationen, seien es Master oder Slaves, einleiten und planen kann

3.1.1.24

Nachricht

(en: message)

<Informationstheorie und Kommunikationstheorie> geordnete Zeichenfolge (in der Regel Oktetts), die zur Beförderung von Informationen vorgesehen ist

[QUELLE: ISO/IEC 2382:2015, 2123205, modifiziert – „(in der Regel Oktetts)“ eingefügt, Anmerkungen und Quelle gestrichen]

3.1.1.25

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.

3.1.1.26

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 bringen 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 durch Ersatz von vier Anmerkungen durch eine andere]

3.1.1.27

Performance Level

(en: performance level)

PL

diskreter Level, der die Fähigkeit von sicherheitsbezogenen Teilen einer Steuerung spezifiziert, eine Sicherheitsfunktion unter vorhersehbaren Bedingungen auszuführen

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

3.1.1.28

Schutzkleinspannung

(en: protective extra-low-voltage)

PELV

auf Schutz Erde bezogener elektrischer Stromkreis, in dem die Spannung folgende Werte nicht überschreiten kann:

UNTER NORMALEN BEDINGUNGEN und EINZELFEHLERBEDINGUNGEN: Die Wechselspannungspegel betragen 30 V Effektivwert bzw. 42,4 V Spitzenwert und der Gleichspannungspegel beträgt 60 V. Bei Betriebsmitteln für eine Anwendung an FEUCHTEN ORTEN betragen die Wechselspannungspegel 16 V Effektivwert bzw. 22,6 V Spitzenwert und der Gleichspannungspegel beträgt 35 V

[QUELLE: IEC 61010-2-201:2017: 3.111, modifiziert – „Stromkreis“ aus dem Begriff und Quelle gestrichen]

3.1.1.29

Redundanz

(en: redundancy)

Vorhandensein von mehr als einem Mittel zum Ausführen einer geforderten Funktion oder zur Darstellung von Informationen

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

3.1.1.30

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 62059-11:2002, 3.17, modifiziert – „automatisiertes System“ verwendet, zwei Anmerkungen hinzugefügt]

3.1.1.31

Restfehlerwahrscheinlichkeit

(en: residual error probability)

RP

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

3.1.1.32

Restfehlerrate

(en: residual error rate)

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

3.1.1.33

Risiko

(en: risk)

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

Anmerkung 1 zum Begriff: Für die 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]

3.1.1.34

Sicherheitskommunikationskanal

(en: safety communication channel)

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.

3.1.1.35

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

3.1.1.36

sichere Verbindung

(en: safety connection)

Verbindung, welche das Sicherheitsprotokoll für Kommunikationstätigkeiten nutzt

3.1.1.37

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.

3.1.1.38

Sicherheitsgerät

(en: safety device)

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

3.1.1.39

Sicherheitskleinspannung

(en: safety extra-low-voltage)

SELV

nicht mit der Schutzterde verbundener elektrischer Stromkreis, in dem die Spannung folgende Werte nicht überschreiten kann:

UNTER NORMALEN BEDINGUNGEN und EINZELFEHLERBEDINGUNGEN: Die Wechselspannungspegel betragen 30 V Effektivwert bzw. 42,4 V Spitzenwert und der Gleichspannungspegel beträgt 60 V. Bei Betriebsmitteln für eine Anwendung an feuchten Orten betragen die Wechselspannungspegel 16 V Effektivwert bzw. 22,6 V Spitzenwert und der Gleichspannungspegel beträgt 35 V

[QUELLE: IEC 61010-2-201:2017: 3.112, modifiziert – „Stromkreis“ aus dem Begriff und Quelle gestrichen]

3.1.1.40

Sicherheitsfunktion

(en: safety function)

Funktion, die von einem sicherheitsbezogenen E/E/PE-System oder anderen risikomindernden Maßnahmen ausgeführt wird und dazu vorgesehen ist, unter Berücksichtigung eines festgelegten gefährlichen Vorfalls einen sicheren Zustand für die EUC zu erreichen oder aufrechtzuerhalten

[QUELLE: IEC 61508-4:2010, 3.5.1, modifiziert – Verweisungen und Beispiel entfernt]

3.1.1.41

Reaktionszeit einer Sicherheitsfunktion

(en: safety function response time)

SFRT

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

Anmerkung 1 zum Begriff: Dieses Konzept wird in IEC 61784-3:—, 5.2.4 eingeführt und von den in diesem Dokument aufgeführten Kommunikationsprofilen für funktional sichere Übertragung verwendet.

3.1.1.42

Sicherheits-Integritätslevel

(en: safety integrity level)

SIL

(eine von vier möglichen) diskrete(n) Stufen, die einem Wertebereich der Sicherheitsintegrität entsprechen, wobei der Sicherheits-Integritätslevel 4 die höchste Stufe der Sicherheitsintegrität und der Sicherheits-Integritätslevel 1 die niedrigste darstellt

Anmerkung 1 zum Begriff: Die Ausfallgrenzen (siehe IEC 61508-4:2010, 3.5.17) für die vier Sicherheits-Integritätslevel sind in IEC 61508-1:2010, Tabellen 2 und 3, festgelegt.

Anmerkung 2 zum Begriff: Sicherheits-Integritätslevel werden eingesetzt zur Festlegung der Anforderungen an die Sicherheitsintegrität von Sicherheitsfunktionen von E/E/PE-sicherheitsbezogenen Systemen.

Anmerkung 3 zum Begriff: Ein Sicherheits-Integritätslevel (SIL) ist nicht Attribut eines Systems, Subsystems, Elements oder einer Komponente. Die richtige Interpretation der Aussage „SIL n sicherheitsbezogenes System“ (wobei n 1, 2, 3 oder 4 sein kann) ist die, dass das System potenziell in der Lage ist, Sicherheitsfunktionen mit einem Sicherheits-Integritätslevel bis n zu unterstützen.

[QUELLE: IEC 61508-4:2010, 3.5.8]

3.1.1.43

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 zum Begriff: In der Praxis werden mehrere Sicherheitsmaßnahmen kombiniert, um den geforderten Sicherheits-Integritätslevel zu erzielen.

