

DIN EN 61784-3-13

ICS 35.160; 35.240.50

Ersatz für
DIN EN 61784-3-13:2012-03
Siehe Anwendungsbeginn

**Industrielle Kommunikationsnetze –
Profile –
Teil 3-13: Funktional sichere Übertragung bei Feldbussen –
Zusätzliche Festlegungen für die Kommunikationsprofilfamilie 13
(IEC 61784-3-13:2016);
Englische Fassung EN 61784-3-13:2017**

Industrial communication networks –

Profiles –

Part 3-13: Functional safety fieldbuses – Additional specifications for CPF 13

(IEC 61784-3-13:2016);

English version EN 61784-3-13:2017

Réseaux de communication industriels –

Profils –

Partie 3-13: Bus de terrain de sécurité fonctionnelle – Spécifications complémentaires pour CPF 13

(IEC 61784-3-13:2016);

Version anglaise EN 61784-3-13:2017

Gesamtumfang 201 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE

Anwendungsbeginn

Anwendungsbeginn für die von CENELEC am 2016-08-19 angenommene Europäische Norm als DIN-Norm ist 2018-09-01.

Für DIN EN 61784-3-13:2012-03 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 61784-3-13 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 61784-3-13:2012-03 wurden folgende Änderungen vorgenommen:

- a) Änderung des Handelsnamens in „openSAFETY™“;
- b) Hinzufügung von „Slim Safety PDU“;

- c) Hinzufügung von „SOD CRC“;
- d) Hinzufügung von „SSDO block transfer services“;
- e) Hinzufügung von „connection valid bit“ zu „SPDO“;
- f) Hinzufügung von „number of retries for reset guarding“;
- g) Hinzufügung von jederzeit schreibbaren User-Parametern;
- h) Korrekturen und redaktionelle Verbesserungen.

Frühere Ausgaben

DIN EN 61784-3-13: 2012-03

Nationaler Anhang NA (informativ)

Auszugsweise Übersetzung^{N1}

0 Einleitung

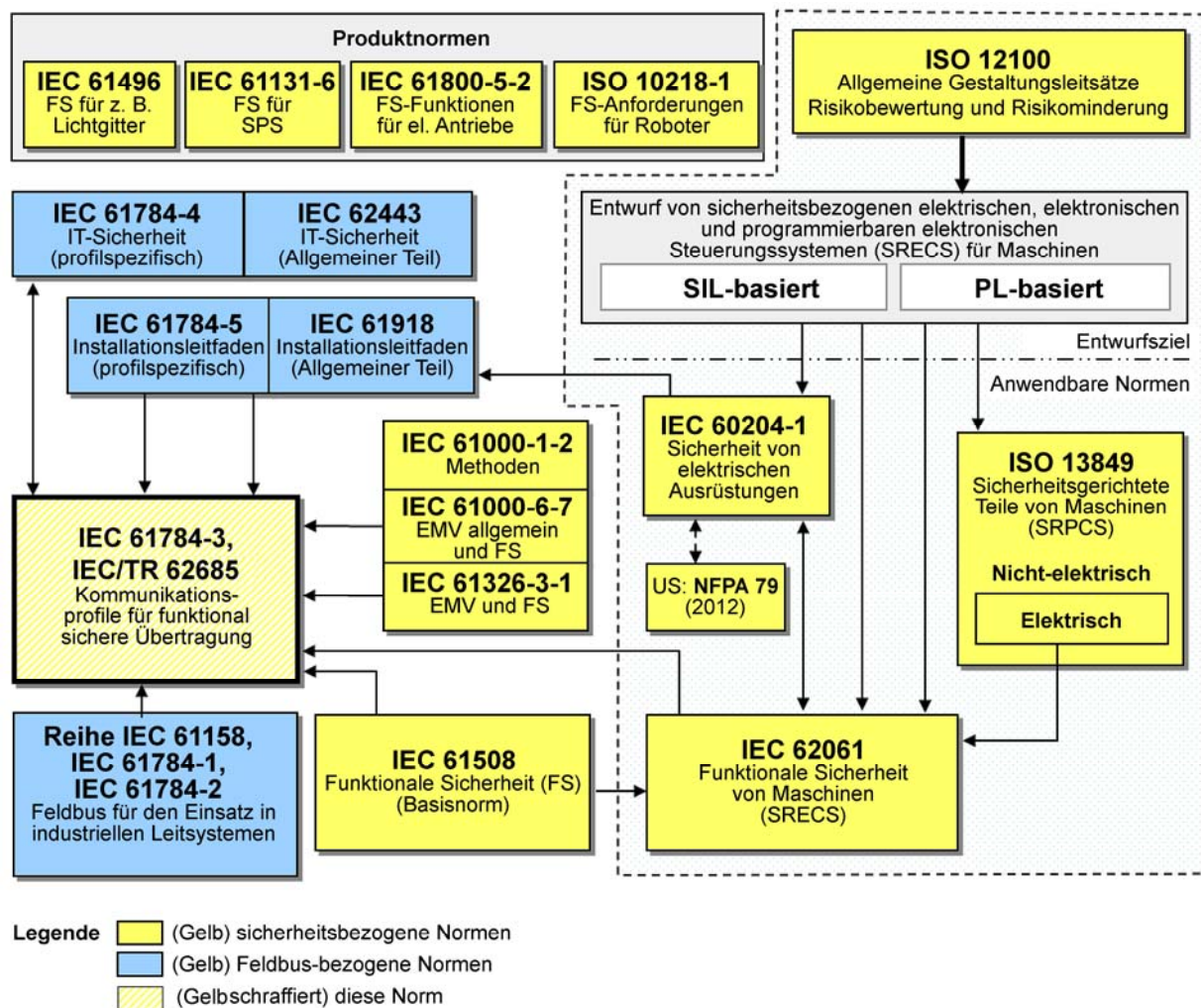
0.1 Allgemeines

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.

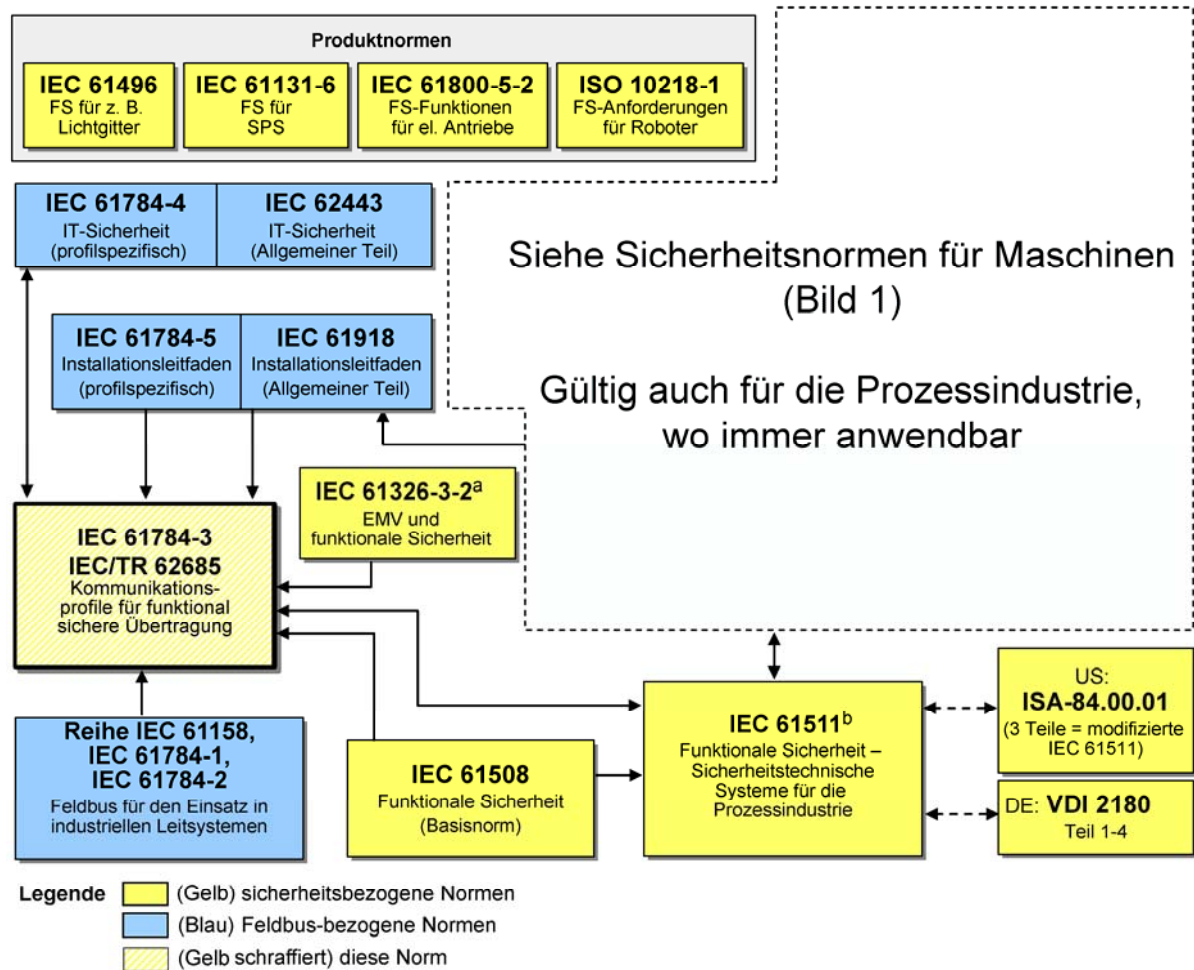
^{N1} Nationale Fußnote: Die Nummerierung aus IEC 61784-3-13:2016-07 wurde beibehalten.



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 mit 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 Ergänzungen der Kommunikationsdienst- und -protokollabschnitte der Reihe IEC 61158 um eine Sicherheitsschicht enthalten.

0.2 Patentangaben

Die Organisation International Electrotechnical Commission (IEC) weist auf Ansprüche hin, die es für eine Übereinstimmung mit diesem Dokument notwendig machen, von Patenten Gebrauch zu machen. Dies betrifft funktional sichere Kommunikationsprofile für die Familie 13, bei denen die Bezeichnung [xx] den Halter der Patentrechte angibt:

AT 504739	[BR]	Anordnung und ein Verfahren zur sicheren Datenkommunikation über ein nicht sicheres Netzwerk
DE 102005032877.6	[BR]	Verfahren zur Zeitsynchronisation von Teilnehmern eines Netzwerkes
DE 102004055685.7	[BR]	Verfahren zur Abgrenzung eines sicheren Netzwerkes
DE 102004055684.9	[BR]	Verfahren zur Absicherung des Datentransfers in einem sicheren Netzwerk mit CRC's variabler Länge
EP 08150038.1	[BR]	Anordnung und ein Verfahren zur sicheren Datenkommunikation über ein nicht sicheres Netzwerk

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:

[BR] Bernecker + Rainer
Industrie-Elektronik Ges.m.b.H.
B&R Straße 1
5142 Eggelsberg
ÖSTERREICH

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

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

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

1 Anwendungsbereich

Dieser Teil der Reihe IEC 61784-3 legt eine Sicherheitskommunikationsschicht (Dienste und Protokoll) auf Basis von CPF 13 in IEC 61784-2 und IEC 61158, Typ 13 fest. 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

Verfügbarkeit

(en: availability)

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

3.1.1.2

Bitfehlerwahrscheinlichkeit

(**P_e**)

en: bit error probability)

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

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.

