

DIN EN IEC 61784-3-8

ICS 35.160; 35.240.50

Ersatz für
DIN EN 61784-3-8:2018-09
Siehe Anwendungsbeginn

**Industrielle Kommunikationsnetze –
Profile –
Teil 3-8: Funktional sichere Übertragung bei Feldbussen –
Zusätzliche Festlegungen für die Kommunikationsprofilfamilie 8
(IEC 61784-3-8:2021);
Englische Fassung EN IEC 61784-3-8:2021**

Industrial communication networks –
Profiles –
Part 3-8: Functional safety fieldbuses –
Additional specifications for CPF8
(IEC 61784-3-8:2021);
English version EN IEC 61784-3-8:2021

Réseaux de communication industriels –
Profils –
Partie 3-8: Bus de terrain de sécurité fonctionnelle –
Spécifications supplémentaires pour CPF 8
(IEC 61784-3-8:2021);
Version anglaise EN IEC 61784-3-8:2021

Gesamtumfang 132 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE

Anwendungsbeginn

Anwendungsbeginn für die von CENELEC am 2021-06-23 angenommene Europäische Norm als DIN-Norm ist 2023-05-01.

Für DIN EN 61784-3-8:2018-09 besteht eine Übergangsfrist bis 2024-06-23.

Nationales Vorwort

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

Dieser Entwurf betrifft auch DIN EN IEC 61784-3-2:2023-04, DIN EN IEC 61784-3-3:2023-04, DIN EN IEC 61784-3-13:2023-05 und DIN EN 61784-3-18/A2:2023-05 und wird erst mit Veröffentlichung aller aufgeführten Normen zurückgezogen.

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 61784-3-8 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 des vorliegenden Dokuments 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.

Dieses Dokument 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 61784-3-8:2018-09 wurden folgende Änderungen vorgenommen:

- a) strukturiert für die Übereinstimmung mit IEC 61784-3 Ed.4;
- b) allgemeine redaktionelle Änderungen und Klarstellungen;
- c) Sicherheitsmaßnahmen (11.5.3);
- d) Sicherheitsanwendungsdienstelemente (11.6.2);
- e) Sicherheits-PDU-Format (11.7.1);
- f) Randbedingungen für die Berechnung von Systemeigenschaften (11.9.5);
- g) Sicherheitsmaßnahmen (12.5.3);
- h) Format der Sicherheits-PDU (12.7.1);
- i) Verhalten (12.7.2);
- j) Beschränkungen für die Berechnung von Systemmerkmalen (12.9.5);
- k) Berechnungen von Hash-Funktionen (Anhang A).

Frühere Ausgaben

DIN EN 61784-3-8: 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.

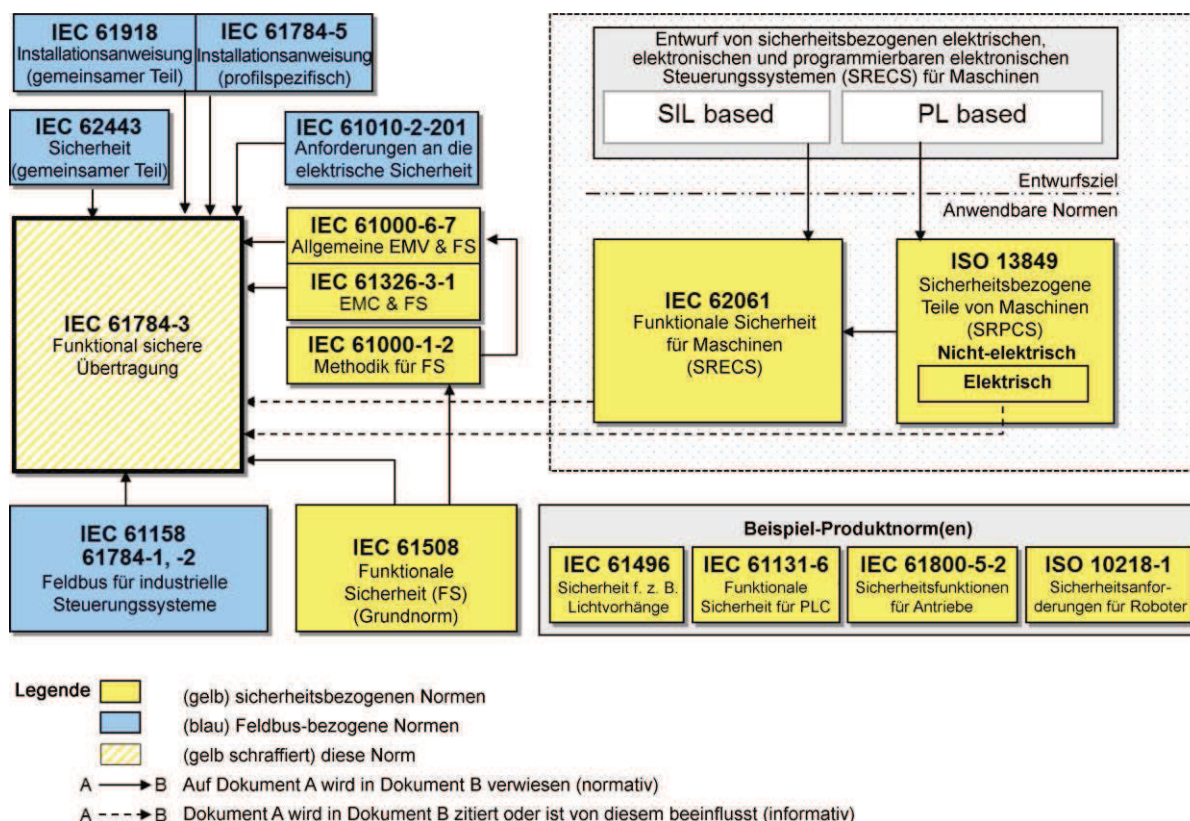
0 Einleitung

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 weder Sicherheitsaspekte noch stellt sie Anforderungen an die IT-Sicherheit.