Anmerkung 2 zum Begriff: Kommunikationsfehler und zugehörige Sicherheitsmaßnahmen sind ausführlich in IEC 61784-3:—, 5.3 und 5.4 beschrieben.

3.1.1.44

Sicherheits-PDU

(en: safety PDU)

SPDU

durch einen Sicherheitskommunikationskanal übertragene PDU

Anmerkung 1 zum Begriff: Die SPDU kann mehr als eine Kopie der sicheren Daten unter Nutzung unterschiedlicher Codierungsstrukturen und Hash-Funktionen, zusammen mit eindeutigen Teilen zusätzlichen Schutzes wie Schlüssel, fortlaufenden Nummern oder einem Zeitstempel, beinhalten.

Anmerkung 2 zum Begriff: Redundante SCLs können zwei unterschiedliche Versionen der SPDU in getrennten Feldern der Feldbus-DLPDU vorsehen.

Anmerkung 3 zum Begriff: Im Sinne von CP 3/4 bis 3/6 ist sie die APDU Anwendungsprotokoll-Dateneinheit.

3.1.1.45

sicherheitsbezogene Anwendung

(en: safety-related application)

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

3.1.1.46

sicherheitsbezogenes System

(en: safety-related system)

System, welches *Sicherheitsfunktionen* nach IEC 61508 ausführt

3.1.1.47

Slave

(en: slave)

Kommunikationseinheit, die Nachrichten empfangen und sie als Antwort an andere Kommunikationseinheiten senden kann, die Master oder Slave sein dürfen

3.1.1.48

unberechtigte Auslösung

(en: spurious trip)

Auslösung in einem Sicherheitssystem ohne Prozessanforderung

3.1.1.49

Gleichverteilung

(en: uniform distribution)

Verteilungsfunktion, bei der sämtliche Werte einer endlichen Menge gleich wahrscheinlich auftreten

Anmerkung 1 zum Begriff: Für ein Bitfeld der Länge i beträgt die Auftrittswahrscheinlichkeit eines bestimmten Feldwertes 2^{-i} , da die Summe aller Auftrittswahrscheinlichkeiten 1 sein muss.

3.1.2 CPF 3: Zusätzliche Begriffe

3.1.2.1

Adresstyp

(en: Address Type)

Adresstyp 1, wenn nur F_DestAdd überprüft wird

Adresstyp 2, wenn F_SourceAdd gemeinsam mit der F_DestAdd überprüft wird

3.1.2.2

Bit

(en: bit)

Binärziffer

(en: binary digit)

verschlüsselte Binärinformation ohne eine technische Einheit

3.1.2.3

Codename

(en: codename)

Kennung der Sicherheitskommunikationsbeziehung zwischen Sicherheitskommunikations-Peers.

Der Codename wird für die eindeutige Identifizierung der Sicherheitskommunikationsbeziehung verwendet.

Der Codename besteht aus F_Source_Address und F_Dest_Address

Anmerkung 1 zum Begriff: Beispiel für die *Verbindungsauthentizität* wie in IEC 61784-3 beschrieben.

3.1.2.4

Konfiguration

(en: configuration)

Festlegung der standardmäßigen Kommunikationsverbindungen und Kommunikationsparameter für Buseinheiten einer bestimmten Anwendung

Anmerkung 1 zum Begriff: Die Konfiguration für eine sichere Kommunikation umfasst die Festlegung der sicheren Verbindungen und F-Parameter für sicherheitsbezogene Buseinheiten einer bestimmten sicherheitsbezogenen Anwendung.

3.1.2.5

CPD-Tool

(en: CPD-Tool)

zugehöriges Programm in Service-Rechnern, das mit dem Feldbus zum Zweck der Konfiguration, Parametrisierung und Diagnose bestimmter Feldgeräte verbunden ist

3.1.2.6

Zyklus

(en: cycle)

Intervall, in dem eine Liste von Anweisungen oder eine Aktivität wiederholt und ununterbrochen ausgeführt wird

3.1.2.7

Gerätezugangspunkt

(en: device access point)

DAP

Element, das verwendet wird, um ein modulares E/A-Gerät als Einheit zu adressieren

Anmerkung 1 zum Begriff: Üblicherweise als Kopfstation bezeichnet.

Anmerkung 2 zum Begriff: Diese Anmerkung ist nur für die französischsprachige Fassung relevant.

3.1.2.8

Geräterückmeldungszeit

(en: device acknowledgement time)

DAT

benötigte Zeit in einem IO-Gerät für das Starten des Empfangs einer Sicherheits-PDU mit einer neuen *MonitoringNumber* im Gerätezugangspunkt bis zu dem Zeitpunkt, an dem die entsprechende Sicherheits-PDU als Antwort generiert und an den Gerätezugangspunkt zurückgegeben wurde

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

3.1.2.9

Treiber

(en: driver)

Softwaremodul, das für die Abstraktion der Hardware in Bezug auf die restliche Anwendungssoftware verwendet wird

3.1.2.10

ausfallsicher

(en: fail-safe)

F

Fähigkeit eines Systems, Gefährdungen bei entsprechenden technischen oder organisatorischen Maßnahmen entweder deterministisch oder indem das Risiko auf ein toleriertes Maß verringert wird, zu verhindern

Anmerkung 1 zum Begriff: Entspricht der funktionalen Sicherheit.

3.1.2.11

ausfallsichere Werte

(en: fail-safe values)

FV

Werte, die anstelle von Prozesswerten ausgegeben werden, wenn die Sicherheitsfunktion auf einen ausfallsicheren Zustand festgelegt wurde

Anmerkung 1 zum Begriff: In diesem Dokument müssen die ausfallsicheren Werte (FV) immer auf „0“ festgelegt werden.

Anmerkung 2 zum Begriff: Diese Anmerkung ist nur für die französischsprachige Fassung relevant.