3.1.1.3

Black Channel

(en: black channel)

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

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

3.1.1.4

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]

3.1.1.5

Kommunikationskanal

(en: communication channel)

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

3.1.1.6

Kommunikationssystem

(en: communication system)

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

3.1.1.7

Verbindung

(en: connection)

logische Verbindung zwischen zwei Anwendungsobjekten in demselben oder in unterschiedlichen Geräten

3.1.1.8

CRC-Prüfung

CRC

(en: cyclic redundancy check)

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

<Methode> Prozedur zur Berechnung der redundanten Daten

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

Anmerkung 2 zum Begriff: Siehe auch: [38], [39]³⁾.

3.1.1.9

festgelegtes Kommunikationssystem

[en: defined communication system; defined channel]

festgelegte Anzahl oder festgelegte maximale Anzahl von Teilnehmern, die über ein *Kommunikationssystem* verbunden sind, mit wohldefinierten und festgelegten Eigenschaften wie 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⁾ Zahlen in eckigen Klammern verweisen auf die Literaturhinweise.

3.1.1.10**Fehler**

(en: error)

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

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

3.1.1.11**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 ersetzt]

3.1.1.12**Fehlzustand**

(en: fault)

nicht normale Bedingung, die eine Verringerung oder den Verlust der Fähigkeit einer Funktionseinheit auslösen 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 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]

3.1.1.13**Feldbus**

(en: fieldbus)

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

3.1.1.14**Feldbussystem**

(en: fieldbus system)

System mit einem *Feldbus* und angeschlossenen Geräten

3.1.1.15**DLPDU**

ABGELEHNT: Rahmen

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

3.1.1.16**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]

3.1.1.17

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

3.1.1.18

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 Octet ersetzt]

3.1.1.19

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]

3.1.1.20

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]

3.1.1.21

Zuverlässigkeit

(en: reliability)

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

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

Anmerkung 2 zum Begriff: Der Begriff „Zuverlässigkeit“ wird ebenfalls zur Kennzeichnung der Überlebenswahrscheinlichkeit (en: reliability performance) genutzt und durch die Wahrscheinlichkeit bemessen.

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

Anmerkung 4 zum Begriff: Zuverlässigkeit unterscheidet sich von Verfügbarkeit.

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

3.1.1.22

Restfehlerrate

(en: residual error rate)

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

3.1.1.23**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, 3.9, modifiziert – andere Anmerkung]

3.1.1.24**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.

3.1.1.25**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

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

3.1.1.26**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.

3.1.1.27**Sicherheitsgerät**

(en: safety device)

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

3.1.1.28**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 die EUC zu erreichen oder aufrechtzuerhalten

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

3.1.1.29**Reaktionszeit einer Sicherheitsfunktion**

(en: safety function response time)

im ungünstigsten Fall benötigte Zeit nach Aktivierung eines am *Feldbus* angeschlossenen Sicherheitsensors, 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.

3.1.1.30

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]

3.1.1.31

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.

3.1.1.32

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.

3.1.1.33

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

3.1.1.34

sicherheitsbezogenes System

(en: safety-related system)

System, welches *Sicherheitsfunktionen* nach IEC 61508 ausführt

3.1.1.35**Slave**

(en: slave)

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

3.1.1.36**Zeitstempel**

(en: time stamp)

Zeitinformation in einer *Nachricht*

3.1.2 CPF 13: Zusätzliche Begriffe**3.1.2.1****Bitfehlerquote**

(en: bit error rate)

Wahrscheinlichkeit einer Fehldeutung eines Bits aufgrund von Elektroräuschen

3.1.2.2**DVI**

(en: device vendor information)

Informationen für die Identifizierung eines *Sicherheitsknotens*

3.1.2.3**Sicherheitsadresse****SADR**

(en: safety address)

Adresse eines *Sicherheitsknotens* in einer *Sicherheitsdomäne*

3.1.2.4**SCM**

(en: safety configuration manager)

Dienst, der für die Verwaltung von sicherheitsbezogenen Diensten verantwortlich ist

Anmerkung 1 zum Begriff: Beispiele von verwalteten sicherheitsbezogenen Diensten sind Konfiguration, Parametrisierung.

3.1.2.5**Sicherheitsknoten****SN**

(en: safety node)

Knoten mit *Sicherheitsfunktion*

3.1.2.6**Sicherheitsdomäne****SD**

(en: safety domain)

Adressbereich für bis zu 1 023 *Sicherheitsknoten*

3.1.2.7**Sicherheitsdomänen-Gateway****SDG**

(en: safety domain gateway)

Gateway für den Austausch von Daten zwischen verschiedenen *Sicherheitsdomänen*

3.1.2.8**Nummer der Sicherheitsdomäne****SDN**

(en: safety domain number)

Identifikation einer *Sicherheitsdomäne*

3.1.2.9

SNMT

(en: safety network management)

Dienste für die Verwaltung der Sicherheitsschicht

3.1.2.10

SOD

(en: safety object dictionary)

Repositorium für alle Datenobjekte, die mittels Diensten des funktionalen Sicherheitsfeldbusses zugänglich sind

3.1.2.11

Sicherheitsprozessdatenobjekt

SPDO

(en: safety process data object)

Objekt für den Austausch von Prozessdaten zwischen verschiedenen *Sicherheitsknoten*

3.1.2.12

Sicherheitsservicedatenobjekt

SSDO

(en: safety service data object)

Objekt für den Austausch von Servicedaten zwischen *Sicherheitsknoten*

3.1.2.13

Initialisierung

(en: initialization)

Ausgangskommunikationszustand von *Sicherheitsknoten*

3.1.2.14

Betrieb

(en: operational)

Kommunikationszustand von *Sicherheitsknoten*, in dem alle funktionalen Sicherheitsfunktionen ordnungsgemäß ausgeführt werden

3.1.2.15

Vor-Betrieb

(en: pre-operational)

Kommunikationszustand von *Sicherheitsknoten*, in dem sich alle Anwendungsausgaben in einem sicheren Zustand befinden

3.1.2.16

UDID

(en: unique device identification)

weltweite eindeutige Identifikation eines Geräts

3.2 Symbole und Abkürzungen

3.2.1 Allgemeine Symbole und Abkürzungen

CP	Kommunikationsprofil	[IEC 61784-1]
CPF	Kommunikationsprofilfamilie	[IEC 61784-1]
CRC	zyklische Redundanzprüfung	
DLL	Sicherungsschicht	[ISO/IEC 7498-1]
DLDPDU	Data Link Protocol Data Unit	
EMC	elektromagnetische Verträglichkeit (EMV)	
EUC	Prüfling (en: equipment under control)	[IEC 61508-4:2010]
E/E/PE	elektrisch/elektronisch/programmierbar elektronisch	[IEC 61508-4:2010]

FAL	Feldbus-Anwendungsschicht	[IEC 61158-5]
FS	funktionale Sicherheit	
FSCP	Kommunikationsprofil für funktional sichere Übertragung (en: functional safety communication profile)	
MTBF	mittlere Betriebszeit zwischen Ausfällen	
MTTF	mittlere Betriebszeit bis zum Ausfall	
PDU	Protokolldateneinheit (en: protocol data unit)	[ISO/IEC 7498-1]
PFH	mittlere Häufigkeit eines gefahrbringenden Ausfalls je Stunde [h^{-1}]	[IEC 61508-4:2010]
PhL	Physical Layer	[ISO/IEC 7498-1]
PL	Performance Level (en: performance level)	[ISO 13849-1]
PLC	speicherprogrammierbare Steuerung (SPS) (en: programmable logic controller)	
SCL	Sicherheitskommunikationsschicht (en: safety communication layer)	
SIL	Sicherheits-Integritätslevel	[IEC 61508-4:2010]
SPDU	Sicherheits-PDU	

3.2.2 CPF 13: Symbole und Abkürzungen

ACM	automatischer Konfigurationsmodus (en: automatic configuration mode)	
ADR	Wählinformation (Quelle oder Ziel)	
APDU	Anwendungsprotokoll-Dateneinheit (en: application protocol data unit)	[ISO/IEC 7498-1]
CN	gesteuerter Knoten	[IEC 61158-3-13]
CT	(en: consecutive time field)	
DBx	Datenoktett	
DSADR	Ziel-Sicherheitsadresse (en: destination SADR)	
DVI	(en: device vendor information)	
ID	PDU-Identifizierung	
LE	Längenfeld	
LSB	niedrigstwertiges Oktett	
MAC	Medienzugriffsschicht (en: medium access layer)	
MCM	manueller Konfigurationsmodus	
MN	Steuerungsknoten	[IEC 61158-3-13]
MSB	höchstwertiges Oktett	
PDO	Prozessdatenobjekt (en: process data object)	[IEC 61158-3-13]
RxSPDO	(en: receive process data objects)	
SADR	Sicherheitsadresse (en: safety address)	
SCM	(en: safety configuration manager)	
SCT	(en: safety control time)	
SD	Sicherheitsdomäne (en: safety domain)	
SDG	Sicherheitsdomänen-Gateway (en: safety domain gateway)	
SDN	Nummer der Sicherheitsdomäne (en: safety domain number)	
SDO	Dienstdatenobjekt (en: service data object)	[IEC 61158-3-13]
SN	Sicherheitsknoten (en: safety node)	
SNMT	(en: safety network management)	
SOD	(en: safety object dictionary)	

SPDO	Sicherheitsprozessdatenobjekt (en: safety process data object)
SPST	(en: safety parameterization software tool)
SSDO	Sicherheitsservicedatenobjekt (en: safety service data object)
SSADR	(en: Source SADR)
TADR	zusätzliche Sicherheitsadresse (SADR) für Zeitinformationen (en: additional SADR for timing information)
TR	(en: time request distinctive number)
TReq	Zeitsynchronisierungsanfrage (en: time synchronization request)
TRes	Zeitsynchronisierungsantwort (en: time synchronization response)
TÜV	Technischer Überwachungsverein
TxSPDO	(en: safety transmit process data objects)
UDID	(en: unique device identification)

3.3 Konventionen

3.3.1 Hexadezimale Werte

Einige Werte in diesem Teil sind in hexadezimaler Schreibweise festgelegt. Diese muss durch Anhängen eines „h“ an den eigentlichen Wert angegeben werden. Die Zeichen 1, 2, 3, 4, 5, 6, 8, 9, 0, a, b, c, d, e, f, A, B, C, D, E und F müssen verwendet werden. Alle Werte in hexadezimaler Schreibweise müssen vollständige Oktette darstellen; daher besteht eine Darstellung eines hexadezimalen Werts stets aus einer geraden Anzahl Zeichen.

BEISPIEL 1 12ABh, 05h, 1234ABCDh

Um Daten darzustellen, wenn eine Folge von Oktetten explizit festgelegt werden muss, muss eine Schreibweise als hexadezimale Folge verwendet werden, um unabhängig von der exakten Speicherdarstellung (Big-Endian oder Little-Endian) zu sein. Jedes Oktett wird durch einen zweistelligen Hexadezimalwert angegeben (ohne den Zusatz „h“), die einzelnen Oktett-Darstellungen müssen durch Bindestriche (-) getrennt werden.

