DIN EN IEC 61784-3-13

ICS 35.160; 35.240.50

Ersatz für
DIN EN 61784-3-13:2018-09
Siehe Anwendungsbeginn

Industrielle Kommunikationsnetze – Profile – Teil 3-13: Funktional sichere Übertragung bei Feldbussen – Zusätzliche Festlegungen für die Kommunikationsprofilfamilie 13 (IEC 61784-3-13:2021); Englische Fassung EN IEC 61784-3-13:2021

Industrial communication networks –
Profiles –
Part 3-13: Functional safety fieldbuses –
Additional specifications for CPF 13
(IEC 61784-3-13:2021);
English version EN IEC 61784-3-13:2021

Réseaux de communication industriels –
Profils –
Partie 3-13: Bus de terrain de sécurité fonctionnelle –
Spécifications supplémentaires pour CPF 13
(IEC 61784-3-13:2021);
Version anglaise EN IEC 61784-3-13:2021

Gesamtumfang 228 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE

Documents
Document Sharing Hub

Full document details: DIN EN IEC 61784-3-13:2023-05

Anwendungsbeginn

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

Für DIN EN 61784-3-13:2018-09 besteht eine Übergangsfrist bis 2024-06-23.

Nationales Vorwort

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

Dieser Entwurf betrifft auch DIN EN IEC 61784-3-2:2023-04, DIN EN IEC 61784-3-3:2023-04, DIN EN IEC 61784-3-8:2023-05 und DIN EN 61784-3-18/A2:2023-05 und wird erst mit Veröffentlichung aller aufgeführten Dokumente zurückgezogen.

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

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

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

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

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

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

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

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

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

Da sich die Benutzer der vorliegenden Norm der englischen Sprache als Fachsprache bedienen, wird die Englische Fassung der EN IEC 61784-3-13 veröffentlicht. Zu deren Einleitung, Abschnitt 1, der den Anwendungsbereich festlegt, und Abschnitt 3, der die Begriffe, Symbole, Abkürzungen und Konventionen festlegt, wurde eine Übersetzung angefertigt und als informativer Nationaler Anhang NA der vorliegenden Norm hinzugefügt. Für die meisten der verwendeten Begriffe existieren keine gebräuchlichen deutschen Benennungen, da sich die deutschen Anwender in der Regel ebenfalls der englischen Benennungen bedienen.

AVA Documents
Document Sharing Hub

Full document details: DIN EN IEC 61784-3-13:2023-05

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

Änderungen

Gegenüber DIN EN 61784-3-13:2018-09 wurden folgende Änderungen vorgenommen:

a) Abschaffung von Block Up-/Download;

b) Hinzufügung von SSDO mit Preload;

c) Hinzufügung von SPDO-Funktionssätzen;

d) Hinzufügung von SPDO mit 40-Bit-Zähler;

e) Hinzufügung von SPDO mit dynamischem SCT;

f) Hinzufügung von zusätzlichen Parametersätzen;

g) Korrekturen und redaktionelle Verbesserungen.

Frühere Ausgaben

DIN EN 61784-3-13: 2012-03, 2018-09

Documents
Document Sharing Hub
Full document details: DIN EN IEC 61784-3-13:2023-05

Nationaler Anhang NA
(informativ)

Auszugsweise Übersetzung

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

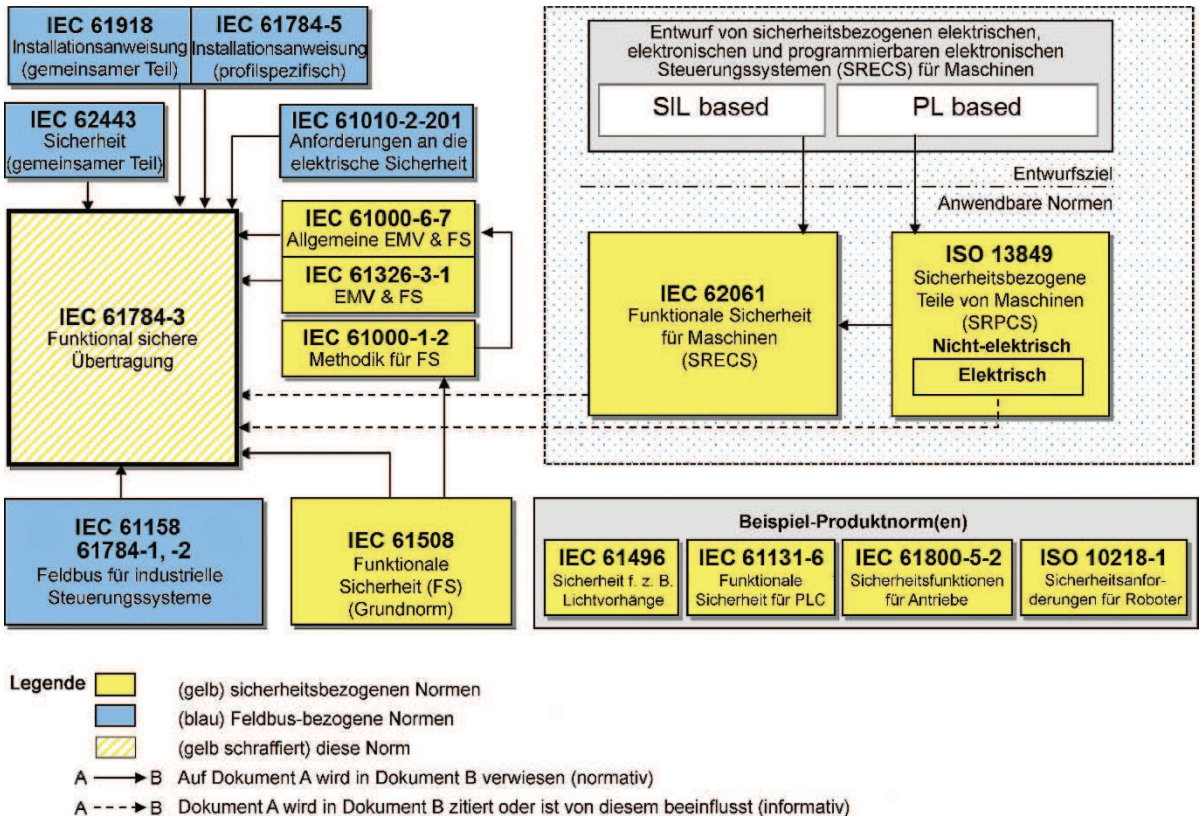
0 Einleitung

0.1 Allgemeines

Die Feldbusnorm IEC 61158 (alle Teile) und ihre Begleitnormen IEC 61784-1 und IEC 61784-2 spezifizieren zusammen mehrere Kommunikationsprotokolle, die die dezentrale Automatisierung von Applikationen ermöglichen. Die Feldbustechnologie hat sich inzwischen in der Praxis bewährt und ist in hohem Maße akzeptiert. So treten nun Feldbuserweiterungen in Erscheinung, die auf Anwendungen für Bereiche wie Echtzeit und sicherheitsbezogene Anwendungen abzielen.

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

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



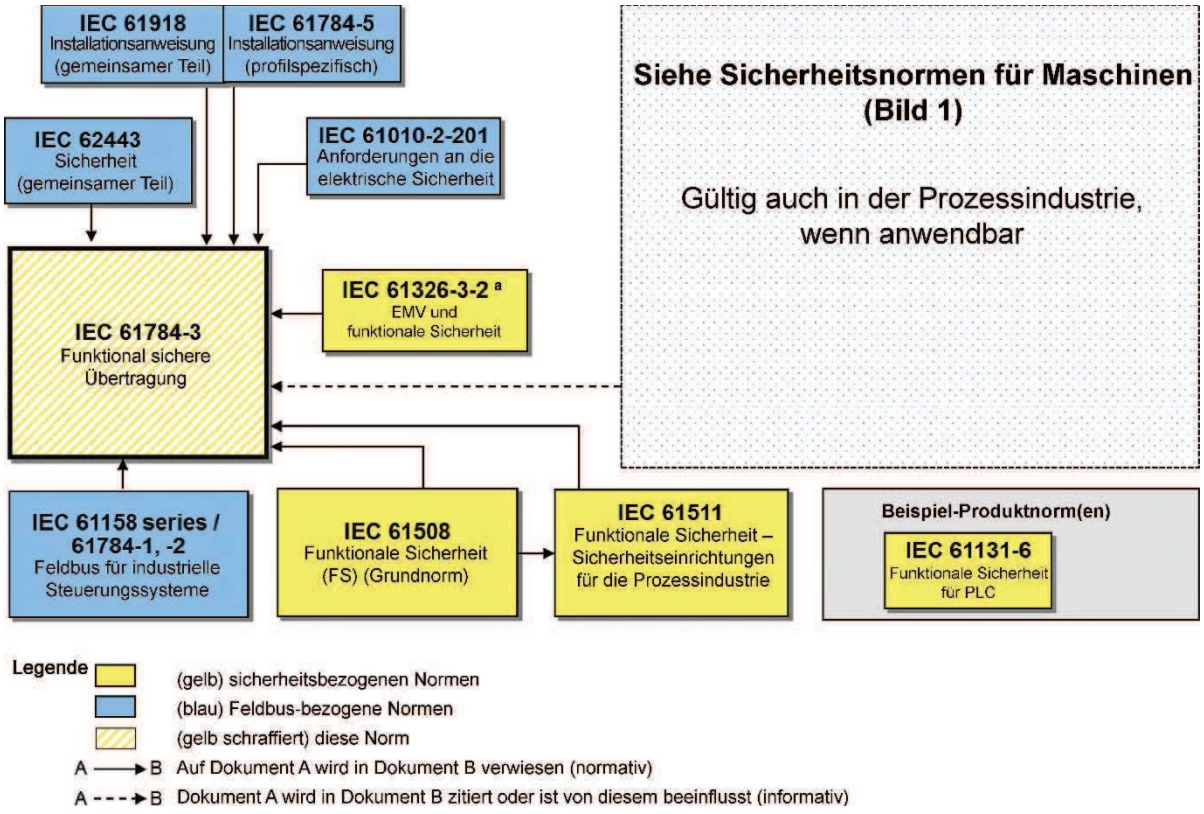
ANMERKUNG IEC 62061 beschreibt das Verhältnis zwischen PL (Kategorie) und SIL.

