DIN EN IEC 61784-3-2

ICS 35.160; 35.240.50

Ersatz für
DIN EN 61784-3-2:2018-09
Siehe Anwendungsbeginn

Industrielle Kommunikationsnetze – Profile – Teil 3-2: Funktional sichere Übertragung bei Feldbussen – Zusätzliche Festlegungen für die Kommunikationsprofilfamilie 2 (IEC 61784-3-2:2021); Englische Fassung EN IEC 61784-3-2:2021

Industrial communication networks –
Profiles –
Part 3-2: Functional safety fieldbuses – Additional specifications for CPF 2
(IEC 61784-3-2:2021);
English version EN IEC 61784-3-2:2021

Réseaux de communication industriels –
Profils –
Partie 3-2: Bus de terrain de sécurité fonctionnelle –
Spécifications supplémentaires pour CPF 2
(IEC 61784-3-2:2021);
Version anglaise EN IEC 61784-3-2:2021

Gesamtumfang 293 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE

Documents
Document Sharing Hub

Full document details: DIN EN IEC 61784-3-2:2023-04

Anwendungsbeginn

Anwendungsbeginn für die von CENELEC am 2021-06-23 angenommene Europäische Norm als DIN-Norm ist 2023-04-01.

Für DIN EN 61784-3-2:2018-09 besteht eine Übergangsfrist bis 2024-06-23.

Nationales Vorwort

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

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.

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

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

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 61784-3-2 veröffentlicht. Zu deren Abschnitt 0, der die Einleitung festlegt, Abschnitt 1, der den Anwendungsbereich festlegt, und Abschnitt 3, der die Begriffe, Abkürzungen und Konventionen festlegt, wurde eine Übersetzung angefertigt und als informativer Nationaler Anhang NA der vorliegenden Norm hinzugefügt. Für einige der verwendeten Begriffe existieren keine gebräuchlichen deutschen Benennungen, da sich die deutschen Anwender in der Regel ebenfalls der englischen Benennungen bedienen. Diese Norm steht nicht in unmittelbarem Zusammenhang mit Rechtsvorschriften und ist nicht als Sicherheitsnorm anzusehen.

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

Documents
Document Sharing Hub

Full document details: DIN EN IEC 61784-3-2:2023-04

Änderungen

Gegenüber DIN EN 61784-3-2:2018-09 wurden folgende Änderungen vorgenommen:

a) Hinzufügung von zwei neuen Safety Supervisor Objektzuständen in 6.6.5.5;
b) Hinzufügung der Anforderung an das Verhalten der Net-LED für den vorschlagenden TUNID-Prozess in 6.6.8, 9.1.2 und 9.1.5;
c) Hinzufügung der Unterstützung von Anwendungspfaden für Prozessvariablen in 6.3.9 und 6.3.10;
d) Hinzufügung der Unterstützung von Mehrportgeräten in 6.6.4, 6.6.5, 6.6.7 und an verschiedenen Stellen;
e) Korrektur der Netzreaktionszeit 56 Gleichungen in 9.3.3;
f) Ergänzung der SIL-Unterstützung bis SIL 3 in 7.6, 8.7, 8.9, 9.5 und diversen Stellen;
g) Bereinigung der Leitlinien für das Konfigurationsverfahren in 8.9.14 und 8.9.15;
h) Erkennung von Schalteränderungen in 9.1.6;
i) Ablehnung des Basisformats in 3.1.2, 7.1.1.1 und 6.3.3.2;
j) Festsetzung des Wertes Max_Fault_Number auf 2 in 6.3.3.4, 6.8.3 und 8.8.3;
k) Aktualisierung der PFH-Berechnung des Netzes in 9.5.2;
l) diverse kleinere Korrekturen seit der letzten Veröffentlichung.