BEISPIEL 2 00-00-00-00-00-00, AC-3E

3.3.2 Binärwerte

Einige Werte in diesem Teil sind in binärer Schreibweise festgelegt. Diese muss durch Anhängen eines „b“ an den eigentlichen Wert angegeben werden. Die Ziffern 1 und 0 müssen verwendet werden.

BEISPIEL 11001010b

3.3.3 Stellen für Stellvertreterzeichen

Falls Teile von gleichbleibenden Werten „Don't-Care“ sind oder eine zusätzliche Bedeutung außerhalb des Anwendungsbereich des beschreibenden Texts haben, muss dies mit einem „x“ an der entsprechenden Stelle des Zeichens angegeben werden.

BEISPIEL 12xBh, 1x0xx010b, 123x45

3.3.4 Diagramme

Grafische Darstellungen nach ISO/IEC 19501 werden in diesem gesamten Teil soweit zutreffend verwendet.

English Version

**Industrial communication networks – Profiles -
Part 3-13: Functional safety fieldbuses – Additional
specifications for CPF 13
(IEC 61784-3-13:2016)**

Réseaux de communication industriels – Profils –
Partie 3-13: Bus de terrain de sécurité fonctionnelle –
Spécifications complémentaires pour CPF 13
(IEC 61784-3-13:2016)

Industrielle Kommunikationsnetze - Profile -
Teil 3-13: Funktional sichere Übertragung bei Feldbussen –
Zusätzliche Festlegungen für die
Kommunikationsprofilfamilie 13
(IEC 61784-3-13:2016)

This European Standard was approved by CENELEC on 2016-08-19. 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: Rue de la Science 23, B-1040 Brussels

European foreword

The text of document 65C/851/FDIS, future edition 2 of IEC 61784-3-13:2016, 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 61784-3-13:2017.

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 61784-3-13:2010.

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 61784-3-13:2016 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 60204-1	NOTE Harmonized as EN 60204-1.
IEC 61000-6-7	NOTE Harmonized as EN 61000-6-7.
IEC 61131-2	NOTE Harmonized as EN 61131-2.
IEC 61131-6	NOTE Harmonized as EN 61131-6.
IEC 61158 (all parts)	NOTE Harmonized as EN 61158 (all parts).
IEC 61326-3-1	NOTE Harmonized as EN 61326-3-1.
IEC 61326-3-2	NOTE Harmonized as EN 61326-3-2.
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 61511 (all parts)	NOTE Harmonized as EN 61511 (all parts).
IEC 61784-1	NOTE Harmonized as EN 61784-1.
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 62061	NOTE Harmonized as EN 62061.
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	14
0.1 General.....	14
0.2 Patent declaration	16
1 Scope.....	17
2 Normative references	17
3 Terms, definitions, symbols, abbreviated terms and conventions	18
3.1 Terms and definitions	18
3.1.1 Common terms and definitions	18
3.1.2 CPF 13: Additional terms and definitions	23
3.2 Symbols and abbreviated terms.....	24
3.2.1 Common symbols and abbreviated terms.....	24
3.2.2 CPF 13: Additional symbols and abbreviated terms.....	25
3.3 Conventions.....	26
3.3.1 Hexadecimal values	26
3.3.2 Binary values	26
3.3.3 Wildcard digits	26
3.3.4 Diagrams	26
4 Overview of FSCP 13/1 (openSAFETY™)	26
4.1 Functional Safety Communication Profile 13/1	26
4.2 Technical overview.....	26
5 General.....	27
5.1 External documents providing specifications for the profile.....	27
5.2 Safety functional requirements	28
5.3 Safety measures	28
5.4 Safety communication layer structure	29
5.5 Relationships with FAL (and DLL, PhL).....	31
5.5.1 General	31
5.5.2 Data types	31
6 Safety communication layer services.....	31
6.1 Modelling	31
6.1.1 Reference model.....	31
6.1.2 Communication model.....	32
6.1.3 Device roles and topology	33
6.2 Life cycle model.....	37
6.2.1 General	37
6.2.2 Concept, planning and implementation	37
6.2.3 Commissioning	38
6.2.4 Operation terms	39
6.2.5 Maintenance terms.....	41
6.3 Non safety communication layer	41
6.3.1 General	41
6.3.2 Requirements for data transport	41
6.3.3 Domain protection and separation	44
7 Safety communication layer protocol	45

7.1	Safety PDU format	45
7.1.1	Structure of Safety PDUs	45
7.1.2	Address field (ADR)	48
7.1.3	PDU identification field (ID)	48
7.1.4	Length field (LE)	49
7.1.5	Consecutive Time field (CT)	49
7.1.6	Payload data field (DB0 to DBn)	50
7.1.7	Cyclic Redundancy Check field (CRC-8 / CRC-16)	50
7.1.8	Time Request Address field (TADR)	50
7.1.9	Time Request Distinctive Number field (TR)	50
7.1.10	UDID of SCM coding (UDID of SCM)	51
7.2	Safety Process Data Object (SPDO)	51
7.2.1	General	51
7.2.2	SPDO telegram types	51
7.2.3	Data Only telegram	52
7.2.4	Data with Time Request telegram	52
7.2.5	Data with Time Response telegram	53
7.3	Safety Service Data Object (SSDO)	54
7.3.1	General	54
7.3.2	SSDO telegram types	54
7.3.3	SSDO services and protocols	55
7.3.4	SSDO Download Initiate	57
7.3.5	SSDO Download Segment	58
7.3.6	SSDO Block Download Initiate	59
7.3.7	SSDO Block Download Segment	60
7.3.8	SSDO Upload Initiate	62
7.3.9	SSDO Upload Segment	63
7.3.10	SSDO Block Upload Initiate	64
7.3.11	SSDO Block Upload Segment	65
7.3.12	SSDO Abort	65
7.4	Safety Network Management (SNMT)	67
7.4.1	General	67
7.4.2	SNMT telegram types	67
7.4.3	SNMT services and protocols	67
7.5	Safety Object dictionary (SOD)	80
7.5.1	General	80
7.5.2	Object dictionary entry definition	80
7.5.3	Data type entry specification	85
7.5.4	Object description	87
7.6	Safety related PDO mapping	122
7.6.1	General	122
7.6.2	Transmit SPDOs	123
7.6.3	Receive SPDOs	123
7.6.4	SPDO mapping parameter	123
7.6.5	SPDO mapping example	124
7.6.6	SPDO error handling	126
7.7	State and sequence diagrams	126
7.7.1	Safety Process Data Object (SPDO)	126

7.7.2	Time synchronization and validation	131
7.7.3	Safety Service Data Object (SSDO).....	140
7.7.4	SOD access.....	142
7.7.5	Safety Network Management Object (SNMT)	152
7.7.6	SN power up	154
7.7.7	SN power down.....	158
7.7.8	SN recovery after Restart / Error	158
7.7.9	SCM power up	158
7.7.10	Address verification.....	161
7.7.11	Commissioning mode	163
7.7.12	Handle single UDID mismatch	163
7.7.13	Activate SN.....	167
7.7.14	Device exchange	168
8	Safety communication layer management.....	168
8.1	General.....	168
8.2	Goals of parameterization	168
8.3	Initial configuration of a device	168
8.3.1	General	168
8.3.2	SD setup by only configuring the SCM	169
8.3.3	SD setup configuring each SN.....	169
8.4	Avoiding of parameterizing the wrong device	169
8.5	Parameter check mechanism.....	169
9	System requirements	170
9.1	Indicators and switches	170
9.2	Installation guidelines.....	170
9.3	Safety function response time.....	170
9.4	Duration of demands	171
9.5	Constraints for calculation of system characteristics	171
9.5.1	General	171
9.5.2	Number of sinks limit.....	171
9.5.3	Message rate limit.....	171
9.5.4	Message payload limit.....	171
9.5.5	Bit error rate considerations	172
9.5.6	Residual error rate	172
9.6	Maintenance	173
9.6.1	Diagnostic information.....	173
9.6.2	Replacement of safety related devices.....	173
9.6.3	Modification	174
9.6.4	Machine part changing	174
9.6.5	Firmware update of safety related nodes	174
9.6.6	Machine check due to service interval	174
9.7	Safety manual	174
10	Assessment.....	174
10.1	General.....	174
10.2	CP 13/1 assessment	175
10.3	FSCP 13/1 conformance test.....	175
10.4	Approval of functional safety by competent assessment body.....	175

Annex A (informative) Additional information for functional safety communication profiles of CPF 13	176
A.1 Hash function calculation	176
A.2	179
Annex B (informative) Information for assessment of the functional safety communication profiles of CPF 13	180
Bibliography	181
Annex ZA (normative) Normative references to international publications with their corresponding European publications.....	185
 Figure 1 – Relationships of IEC 61784-3 with other standards (machinery)	14
Figure 2 – Relationships of IEC 61784-3 with other standards (process)	15
Figure 3 – Producer consumer example	27
Figure 4 – Client server example.....	27
Figure 5 – Communication layer structure	30
Figure 6 – Safety communication channel	31
Figure 7 – Characteristic producer / consumer communication.....	32
Figure 8 – Extended producer / consumer communication	33
Figure 9 – Client Server communication	33
Figure 10 – Topology overview	34
Figure 11 – Safety Domain protection (example)	35
Figure 12 – Safety Domain separation (example)	36
Figure 13 – Data flow example.....	40
Figure 14 – Communication model	41
Figure 15 – SPDO transport.....	42
Figure 16 – SSDO transport.....	43
Figure 17 – Diagnostic data representation	44
Figure 18 – Safety PDUs inside a CP 13/1 PDU	45
Figure 19 – Basic Safety PDU for n = 0 – 8 octet payload data	45
Figure 20 – Basic Safety PDU from 9 octet payload data	46
Figure 21 – Slim Safety PDU for n = 0 – 8 octet payload data	47
Figure 22 – Slim Safety PDU from 9 octet payload data.....	47
Figure 23 – SPDO_Data_Only telegram	52
Figure 24 – SPDO_Data_with_Time_Request telegram	53
Figure 25 – SPDO_Data_with_Time_Response telegram.....	53
Figure 26 – SSDO download protocols	56
Figure 27 – SSDO upload protocols	57
Figure 28 – SSDO Download Initiate protocol.....	57
Figure 29 – SSDO Download Segment protocol.....	59
Figure 30 – SSDO Block Download Initiate protocol.....	59
Figure 31 – SSDO Block Download Segment protocol	61
Figure 32 – SSDO Upload Initiate protocol	62
Figure 33 – SSDO Upload Segment protocol.....	63