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

AVA Documents Document Sharing Hub

Full document details: DIN EN IEC 61784-3-13:2023-05

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



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

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

Die als Bestandteile eines sicherheitsbezogenen Systems nach IEC 61508 (alle Teile) implementierten Sicherheitskommunikationsschichten stellen 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 sicher.

Die in IEC 61784-3 (alle Teile) spezifizierten Sicherheitskommunikationsschichten tun dies dergestalt, dass ein Feldbus in Anwendungen mit funktionaler Sicherheit bis zu dem Sicherheits-Integritätslevel (SIL) eingesetzt werden kann, der im jeweiligen Kommunikationsprofil für funktional sichere Übertragung festgelegt ist.

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

IEC 61784-3 (alle Teile) beschreibt:

– grundlegende Prinzipien für die Erfüllung der Anforderungen von IEC 61508 (alle Teile) für die funktional sichere Kommunikation, einschließlich möglicher Übertragungsfehler, deren Abhilfemaßnahmen und Betrachtungen zur Datenintegrität;

– funktional sichere Kommunikationsprofile für mehrere Kommunikationsprofilfamilien von IEC 61784-1 und IEC 61784-2, welche Ergänzungen der Kommunikationsdienst- und -protokollabschnitte von IEC 61158 (alle Teile) um eine Sicherheitsschicht enthalten.

AVA Documents Document Sharing Hub

Full document details: DIN EN IEC 61784-3-13:2023-05

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

Der Halter dieser Patentrechte hat IEC zugesichert, dass er bereit ist, über Lizenzen zu vernünftigen und nicht diskriminierenden Geschäftsbedingungen mit Antragstellern in der ganzen Welt zu verhandeln. In diesem Zusammenhang ist die Erklärung des Halters dieser Patentrechte bei IEC registriert. Informationen sind bei der Patentdatenbank unter: http://patents.iec.ch erhältlich.

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

1 Anwendungsbereich

Dieser Teil von IEC 61784-3 (alle Teile) legt eine Sicherheitsschicht (Dienste und Protokoll) fest, die auf CPF 13 von IEC 61784-2 und IEC 61158, Typ 13, beruht. Sie stellt die Grundsätze der funktional sicheren Kommunikation nach IEC 61784-3 fest, die für diese Sicherheitskommunikationsschicht wichtig sind. Diese Sicherheitskommunikationsschicht ist für die ausschließliche Implementierung in Sicherheitsgeräten vorgesehen.

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

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

Dieses Dokument enthält Leitlinien sowohl für Entwickler als auch Gutachter von entsprechenden Geräten und Systemen.

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

3 Begriffe, Symbole, Abkürzungen und Konventionen

3.1 Begriffe

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

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

- IEC Electropedia: verfügbar unter http://www.electropedia.org/
- ISO-Online-Browsing Platform: verfügbar unter http://www.iso.org/obp

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

Documents
Document Sharing Hub
Full document details: DIN EN IEC 61784-3-13:2023-05

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

3.1.1 Allgemeine Begriffe

ANMERKUNG Diese allgemeinen Begriffe wurden aus IEC 61784-3:2021 übernommen.

3.1.1.1
Bitfehlerwahrscheinlichkeit
en **bit error probability**
Pe
Wahrscheinlichkeit, dass für ein gegebenes Bit der falsche Wert empfangen wird

3.1.1.2
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.

3.1.1.3
geschlossenes Kommunikationssystem
en **closed communication system**
festgelegte Anzahl oder festgelegte maximale Anzahl von Teilnehmern, die über ein *Kommunikationssystem* verbunden sind, mit wohldefinierten und festgelegten Eigenschaften und wo das *Risiko* eines unerlaubten Zugriffs als vernachlässigbar betrachtet wird

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

3.1.1.4
Kommunikationskanal
en **communication channel**
logische *Verbindung* zwischen zwei Endpunkten in einem *Kommunikationssystem*

3.1.1.5
Kommunikationssystem
en **communication system**
Anordnung von Hardware, Software und Ausbreitungsmedien zur Übertragung von *Nachrichten* (ISO/IEC 7498-1-Anwendungsschicht) von einer Anwendung zur anderen

3.1.1.6
Verbindung
en **connection**
logische Verbindung zwischen zwei Anwendungsobjekten in demselben oder in unterschiedlichen Geräten

3.1.1.7
zyklische Redundanzprüfung
en **Cyclic Redundancy Check**
CRC
<Wert> redundante Daten, abgeleitet von einem Block von Daten und mit diesen zusammen gespeichert oder übertragen zur Aufdeckung von Datenverfälschungen;

<Methode> Prozedur zur Berechnung der redundanten Daten

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

Documents
Document Sharing Hub
Full document details: DIN EN IEC 61784-3-13:2023-05

Anmerkung 2 zum Begriff: Siehe auch: [31][32][2].

3.1.1.8
festgelegtes Kommunikationssystem
en **defined communication system**
defined channel
festgelegte Anzahl oder festgelegte maximale Anzahl von Teilnehmern, die über ein Kommunikationssystem verbunden sind, mit wohldefinierten und festgelegten Eigenschaften wie beispielsweise Aufbaubedingungen, elektromagnetische Störfestigkeit, industrielle (aktive) Netzwerkkomponenten und wo das Risiko eines unerlaubten Zugriffs nach dem Lebenszyklusmodell der IEC 62443 (alle Teile) auf ein toleriertes Maß reduziert ist durch zum Beispiel Zonen und Durchleitungen

3.1.1.9
DLPDU
ABGELEHNT: frame
Data Link Protocol Data Unit

3.1.1.10
Fehler
en **error**
Unterschied zwischen einem berechneten, beobachteten bzw. gemessenen Wert oder Zustand und dem wahren, spezifizierten bzw. theoretisch korrekten Wert oder Zustand

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

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

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

3.1.1.12
Fehler
en **fault**
nicht normale Bedingung, die eine Verminderung oder den Verlust der Fähigkeit einer Funktionseinheit verursachen kann, eine geforderte Funktion auszuführen

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

[QUELLE: IEC 61508-4:2010, 3.6.1, modifiziert – Referenz auf Bild entfernt]

[2] Die Zahlen in eckigen Klammern verweisen auf die Literaturhinweise.

Documents
Document Sharing Hub
Full document details: DIN EN IEC 61784-3-13:2023-05

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
Hash-Funktion
en **hash function**
(mathematische) Funktion, die Werte aus einem (möglicherweise sehr) großen Wertebereich in einem (üblicherweise) kleineren Wertebereich abbildet

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

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

3.1.1.16
Gefährdung
en **hazard**
potentielle Schadensquelle

Anmerkung 1 zum Begriff: Der Begriff umfasst sowohl kurzfristig auftretende Gefahren für Personen (z. B. Brand und Explosion) als auch solche, die sich langfristig auf die Gesundheit auswirken (z. B. Freisetzung eines giftigen Stoffes).

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

3.1.1.17
Master
en **master**
aktive Kommunikationseinheit, die Kommunikationsaktivitäten anderer Stationen, seien es Master oder Slaves, einleiten und planen kann

3.1.1.18
Nachricht
en **message**
geordnete Folge von Octets, bestimmt für die Übermittlung von Information

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

3.1.1.19
Performance Level
en **performance level**
PL
diskreter Level, der die Fähigkeit von sicherheitsbezogenen Teilen einer Steuerung spezifiziert, eine *Sicherheitsfunktion* unter vorhersehbaren Bedingungen auszuführen

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

3.1.1.20
Redundanz
en **redundancy**
Vorhandensein von mehr als einem Mittel zum Ausführen einer geforderten Funktion oder zur Darstellung von Informationen

AVA Documents
Document Sharing Hub

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

3.1.1.21
Restfehlerrate
en **residual error rate**
statistische Rate, mit der die *Sicherheitsmaßnahmen* im SCL *Fehler* nicht aufdecken

3.1.1.22
Risiko
en **risk**
Kombination aus der Wahrscheinlichkeit, mit der ein Schaden auftritt, und dem Ausmaß dieses Schadens

Anmerkung 1 zum Begriff: Für die weitere Diskussion dieses Begriffs siehe IEC 61508-5:2010, Anhang A.

[QUELLE: IEC 61508-4:2010, 3.1.6 und ISO/IEC Guide 51:2014, Definition 3.9, modifiziert – andere Anmerkung]

3.1.1.23
Sicherheitskommunikationskanal
en **safety communication channel**
Kommunikationskanal beginnend auf dem SCL der Nachrichtenquelle und endend auf dem SCL der Nachrichtensenke

Anmerkung 1 zum Begriff: Er kann als zwei SCLs modelliert werden, die über einen „*Black Channel*“, ein *festgelegtes Kommunikationssystem* oder einen *festgelegten Kanal* verbunden sind.