Frühere Ausgaben

DIN EN 61784-3-2: 2008-11, 2012-03, 2018-09

Documents
Document Sharing Hub
Full document details: DIN EN IEC 61784-3-2:2023-04

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

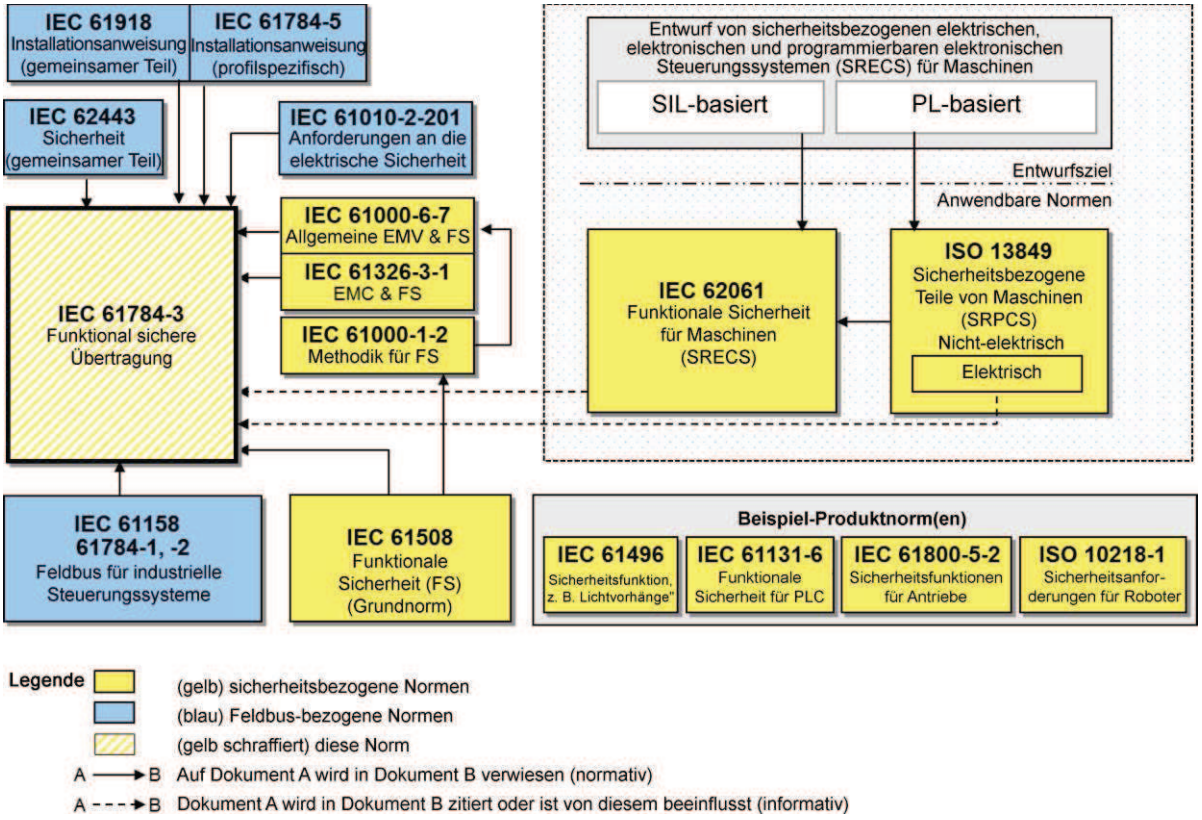
Die Feldbusnorm IEC 61158 (alle Teile) und ihre Begleitnormen IEC 61784-1 und IEC 61784-2 spezifizieren zusammen mehrere Kommunikationsprotokolle, die die dezentrale Automatisierung von Applikationen ermöglichen. Die Feldbustechnologie hat sich inzwischen in der Praxis bewährt und ist in hohem Maße akzeptiert. 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.