3.1.2.12

ausfallsicherer Zustand

(en: fail-safe state)

Betriebsmodus einer Sicherheitsfunktion oder eines Endelements (Aktor), in dem Gefährdungen bei entsprechenden technischen Maßnahmen entweder deterministisch oder indem das Risiko auf ein toleriertes Maß verringert wird, verhindert werden

Anmerkung 1 zum Begriff: In Abhängigkeit von der bestimmten Sicherheitsfunktion stellt das Abschalten möglicherweise nicht die einzige Möglichkeit für einen ausfallsicheren Zustand dar.

3.1.2.13

F-Host-Kanaltreiber

(en: F-Host channel driver)

Treiber innerhalb der F-Hosts nach den FSCP 3/1-Spezifikationen zur Repräsentation von F-E/A-Daten im F-Host-Anwendungsprogramm

3.1.2.14

F-Gerät

(en: F-Device)

Der Begriff F-Gerät in vorhergehenden Versionen dieses Profils wird durch „F-Gerät-Treiber“ ersetzt

3.1.2.15

F-Gerät-Treiber

(en: F-Device)

Software zur Verwaltung von Sicherheits-PDU innerhalb von F- (Sub-) Modulen nach den FSCP 3/1-Spezifikationen, ausgelöst durch den F-Host-Treiber für den Datenaustausch

3.1.2.16

F-Treiber

(en: F-Driver)

Software zur Verwaltung der Sicherheits-PDUs als F-Host- oder F-Gerät-Treiber nach den FSCP 3/1-Spezifikationen

3.1.2.17

F-Host

(en: F-Host)

Datenverarbeitungseinheit, die das FSCP 3/1-Protokoll ausführen kann und die den Black Channel bedient

Anmerkung 1 zum Begriff: Dies ist üblicherweise in einem PLC oder IPC mit einem entsprechenden Betriebssystem implementiert.

3.1.2.18

F-Host-Treiber

(en: F-Host driver)

Software zur Verwaltung der Sicherheits-PDUs in F-Hosts nach den FSCP 3/1-Spezifikationen

3.1.2.19

F- (Sub-) Modul

(en: F-(Sub)Module)

Kommunikations-Peer innerhalb eines modularen E/A-Slave oder E/A-Geräts, das in der Lage ist, das Protokoll CP 3/1 oder CP 3/4 bis CP 3/6 auszuführen. Das F- (Sub-) Modul enthält den F-Device-Treiber

Anmerkung 1 zum Begriff: Hierbei handelt es sich üblicherweise um ein sicherheitsbezogenes Eingabe- oder Ausgabemodul.

3.1.2.20

F-Slave

(en: F-Slave)

CP 3/1- oder CP 3/2-Kommunikations-Peer, der das FSCP 3/1-Protokoll ausführen kann und der üblicherweise von dem F-Host für den Datenaustausch aktiviert wird

3.1.2.21

Fehlreaktion

(en: fault reaction)

Angabe einer Kommunikationsfehlfunktion durch Setzen der Fehlerbits im Status-Byte und einer entsprechenden automatischen sicheren Reaktion innerhalb der Komponenten

Anmerkung 1 zum Begriff:

Innerhalb einer F-Ausgabe: Abschalten der Ausgabegeräte und/oder automatische sichere Reaktion der Aktoreinheit.

Innerhalb einer F-CPU: Entsprechende Reaktion des Anwendungsprogramms möglich. F-E/A-Daten sind auf ausfallsichere Werte festzulegen.

Innerhalb einer F-Eingabe: Bei Kommunikationsfehlern, die durch die F-Eingabe ermittelt wurden:

Fehlerbits werden im Status-Byte gesetzt.

Bei Kommunikationsfehlern, die durch den F-Host ermittelt wurden:

F-Eingabedaten sind auf ausfallsichere Werte festzulegen.

3.1.2.22

Funktionsblock

(en: function block)

FB

eigenständiger Programmteil mit besonderer Funktionalität

Anmerkung 1 zum Begriff: Diese Anmerkung gilt nur für die französische Sprachfassung.

3.1.2.23

Hostrückmeldungszeit

(en: host acknowledgement time)

HAT

Zeit, die in einem F-Host für das Starten des Empfangs einer Sicherheits-PDU mit einer bestimmten *MonitoringNumber* bis zu dem Zeitpunkt, an dem die entsprechende Sicherheits-PDU mit einer inkrementierten *MonitoringNumber* generiert und an den Master bzw. E/A-Controller zurückgegeben wurde, benötigt wird

Anmerkung 1 zum Begriff: Diese Anmerkung gilt nur für die französische Sprachfassung.

3.1.2.24

E/A-Controller

(en: IO-Controller)

aktive Kommunikationseinheit, die CP 3/4- bis CP 3/6-Kommunikationsaktivitäten anderer Einheiten, seien es E/A-Controller oder E/A-Geräte, einrichten und festlegen kann

Anmerkung 1 zum Begriff: Im CP 3/1 entspricht diese Task einem Master Klasse 1.

Anmerkung 2 zum Begriff: Die E/A-Controller-Schnittstelle wird nach IEC 61158-5-10 als FSPMCTL bezeichnet.

3.1.2.25

E/A-Gerät

(en: IO-Device)

Kommunikationseinheit, die Nachrichten empfangen und sie als Antwort an eine andere CP 3/4- bis CP 3/6-Kommunikationseinheit, sei es ein E/A-Controller oder ein anderes E/A-Gerät, senden kann

Anmerkung 1 zum Begriff: Im CP 3/1 entspricht diese Task einem Slave.

Anmerkung 2 zum Begriff: Die E/A-Geräte-Schnittstelle wird nach IEC 61158-5-10 als FSPMDEV bezeichnet.

3.1.2.26

E/A-Modul

(en: IO-Module)

adressierbare untergeordnete Eingabe/Ausgabe-Einheit in einem modularen E/A-Gerät

3.1.2.27

E/A-Supervisor

(en: IO-Supervisor)

Engineering-Station, die Daten aus einem E/A-Gerät lesen und auf ein E/A-Gerät schreiben kann

Anmerkung 1 zum Begriff: Ein E/A-Supervisor wird zu Installations- und Diagnosezwecken verwendet. Im Gegensatz zu einem E/A-Controller übernimmt der E/A-Supervisor keine aktive Rolle während des Hochfahrens eines E/A-Systems. Ein E/A-Supervisor ist nicht Teil des E/A-Systems.