Figure 34 – SSDO Block Upload Initiate protocol	64
Figure 35 – SSDO Block Upload Segment protocol	65
Figure 36 – SSDO Abort protocol	66
Figure 37 – UDID Request / Response protocol	68
Figure 38 – SADR Assignment protocol	69
Figure 39 – Reset Node Guarding Time protocol	70
Figure 40 – SN set to Pre-Operational protocol	71
Figure 41 – SN set to Operational protocol	73
Figure 42 – SN Acknowledge protocol	75
Figure 43 – SN set to stop protocol	75
Figure 44 – SCM set to Operational protocol	76
Figure 45 – Node Guarding protocol	77
Figure 46 – Additional SADR Assignment protocol	78
Figure 47 – UDID of SCM Assignment protocol	79
Figure 48 – SPDO mapping example	124
Figure 49 – State diagram TxSPDO	127
Figure 50 – SPDO communication producer	127
Figure 51 – State diagram RxSPDO	128
Figure 52 – SPDO communication consumer	129
Figure 53 – State diagram process data	130
Figure 54 – Time synchronization and validation	131
Figure 55 – Time synchronization detail	132
Figure 56 – Calculation of propagation delay	133
Figure 57 – Time validation, propagation delay explanation limits	134
Figure 58 – Time synchronization on a nonsafe network	135
Figure 59 – Explanation of time synchronization	136
Figure 60 – Time synchronization failure	137
Figure 61 – State diagram time synchronization producer	138
Figure 62 – State diagram time synchronization consumer	139
Figure 63 – State diagram SSDO client	141
Figure 64 – State diagram SSDO server	142
Figure 65 – Expedited SOD access	143
Figure 66 – State diagram segmented SOD download access client	144
Figure 67 – Segmented SOD download access	145
Figure 68 – State diagram segmented SOD download access server	146
Figure 69 – State diagram SOD block download access client	148
Figure 70 – SOD block download access	149
Figure 71 – State diagram SOD block download access server	151
Figure 72 – State diagram SNMT master	153
Figure 73 – State diagram SNMT slave	154
Figure 74 – State diagram SN power up	155
Figure 75 – State diagram SN Pre-Operational	156

Figure 76 – State diagram SN Operational	157
Figure 77 – Life Guarding telegram	158
Figure 78 – State diagram SCM power up	159
Figure 79 – State diagram SCM Operational.....	160
Figure 80 – State diagram SCM address verification.....	162
Figure 81 – State diagram SCM handle single UDID mismatch	164
Figure 82 – State diagram SCM verify parameters.....	166
Figure 83 – State diagram activate SN	167
Figure 84 – Safety function response time.....	170
Figure 85 – Assessment flow of devices	175

Table 1 – Communication errors and detection measures (cyclic)	28
Table 2 – Communication errors and detection measures (acyclic)	29
Table 3 – Device roles	34
Table 4 – Basic Safety PDU format	46
Table 5 – Slim Safety PDU format.....	47
Table 6 – PDU identification field (ID)	48
Table 7 – Used ID field combinations	49
Table 8 – Request / response identification	49
Table 9 – Type of CRC depending on LE.....	49
Table 10 – CRC polynoms for SPDUs	50
Table 11 – SPDO telegram types (ID field, bits 2, 3 and 4)	51
Table 12 – Fields of SPDO_Data_Only telegram	52
Table 13 – Fields of SPDO_Data_with_Time_Request telegram	53
Table 14 – Fields of SPDO_Data_with_Time_Response telegram	54
Table 15 – SSDO telegram types (ID field, bits 2, 3 and 4)	54
Table 16 – SOD Access Command (SACmd) – bit coding	55
Table 17 – Fields of Download Initiate SSDO_Service_Request telegram	58
Table 18 – Fields of Download Initiate SSDO_Service_Response telegram.....	58
Table 19 – Fields of Download Segment SSDO_Service_Request telegram	59
Table 20 – Fields of Download Segment SSDO_Service_Response telegram	59
Table 21 – Fields of Block Download Initiate SSDO_Service_Request telegram	60
Table 22 – Fields of Block Download Initiate SSDO_Service_Response telegram	60
Table 23 – Fields of Block Download Segment SSDO_Service_Request telegram.....	61
Table 24 – Fields of Block Download Segment SSDO_Service_Response telegram	61
Table 25 – Fields of Upload Initiate SSDO_Service_Request telegram.....	62
Table 26 – Fields of Upload Initiate SSDO_Service_Response telegram	62
Table 27 – Fields of Upload Segment SSDO_Service_Request telegram	63
Table 28 – Fields of Upload Segment SSDO_Service_Response telegram.....	63
Table 29 – Fields of Block Upload Initiate SSDO_Service_Request telegram	64
Table 30 – Fields of Block Upload Initiate SSDO_Service_Response telegram.....	64
Table 31 – Fields of Block Upload Segment SSDO_Service_Response telegram	65

Table 32 – Fields of SSDO Abort telegram	66
Table 33 – SSDO Abort codes.....	66
Table 34 – SNMT telegram types (ID field, bits 2, 3 and 4).....	67
Table 35 – Fields of SNMT_Request_UDID telegram	68
Table 36 – Fields of SNMT_Response_UDID telegram	68
Table 37 – Fields of SNMT_Assign_SADR telegram	69
Table 38 – Fields of SNMT_SADR_Assigned telegram	70
Table 39 – Fields of SNMT_SN_reset_guarding_SCM telegram	70
Table 40 – SNMT request telegram types	71
Table 41 – SNMT response telegram types	71
Table 42 – Fields of SNMT_SN_set_to_PRE_OP telegram	72
Table 43 – Fields of SNMT_SN_status_PRE_OP telegram.....	72
Table 44 – Fields of SNMT_SN_set_to_OP telegram	73
Table 45 – Fields of SNMT_SN_status_OP telegram	73
Table 46 – Fields of SNMT_SN_busy telegram.....	74
Table 47 – Fields of SNMT_SN_FAIL telegram.....	74
Table 48 – SNMT_SN_FAIL Error Group values	74
Table 49 – SNMT_SN_FAIL Error Code values.....	74
Table 50 – Fields of SNMT_SN_ACK telegram	75
Table 51 – Fields of SNMT_SCM_set_to_STOP telegram	76
Table 52 – Fields of SNMT_SCM_set_to_OP telegram	76
Table 53 – Fields of SNMT_SCM_guard_SN telegram	77
Table 54 – Fields of SNMT_SN_status_OP/SNMT_SN_status_OP telegrams.....	77
Table 55 – Fields of SNMT_assign_additional_SADR telegram	78
Table 56 – Fields of SNMT_assigned_additional_SADR telegram	78
Table 57 – Fields of SNMT_assign_UDID_of_SCM telegram.....	79
Table 58 – Fields of SNMT_assigned_UDID_of_SCM telegram	79
Table 59 – Object type definition	80
Table 60 – Access attributes for data objects.....	82
Table 61 – SPDO mapping attributes for data objects	82
Table 62 – Basic data type object definition example	83
Table 63 – Compound data type object definition example	83
Table 64 – Sub index interpretation	83
Table 65 – NumberOfEntries sub index specification	84
Table 66 – RECORD type object sub index specification.....	84
Table 67 – ARRAY type object sub index specification.....	85
Table 68 – StructureOfObject encoding	85
Table 69 – Object dictionary data types	86
Table 70 – 0021h Compound data type description example	87
Table 71 – 0021h Compound sub index descriptions example.....	87
Table 72 – Standard objects	87
Table 73 – Common communication objects	88

Table 74 – Receive SPDO communication objects.....	88
Table 75 – Receive SPDO mapping objects	88
Table 76 – Transmit SPDO communication objects.....	89
Table 77 – User parameter (writeable at any time)	89
Table 78 – Transmit SPDO mapping objects	89
Table 79 – SADR DVI list.....	89
Table 80 – Additional SADR list	90
Table 81 – SADR UDID list	90
Table 82 – Object 1001h Error Register	90
Table 83 – Object 1001h Error Register value interpretation	91
Table 84 – Object 1002h Manufacturer status register	91
Table 85 – Object 1003h Pre defined error field.....	92
Table 86 – Object 1003h sub index 00h	92
Table 87 – Object 1003h sub index 01h	92
Table 88 – Object 1003h sub index 02h to FEh	92
Table 89 – Object 100Ch Life Guarding.....	93
Table 90 – Object 100Ch sub index 00h	93
Table 91 – Object 100Ch sub index 01h	93
Table 92 – Object 100Ch sub index 02h	94
Table 93 – Object 100Dh Refresh Interval of Reset Guarding	94
Table 94 – Object 100Dh Refresh Interval of Reset Guarding	95
Table 95 – Object 1018h Device Vendor Information	95
Table 96 – Object 1018h sub index 00h	95
Table 97 – Object 1018h sub index 01h	96
Table 98 – Object 1018h sub index 02h	96
Table 99 – Object 1018h sub index 03h	96
Table 100 – Object 1018h sub index 04h.....	97
Table 101 – Object 1018h sub index 05h.....	97
Table 102 – Object 1018h sub index 06h.....	97
Table 103 – Object 1018h sub index 07h.....	98
Table 104 – Structure of Revision Number	98
Table 105 – Structure of parameter checksum domain.....	98
Table 106 – CRC polynom for parameter checksum	98
Table 107 – Object 1019h Unique Device ID	99
Table 108 – Object 101Ah Parameter Download.....	100
Table 109 – Format of Parameter Download.....	100
Table 110 – Object 101Bh SCM Parameters.....	100
Table 111 – Object 101Bh sub index 00h	101
Table 112 – Object 101Bh sub index 01h	101
Table 113 – Object 1200h Common Communication Parameter	101
Table 114 – Object 1200h sub index 00h.....	102
Table 115 – Object 1200h sub index 01h.....	102

Table 116 – Object 1200h sub index 02h.....	102
Table 117 – Object 1200h sub index 03h.....	103
Table 118 – Object 1200h sub index 04h.....	103
Table 119 – Object 1201h SSDO Communication Parameter	104
Table 120 – Object 1201h sub index 00h.....	104
Table 121 – Object 1201h sub index 01h.....	104
Table 122 – Object 1201h sub index 02h.....	104
Table 123 – Object 1202h SNMT Communication Parameter	105
Table 124 – Object 1202h sub index 00h.....	105
Table 125 – Object 1202h sub index 01h.....	105
Table 126 – Object 1202h sub index 02h.....	106
Table 127 – Object 1400h – 17FEh RxSPDO Communication Parameter	106
Table 128 – Object 1400h – 17FEh sub index 00h	106
Table 129 – Object 1400h – 17FEh sub index 01h	107
Table 130 – Object 1400h – 17FEh sub index 02h	107
Table 131 – Object 1400h – 17FEh sub index 03h	107
Table 132 – Object 1400h – 17FEh sub index 04h	108
Table 133 – Object 1400h – 17FEh sub index 05h	108
Table 134 – Object 1400h – 17FEh sub index 06h	108
Table 135 – Object 1400h – 17FEh sub index 07h	109
Table 136 – Object 1400h – 17FEh sub index 08h	109
Table 137 – Object 1400h – 17FEh sub index 09h	109
Table 138 – Object 1400h – 17FEh sub index 0Ah.....	110
Table 139 – Object 1400h – 17FEh sub index 0Bh.....	110
Table 140 – Object 1400h – 17FEh sub index 0Ch	110
Table 141 – Object 1800h – 1BFEh RxSPDO communication parameter	111
Table 142 – Object 1800h – 1BFEh sub index 00h.....	111
Table 143 – Object 1800h – 1BFEh sub index 01h.....	111
Table 144 – Object 1800h – 1BFEh sub index 02h – FEh.....	111
Table 145 – 1Object C00h – 1FFEh TxSPDO communication parameter	112
Table 146 – Object 1C00h – 1FFEh sub index 00h	112
Table 147 – Object 1C00h – 1FFEh sub index 01h	112
Table 148 – Object 1C00h – 1FFEh sub index 02h	113
Table 149 – Object 1C00h – 1FFEh sub index 03h	113
Table 150 – Object C000h – C3FEh TxSPDO mapping parameter.....	114
Table 151 – Object C000h – C3FEh sub index 00h.....	114
Table 152 – Object C000h – C3FEh sub index 01h	114
Table 153 – Object C000h – C3FEh sub index 02h – FEh	114
Table 154 – Object C400h – C7FEh SADR-DVI list.....	115
Table 155 – Object C400h – C7FEh sub index 00h.....	115
Table 156 – Object C400h – C7FEh sub index 01h	115
Table 157 – Object C400h – C7FEh sub index 02h	116