AVA Documents
Document Sharing Hub

Full document details: DIN EN IEC 61784-3-2:2023-04

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

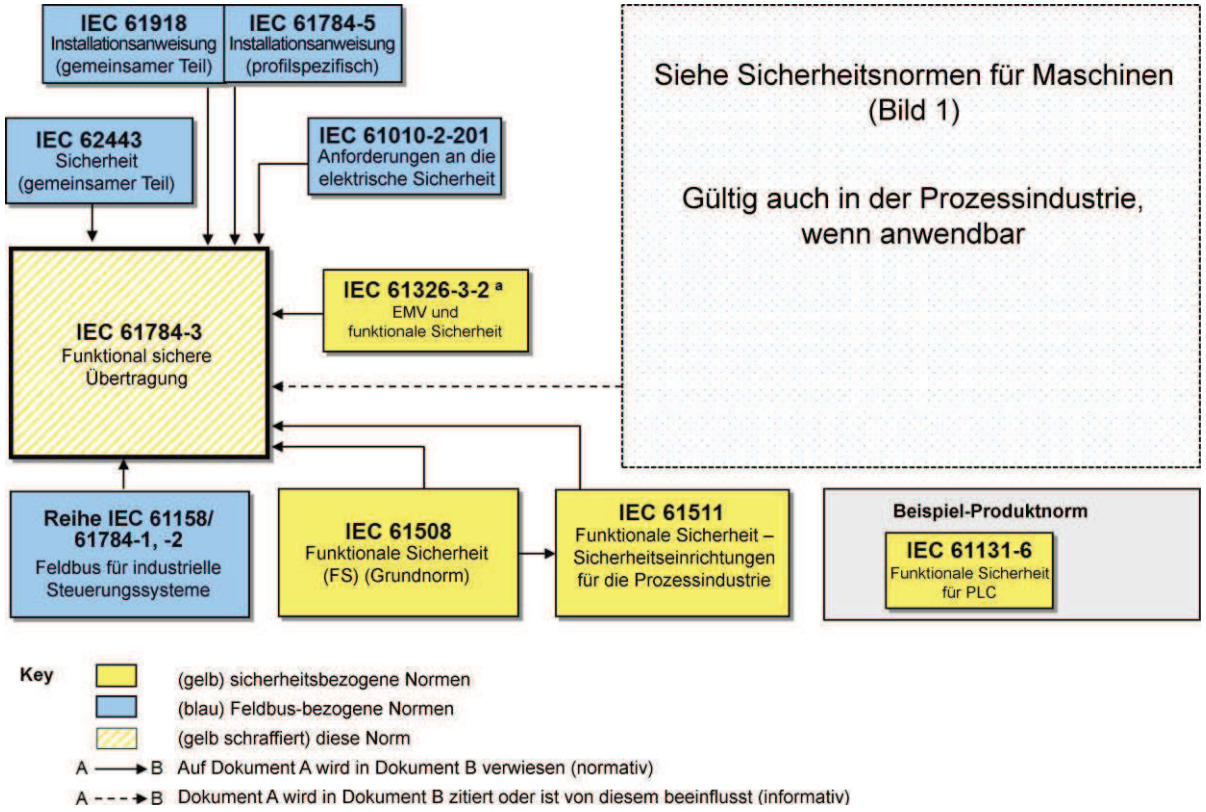


ANMERKUNG IEC 62061 beschreibt das Verhältnis zwischen PL (Kategorie) und SIL.

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

Documents
Document Sharing Hub
Full document details: DIN EN IEC 61784-3-2:2023-04

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



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

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

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

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

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

Documents
Document Sharing Hub
Full document details: DIN EN IEC 61784-3-2:2023-04

IEC 61784-3 (alle Teile) beschreibt:

- grundlegende Prinzipien für die Erfüllung der Anforderungen von IEC 61508 (alle Teile) für die funktional sichere Kommunikation, einschließlich möglicher Übertragungsfehler, deren Abhilfemaßnahmen und Betrachtungen zur Datenintegrität;
- funktional sichere Kommunikationsprofile für mehrere Kommunikationsprofilfamilien der IEC 61784-1 und IEC 61784-2, welche Ergänzungen der Kommunikationsdienst- und -protokollabschnitte von IEC 61158 (alle Teile) um eine Sicherheitsschicht enthalten.

