

DIN EN IEC 61784-3-3

ICS 35.160; 35.240.50

Ersatz für
DIN EN 61784-3-3:2018-09
Siehe Anwendungsbeginn

**Industrielle Kommunikationsnetze –
Profile –
Teil 3-3: Funktional sichere Übertragung bei Feldbussen –
Zusätzliche Festlegungen für die Kommunikationsprofilfamilie 3
(IEC 61784-3-3:2021);
Englische Fassung EN IEC 61784-3-3:2021**

Industrial communication networks –
Profiles –
Part 3-3: Functional safety fieldbuses – Additional specifications for CPF 3
(IEC 61784-3-3:2021);
English version EN IEC 61784-3-3:2021

Réseaux de communication industriels –
Profils –
Partie 3-3: Bus de terrain de sécurité fonctionnelle –
Spécifications supplémentaires pour CPF 3
(IEC 61784-3-3:2021);
Version anglaise EN IEC 61784-3-3:2021

Gesamtumfang 174 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE

Anwendungsbeginn

Anwendungsbeginn für die von CENELEC am 2021-06-09 angenommene Europäische Norm als DIN-Norm ist 2023-04-01.

Für DIN EN 61784-3-3:2018-09 besteht eine Übergangsfrist bis 2024-06-09.

Nationales Vorwort

Vorausgegangener Norm-Entwurf: E DIN EN IEC 61784-3-100:2021-04.

Dieser Entwurf betrifft auch die in Vorbereitung befindlichen Dokumente DIN EN IEC 61784-3-2, DIN EN IEC 61784-3-8, DIN EN IEC 61784-3-13 und DIN EN IEC 61784-3-18 und wird erst mit Veröffentlichung aller aufgeführten Dokumente zurückgezogen werden.

Für dieses Dokument ist das nationale Arbeitsgremium DKE/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.

Die enthaltene IEC-Publikation wurde vom IEC/SC 65C „Industrial networks“ erarbeitet und unterliegt dem Copyright der IEC .

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

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

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

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

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

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

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

Diese Norm steht nicht in unmittelbarem Zusammenhang mit Rechtsvorschriften und ist nicht als Sicherheitsnorm anzusehen.

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

Änderungen

Gegenüber DIN EN 61784-3-3:2018-09 wurden folgende Änderungen vorgenommen:

- a) redaktionelle Änderungen hinsichtlich der Timeliness, Umwandlung von Kommentaren in der Tabelle in Anweisungen;
- b) Verwendung von Abkürzungen bei PROFINET;
- c) Informationen über Prüfungen und Sicherheitshandbuch für PROFIsafe-Adressen Typ 1 und 2 hinzugefügt;
- d) Hinzufügung von Informationen über PFDavg, Unterstützung von automatischen Tests, Hinzufügung von Diagnosemeldungen;
- e) Erläuterung und Spezifikation von optionalen Statemachines für die Reaktion auf Gerätefehler;
- f) neue optionale Variable „OAD_Nec_C“ für die optionale Funktion „Reaktion auf Gerätefehler in F_Host“;
- g) Spezifikation des optionalen F-Host-Merkmals für „Deaktivierung des F-(Sub)Moduls“;
- h) Festlegung der Anforderungen für FSCP 3/1 und PROFIenergy;
- i) Spezifikation der Anforderungen für mehrere F-Hosts, die mit einem einzigen F-(Sub)Modul kommunizieren; Aktualisierung des Sicherheitshandbuchs;
- j) diverse Fehlerkorrekturen, Korrekturen von Tippfehlern und Aktualisierungen von Referenzen;
- k) aktualisierte Literaturhinweise.

Frühere Ausgaben

DIN EN 61784-3-3: 2008-11, 2012-03, 2018-09

Nationaler Anhang NA (informativ)

Auszugsweise Übersetzung

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

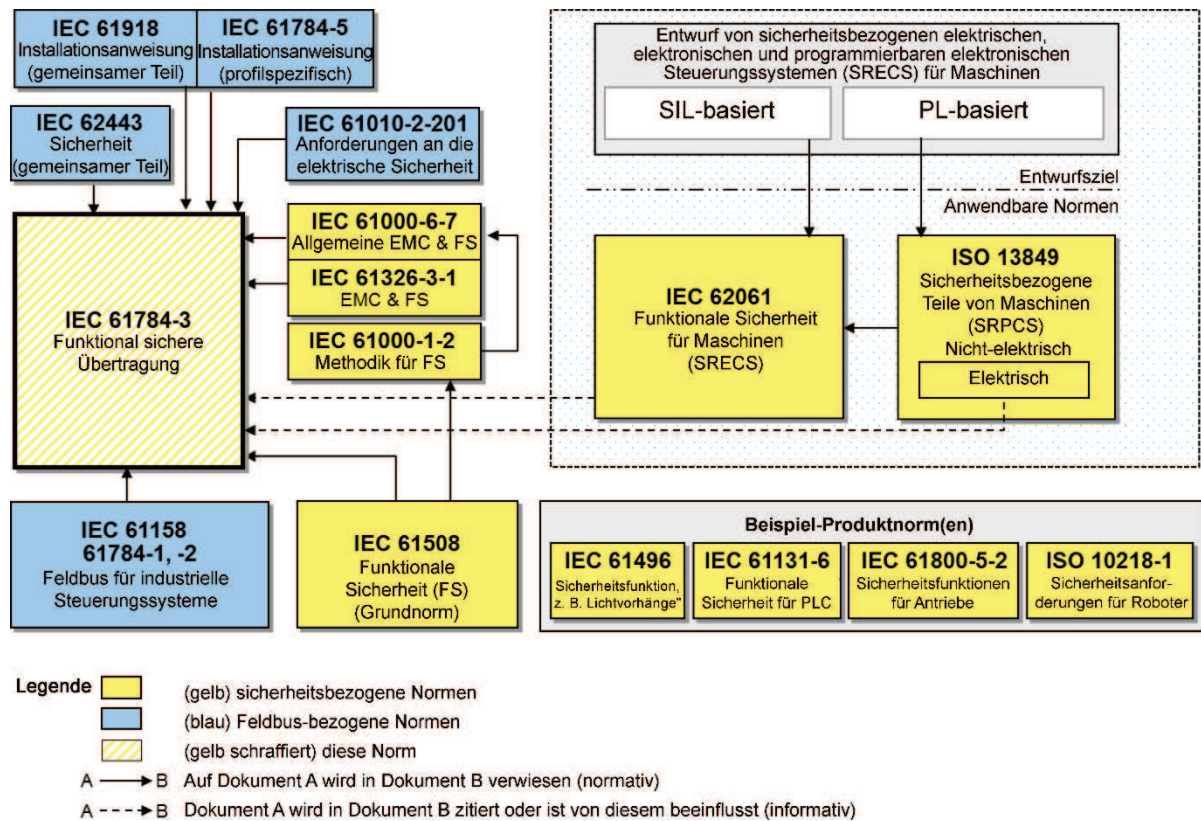
0 Einleitung

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.

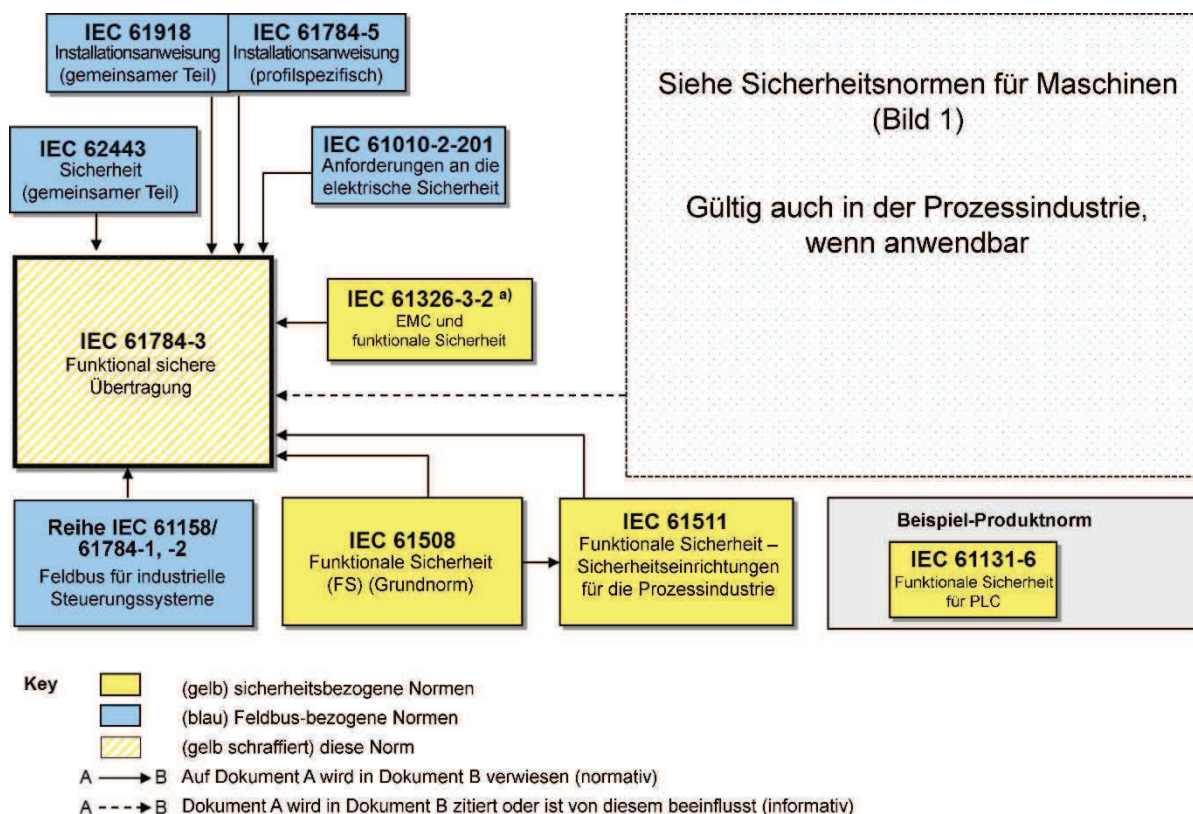
Bild 1 zeigt die Beziehungen zwischen IEC 61784-3 (alle Teile) und den für die Fertigungsautomatisierung relevanten Sicherheits- und Feldbusnormen.



