

DIN EN 61784-3-8

ICS 35.160; 35.240.50

Ersatz für
DIN EN 61784-3-8:2012-03
Siehe Anwendungsbeginn

**Industrielle Kommunikationsnetze –
Profile –
Teil 3-8: Funktional sichere Übertragung bei Feldbussen –
Zusätzliche Festlegungen für die Kommunikationsprofilfamilie 8
(IEC 61784-3-8:2016);
Englische Fassung EN 61784-3-8:2017**

Industrial communication networks –
Profiles –
Part 3-8: Functional safety fieldbuses –
Additional specifications for CPF 8
(IEC 61784-3-8:2016);
English version EN 61784-3-8:2017

Réseaux de communication industriels –
Profils –
Partie 3-8: Bus de terrain de sécurité fonctionnelle –
Spécification supplémentaire pour CPF 8
(IEC 61784-3-8:2016);
Version anglaise EN 61784-3-8:2017

Gesamtumfang 123 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE

Anwendungsbeginn

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

Für DIN EN 61784-3-8:2012-03 besteht eine Übergangsfrist bis 2020-12-01.

Nationales Vorwort

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

Für dieses Dokument ist das nationale Arbeitsgremium UK 914.1 „Profile für funktional sichere Kommunikationssysteme“ der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE (www.dke.de) zuständig.

Die enthaltene IEC-Publikation wurde vom SC 65C „Industrial networks“ erarbeitet.

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

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

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

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

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

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

Da sich die Benutzer der vorliegenden Norm der englischen Sprache als Fachsprache bedienen, wird die Englische Fassung der EN 61784-3-8 veröffentlicht. Zu deren Abschnitt 0, Einleitung, Abschnitt 1, der den Anwendungsbereich festlegt, und Abschnitt 3, der die Begriffe, Symbole, Abkürzungen und Konventionen festlegt, wurde eine Übersetzung angefertigt die als informativer Nationaler Anhang NA Bestandteil der vorliegenden Norm ist. Für die meisten der verwendeten Begriffe existieren keine gebräuchlichen deutschen Begriffe, da sich die deutschen Anwender in der Regel ebenfalls der englischen Begriffe 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 61784-3-8:2012-03 wurden folgende Änderungen vorgenommen:

- a) FSCP 8/2 wurde hinzugefügt;
- b) FSCP 8/2, Abschnitt 12, wurde hinzugefügt;
- c) hinzugefügter Inhalt für FSCP 8/2 in den Abschnitten 1 bis 3 (Anwendungsbereich, normative Verweisungen, Begriffe);
- d) das bisherige FSCP 8/1 wurde in Abschnitt 11 verschoben (alle alten Überschriften wurden um eine Ebene heruntergestuft);
- e) die alten Abschnitte 4 bis 10 wurden umstrukturiert, um, soweit zutreffend, auf die geeigneten Unterabschnitte zu verweisen..

Frühere Ausgaben

DIN EN 61784-3-8: 2012-03

Nationaler Anhang NA (informativ)

Auszugsweise Übersetzung^{N1}

0 Einleitung

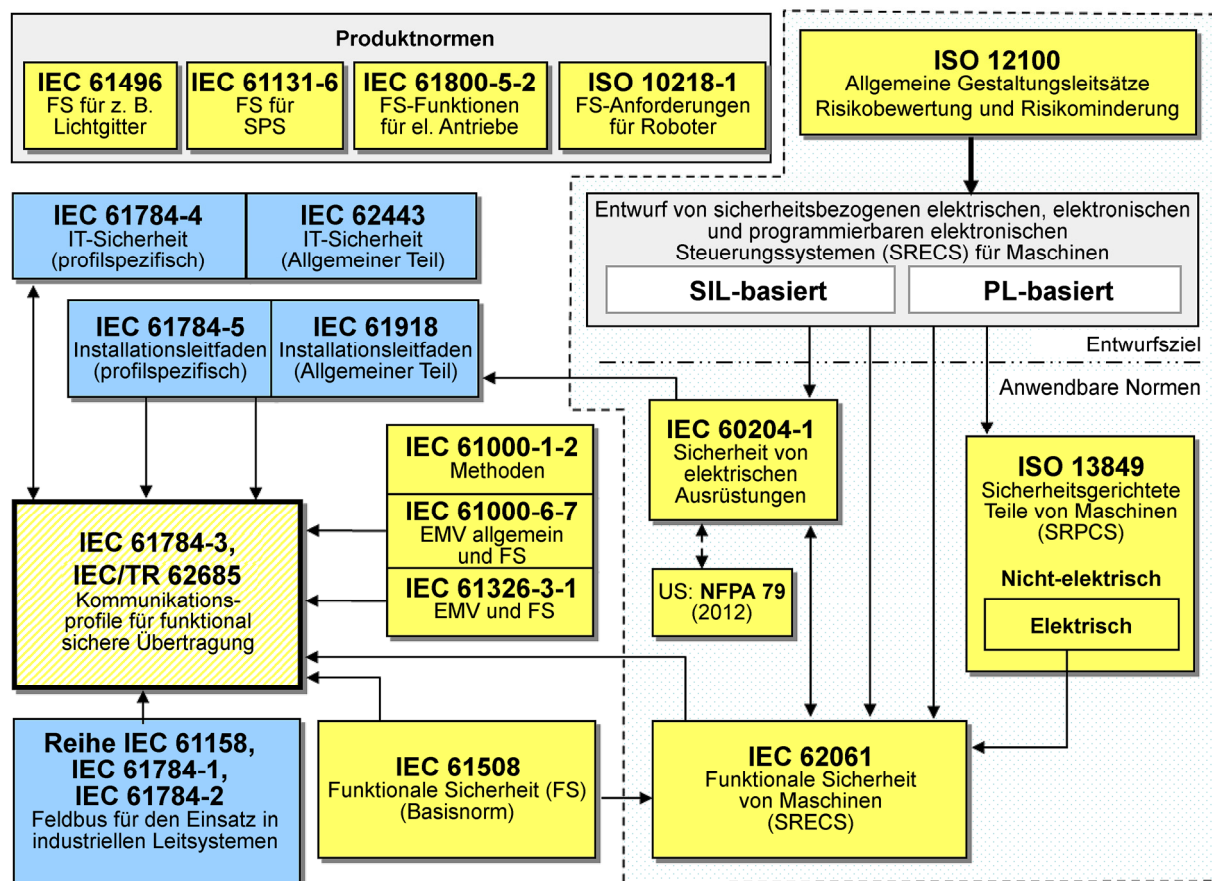
0.1 Allgemeines

Die IEC 61158-Feldbusnorm 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, funktionale Sicherheit und Informationssicherheit abzielen.