0.2 Patentangaben

Die Organisation International Electrotechnical Commission (IEC) weist auf Ansprüche hin, die es für eine Übereinstimmung mit diesem Dokument notwendig machen, von Patenten Gebrauch zu machen. Dies betrifft funktional sichere Kommunikationsprofile für die Familie 2. 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 erhältlich aus der Patentdatenbank unter http://patents.iec.ch.

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

AVA Documents
Document Sharing Hub

Full document details: DIN EN IEC 61784-3-2:2023-04

1 Anwendungsbereich

Dieser Teil von IEC 61784-3 (alle Teile) legt eine Sicherheitskommunikationsschicht (Dienste und Protokoll) auf der Basis von CPF 2 in IEC 61784-1, IEC 61784-2 und IEC 61158 Typ 2 fest. Sie stellt die Grundsätze der funktional sicheren Kommunikation nach IEC 61784-3 fest, die für diese Sicherheitskommunikationsschicht wichtig sind. Diese Sicherheitskommunikationsschicht ist für die ausschließliche Implementierung in Sicherheitsgeräten vorgesehen.

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

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

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

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

3 Begriffe, Symbole, Abkürzungen und Konventionen

3.1 Begriffe

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

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

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

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

3.1.1 Allgemeine Begriffe

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

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

3.1.1.2
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.

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

Documents
Document Sharing Hub
Full document details: DIN EN IEC 61784-3-2:2023-04

3.1.1.3
Bridge
abstraktes Gerät, welches auf der Ebene der Sicherungsschicht mehrere Netzwerksegmente verbindet

3.1.1.4
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]

3.1.1.5
Kommunikationskanal
en **communication channel**
logische *Verbindung* zwischen zwei Endpunkten in einem *Kommunikationssystem*

3.1.1.6
Kommunikationssystem
en **communication system**
Anordnung von Hardware, Software und Ausbreitungsmedien zur Übertragung von Nachrichten (ISO/IEC 7498-1-Anwendungsschicht) von einer Anwendung zur anderen

3.1.1.7
Verbindung
en **connection**
logische Verbindung zwischen zwei Anwendungsobjekten in demselben oder in unterschiedlichen Geräten

3.1.1.8
zyklische Redundanzprüfung
CRC
en **cyclic redundancy check**
<Wert> redundante Daten, abgeleitet von einem Block von Daten und mit diesen zusammen gespeichert oder übertragen zur Aufdeckung von Datenverfälschungen;
<Methode> Prozedur zur Berechnung der redundanten Daten

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

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

3.1.1.9
festgelegtes Kommunikationssystem
en **defined communication system**
en **defined channel**
festgelegte Anzahl oder festgelegte maximale Anzahl von Teilnehmern, die über ein *Kommunikationssystem* verbunden sind, mit wohldefinierten und festgelegten Eigenschaften wie beispielsweise Aufbaubedingungen, elektromagnetische Störfestigkeit, industrielle *(aktive) Netzwerkkomponenten* und wo das *Risiko* eines unerlaubten Zugriffs gemäß Lebenszyklusmodell der IEC 62443 (alle Teile) auf ein toleriertes Maß reduziert ist durch zum Beispiel Zonen und Durchleitungen

3.1.1.10
Gerät
en **device**
an den Feldbus angeschlossene physische Instanz, die aus einem Datenübermittlungselement und möglicherweise anderen funktionalen Elementen besteht

[QUELLE: IEC 61158-2:2014, 3.1.13, modifiziert – Anmerkung zum Begriff und einige Einzelheiten wurden gestrichen.]