3.1.2.28

E/A-System

(en: IO-System)

E/A-Controller und die zugehörigen E/A-Geräte

3.1.2.29

iParameter

individuelle oder technologiespezifische Parameter für F- (Sub-) Module

Anmerkung 1 zum Begriff: Typische iParameter sind die Koordinaten der Schutzzone eines Laserscanners.

3.1.2.30

iPar-Server

(en: iPar-Server)

genormter Mechanismus, mit dem individuelle oder technologiespezifische Parameter für F- (Sub-) Module im Standardteil eines F-Hosts oder seines gesteuerten Teilsystems gespeichert und abgerufen werden können

3.1.2.31

Master (Klasse 1)

(en: master (class 1))

aktiver CP 3/1-Kommunikations-Peer, der Slaves für den Datenaustausch aktiviert

Anmerkung 1 zum Begriff: Der Begriff „Master“ allein wird als Kurzform für „Master (Klasse 1)“ benutzt.

3.1.2.32

MonitoringNumber

(en: MonitoringNumber)

MNR

Mittel zur Sicherung der Authentizität und der richtigen Reihenfolge der übertragenen sicheren PDUs

Anmerkung 1 zum Begriff: Beispiel für die *laufende Nummer* wie in IEC 61784-3 beschrieben.

Anmerkung 2 zum Begriff: Die MonitoringNumber wird über die übertragene CRC-Signatur gesichert.

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

3.1.2.33

Prozesswerte

(en: process values)

PV

Eingabe- und Ausgabedaten (in einer Sicherheits-PDU), die für die Steuerung eines automatisierten Prozesses erforderlich sind

Anmerkung 1 zum Begriff: Diese Anmerkung gilt nur für die französische Sprachfassung.

3.1.2.34

Wertstatus

(en: qualifier)

zusätzliche kennzeichnende Bits in *Prozesswerten*, die den Status jeder individuellen Eingabe angeben

3.1.2.35

Erhaltende Codename-Auswahl

Die erhaltende Codename-Auswahl ist der erhaltend im F- (Sub-) Modul gespeicherte Codename oder ein Teil davon.

3.1.2.36

gemeinsame E/A

(en: shared I/O)

Eingaben und Ausgaben in Feldgeräten, auf die über mehrere Controller zugegriffen werden kann

Anmerkung 1 zum Begriff: Obwohl gemeinsame E/A in CP 3/4 bis CP 3/6 zulässig ist, ist sie im FSCP 3/1 nicht erlaubt.

3.1.2.37

Toggle-Bit

(en: toggle bit)

ein Bit des Control- und Status-Bytes, das die (virtuellen) *MonitoringNumber* sowohl im F-Host-Treiber als auch im F-Gerät-Treiber synchronisiert

3.1.2.38

USB

(en: universal serial bus)

externer Busstandard

Anmerkung 1 zum Begriff: USB ersetzt serielle und parallele Computerports und wird für schnelle Direktverbindungen zwischen Service-Rechnern und Feldgeräten verwendet.

Anmerkung 2 zum Begriff: Diese Anmerkung ist nur für die französischsprachige Fassung relevant.

3.1.2.39

V2-Modus

(en: V2-mode)

FSCP 3/1-Dienste und Protokoll nach diesem Dokument

3.2 Symbole und Abkürzungen

3.2.1 Allgemeine Symbole und Abkürzungen

BSC	binärsymmetrischer Kanal (en: Binary Symmetric Channel)	
CP	Kommunikationsprofil (en: Communication Profile)	[IEC 61784-1/2]
CPF	Kommunikationsprofilfamilie (en: Communication Profile Family)	[IEC 61784-1/2]
CRC	zyklische Redundanzprüfung (en: Cyclic Redundancy Check)	
DLL	Sicherungsschicht (en: Data Link Layer)	
DLPDU (en: Data Link Protocol Data Unit)	Protokolldateneinheit der Sicherungsschicht (en: Data Link Protocol Data Unit)	
EMC	elektromagnetische Verträglichkeit	
EMI	elektromagnetische Störung (en: Electromagnetic Interference)	

E DIN EN IEC 61784-3-100:2021-04

EUC	Prüfling (en: equipment under control)	[IEC 61508-4:2010]
E/E/PE	elektrisch/elektronisch/programmierbar elektronisch (en: Electrical/Electronic/Programmable Electronic)	[IEC 61508-4:2010]
FAL	Feldbusanwendungsschicht (en: Fieldbus Application Layer)	[IEC 61158-5]
FCS	Blockprüfzeichenfolge (en: Frame Check Sequence)	
FIT	Ausfälle je Zeiteinheit (10 ⁻⁹ Ausfälle je h) (en: Failure In Time)	
FS	funktionale Sicherheit (en: Functional Safety)	
FSCP	funktional sicheres Kommunikationsprofil (en: Functional Safety Communication Profile)	
IACS	industrielles Automatisierungs- und Steuerungssystem (en: Industrial Automation and Control System)	
MTBF	mittlere Zeit zwischen Ausfällen (en: Mean Time Between Failures)	
MTTF	mittlere Zeit bis zu einem Ausfall (en: Mean Time To Failure)	
NSR	nicht-sicherheitsbezogen (en: Non Safety Related)	
PDU	Protokolldateneinheit (en: Protocol Data Unit)	[ISO/IEC 7498-1]
PELV	Schutzkleinspannung (en: Protective Extra Low Voltage)	
PFD	mittlere Wahrscheinlichkeit eines gefahrbringenden Ausfalls bei Anforderung (en: Average probability of dangerous Failure on Demand)	[IEC 61508-4:2010]
PFH	mittlere Häufigkeit eines gefahrbringenden Ausfalls je Stunde [h ⁻¹]	[IEC 61508-4:2010]
PhL	Bitübertragungsschicht (en: Physical Layer)	[ISO/IEC 7498-1]
PL	Performance Level	[ISO 13849-1]
PLC	speicherprogrammierbare Steuerung (en: Programmable Logic Controller)	
RP	Restfehlerwahrscheinlichkeit (en: Residual Error Probability)	
SCL	Sicherheitskommunikationsschicht (en: Safety Communication Layer)	
SELV	Sicherheitskleinspannung (en: Safety Extra Low Voltage)	
SIL	Sicherheits-Integritätslevel (en: safety integrity level)	[IEC 61508-4:2010]
SIS	sicherheitstechnische Systeme (en: Safety Instrumented Systeme)	
SL	Security-Level	[IEC 62443]