3.1.1.24
Sicherheitskommunikationsschicht
en **safety communication layer**
SCL
Kommunikationsschicht über dem FAL, die die notwendigen zusätzlichen Mittel beinhaltet, um die sichere Übertragung von Daten entsprechend den Anforderungen von IEC 61508 sicherzustellen

3.1.1.25
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.

3.1.1.26
Sicherheitsgerät
en **safety device**
Gerät, welches nach IEC 61508 ausgeführt wurde und das funktional sichere Kommunikationsprofil zur Anwendung bringt

3.1.1.27
Sicherheitsfunktion
en **safety function**
Funktion, die von einem *sicherheitsbezogenen E/E/PE-System* oder anderen *risiko*mindernden Maßnahmen ausgeführt wird und dazu vorgesehen ist, unter Berücksichtigung eines festgelegten gefährlichen Vorfalls einen sicheren Zustand für die EUC zu erreichen oder aufrechtzuerhalten

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

Documents
Document Sharing Hub
Full document details: DIN EN IEC 61784-3-13:2023-05

3.1.1.28
Reaktionszeit einer Sicherheitsfunktion
en **safety function response time**
im ungünstigsten Fall benötigte Zeit nach Aktivierung eines am *Feldbus* angeschlossenen Sicherheitssensors, bis der zugehörige sichere Zustand des Sicherheitsaktors erreicht wurde unter Berücksichtigung von gleichzeitig auftretenden *Fehlern* und *Ausfällen* in der *Sicherheitsfunktion*

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

3.1.1.29
Sicherheits-Integritätslevel
en **safety integrity level**
SIL
eine von vier diskreten Stufen, die einem Wertebereich der Sicherheitsintegrität entsprechen, wobei der Sicherheits-Integritätslevel 4 die höchste Stufe der Sicherheitsintegrität und der Sicherheits-Integritätslevel 1 die niedrigste darstellt

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

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

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

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

3.1.1.30
Sicherheitsmaßnahme
en **safety measure**
Mittel zur Beherrschung möglicher Kommunikations*fehler*, welches in Übereinstimmung mit den Anforderungen der IEC 61508 entworfen und ausgeführt wurde

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

Anmerkung 2 zum Begriff: Kommunikations*fehler* und zugehörige Sicherheitsmaßnahmen sind ausführlich in IEC 61784-3:2021, 5.3 und 5.4 beschrieben.

3.1.1.31
Sicherheits-PDU
en **safety PDU**
SPDU
durch einen *Sicherheitskommunikationskanal* übertragene PDU

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

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

AVA Documents
Document Sharing Hub
Full document details: DIN EN IEC 61784-3-13:2023-05

3.1.1.32
sicherheitsbezogene Anwendung
en **safety-related application**
Programme, welche in Übereinstimmung mit den Anforderungen von IEC 61508 ausgeführt sind, um die SIL-Anforderungen einer Anwendung einzuhalten

3.1.1.33
sicherheitsbezogenes System
en **safety-related system**
System, welches *Sicherheitsfunktionen* nach IEC 61508 ausführt

3.1.1.34
Slave
en **slave**
Kommunikationseinheit, die *Nachrichten* empfangen und sie als Antwort an andere Kommunikationseinheiten senden kann, die *Master* oder Slave sein können, aber nicht, um Kommunikationsaktivitäten zu initiieren

3.1.1.35
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 Elektrorauschen

3.1.2.2
DVI
en **device vendor information**
Informationen für die Identifizierung eines *Sicherheitsknotens*

3.1.2.3
Sicherheitsadresse
en **safety address**
SADR
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
en **safety node**
SN
Knoten mit *Sicherheitsfunktion*

3.1.2.6
Sicherheitsdomäne
en **safety domain**
SD
Adressbereich für bis zu 1 023 *Sicherheitsknoten*

Documents
Document Sharing Hub
Full document details: DIN EN IEC 61784-3-13:2023-05

3.1.2.7
Sicherheitsdomänen-Gateway
en **safety domain gateway**
SDG
Gateway für den Austausch von Daten zwischen verschiedenen *Sicherheitsdomänen*

3.1.2.8
Nummer der Sicherheitsdomäne
en **safety domain number**
SDN
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 Sicherheits*feldbusses* zugänglich sind

3.1.2.11
Sicherheitsprozessdatenobjekt
en **safety process data object**
SPDO
Objekt für den Austausch von Prozessdaten zwischen verschiedenen *Sicherheitsknoten*

3.1.2.12
Sicherheitsservicedatenobjekt
en **safety service data object**
SSDO
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

Documents
Document Sharing Hub
Full document details: DIN EN IEC 61784-3-13:2023-05

3.2 Symbole und Abkürzungen

3.2.1 Allgemeine Symbole und Abkürzungen

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

3.2.2 CPF 13: Zusätzliche Symbole und Abkürzungen

ACM	Automatischer Konfigurationsmodus (en: automatic configuration mode)	
ADR	Wählinformation (Quelle oder Ziel) (en: address information)	
APDU	Anwendungsprotokoll-Dateneinheit (en: application protocol data unit)	[ISO/IEC 7498-1]

Documents
Document Sharing Hub
Full document details: DIN EN IEC 61784-3-13:2023-05

CN	gesteuerter Knoten (en: controlled node)	[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 (en: least significant octet)	
MAC	Medienzugriffsschicht (en: medium access layer)	
MCM	manueller Konfigurationsmodus (en: manual configuration mode)	
MN	Steuerungsknoten (en: managing node)	[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)	

AVA Documents
Document Sharing Hub
Full document details: DIN EN IEC 61784-3-13:2023-05

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 Dokument 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 Anwendungsbereichs 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.

Documents
Document Sharing Hub
Full document details: DIN EN IEC 61784-3-13:2023-05

EUROPEAN STANDARD

NORME EUROPÉENE

EUROPÄISCHE NORM

EN IEC 61784-3-13

June 2021

ICS 25.040.40; 35.100.05

Supersedes EN 61784-3-13:2017 and all of its amendments and corrigenda (if any)

English version

Industrial communication networks – Profiles – Part 3-13: Functional safety fieldbuses – Additional specifications for CPF 13 (IEC 61784-3-13:2021)

Réseaux de communication industriels – Profils – Partie 3-13: Bus de terrain de sécurité fonctionnelle – Spécifications supplémentaires pour CPF 13 (IEC 61784-3-13:2021)

Industrielle Kommunikationsnetze – Profile – Teil 3-13: Funktional sichere Übertragung bei Feldbussen – Zusätzliche Festlegungen für die Kommunikationsprofilfamilie 13 (IEC 61784-3-13:2021)

This European Standard was approved by CENELEC on 2021-06-23. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

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

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

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



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

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

Documents
Document Sharing Hub

Full document details: DIN EN IEC 61784-3-13:2023-05

European foreword

The text of document 65C/1083/FDIS, future edition 3 of IEC 61784-3-13, prepared by SC 65C "Industrial networks" of IEC/TC 65 "Industrial-process measurement, control and automation" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN IEC 61784-3-13:2021.

The following dates are fixed:

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

This document supersedes EN 61784-3-13:2017 and all of its amendments and corrigenda (if any).

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

Endorsement notice

The text of the International Standard IEC 61784-3-13:2021 was approved by CENELEC as a European Standard without any modification.

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

IEC 61000-1-2	NOTE	Harmonized as EN 61000-1-2
IEC 61000-6-7	NOTE	Harmonized as EN 61000-6-7
IEC 61010-2-201	NOTE	Harmonized as EN IEC 61010-2-201
IEC 61131-2	NOTE	Harmonized as EN 61131-2
IEC 61131-6	NOTE	Harmonized as EN 61131-6
IEC 61158 (series)	NOTE	Harmonized as EN 61158 (series)
IEC 61158-5 (series)	NOTE	Harmonized as EN 61158-5 (series)
IEC 61326-3-1	NOTE	Harmonized as EN 61326-3-1
IEC 61326-3-2	NOTE	Harmonized as EN IEC 61326-3-2
IEC 61496 (series)	NOTE	Harmonized as EN IEC 61496 (series)
IEC 61508-1:2010	NOTE	Harmonized as EN 61508-1:2010 (not modified)
IEC 61508-4:2010	NOTE	Harmonized as EN 61508-4:2010 (not modified)
IEC 61508-5:2010	NOTE	Harmonized as EN 61508-5:2010 (not modified)
IEC 61511 (series)	NOTE	Harmonized as EN 61511 (series)
IEC 61784-1	NOTE	Harmonized as EN IEC 61784-1
IEC 61784-3 (series)	NOTE	Harmonized as EN 61784-3 (series)
IEC 61784-5 (series)	NOTE	Harmonized as EN IEC 61784-5 (series)
IEC 61800-5-2	NOTE	Harmonized as EN 61800-5-2
IEC 62061	NOTE	Harmonized as EN 62061
IEC 62443 (series)	NOTE	Harmonized as EN IEC 62443 (series)
ISO 10218-1	NOTE	Harmonized as EN ISO 10218-1
ISO 13849 (series)	NOTE	Harmonized as EN ISO 13849 (series)
ISO 13849-1:2015	NOTE	Harmonized as EN ISO 13849-1:2015 (not modified)
ISO 13849-2	NOTE	Harmonized as EN ISO 13849-2

Documents
Document Sharing Hub
Full document details: DIN EN IEC 61784-3-13:2023-05

Annex ZA
(normative)

Normative references to international publications with their corresponding European publications