Table 158 – Object C400h – C7FEh sub index 03h	116
Table 159 – Object C400h – C7FEh sub index 04h	116
Table 160 – Object C400h – C4FEh sub index 05h	117
Table 161 – Object C400h – C7FEh sub index 06h	117
Table 162 – Object C400h – C7FEh sub index 07h	117
Table 163 – Object C400h – C7FEh sub index 08h	118
Table 164 – Object C400h – C7FEh sub index 09h	118
Table 165 – Object C400h – C7FEh sub index 0Ah	118
Table 166 – Object C400h – C7FEh sub index 0Bh	119
Table 167 – Object C400h – C7FEh sub index 0Ch	119
Table 168 – Bit field of optional features	119
Table 169 – Object C400h – C7FEh sub index 0Dh	119
Table 170 – Object C801h – CBFFh Additional SADR list	120
Table 171 – Object C801h – CBFFh sub index 00h	120
Table 172 – Object C801h – CBFFh sub index 01h	120
Table 173 – Object C801h – CBFFh sub index 02h	121
Table 174 – Object Additional SADR List Example	121
Table 175 – Object CC01h – CFFFh SADR-UDID list	122
Table 176 – Object CC01h – CFFFh sub index 00h	122
Table 177 – Object CC01h – CFFFh sub index 01h – FEh	122
Table 178 – SADR-UDID List Example	122
Table 179 – Structure of SPDO mapping entry	124
Table 180 – Mapping example table 1	125
Table 181 – Mapping example table 2	125
Table 182 – Mapping example table 3	125
Table 183 – Mapping example table 4	125
Table 184 – Mapping example table 5	125
Table 185 – Mapping example table 6	126
Table 186 – Mapping example table 7	126
Table 187 – SPDO communication producer item description	127
Table 188 – SPDO communication producer state description	128
Table 189 – SPDO communication consumer item description	129
Table 190 – SPDO communication consumer state description	129
Table 191 – SPDO communication consumer telegram validation item description	130
Table 192 – SPDO communication consumer telegram validation state description	131
Table 193 – Time synchronization item description	132
Table 194 – Time validation item description	134
Table 195 – Extended time synchronization item description	137
Table 196 – Time synchronization producer item description	138
Table 197 – Time synchronization producer state description	139
Table 198 – Time synchronization consumer item description	140
Table 199 – Time synchronization consumer state description	140

Table 200 – SSDO client item description.....	141
Table 201 – SSDO client state description.....	141
Table 202 – SSDO server state description	142
Table 203 – SOD access item description	143
Table 204 – Segmented SOD access client item description	145
Table 205 – Segmented SOD download access client state description.....	145
Table 206 – Segmented SOD access server item description.....	147
Table 207 – Segmented SOD access server state description.....	147
Table 208 – SOD block download access client item description	149
Table 209 – SOD block download access client state description	149
Table 210 – SOD block download access server item description.....	152
Table 211 – SOD block download access server state description.....	152
Table 212 – SNMT master item description	153
Table 213 – SNMT master state description	153
Table 214 – SNMT slave state description.....	154
Table 215 – SN power up state description.....	155
Table 216 – State and communication object relation	155
Table 217 – SN Pre-Operational state item description	157
Table 218 – SN Pre-Operational state description	157
Table 219 – SN Operational state item description	158
Table 220 – SN Operational state description.....	158
Table 221 – SCM power up state description.....	159
Table 222 – State and communication object relation	159
Table 223 – SCM Operational state item description.....	161
Table 224 – SCM Operational state description	161
Table 225 – Address verification item description	163
Table 226 – Address verification state description	163
Table 227 – SCM handle single UDID mismatch state description	165
Table 228 – SCM verify parameters state description	167
Table 229 – Activate SN state description	168
Table 230 – Residual error rate.....	172

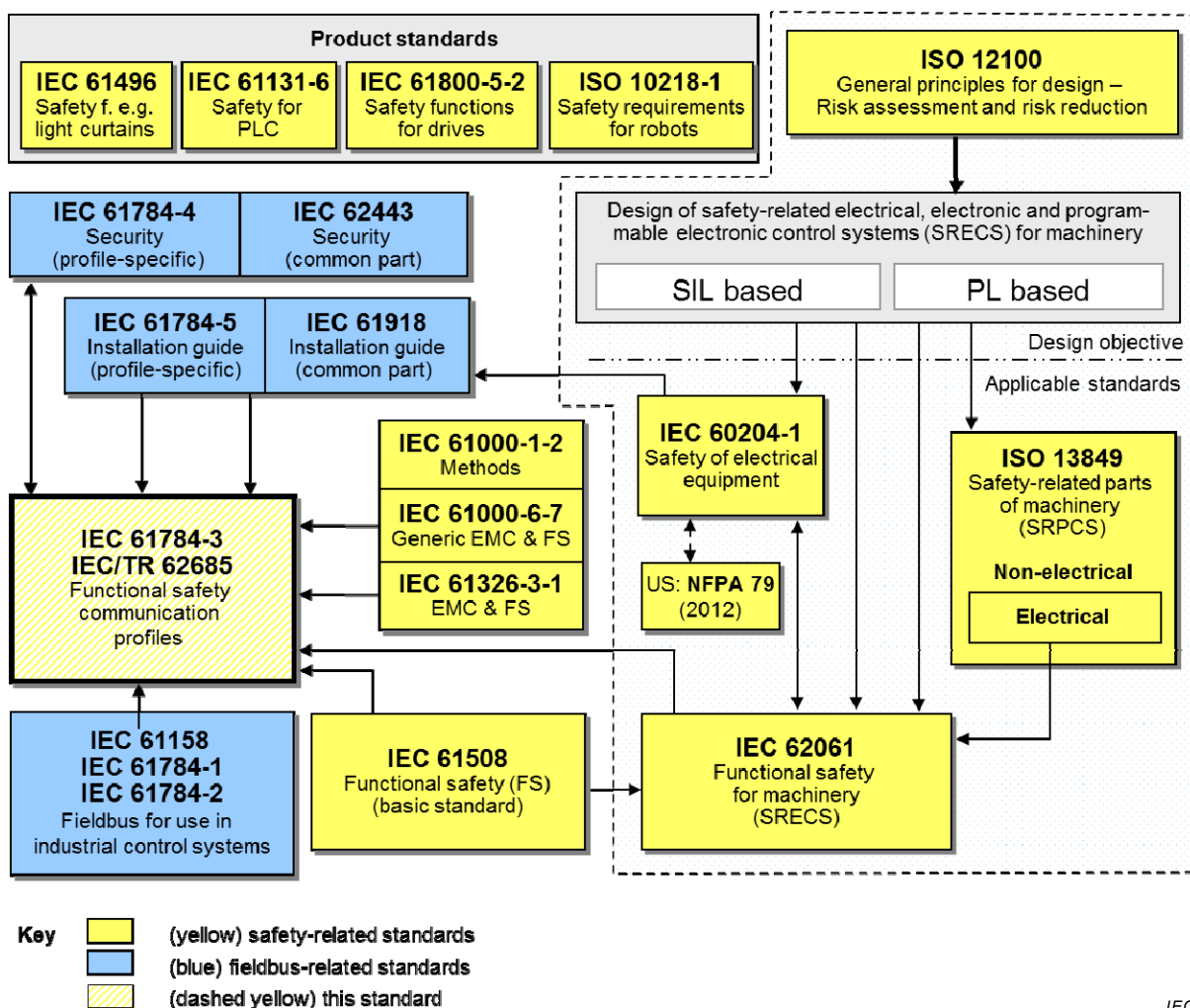
0 Introduction

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.

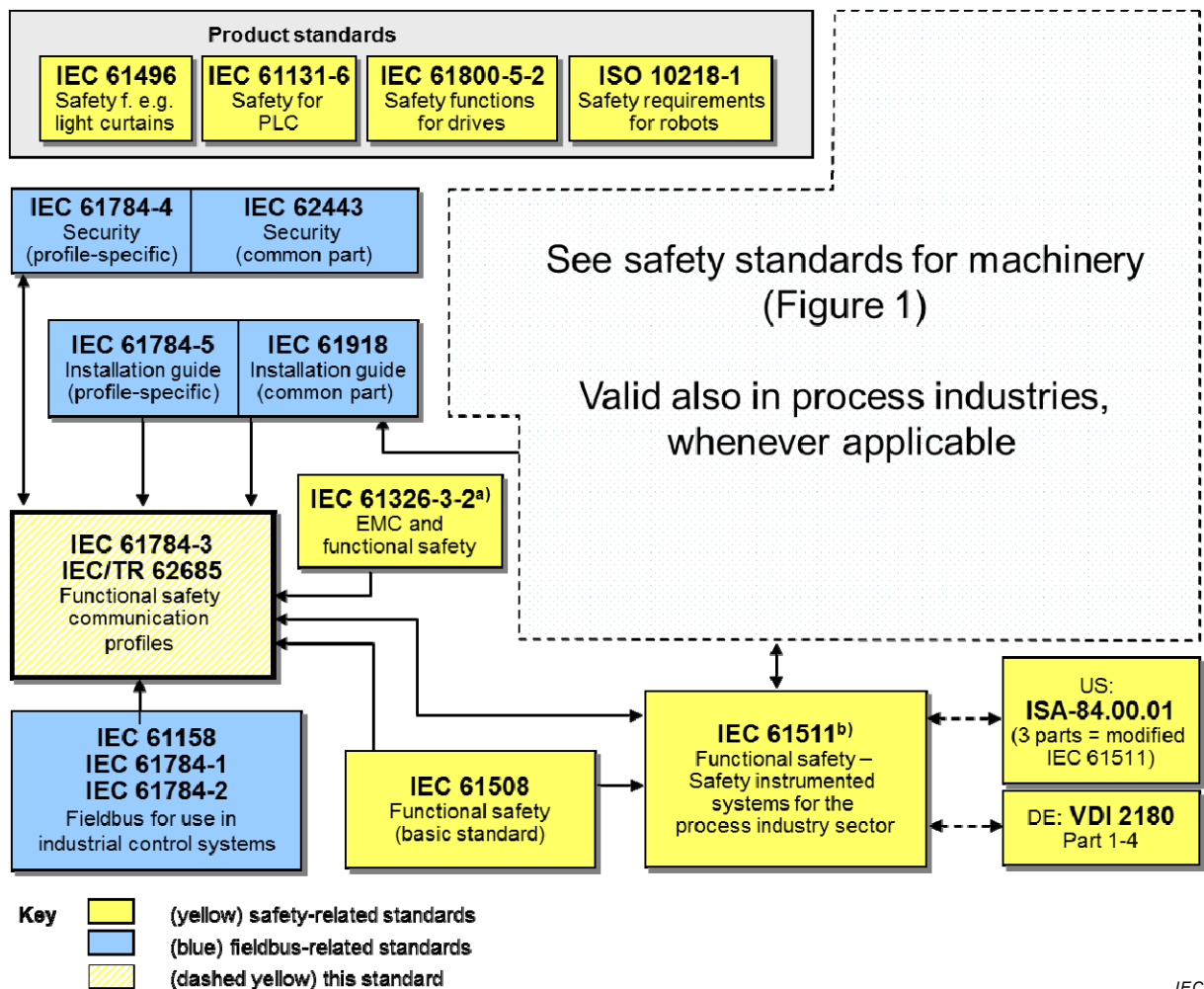
Figure 1 shows the relationships between this standard and relevant safety and fieldbus standards in a machinery environment.