Diese Norm erläutert die relevanten Prinzipien für funktional sichere Kommunikation bezogen auf Normen der Reihe IEC 61508. Sie spezifiziert mehrere Sicherheitskommunikationsschichten (Profile und entsprechende Protokolle) basierend auf den Kommunikationsprofilen und Protokollschichten der IEC 61784-1, IEC 61784-2 und der Reihe IEC 61158. Sie deckt Aspekte der elektrischen Sicherheit und der Eigensicherheit nicht ab.

Bild 1 zeigt die Beziehungen dieser Norm zu für die Fertigungsautomatisierung relevanten Sicherheits- und Feldbusnormen.

^{N1} Nationale Fußnote: Die Nummerierung aus IEC 61784-3-8:2016-07 wurde beibehalten.



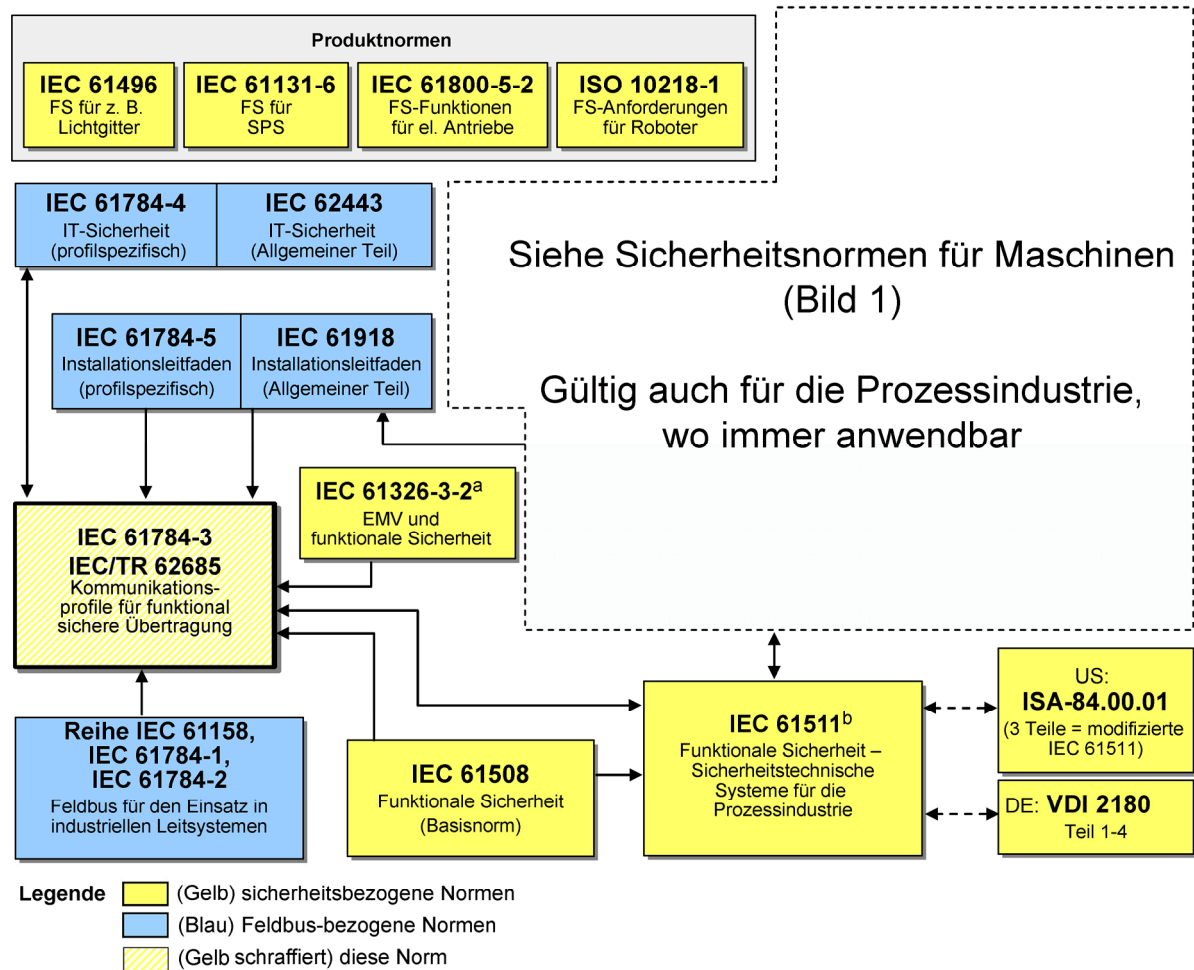
Legende

- (Gelb) sicherheitsbezogene Normen
- (Gelb) Feldbus-bezogene Normen
- (Gelbschraffiert) diese Norm

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

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

Bild 2 zeigt die Beziehungen dieser Norm zu für die Prozessautomatisierung relevanten Sicherheits- und Feldbusnormen.



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

^b Als EN ratifiziert.

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

Die als Bestandteile eines sicherheitsbezogenen Systems nach Reihe IEC 61508 implementierten Sicherheitskommunikationsschichten gewährleisten das notwendige Vertrauen in den Transport von Nachrichten (Informationen) zwischen zwei oder mehr Feldbusteilnehmern in einem sicherheitsbezogenen System bzw. ausreichendes Vertrauen in das Sicherheitsverhalten beim Auftreten von Feldbusfehlern oder -ausfällen.

Die in dieser Norm spezifizierten Sicherheitskommunikationsschichten tun dies dergestalt, dass ein Feldbus in Anwendungen mit funktionaler Sicherheit bis zu einer Sicherheitsstufe (SIL) eingesetzt werden kann, wie sie im jeweiligen Kommunikationsprofil für funktional sichere Übertragung festgelegt ist.

Der resultierende SIL-Anspruch eines Systems hängt von der Implementierung des gewählten Kommunikationsprofils für funktional sichere Übertragung (FSCP) in diesem System ab – eine Implementierung eines funktional sicheren Kommunikationsprofils in einem Standardgerät reicht nicht aus, um es als Sicherheitsgerät zu qualifizieren.

Diese Norm beschreibt:

- grundlegende Prinzipien für die Erfüllung der Anforderungen der Reihe IEC 61508 für die funktional sichere Kommunikation, einschließlich möglicher Übertragungsfehler, deren Abhilfemaßnahmen und Betrachtungen zur Datenintegrität;
- funktional sichere Kommunikationsprofile für mehrere Kommunikationsprofilfamilien der IEC 61784-1 und IEC 61784-2, welche Erweiterungen der Kommunikationsdienst- und -protokollabschnitte der Reihe IEC 61158 enthalten.