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

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

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

Publication	Year	Title	EN/HD	Year
IEC 61131-3	-	Programmable controllers – Part 3: Programming languages	EN 61131-3	-
IEC 61158-3-13	-	Industrial communication networks – Fieldbus specifications – Part 3-13: Data link layer service definition – Type 13 elements	EN 61158-3-13	-
IEC 61158-4-13	-	Industrial communication networks – Fieldbus specifications – Part 4-13: Data-link layer protocol specificationn – Type 13 elements	EN 61158-4-13	-
IEC 61158-5-13	-	Industrial communication networks – Fieldbus specifications – Part 5-13: Application layer service definition – Type 13 elements	EN 61158-5-13	-
IEC 61158-6-13	-	Industrial communication networks – Fieldbus specifications – Part 6-13: Application layer protocol specification – Type 13 elements	EN 61158-6-13	-
IEC 61508	series	Functional safety of electrical/electronic/programmable electronic safety-related systems	EN 61508	series
IEC 61784-2	-	Industrial communication networks – Profiles – Part 2: Additional fieldbus profiles for real-time networks based on ISO/IEC/IEEE 8802-3	EN IEC 61784-2	-
IEC 61784-3	2021	Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions	EN IEC 61784-3	2021
IEC 61784-5-13	-	Industrial communication networks – Profiles – Part 5-13: installation of fieldbuses – Installation profiles for CPF 13	EN 61784-5-13	-

Documents
Document Sharing Hub

IEC 61918	-	Industrial communication networks – Installation of communication networks in industrial premises	EN IEC 61918	-
ISO/IEC 19501	-	Information technology – Open Distributed Processing – Unified Modeling Language (UML) Version 1.4.2	-	-

Documents
Document Sharing Hub

Full document details: DIN EN IEC 61784-3-13:2023-05

CONTENTS

European foreword 18
Endorsement notice 18
Annex ZA (normative) Normative references to international publications with their corresponding European publications 19
0 Introduction 34
0.1 General 34
0.2 Patent declaration 36
1 Scope 37
2 Normative references 37
3 Terms, definitions, symbols, abbreviated terms and conventions 38
3.1 Terms and definitions 38
3.1.1 Common terms and definitions 38
3.1.2 CPF 13: Additional terms and definitions 42
3.2 Symbols and abbreviated terms 44
3.2.1 Common symbols and abbreviated terms 44
3.2.2 CPF 13: Additional symbols and abbreviated terms 44
3.3 Conventions 45
3.3.1 Hexadecimal values 45
3.3.2 Binary values 46
3.3.3 Wildcard digits 46
3.3.4 Diagrams 46
4 Overview of FSCP 13/1 (openSAFETY™) 46
4.1 Functional Safety Communication Profile 13/1 46
4.2 Technical overview 46
5 General 47
5.1 External documents providing specifications for the profile 47
5.2 Safety functional requirements 47
5.3 Safety measures 48
5.4 Safety communication layer structure 49
5.5 Relationships with FAL (and DLL, PhL) 51
5.5.1 General 51
5.5.2 Data types 51
6 Safety communication layer services 51
6.1 Modelling 51
6.1.1 Reference model 51
6.1.2 Communication model 52
6.1.3 Device roles and topology 53
6.2 Life cycle model 57

Documents
Document Sharing Hub
Full document details: DIN EN IEC 61784-3-13:2023-05

6.2.1 General ... 57
6.2.2 Concept, planning and implementation ... 57
6.2.3 Commissioning ... 58
6.2.4 Operation terms ... 59
6.2.5 Maintenance terms ... 61
6.3 Non safety communication layer ... 61
6.3.1 General ... 61
6.3.2 Requirements for data transport ... 61
6.3.3 Domain protection and separation ... 64
7 Safety communication layer protocol ... 65
7.1 Safety PDU format ... 65
7.1.1 Structure of Safety PDUs ... 65
7.1.2 Address field (ADR) ... 69
7.1.3 PDU identification field (ID) ... 69
7.1.4 Length field (LE) ... 71
7.1.5 Consecutive Time field (CT) ... 71
7.1.6 Payload data field (DB0 to DBn) ... 71
7.1.7 Cyclic Redundancy Check field (CRC-8 / CRC-16) ... 71
7.1.8 Time Request Address field (TADR) ... 72
7.1.9 Time Request Distinctive Number field (TR) ... 72
7.1.10 UDID of SCM coding (UDID of SCM) ... 72
7.2 Safety Process Data Object (SPDO) ... 73
7.2.1 General ... 73
7.2.2 SPDO telegram types ... 73
7.2.3 Data Only telegram ... 73
7.2.4 Data with Time Request telegram ... 74
7.2.5 Data with Time Response telegram ... 75
7.3 Safety Service Data Object (SSDO) ... 76
7.3.1 General ... 76
7.3.2 SSDO telegram types ... 76
7.3.3 SSDO services and protocols ... 77
7.3.4 SSDO Download Initiate ... 79
7.3.5 SSDO Download Segment ... 80
7.3.6 SSDO Download Initiate with Preload ... 81
7.3.7 SSDO Download Segment with Preload ... 82
7.3.8 SSDO Upload Initiate ... 84
7.3.9 SSDO Upload Segment ... 85
7.3.10 SSDO Upload Initiate with Preload ... 86
7.3.11 SSDO Upload Segment with Preload ... 87

Documents
Document Sharing Hub
Full document details: DIN EN IEC 61784-3-13:2023-05

7.3.12 SSDO Abort 89
7.3.13 SSDO Preload 90
7.4 Safety Network Management (SNMT) 91
7.4.1 General 91
7.4.2 SNMT telegram types 91
7.4.3 SNMT services and protocols 92
7.5 Safety Object dictionary (SOD) 106
7.5.1 General 106
7.5.2 Object dictionary entry definition 106
7.5.3 Data type entry specification 112
7.5.4 Object description 114
7.6 Safety related PDO mapping 161
7.6.1 General 161
7.6.2 Transmit SPDOs 162
7.6.3 Receive SPDOs 162
7.6.4 SPDO mapping parameter 162
7.6.5 SPDO mapping example 163
7.6.6 SDPO Feature Set 165
7.6.7 SPDO error handling 166
7.7 State and sequence diagrams 167
7.7.1 Safety Process Data Object (SPDO) 167
7.7.2 Time synchronization and validation 171
7.7.3 Safety Service Data Object (SSDO) 182
7.7.4 SOD access 183
7.7.5 Safety Network Management Object (SNMT) 193
7.7.6 SN power up 195
7.7.7 SN power down 203
7.7.8 SN recovery after Restart / Error 203
7.7.9 SCM power up 203
7.7.10 Address verification 206
7.7.11 Commissioning mode 208
7.7.12 Handle single UDID mismatch 208
7.7.13 Activate SN 212
7.7.14 Device exchange 213
8 Safety communication layer management 213
8.1 General 213
8.2 Configuration of a Safety Domain 213
8.3 Parameter check mechanism 214
9 System requirements 214

Documents
Document Sharing Hub
Full document details: DIN EN IEC 61784-3-13:2023-05

9.1 Indicators and switches 214
9.2 Installation guidelines 214
9.3 Safety function response time 214
9.4 Duration of demands 215
9.5 Constraints for calculation of system characteristics 215
9.5.1 General 215
9.5.2 Number of sinks limit 216
9.5.3 Message rate limit 216
9.5.4 Message payload limit 216
9.5.5 Bit error rate considerations 216
9.5.6 Residual error rate 217
9.6 Maintenance 218
9.6.1 Diagnostic information 218
9.6.2 Replacement of safety related devices 218
9.6.3 Modification 219
9.6.4 Machine part changing 219
9.6.5 Firmware update of safety related nodes 219
9.6.6 Machine check due to service interval 219
9.7 Safety manual 219
10 Assessment 219
10.1 General 219
10.2 CP 13/1 assessment 220
10.3 FSCP 13/1 conformance test 220
10.4 Approval of functional safety by competent assessment body 220
Anhang A (informative) Additional information for functional safety communication profiles of CPF 13 221
A.1 Hash function calculation 221
A.2 Void 224
Anhang B (informative) Information for assessment of the functional safety communication profiles of CPF 13 225
Bibliography 226

Figure 1 – Relationships of IEC 61784-3 with other standards (machinery) 34
Figure 2 – Relationships of IEC 61784-3 with other standards (process) 35
Figure 3 – Producer consumer example 47
Figure 4 – Client server example 47
Figure 5 – Communication layer structure 50
Figure 6 – Safety communication channel 51
Figure 7 – Characteristic producer / consumer communication 52
Figure 8 – Extended producer / consumer communication 53

Documents
Document Sharing Hub
Full document details: DIN EN IEC 61784-3-13:2023-05

Figure 9 – Client Server communication 53
Figure 10 – Topology overview 54
Figure 11 – Safety Domain protection (example) 55
Figure 12 – Safety Domain separation (example) 56
Figure 13 – Data flow example 60
Figure 14 – Communication model 61
Figure 15 – SPDO transport 62
Figure 16 – SSDO transport 63
Figure 17 – Diagnostic data representation 64
Figure 18 – Safety PDUs inside a CP 13/1 PDU 65
Figure 19 – Basic Safety PDU for n = 0 – 8 octet payload data 65
Figure 20 – Basic Safety PDU from 9 octet payload data 66
Figure 21 – Slim Safety PDU for n = 0 – 8 octet payload data 67
Figure 22 – Slim Safety PDU from 9 octet payload data 67
Figure 23 – Safety PDU with 40 bit counter for n = 0 – 8 octet payload data 68
Figure 24 – Safety PDU with 40 bit counter from 9 octet payload data 68
Figure 25 – SPDO_Data_Only telegram 74
Figure 26 – SPDO_Data_with_Time_Request telegram 75
Figure 27 – SPDO_Data_with_Time_Response telegram 75
Figure 28 – SSDO download protocols 78
Figure 29 – SSDO upload protocols 79
Figure 30 – SSDO Download Initiate protocol 79
Figure 31 – SSDO Download Segment protocol 80
Figure 32 – SSDO Download Initiate protocol with Preload 81
Figure 33 – SSDO Download Segment protocol with Preload 83
Figure 34 – SSDO Upload Initiate protocol 84
Figure 35 – SSDO Upload Segment protocol 85
Figure 36 – SSDO Upload Initiate protocol with Preload 86
Figure 37 – SSDO Upload Segment protocol with Preload 88
Figure 38 – SSDO Abort protocol 89
Figure 39 – UDID Request / Response protocol 92
Figure 40 – SADR Assignment protocol 93
Figure 41 – Reset Node Guarding Time protocol 94
Figure 42 – SN set to Pre-Operational protocol 96
Figure 43 – SN set to Operational protocol 97
Figure 44 – SN Acknowledge protocol 100
Figure 45 – SN set to stop protocol 100
Figure 46 – SCM set to Operational protocol 101
Figure 47 – Node Guarding protocol 102