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.

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. 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.

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

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)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 61784-3:2021 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.

[QUELLE: IEC 61918:2018, 3.1.2]

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

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 diesem Dokument verwendet sein, um redundante Daten zu kennzeichnen.

Anmerkung 2 zum Begriff: Siehe auch [29],[30]².

² 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 (alle Teile) auf ein toleriertes Maß reduziert ist durch zum Beispiel Zonen und Durchleitungen

3.1.1.10

DLPDU

DEPRECATED: frame

Data Link Protocol Data Unit

3.1.1.11

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]

3.1.1.12

expliziter Code

en **explicit code**

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

3.1.1.13

explizite Daten

en **explicit data**

übertragene Daten

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

3.1.1.14

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]

3.1.1.15

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]

3.1.1.16

Feldbus

en **fieldbus**

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

3.1.1.17

Feldbussystem

en **fieldbus system**

System mit einem *Feldbus* und angeschlossenen Geräten

3.1.1.18

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]

3.1.1.19

funktional sicheres Kommunikationsprofil

en **functional safety communication profile**

FSCP

Technikspezifikation für die Implementierung eines SCL

3.1.1.20

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.

3.1.1.21

Gefährdung

en **hazard**

potentielle Schadensquelle

Anmerkung 1 zum Begriff: Der Begriff schließt die Gefährdungen von Personen ein, die innerhalb einer kurzen Zeitspanne entstehen (zum Beispiel durch Feuer und Explosion), und auch die, die eine Langzeitwirkung auf die Gesundheit einer Person haben (zum Beispiel durch Freisetzung einer giftigen Substanz).

[QUELLE: IEC 61508-4:2010, 3.1.2, und ISO/IEC Guide 51:2014, Definition 3.2]

3.1.1.22

impliziter Code

en **implicit code**

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

3.1.1.23

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“]

3.1.1.24

Master

en **master**

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

3.1.1.25

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]

3.1.1.26

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**Restfehlerwahrscheinlichkeit**en **residual error probability**

RP

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

3.1.1.31**Restfehlerrate**en **residual error rate**

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

3.1.1.32**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]

3.1.1.33**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.

3.1.1.34**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

3.1.1.35**sichere Verbindung**en **safety connection**

Verbindung, welche das Sicherheitsprotokoll für Kommunikationstätigkeiten nutzt

3.1.1.36**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.

3.1.1.37

Sicherheitsgerät

en **safety device**

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

3.1.1.38

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 Wechsellspannungspegel 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 Wechsellspannungspegel 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]

3.1.1.39

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]

3.1.1.40

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 61784-3:2021, 5.2.4 eingeführt und von den in diesem Dokument aufgeführten Kommunikationsprofilen für funktional sichere Übertragung verwendet.

3.1.1.41

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]

3.1.1.42**Sicherheitsmaßnahme**en **safety measure**

Mittel zur Beherrschung möglicher Kommunikations*fehler*, 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: Kommunikations*fehler* und zugehörige Sicherheitsmaßnahmen sind ausführlich in IEC 61784-3:2021, 5.3 und 5.4 beschrieben.

3.1.1.43**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.

3.1.1.44**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

3.1.1.45**sicherheitsbezogenes System**en **safety-related system**

System, welches *Sicherheitsfunktionen* nach IEC 61508 ausführt

3.1.1.46**Slave**en **slave**

Kommunikationseinheit, die Nachrichten empfangen und sie als Antwort an eine andere Kommunikationseinheit senden kann, die Master oder Slave sein darf, aber nicht um Kommunikationsaktivitäten zu initiieren

3.1.1.47**unberechtigte Auslösung**en **spurious trip**

Auslösung in einem Sicherheitssystem ohne Prozessanforderung

3.1.1.48**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.

Anmerkung 1 zum Begriff: Der Codename wird für die eindeutige Identifizierung der Sicherheitskommunikationsbeziehung verwendet.

Anmerkung 2 zum Begriff: Der Codename besteht aus F_Source_Address und F_Dest_Address

Anmerkung 3 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.

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

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.

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 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.

Anmerkung 1 zum Begriff: Das F-(Sub-) Modul enthält den F-Device-Treiber.

Anmerkung 2 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

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

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 „FAL Dienste des E/A-Controllers“ 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 „FAL Dienste des E/A-Geräts“ 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**en **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.

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

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

en **Retentive Selection of the Codename**

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**externer Busstandard**en **universal serial bus**

USB

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

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	Protokolldateneinheit der Sicherungsschicht (en: Data Link Protocol Data Unit)	
EMC	elektromagnetische Verträglichkeit	
EMI	elektromagnetische Störung (en: Electromagnetic Interference)	
EUC	Prüfling (en: equipment under control)	[IEC 61508-4:2010]
E/E/PE	elektrisch/elektronisch/programmierbar elektronisch Electrical/Electronic/Programmable Electronic)	(en:[IEC 61508-4:2010]
FAL	Feldbusanwendungsschicht (en: Fieldbus Application Layer)	[IEC 61158-5] (alle Teile)
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)	[IEC 61010-2:2011]
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)	[IEC 61010-2-201]
SIL	Sicherheits-Integritätslevel (en: safety integrity level)	[IEC 61508-4:2010]
SIS	sicherheitstechnische Systeme (en: Safety Instrumented Systeme)	
SL	Security-Level	[IEC 62443] (alle Teile)
SMS	Managementsystem für IT-Sicherheit (en: Security Management System)	[IEC 62443] (alle Teile)
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 ³
CP 3/2	Kommunikationsprofil, allgemein bekannt als PROFIBUS PA
CP 3/4 bis CP 3/6	Kommunikationsprofil, allgemein bekannt als PROFINET

³ Zur Angabe von Handelsnamen siehe Abschnitt 4.

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 acknowledgement time)	Geräterückmeldungszeit (en: device acknowledgment time)
DP	Dezentralisierte Peripheriegeräte (en: decentralized peripherals)
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	[43]
USB	Universal Serial Bus	[48]
WCDT	Worst-Case-Verzögerungszeit (en: Worst Case Delay Time)	
WDTime	Watchdog-Zeit (en: watchdog time)	
XML	eXtensible Markup Language	[45], [46], [47]

3.3 Konventionen

In diesem Dokument ist die Abkürzung "F" ein Hinweis auf sicherheitsrelevante Gegenstände, Technologien, Systeme und Einheiten (ausfallsicher, funktional sicher).

In diesem Dokument werden die Standarddaten, die im Falle von Geräteausfällen oder -fehlern verwendet werden sollen, als ausfallsichere Werte (FV) bezeichnet und auf "0" gesetzt.

In diesem Dokument werden die reservierten Bits ("res") im Status/Control Byte und in den F-Parametern auf "0" gesetzt und vom Empfänger ignoriert, um Probleme mit zukünftigen Versionen der FSCP 3/1-Geräte zu vermeiden.

In diesem Dokument wird für jede CRC-Signaturberechnung, die einen "0"-Wert ergibt, stattdessen der Wert "1" verwendet. Einzige Ausnahme siehe 8.1.8.

Die Abkürzung "CP 3/4 bis CP 3/6" umfasst in diesem Dokument die drei Kommunikationsprofile CP 3/4, CP 3/5, und CP 3/6. CP 3/4 bis CP 3/6 ist allgemein als PROFINET bekannt.