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

Documents
Document Sharing Hub
Full document details: DIN EN IEC 61784-3-2:2023-04

3.1.1.11
DLPDU
en **Data Link Protocol Data Unit**
ABGELEHNT: frame
Data Link Protocol Data Unit

3.1.1.12
Abweichung
en **error**
Nichtübereinstimmung zwischen Rechenergebnissen, beobachteten oder gemessenen Werten oder Beschaffenheiten und den betreffenden wahren, spezifizierten oder theoretisch richtigen Werten oder Beschaffenheiten

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

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

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

3.1.1.13
Ausfall
Versagen
en **failure**
Beendigung der Fähigkeit einer Funktionseinheit, eine geforderte Funktion auszuführen, oder Betrieb einer Funktionseinheit in irgendeiner Art anders als gefordert

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

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

3.1.1.14
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 „Fehler“ als einen Zustand, der durch das Unvermögen gekennzeichnet ist, eine geforderte Funktion auszuführen, jedoch nicht ein Unvermögen während vorbeugender Instandhaltung, anderer geplanter Aktionen oder auf Grund fehlender externer Betriebsmittel.

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

3.1.1.15
Feldbus
en **fieldbus**
Kommunikationssystem basierend auf serieller Datenübertragung und eingesetzt in der industriellen Automatisierung oder in Prozessleitsystemen

3.1.1.16
funktional sicheres Kommunikationsprofil
FSCP
en **functional safety communication profile**
Technikspezifikation für die Implementierung eines SCL

3.1.1.17
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.

AVA Documents
Document Sharing Hub

Full document details: DIN EN IEC 61784-3-2:2023-04

3.1.1.18
Gefährdung
en **hazard**
potentielle Schadensquelle

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

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

3.1.1.19
Master
Kommunikationseinheit, die Kommunikationsaktivitäten anderer Stationen, seien es Master oder Slaves, einleiten und planen kann

3.1.1.20
Nachricht
en **message**
<Informationstheorie und Kommunikationstheorie> geordnete Zeichenfolge (in der Regel in Oktetten), die zur Beförderung von Informationen vorgesehen ist

[QUELLE: ISO/IEC 2382:2015, 2123205, modifiziert – „(in der Regel in Oktetten)“ wurde eingefügt, Anmerkungen und Quelle wurden gestrichen]

3.1.1.21
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]

3.1.1.22
Redundanz
en **redundancy**
das Vorhandensein von mehr als einem Mittel zum Ausführen einer geforderten Funktion oder zur Darstellung von Informationen

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

3.1.1.23
Restfehlerrate
en **residual error rate**
statistische Rate, mit der die *Sicherheitsmaßnahmen* im SCL *Fehler* nicht aufdecken

3.1.1.24
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]

3.1.1.25
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.

Documents
Document Sharing Hub
Full document details: DIN EN IEC 61784-3-2:2023-04

3.1.1.26
Sicherheitskommunikationsschicht
SCL
en **safety communication layer**
Kommunikationsschicht über dem FAL, die die notwendigen zusätzlichen Mittel beinhaltet, um die sichere Übertragung von Daten entsprechend den Anforderungen der IEC 61508 zu gewährleisten

3.1.1.27
sichere Verbindung
en **safety connection**
Verbindung, welche das Sicherheitsprotokoll für Kommunikationstätigkeiten nutzt

3.1.1.28
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.

3.1.1.29
Sicherheitsgerät
en **safety device**
Gerät, welches nach IEC 61508 ausgeführt wurde und das funktional sichere Kommunikationsprofil zur Anwendung bringt

3.1.1.30
Sicherheitsfunktion
en **safety function**
Funktion, die von einem sicherheitsbezogenen E/E/PE-System oder anderen risikomindernden Maßnahmen ausgeführt wird, und dazu vorgesehen ist, unter Berücksichtigung eines festgelegten gefährlichen Vorfalls einen sicheren Zustand für die EUC zu erreichen oder aufrechtzuerhalten

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

3.1.1.31
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.