SMS	Managementsystem für IT-Sicherheit (en: Security Management System)	[IEC 62443]
SPDU	Sicherheits-PDU (en: Safety PDU)	
SR	sicherheitsbezogen (en: Safety Related)	

3.2.2 CPF 3: Zusätzliche Symbole und Abkürzungen

AES-CCMP	Advanced Encryption Standard – Counter Mode with Cipher Block Chaining Message Authentication Code Protocol	
AP	Anwendungsprozess (en: application process)	
API	Anwendungsprozesskennung (en: application process identifier)	
AR	Anwendungsbeziehung (en: application relationship)	
ASE	Anwendungsdienstelement (en: application service element)	
ASIC	anwendungsspezifischer integrierter Schaltkreis (en: application specific integrated circuit)	
C	Abdeckung (en: coverage)	
CGP	kanalgranulare Passivierung (en: channel-granular passivation)	
DR	Dynamische Rekonfiguration (en: dynamic reconfiguration)	
CP 3/1	Kommunikationsprofil, allgemein bekannt als PROFIBUS DP ⁶⁾	
CP 3/2	Kommunikationsprofil, allgemein bekannt als PROFIBUS PA	
CP 3/4 bis CP 3/6	Kommunikationsprofil, allgemein bekannt als PROFINET	
CPU	Zentrale Recheneinheit (en: central processing unit)	
CR	Kommunikationsbeziehung (en: communication relationship)	
CRC_FP	Startwert der 16-Bit-CRC2 des F-Host (über F-Parameter = F_Par_CRC)	
CRC_FP+	32-Bit-CRC-Wert über F-Parameter	
DAP (en: device access point)	Gerätezugangspunkt (en: device access point)	
DAT (en: device acknowledge ment time)	Geräterückmeldungszeit (en: device acknowledgment time)	
DP	Dezentralisierte Peripheriegeräte (en: decentralized peripherals)	

⁶⁾ Zur Angabe von Handelsnamen siehe Abschnitt 4.

E DIN EN IEC 61784-3-100:2021-04

F	Kennung für Sicherheitselemente (ausfallsicher, funktional sicher)	
FB	Funktionsblock (en: function block)	
FV	ausfallsichere Werte (en: fail-safe values)	
GSD	Allgemeine Stationsbeschreibung (dem Gerät zugeordnete Datei) (en: general station description)	
GSDL	Allgemeine Stationsbeschreibungssprache (für CP 3/1- und CP 3/2-Geräte) (en: general station description language)	
GSDML	Allgemeine Stationsbeschreibungs-Auszeichnungssprache (für CP 3/4- bis CP 3/6-Geräte) (en: general station description markup language)	
HAT	Hostrückmeldungszeit (en: host acknowledgment time)	
HD	Hamming-Distanz	
E/A	Eingang/Ausgang (en: input/output)	
LED	lichtemittierende Diode (en: light emitting diode)	
LIV	letzter Eingabewert (en: last input value)	
LOV	letzter Ausgabewert (en: last output value)	
MNR	MonitoringNumber	
PA	Prozessautomation (en: process automation)	
Pe	Bitfehlerwahrscheinlichkeit (en: bit error probability)	
PN	PROFINET = CP 3/4 bis CP 3/6	
PiR	Parametrisierung im Lauf (en: parameterization in run)	
PV	Prozesswerte (en: process values)	
SFRT	Reaktionszeit einer Sicherheitsfunktion (en: safety function response time)	
RADIUS	Einwahl-Benutzerdienst zur Fernauthentifizierung (en: remote authentication dial in user service)	
S	<i>Norm (en: standard)</i>	
TPF	Temporäre Parameterdatei (XML-Datei) (en: temporary parameter file)	
UML	Unified Modeling Language	[46]
USB	Universal Serial Bus	[51]
WCDT	Worst-Case-Verzögerungszeit (en: Worst Case Delay Time)	
WDTIME	Watchdog-Zeit (en: watchdog time)	
XML	eXtensible Markup Language	[48], [49], [50]

E DIN EN IEC 61784-3-8

0.2 Patentangaben

Die Internationale Elektrotechnische Kommission (IEC) weist darauf hin, dass die Übereinstimmung mit diesem Dokument die Verwendung von Patenten hinsichtlich FSCP 8/2 in Abschnitt 12, wie folgt, bedeuten kann:

JP 2012-533784 US 13/821733 DE 112010005881.4 KR 10-2013-7006469 CN 201080069108.6	[MEC]	Communication apparatus and delay detecting method
--	-------	--

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. Informationen sind erhältlich bei:

[MEC]	Mitsubishi Electric Corporation Corporate Licensing Division 2-7-3 Marunouchi, Chiyoda-ku Tokyo 100-8310 Japan
-------	---

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können, ohne dass diese vorstehend identifiziert wurden. 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 Normenreihe IEC 61784-3 legt eine Sicherheitsschicht (Dienste und Protokoll) fest, die auf der Kommunikationsprofilfamilie 8 der IEC 61784-1, IEC 61784-2 und IEC 61158, Typ 18 und Typ 23, beruht. Sie stellt die Grundsätze der funktional sicheren Kommunikation nach IEC 61784-3 fest, die für diese Sicherheitskommunikationsschicht wichtig sind. Diese Sicherheitskommunikationsschicht ist für die ausschließliche Implementierung in Sicherheitsgeräten vorgesehen.

ANMERKUNG 1 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.

Dieser Teil⁷⁾ legt Mechanismen fest für die Übertragung von sicherheitsrelevanten Nachrichten zwischen Teilnehmern in einem verteilten Netzwerk unter Verwendung von Feldbus-Technologie in Übereinstimmung mit der Normenreihe IEC 61508⁷⁾ für funktionale Sicherheit. Diese Mechanismen dürfen in verschiedenen Industrieanwendungen verwendet werden, wie Prozesssteuerung, Fertigungsautomatisierung und Maschinen.