In diesem Dokument wird für die Zeichnung der Zustandsdiagramme die UML2-Notation und für die Sequenzdiagramme eine verkürzte Form verwendet [43]. Die Darstellung der Übergangstabellen erfolgt in Anlehnung an die Empfehlungen der IEC 62390.

EUROPEAN STANDARD

EN IEC 61784-3-3

NORME EUROPÉENNE

EUROPÄISCHE NORM

June 2021

ICS 25.040.40; 35.100.05

Supersedes EN 61784-3-3:2017 and all of its
amendments and corrigenda (if any)

English version

**Industrial communication networks – Profiles – Part 3-3:
Functional safety fieldbuses – Additional specifications for CPF 3
(IEC 61784-3-3:2021)**

Réseaux de communication industriels – Profils –
Partie 3-3: Bus de terrain de sécurité fonctionnelle –
Spécifications supplémentaires pour CPF 3
(IEC 61784-3-3:2021)

Industrielle Kommunikationsnetze – Profile – Teil 3-3:
Funktional sichere Übertragung bei Feldbussen – Zusätzliche
Festlegungen für die Kommunikationsprofilfamilie 3
(IEC 61784-3-3:2021)

This European Standard was approved by CENELEC on 2021-06-09. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and the United Kingdom.



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

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

European foreword

The text of document 65C/1083/FDIS, future edition 4 of IEC 61784-3-3, prepared by SC 65C "Industrial networks" of IEC/TC 65 "Industrial-process measurement, control and automation" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN IEC 61784-3-3:2021.

The following dates are fixed:

- latest date by which the document has to be implemented at national level by (dop) 2022-03-09
publication of an identical national standard or by endorsement
- latest date by which the national standards conflicting with the (dow) 2024-06-09
document have to be withdrawn

This document supersedes EN 61784-3-3:2017 and all of its amendments and corrigenda (if any).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CENELEC shall not be held responsible for identifying any or all such patent rights.

Endorsement notice

The text of the International Standard IEC 61784-3-3:2021 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following notes have to be added for the standards indicated:

IEC 60870-5-1	NOTE	Harmonized as EN 60870-5-1
IEC 61000-1-2	NOTE	Harmonized as EN 61000-1-2
IEC 61131-6	NOTE	Harmonized as EN 61131-6
IEC 61158 (series)	NOTE	Harmonized as EN 61158 (series)
IEC 61496 (series)	NOTE	Harmonized as EN IEC 61496 (series)
IEC 61508-1:2010	NOTE	Harmonized as EN 61508-1:2010 (not modified)
IEC 61508-4:2010	NOTE	Harmonized as EN 61508-4:2010 (not modified)
IEC 61508-5:2010	NOTE	Harmonized as EN 61508-5:2010 (not modified)
IEC 61508-6:2010	NOTE	Harmonized as EN 61508-6:2010 (not modified)
IEC 61158-3-3	NOTE	Harmonized as EN 61158-3-3
IEC 61158-4-3	NOTE	Harmonized as EN IEC 61158-4-3
IEC 61158-5 (series)	NOTE	Harmonized as EN 61158-5 (series)
IEC 61784-3 (series)	NOTE	Harmonized as EN 61784-3 (series)
IEC 61784-5 (series)	NOTE	Harmonized as EN IEC 61784-5 (series)
IEC 61800-5-2	NOTE	Harmonized as EN 61800-5-2
IEC 61804 (series)	NOTE	Harmonized as EN IEC 61804 (series)
ISO 10218-1	NOTE	Harmonized as EN ISO 10218-1
ISO 13849 (series)	NOTE	Harmonized as EN ISO 13849 (series)

Annex ZA (normative)

Normative references to international publications with their corresponding European publications

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

NOTE 1 Where an International Publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

NOTE 2 Up-to-date information on the latest versions of the European Standards listed in this annex is available here: www.cenelec.eu.

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
IEC 60204-1	-	Safety of machinery - Electrical equipment of machines - Part 1: General requirements	EN 60204-1	-
IEC 61000-6-7	-	Electromagnetic compatibility (EMC) - Part 6-7: Generic standards - Immunity requirements for equipment intended to perform functions in a safety-related system (functional safety) in industrial locations	EN 61000-6-7	-
IEC 61010-2-201	2017	Safety requirements for electrical equipment for measurement, control, and laboratory use - Part 2-201: Particular requirements for control equipment	EN IEC 61010-2-201	2018
IEC 61158-2	-	Industrial communication networks - Fieldbus specifications - Part 2: Physical layer specification and service definition	EN 61158-2	-
IEC 61158-5-3	-	Industrial communication networks - Fieldbus specifications - Part 5-3: Application layer service definition - Type 3 elements	EN 61158-5-3	-
IEC 61158-5-10	-	Industrial communication networks - Fieldbus specifications - Part 5-10: Application layer service definition - Type 10 elements	EN IEC 61158-5-10	-
IEC 61158-6-3	-	Industrial communication networks - Fieldbus specifications - Part 6-3: Application layer protocol specification - Type 3 elements	EN IEC 61158-6-3	-
IEC 61158-6-10	-	Industrial communication networks - Fieldbus specifications - Part 6-10: Application layer protocol specification - Type 10 elements	EN IEC 61158-6-10	-
IEC 61326-3-1	-	Electrical equipment for measurement, control and laboratory use - EMC requirements - Part 3-1: Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety) – General industrial applications	EN 61326-3-1	-

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
IEC 61326-3-2	-	Electrical equipment for measurement, control and laboratory use - EMC requirements - Part 3-2: Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety) - Industrial applications with specified electromagnetic environment	EN IEC 61326-3-2	-
IEC 61508	series	Functional safety of electrical/electronic/programmable electronic safety-related systems	of EN 61508	series
IEC 61508-2	-	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems (see Functional Safety and IEC 61508)	of EN 61508-2	-
IEC 61511	series	Functional safety - Safety instrumented systems for the process industry sector	EN 61511	series
IEC 61784-1	-	Industrial communication networks - Profiles Part 1: Fieldbus profiles	EN IEC 61784-1	-
IEC 61784-2	-	Industrial communication networks - Profiles - Part 2: Additional fieldbus profiles for real-time networks based on ISO/IEC/IEEE 8802-3	EN IEC 61784-2	-
IEC 61784-3	2021	Industrial communication networks - Profiles - Part 3: Functional safety fieldbuses - General rules and profile definitions	EN IEC 61784-3	2021
IEC 61784-5-3	-	Industrial communication networks – Profiles – Part 5-3: Installation of fieldbuses – Installation profiles for CPF 3	EN IEC 61784-5-3	-
IEC 61918	2018	Industrial communication networks - Installation of communication networks in industrial premises	EN IEC 61918	2018
IEC 62061	-	Safety of machinery - Functional safety of safety-related control systems	EN IEC 62061	-
IEC 62280	2014	Railway applications - Communication, signalling and processing systems - Safety related communication in transmission systems		-
IEC 62443	series	Security for industrial automation and control systems	EN IEC 62443	series
ISO 13849-1	2015	Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design	EN ISO 13849-1	2015
ISO 13849-2	2012	Safety of machinery - Safety-related parts of control systems - Part 2: Validation	EN ISO 13849-2	2012

CONTENTS

European foreword	26
Annex ZA (normative) Normative references to international publications with their corresponding European publications	27
0.1 General.....	37
0.2 Patent declaration	38
1 Scope	40
2 Normative references	40
3 Terms, definitions, symbols, abbreviated terms and conventions	41
3.1 Terms and definitions	41
3.1.1 Common terms and definitions	42
3.1.2 CPF 3: Additional terms and definitions	47
3.2 Symbols and abbreviated terms	51
3.2.1 Common symbols and abbreviated terms.....	51
3.2.2 CPF 3: Additional symbols and abbreviated terms.....	52
3.3 Conventions	54
4 Overview of FSCP 3/1 (PROFIsafe™).....	54
5 General.....	57
5.1 External documents providing specifications for the profile	57
5.2 Safety functional requirements	57
5.3 Safety measures	57
5.4 Safety communication layer structure	58
5.4.1 Principle of FSCP 3/1 safety communications.....	58
5.4.2 CPF 3 communication structures.....	60
5.5 Relationships with FAL (and DLL, PhL)	62
5.5.1 Device model	62
5.5.2 Application and communication relationships.....	63
5.5.3 Data types.....	63
6 Safety communication layer services.....	64
6.1 F-Host driver services	64
6.2 F-Device driver services.....	67
6.3 Diagnosis	69
6.3.1 Safety alarm generation	69
6.3.2 F-(Sub)Module safety layer diagnosis.....	69
7 Safety communication layer protocol	71
7.1 Safety PDU format	71
7.1.1 Safety PDU structure.....	71
7.1.2 Safety IO data.....	71
7.1.3 Status and Control Byte	71