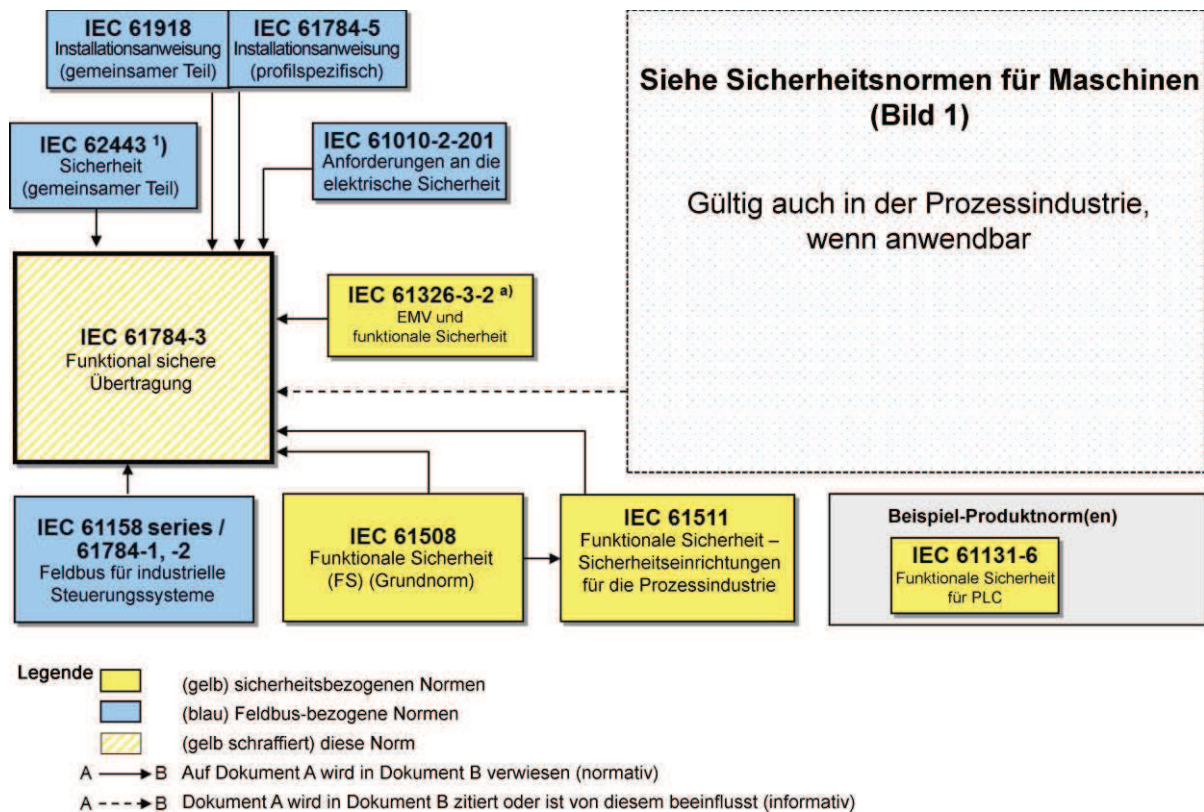
Bild 1 zeigt die Beziehungen zwischen IEC 61784-3 (alle Teile) und den für die Fertigungsautomatisierung relevanten Sicherheits- und Feldbusnormen.



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 der Weise, 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 Internationale Elektrotechnische Kommission (IEC) weist darauf hin, dass die Übereinstimmung mit diesem Dokument die Verwendung von Patenten hinsichtlich der Kommunikationsprofile für funktionale Sicherheit der Familie 8 beinhalten kann. IEC übernimmt keine Verantwortung hinsichtlich Nachweisen, Gültigkeit und Anwendungsbereich von Patentrechten.

Die Halter der Patentrechte haben IEC gegenüber versichert, dass sie bereit sind, Anwendern weltweit Nutzungsrechte zu angemessenen und nicht diskriminierenden Bedingungen einzuräumen. Diesbezügliche Aussagen der Halter von solchen Patentrechten sind bei der IEC hinterlegt. Informationen sind bei der Patentdatenbank unter: <http://patents.iec.ch> erhältlich.

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 der Normenreihe IEC 61784-3 legt eine Sicherheitsschicht (Dienste und Protokoll) fest, die auf der Kommunikationsprofilfamilie 8 der IEC 61784-1, IEC 61784-2 und IEC 61158, Typ 18 und Typ 23, beruht. Sie stellt die Grundsätze der funktional sicheren Kommunikation nach IEC 61784-3 fest, die für diese Sicherheitskommunikationsschicht wichtig sind. Diese Sicherheitskommunikationsschicht ist für die ausschließliche Implementierung in Sicherheitsgeräten vorgesehen.

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

Dieser Teil legt Mechanismen fest für die Übertragung von sicherheitsrelevanten Nachrichten zwischen Teilnehmern in einem verteilten Netzwerk unter Verwendung von Feldbus-Technologie in Übereinstimmung mit der Normenreihe IEC 61508¹ für funktionale Sicherheit. Diese Mechanismen dürfen in verschiedenen Industrieanwendungen verwendet werden, wie Prozesssteuerung, Fertigungsautomatisierung und Maschinen.

Dieser Teil enthält Leitlinien sowohl für Entwickler als auch Gutachter von entsprechenden Geräten und Systemen.

ANMERKUNG 2 Der resultierende SIL-Anspruch eines Systems hängt von der Implementierung des gewählten Kommunikationsprofils für funktional sichere Übertragung in diesem System ab – eine Implementierung eines funktional sicheren Kommunikationsprofils nach diesem 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/>

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

- 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

absoluter Zeitstempel

en **absolute time stamp**

Zeitstempel, der sich auf eine zentrale Zeit bezieht, welche für eine Gruppe von Geräten an einem *Feldbus* gleich ist

[QUELLE: IEC 62280:2014, 3.1.1, modifiziert – „Geräte“ und „Feldbus“ verwendet, anstelle von „Einrichtungen“ und „Übertragungsnetz“]

3.1.1.2

aktives Netzelement

en **active network element**

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

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

[QUELLE: IEC 61918:2018, 3.1.2]

3.1.1.3

Bitfehlerwahrscheinlichkeit

PE, en **bit error probability**

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

3.1.1.4

Black Channel

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

Bridge

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

3.1.1.6

geschlossenes Kommunikationssystem

en **closed communication system**

festgelegte Anzahl oder festgelegte maximale Anzahl von Teilnehmern, die über ein *Kommunikationssystem* verbunden sind, mit wohldefinierten und festgelegten Eigenschaften und wo das *Risiko* eines unerlaubten Zugriffs als vernachlässigbar betrachtet wird

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

3.1.1.7

Kommunikationskanal

en **communication channel**

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

3.1.1.8

Kommunikationssystem

en **communication system**

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

3.1.1.9

Verbindung

en **connection**

logische Verbindung zwischen zwei Anwendungsobjekten in demselben oder in unterschiedlichen Geräten

3.1.1.10

zyklische Redundanzprüfung

CRC, en **Cyclic Redundancy Check**

<Wert>redundante Daten, abgeleitet von einem Block von Daten und mit diesen zusammen gespeichert oder übertragen zur Aufdeckung von Datenverfälschungen

<Methode>Prozedur zur Berechnung der redundanten Daten

Anmerkung 1 zum Begriff: Begriffe wie „CRC-Code“ und „CRC-Signatur“ und Bezeichnungen wie CRC1, CRC2 können ebenfalls in diesem Dokument verwendet sein, um redundante Daten zu kennzeichnen.

Anmerkung 2 zum Begriff: Siehe auch [26][27]².