Dieser Teil enthält Leitlinien sowohl für Entwickler als auch Gutachter von entsprechenden 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 diesem Teil 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 Begriffe nach IEC 61784-3 und die folgenden Begriffe.

ISO und IEC stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

- IEC Electropedia: verfügbar unter <http://www.electropedia.org/>
- ISO-Online-Rechercheplattform: verfügbar unter <http://www.iso.org/obp>

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

3.1.1 Allgemeine Begriffe

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

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

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

⁷⁾ In den nachfolgenden Seiten dieses Dokuments bedeutet „IEC 61508“ stets „IEC 61508 (alle Teile)“.

3.1.1.2

aktives Netzelement

(en: active network element)

Netzelement, das aktive elektrische und/oder aktive optische Komponenten zur Erweiterung des Netzes enthält

Anmerkung 1 zum Begriff: Beispiele für aktive Netzelemente sind Repeater und Switches

[QUELLE: IEC 61918:2013, 3.1.2]

3.1.1.3

Verfügbarkeit

(en: availability)

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

3.1.1.4

Bitfehlerwahrscheinlichkeit

(en: bit error probability)

Pe

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

3.1.1.5

Black Channel

(en: 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.

3.1.1.6

Bridge

abstraktes Gerät, welches auf der Ebene der Sicherungsschicht mehrere Netzwerksegmente verbindet

3.1.1.7

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 62280:2014, 3.1.6, modifiziert – Übertragung ersetzt durch Kommunikation]

3.1.1.8

Kommunikationskanal

(en: communication channel)

logische Verbindung zwischen zwei Endpunkten in einem Kommunikationssystem

3.1.1.9

Kommunikationssystem

(en: communication system)

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

3.1.1.10

Verbindung

(en: connection)

logische Verbindung zwischen zwei Anwendungsobjekten in demselben oder in unterschiedlichen Geräten

3.1.1.11

zyklische Redundanzprüfung

(en: Cyclic Redundancy Check)

CRC

<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: [29][30]⁸⁾ Siehe auch [20], [21].

3.1.1.12

definiertes Kommunikationssystem

(en: defined communication system)

definierter Kanal

(en: defined channel)

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

3.1.1.13

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]

3.1.1.14

Abweichung

(en: error)

Nichtübereinstimmung zwischen Rechenergebnissen, beobachteten oder gemessenen Werten oder Beschaffenheiten und den betreffenden wahren, spezifizierten oder theoretisch richtigen Werten oder Beschaffenheiten

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

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

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

3.1.1.15

Ausfall

(en: failure)

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

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

⁸⁾ Zahlen in rechteckigen Klammern beziehen sich auf die Literaturhinweise.

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

3.1.1.16

Fehler

(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 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]

3.1.1.17

Feldbus

(en: fieldbus)

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

3.1.1.18

Feldbussystem

(en: fieldbus system)

System mit einem Feldbus und angeschlossenen Geräten

3.1.1.19

DLPDU

DEPRECATED: frame

Data Link Protocol Data Unit

3.1.1.20

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 [29][30]

3.1.1.21

Hash-Funktion

(en: hash function)

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

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

Anmerkung 2 zum Begriff: Gebräuchliche Hash-Funktionen sind Paritätsbit, Prüfsummen oder CRC.

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

3.1.1.22

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

3.1.1.23

Master

(en: master)

aktive Kommunikationseinheit, die Kommunikationsaktivitäten anderer Stationen, seien es Master oder Slaves, einleiten und planen kann

3.1.1.24

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]

3.1.1.25

Nachrichtensenke

(en: message sink)

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

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

3.1.1.26

Nachrichtenquelle

(en: message source)

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

[QUELLE: ISO/IEC 2382-16:1996, 16.02.2002]

3.1.1.27

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.

3.1.1.28

Performance Level

(en: performance level)

PL

diskreter Level, der die Fähigkeit von sicherheitsbezogenen Teilen einer Steuerung spezifiziert, eine Sicherheitsfunktion unter vorhersehbaren Bedingungen auszuführen

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

3.1.1.29

Redundanz

(en: redundancy)

Vorhandensein von mehr als einem Mittel zum Ausführen einer geforderten Funktion oder zur Darstellung von Informationen

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

3.1.1.30

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, modifiziert – Format angepasst]

3.1.1.31

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 62059-11:2002, 3.17, modifiziert – „automatisiertes System“ verwendet, zwei Anmerkungen hinzugefügt]

3.1.1.32

Restfehlerwahrscheinlichkeit

(en: residual error probability)

RP

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

3.1.1.33

Restfehlerrate

(en: residual error rate)

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

3.1.1.34

Risiko

(en: risk)

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

Anmerkung 1 zum Begriff: Für die 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]

3.1.1.35

Sicherheitskommunikationskanal

(en: safety communication channel)

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.

3.1.1.36

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.

3.1.1.37

sichere Verbindung

(en: safety connection)

Verbindung, welche das Sicherheitsprotokoll für Kommunikationstätigkeiten nutzt

3.1.1.38

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.

3.1.1.39

Sicherheitsgerät

(en: safety device)

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

3.1.1.40

Sicherheitskleinspannung

(en: safety extra-low-voltage)

SELV

electrical circuit in which the voltage cannot exceed a.c. 30 V r.m.s., 42,4 V peak or d.c. 60 V in normal and single-*fault* condition, including earth *faults* in other circuits

Anmerkung 1 zum Begriff: Ein SELV-Stromkreis ist nicht mit der Schutz Erde verbunden.