7.1.4	(Virtual) MonitoringNumber	73
7.1.5	(Virtual) MNR mechanism (F_CRC_Seed=0)	74
7.1.6	(Virtual) MNR mechanism (F_CRC_Seed=1)	75
7.1.7	CRC2 Signature (F_CRC_Seed=0).....	76
7.1.8	CRC2 Signature (F_CRC_Seed=1).....	78
7.1.9	Non-safety IO data.....	79
7.2	FSCP 3/1 behavior.....	79
7.2.1	General.....	79
7.2.2	F-Host driver state diagram	79
7.2.3	F-Device driver state diagram	84
7.2.4	F-Device driver restart.....	88
7.2.5	Sequence diagrams	88
7.2.6	Timing diagram for a MonitoringNumber reset.....	95
7.2.7	Monitoring of safety times	95
7.3	Reaction in the event of a malfunction	98
7.3.1	Corruption of safety data	98
7.3.2	Unintended repetition	98
7.3.3	Incorrect sequence	99
7.3.4	Loss.....	99
7.3.5	Unacceptable delay	99
7.3.6	Insertion.....	99
7.3.7	Masquerade.....	99
7.3.8	Addressing.....	99
7.3.9	Out-of-sequence	100
7.3.10	Loop-back.....	100
7.3.11	Network boundaries and router	100
7.4	F-Startup and parameter change at runtime	101
7.4.1	Standard startup procedure.....	101
8	Safety communication layer management	101
8.1	F-Parameter	101
8.1.1	Summary	101
8.1.2	F_Source/Destination_Address (Codename).....	102
8.1.3	F_WD_Time (F-Watchdog time).....	102
8.1.4	F_WD_Time_2 (secondary F-Watchdog time).....	103
8.1.5	F_Prm_Flag1 (Parameters for the safety layer management).....	103
8.1.6	F_Prm_Flag2 (Parameters for the safety layer management).....	105
8.1.7	F_iPar_CRC (value of iPar_CRC across iParameters)	107
8.1.8	F_Par_CRC calculation (across F-Parameters).....	107
8.1.9	Structure of the F-Parameter record data object	108

8.2	iParameter and iPar_CRC	108
8.3	Safety parameterization	109
8.3.1	Objectives	109
8.3.2	GSDL and GSDML safety extensions	110
8.3.3	Securing safety parameters and GSD data	112
8.4	Safety configuration	116
8.4.1	Order of IO data types	116
8.4.2	Securing the safety IO data description	117
8.4.3	Dataltem data type section examples	118
8.5	Data type information usage	122
8.5.1	F-Host Channel driver	122
8.5.2	Rules for standard F-Host Channel drivers	123
8.5.3	Recommendations for the use of F-Host Channel drivers	124
8.6	Safety parameter assignment mechanisms	125
8.6.1	F-Parameter assignment	125
8.6.2	General iParameter assignment	125
8.6.3	System integration requirements for iParameterization tools	125
8.6.4	iPar-Server	127
9	System requirements	138
9.1	Indicators and switches	138
9.2	Installation guidelines	138
9.3	Safety function response time	138
9.3.1	Model	138
9.3.2	Calculation and optimization	140
9.3.3	Adjustment of watchdog times for FSCP 3/1	142
9.3.4	Engineering tool support	143
9.3.5	Retries (repetition of messages)	143
9.4	Duration of demands	144
9.5	Constraints for the calculation of system characteristics	144
9.5.1	Probabilistic considerations	144
9.5.2	Safety related assumptions	146
9.5.3	Non safety related constraints (availability)	147
9.6	Maintenance	147
9.6.1	F-(Sub)Module commissioning / replacement	147
9.6.2	Identification and maintenance functions	147
9.7	Safety manual	148
9.8	Wireless transmission channels	149
9.8.1	Black channel approach	149
9.8.2	Availability	149

9.8.3	Security measures	149
9.8.4	Stationary and mobile applications	150
9.9	Relationship between functional safety and security	150
9.10	Conformance classes.....	150
10	Assessment.....	152
10.1	Safety policy	152
10.2	Obligations.....	152
Anhang A (informative)	Additional information for functional safety communication profiles of CPF 3.....	153
A.1	Hash function calculation	153
A.2	Example values for MonitoringNumbers (MNR).....	157
Anhang B (informative)	Information for assessment of the functional safety communication profiles of CPF 3	158
Anhang C (normative)	Optional features	159
C.1	Reaction on Device_Fault in F-Host	159
C.1.1	Situation	159
C.1.2	Documentation for the user	159
C.1.3	Optional extensions of F-Host driver Transition Table.....	159
C.1.4	Recommendation for the case without Extensions of F-Host driver Transitions	162
C.1.4.1	Required behavior in relation to F-Device driver and application	162
C.1.4.2	Prevent unintentional restart by application measures	162
C.2	Optional extensions of F-Host driver to "Disable F-(Sub)Module".....	163
C.3	Combination of "Disable F-(Sub)Module" and "reaction on Device_Fault"	166
C.4	FSCP 3/1 and PROFIenergy	169
C.4.1	Use of FSCP 3/1-Devices with PROFIenergy	169
C.4.2	Sequence in case of PROFIenergy power off on	169
C.5	Requirement multiple F-Hosts communicate with single F-(Sub)Module	169
C.6	FSCP 3/1 PiR	170
Bibliography		171
Figure 1 – Relationships of IEC 61784-3 with other standards (machinery).....		37
Figure 2 – Relationships of IEC 61784-3 with other standards (process)		38
Figure 3 – Basic communication preconditions for FSCP 3/1		55
Figure 4 – Structure of an FSCP 3/1 safety PDU.....		55
Figure 5 – Safety communication on CPF 3		56
Figure 6 – Standard CPF 3 transmission system.....		59
Figure 7 – Safety layer architecture.....		60
Figure 8 – Basic communication layers		60
Figure 9 – Crossing network borders with routers.....		61
Figure 10 – Complete safety transmission paths		62
Figure 11 – IO Device model.....		63

Figure 12 – FSCP 3/1 communication structure.....	64
Figure 13 – F application interface of F-Host driver instances	65
Figure 14 – Motivation for "Channel-related Passivation"	66
Figure 15 – F-Device driver interfaces.....	68
Figure 16 – Safety PDU for CPF 3	71
Figure 17 – Status Byte.....	72
Figure 18 – Control Byte	72
Figure 19 – The Toggle Bit function.....	73
Figure 20 – MonitoringNumber integration.....	74
Figure 21 – F-Host driver CRC2 signature generation (F_CRC_Seed=0)	77
Figure 22 – Details of the CRC2 signature calculation (F_CRC_Seed=0)	77
Figure 23 – CRC2 signature calculation (F_CRC_Seed=1).....	78
Figure 24 – Details of the CRC2 signature calculation (F_CRC_Seed=1)	78
Figure 25 – Safety layer communication relationship	79
Figure 26 – F-Host driver state diagram	80
Figure 27 – F-Device driver state diagram.....	84
Figure 28 – Interaction F-Host driver / F-Device driver during start-up	89
Figure 29 – Interaction F-Host driver / F-Device driver during F-Host power off > on.....	90
Figure 30 – Interaction F-Host driver / F-Device driver with delayed power on	91
Figure 31 – Interaction F-Host driver / F-Device driver during power off → on.....	92
Figure 32 – Interaction while F-Host driver recognizes CRC error.....	93
Figure 33 – Interaction while F-Device driver recognizes CRC error	94
Figure 34 – Impact of the MNR reset signal.....	95
Figure 35 – Monitoring the message transit time F-Host ↔ F-(Sub)Module	96
Figure 36 – Extended watchdog time on request	98
Figure 37 – Effect of F_WD_Time_2	103
Figure 38 – F_Prm_Flag1	103
Figure 39 – F_Check_iPar	104
Figure 40 – F_SIL	104
Figure 41 – F_CRC_Length	105
Figure 42 – F_CRC_Seed.....	105
Figure 43 – F_Prm_Flag2	106
Figure 44 – F_Passivation.....	106
Figure 45 – F_Block_ID	106
Figure 46 – F_Par_Version	107
Figure 47 – F-Parameter	108
Figure 48 – iParameter block	109
Figure 49 – F-Parameter extension within the GSDML specification	111
Figure 50 – F_Par_CRC signature including iPar_CRC	112