Documents
Document Sharing Hub
Full document details: DIN EN IEC 61784-3-13:2023-05

Figure 48 – Additional SADR Assignment protocol 103
Figure 49 – UDID of SCM Assignment protocol 104
Figure 50 – Init CT value assignment protocol 105
Figure 51 – SPDO mapping example 163
Figure 52 – State diagram TxSPDO 167
Figure 53 – SPDO communication producer 167
Figure 54 – State diagram RxSPDO 168
Figure 55 – SPDO communication consumer 169
Figure 56 – State diagram process data 170
Figure 57 – Time synchronization and validation 171
Figure 58 – Time synchronization detail 172
Figure 59 – Calculation of propagation delay 174
Figure 60 – Time validation, propagation delay explanation limits 174
Figure 61 – Time synchronization on a nonsafe network 176
Figure 62 – Explanation of time synchronization 176
Figure 63 – Time synchronization failure 177
Figure 64 – State diagram time synchronization producer 178
Figure 65 – State diagram time synchronization consumer 180
Figure 66 – State diagram SSDO client 182
Figure 67 – State diagram SSDO server 183
Figure 68 – Expedited SOD access 184
Figure 69 – State diagram segmented SOD download access client 185
Figure 70 – Segmented SOD download access 186
Figure 71 – State diagram segmented SOD download access server 187
Figure 72 – State diagram SOD preload download access client 189
Figure 73 – SOD preload download access 190
Figure 74 – State diagram SOD preload download access server 192
Figure 75 – State diagram SNMT master 194
Figure 76 – State diagram SNMT slave 195
Figure 77 – State diagram SN power up 196
Figure 78 – State diagram SN Pre-Operational 198
Figure 79 – State diagram SN additional paramters 201
Figure 80 – State diagram SN Operational 202
Figure 81 – Life Guarding telegram 203
Figure 82 – State diagram SCM power up 204
Figure 83 – State diagram SCM Operational 205
Figure 84 – State diagram SCM address verification 207
Figure 85 – State diagram SCM handle single UDID mismatch 209
Figure 86 – State diagram SCM verify parameters 211

Documents
Document Sharing Hub
Full document details: DIN EN IEC 61784-3-13:2023-05

Figure 87 – State diagram activate SN 212
Figure 88 – Safety function response time 214
Figure 89 – Assessment flow of devices 220

Table 1 – Communication errors and detection measures (cyclic) 48
Table 2 – Communication errors and detection measures (acyclic) 49
Table 3 – Device roles 54
Table 4 – Basic Safety PDU format 66
Table 5 – Slim Safety PDU format 67
Table 6 – Safety PDU with 40 bit counter 69
Table 7 – PDU identification field (ID) 70
Table 8 – Used ID field combinations 70
Table 9 – Request / response identification 71
Table 10 – Type of CRC depending on LE 71
Table 11 – CRC polynoms for SPDUs 72
Table 12 – SPDO telegram types (ID field, bits 2, 3 and 4) 73
Table 13 – Fields of SPDO_Data_Only telegram 74
Table 14 – Fields of SPDO_Data_with_Time_Request telegram 75
Table 15 – Fields of SPDO_Data_with_Time_Response telegram 76
Table 16 – SSDO telegram types (ID field, bits 2, 3 and 4) 76
Table 17 – SOD Access Command (SACmd) – bit coding 77
Table 18 – Fields of Download Initiate SSDO_Service_Request telegram 79
Table 19 – Fields of Download Initiate SSDO_Service_Response telegram 80
Table 20 – Fields of Download Segment SSDO_Service_Request telegram 81
Table 21 – Fields of Download Segment SSDO_Service_Response telegram 81
Table 22 – Fields of Download Initiate SSDO_Service_Request telegram with Preload 82
Table 23 – Fields of Download Initiate SSDO_Service_Response telegram with Preload 82
Table 24 – Fields of Download Segment SSDO_Service_Request telegram with Preload 83
Table 25 – Fields of Download Segment SSDO_Service_Response telegram with Preload 83
Table 26 – Fields of Upload Initiate SSDO_Service_Request telegram 84
Table 27 – Fields of Upload Initiate SSDO_Service_Response telegram 84
Table 28 – Fields of Upload Segment SSDO_Service_Request telegram 85
Table 29 – Fields of Upload Segment SSDO_Service_Response telegram 86
Table 30 – Fields of Upload Initiate SSDO_Service_Request telegram with Preload 86
Table 31 – Fields of Upload Initiate SSDO_Service_Response telegram with Preload 87
Table 32 – Fields of Upload Segment SSDO_Service_Request telegram with PreLoad 88
Table 33 – Fields of Upload Segment SSDO_Service_Response telegram with Preload 88
Table 34 – Fields of SSDO Abort telegram 89
Table 35 – SSDO Abort codes 89

Documents
Document Sharing Hub
Full document details: DIN EN IEC 61784-3-13:2023-05

Table 36 – TR field usage for SSDO Preload 90
Table 37 – Bit fields inside TR field for SSDO Preload 91
Table 38 – SNMT telegram types (ID field, bits 2, 3 and 4) 91
Table 39 – Fields of SNMT_Request_UDID telegram 92
Table 40 – Fields of SNMT_Response_UDID telegram 93
Table 41 – Fields of SNMT_Assign_SADR telegram 93
Table 42 – Fields of SNMT_SADR_ Assigned telegram 94
Table 43 – Fields of SNMT_SN_reset_guarding_SCM telegram 95
Table 44 – SNMT request telegram types 95
Table 45 – SNMT response telegram types 95
Table 46 – Fields of SNMT_SN_set_to_PRE_OP telegram 96
Table 47 – Fields of SNMT_SN_status_PRE_OP telegram 96
Table 48 – Fields of SNMT_SN_set_to_OP telegram 97
Table 49 – Fields of SNMT_SN_status_OP telegram 98
Table 50 – Fields of SNMT_SN_busy telegram 98
Table 51 – Fields of SNMT_SN_FAIL telegram 98
Table 52 – SNMT_SN_FAIL Error Group values 99
Table 53 – SNMT_SN_FAIL Error Code values 99
Table 54 – SNMT_SN_FAIL Error Code values in case of Error Group Code 5 99
Table 55 – Fields of SNMT_SN_ACK telegram 100
Table 56 – Fields of SNMT_SCM_set_to_STOP telegram 100
Table 57 – Fields of SNMT_SCM_set_to_OP telegram 101
Table 58 – Fields of SNMT_SCM_guard_SN telegram 102
Table 59 – Fields of SNMT_SN_status_OP/SNMT_SN_status_OP telegrams 102
Table 60 – Fields of SNMT_assign_additional_SADR telegram 103
Table 61 – Fields of SNMT_assigned_additional_SADR telegram 103
Table 62 – Fields of SNMT_assign_UDID_of_SCM telegram 104
Table 63 – Fields of SNMT_assigned_UDID_of_SCM telegram 105
Table 64 – Fields of SNMT_assign_Init_CT telegram 105
Table 65 – Fields of SNMT_assigned_Init_CT telegram 106
Table 66 – Object type definition 107
Table 67 – Access attributes for data objects 108
Table 68 – SPDO mapping attributes for data objects 109
Table 69 – Basic data type object definition example 109
Table 70 – Compound data type object definition example 109
Table 71 – Sub index interpretation 110
Table 72 – NumberOfEntries sub index specification 110
Table 73 – RECORD type object sub index specification 111
Table 74 – ARRAY type object sub index specification 111

Documents
Document Sharing Hub

Full document details: DIN EN IEC 61784-3-13:2023-05

Table 75 – StructureOfObject encoding 112
Table 76 – Object dictionary data types 112
Table 77 – 0021h Compound data type description example 114
Table 78 – 0021h Compound sub index descriptions example 114
Table 79 – Standard objects 115
Table 80 – Common communication objects 115
Table 81 – Receive SPDO communication objects 115
Table 82 – Receive SPDO mapping objects 116
Table 83 – Transmit SPDO communication objects 116
Table 84 – User parameter (writeable at any time) 116
Table 85 – Transmit SPDO mapping objects 116
Table 86 – SADR DVI list 117
Table 87 – Additional SADR list 117
Table 88 – SADR UDID list 117
Table 89 – Additional parameter list 117
Table 90 – Object 1001h Error Register 118
Table 91 – Object 1001h Error Register value interpretation 118
Table 92 – Object 1002h Manufacturer status register 118
Table 93 – Object 1003h Pre defined error field 119
Table 94 – Object 1003h sub index 00h 119
Table 95 – Object 1003h sub index 01h 120
Table 96 – Object 1003h sub index 02h to FEh 120
Table 97 – Object 1003h Error statistics 120
Table 98 – Object 1004h sub index 00h 121
Table 99 – Object 1004h sub index 01h 121
Table 100 – Object 1004h sub index 02h 121
Table 101 – Object 1004h sub index 03h 122
Table 102 – Object 1004h sub index 04h 122
Table 103 – Object 1004h sub index 05h 122
Table 104 – Object 1004h sub index 06h 123
Table 105 – Object 1004h sub index 07h 123
Table 106 – Object 1004h sub index 08h 123
Table 107 – Object 1004h sub index 09h 124
Table 108 – Object 1004h sub index 0Ah 124
Table 109 – Object 1004h sub index 0Bh 124
Table 110 – Object 1004h sub index 0Ch 125
Table 111 – Object 1004h sub index 0Dh 125
Table 112 – Object 1004h sub index 0Eh 125
Table 113 – Object 100Ch Life Guarding 126