3.1.1.11

definiertes Kommunikationssystem

definierter Kanal

en **defined communication system**

en **defined channel**

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

3.1.1.12

Diversität

en **diversity**

ungleichartige Mittel zur Ausführung einer geforderten Funktion

Anmerkung 1 zum Begriff: Diversität kann durch unterschiedliche physikalische Methoden oder unterschiedliche Lösungen für dieselbe Aufgabenstellung erreicht werden.

[QUELLE: IEC 61508-4:2010, 3.3.7]

3.1.1.13

DLPDU

ABGELEHNT: frame

Data Link Protocol Data Unit

² Zahlen in rechteckigen Klammern beziehen sich auf die Literaturhinweise.

3.1.1.14**Abweichung**en **error**

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

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

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

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

3.1.1.15**Ausfall**en **failure**

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

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

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

3.1.1.16**Fehler**en **fault**

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

Anmerkung 1 zum Begriff: IEC 60050-191:1990, 191-05-01 definiert „fault“ als einen Zustand, der durch das Unvermögen gekennzeichnet ist, eine geforderte Funktion auszuführen, jedoch nicht ein Unvermögen während vorbeugender Instandhaltung, anderer geplanter Aktionen oder auf Grund fehlender externer Betriebsmittel.

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

3.1.1.17**Feldbus**en **fieldbus**

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

3.1.1.18**Feldbussystem**en **fieldbus system**

System mit einem Feldbus und angeschlossenen Geräten

3.1.1.19**Blockprüfzeichenfolge**FCS, en **Frame Check Sequence**

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 [26][27]

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 sind Paritätsbit, Prüfsummen oder CRC.

3.1.1.21

Gefährdung

en **hazard**

mögliche Schadensquelle

Anmerkung 1 zum Begriff: Der Begriff umfasst sowohl Gefahren für Personen, die innerhalb eines kurzen Zeitraums auftreten (z. B. Feuer und Explosion), als auch solche, die sich langfristig auf die Gesundheit einer Person auswirken (z. B. Freisetzung eines giftigen Stoffes).

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

3.1.1.22

Master

en **master**

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

3.1.1.23

Nachricht

en **message**

<Informationstheorie und Kommunikationstheorie> geordnete Folge von Zeichen (in der Regel Oktette) zur Übermittlung von Informationen

[QUELLE: ISO/IEC 2382:2015, 2123205, modifiziert – Einfügung von "(in der Regel Oktette)", Streichung von Anmerkungen und Quelle]

3.1.1.24

Nachrichtensenke

Informationssenke

en **message sink**

en **information sink**

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

[QUELLE: ISO/IEC 2382:2015, 2123207, modifiziert – Streichung von Anmerkungen und Quelle]

3.1.1.25

Nachrichtenquelle

Informationsquelle

en **message source**

en **information source**

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

[QUELLE: ISO/IEC 2382:2015, 2123206, modifiziert – Streichung von Anmerkungen und Quelle]

3.1.1.26

Performance Level

PL, en **performance level**

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]

3.1.1.27**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]

3.1.1.28**relativer Zeitstempel**en **relative time stamp**

Zeitstempel, der sich auf die lokale Zeit einer Einheit bezieht

Anmerkung 1 zum Begriff: Im Allgemeinen gibt es keine Beziehungen zu den Zeitgebern in anderen Einheiten.

[QUELLE: IEC 62280:2014, 3.1.43, modifiziert – Format angepasst]

3.1.1.29**Restfehlerwahrscheinlichkeit**RP, en **residual error probability**

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

3.1.1.30**Restfehlerrate**en **residual error rate**

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

3.1.1.31**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]

3.1.1.32**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.**3.1.1.33****Sicherheitskommunikationsschicht**SCL, en **safety communication layer**

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

3.1.1.34**sichere Verbindung**en **safety connection**

Verbindung, welche das Sicherheitsprotokoll für Kommunikationstätigkeiten nutzt

3.1.1.35

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.

3.1.1.36

Sicherheitsgerät

en **safety device**

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

3.1.1.37

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]

3.1.1.38

Reaktionszeit einer Sicherheitsfunktion

en **safety function response time**

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

Anmerkung 1 zum Begriff: Dieses Konzept wird in IEC 61784-3:2021, 5.2.4, eingeführt und von den in diesem Dokument aufgeführten Kommunikationsprofilen für funktional sichere Übertragung verwendet.

3.1.1.39

Sicherheits-Integritätslevel

SIL, en **safety integrity level**

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

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

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

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

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

3.1.1.40

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: Kommunikationsfehler und zugehörige Sicherheitsmaßnahmen sind ausführlich in IEC 61784-3:2021, 5.3 und 5.4 beschrieben.

3.1.1.41

Sicherheits-PDU

SPDU, en **safety PDU**

durch einen Sicherheitskommunikationskanal übertragene PDU

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

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

3.1.1.42

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

3.1.1.43

sicherheitsbezogenes System

en **safety-related system**

System, welches *Sicherheitsfunktionen* nach IEC 61508 ausführt

3.1.1.44

Slave

en **slave**

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

3.1.1.45

unberechtigte Auslösung

en **spurious trip**

Auslösung in einem Sicherheitssystem ohne Prozessanforderung

3.1.1.46

Aktualitätscode

en **timeliness code**

Zeitinformation in einer Nachricht

3.1.1.47

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 ist.

3.1.1.48

White Channel

en **white channel**

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

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

3.1.2 CPF 8: Zusätzliche Begriffe

3.1.2.1

Zyklus

en **cycle**

Intervall, in dem eine Aktivität wiederholt und fortlaufend ausgeführt wird

3.1.2.2

Sicherheitsanwendungsbeziehung

SAR, en **safety application relationship**

Anwendungsbeziehung zwischen zwei oder mehreren Beziehungsendpunkten sicherheitsbezogener Anwendungen

3.1.2.3

Dienstelement der Sicherheitsanwendung

SASE, en **safety application service element**

Serviceelement einer sicherheitsbezogenen Anwendung

3.1.2.4

Sicherheitsuhr

en **safety clock**

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

3.1.2.5

Zeitschalter für Sicherheitsdatenüberwachung

en **safety data monitor timer**

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

3.1.2.6

Zeitschalter für Sicherheitsüberwachung

en **safety monitor timer**

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

3.1.2.7

sicherheitsbezogene Aktualisierung

en **safety refresh**

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

3.1.2.8

Slot

en **slot**

Menge (Granularität) der positionsabhängigen Zuordnung der zyklischen Datenfelder