0.2 Patentangaben

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

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

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

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

Informationen sind erhältlich bei:

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

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

ISO (www.iso.org/patents) und IEC (<http://patents.iec.ch>) unterhalten Online-Datenbanken mit Patenten, die für ihre jeweiligen Normen relevant sind. Den Anwendern wird geraten, diese Datenbanken zu nutzen, um aktuellste Informationen über Patente zu erlangen.

1 Anwendungsbereich

Dieser Teil der Reihe IEC 61784-3 legt eine Sicherheitsschicht (Dienste und Protokoll) fest, die auf der Kommunikationsprofilfamilie 8 der IEC 61158, Typ 18 und Typ 23, IEC 61784-1 und IEC 61784-2, beruht. Er 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 Er 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 Teil¹ 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 61508² für funktionale Sicherheit. Diese Mechanismen dürfen in verschiedenen Industrieanwendungen verwendet werden, wie Prozesssteuerung, Fertigungsautomatisierung und Maschinen.

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

ANMERKUNG 2 Der resultierende SIL-Anspruch eines Systems hängt von der Implementierung des gewählten Kommunikationsprofils für funktional sichere Übertragung in diesem System ab – eine Implementierung eines funktional sicheren Kommunikationsprofils nach diesem Teil in einem Standardgerät reicht nicht aus, um es als Sicherheitsgerät zu qualifizieren.

3 Begriffe, Symbole, Abkürzungen und Konventionen

3.1 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

ANMERKUNG Kursive Schrift wird in den Definitionen verwendet, um Begriffe hervorzuheben, die ebenfalls in 3.1 definiert sind.

3.1.1 Allgemeine Begriffe

ANMERKUNG Diese allgemeinen Begriffe sind IEC 61784-3-3 entnommen.

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]

3.1.1.2

aktives Netzwerkelement

(en: active network element)

Netzwerkelement mit elektrischen und/oder optischen aktiven Bauteilen, die eine Erweiterung des Netzwerkes ermöglichen

¹ Auf den folgenden Seiten dieser Norm wird „dieser Teil“ im Sinne von „dieser Teil der Normenreihe IEC 61784-3“ verwendet.

² Auf den folgenden Seiten dieser Norm wird „IEC 61508“ im Sinne von „Normenreihe IEC 61508“ verwendet.

Anmerkung 1 zum Begriff: Beispiele für aktive Netzwerkelemente sind Signalverstärker und Switches.

[QUELLE: IEC 61918:2013, 3.1.2]

3.1.1.3

Verfügbarkeit

(en: availability)

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

3.1.1.4

Bitfehlerwahrscheinlichkeit

Pe

(en: bit error probability)

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

3.1.1.5

Black Channel

(en: black channel)

festgelegtes Kommunikationssystem, bestehend aus einem oder mehreren Elementen ohne Nachweis des Entwurfs oder der Validierung nach IEC 61508

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

3.1.1.6

Bridge

abstraktes (Kommunikations-)Element, welches auf der Ebene des Data Link Layer mehrere Netzwerksegmente verbindet

3.1.1.7

geschlossenes Kommunikationssystem

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

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

3.1.1.8

Kommunikationskanal

(en: communication channel)

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

3.1.1.9

Kommunikationssystem

(en: communication system)

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

3.1.1.10

Verbindung

(en: connection)

logische Verbindung zwischen zwei Anwendungsobjekten in demselben oder in unterschiedlichen Geräten

3.1.1.11

CRC-Prüfung

CRC

(en: cyclic redundancy check)

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

<Methode> Prozedur zur Berechnung der redundanten Daten

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

Anmerkung 2 zum Begriff: Siehe auch: [29], [30]⁴.

3.1.1.12

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 z. B. Aufbaubedingungen, elektromagnetische Störfestigkeit, industrielle (*aktive*) *Netzwerkkomponenten* und, wo das *Risiko* eines unerlaubten Zugriffs gemäß Lebenszyklusmodell der IEC 62443 auf ein toleriertes Maß reduziert ist, durch zum Beispiel Zonen und Durchleitungen

3.1.1.13

Diversität

(en: diversity)

ungleichartige Mittel zur Ausführung einer geforderten Funktion

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

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

3.1.1.14

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 andere Effekte.

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

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

3.1.1.15

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 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]

3.1.1.16

Fehlzustand

(en: fault)

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

⁴ Zahlen in eckigen Klammern verweisen auf die Literaturhinweise.

Anmerkung 1 zum Begriff: IEC 60050-191:1990, 191.05.01 definiert „fault“ als einen Zustand, der durch das Unvermögen gekennzeichnet ist, eine geforderte Funktion auszuführen, jedoch nicht durch dieses Unvermögen während vorbeugender Instandhaltung, anderer geplanter Aktionen oder auf Grund fehlender externer Betriebsmittel.

[QUELLE: IEC 61508-4:2010, 3.6.1, modifiziert – die Verweisung auf das Bild wurde 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

Telegrammrahmen

(en: frame)

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

3.1.1.20

Blockprüfzeichenfolge

FCS

(en: Frame Check Sequence)

redundante Daten, mittels Hash-Funktion aus einem Block von Daten in einer DLPDU abgeleitet und mit diesem 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 [34], [35].

3.1.1.21

Hash-Funktion

(en: hash function)

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

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

Anmerkung 2 zum Begriff: Gebräuchliche Hash-Funktionen schließen Parity-Bit, Quersummen oder CRC mit ein.

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

3.1.1.22

Gefährdung

(en: hazard)

Zustand oder Umstände in einem System, der/die zusammen mit weiteren Bedingungen zwangsläufig zu einem Schaden an Personen, Eigentum oder der Umwelt führt/führen

3.1.1.23

Master

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

3.1.1.24**Nachricht**

(en: message)

geordnete Folge von Oktets, bestimmt für die Übermittlung von Information

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

3.1.1.25**Nachrichtensenke**

(en: message sink)

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

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

3.1.1.26**Nachrichtenquelle**

(en: message source)

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

[QUELLE: ISO/IEC 2382-16:1996, 16.02.02]

3.1.1.27**Fehlauslösung**

(en: nuisance trip)

unberechtigte Auslösung ohne schädliche Wirkung

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

3.1.1.28**Performance Level****PL**

(en: performance level)

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

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

3.1.1.29**Schutzkleinspannung****PELV**

(en: protective extra-low-voltage)

Stromkreis, in dem unter Normalbedingungen oder unter den Bedingungen eines Einzelfehlers die Spannung AC 30 V, 42,4 V Scheitelwert oder DC 60 V nicht überschritten wird, ausgenommen durch *Erdungsfehler* in anderen Stromkreisen

Anmerkung 1 zum Begriff: Ein PELV-Stromkreis ähnelt einem SELV-Stromkreis, der mit einer Schutz Erde verbunden ist.