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 patents concerning the functional safety communication profiles for family 13 as follows, where the [xx] notation indicates the holder of the patent rights:

AT 504739	[BR]	Anordnung und ein Verfahren zur sicheren Datenkommunikation über ein nicht sicheres Netzwerk
DE 102005032877.6	[BR]	Verfahren zur Zeitsynchronisation von Teilnehmern eines Netzwerkes
DE 102004055685.7	[BR]	Verfahren zur Abgrenzung eines sicheren Netzwerkes
DE 102004055684.9	[BR]	Verfahren zur Absicherung des Datentransfers in einem sicheren Netzwerk mit CRC's variabler Länge
EP 08150038.1	[BR]	Anordnung und ein Verfahren zur sicheren Datenkommunikation über ein nicht sicheres Netzwerk

IEC takes no position concerning the evidence, validity and scope of these patent rights.

The holder of these patent rights 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 these patent rights is registered with IEC.

Information may be obtained from:

[BR] Bernecker + Rainer
Industrie-Elektronik Ges.m.b.H.
B&R Strasse 1
5142 Eggelsberg
AUSTRIA

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

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 3-13: Functional safety fieldbuses – Additional specifications for CPF 13

1 Scope

This part of the IEC 61784-3 series specifies a safety communication layer (services and protocol) based on CPF 13 of IEC 61784-2 and IEC 61158 Type 13. 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 61131-3, *Programmable controllers – Part 3: Programming languages*

IEC 61158-3-13, *Industrial communication networks – Fieldbus specifications – Part 3-13: Data-link layer service definition – Type 13 elements*

IEC 61158-4-13, *Industrial communication networks – Fieldbus specifications – Part 4-13: Data-link layer protocol specification – Type 13 elements*

IEC 61158-5-13, *Industrial communication networks – Fieldbus specifications – Part 5-13: Application layer service definition – Type 13 elements*

IEC 61158-6-13, *Industrial communication networks – Fieldbus specifications – Part 6-13: Application layer protocol specification – Type 13 elements*

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

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 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 61784-5-13, *Industrial communication networks – Profiles – Part 5-13: Installation of fieldbuses – Installation profiles for CPF 13*

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

ISO/IEC 19501, *Information technology – Open Distributed Processing – Unified Modeling Language (UML) Version 1.4.2*

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.

3.1.1 Common terms and definitions

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

3.1.1.1

availability

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

3.1.1.2

bit error probability

P_e

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

3.1.1.3

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.

3.1.1.4

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]

3.1.1.5

communication channel

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

³ To be published

3.1.1.6

communication system

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

3.1.1.7

connection

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

3.1.1.8

Cyclic Redundancy Check

CRC

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

<method> procedure used to calculate the redundant data

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

Note 2 to entry: See also [38], [39]⁴.

3.1.1.9

defined communication system

defined channel

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

3.1.1.10

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]

3.1.1.11

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]

3.1.1.12

fault

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

⁴ Figures in square brackets refer to the bibliography.

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]

3.1.1.13

fieldbus

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

3.1.1.14

fieldbus system

system using a *fieldbus* with connected devices

3.1.1.15

frame

denigrated synonym for DLPDU

3.1.1.16

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]

3.1.1.17

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

3.1.1.18

message

ordered series of octets intended to convey information

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

3.1.1.19

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]

3.1.1.20

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]

3.1.1.21 **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]

3.1.1.22 **residual error rate**

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

3.1.1.23 **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]

3.1.1.24 **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*.

3.1.1.25 **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

3.1.1.26 **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.

3.1.1.27 **safety device**

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

3.1.1.28 **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]

3.1.1.29

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.

3.1.1.30

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]

3.1.1.31

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.

3.1.1.32

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*.

3.1.1.33

safety-related application

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

3.1.1.34

safety-related system

system performing *safety functions* according to IEC 61508

3.1.1.35

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

3.1.1.36

time stamp

time information included in a *message*

3.1.2 CPF 13: Additional terms and definitions

3.1.2.1

bit error rate

likelihood of a bit misinterpretation due to electrical noise

3.1.2.2

Device Vendor Information

DVI

information for identifying a *safety node*

3.1.2.3

Safety Address

SADR

address of a *safety node* within a *safety domain*

3.1.2.4

Safety Configuration Manager

SCM

service which is responsible to manage safety related services

Note 1 to entry: Examples of managed safety related services are configuration, parameterization.

3.1.2.5

Safety Node

SN

node with *safety function*

3.1.2.6

Safety Domain

SD

address space for up to 1 023 *safety nodes*

3.1.2.7

Safety Domain Gateway

SDG

gateway to share data between different *safety domains*

3.1.2.8

Safety Domain Number

SDN

identification of a *safety domain*

3.1.2.9

Safety Network Management

SNMT

services for safety layer management

3.1.2.10

Safety Object Dictionary

SOD

repository of all data objects accessible using services of the functional safety *fieldbus*

3.1.2.11

Safety Process Data Object

SPDO

object for process data exchange between different *safety nodes*

3.1.2.12

Safety Service Data Object

SSDO

object for service data exchange between *safety nodes*

3.1.2.13

initialization

initial *safety node* communication state

3.1.2.14

operational

safety node communication state where all functional safety functions are working properly

3.1.2.15

pre-operational

safety node communication state where all application outputs are in safe state

3.1.2.16

Unique Device Identification

UDID

worldwide unique identification of a device

3.2 Symbols and abbreviated terms

3.2.1 Common symbols and abbreviated terms

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]
FS	Functional Safety	
FSCP	Functional Safety Communication Profile	
MTBF	Mean Time Between Failures	
MTTF	Mean Time To Failure	
PDU	Protocol Data Unit	[ISO/IEC 7498-1]
PFH	Average frequency of dangerous failure [h ⁻¹] per hour	[IEC 61508-4:2010]
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	

3.2.2 CPF 13: Additional symbols and abbreviated terms

ACM	Automatic Configuration Mode	
ADR	Address information (source or destination)	
APDU	Application Protocol Data Unit	[ISO/IEC 7498-1]
CN	Controlled Node	[IEC 61158-3-13]
CT	Consecutive Time field	
DBx	Data Octet	
DSADR	Destination SADR	
DVI	Device Vendor Information	
ID	PDU Identification	
LE	Length field	
LSB	Least Significant Octet	
MAC	Medium Access Layer	
MCM	Manual Configuration Mode	
MN	Managing Node	[IEC 61158-3-13]
MSB	Most Significant Octet	
PDO	Process Data Object	[IEC 61158-3-13]
RxSPDO	Receive Process data objects	
SADR	Safety Address	
SCM	Safety Configuration Manager	
SCT	Safety Control Time	
SD	Safety Domain	
SDG	Safety Domain Gateway	
SDN	Safety Domain Number	
SDO	Service Data Object	[IEC 61158-3-13]
SN	Safety Node	
SNMT	Safety Network Management	
SOD	Safety Object Dictionary	
SPDO	Safety Process Data Object	
SPST	Safety Parameterization Software Tool	
SSDO	Safety Service Data Object	
SSADR	Source SADR	
TADR	Additional SADR for timing information	
TR	Time Request Distinctive Number	
TReq	Time Synchronization Request	
TRes	Time Synchronization Response	
TÜV	Technischer Überwachungsverein	
TxSPDO	Safety Transmit Process data objects	
UDID	Unique Device Identification	

3.3 Conventions

3.3.1 Hexadecimal values

Some values within this part are specified in hexadecimal notation. This shall be depicted by appending a "h" to the value itself. The characters 1, 2, 3, 4, 5, 6, 8, 9, 0, a, b, c, d, e, f, A, B, C, D, E and F shall be used. All values in hexadecimal notation shall depict whole octets; therefore a hexadecimal value representation always consists of an even number of characters.

EXAMPLE 1 12ABh, 05h, 1234ABCDh

To depict data where a sequence of octets shall explicitly be defined – to be independent from the exact memory representation (Big-Endian or Little-Endian) – a hexadecimal sequence notation shall be used. Every octet is shown by a two digit hexadecimal value (without the h suffix), the single octet representations shall be separated by a dash (-).

EXAMPLE 2 00-00-00-00-00-00, AC-3E

3.3.2 Binary values

Some values within this part are specified in binary notation. This shall be depicted by appending a "b" to the value itself. The characters 1 and 0 shall be used.

EXAMPLE 11001010b

3.3.3 Wildcard digits

If parts of constant values are "don't care", or have additional meaning outside the scope of the descriptive text, this shall be depicted by an x at the respective digit position.

EXAMPLE 12xBh, 1x0xx010b, 123x45

3.3.4 Diagrams

Graphical notations according to ISO/IEC 19501 are used throughout this part where appropriate.

4 Overview of FSCP 13/1 (openSAFETY™)

4.1 Functional Safety Communication Profile 13/1

Communication Profile Family 13 (commonly known as Ethernet POWERLINK™⁵) defines communication profiles based on IEC 61158-3-13, IEC 61158-4-13, IEC 61158-5-13, and IEC 61158-6-13.

The basic profile CP 13/1 is defined in IEC 61784-2. The CPF 13 functional safety communication profile FSCP 13/1 (openSAFETY™) is based on the CPF 13 basic profiles in IEC 61784-2 and the safety communication layer specifications defined in this part.

4.2 Technical overview

FSCP 13/1 defines an open safety protocol for Ethernet-based communication down to the microsecond range.

⁵ Ethernet POWERLINK™ and openSAFETY™ are trade names of the non-profit organization Ethernet POWERLINK™ Standardization Group (EPSG). This information is given for the convenience of users of this International Standard and does not constitute an endorsement by IEC of the trade name holder or any of its products. Compliance to this standard does not require use of the trade names Ethernet POWERLINK™ or openSAFETY™. Use of the trade names Ethernet POWERLINK™ or openSAFETY™ requires permission of Ethernet POWERLINK Standardization Group (EPSG) and compliance with conditions for their use (such as testing and validation).

The FSCP 13/1 services and protocol specify safety related data communication between Safety Nodes (SNs). The FSCP 13/1 protocol technology is designed to provide SIL 3 safety function according to IEC 61508. The network configuration is done by using the Safety Configuration Manager (SCM). Safety Network Management (SNMT) services are used for booting and runtime diagnosis of FSCP 13/1 networks. The Safety Object Dictionary (SOD) is database provided by every SN containing configuration and user data. Safety Service Data Objects (SSDO) are used for the exchange of spontaneous data. Safety Process Data Objects (SPDO) provide services for exchange of synchronous data.