3.1.2.9

Station

en **station**

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

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

3.1.2.10

Übertragungsinformation des Sicherheitsprotokolls

en **safety protocol transmission information**

Information, die sicherheitsbezogene Nachrichten voneinander unterscheidet

3.2 Symbole und Abkürzungen

3.2.1 Allgemeine Symbole und Abkürzungen

A-code	Authentication code	
CP	Kommunikationsprofil (en: Communication Profile)	[IEC 61784-1]
CPF	Kommunikationsprofilfamilie (en: Communication Profile Family)	[IEC 61784-1]
CRC	zyklische Redundanzprüfung (en: Cyclic Redundancy Check)	
DLL	Sicherungsschicht (en: Data Link Layer)	[ISO/IEC 7498-1]
DLPDU	Protokolldateneinheit der Sicherungsschicht (en: Data Link Protocol Data Unit)	
EMC	elektromagnetische Verträglichkeit (en: Electromagnetic Compatibility)	
EUC	Prüfling (en: equipment under control)	[IEC 61508-4:2010]
E/E/PE	elektrisch/elektronisch/programmierbar elektronisch (en: Electrical/Electronic/Programmable Electronic)	[IEC 61508-4:2010]
FAL	Feldbusanwendungsschicht (en: Fieldbus Application Layer)	[IEC 61158-5 (alle Teile)]
FS	funktionale Sicherheit (en: Functional Safety)	
FSCP	funktional sicheres Kommunikationsprofil (en: Functional Safety Communication Profile)	
FSPM	FAL Service Protocol Machine	[IEC 61158-1]
MTBF	mittlere Zeit zwischen Ausfällen (en: Mean Time Between Failures)	
MTTF	mittlere Zeit bis zu einem Ausfall (en: Mean Time To Failure)	
PDU	Protokolldateneinheit (en: Protocol Data Unit)	[ISO/IEC 7498-1]
Pe	Bitfehlerwahrscheinlichkeit (en: bit error probability)	
PhL	Bitübertragungsschicht (en: Physical Layer)	[ISO/IEC 7498-1]
PL	Performance Level	[ISO 13849-1]
PLC	speicherprogrammierbare Steuerung (en: Programmable Logic Controller)	
SCL	Sicherheitskommunikationsschicht (en: Safety Communication Layer)	
SIL	Sicherheits-Integritätslevel (en: safety integrity level)	[IEC 61508-4:2010]

SPDU	Sicherheits-PDU (en: Safety PDU)
T-code	Aktualitätscode (en: Timeliness code)

3.2.2 CPF 8: Zusätzliche Symbole und Abkürzungen

AR	Anwendungsbeziehung (en: application relationship)
ASE	Anwendungsdienstelement (en: application service element)
CC	Carry Counter
CID	Verbindungskennung (en: connection identifier)
CMD	(en: command data)
LED	lichtemittierende Diode
LID	(en: link identifier)
OBL	Offset Baseline
RNO	laufende Nummer (en: running number)
SAR	Sicherheitsanwendungsbeziehung (en: safety application relationship)
SAREP	Endpunkt der Sicherheitsanwendungsbeziehung (en: safety application relationship endpoint)
SARPM	Protokollzustandsautomat der Sicherheitsanwendungsbeziehung (en: safety application relationship protocol state machine)
SASE	Dienstelement der Sicherheitsanwendung (en: safety application service element)
SFSPM	Sicherheits-FSPM (angehängter -S-Slave oder -M-Master)
SRC	(en: safety relevant controller)
SRP	(en: safety relevant peripheral)
TPI	(en: safety transmission packet information)
TPI-T	(en: safety transmission packet information from master)
TPI-R	(en: safety transmission packet information from slave)
TS	Zeitstempel (en: time stamp)

3.3 Konventionen

Die in diesem Dokument verwendeten Konventionen sind in IEC 61158 Typ 18 und Typ 23, IEC 61784-1 CPF 8 und IEC 61784-2 CPF 8 definiert.

Zur Unterstützung des Lesers, der mit der Nummerierung der Abschnitte der Norm vertraut ist, und zum Zwecke der Konsistenz und Angleichung an IEC 61784-3 verweisen die Abschnitte 4 bis 10 auf die Abschnitte 11 bis 17 für FSCP 8/1 und die Abschnitte 18 bis 24 für FSCP 8/2.

EUROPEAN STANDARD

EN IEC 61784-3-8

NORME EUROPÉENNE

EUROPÄISCHE NORM

June 2021

ICS 25.040.40; 35.100.05

Supersedes EN 61784-3-8:2017 and all of its amendments and corrigenda (if any)

English version

**Industrial communication networks – Profiles – Part 3-8:
Functional safety fieldbuses – Additional specifications for CPF8
(IEC 61784-3-8:2021)**

Réseaux de communication industriels – Profils –
Partie 3-8: Bus de terrain de sécurité fonctionnelle –
Spécifications supplémentaires pour CPF 8
(IEC 61784-3-8:2021)

Industrielle Kommunikationsnetze – Profile – Teil 3-8:
Funktional sichere Übertragung bei Feldbussen – Zusätzliche
Festlegungen für die Kommunikationsprofilfamilie 8
(IEC 61784-3-8:2021)

This European Standard was approved by CENELEC on 2021-06-23. 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 3 of IEC 61784-3-8, 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 61784-3-8:2021.

The following dates are fixed:

- latest date by which the document has to be implemented at national level by (dop) 2022-03-23
publication of an identical national standard or by endorsement
- latest date by which the national standards conflicting with the (dow) 2024-06-23
document have to be withdrawn

This document supersedes EN 61784-3-8:2017 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 61784-3-8:2021 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 61000-1-2	NOTE	Harmonized as EN 61000-1-2
IEC 61000-6-7	NOTE	Harmonized as EN 61000-6-7
IEC 61010-2-201	NOTE	Harmonized as EN IEC 61010-2-201
IEC 61131-6	NOTE	Harmonized as EN 61131-6
IEC 61158-1	NOTE	Harmonized as EN IEC 61158-1
IEC 61158-5 (series)	NOTE	Harmonized as EN 61158-5 (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 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 61918:2018	NOTE	Harmonized as EN IEC 61918:2018 (not modified)
IEC 62443 (series)	NOTE	Harmonized as EN IEC 62443 (series)
ISO 10218-1	NOTE	Harmonized as EN ISO 10218-1
ISO 13849 (series)	NOTE	Harmonized as EN ISO 13849 (series)
ISO 13849-1:2015	NOTE	Harmonized as EN ISO 13849-1:2015 (not modified)
ISO 13849-2	NOTE	Harmonized as EN ISO 13849-2

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 61131-2	-	Industrial-process measurement and control - Programmable controllers - Part 2: Equipment requirements and tests	-	-
IEC 61158	series	Industrial communication networks - Fieldbus specifications	EN IEC 61158	series
IEC 61158-2	-	Industrial communication networks - Fieldbus specifications - Part 2: Physical layer specification and service definition	EN 61158-2	-
IEC 61158-3-18	-	Industrial communication networks - Fieldbus specifications - Part 3-18: Data-link layer service definition - Type 18 elements	EN 61158-3-18	-
IEC 61158-4-18	-	Industrial communication networks - Fieldbus specifications - Part 4-18: Data-link layer protocol specification - Type 18 elements	EN 61158-4-18	-
IEC 61158-5-18	-	Industrial communication networks - Fieldbus specifications - Part 5-18: Application layer service definition - Type 18 elements	EN 61158-5-18	-
IEC 61158-5-23	-	Industrial communication networks - Fieldbus specifications - Part 5-23: Application layer service definition - Type 23 elements	EN IEC 61158-5-23	-
IEC 61158-6-18	-	Industrial communication networks - Fieldbus specifications - Part 6-18: Application layer protocol specification - Type 18 elements	EN 61158-6-18	-