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

3.1.1.30**Redundanz**

(en: redundancy)

Vorhandensein von mehr als einem Mittel, um eine geforderte Funktion auszuführen oder eine Information darzustellen

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

3.1.1.31

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]

3.1.1.32

Zuverlässigkeit

(en: reliability)

Wahrscheinlichkeit, dass ein automatisiertes System eine geforderte Funktion unter bestimmten Voraussetzungen in einem bestimmten Zeitintervall (t_1 , t_2) ausführen kann

Anmerkung 1 zum Begriff: Es wird allgemein angenommen, dass das automatisierte System sich am Anfang des Zeitintervalls in einem Zustand befindet, um die geforderte Funktion ausführen zu können.

Anmerkung 2 zum Begriff: Die Benennung „Zuverlässigkeit“ wird ebenfalls zur Kennzeichnung der Überlebenswahrscheinlichkeit genutzt und durch die Wahrscheinlichkeit bemessen.

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

Anmerkung 4 zum Begriff: Zuverlässigkeit unterscheidet sich von *Verfügbarkeit*.

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

3.1.1.33

Restfehlerwahrscheinlichkeit

RP

(en: residual error probability)

Wahrscheinlichkeit eines *Fehlers*, dass er durch die *Sicherheitsmaßnahmen* im SCL nicht aufgedeckt wird

3.1.1.34

Restfehlerrate

(en: residual error rate)

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

3.1.1.35

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]

3.1.1.36

Sicherheitskommunikationskanal

(en: safety communication channel)

Kommunikationskanal beginnend auf der SCL der Nachrichtenquelle und endend auf der 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.

3.1.1.37**Sicherheitskommunikationsschicht****SCL**

(en: safety communication layer)

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

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

3.1.1.38**sichere Verbindung**

(en: safety connection)

Verbindung, welche das Sicherheitsprotokoll für Kommunikationstätigkeiten nutzt

3.1.1.39**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.

3.1.1.40**Sicherheitsgerät**

(en: safety device)

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

3.1.1.41**Sicherheitskleinspannung****SELV**

(en: safety extra-low-voltage)

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

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

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

3.1.1.42**Sicherheitsfunktion**

(en: safety function)

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

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

3.1.1.43**Reaktionszeit einer Sicherheitsfunktion**

(en: safety function response time)

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

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

3.1.1.44

Sicherheits-Integritätslevel

SIL

(en: safety integrity level)

eine von vier diskreten Stufen zur Spezifizierung der Anforderung für die Sicherheitsintegrität der Sicherheitsfunktionen, die dem E/E/PE-sicherheitsbezogenen System zugeordnet werden, 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 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]

3.1.1.45

Sicherheitsmaßnahme

(en: safety measure)

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

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

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

3.1.1.46

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 z. B. einem Schlüssel, einer fortlaufenden Nummer oder einem *Zeitstempel*, beinhalten.

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

3.1.1.47

sicherheitsbezogene Anwendung

(en: safety-related application)

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

3.1.1.48

sicherheitsbezogenes System

(en: safety-related system)

System, welches *Sicherheitsfunktionen* nach IEC 61508 ausführt

3.1.1.49**Slave**

(en: slave)

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

3.1.1.50**unberechtigte Auslösung**

(en: spurious trip)

Auslösung in einem Sicherheitssystem ohne Prozessanforderung

3.1.1.51**Zeitstempel**

(en: time stamp)

Zeitinformation in einer *Nachricht*

3.1.1.52**Gleichverteilung**

(en: uniform distribution)

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

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

3.1.1.53**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

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

3.1.2.3**Sicherheitsanwendungs-Dienstelement****SASE**

(en: safety application service element)

Serviceelement einer sicherheitsbezogenen Anwendung

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

3.1.2.4**Sicherheitsuhr**

Uhr (Zähler) zum Aufzeichnen des Zeitpunkts des Auftretens von Ereignissen, wie z. B. 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

Menge (Granularität) der positionsabhängigen Zuordnung der zyklischen Datenfelder

3.1.2.9

Station

Gerät und seine 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

CP	Kommunikationsprofil	[IEC 61784-1]
CPF	Kommunikationsprofilfamilie	[IEC 61784-1]
CRC	CRC-Prüfung	
DLL	Sicherungsschicht	[ISO/IEC 7498-1]
DLPDU	Protokolldateneinheit der Sicherungsschicht [en: data link protocol data unit]	
EMV	elektromagnetische Verträglichkeit [en: EMC]	
EUC	Prüfling [en: equipment under control]	[IEC 61508-4:2010]
E/E/PE	elektrisch/elektronisch/programmierbar elektronisch	[IEC 61508-4:2010]
FAL	Feldbusanwendungsschicht [en: fieldbus application layer]	[IEC 61158-5]
(FCS)	Blockprüfzeichenfolge	
FS	funktionale Sicherheit	
FSCP	funktional sicheres Kommunikationsprofil [en: functional safety communication profile]	
FSPM	FAL Service Protocol Machine	[IEC 61158-1]
MTBF	mittlere Zeit zwischen Ausfällen	
MTTF	mittlere Zeit bis zu einem Ausfall	
PDU	Protokolldateneinheit [en: protocol data unit]	[ISO/IEC 7498-1]

Pe	Bitfehlerwahrscheinlichkeit [en: bit error probability]	
PELV	Schutzkleinspannung	
PhL	Physical Layer	[ISO/IEC 7498-1]
PL	Performance Level [en: performance level]	[ISO 13849-1]
SPS	speicherprogrammierbare Steuerung [en: PLC]	
SCL	Sicherheitskommunikationsschicht	
SELV	Sicherheitskleinspannung	
SIL	Sicherheits-Integritätslevel	[IEC 61508-4:2010]
SPDU	Sicherheits-PDU	

3.2.2 CPF 8: Zusätzliche Symbole und Abkürzungen

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

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 festgelegt.

Als Hilfestellung für den Leser, der mit der Abschnittsbenummerung der Norm vertraut ist, und zum Zweck der Konsistenz und Angleichung an IEC 61784-3, Abschnitte 4 bis 10, wird verwiesen auf die Abschnitte 11 bis 17 für FSCP 8/1 und auf die Abschnitte 18 bis 24 für FSCP 8/2.