Figure 51 – F-Host Channel driver as "glue" between F-(Sub)Module and application program	123
Figure 52 – Layout example of an F-Host Channel driver	124
Figure 53 – F-Parameter assignment for F-(Sub)Modules	125
Figure 54 – System integration of CPD-Tools.....	127
Figure 55 – iPar-Server mechanism (commissioning).....	128
Figure 56 – iPar-Server mechanism (for example F-(Sub)Module replacement)	129
Figure 57 – iPar-Server request coding ("status model").....	130
Figure 58 – Coding of SR_Type.....	131
Figure 59 – iPar-Server request coding ("alarm model").....	132
Figure 60 – iPar-Server state diagram.....	135
Figure 61 – Example safety function with a critical response time path	139
Figure 62 – Simplified typical response time model	139
Figure 63 – Frequency distributions of typical response times of the model	140
Figure 64 – Context of delay times and watchdog times	141
Figure 65 – Timing sections forming the FSCP 3/1 F_WD_Time	142
Figure 66 – Frequency distribution of response times with message retries	143
Figure 67 – Residual error probabilities for the 24-bit CRC polynomial	144
Figure 68 – Residual error probabilities for the 32-bit CRC polynomial	145
Figure 69 – Monitoring of corrupted messages.....	146
Figure A.1 – Typical "C" procedure of a cyclic redundancy check.....	153
Figure C.1 – F-Host driver application interface with feature Reaction on Device_Fault	159
Figure C.2 – F-Host driver application interface with feature Disable F-(Sub)Module	163
Figure C.3 – Timing diagram to use Disable F-(Sub)Module.....	164
Table 1 – Deployed measures to master errors	57
Table 2 – Data types for FSCP 3/1.....	63
Table 3 – F_MessageTrailer for FSCP 3/1	63
Table 4 – Safety layer diagnosis messages.....	69
Table 5 – Buffer entry on CRC2 error.....	70
Table 6 – MonitoringNumber of an F-Host driver SPDU	74
Table 7 – MonitoringNumber of an F-Device driver SPDU	75
Table 8 – MonitoringNumber of an F-Host driver SPDU	75
Table 9 – MonitoringNumber of an F-Device driver SPDU	75
Table 10 – Definition of terms used in F-Host driver state diagram	80
Table 11 – F-Host driver states and transitions.....	81
Table 12 – Definition of terms used in Figure 27.....	85
Table 13 – F-Device driver states and transitions	85

Table 14 – SIL monitor times.....	97
Table 15 – Safety network boundaries	101
Table 16 – Codename octet order	102
Table 17 – Allowed combinations of F_CRC_Seed and F_Passivation	105
Table 18 – GSDL keywords for F-Parameters and F-IO structures	110
Table 19 – Algorithm to build CRC0	113
Table 20 – GSD example in GSDL notation.....	114
Table 21 – GSD example in GSDML notation.....	115
Table 22 – Serialized octet stream for the examples.....	115
Table 23 – Order of IO data types	117
Table 24 – IO data structure items	117
Table 25 – DataItem section for F_IN_OUT_1	119
Table 26 – DATA_STRUCTURE_CRC for F_IN_OUT_1	119
Table 27 – DataItem section for F_IN_OUT_2.....	120
Table 28 – DATA_STRUCTURE_CRC for F_IN_OUT_2.....	120
Table 29 – DataItem section for F_IN_OUT_5.....	121
Table 30 – DATA_STRUCTURE_CRC for F_IN_OUT_5.....	121
Table 31 – DataItem section for F_IN_OUT_6.....	122
Table 32 – DATA_STRUCTURE_CRC for F_IN_OUT_6.....	122
Table 33 – Sample F-Host Channel drivers	123
Table 34 – Requirements for iParameterization	126
Table 35 – Specifier for the iPar-Server Request.....	130
Table 36 – Structure of the Read_RES_PDU ("read record").....	133
Table 37 – Structure of the Write_REQ_PDU ("write record")	133
Table 38 – Structure of the Pull_RES_PDU ("Pull")	133
Table 39 – Structure of the Push_REQ_PDU ("Push").....	134
Table 40 – iPar-Server states and transitions	136
Table 41 – iPar-Server management measures.....	137
Table 42 – Definition of terms in Figure 69	146
Table 43 – Information to be included in the safety manual.....	148
Table 44 – F-Host conformance class requirements	150
Table 45 – Main characteristics of protocol versions.....	151
Table 46 – F-Host driver / F-Device driver conformance matrix.....	152
Table A.1 – The table "Crctab24" for 24 bit CRC signature calculations	153
Table A.2 – The table "Crctab32" for 32 bit CRC signature calculations	155
Table A.3 – The table "Crctab16" for 16 bit CRC signature calculations	156
Table A.4 – Values of CN_incrNR_64 and MNR for F-Host PDU	157
Table C.1 – Definition of additional terms used in driver transitions.....	160

Table C.2 – F-Host driver transitions – added with reaction on Device_Fault160

Table C.3 – Prevent unintentional restart by application measures162

Table C.4 – F-Host driver transitions – with feature Disable F-(Sub)Module.....164

Table C.5 – F-Host driver transitions – added with "reaction on Device_Fault" and "Disable F-(Sub)Module"166

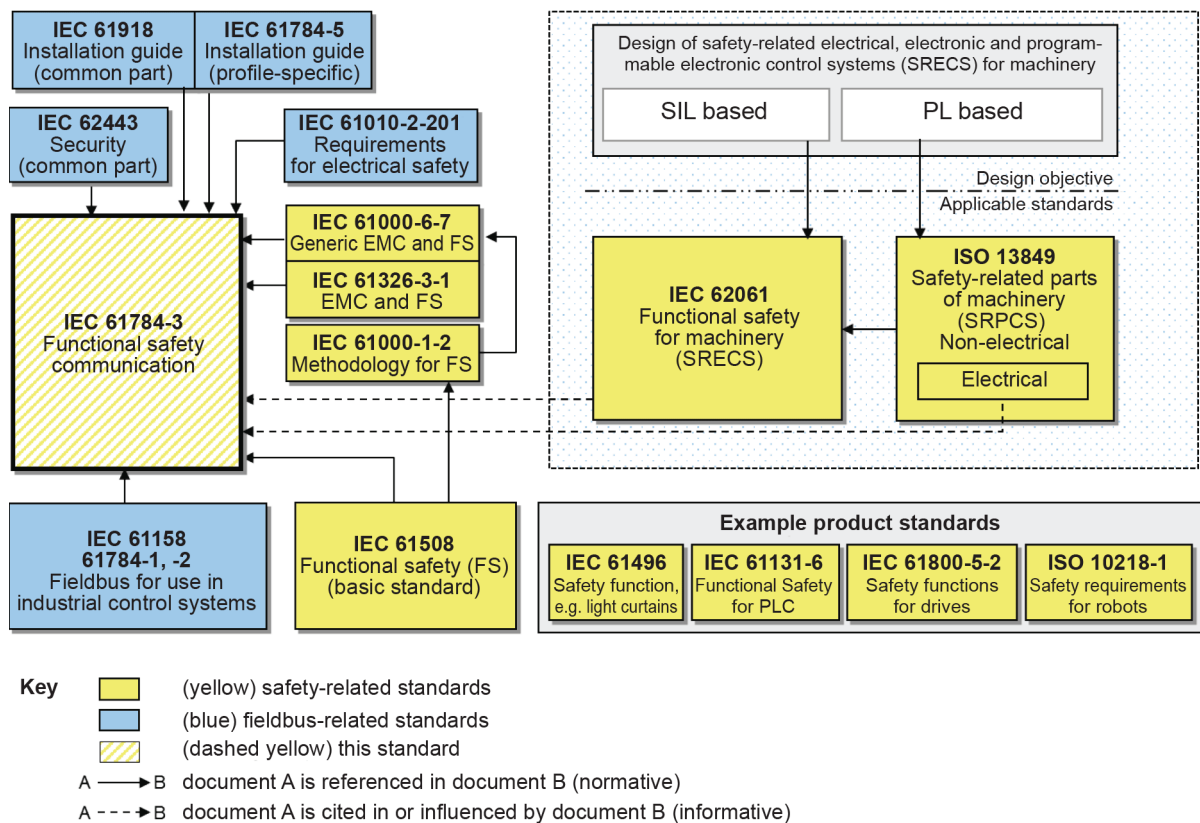
0 Introduction

0.1 General

The IEC 61158 (all parts) fieldbus standard together with its companion standards IEC 61784-1 and IEC 61784-2 defines a set of communication protocols that enable distributed control of automation applications. Fieldbus technology is now considered well accepted and well proven. Thus fieldbus enhancements continue to emerge, addressing applications for areas such as real time and safety-related applications.

IEC 61784-3 (all parts) explains the relevant principles for functional safety communications with reference to IEC 61508 (all parts) and specifies several safety communication layers (profiles and corresponding protocols) based on the communication profiles and protocol layers of IEC 61784-1, IEC 61784-2 and IEC 61158 (all parts). It does not cover electrical safety and intrinsic safety aspects. It also does not cover security aspects nor does it provide any requirements for security.