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
IEC 61158-6-23	-	Industrial communication networks - Fieldbus specifications - Part 6-23: Application layer protocol specification - Type 23 elements	EN IEC 61158-6-23	-
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	-
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	EN 61508	series
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 62061	-	Safety of machinery - Functional safety of safety-related control systems	EN IEC 62061	-
ISO/IEC/IEEE 8802-3	-	Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 3: Standard for Ethernet	-	-

CONTENTS

Nationaler Anhang NA (informativ) Auszugsweise Übersetzung	4
Annex ZA (normative) Normative references to international publications with their corresponding European publications	19
CONTENTS	21
0.1 General	27
0.2 Patent declaration	28
1 Scope	30
2 Normative references	30
3 Terms, definitions, symbols, abbreviated terms and conventions	31
3.1 Terms and definitions	31
3.1.1 Common terms and definitions	31
3.1.2 CPF 8: Additional terms and definitions	37
3.2 Symbols and abbreviated terms	38
3.2.1 Common symbols and abbreviated terms	38
3.2.2 CPF 8: Additional symbols and abbreviated terms	39
3.3 Conventions	39
4 Overview	39
5 General	39
6 Safety communication layer services	40
7 Safety communication layer protocol	40
8 Safety communication layer management	40
9 System requirements	40
10 Assessment	40
11 FSCP 8/1	40
11.1 Scope – FSCP 8/1	40
11.2 Normative references – FSCP 8/1	40
11.3 Terms, definitions, symbols, abbreviated terms and conventions – FSCP 8/1	40
11.4 Overview of FSCP 8/1 (CC-Link Safety™)	40
11.5 General – FSCP 8/1	41
11.5.1 External documents providing specifications for the profile	41
11.5.2 Safety functional requirements	41
11.5.3 Safety measures	41
11.5.4 Safety communication layer structure	43
11.5.5 Relationships with FAL (and DLL, PhL)	44
11.6 Safety communication layer services for FSCP 8/1	44
11.6.1 General	44
11.6.2 SASEs	44
11.6.3 SARs	45

11.6.4	Process data SAR ASEs	46
11.7	Safety communication layer protocol for FSCP 8/1	48
11.7.1	Safety PDU format	48
11.7.2	State description	56
11.8	Safety communication layer management for FSCP 8/1	61
11.8.1	General	61
11.8.2	Connection establishment and confirmation processing	61
11.8.3	Safety slave verification	61
11.9	System requirements for FSCP 8/1	62
11.9.1	Indicators and switches	62
11.9.2	Installation guidelines	63
11.9.3	Safety function response time	63
11.9.4	Duration of demands	65
11.9.5	Constraints for calculation of system characteristics	65
11.9.6	Maintenance	65
11.9.7	Safety manual	66
11.10	Assessment for FSCP 8/1	66
12	FSCP 8/2	66
12.1	Scope – FSCP 8/2	66
12.2	Normative references – FSCP 8/2	66
12.3	Terms, definitions, symbols, abbreviated terms and conventions – FSCP 8/2	66
12.4	Overview of FSCP 8/2 (CC-Link IE™ Safety communication function)	67
12.5	General – FSCP 8/2	67
12.5.1	External documents providing specifications for the profile	67
12.5.2	Safety functional requirements	67
12.5.3	Safety measures	68
12.5.4	Safety communication layer structure	72
12.5.5	Relationships with FAL (and DLL, PhL)	73
12.6	Safety communication layer services for FSCP 8/2	73
12.6.1	General	73
12.6.2	Connection reestablishment services	73
12.6.3	Data transmission services	74
12.6.4	Connection termination notification services	75
12.7	Safety communication layer protocol for FSCP 8/2	76
12.7.1	Safety PDU format	76
12.7.2	Safety FAL service protocol machine (SFSPM)	82
12.8	Safety communication layer management for FSCP 8/2	108
12.8.1	Parameter Definitions	108
12.8.2	Parameter Setup	115

12.8.3 Management Services.....	115
12.9 System requirements for FSCP 8/2	119
12.9.1 Indicators and switches	119
12.9.2 Installation guidelines	121
12.9.3 Safety function response time	121
12.9.4 Duration of demands	123
12.9.5 Constraints for calculation of system characteristics	123
12.9.6 Maintenance	124
12.9.7 Safety manual.....	125
12.10 Assessment for FSCP 8/2	125
Annex A (informative) Additional information for functional safety communication profiles of CPF 8	126
A.1 Hash function calculation for FSCP 8/1	126
A.2 Hash function calculation for FSCP 8/2	126
A.3 Meaning of response time calculation formula for FSCP 8/2	127
Annex B (informative) Information for assessment of the functional safety communication profiles of CPF 8	129
Bibliography	130
Figure 1 – Relationships of IEC 61784-3 with other standards (machinery).....	27
Figure 2 – Relationships of IEC 61784-3 with other standards (process).....	28
Figure 3 – Relationship between SCL and the other layers of IEC 61158 Type 18	44
Figure 4 – State diagram.....	57
Figure 5 – Detection of unintended repetition	69
Figure 6 – Detection of incorrect sequence.....	70
Figure 7 – Detection of loss.....	70
Figure 8 – Detection of unacceptable delay by time stamps.....	71
Figure 9 – Detection of unacceptable delay by timer.....	72
Figure 10 – Protocol Hierarchy	73
Figure 11 – Safety PDU Structure	76
Figure 12 – CTRL Configuration.....	77
Figure 13 – SASE-M and SASE-S TS	80
Figure 14 – S-Data during safety refresh	80
Figure 15 – S-Data not during safety refresh	80
Figure 16 – S-Data header configuration	81
Figure 17 – CRC calculation.....	82
Figure 18 – Communication models	82
Figure 19 – SFSPM state transition diagram	83
Figure 20 – Connection establishment sequence	85
Figure 21 – Optional sequence during connection establishment sequence.....	86
Figure 22 – Communication sequence during safety refresh communication	87