Documents
Document Sharing Hub
Full document details: DIN EN IEC 61784-3-13:2023-05

Table 114 – Object 100Ch sub index 00h 126
Table 115 – Object 100Ch sub index 01h 126
Table 116 – Object 100Ch sub index 02h 127
Table 117 – Object 100Dh Refresh Interval of Reset Guarding 127
Table 118 – Object 100Eh Number of Retries for Reset Guarding 128
Table 119 – Object 1018h Device Vendor Information 128
Table 120 – Object 1018h sub index 00h 129
Table 121 – Object 1018h sub index 01h 129
Table 122 – Object 1018h sub index 02h 129
Table 123 – Object 1018h sub index 03h 130
Table 124 – Object 1018h sub index 04h 130
Table 125 – Object 1018h sub index 05h 130
Table 126 – Object 1018h sub index 06h 131
Table 127 – Object 1018h sub index 07h 131
Table 128 – Object 1018h sub index 08h 131
Table 129 – Object 1018h sub index 09h 132
Table 130 – Structure of Revision Number 132
Table 131 – Structure of parameter checksum domain 132
Table 132 – CRC polynom for parameter checksum 133
Table 133 – Structure of Stack Version 133
Table 134 – Object 1019h Unique Device ID 134
Table 135 – Object 101Ah Parameter Download 134
Table 136 – Format of Parameter Download 134
Table 137 – Format of additional parameter header 135
Table 138 – Object 101Bh SCM Parameters 135
Table 139 – Object 101Bh sub index 00h 135
Table 140 – Object 101Bh sub index 01h 136
Table 141 – Object 1200h Common Communication Parameter 136
Table 142 – Object 1200h sub index 00h 136
Table 143 – Object 1200h sub index 01h 137
Table 144 – Object 1200h sub index 02h 137
Table 145 – Object 1200h sub index 03h 137
Table 146 – Object 1200h sub index 04h 138
Table 147 – Object 1201h SSDO Communication Parameter 138
Table 148 – Object 1201h sub index 00h 139
Table 149 – Object 1201h sub index 01h 139
Table 150 – Object 1201h sub index 02h 139
Table 151 – Object 1202h SNMT Communication Parameter 140
Table 152 – Object 1202h sub index 00h 140

Documents
Document Sharing Hub

Full document details: DIN EN IEC 61784-3-13:2023-05

Table 153 – Object 1202h sub index 01h 140
Table 154 – Object 1202h sub index 02h 141
Table 155 – Object 1400h – 17FEh RxSPDO Communication Parameter 141
Table 156 – Object 1400h – 17FEh sub index 00h 142
Table 157 – Object 1400h – 17FEh sub index 01h 142
Table 158 – Object 1400h – 17FEh sub index 02h 142
Table 159 – Object 1400h – 17FEh sub index 03h 143
Table 160 – Object 1400h – 17FEh sub index 04h 143
Table 161 – Object 1400h – 17FEh sub index 05h 143
Table 162 – Object 1400h – 17FEh sub index 06h 144
Table 163 – Object 1400h – 17FEh sub index 07h 144
Table 164 – Object 1400h – 17FEh sub index 08h 144
Table 165 – Object 1400h – 17FEh sub index 09h 145
Table 166 – Object 1400h – 17FEh sub index 0Ah 145
Table 167 – Object 1400h – 17FEh sub index 0Bh 146
Table 168 – Object 1400h – 17FEh sub index 0Ch 146
Table 169 – Object 1800h – 1BFEh RxSPDO communication parameter 147
Table 170 – Object 1800h – 1BFEh sub index 00h 147
Table 171 – Object 1800h – 1BFEh sub index 01h 147
Table 172 – Object 1800h – 1BFEh sub index 02h – FEh 147
Table 173 – 1Object C00h – 1FFEh TxSPDO communication parameter 148
Table 174 – Object 1C00h – 1FFEh sub index 00h 148
Table 175 – Object 1C00h – 1FFEh sub index 01h 148
Table 176 – Object 1C00h – 1FFEh sub index 02h 149
Table 177 – Object 1C00h – 1FFEh sub index 03h 149
Table 178 – Object C000h – C3FEh TxSPDO mapping parameter 150
Table 179 – Object C000h – C3FEh sub index 00h 150
Table 180 – Object C000h – C3FEh sub index 01h 150
Table 181 – Object C000h – C3FEh sub index 02h – FEh 151
Table 182 – Object C400h – C7FEh SADR-DVI list 151
Table 183 – Object C400h – C7FEh sub index 00h 152
Table 184 – Object C400h – C7FEh sub index 01h 152
Table 185 – Object C400h – C7FEh sub index 02h 152
Table 186 – Object C400h – C7FEh sub index 03h 153
Table 187 – Object C400h – C7FEh sub index 04h 153
Table 188 – Object C400h – C4FEh sub index 05h 153
Table 189 – Object C400h – C7FEh sub index 06h 154
Table 190 – Object C400h – C7FEh sub index 07h 154
Table 191 – Object C400h – C7FEh sub index 08h 154

Documents
Document Sharing Hub
Full document details: DIN EN IEC 61784-3-13:2023-05

Table 192 – Object C400h – C7FEh sub index 09h 155
Table 193 – Object C400h – C7FEh sub index 0Ah 155
Table 194 – Object C400h – C7FEh sub index 0Bh 155
Table 195 – Object C400h – C7FEh sub index 0Ch 156
Table 196 – Bit field of optional features 156
Table 197 – Object C400h – C7FEh sub index 0Dh 156
Table 198 – Object C400h – C7FEh sub index 0Eh 157
Table 199 – Object C400h – C7FEh sub index 0Fh 157
Table 200 – Object C801h – CBFFh Additional SADR list 157
Table 201 – Object C801h – CBFFh sub index 00h 158
Table 202 – Object C801h – CBFFh sub index 01h 158
Table 203 – Object C801h – CBFFh sub index 02h 158
Table 204 – Object Additional SADR List Example 159
Table 205 – Object CC01h – CFFFh SADR-UDID list 159
Table 206 – Object CC01h – CFFFh sub index 00h 160
Table 207 – Object CC01h – CFFFh sub index 01h – FEh 160
Table 208 – SADR-UDID List Example 160
Table 209 – Object E400h – E7FEh SSCM additional parameter list 161
Table 210 – Object E400h – E7FEh sub index 00h 161
Table 211 – Object E400h – E7FEh sub index 01h – 10h 161
Table 212 – Structure of SPDO mapping entry 163
Table 213 – Mapping example table 1 163
Table 214 – Mapping example table 2 164
Table 215 – Mapping example table 3 164
Table 216 – Mapping example table 4 164
Table 217 – Mapping example table 5 164
Table 218 – Mapping example table 6 165
Table 219 – Mapping example table 7 165
Table 220 – SPDO telegram features (TR field, bits 2-7) 166
Table 221 – SPDO communication producer item description 167
Table 222 – SPDO communication producer state description 168
Table 223 – SPDO communication consumer item description 169
Table 224 – SPDO communication consumer state description 169
Table 225 – SPDO communication consumer telegram validation item description 170
Table 226 – SPDO communication consumer telegram validation state description 171
Table 227 – Time synchronization item description 172
Table 228 – Time validation item description 175
Table 229 – Extended time synchronization item description 177
Table 230 – Time synchronization producer item description 179

Documents
Document Sharing Hub
Full document details: DIN EN IEC 61784-3-13:2023-05

Table 231 – Time synchronization producer state description 179
Table 232 – Time synchronization consumer item description 180
Table 233 – Time synchronization consumer state description 181
Table 234 – SSDO client item description 182
Table 235 – SSDO client state description 182
Table 236 – SSDO server state description 183
Table 237 – SOD access item description 184
Table 238 – Segmented SOD access client item description 186
Table 239 – Segmented SOD download access client state description 186
Table 240 – Segmented SOD access server item description 188
Table 241 – Segmented SOD access server state description 188
Table 242 – SOD preload download access client item description 190
Table 243 – SOD preload download access client state description 190
Table 244 – SOD preload download access server item description 192
Table 245 – SOD preload download access server state description 193
Table 246 – SNMT master item description 194
Table 247 – SNMT master state description 194
Table 248 – SNMT slave state description 195
Table 249 – SN power up state description 196
Table 250 – State and communication object relation 196
Table 251 – SN Pre-Operational state item description 199
Table 252 – SN Pre-Operational state description 199
Table 253 – SN additional parameter state description 202
Table 254 – SN Operational state item description 203
Table 255 – SN Operational state description 203
Table 256 – SCM power up state description 204
Table 257 – State and communication object relation 204
Table 258 – SCM Operational state item description 206
Table 259 – SCM Operational state description 206
Table 260 – Address verification item description 208
Table 261 – Address verification state description 208
Table 262 – SCM handle single UDID mismatch state description 209
Table 263 – SCM verify parameters state description 211
Table 264 – Activate SN state description 213
Table 265 – Residual error rate 217