– Leerseite –

English Version

**Industrial communication networks - Profiles - Part 3-8:
Functional safety fieldbuses - Additional specifications for CPF 8
(IEC 61784-3-8:2016)**

Réseaux de communication industriels - Profils - Partie 3-8:
Bus de terrain de sécurité fonctionnelle - Spécification
supplémentaire pour CPF 8
(IEC 61784-3-8:2016)

Industrielle Kommunikationsnetze - Profile - Teil 3-8:
Funktional sichere Übertragung bei Feldbussen -
Zusätzliche Festlegungen für die
Kommunikationsprofilfamilie 8
(IEC 61784-3-8:2016)

This European Standard was approved by CENELEC on 2016-09-01. 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, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.



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

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

European foreword

The text of document 65C/851/FDIS, future edition 2 of IEC 61784-3-8:2016, 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 61784-3-8:2017.

The following dates are fixed:

- latest date by which this document has (dop) 2018-06-01
to be implemented at national level by
publication of an identical national
standard or by endorsement
- latest date by which the national (dow) 2020-12-01
standards conflicting with this
document have to be withdrawn

This document supersedes EN 61784-3-8:2010.

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 61784-3-8:2016 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 61000-6-7	NOTE Harmonized as EN 61000-6-7.
IEC 61131-6	NOTE Harmonized as EN 61131-6.
IEC 61496 (all parts)	NOTE Harmonized as EN 61496 (all parts).
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 61784-2	NOTE Harmonized as EN 61784-2.
IEC 61784-5 (all parts)	NOTE Harmonized as EN 61784-5 (all parts).
IEC 61800-5-2	NOTE Harmonized as EN 61800-5-2.
IEC 61918	NOTE Harmonized as EN 61918.
IEC 62443 (all parts)	NOTE Harmonized as prEN 62443 (all parts).
IEC/TR 62685	NOTE Harmonized as CLC/TR 62685.
ISO 10218-1	NOTE Harmonized as EN ISO 10218-1.
ISO 12100	NOTE Harmonized as EN ISO 12100.
ISO 13849-1	NOTE Harmonized as EN ISO 13849-1.
ISO 13849-2	NOTE Harmonized as EN ISO 13849-2.

CONTENTS

European foreword	2
0 Introduction	8
0.1 General.....	8
0.2 Patent declaration	10
1 Scope.....	11
2 Normative references	11
3 Terms, definitions, symbols, abbreviated terms and conventions	12
3.1 Terms and definitions	12
3.1.1 Common terms and definitions	13
3.1.2 CPF 8: Additional terms and definitions	19
3.2 Symbols and abbreviated terms.....	20
3.2.1 Common symbols and abbreviated terms.....	20
3.2.2 CPF 8: Additional symbols and abbreviated terms.....	21
3.3 Conventions.....	21
4 Overview	21
5 General	21
6 Safety communication layer services.....	22
7 Safety communication layer protocol	22
8 Safety communication layer management.....	22
9 System requirements	22
10 Assessment.....	22
11 FSCP 8/1	22
11.1 Scope – FSCP 8/1.....	22
11.2 Normative references – FSCP 8/1.....	22
11.3 Terms, definitions, symbols, abbreviated terms and conventions – FSCP 8/1.....	22
11.4 Overview of FSCP 8/1 (CC-Link Safety™)	22
11.5 General – FSCP 8/1	23
11.5.1 External documents providing specifications for the profile.....	23
11.5.2 Safety functional requirements	23
11.5.3 Safety measures	23
11.5.4 Safety communication layer structure	25
11.5.5 Relationships with FAL (and DLL, PhL).....	25
11.6 Safety communication layer services for FSCP 8/1	26
11.6.1 General	26
11.6.2 SASEs	26
11.6.3 SARs	27
11.6.4 Process data SAR ASEs	28
11.7 Safety communication layer protocol for FSCP 8/1	29
11.7.1 Safety PDU format	29
11.7.2 State description	35
11.8 Safety communication layer management for FSCP 8/1	39
11.8.1 General	39
11.8.2 Connection establishment and confirmation processing.....	40
11.8.3 Safety slave verification	40

11.9	System requirements for FSCP 8/1	41
11.9.1	Indicators and switches	41
11.9.2	Installation guidelines	42
11.9.3	Safety function response time	42
11.9.4	Duration of demands	44
11.9.5	Constraints for calculation of system characteristics	44
11.9.6	Maintenance	45
11.9.7	Safety manual	46
11.10	Assessment for FSCP 8/1	46
12	FSCP 8/2	46
12.1	Scope – FSCP 8/2	46
12.2	Normative references – FSCP 8/2	46
12.3	Terms, definitions, symbols, abbreviated terms and conventions – FSCP 8/2	46
12.4	Overview of FSCP 8/2 (CC-Link IE™ Safety communication function)	46
12.5	General – FSCP 8/2	47
12.5.1	External documents providing specifications for the profile	47
12.5.2	Safety functional requirements	47
12.5.3	Safety measures	48
12.5.4	Safety communication layer structure	52
12.5.5	Relationships with FAL (and DLL, PhL)	53
12.6	Safety communication layer services for FSCP 8/2	53
12.6.1	General	53
12.6.2	Connection reestablishment services	53
12.6.3	Data transmission services	54
12.6.4	Connection termination notification services	55
12.7	Safety communication layer protocol for FSCP 8/2	56
12.7.1	Safety PDU format	56
12.7.2	Safety FAL service protocol machine (SFSPM)	61
12.8	Safety communication layer management for FSCP 8/2	85
12.8.1	Parameter Definitions	85
12.8.2	Parameter Setup	89
12.8.3	Management Services	89
12.9	System requirements for FSCP 8/2	92
12.9.1	Indicators and switches	92
12.9.2	Installation guidelines	94
12.9.3	Safety function response time	94
12.9.4	Duration of demands	95
12.9.5	Constraints for calculation of system characteristics	95
12.9.6	Maintenance	97
12.9.7	Safety manual	97
12.10	Assessment for FSCP 8/2	98
Annex A (informative)	Additional information for functional safety communication profiles of CPF 8	99
A.1	Hash function calculation for FSCP 8/1	99
A.2	Hash function calculation for FSCP 8/2	99
A.3	Meaning of response time calculation formula for FSCP 8/2	99
Annex B (informative)	Information for assessment of the functional safety communication profiles of CPF 8	100