Figure 23 – Offset measurement and generation sequence during safety refresh communication	87
Figure 24 – SFSPM-M state transition diagram	88
Figure 25 – Sequence other than during safety refresh	92
Figure 26 – S-Connect-req.....	92
Figure 27 – S-InitConfirmNetPrm-req	93
Figure 28 – net_prm_list	93
Figure 29 – S-InitVerifyStnPrm-req.....	94
Figure 30 – stn_prm_list.....	94
Figure 31 – S-InvokeFunc-req.....	94
Figure 32 – S-WriteErrorInfo-req	95
Figure 33 – date_and_time_of_occurence.....	96
Figure 34 – SFSPM-S state transition diagram	97
Figure 35 – Sequence other than during safety refresh	102
Figure 36 – S-Connect-rsp.....	103
Figure 37 – S-InitConfirmNetPrm-rsp	103
Figure 38 – S-InitVerifyStnPrm-rsp.....	103
Figure 39 – S-InvokeFunc-rsp.....	104
Figure 40 – Offset calculation procedure of safety clock	105
Figure 41 – Relationship between transmission interval fluctuation and transmission_interval	109
Figure 42 – Calculation of allowable_refresh_interval	112
Figure 43 – Calculation of allowable_delay.....	115
Figure 44 – Calculation of response time between safety PLCs.....	121
Figure 45 – Constraints on N_{SE} and m	124
Figure A.1 – Allowable_delay and offset calculation deviation	128
Table 1 – Selection of the various measures for possible errors	42
Table 2 – M1 safety device manager attribute format	48
Table 3 – S1 safety device manager attribute format.....	48
Table 4 – M1 safety connection manager attribute format.....	48
Table 5 – S1 safety connection manager attribute format	49
Table 6 – M1 safety cyclic transmission attribute format	49
Table 7 – S1 safety cyclic transmission attribute format.....	50
Table 8 – M1 safety device manager attribute encoding	51
Table 9 – S1 safety device manager attribute encoding.....	51
Table 10 – M1 safety connection manager attribute encoding	51
Table 11 – S1 safety connection manager attribute encoding	52
Table 12 – M1 safety cyclic transmission attribute encoding	52
Table 13 – S1 safety cyclic transmission attribute encoding	55
Table 14 – Safety master monitor timer operation	59

Table 15 – Safety slave monitor timer operation	59
Table 16 – Safety data monitor timer operation	59
Table 17 – Details of connection establishment and confirmation processing.....	61
Table 18 – Details of slave information verification processing.....	61
Table 19 – Details of safety slave parameter transmission processing.....	62
Table 20 – Monitor LEDs.....	63
Table 21 – Safety function response time calculation	64
Table 22 – Safety function response time definition of terms	65
Table 23 – Selection of the various measures for possible errors.....	68
Table 24 – SS-Start	73
Table 25 – SS-Restart.....	74
Table 26 – SS-InvokeFunc.....	74
Table 27 – SS-Read.....	75
Table 28 – SS-Write.....	75
Table 29 – SS-Terminate	75
Table 30 – Safety PDU elements	76
Table 31 – CTRL Elements	77
Table 32 – State list	84
Table 33 – SFSPM-M timers	88
Table 34 – SFSPM-M state transition table.....	89
Table 35 – support_functions	93
Table 36 – error_category	95
Table 37 – error_category for AL errors.....	95
Table 38 – error_code.....	96
Table 39 – SFSPM-S timers.....	97
Table 40 – SFSPM-S state transition table	98
Table 41 – Parameters used by safety communication layer	108
Table 42 – SM-SetSafetyStationInfo.....	115
Table 43 – Safety station information setting parameters of SM-SetSafetyStationInfo.....	116
Table 44 – SM-SetSafetyNetworkParameter	116
Table 45 – Safety network parameters of SM-SetSafetyNetworkParameter	117
Table 46 – SM-GetSafetyStationInfo	117
Table 47 – Safety station information parameters of SM-GetSafetyStationInfo (Request)	117
Table 48 – Safety station information parameters of SM-GetSafetyStationInfo (Response).....	118
Table 49 – SM-GetSafetyNetworkParameter	118
Table 50 – Parameters of SM-GetSafetyNetworkParameter request.....	118
Table 51 – Parameters of SM-GetSafetyNetworkParameter response.....	119
Table 52 – Monitor LEDs.....	120
Table 53 – Communication port monitor LEDs.....	121

Table A.1 – Residual error probability for FSCP 8/1 CRC 126

Table A.2 – Residual error probability for FSCP 8/2 CRC 127

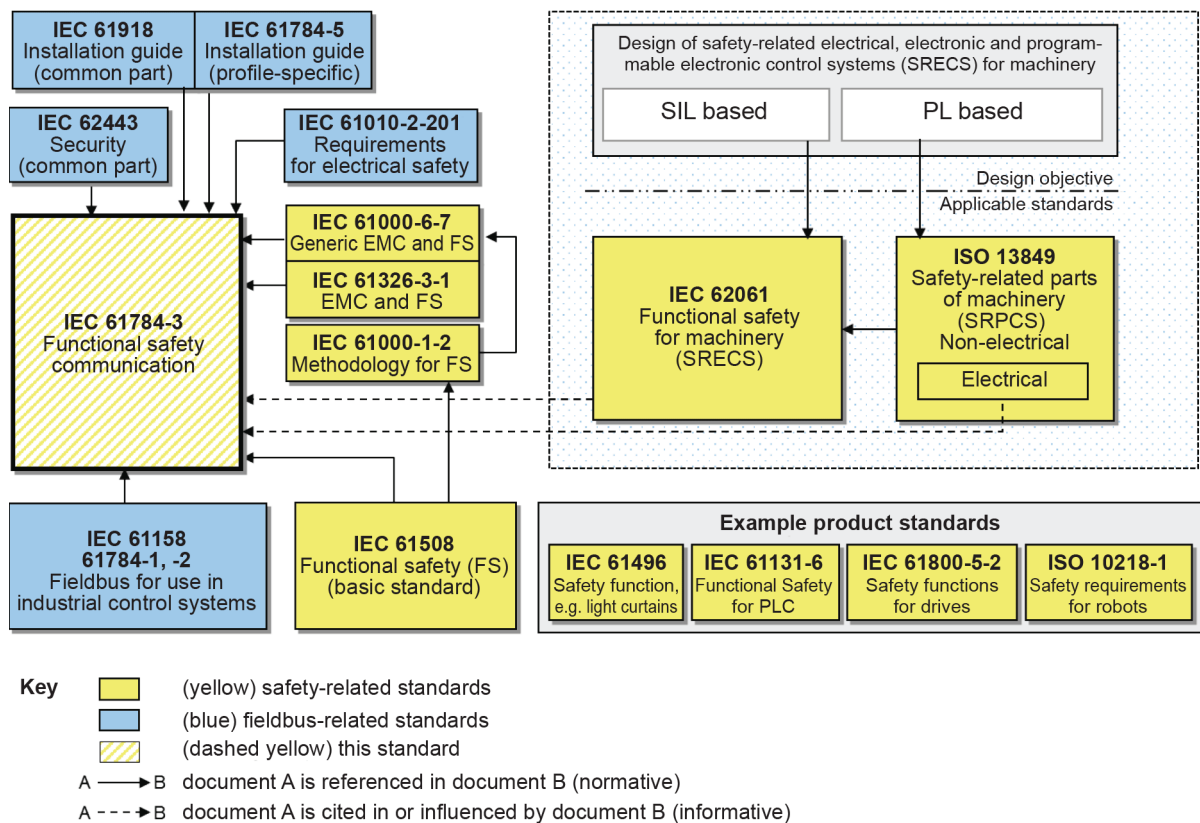
0 Introduction

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.