Synchronous data communication between SNs is modelled according to the publisher subscriber model (see Figure 3), whereas spontaneous data communication use the client server model (see Figure 4).

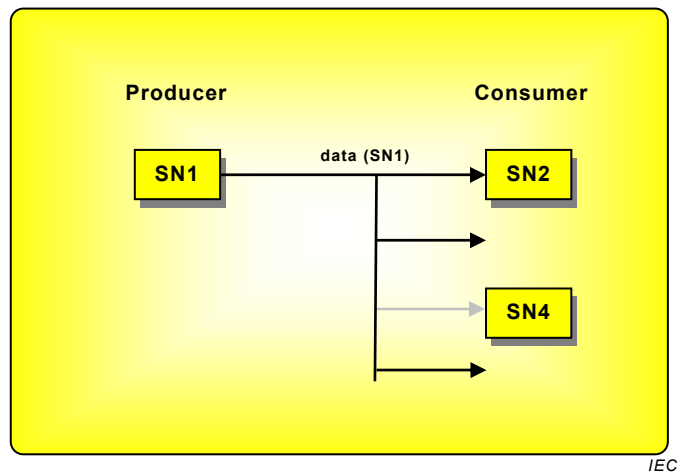


Figure 3 – Producer consumer example

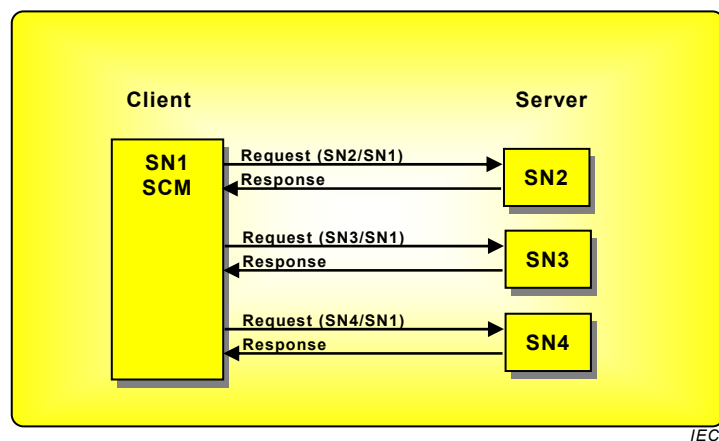


Figure 4 – Client server example

5 General

5.1 External documents providing specifications for the profile

The documents [46] and [47] may help understanding FSCP 13/1 concepts.

5.2 Safety functional requirements

The following requirements were used in the development of FSCP 13/1 and shall apply to the development of devices that implement the FSCP 13/1 protocol:

- FSCP 13/1 shall support Safety Integrity Level 3 (SIL 3) according to IEC 61508,
- The basic requirements for the development of FSCP 13/1 are specified in IEC 61784-3,
- FSCP 13/1 utilizes services defined in IEC 61158-5-13,
- FSCP 13/1 protocol is based on a black channel approach; there is no safety related dependency on the CPF 13 communication profile,
- Implementations of FSCP 13/1 shall comply with IEC 61508,
- CPF 13 requirements shall be unchanged for safety unless specified otherwise in this part,
- Safety communication and standard communication shall be independent. However, standard devices and FSCP 13/1 devices shall be able to use the same communication channel,
- Non safety related network infrastructure devices shall be usable to build a FSCP 13/1 network,
- Up to 1 023 safety related devices shall be supported within one safety domain,
- Up to 1 023 safety domains shall be supported,
- Bandwidth used by safety messages shall be kept as low as possible, safety PDUs shall be optimized for devices with less data (e.g. digital IO), and
- Unless specified otherwise in this part, the safe state of any value shall be zero (0).

5.3 Safety measures

FSCP 13/1 shall use the safety measures listed in Table 1 to detect communication errors for cyclic data transferred in SPDO (see 7.2). The safety measures shall be processed and monitored within each FSCP 13/1 device.

Table 1 – Communication errors and detection measures (cyclic)

Communication errors	Safety measures							
	Sequence number	Time stamp	Time expectation	Connection authentication	Feedback message	Data integrity assurance	Redundancy with cross checking	Different data integrity assurance systems
Corruption						X	X	
Unintended repetition		X						
Incorrect sequence		X						
Loss			X ^a					
Unacceptable delay		X	X					
Insertion			X ^b					
Masquerade			X			X	X	X
Addressing				X				
NOTE The errors "loss" and "insertion" will not be detected by the use of a time stamp. A loss of data is detected within the maximum reaction time by the use of a watchdog. If a message was sent more than once (insertion), the timestamp is unchanged and the receiving device ignores this message.								
^a Missing PDUs shall be detected within maximum reaction time.								
^b Only one message shall be accepted during a defined time frame.								

FSCP 13/1 shall use the safety measures listed in Table 2 to detect communication errors for acyclic data transferred in SSDO (see 7.3) or SNMT (see 7.4). The safety measures shall be processed and monitored within each FSCP 13/1 device.

Table 2 – Communication errors and detection measures (acyclic)

Communication errors	Safety measures							
	Sequence number	Time stamp	Time expectation	Connection authentication	Feedback message	Data integrity assurance	Redundancy with cross checking	Different data integrity assurance systems
Corruption					X	X	X	
Unintended repetition	X							
Incorrect sequence	X							
Loss	X				X			
Unacceptable delay			X					
Insertion	X				X			
Masquerade						X	X	X
Addressing				X				
NOTE The errors "loss" and "insertion" will not be detected by the use of a time stamp. A loss of data is detected within the maximum reaction time by the use of a watchdog. If a message was sent more than once (insertion), the timestamp is unchanged and the receiving device ignores this message.								

In order to avoid systematic and stochastic errors, the following guidelines shall be considered during development and implementation of FSCP 13/1 (see 7.1):

- The producer of safety data shall:
 - generate a time stamp,
NOTE Any new SPDU contains a new time stamp.
 - generate CRCs, and
 - duplicate the safety message depending on the used Safety PDU;
- The consumer of a safety message data shall:
 - check PDU part one with CRC,
 - check PDU part two with CRC,
 - compare PDU part one and two data area bit-for-bit,
 - check the received address,
 - reset the internal watchdog (counter) if a new valid PDU has been received,
 - if a PDU has the same time stamp as the last one or an older one, the PDU shall be ignored,
 - if no valid PDU is received within a defined time (Safety Control Time, see 7.5.4.15), the device shall enter the safe state, and
 - if the watchdog (counter elapsed) has an overrun (not been reset within the maximum time), the device shall enter a safe state.

5.4 Safety communication layer structure

The FSCP 13/1 protocol is layered on top of a standard communication channel, which shall be considered a black channel. Figure 5 shows how the safety communication layer relates to the standard communication channel.

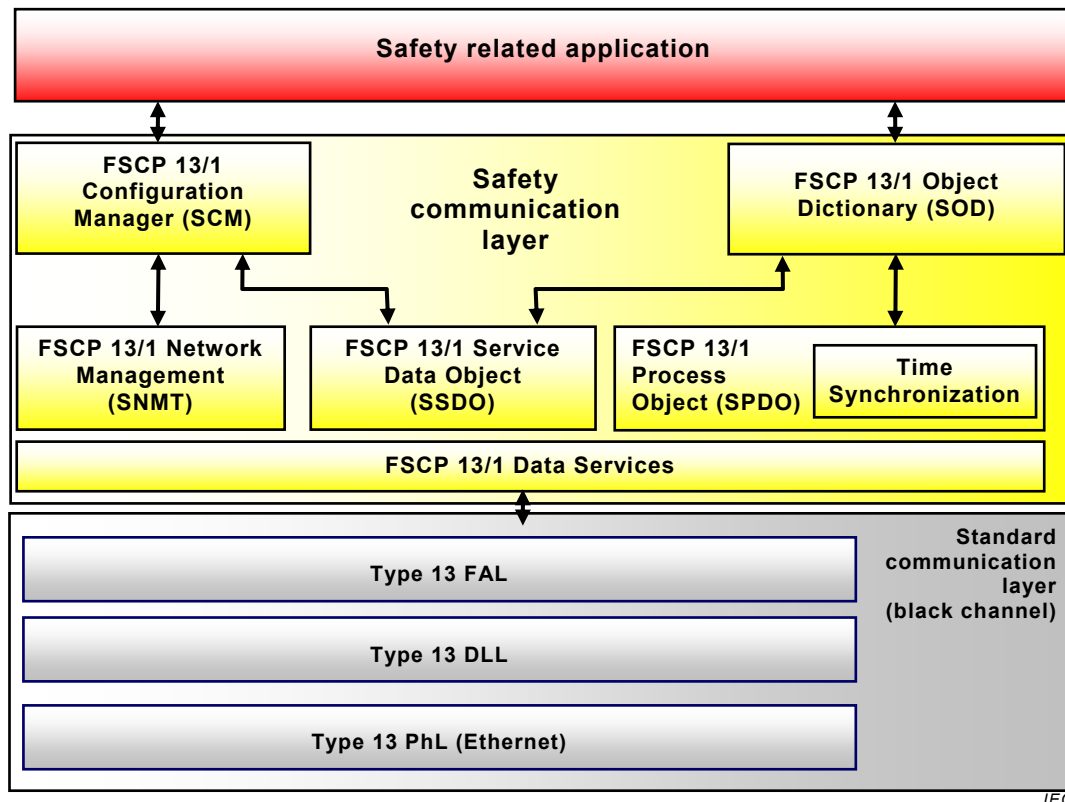


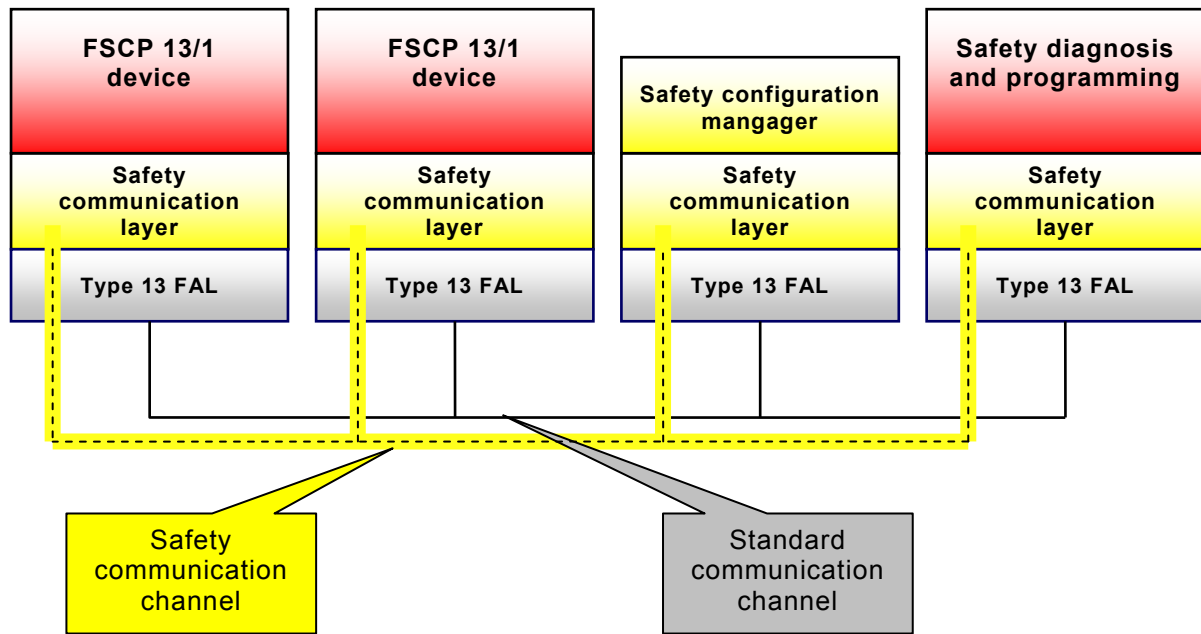
Figure 5 – Communication layer structure

Safety data is produced by the safety-related application entity. This data is encapsulated in a safety message by the safety communication layers and sent via the standard communication channel. The safety communication layer in the receiving device decodes the safety message and verifies integrity and timeliness of the data. The data is presented to the safety-related application entity. If no data is received within a defined time frame, the application entity is informed of this event, which may be used to set all outputs to the safe state.