3.1.1.32
Sicherheits-Integritätslevel
SIL
en **safety integrity level**
eine von vier diskreten Stufen, die einem Wertebereich der Sicherheitsintegrität entsprechen, wobei der Sicherheits-Integritätslevel 4 die höchste Stufe der Sicherheitsintegrität und der Sicherheits-Integritätslevel 1 die niedrigste darstellt

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

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

Documents
Document Sharing Hub
Full document details: DIN EN IEC 61784-3-2:2023-04

Anmerkung 3 zum Begriff: Ein Sicherheits-Integritätslevel (SIL) ist keine Eigenschaft eines Systems, Teilsystems, Elements oder Bauteils. Die korrekte Deutung der Redensart „*sicherheitsbezogenes System* mit SIL n“ (wobei n 1, 2, 3 oder 4 ist) ist, dass das System möglicherweise fähig ist, *Sicherheitsfunktionen* mit einem Sicherheits-Integritätslevel bis zu n zu unterstützen.

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

3.1.1.33
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.

3.1.1.34
Sicherheits-PDU
SPDU
en **safety PDU**
durch einen Sicherheitskommunikationskanal übertragene PDU

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

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

3.1.1.35
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

3.1.1.36
sicherheitsbezogenes System
en **safety-related system**
System, welches *Sicherheitsfunktionen* nach IEC 61508 ausführt

3.1.1.37
Slave
Kommunikationseinheit, die Nachrichten empfangen und sie als Antwort an andere Kommunikationseinheiten senden kann, die Master oder Slave sein können, aber nicht zum Einrichten von Kommunikationsaktivitäten dient

3.1.1.38
unberechtigte Auslösung
en **spurious trip**
Auslösung in einem Sicherheitssystem ohne Prozessanforderung

3.1.1.39
Zeitstempel
en **time stamp**
Zeitinformation in einer *Nachricht*

AVA Documents
Document Sharing Hub

3.1.2 CPF 2: Zusätzliche Begriffe

3.1.2.1
Basisformat
en **base format**
Format, das für Verbindungs-RPIs von kleiner als 100 ms oder für Anwendungen, bei denen unterbrochene Verbindungen toleriert werden, verwendet wird

3.1.2.2
ablehnen
en **deprecate**
Maßnahme, mit der die offizielle Unterstützung für etwas (z. B. ein Softwareprodukt) zugunsten einer neueren oder besseren Alternative zurückgezogen oder von dessen Verwendung abgeraten wird

3.1.2.3
erweitertes Format
en **extended format**
Format, das für Verbindungs-RPIs von größer als 100 ms oder für Anwendungen, bei denen unterbrochene Verbindungen dringend vermieden werden müssen, verwendet wird

3.1.2.4
Ping
Anforderung an den Verbraucher, den Empfang einer Nachricht zu bestätigen

3.1.2.5
Ping-Antwort
en **ping response**
Antwort auf einen Ping

3.1.2.6
Urheber
en **originator**
Knoten, der die Herstellung einer Verbindung anfordert

3.1.2.7
Signatur
en **signature**
Verfahren zur eindeutigen Identifizierung einer Datenmenge

Anmerkung 1 zum Begriff: Dies könnte durch Verfahren wie Änderung, Quersumme, oder andere Verfahren, die von den versendenden und Zielgeräten vereinbart wurden, umgesetzt werden.

3.1.2.8
Gerät mit einzelnem Sicherheitsanschluss
en **single safety port device**
Urheber-, Ziel- oder gemischtes Urheber-/Zielgerät, das Sicherheitskommunikation über einen einzigen Sicherheitsanschluss durchführt

3.1.2.9
systematische Eignung
en **systematic capability**
Maß des Vertrauens (ausgedrückt auf einer Skala von SC 1 bis SC 4), dass die systematische Sicherheitsintegrität eines Elements den Anforderungen des festgelegten SILs hinsichtlich der festgelegten Element-Sicherheitsfunktion entspricht, wenn das Element in Übereinstimmung mit den im Sicherheitshandbuch für konforme Objekte für das Element festgelegten Anweisungen angewendet wird

[QUELLE: IEC 61508-4:2010, 3.5.9, modifiziert – Anmerkungen wurden entfernt]

Documents
Document Sharing Hub
Full document details: DIN EN IEC 61784-3-2:2023-04