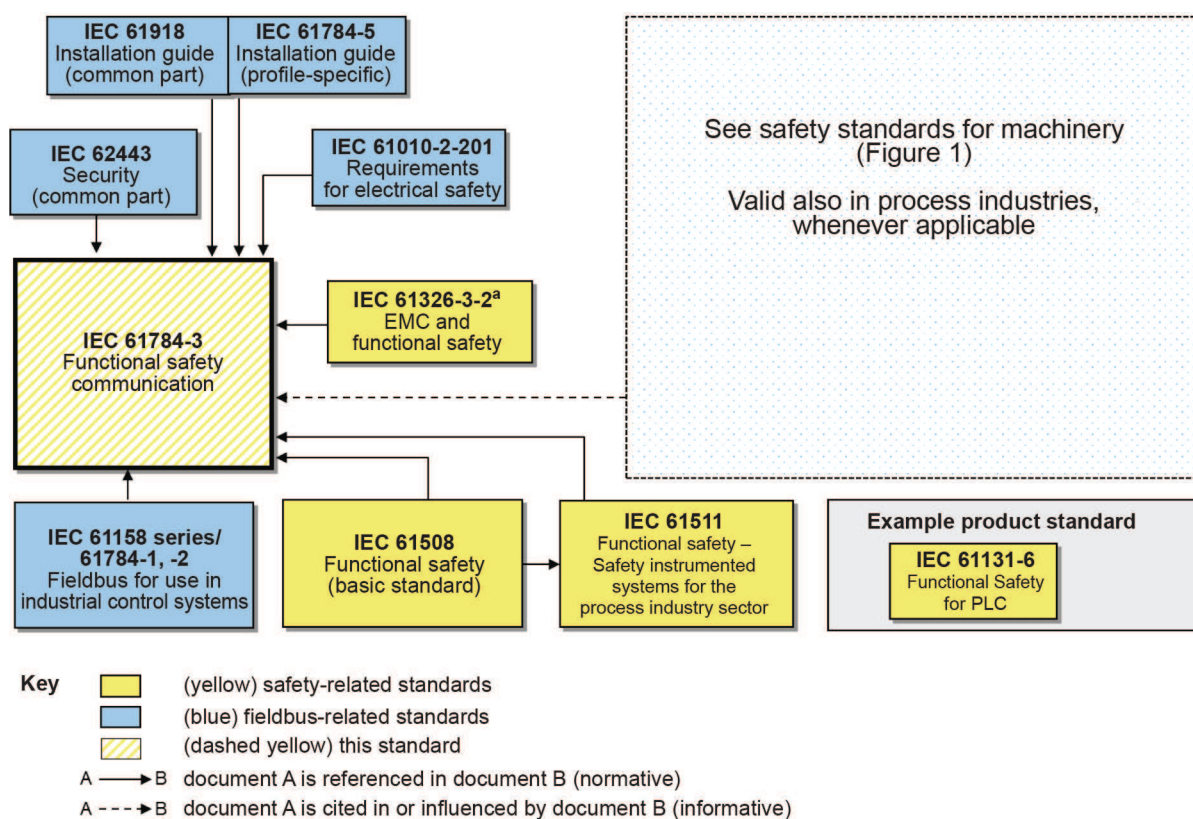


IEC

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 a patent concerning the functional safety communication profiles for family 8. IEC takes no position concerning the evidence, validity, and scope of this patent right.

The holder of this patent right 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 this patent right 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 3-8: Functional safety fieldbuses – Additional specifications for CPF 8

1 Scope

This part of IEC 61784-3 (all parts) specifies a safety communication layer (services and protocol) based on CPF 8 of IEC 61784-1, IEC 61784-2 and IEC 61158 Type 18 and Type 23. 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)³ 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 61131-2, *Industrial-process measurement and control – Programmable controllers – Part 2: Equipment requirements and tests*

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

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

IEC 61158-3-18, *Industrial communication networks – Fieldbus specifications – Part 3-18: Data-link layer service definition – Type 18 elements*

IEC 61158-4-18, *Industrial communication networks – Fieldbus specifications – Part 4-18: Data-link layer protocol specification – Type 18 elements*

³ In the following pages of this document, "IEC 61508" will be used for "IEC 61508 (all parts)".

IEC 61158-5-18, *Industrial communication networks – Fieldbus specifications – Part 5-18: Application layer service definition – Type 18 elements*

IEC 61158-5-23, *Industrial communication networks – Fieldbus specifications – Part 5-23: Application layer service definition – Type 23 elements*

IEC 61158-6-18, *Industrial communication networks – Fieldbus specifications – Part 6-18: Application layer protocol specification – Type 18 elements*

IEC 61158-6-23, *Industrial communication networks – Fieldbus specifications – Part 6-23: Application layer protocol specification – Type 23 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 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 62061, *Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems*

ISO/IEC/IEEE 8802-3, *Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 3: Standard for Ethernet*

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

absolute time stamp

time stamp referenced to a global time which is common for a group of devices using a *fieldbus*

[SOURCE: IEC 62280:2014, 3.1.1, modified – use of "devices" and "fieldbus" instead of "entities" and "transmission system"]

3.1.1.2

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]

3.1.1.3

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

bridge

abstract device that connects multiple network segments along the data link layer

3.1.1.6

closed communication system

fixed number or fixed maximum number of participants linked by a *communication system* with well-known and fixed properties, and where the *risk* of unauthorized access is considered negligible

[SOURCE: IEC 62280:2014, 3.1.6, modified – transmission replaced by communication]

3.1.1.7

communication channel

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

3.1.1.8

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

3.1.1.9

connection

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

3.1.1.10

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 [26], [27]⁴.

3.1.1.11
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

3.1.1.12
diversity

different means of performing a required function

Note 1 to entry: Diversity may be achieved by different physical methods or different design approaches.

[SOURCE: IEC 61508-4:2010, 3.3.7]

3.1.1.13
DLPDU
DEPRECATED: frame
Data Link Protocol Data Unit

3.1.1.14
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]

3.1.1.15
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]

3.1.1.16
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]

3.1.1.17
fieldbus

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

⁴ Figures in square brackets refer to the bibliography.

3.1.1.18

fieldbus system

system using a *fieldbus* with connected devices

3.1.1.19

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 [26], [27].

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

master

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

3.1.1.23

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]

3.1.1.24

message sink

information sink

part of a *communication system* in which *messages* are considered to be received

[SOURCE: ISO/IEC 2382:2015, 2123207, modified – deletion of notes and source]

3.1.1.25

message source

information source

part of a *communication system* from which *messages* are considered to originate

[SOURCE: ISO/IEC 2382:2015, 2123206, modified – deletion of notes and source]

3.1.1.26

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]

3.1.1.27

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]

3.1.1.28

relative time stamp

time stamp referenced to the local clock of an entity

Note 1 to entry: In general, there is no relationship to clocks of other entities.