Figure 1 shows the relationships between IEC 61784-3 (all parts) and relevant safety and fieldbus standards in a machinery environment.

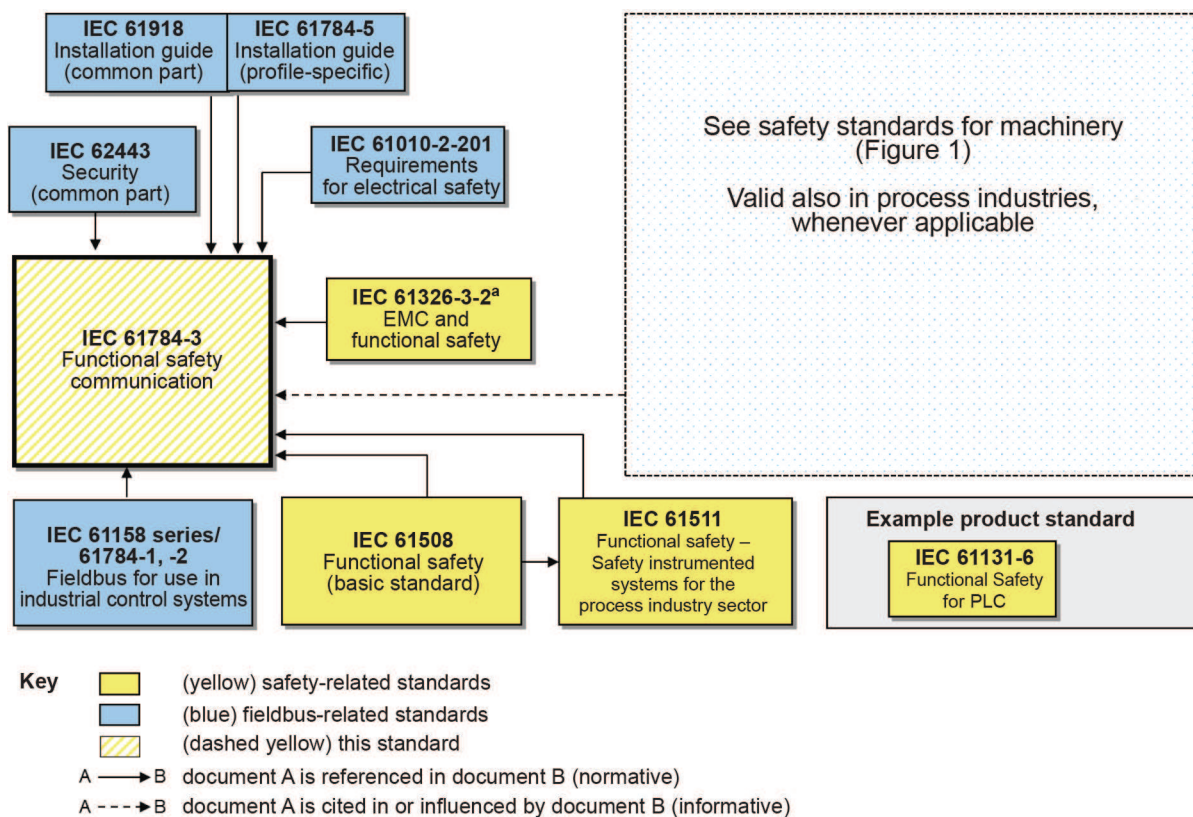


IEC

NOTE IEC 62061 specifies the relationship between PL (Category) and SIL.

Figure 1 – Relationships of IEC 61784-3 with other standards (machinery)

Figure 2 shows the relationships between IEC 61784-3 (all parts) and relevant safety and fieldbus standards in a process environment.



IEC

^a For specified electromagnetic environments; otherwise IEC 61326-3-1 or IEC 61000-6-7.

Figure 2 – Relationships of IEC 61784-3 with other standards (process)

Safety communication layers which are implemented as parts of safety-related systems according to IEC 61508 (all parts) provide the necessary confidence in the transportation of messages (information) between two or more participants on a fieldbus in a safety-related system, or sufficient confidence of safe behaviour in the event of fieldbus errors or failures.

Safety communication layers specified in IEC 61784-3 (all parts) do this in such a way that a fieldbus can be used for applications requiring functional safety up to the Safety Integrity Level (SIL) specified by its corresponding functional safety communication profile.

The resulting SIL claim of a system depends on the implementation of the selected functional safety communication profile (FSCP) within this system – implementation of a functional safety communication profile in a standard device is not sufficient to qualify it as a safety device.

IEC 61784-3 (all parts) describes:

- basic principles for implementing the requirements of IEC 61508 (all parts) for safety-related data communications, including possible transmission faults, remedial measures and considerations affecting data integrity;
- functional safety communication profiles for several communication profile families in IEC 61784-1 and IEC 61784-2, including safety layer extensions to the communication service and protocols sections of IEC 61158 (all parts).

0.2 Patent declaration

The International Electrotechnical Commission (IEC) draws attention to the fact that it is claimed that compliance with this document may involve the use of patents concerning the functional safety communication profiles for family 3. IEC takes no position concerning the evidence, validity, and scope of these patent rights.

The holder of these patent rights has assured IEC that s/he is willing to negotiate licences under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statement of the holder of these patent rights is registered with IEC. Information may be obtained from the patent database available at <http://patents.iec.ch>.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights other than those in the patent database. IEC shall not be held responsible for identifying any or all such patent rights.

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES –

Part 3-3: Functional safety fieldbuses – Additional specifications for CPF 3

Scope

This part of IEC 61784-3 (all parts) specifies a safety communication layer (services and protocol) based on CPF 3 of IEC 61784-1, IEC 61784-2 (CP 3/1, CP 3/2, CP 3/4, CP 3/5 and CP 3/6) and IEC 61158 Types 3 and 10. It identifies the principles for functional safety communications defined in IEC 61784-3 that are relevant for this safety communication layer. This safety communication layer is intended for implementation in safety devices only.

NOTE 1 It does not cover electrical safety and intrinsic safety aspects. Electrical safety relates to hazards such as electrical shock. Intrinsic safety relates to hazards associated with potentially explosive atmospheres.

This document defines mechanisms for the transmission of safety-relevant messages among participants within a distributed network using fieldbus technology in accordance with the requirements of IEC 61508 (all parts)⁴ for functional safety. These mechanisms may be used in various industrial applications such as process control, manufacturing automation and machinery.

This document provides guidelines for both developers and assessors of compliant devices and systems.

NOTE 2 The resulting SIL claim of a system depends on the implementation of the selected functional safety communication profile within this system – implementation of a functional safety communication profile according to this document in a standard device is not sufficient to qualify it as a safety device.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 60204-1, *Safety of machinery – Electrical equipment of machines – Part 1: General requirements*

IEC 61000-6-7, *Electromagnetic compatibility (EMC) – Part 6-7: Generic standards – Immunity requirements for equipment intended to perform functions in a safety-related system (functional safety) in industrial locations*

IEC 61010-2-201:2017, *Safety requirements for electrical equipment for measurement, control and laboratory use – Part 2-201: Particular requirements for control equipment*

IEC 61158-2, *Industrial communication networks – Fieldbus specifications – Part 2: Physical layer specification and service definition*

IEC 61158-5-3, *Industrial communication networks – Fieldbus specifications – Part 5-3: Application layer service definition – Type 3 elements*

IEC 61158-5-10, *Industrial communication networks – Fieldbus specifications – Part 5-10: Application layer service definition – Type 10 elements*

⁴ In the following pages of this document, "IEC 61508" will be used for "IEC 61508 (all parts)".

IEC 61158-6-3, *Industrial communication networks – Fieldbus specifications – Part 6-3: Application layer protocol specification – Type 3 elements*

IEC 61158-6-10, *Industrial communication networks – Fieldbus specifications – Part 6-10: Application layer protocol specification – Type 10 elements*

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

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

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

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

IEC 61511 (all parts), *Functional safety – Safety instrumented systems for the process industry sector*

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

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

IEC 61784-3:2021, *Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions*

IEC 61784-5-3, *Industrial communication networks – Profiles – Part 5-3: Installation of fieldbuses – Installation profiles for CPF 3*

IEC 61918:2018, *Industrial communication networks – Installation of communication networks in industrial premises*

IEC 62061, *Safety of machinery – Functional safety of safety-related control systems*

IEC 62280:2014, *Railway applications – Communication, signalling and processing systems – Safety related communication in transmission systems*

IEC 62443 (all parts), *Industrial communication networks – Network and system security*

ISO 13849-1:2015, *Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design*

ISO 13849-2:2012, *Safety of machinery – Safety-related parts of control systems – Part 2: Validation*

3 Terms, definitions, symbols, abbreviated terms and conventions

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC 61784-3 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at <http://www.electropedia.org/>
- ISO Online browsing platform: available at <http://www.iso.org/obp>

NOTE *Italics are used in the definitions to highlight terms which are themselves defined in 3.1.*

3.1.1 Common terms and definitions

NOTE These common terms and definitions are inherited from IEC 61784-3:2021.