Bibliography	101
Annex ZA (normative) Normative references to international publications with their corresponding European publications	104
Figure 1 – Relationships of IEC 61784-3 with other standards (machinery).....	8
Figure 2 – Relationships of IEC 61784-3 with other standards (process)	9
Figure 3 – Relationship between SCL and the other layers of IEC 61158 Type 18	26
Figure 4 – State diagram.....	36
Figure 5 – Detection of unintended repetition	49
Figure 6 – Detection of incorrect sequence.....	50
Figure 7 – Detection of loss	50
Figure 8 – Detection of unacceptable delay by time stamps	51
Figure 9 – Detection of unacceptable delay by timer	52
Figure 10 – Protocol Hierarchy	53
Figure 11 – Safety PDU Structure	56
Figure 12 – CTRL Configuration	56
Figure 13 – SASE-M and SASE-S TS	59
Figure 14 – S-Data during safety refresh	59
Figure 15 – S-Data not during safety refresh	60
Figure 16 – S-Data header configuration	60
Figure 17 – CRC calculation.....	61
Figure 18 – Communication models.....	61
Figure 19 – SFSPM state transition diagram.....	62
Figure 20 – Connection establishment sequence	64
Figure 21 – Communication sequence during safety refresh communication.....	64
Figure 22 – Offset measurement and generation sequence during safety refresh communication	65
Figure 23 – SFSPM-M state transition diagram.....	66
Figure 24 – Sequence other than during safety refresh	69
Figure 25 – S-Connect-req	70
Figure 26 – S-InitConfirmNetPrm-req	71
Figure 27 – net_prm_list	71
Figure 28 – S-InitVerifyStnPrm-req.....	71
Figure 29 – stn_prm_list	72
Figure 30 – S-InvokeFunc-req	72
Figure 31 – S-WriteErrorInfo-req	73
Figure 32 – date_and_time_of_occurence	74
Figure 33 – SFSPM-S state transition diagram	75
Figure 34 – Sequence other than during safety refresh	79
Figure 35 – S-Connect-rsp	80
Figure 36 – S-InitConfirmNetPrm-rsp.....	80
Figure 37 – S-InitVerifyStnPrm-rsp	81
Figure 38 – S-InvokeFunc-rsp	81

Figure 39 – Offset calculation procedure of safety clock	83
Figure 40 – Relationship between transmission interval fluctuation and transmission_interval86	
Figure 41 – Calculation of allowable_refresh_interval	88
Figure 42 – Calculation of allowable_delay	89
Figure 43 – Calculation of response time between safety PLCs	94
Figure 44 – Relationship between safety connections and residual error rate	97
Figure A.1 – allowable_delay and offset calculation deviation	99

Table 1 – Selection of the various measures for possible errors.....	24
Table 2 – M1 safety device manager attribute format.....	29
Table 3 – S1 safety device manager attribute format	29
Table 4 – M1 safety connection manager attribute format	29
Table 5 – S1 safety connection manager attribute format.....	30
Table 6 – M1 safety cyclic transmission attribute format	30
Table 7 – S1 safety cyclic transmission attribute format.....	30
Table 8 – M1 safety device manager attribute encoding.....	31
Table 9 – S1 safety device manager attribute encoding	31
Table 10 – M1 safety connection manager attribute encoding	32
Table 11 – S1 safety connection manager attribute encoding.....	32
Table 12 – M1 safety cyclic transmission attribute encoding	32
Table 13 – S1 safety cyclic transmission attribute encoding.....	34
Table 14 – Safety master monitor timer operation.....	38
Table 15 – Safety slave monitor timer operation	38
Table 16 – Safety data monitor timer operation	38
Table 17 – Details of connection establishment and confirmation processing	40
Table 18 – Details of slave information verification processing.....	40
Table 19 – Details of safety slave parameter transmission processing	41
Table 20 – Monitor LEDs	42
Table 21 – Safety function response time calculation.....	43
Table 22 – Safety function response time definition of terms.....	43
Table 23 – Number of occupied slots and safety data	44
Table 24 – Residual error rate Λ (occupied slots = 1)	45
Table 25 – Residual error rate Λ (occupied slots = 2)	45
Table 26 – Selection of the various measures for possible errors	48
Table 27 – SS-Start	53
Table 28 – SS-Restart	54
Table 29 – SS-InvokeFunc.....	54
Table 30 – SS-Read	55
Table 31 – SS-Write	55
Table 32 – SS-Terminate	55
Table 33 – Safety PDU elements	56
Table 34 – CTRL Elements	57

Table 35 – State list.....	62
Table 36 – SFSPM-M timers	66
Table 37 – SFSPM-M state transition table.....	66
Table 38 – support_functions	70
Table 39 – error_category	73
Table 40 – error_category for AL errors.....	73
Table 41 – error_code.....	74
Table 42 – SFSPM-S timers	75
Table 43 – SFSPM-S state transition table	75
Table 44 – Parameters used by safety communication layer	85
Table 45 – SM-SetSafetyStationInfo.....	89
Table 46 – Safety station information setting parameters of SM-SetSafetyStationInfo	90
Table 47 – SM-SetSafetyNetworkParameter	90
Table 48 – Safety network parameters of SM-SetSafetyNetworkParameter	91
Table 49 – SM-GetSafetyStationInfo	91
Table 50 – Safety station information parameters of SM-GetSafetyStationInfo (Request).....	91
Table 51 – Safety station information parameters of SM-GetSafetyStationInfo (Response) ...	91
Table 52 – SM-GetSafetyNetworkParameter.....	92
Table 53 – Parameters of SM-GetSafetyNetworkParameter request.....	92
Table 54 – Parameters of SM-GetSafetyNetworkParameter response	92
Table 55 – Monitor LEDs.....	93
Table 56 – Communication port monitor LEDs	94