[SOURCE: IEC 62280:2014, 3.1.43, modified – format adjusted]

3.1.1.29

residual error probability

RP

probability of an *error* undetected by the SCL *safety measures*

3.1.1.30

residual error rate

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

3.1.1.31

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]

3.1.1.32

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*.

3.1.1.33

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

3.1.1.34

safety connection

connection that utilizes the safety protocol for communications transactions

3.1.1.35

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.

3.1.1.36

safety device

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

3.1.1.37

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]

3.1.1.38

safety function response time

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.

3.1.1.39

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 "SILn *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]

3.1.1.40

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.

3.1.1.41

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*.

3.1.1.42

safety-related application

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

3.1.1.43

safety-related system

system performing *safety functions* according to IEC 61508

3.1.1.44

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

3.1.1.45

spurious trip

trip caused by the safety system without a process demand

3.1.1.46

timeliness code

time information included in a *message*

3.1.1.47

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.

3.1.1.48

white channel

defined communication system in which all relevant hardware and software elements are designed, implemented and validated according to IEC 61508

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

3.1.2 CPF 8: Additional terms and definitions

3.1.1.49

cycle

interval at which an activity is repetitively and continuously executed

3.1.1.50

safety application relationship

SAR

application relationship between two or more safety related application relationship endpoints

3.1.1.51

safety application service element

SASE

safety related application service element

3.1.1.52

safety clock

clock (counter) for recording the time of occurrence of events such as the transmission and reception of safety communication related messages

3.1.1.53

safety data monitor timer

timer used by the time expectation function for safety data transmission

3.1.1.54

safety monitor timer

timer used by the time expectation function for safety connection management

3.1.1.55

safety refresh

periodic transmission and reception of safety data between master and slave stations

3.1.1.56

slot

one quantum (granularity) of the position dependent mapping of the cyclic data fields

3.1.1.57

station

device and its corresponding SAREP associated with the transmission and reception of safety data

Note 1 to entry: The station number is used in the position dependent mapping of the cyclic data fields (a station occupies one or more slots).

3.1.1.58

safety protocol transmission information

information distinguishing safety relevant messages

3.2 Symbols and abbreviated terms

3.2.1 Common symbols and abbreviated terms

A-code	Authentication code	
CP	Communication Profile	[IEC 61784-1]
CPF	Communication Profile Family	[IEC 61784-1]
CRC	Cyclic Redundancy Check	
DLL	Data Link Layer	[ISO/IEC 7498-1]
DLPDU	Data Link Protocol Data Unit	
EMC	Electromagnetic Compatibility	
EUC	Equipment Under Control	[IEC 61508-4:2010]
E/E/PE	Electrical/Electronic/Programmable Electronic	[IEC 61508-4:2010]
FAL	Fieldbus Application Layer	[IEC 61158-5 (all parts)]
FS	Functional Safety	
FSCP	Functional Safety Communication Profile	
FSPM	FAL Service Protocol Machine	[IEC 61158-1]
MTBF	Mean Time Between Failures	
MTTF	Mean Time To Failure	
PDU	Protocol Data Unit	[ISO/IEC 7498-1]
Pe	Bit error probability	
PhL	Physical Layer	[ISO/IEC 7498-1]
PL	Performance Level	[ISO 13849-1]
PLC	Programmable Logic Controller	
SCL	Safety Communication Layer	
SIL	Safety Integrity Level	[IEC 61508-4:2010]
SPDU	Safety PDU	
T-code	Timeliness code	

3.2.2 CPF 8: Additional symbols and abbreviated terms

AR	Application Relationship
ASE	Application Service Element
CC	Carry Counter
CID	Connection Identifier
CMD	Command Data
LED	Light Emitting Diode
LID	Link Identifier
OBL	Offset Baseline
RNO	Running Number
SAR	Safety Application Relationship
SAREP	Safety Application Relationship Endpoint
SARPM	Safety Application Relationship Protocol State Machine
SASE	Safety Application Service Element
SFSPM	Safety FSPM (appended with -S Slave or -M Master)
SRC	Safety Relevant Controller
SRP	Safety Relevant Peripheral
TPI	Safety Transmission Packet Information
TPI-T	Safety Transmission Packet Information from master
TPI-R	Safety Transmission Packet Information from slave
TS	Time Stamp

3.3 Conventions

Conventions used in this document are defined in IEC 61158 Type 18 and Type 23, IEC 61784-1 CPF 8 and IEC 61784-2 CPF 8.

In order to assist the reader familiar with the standard clause numbering and for the purpose of consistency and alignment with IEC 61784-3, Clauses 4 to 10 reference Clauses 11 to 17 for FSCP 8/1 and Clauses 18 to 24 for FSCP 8/2.

4 Overview

For overview information pertaining to FSCP 8/1, see 11.4. For overview information pertaining to FSCP 8/2, see 12.4.

5 General

For general information pertaining to FSCP 8/1, see 11.5. For general information pertaining to FSCP 8/2, see 12.5.

6 Safety communication layer services

For safety communication layer services information pertaining to FSCP 8/1, see 11.6. For safety communication layer services information pertaining to FSCP 8/2, see 12.6.

7 Safety communication layer protocol

For safety communication layer protocol information pertaining to FSCP 8/1, see 11.7. For safety communication layer protocol information pertaining to FSCP 8/2, see 12.7.

8 Safety communication layer management

For safety communication layer management information pertaining to FSCP 8/1, see 11.8. For safety communication layer management information pertaining to FSCP 8/2, see 12.8.

9 System requirements

For system requirements information pertaining to FSCP 8/1, see 11.9. For system requirements information pertaining to FSCP 8/2, see 12.9.

10 Assessment

For assessment information pertaining to FSCP 8/1, see 11.10. For assessment information pertaining to FSCP 8/2, see 12.10.

11 FSCP 8/1

11.1 Scope – FSCP 8/1

See Clause 1.

11.2 Normative references – FSCP 8/1

See Clause 2.

11.3 Terms, definitions, symbols, abbreviated terms and conventions – FSCP 8/1

See Clause 3.

11.4 Overview of FSCP 8/1 (CC-Link Safety™)

Communication Profile Family 8 (commonly known as CC-Link™⁵) defines communication profiles based on IEC 61158-2 Type 18, IEC 61158-3-18, IEC 61158-4-18, IEC 61158-5-18, and IEC 61158-6-18.

⁵ CC-Link™ and CC-Link Safety™ are trade names of the non-profit organization CC-Link Partner Association. This information is given for the convenience of users of this document and does not constitute an endorsement by IEC of the trade name holder or any of its products. Compliance to this document does not require use of the trade names CC-Link™ or CC-Link Safety™. Use of the trade names CC-Link™ or CC-Link Safety™ requires permission of CC-Link Partner Association and compliance with conditions for their use (such as testing and validation).