The safety communication layer provides for:

- safe data transport (integrity and time monitoring),
- network bootup,
- run time diagnosis,
- commissioning,
- program and firmware download,
- parameterization, and
- device replacement.

All these functionalities can be accessed and controlled via the safety communication channel (see Figure 6).



IEC

Figure 6 – Safety communication channel

5.5 Relationships with FAL (and DLL, PhL)

5.5.1 General

FSCP 13/1 shall use the services defined in IEC 61158-5-13.

5.5.2 Data types

Profiles defined in this part support all the CPF 13 data types as defined in IEC 61158-5-13.

6 Safety communication layer services

6.1 Modelling

6.1.1 Reference model

6.1.1.1 General

A FSCP 13/1 compliant implementation shall provide the following application objects:

- Safety Network Management (SNMT),
- Safety Configuration Manager (SCM),
- Safety Service Data Objects (SSDO),
- Safety Object Dictionary (SOD), and
- Safety Process Data Objects (SPDO).

How these application objects relate to each other is shown in Figure 5.

The usage of an underlying communication layer shall be mandatory.

6.1.1.2 Safety network management (SNMT)

The SNMT shall provide the required services for the Safety Configuration Manager (SCM) to configure and verify the safety related nodes within the network.

6.1.1.3 Safety service data objects (SSDO)

The SSDO shall provide the required services to access the Safety Object Dictionary (SOD) and to support the SCM.

6.1.1.4 Safety process data objects (SPDO)

The SPDO shall provide the required services for safety related process data exchange between certain entries within the SOD of communicating nodes. The time synchronization services, which are part of SPDO, shall verify the network performance between the communicating nodes.

6.1.1.5 Safety object dictionary (SOD)

The SOD shall describe the format and access services of the device specific data.

6.1.1.6 Safety configuration manager (SCM)

The SCM shall provide the required services for start-up, parameterization and all further measures to ensure safe operation over the entire life cycle of the application.

6.1.2 Communication model

FSCP 13/1 shall use FAL services defined in IEC 61158-5-13 for data exchange between Safety Nodes (SNs). FSCP 13/1 defines a producer / consumer communication model, built using these services. FSCP 13/1 nodes shall be logically separated into producer and consumer nodes.

Producer nodes shall send data identified by a specific Safety Address (SADR). Any SN within the Safety Domain may receive this data. This is done using the mechanism as described in 7.5. As a result of this communication model, the SADR uniquely identifies an SN as well as a safety PDU sent from a specific node.

Figure 7 shows characteristic producer / consumer communication. The producer node SN1 sends data. The data is uniquely identified by the producers SADR. Each node within the Safety Domain is able to receive this data.

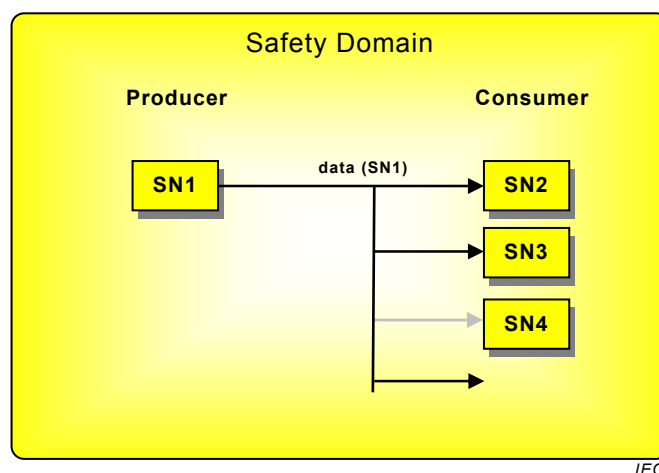


Figure 7 – Characteristic producer / consumer communication

Figure 8 demonstrates an extended version of the producer / consumer communication model which allows the producer to produce separated data for individual consumers. The producer shall use SADR for this. The Safety Configuration Manager (SCM) shall ensure that the SADR used are still unique within the Safety Domain.

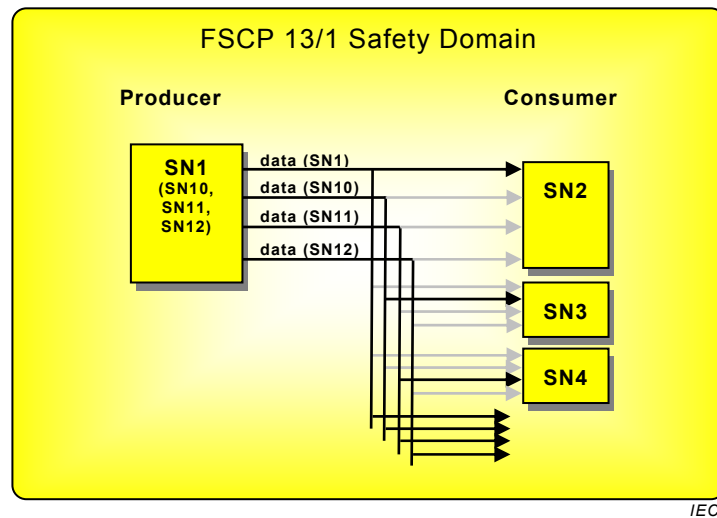


Figure 8 – Extended producer / consumer communication

Figure 9 shows the client server communication which shall be used for configuration services and network management. The SCM (or a dedicated configuration tool, see Clause 8) shall act as the client. SNs shall be limited to the server role.

Using the client server communication model, the client (SCM or Tool) sends a request to the server (SN) which is addressed within the ADR Field (see 7.1.2) using the server address and also contains the client address within the TADR Field (see 7.1.8). The server replies with a response which is addressed within the ADR Field (see 7.1.2) using the server address and also contains the client address within the TADR Field (see 7.1.8).

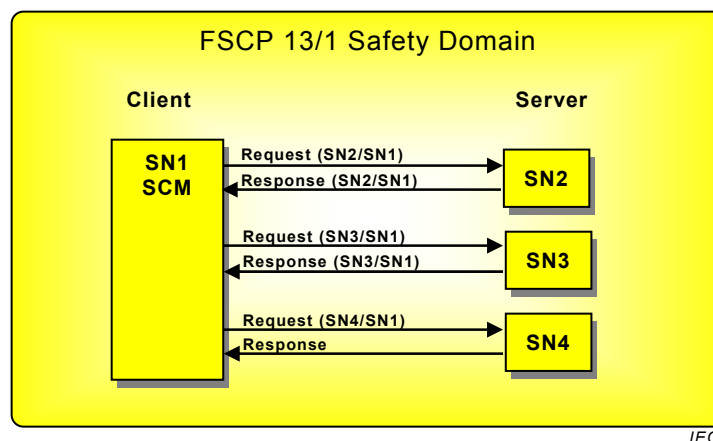


Figure 9 – Client Server communication

6.1.3 Device roles and topology

6.1.3.1 General

FSCP 13/1 device roles are defined in Table 3.

Table 3 – Device roles

Device role	Description
Safety Node (SN)	A FSCP 13/1 compliant device
Safety Configuration Manager(SCM)	Central service for managing a Safety Domain (SD) ^a
Safety Domain Gateway (SDG)	FSCP 13/1 device to exchange data between different SDs
^a A Safety Domain defines an isolated address space of up to 1 023 SNs.	

An FSCP 13/1 device shall implement the device role of an SN and may implement SCM and/or an SDG.

Figure 10 gives an overview of possible interrelationships of device roles and Safety Domains. SD1 gives an example of a simple Safety Domain. Safety related communication of the FSCP 13/1 devices within SD1 is limited to the SNs within SD1.

SD2 in combination with SD3 shows the possibility to set up a FSCP 13/1 communication between different Safety Domains. This is done using a special SDG which is able to communicate with different Safety Domains. Inter-domain communication is handled by the device internally. SDG capability is independent from the SCM capability of a device. The SDG shall have one SADR in SD2 and one SADR in SD3.

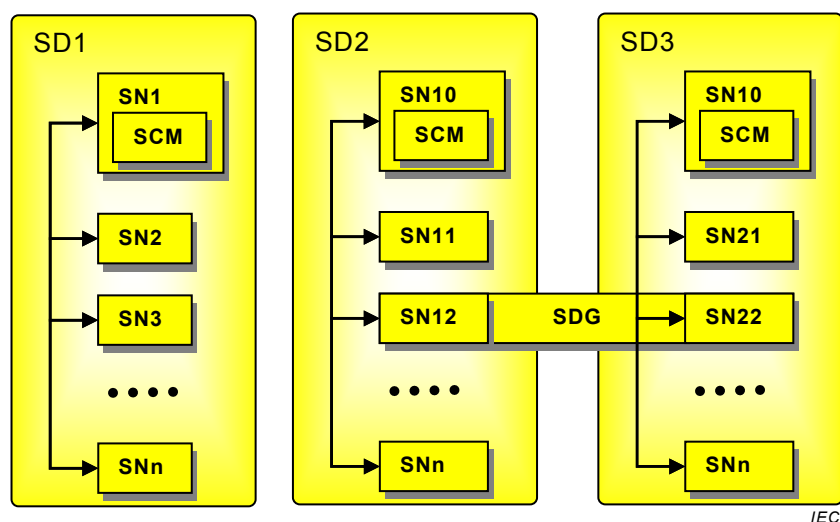


Figure 10 – Topology overview

6.1.3.2 Safety Node (SN)

An SN is a node within any network which conforms to this part. An SN shall be identified by:

- A logical address which is unique within an SD, called Safety Address (SADR). The number range for the SADR shall be 1 – 1 023 (0 is reserved and shall not be used). The SADR shall be defined at the application planning stage. Duplicate SADR within an SD shall be detected by the SCM during network verification at start-up of the SCM or at start-up of any node within the Safety Domain.
- A physical address which is globally unique within all FSCP 13/1 compliant devices, called Unique Device Identification (UDID). Duplicate UDIDs within an SD shall be detected by the SCM.