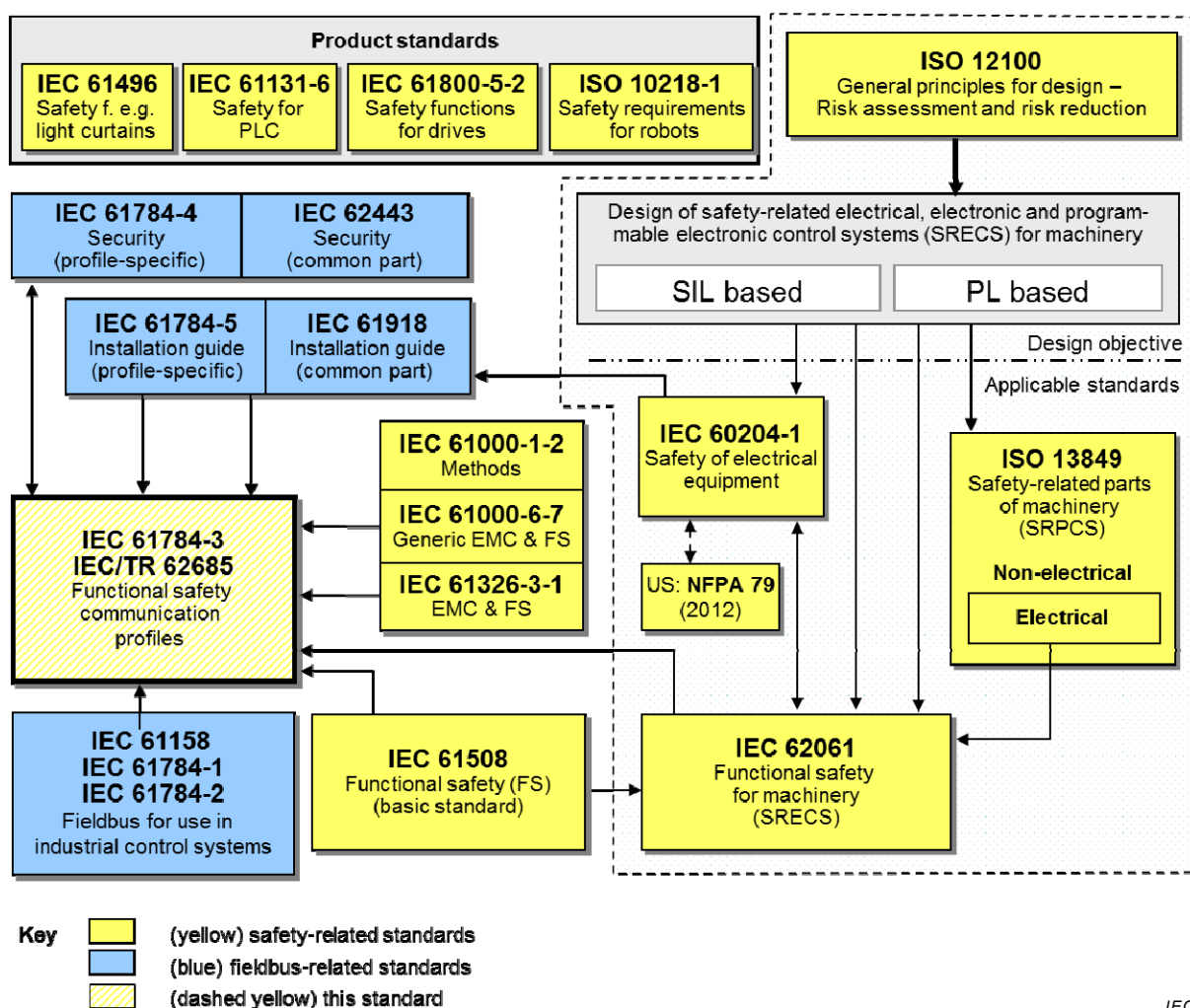
0 Introduction

0.1 General

The IEC 61158 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, safety-related and security-related applications.

This standard explains the relevant principles for functional safety communications with reference to IEC 61508 series 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 the IEC 61158 series. It does not cover electrical safety and intrinsic safety aspects.

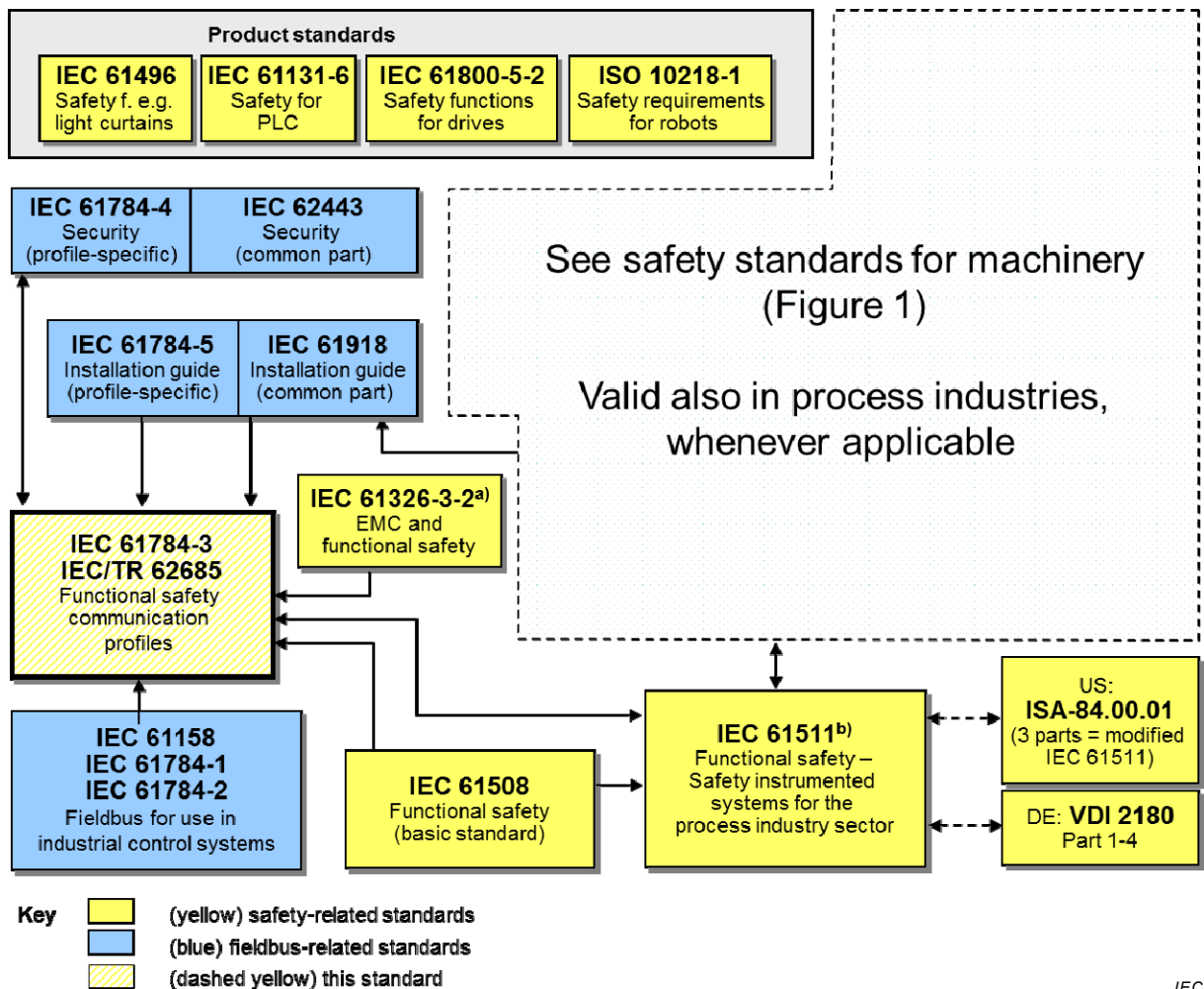
Figure 1 shows the relationships between this standard and relevant safety and fieldbus standards in a machinery environment.