Documents
Document Sharing Hub
Full document details: DIN EN IEC 61784-3-13:2023-05

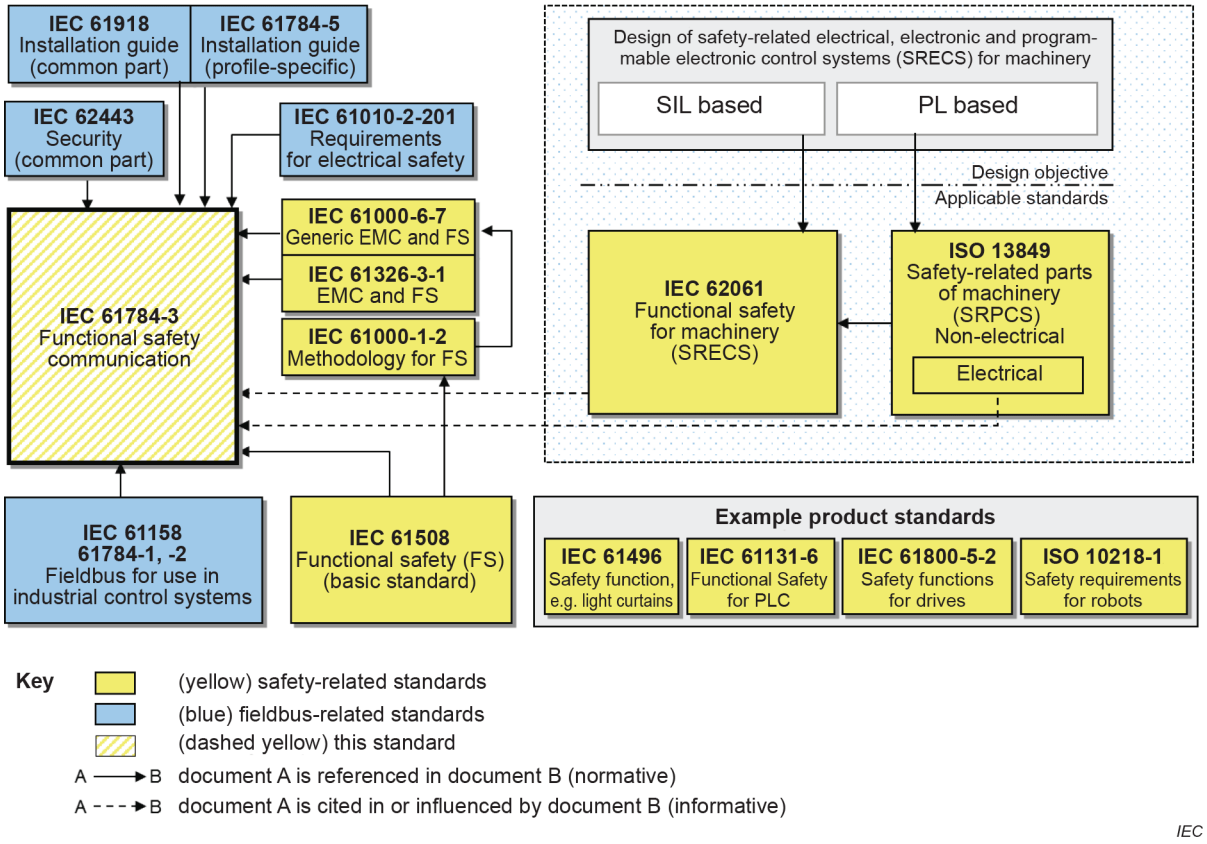
0 Introduction

0.1 General

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

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

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

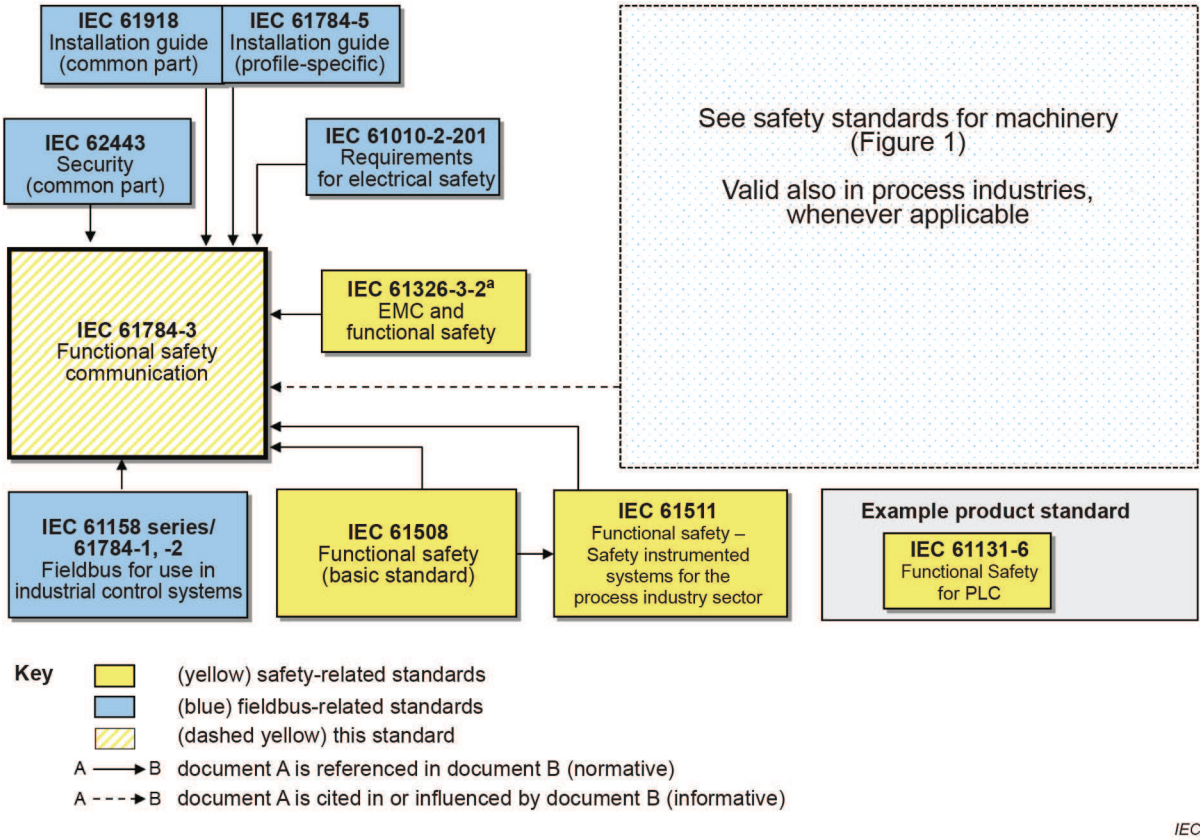


NOTE IEC 62061 specifies the relationship between PL (Category) and SIL.

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

Documents
Document Sharing Hub
Full document details: DIN EN IEC 61784-3-13:2023-05

Figure 2 shows the relationships between IEC 61784-3 (all parts) 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.

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

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

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

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

IEC 61784-3 (all parts) describes:

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

Documents
Document Sharing Hub
Full document details: DIN EN IEC 61784-3-13:2023-05

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

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

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

Documents
Document Sharing Hub

Full document details: DIN EN IEC 61784-3-13:2023-05

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES –

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

1 Scope

This part of IEC 61784-3 (all parts) 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 document defines mechanisms for the transmission of safety-relevant messages among participants within a distributed network using fieldbus technology in accordance with the requirements of IEC 61508 (all parts)[3] for functional safety. These mechanisms may be used in various industrial applications such as process control, manufacturing automation and machinery.

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

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

2 Normative references

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

IEC 61131-3, *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*

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

Documents
Document Sharing Hub
Full document details: DIN EN IEC 61784-3-13:2023-05

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

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

IEC 61784-5-13, *Industrial communication networks – Profiles – Part 5-13: Installation of fielbuses – 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 terms and definitions given in IEC 61784-3 and the following apply.

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

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

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

3.1.1 Common terms and definitions

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

3.1.1.1
bit error probability
Pe
probability for a given bit to be received with the incorrect value

3.1.1.2
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.

3.1.1.3
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]

3.1.1.4
communication channel
logical *connection* between two end-points within a *communication system*

3.1.1.5
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

Documents
Document Sharing Hub
Full document details: DIN EN IEC 61784-3-13:2023-05

3.1.1.6
connection
logical binding between two application objects within the same or different devices

3.1.1.7
Cyclic Redundancy Check
CRC
<value> redundant data derived from, and stored or transmitted together with, a block of data in order to detect data corruption
<method> procedure used to calculate the redundant data

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

Note 2 to entry: See also [31], [32][4].

3.1.1.8
defined communication system
defined channel
fixed number or fixed maximum number of participants linked by a fieldbus based communication system with well-known and fixed properties, such as installation conditions, electromagnetic immunity, industrial (active) network elements, and where the risk of unauthorized access is reduced to a tolerated level according to the lifecycle model of IEC 62443 (all parts), using for example zones and conduits

3.1.1.9
DLPDU
DEPRECATED: frame
Data Link Protocol Data Unit

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

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.

[4] Figures in square brackets refer to the bibliography.