3.1.2.10
systematische Sicherheitsintegrität
en **systematic safety integrity**
Teil der Sicherheitsintegrität eines sicherheitsbezogenen Systems, der sich auf systematische Ausfälle mit gefahrbringender Ausfallart bezieht

[QUELLE: IEC 61508-4:2010, 3.5.6, modifiziert – Anmerkung entfernt]

3.1.2.11
Ziel
en **target**
Knoten, der eine Anforderung zur Herstellung einer Verbindung empfängt

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)	
EMC	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]
PFD	mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung (en: Probability of dangerous Failure on Demand)	[IEC 61508-4:2010]
PFH	mittlere Häufigkeit eines gefahrbringenden Ausfalls je Stunde [h^{-1}]	[IEC 61508-4:2010]
PhL	Bitübertragungsschicht (en: Physical Layer)	[ISO/IEC 7498-1]
PL	Performance Level	[ISO 13849-1]
PLC	speicherprogrammierbare Steuerung (en: Programmable Logic Controller)	
SCL	Sicherheitskommunikationsschicht (en: Safety Communication Layer)	
SIL	Sicherheits-Integritätslevel (en: safety integrity level)	[IEC 61508-4:2010]

Documents
Document Sharing Hub
Full document details: DIN EN IEC 61784-3-2:2023-04

3.2.2 CPF 2: Zusätzliche Symbole und Abkürzungen

AIRS	Bereits im angeforderten Modus/Zustand (en: already in requested mode/state)
BER	Bitfehlerquote (en: bit error rate)
BF	Basisformat (en: base format)
CCO	Verbindungskonfigurationsobjekt (en: connection configuration object)
CFUNID	Konfigurations-UNID (en: configuration UNID)
CNP	Verbindungspunkt (en: connection point)
CID	Verbraucher-ID (en: consumer ID)
CIP™[3)]	Common Industrial Protocol (Anwendungs-Framework, das von den CPF-2-Kommunikationsprofilen gemeinsam genutzt wird)
CPCRC	Verbindungsparameter-CRC
CTM	Multiplikator der Verbindungszeitüberschreitung (en: connection timeout multiplier)
EDS	elektronisches Datenblatt (en: electronic data sheet)
EF	erweitertes Format (en: extended format)
EPI	erwartetes Paketintervall (en: expected packet interval)
LED	lichtemittierende Diode
MACID	Physikalische Adresse des Geräts (CP 2/3)
MOD	Modul
NodeID	Für CP 2/3-Sicherheitsgeräte ist dies die MACID des Geräts im Netzwerk. Für CP 2/2-Sicherheitsgeräte ist dies die IP-Adresse des Geräts im Netzwerk. Für CP 16/3-Sicherheitsgeräte ist dies die SDID des Geräts im Netzwerk.
NV	nichtflüchtig (en: non-volatile)
NVS	nichtflüchtiger Speicher (en: non-volatile storage)
OCPUNID	Eigner-UNID der Ausgangsverbindung (output connection owner UNID)
OSC	Objektstatuskonflikt (en: object status conflict)
O-to-T	Urheber-zu-Ziel (en: originator to target)
OUNID	Urheber-UNID (en: originator UNID)
PID	Erzeugerkennung (en: producer identifier)
PS	Energieversorgung (en: power supply)
Res.	reserviert (en: reserved)
RPI	angefordertes Paketintervall (en: requested packet interval)
SCCRC	Sicherheitskonfigurationsdaten-CRC (en: safety configuration data CRC)
SCID	Identifizierte Sicherheitskonfiguration (en: safety configuration identified)
SCTS	Zeitstempel der Sicherheitskonfiguration (en: safety configuration time stamp)
SNCT	Sicherheitsnetzwerkkonfigurationswerkzeug (en: safety network configuration tool)
SNN	Sicherheitsnetzwerknummer (en: safety network number)
T-to-O	Ziel-zu-Urheber (en: target-to-originator)
TBD	festzulegen (en: to be defined)
TNS	TUNID nicht gesetzt (en: TUNID not set)

[3] Zur Angabe von Handelsnamen siehe Abschnitt 4.