NOTE Subclauses 6.7.6.4 (high complexity) and 6.7.8.1.6 (low complexity) of IEC 62061 specify the relationship between PL (Category) and SIL.

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

Figure 2 shows the relationships between this standard and relevant safety and fieldbus standards in a process environment.



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

^b EN ratified.

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 series 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 this standard 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.

This standard describes:

- basic principles for implementing the requirements of IEC 61508 series 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 the IEC 61158 series.

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 FSCP 8/2 given in Clause 12 as follows:

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

IEC takes no position concerning the evidence, validity and scope of this patent right.

The holder of this patent right has assured the IEC that he/she is willing to negotiate licences either free of charge or 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:

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

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

ISO (www.iso.org/patents) and IEC (<http://patents.iec.ch>) maintain on-line data bases of patents relevant to their standards. Users are encouraged to consult the data bases for the most up-to-date information concerning patents.

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES –

Part 3-8: Functional safety fieldbuses – Additional specifications for CPF 8

1 Scope

This part of the IEC 61784-3 series 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 part¹ 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 series² for functional safety. These mechanisms may be used in various industrial applications such as process control, manufacturing automation and machinery.

This part 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 part in a standard device is not sufficient to qualify it as a safety device.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. 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 61131-2:2007, *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*

¹ In the following pages of this standard, “this part” will be used for “this part of the IEC 61784-3 series”.

² In the following pages of this standard, “IEC 61508” will be used for “IEC 61508 series”.

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 8802-3*

IEC 61784-3:—³, *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*

IEEE 802.3, *IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method And Physical Layer Specifications*

3 Terms, definitions, symbols, abbreviated terms and conventions

3.1 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

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

³ To be published.

3.1.1 Common terms and definitions

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

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 devices and fieldbus]

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 61918:2013, 3.1.2]

3.1.1.3

availability

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

3.1.1.4

bit error probability

P_e

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

3.1.1.5

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.

3.1.1.6

bridge

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

3.1.1.7

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]

3.1.1.8

communication channel

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

3.1.1.9

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

3.1.1.10

connection

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

3.1.1.11

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 standard to refer to the redundant data.

Note 2 to entry: See also [29], [30]⁴.

3.1.1.12

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, using for example zones and conduits

3.1.1.13

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]

3.1.1.14

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]

⁴ Figures in square brackets refer to the bibliography.

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

3.1.1.18

fieldbus system

system using a *fieldbus* with connected devices

3.1.1.19

frame

denigrated synonym for DLPDU

3.1.1.20

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 [29], [30].

3.1.1.21

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.

[SOURCE: IEC TR 62210:2003, 4.1.12, modified – addition of “usually” and notes]

3.1.1.22

hazard

state or set of conditions of a system that, together with other related conditions will inevitably lead to harm to persons, property or environment

3.1.1.23

master

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

3.1.1.24

message

ordered series of octets intended to convey information

[SOURCE: ISO/IEC 2382-16:1996, 16.02.01, modified – character replaced by octet]

3.1.1.25

message sink

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

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

3.1.1.26

message source

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

[SOURCE: ISO/IEC 2382-16:1996, 16.02.02]

3.1.1.27

nuisance trip

spurious trip with no harmful effect

Note 1 to entry: Internal abnormal *errors* can be caused in *communication systems* such as wireless transmission, for example by too many retries in the presence of interferences.

3.1.1.28

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 13849-1:2006, 3.1.23]

3.1.1.29

protective extra-low-voltage

PELV

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

Note 1 to entry: A PELV circuit is similar to an SELV circuit that is connected to protective earth.

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

3.1.1.30

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]

3.1.1.31

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]

3.1.1.32

reliability

probability that an automated system can perform a required function under given conditions for a given time interval (t_1, t_2)

Note 1 to entry: It is generally assumed that the automated system is in a state to perform this required function at the beginning of the time interval.

Note 2 to entry: The term "reliability" is also used to denote the reliability performance quantified by this probability.

Note 3 to entry: Within the MTBF or MTTF period of time, the probability that an automated system will perform a required function under given conditions is decreasing.

Note 4 to entry: Reliability differs from *availability*.

[SOURCE: IEC 62059-11:2002, 3.17, modified – use automated system, two notes added]

3.1.1.33 **residual error probability**

RP

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

3.1.1.34 **residual error rate**

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

3.1.1.35 **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], [SOURCE: ISO/IEC Guide 51:2014, definition 3.9, modified – different note]

3.1.1.36 **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*.

3.1.1.37 **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

Note 1 to entry: This note applies to the French language only.

3.1.1.38 **safety connection**

connection that utilizes the safety protocol for communications transactions

3.1.1.39 **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.

3.1.1.40 **safety device**

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

3.1.1.41

safety extra-low-voltage

SELV

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

Note 1 to entry: An SELV circuit is not connected to protective earth.

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

3.1.1.42

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]

3.1.1.43

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:—, 5.2.4 and addressed by the functional safety communication profiles defined in this part.

3.1.1.44

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]

3.1.1.45

safety measure

<this standard> 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:—, 5.3 and 5.4.

3.1.1.46

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*.

3.1.1.47

safety-related application

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

3.1.1.48

safety-related system

system performing *safety functions* according to IEC 61508

3.1.1.49

slave

passive communication entity able to receive *messages* and send them in response to another communication entity which may be a *master* or a slave

3.1.1.50

spurious trip

trip caused by the safety system without a process demand

3.1.1.51

time stamp

time information included in a *message*

3.1.1.52

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.

3.1.1.53

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

3.1.2.1

cycle

interval at which an activity is repetitively and continuously executed

3.1.2.2

safety application relationship

SAR

application relationship between two or more safety related application relationship endpoints

Note 1 to entry: This note applies to the French language only.

3.1.2.3

safety application service element

SASE

safety related application service element

Note 1 to entry: This note applies to the French language only.