3.1.1.1

active network element

network element containing electrically and/or optically active components that allows extension of the network

Note 1 to entry: Examples of active network elements are repeaters and switches.

[SOURCE: IEC 61918:2018, 3.1.2]

3.1.1.2

availability

probability for an automated system that for a given period of time there are no unsatisfactory system conditions such as loss of production

3.1.1.3

bit error probability

Pe

probability for a given bit to be received with the incorrect value

3.1.1.4

black channel

defined communication system containing one or more *elements* without evidence of design or validation according to IEC 61508

Note 1 to entry: This definition expands the usual meaning of channel to include the system that contains the channel.

3.1.1.5

communication channel

logical connection between two end-points within a *communication system*

3.1.1.6

communication system

arrangement of hardware, software and propagation media to allow the transfer of *messages* (ISO/IEC 7498-1 application layer) from one application to another

3.1.1.7

connection

logical binding between two application objects within the same or different devices

3.1.1.8

Cyclic Redundancy Check

CRC

<value> redundant data derived from, and stored or transmitted together with, a block of data in order to detect data corruption

<method> procedure used to calculate the redundant data

Note 1 to entry: Terms "CRC code" and "CRC signature", and labels such as CRC1, CRC2, may also be used in this document to refer to the redundant data.

Note 2 to entry: See also [27],[28]⁵.

⁵ Figures in square brackets refer to the bibliography.

3.1.1.9

defined communication system

defined channel

fixed number or fixed maximum number of participants linked by a *fieldbus* based *communication system* with well-known and fixed properties, such as installation conditions, electromagnetic immunity, industrial (*active*) *network elements*, and where the *risk* of unauthorized access is reduced to a tolerated level according to the lifecycle model of IEC 62443 (all parts), using for example zones and conduits

3.1.1.10

DLPDU

DEPRECATED: frame

Data Link Protocol Data Unit

3.1.1.11

error

discrepancy between a computed, observed or measured value or condition and the true, specified or theoretically correct value or condition

Note 1 to entry: Errors may be due to design mistakes within hardware/software and/or corrupted information due to electromagnetic interference and/or other effects.

Note 2 to entry: Errors do not necessarily result in a *failure* or a *fault*.

[SOURCE: IEC 61508-4:2010, 3.6.11, modified – notes added]

3.1.1.12

explicit code

code for safety measure that is actually transmitted within the SPDU and is known to the sender and receiver

3.1.1.13

explicit data

data that is transmitted

Note 1 to entry: Explicit data is defined in contrast to implicit data.

3.1.1.14

failure

termination of the ability of a functional unit to perform a required function or operation of a functional unit in any way other than as required

Note 1 to entry: Failure may be due to an *error* (for example, problem with hardware/software design or message disruption).

[SOURCE: IEC 61508-4:2010, 3.6.4, modified – notes and figures replaced]

3.1.1.15

fault

abnormal condition that may cause a reduction in, or loss of, the capability of a functional unit to perform a required function

Note 1 to entry: IEC 60050-191:1990, 191-05-01 defines "fault" as a state characterized by the inability to perform a required function, excluding the inability during preventive maintenance or other planned actions, or due to lack of external resources.

[SOURCE: IEC 61508-4:2010, 3.6.1, modified – figure reference deleted]

3.1.1.16

fieldbus

communication system based on serial data transfer and used in industrial automation or process control applications

3.1.1.17

fieldbus system

system using a *fieldbus* with connected devices

3.1.1.18

Frame Check Sequence

FCS

redundant data derived from a block of data within a DLPDU (frame), using a hash function, and stored or transmitted together with the block of data, in order to detect data corruption

Note 1 to entry: An FCS can be derived using for example a CRC or other hash function.

Note 2 to entry: See also [27], [28].

3.1.1.19

functional safety communication profile

FSCP

technology specification for the implementation of an SCL

3.1.1.20

hash function

(mathematical) function that maps values from a (possibly very) large set of values into a (usually) smaller range of values

Note 1 to entry: Hash functions can be used to detect data corruption.

Note 2 to entry: Common hash functions include parity, checksum or CRC.

3.1.1.21

hazard

potential source of harm

Note 1 to entry: The term includes danger to persons arising within a short time scale (for example, fire and explosion) and also those that have a long-term effect on a person's health (for example, release of a toxic substance).

[SOURCE: IEC 61508-4:2010, 3.1.2 and ISO/IEC Guide 51:2014, definition 3.2]

3.1.1.22

implicit code

code for safety measure that is not transmitted within the SPDU but is known to the sender and receiver

3.1.1.23

implicit data

additional data that is not transmitted but is known to the sender and receiver, and used in the encoding and decoding of the message/SPDU

Note 1 to entry: Implicit data is defined in contrast to explicit data.

[SOURCE: IEC 62280:2014, 3.1.25, modified – addition of ", and used in the encoding and decoding of the message/SPDU"]

3.1.1.24

master

communication entity able to initiate and schedule communication activities by other stations which may be masters or slaves

3.1.1.25

message

<information theory and communication theory> ordered sequence of characters (usually octets) intended to convey information

[SOURCE: ISO/IEC 2382:2015, 2123205, modified – insertion of "(usually octets)", deletion of notes and source]

3.1.1.26

proof test

periodic test performed to detect dangerous hidden failures in a *safety-related system* so that, if necessary, a repair can restore the system to an "as new" condition or as close as practical to this condition

Note 1 to entry: A proof test is intended to confirm that the safety-related system is in a condition that assures the specified safety integrity.

[SOURCE: IEC 61508-4:2010, 3.8.5, modified by replacement of the four notes with another one]

3.1.1.27

performance level

PL

discrete level used to specify the ability of safety-related parts of control systems to perform a safety function under foreseeable conditions

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

3.1.1.28

protective extra-low-voltage

PELV

protective earth referenced electrical circuit in which the voltage cannot exceed the following:

NORMAL CONDITION and SINGLE FAULT CONDITION: The AC voltage levels are 30 V RMS 42,4 V peak and the DC voltage level is 60 V. For equipment intended for use in WET LOCATIONS, the AC voltage levels are 16 V RMS, 22,6 V peak and the DC voltage level is 35 V.

[SOURCE: IEC 61010-2-201:2017, 3.111, modified – deletion of "circuit" from term, and deletion of source]

3.1.1.29

redundancy

existence of more than one means for performing a required function or for representing information

[SOURCE: IEC 61508-4:2010, 3.4.6, modified – example and notes deleted]

3.1.1.30

residual error probability

RP

probability of an error undetected by the SCL safety measures

3.1.1.31

residual error rate

statistical rate at which the SCL safety measures fail to detect errors

3.1.1.32

risk

combination of the probability of occurrence of harm and the severity of that harm

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6, and ISO/IEC Guide 51:2014, definition 3.9, modified – different note]

3.1.1.33

safety communication channel

communication channel starting at the top of the SCL of the source and ending at the top of the SCL of the sink

Note 1 to entry: It can be modelled as two SCLs connected by a black channel or a defined communication system, or a defined channel.

3.1.1.34

safety communication layer

SCL

communication layer above the FAL that includes all necessary additional measures to ensure safe transmission of data in accordance with the requirements of IEC 61508

3.1.1.35

safety connection

connection that utilizes the safety protocol for communications transactions

3.1.1.36

safety data

data transmitted across a safety network using a safety protocol

Note 1 to entry: The Safety Communication Layer does not ensure safety of the data itself, only that the data is transmitted safely.

3.1.1.37

safety device

device designed in accordance with IEC 61508 and which implements the functional safety communication profile

3.1.1.38

safety extra-low-voltage

SELV

non-protective earth referenced electrical circuit in which the voltage cannot exceed the following:

NORMAL CONDITION and SINGLE FAULT CONDITION: The AC voltage levels are 30 V RMS, 42,4 V peak and the DC voltage level is 60 V. For equipment intended for use in WET LOCATIONS, the AC voltage levels are 16 V RMS, 22,6 V peak and the DC voltage level is 35 V.

[SOURCE: IEC 61010-2-201:2017, 3.112, modified – deletion of "circuit" from term, and deletion of source]

3.1.1.39

safety function

function to be implemented by an E/E/PE safety-related system or other risk reduction measures, that is intended to achieve or maintain a safe state for the EUC, in respect of a specific hazardous event

[SOURCE: IEC 61508-4:2010, 3.5.1, modified – references and example deleted]

3.1.1.40

safety function response time

SFRT

worst case elapsed time following an actuation of a safety sensor connected to a fieldbus, until the corresponding safe state of its safety actuator(s) is achieved in the presence of errors or failures in the safety function

Note 1 to entry: This concept is introduced in IEC 61784-3:2021, 5.2.4 and addressed by the functional safety communication profiles defined in this document.