[QUELLE: IEC 61131-2:2007, 3.59]

3.1.1.41

Sicherheitsfunktion

(en: safety function)

Funktion, die von einem sicherheitsbezogenen E/E/PE-System oder anderen risikomindernden Maßnahmen ausgeführt wird und dazu vorgesehen ist, unter Berücksichtigung eines festgelegten gefährlichen Vorfalls einen sicheren Zustand für die EUC zu erreichen oder aufrechtzuerhalten

[QUELLE: IEC 61508-4:2010, 3.5.1, modifiziert – Verweisungen und Beispiel entfernt]

3.1.1.42

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 Sicherheitsaktors erreicht wurde unter Berücksichtigung von gleichzeitig auftretenden *Fehlern* und *Ausfällen* in der *Sicherheitsfunktion*

Anmerkung 1 zum Begriff: Dieses Konzept wird in IEC 61784-3:—, 5.2.4 eingeführt und von den in diesem Normteil aufgeführten Kommunikationsprofilen für funktional sichere Übertragung verwendet.

3.1.1.43

Sicherheits-Integritätslevel

(en: safety integrity level)

SIL

eine von vier diskreten Stufen, die einem Wertebereich der Sicherheitsintegrität entsprechen, wobei der Sicherheits-Integritätslevel 4 die höchste Stufe der Sicherheitsintegrität und der Sicherheits-Integritätslevel 1 die niedrigste darstellt

Anmerkung 1 zum Begriff: Die Ausfallgrenzen (siehe IEC 61508-4:2010, 3.5.17) für die vier Sicherheits-Integritätslevel sind in IEC 61508-1:2010, Tabellen 2 und 3, festgelegt.

Anmerkung 2 zum Begriff: Sicherheits-Integritätslevel werden zur Festlegung der Anforderungen an die Sicherheitsintegrität der Sicherheitsfunktionen, die dem sicherheitsbezogenen E/E/PE-System zugeordnet werden, verwendet.

Anmerkung 3 zum Begriff: Ein Sicherheits-Integritätslevel (SIL) ist keine Eigenschaft eines Systems, Teilsystems, Elements oder Bauteils. Die richtige Interpretation der Aussage „SIL n *sicherheitsbezogenes System*“ (wobei n 1, 2, 3 oder 4 sein kann) ist die, dass das System potenziell in der Lage ist, *Sicherheitsfunktionen* mit einem Sicherheits-Integritätslevel bis n zu unterstützen.

[QUELLE: IEC 61508-4:2010, 3.5.8]

3.1.1.44

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 zum Begriff: In der Praxis werden mehrere Sicherheitsmaßnahmen kombiniert, um den geforderten Sicherheits-Integritätslevel zu erzielen.

Anmerkung 2 zum Begriff: Kommunikationsfehler und zugehörige Sicherheitsmaßnahmen sind ausführlich in IEC 61784-3:—, 5.3 und 5.4 beschrieben.

3.1.1.45

Sicherheits-PDU

(en: safety PDU)

SPDU

durch einen Sicherheitskommunikationskanal übertragene PDU

Anmerkung 1 zum Begriff: Die SPDU kann mehr als eine Kopie der *sicheren Daten* unter Nutzung unterschiedlicher Codierungsstrukturen und *Hash-Funktionen*, zusammen mit eindeutigen Teilen zusätzlichen Schutzes wie Schlüssel, fortlaufenden Nummern oder einem *Zeitstempel*, beinhalten.

Anmerkung 2 zum Begriff: Redundante SCLs können zwei unterschiedliche Versionen der SPDU in getrennten Feldern der Feldbus-DLPDU vorsehen.

3.1.1.46

sicherheitsbezogene Anwendung

(en: safety-related application)

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

3.1.1.47

sicherheitsbezogenes System

(en: safety-related system)

System, welches *Sicherheitsfunktionen* nach IEC 61508 ausführt

3.1.1.48

Slave

(en: slave)

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

3.1.1.49

unberechtigte Auslösung

(en: spurious trip)

Auslösung in einem Sicherheitssystem ohne Prozessanforderung

3.1.1.50

Aktualitätscode

(en: Timeliness code)

Zeitinformation in einer Nachricht

3.1.1.51

Gleichverteilung

(en: uniform distribution)

Verteilungsfunktion, bei der sämtliche Werte einer endlichen Menge gleich wahrscheinlich auftreten

Anmerkung 1 zum Begriff: Für ein Bitfeld der Länge i beträgt die Auftrittswahrscheinlichkeit eines bestimmten Feldwertes 2^{-i} , da die Summe aller Auftrittswahrscheinlichkeiten 1 sein muss.

3.1.1.52

White Channel

(en: white channel)

festgelegtes Kommunikationssystem, bei dem alle relevanten Hardware- und Softwareelemente nach IEC 61508 entworfen, implementiert und geprüft sind

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

3.1.2 CPF 8: Zusätzliche Begriffe

3.1.2.1

Zyklus

(en: cycle)

Intervall, in dem eine Aktivität wiederholt und fortlaufend ausgeführt wird

3.1.2.2

Sicherheitsanwendungsbeziehung

(en: safety application relationship)

SAR

Anwendungsbeziehung zwischen zwei oder mehreren Beziehungsendpunkten sicherheitsbezogener Anwendungen

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

3.1.2.3

Sicherheitsanwendungsbeziehung

(en: safety application service element)

SASE

Serviceelement einer sicherheitsbezogenen Anwendung

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

3.1.2.4

Sicherheitsuhr

(en: safety clock)

Uhr (Zähler) zum Aufzeichnen des Zeitpunkts des Auftretens von Ereignissen, wie der Übertragung und des Empfangs von sicherheitskommunikationsbezogenen Nachrichten

3.1.2.5

Zeitschalter für Sicherheitsdatenüberwachung

(en: safety data monitor timer)

Zeitschalter, der von der Zeiterwartungsfunktion für die Übertragung von Sicherheitsdaten verwendet wird

3.1.2.6

Zeitschalter für Sicherheitsüberwachung

(en: safety monitor timer)

Zeitschalter, der von der Zeiterwartungsfunktion für die Verwaltung der sicheren Verbindung verwendet wird

3.1.2.7

sicherheitsbezogene Aktualisierung

(en: safety refresh)

regelmäßige Übertragung und Empfang von Sicherheitsdaten zwischen Master- und Slave-Stationen.