Documents
Document Sharing Hub
Full document details: DIN EN IEC 61784-3-13:2023-05

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

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

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

3.1.1.16
hazard
potential source of harm

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

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

3.1.1.17
master
communication entity able to initiate and schedule communication activities by other stations which may be masters or slaves

3.1.1.18
message
<information theory and communication theory> ordered sequence of characters (usually octets) intended to convey information

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

3.1.1.19
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 13849-1:2015, 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
residual error rate
statistical rate at which the SCL *safety measures* fail to detect *errors*

3.1.1.22
risk
combination of the probability of occurrence of harm and the severity of that harm

Documents
Document Sharing Hub

Full document details: DIN EN IEC 61784-3-13:2023-05

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

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

3.1.1.23
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*.

3.1.1.24
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

3.1.1.25
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.

3.1.1.26
safety device
device designed in accordance with IEC 61508 and which implements the functional safety communication profile

3.1.1.27
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]

3.1.1.28
safety function response time
worst case elapsed time following an actuation of a safety sensor connected to a *fieldbus*, until the corresponding safe state of its safety actuator(s) is achieved in the presence of *errors* or *failures* in the *safety function*

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

3.1.1.29
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]

AVA Documents
Document Sharing Hub

Full document details: DIN EN IEC 61784-3-13:2023-05

3.1.1.30
safety measure
measure to control possible communication *errors* that is designed and implemented in compliance with the requirements of IEC 61508

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

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

3.1.1.31
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*.

3.1.1.32
safety-related application
programs designed in accordance with IEC 61508 to meet the SIL requirements of the application

3.1.1.33
safety-related system
system performing *safety functions* according to IEC 61508

3.1.1.34
slave
communication entity able to receive *messages* and send them in response to another communication entity which may be a *master* or a slave, but not to initiate communication activities

3.1.1.35
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*

3.1.1.3
Safety Address
SADR
address of a *safety node* within a *safety domain*

3.1.1.4
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.

Documents
Document Sharing Hub
Full document details: DIN EN IEC 61784-3-13:2023-05

3.1.1.5
Safety Node
SN
node with *safety function*

3.1.1.6
Safety Domain
SD
address space for up to 1 023 *safety nodes*

3.1.1.7
Safety Domain Gateway
SDG
gateway to share data between different *safety domains*

3.1.1.8
Safety Domain Number
SDN
identification of a *safety domain*

3.1.1.9
Safety Network Management
SNMT
services for safety layer management

3.1.1.10
Safety Object Dictionary
SOD
repository of all data objects accessible using services of the functional safety *fieldbus*

3.1.1.11
Safety Process Data Object
SPDO
object for process data exchange between different *safety nodes*

3.1.1.12
Safety Service Data Object
SSDO
object for service data exchange between *safety nodes*

3.1.1.13
initialization
initial *safety node* communication state

3.1.1.14
operational
safety node communication state where all functional safety functions are working properly

3.1.1.15
pre-operational
safety node communication state where all application outputs are in safe state

3.1.1.16
Unique Device Identification
UDID
worldwide unique identification of a device

Documents
Document Sharing Hub
Full document details: DIN EN IEC 61784-3-13:2023-05

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 (all parts)]
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	

Documents
Document Sharing Hub
Full document details: DIN EN IEC 61784-3-13:2023-05

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 document 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

Documents
Document Sharing Hub
Full document details: DIN EN IEC 61784-3-13:2023-05

3.3.2 Binary values

Some values within this document 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 document 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 document.

4.2 Technical overview

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

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 uses the client server model (see Figure 4).

---

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 document and does not constitute an endorsement by IEC of the trade name holder or any of its products. Compliance to this document does not require use of the trade names 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).

Documents
Document Sharing Hub
Full document details: DIN EN IEC 61784-3-13:2023-05

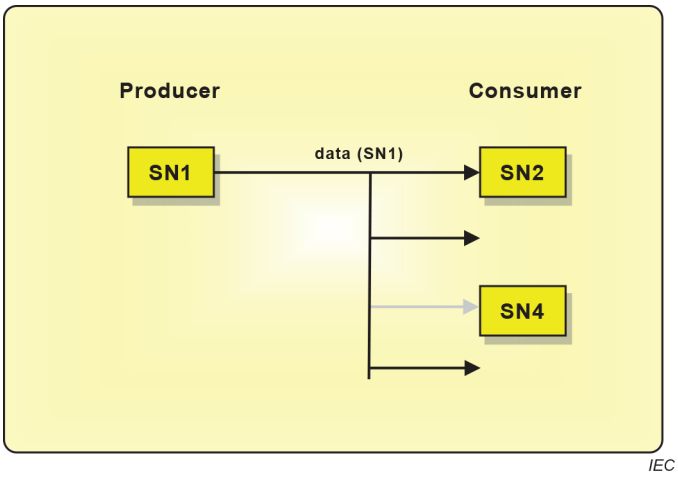


Figure 3 – Producer consumer example

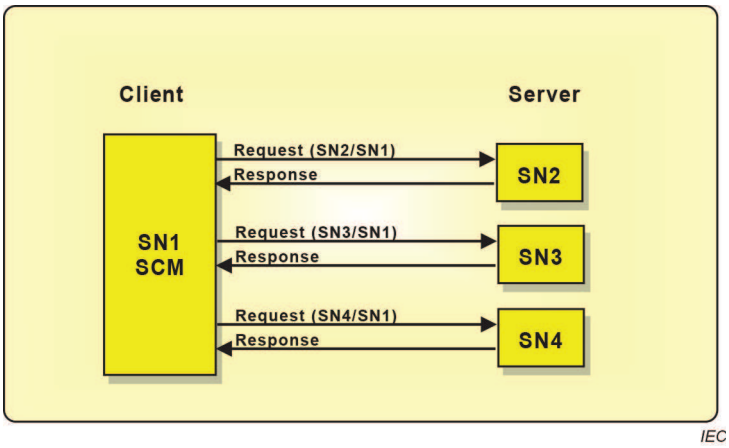


Figure 4 – Client server example

5 General

5.1 External documents providing specifications for the profile

The documents [38] and [39] 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 document,

Documents
Document Sharing Hub
Full document details: DIN EN IEC 61784-3-13:2023-05

- 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 document, 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.

Documents
Document Sharing Hub
Full document details: DIN EN IEC 61784-3-13:2023-05

Table 2 – Communication errors and detection measures (acyclic)

Communication errors	Safety measures							
	Sequence number	Time stamp	Time expectation	Connection authentication	Feedback message[e]	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 SCT_U32, Table 158), 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.

Documents
Document Sharing Hub
Full document details: DIN EN IEC 61784-3-13:2023-05

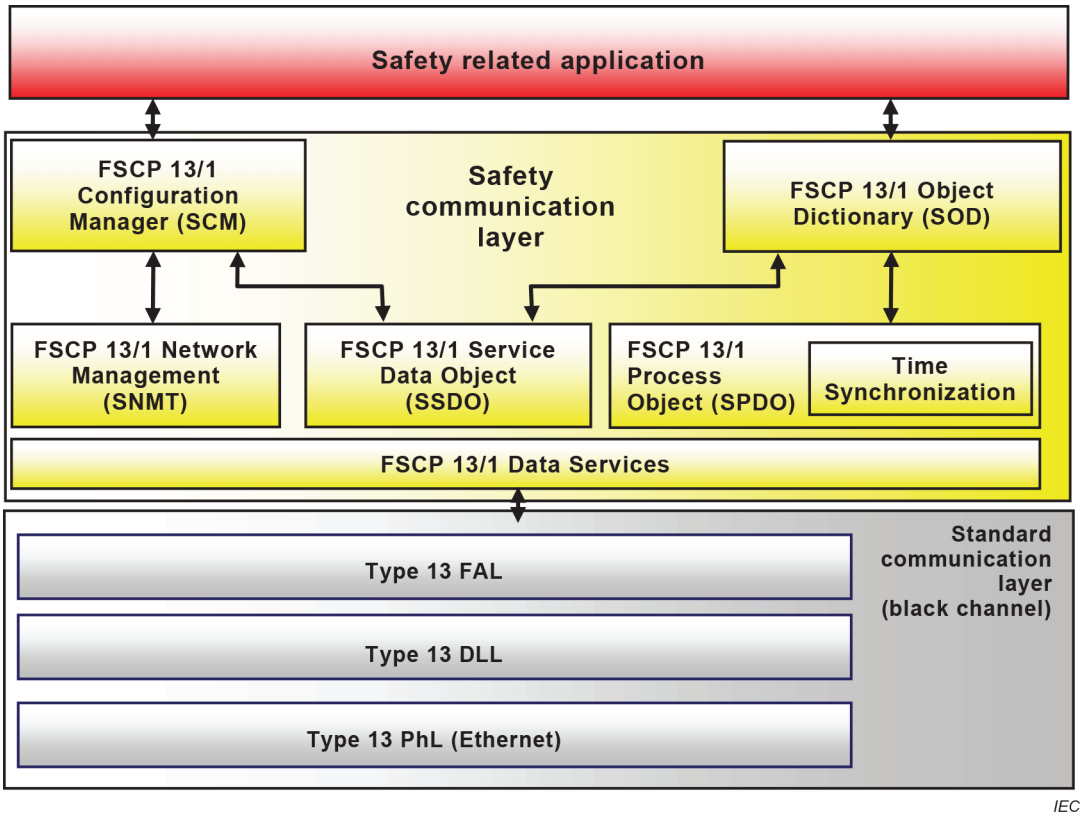


Figure 5 – Communication layer structure

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).

Documents
Document Sharing Hub
Full document details: DIN EN IEC 61784-3-13:2023-05