3.1.1.41

safety integrity level

SIL

discrete level (one out of a possible four), corresponding to a range of safety integrity values, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest

Note 1 to entry: The target failure measures (see IEC 61508-4:2010, 3.5.17) for the four safety integrity levels are specified in Tables 2 and 3 of IEC 61508-1:2010.

Note 2 to entry: Safety integrity levels are used for specifying the safety integrity requirements of the safety functions to be allocated to the E/E/PE safety-related systems.

Note 3 to entry: A safety integrity level (SIL) is not a property of a system, subsystem, element or component. The correct interpretation of the phrase "SIL_n safety-related system" (where *n* is 1, 2, 3 or 4) is that the system is potentially capable of supporting safety functions with a safety integrity level up to *n*.

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

3.1.1.42

safety measure

measure to control possible communication *errors* that is designed and implemented in compliance with the requirements of IEC 61508

Note 1 to entry: In practice, several safety measures are combined to achieve the required safety integrity level.

Note 2 to entry: Communication *errors* and related safety measures are detailed in IEC 61784-3:2021, 5.3 and 5.4.

3.1.1.43

safety PDU

SPDU

PDU transferred through the safety communication channel

Note 1 to entry: The SPDU may include more than one copy of the safety data using differing coding structures and hash functions together with explicit parts of additional protections such as a key, a sequence count, or a time stamp mechanism.

Note 2 to entry: Redundant SCLs may provide two different versions of the SPDU for insertion into separate fields of the fieldbus frame.

Note 3 to entry: In terms of CP 3/4 to 3/6 it is the APDU Application Protocol Data Unit.

3.1.1.44

safety-related application

programs designed in accordance with IEC 61508 to meet the SIL requirements of the application

3.1.1.45

safety-related system

system performing *safety functions* according to IEC 61508

3.1.1.46

slave

communication entity able to receive messages and send them in response to another communication entity which may be a master or a slave, but not to initiate communication activities

3.1.1.47

spurious trip

trip caused by the safety system without a process demand

3.1.1.48

uniform distribution

probability distribution where all values from a finite set are equally likely to occur

Note 1 to entry: For a field of bit length i the probability of occurrence of a particular field value is 2^{-i} since the sum of all probabilities of occurrence is equal to 1.

3.1.2 CPF 3: Additional terms and definitions

3.1.2.1

Address Type

Address Type 1 if F_DestAdd is checked only

Address Type 2 if F_SourceAdd is checked together with the F_DestAdd

3.1.2.2

Bit

Binary Digit

encoded binary information without a technical unit

3.1.2.3

Codename

Identification of the safety communication relationship between safety communication peers.

Note 1 to entry: The Codename is used for the unique identification of the safety communication relationship.

Note 2 to entry: The Codename consists of F_Source_Address and F_Dest_Address.

Note 3 to entry: Instance of *connection authentication* as described in IEC 61784-3.

3.1.2.4 configuration

definition of the standard communication connections and communication parameters for bus entities of a particular application

Note 1 to entry: The configuration for safety communication comprises the definition of the safety connections and F-Parameters for safety-related bus entities of a particular safety-related application.

3.1.1.5 CPD-Tool

dedicated program in service computers connected to the fieldbus for the purpose of Configuration, Parameterization and Diagnosis of particular field devices

3.1.1.6 cycle

interval at which a list of instructions or an activity is repetitively and continuously executed

3.1.1.7 device access point DAP

item used to address a modular IO device as an entity

Note 1 to entry: Usually this is called a head station.

3.1.1.8 device acknowledgment time DAT

elapsed time in an IO-Device starting with the reception of a safety PDU with a new *MonitoringNumber* in the device access point until an appropriate response safety PDU has been generated and returned to the device access point

3.1.1.9 driver

software module used for abstracting the hardware with respect to the remaining application software

3.1.1.10 fail-safe F

ability of a system that, by adequate technical or organizational measures, prevents from hazards either deterministically or by reducing the risk to a tolerable measure

Note 1 to entry: Equivalent to functional safety.

3.1.1.11 fail-safe values FV

values which are issued instead of process values when the safety function is set to a fail-safe state

Note 1 to entry: In this document, the fail-safe values (FV) shall always be set to "0".

3.1.1.12 fail-safe state

operational mode of a safety function or final element (actuator) that by adequate technical measures prevents from hazards either deterministically or by reducing the risk to a tolerable measure

Note 1 to entry: Depending on a particular safety function, de-energizing is not the only possibility for a fail-safe state.

3.1.1.13

F-Host Channel driver

driver within F-Hosts according to the FSCP 3/1 specifications to represent F IO data in the F-Host application program

3.1.1.14

F-Device

The term F-Device used in previous versions of this profile is substituted by "F-Device driver"

3.1.1.15

F-Device driver

software administering safety PDUs within F-(Sub)Module according to the FSCP 3/1 specifications triggered by the F-Host driver for data exchange

3.1.1.16

F driver

software administering safety PDUs as F-Host driver or F-Device driver according to the FSCP 3/1 specifications

3.1.1.17

F-Host

data processing unit that is able to perform the FSCP 3/1 protocol and to service the black channel

Note 1 to entry: This is usually implemented in a PLC or an IPC with an adequate operating system.

3.1.1.18

F-Host driver

software administering safety PDUs within F-Hosts according to the FSCP 3/1 specifications

3.1.1.19

F-(Sub)Module

communication peer within a modular IO-Slave or IO-Device that is able to perform the CP 3/1 or CP 3/4 to CP 3/6 protocol

Note 1 to entry: The F-(Sub)Module is hosting the F-Device driver.

Note 2 to entry: This is usually a safety-related input or output module.

3.1.1.20

F-Slave

CP 3/1 or CP 3/2 communication peer that is able to perform the FSCP 3/1 protocol, usually triggered by the F-Host for data exchange

3.1.1.21

fault reaction

indication of a communication malfunction by setting the fault bits in the Status Byte and a corresponding automatic safe reaction within the components

Note 1 to entry:

Within F-Output: Shutting down the outputs, and/or automatic safe reaction of the actuator unit.

Within F-CPU: Corresponding application program reaction possible. F-IO data to be set to fail-safe values.

Within F-Input: On communication faults detected from F-Input:

Fault bits set in the Status Byte.

On communication faults detected from F-Host:

F-Input data to be set to fail-safe values.

3.1.1.22

function block

FB

self-contained program part possessing a specific functionality

3.1.1.23

host acknowledgment time

HAT

elapsed time in an F-Host starting with the reception of a safety PDU with a certain *MonitoringNumber* until an appropriate safety PDU with a changed *MonitoringNumber* has been generated and returned to the master/IO-Controller

3.1.1.24

IO-Controller

active communication entity able to initiate and schedule CP 3/4 to CP 3/6 communication activities by other entities which may be IO-Controllers or IO-Devices

Note 1 to entry: Within CP 3/1 this task is corresponding to a master class 1.

Note 2 to entry: The IO-Controller interface is called "FAL services of the IO controller" according to IEC 61158-5-10.

3.1.1.25

IO-Device

communication entity able to receive messages and send them in response to another CP 3/4 to CP 3/6 communication entity which may be an IO-Controller or other IO-Devices

Note 1 to entry: Within CP 3/1 this task is corresponding to a slave.

Note 2 to entry: The IO-Device interface is called "FAL services of the IO device" according to IEC 61158-5-10.

3.1.1.26

IO-Module

addressable sub input/output unit within a modular IO-Device

3.1.1.27

IO-Supervisor

engineering station enabled to read and write data from and to an IO-Device

Note 1 to entry: It is used for commissioning or diagnostics purposes. In contrast to an IO-Controller it does not take over an active role during the run-up of an IO-System. An IO-Supervisor is not part of the IO-System.

3.1.1.28

IO-System

IO-Controller and its associated IO-Devices

3.1.1.29

iParameter

individual or technology specific F-(Sub)Module parameters

Note 1 to entry: Typical iParameters are the protection zone coordinates of a laser scanner.

3.1.1.30

iPar-Server

standardised mechanism to store and retrieve individual or technology specific F-(Sub)Module parameters within the standard part of an F-Host or its controlled subsystem

3.1.1.31

master (class 1)

active CP 3/1 communication peer triggering slaves for data exchange

Note 1 to entry: The term "master" alone is used as a short form for "master class 1".

3.1.1.32

MonitoringNumber

MNR

means to ensure authenticity and the correct order of transmitted safety PDUs