3.1.2.8

Slot

(en: slot)

Menge (Granularität) der positionsabhängigen Zuordnung der zyklischen Datenfelder

3.1.2.9

Station

(en: station)

Gerät und die entsprechenden SAREPs, die für die Übertragung und den Empfang von Sicherheitsdaten vorgesehen sind

Anmerkung 1 zum Begriff: Die Nummer der Station wird in der positionsabhängigen Zuordnung der zyklischen Datenfelder verwendet (eine Station belegt einen oder mehrere Slots).

3.1.2.10

Übertragungsinformation des Sicherheitsprotokolls

(en: safety protocol transmission information)

Information, die sicherheitsbezogene Nachrichten voneinander unterscheidet

3.2 Symbole und Abkürzungen

3.2.1 Allgemeine Symbole und Abkürzungen

A-code	Authentication code	
CP	Kommunikationsprofil (en: Communication Profile)	[IEC 61784-1]
CPF	Kommunikationsprofilfamilie (en: Communication Profile Family)	[IEC 61784-1]
CRC	zyklische Redundanzprüfung (en: Cyclic Redundancy Check)	
DLL	Sicherungsschicht (en: Data Link Layer)	[ISO/IEC 7498-1]
DLPDU (en: Data Link Protocol Data Unit)	Protokolldateneinheit der Sicherungsschicht (en: Data Link Protocol Data Unit)	
EMC	elektromagnetische Verträglichkeit	
EUC	Prüfling (en: equipment under control)	[IEC 61508-4:2010]
E/E/PE	elektrisch/elektronisch/programmierbar elektronisch (en: Electrical/Electronic/Programmable Electronic)	[IEC 61508-4:2010]
FAL	Feldbusanwendungsschicht (en: Fieldbus Application Layer)	[IEC 61158-5]

E DIN EN IEC 61784-3-100:2021-04

FS	funktionale Sicherheit (en: Functional Safety)	
FSCP	funktional sicheres Kommunikationsprofil (en: Functional Safety Communication Profile)	
FSPM	FAL Service Protocol Machine	[IEC 61158-1]
MTBF	mittlere Zeit zwischen Ausfällen (en: Mean Time Between Failures)	
MTTF	mittlere Zeit bis zu einem Ausfall (en: Mean Time To Failure)	
PDU	Protokolldateneinheit (en: Protocol Data Unit)	[ISO/IEC 7498-1]
Pe	Bitfehlerwahrscheinlichkeit (en: bit error probability)	
PhL	Bitübertragungsschicht (en: Physical Layer)	[ISO/IEC 7498-1]
PL	Performance Level	[ISO 13849-1]
PLC	speicherprogrammierbare Steuerung (en: Programmable Logic Controller)	
SCL	Sicherheitskommunikationsschicht (en: Safety Communication Layer)	
SELV	Sicherheitskleinspannung (en: Safety Extra Low Voltage)	
SIL	Sicherheits-Integritätslevel (en: safety integrity level)	[IEC 61508-4:2010]
SPDU	Sicherheits-PDU (en: Safety PDU)	
T-code	Aktualitätscode (en: Timeliness code)	

3.2.2 CPF 8: Zusätzliche Symbole und Abkürzungen

AR	Anwendungsbeziehung (en: application relationship)
ASE	Anwendungsdienstelement (en: application service element)
CC	Carry Counter
CID	Verbindungskennung (en: connection identifier)
CMD	(en: command data)
LED	lichtemittierende Diode
LID	(en: link identifier)
OBL	Offset Baseline
RNO	laufende Nummer (en: running number)

SAR	Sicherheitsanwendungsbeziehung (en: safety application relationship)
SAREP	Endpunkt der Sicherheitsanwendungsbeziehung (en: safety application relationship endpoint)
SARPM	Protokollzustandsautomat der Sicherheitsanwendungsbeziehung (en: safety application relationship protocol state machine)
SASE	Dienstelement der Sicherheitsanwendung (en: safety application service element)
SFSPM	Sicherheits-FSPM (angehängter -S-Slave oder -M-Mater)
SRC	(en: safety relevant controller)
SRP	(en: safety relevant peripheral)
TPI	(en: safety transmission packet information)
TPI-T	(en: safety transmission packet information from master)
TPI-R	(en: safety transmission packet information from slave)
TS	Zeitstempel (en: time stamp)

E DIN EN IEC 61784-3-13

0.2 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 Familie 13, bei denen die Bezeichnung [xx] den Halter der Patentrechte angibt:

AT 504739	[BR]	Anordnung und ein Verfahren zur sicheren Datenkommunikation über ein nicht sicheres Netzwerk
DE 102005032877.6	[BR]	Verfahren zur Zeitsynchronisation von Teilnehmern eines Netzwerkes
DE 102004055685.7	[BR]	Verfahren zur Abgrenzung eines sicheren Netzwerkes
DE 102004055684.9	[BR]	Verfahren zur Absicherung des Datentransfers in einem sicheren Netzwerk mit CRC's variabler Länge
EP 1990941 B1	[BR]	Anordnung und ein Verfahren zur sicheren Datenkommunikation über ein nicht sicheres Netzwerk

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

Der Halter dieser Patentrechte hat ISO [und/oder] IEC zugesichert, dass er bereit ist, entweder kostenfrei oder über Lizenzen zu vernünftigen und nicht diskriminierenden Geschäftsbedingungen mit Antragstellern in der ganzen Welt zu verhandeln. In diesem Zusammenhang ist die Erklärung des Halters dieser Patentrechte bei ISO [und/oder] IEC registriert.

Informationen sind erhältlich bei:

[BR] B&R Industrial Automation GmbH
 B&R Strasse 1
 5142 Eggelsberg
 AUSTRIA

 Tel.: +43 7748 6586-0
 Fax.: +43 7748 6586-26

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

CEN (<http://www.cen.eu/cen/WorkArea/IPR/Pages/default.aspx>) und CENELEC (<http://www.cenelec.eu/membersandexperts/toolsandapplications/index.html>) stellen online eine aktuelle Liste mit den für ihre Normen relevanten Patenten bereit. Anwender werden ermutigt, sich diese Liste anzusehen, um die aktuellsten Informationen hinsichtlich Patenten zu erhalten.