Documents
Document Sharing Hub
Full document details: DIN EN IEC 61784-3-2:2023-04

TUNID	Ziel-UNID (en: target TUNID)	
UML	Universal Modeling Language	[ISO/IEC 19501]
UNID	eindeutige Netzwerkkennung (en: unique network identifier)	

3.3 Konventionen

Die Konventionen für die Beschreibung von Objekten, Diensten und Protokollen sind in IEC 61158-3-2, IEC 61158-4-2, IEC 61158-5-2 und IEC 61158-6-2 beschrieben.

Wie angemessen verwendet dieses Dokument Flussdiagramme, UML-Sequenzdiagramme und „C“ Pseudo-Code, um Konzepte zu beschreiben.

Documents
Document Sharing Hub
Full document details: DIN EN IEC 61784-3-2:2023-04

– Leerseite –

Documents
Document Sharing Hub

Full document details: DIN EN IEC 61784-3-2:2023-04

EUROPEAN STANDARD

NORME EUROPÉENE

EUROPÄISCHE NORM

EN IEC 61784-3-2

June 2021

ICS 25.040.40; 35.100.05

Supersedes EN 61784-3-2:2017 and all of its amendments and corrigenda (if any)

English version

Industrial communication networks – Profiles – Part 3-2: Functional safety fieldbuses – Additional specifications for CPF 2 (IEC 61784-3-2:2021)

Réseaux de communication industriels – Profils – Partie 3-2: Bus de terrain de sécurité fonctionnelle – Spécifications supplémentaires pour CPF 2 (IEC 61784-3-2:2021)

Industrielle Kommunikationsnetze – Profile – Teil 3-2: Funktional sichere Übertragung bei Feldbussen – Zusätzliche Festlegungen für die Kommunikationsprofilfamilie 2 (IEC 61784-3-2:2021)

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 61784-3-2:2023-04

European foreword

The text of document 65C/1083/FDIS, future edition 4 of IEC 61784-3-2, 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 61784-3-2:2021.

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 61784-3-2:2017 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 61784-3-2:2021 was approved by CENELEC as a European Standard without any modification.

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

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

Documents
Document Sharing Hub
Full document details: DIN EN IEC 61784-3-2:2023-04

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 61131-2	-	Industrial-process measurement and control - Programmable controllers - Part 2: Equipment requirements and tests	-	-
IEC 61131-3	-	Programmable controllers - Part 3: Programming languages	EN 61131-3	-
IEC 61158-2	2014	Industrial communication networks - Fieldbus specifications - Part 2: Physical layer specification and service definition	EN 61158-2	2014
IEC 61158-3-2	-	Industrial communication networks - Fieldbus specifications - Part 3-2: Data-lonk layer service definition - Type 2 elements	EN 61158-3-2	-
IEC 61158-3-19	-	Industrial communication networks - Fieldbus specifications - Part 3-19: Data-link layer service definition - Type 19 elements	EN IEC 61158-3-19	-
IEC 61158-4-2	2019	Industrial communication networks - Fieldbus specifications - Part 4-2: Data-link layer protocol specification - Type 2 elements	EN IEC 61158-4-2	2019
IEC 61158-4-19	-	Industrial communication networks - Fieldbus specifications - Part 4 -19: Data-link layer protocol specification - Type 19 elements	EN IEC 61158-4-19	-
IEC 61158-5-2	-	Industrial communication networks - Fieldbus specifications - Part 5-2: Application layer service definition - Type 2 elements	EN IEC 61158-5-2	-
IEC 61158-5-19	-	Industrial communication networks - Fieldbus specifications - Part 5-19: Application layer service definition - Type 19 elements	EN IEC 61158-5-19	-
IEC 61158-6-2	-	Industrial communication networks - Fieldbus specifications - Part 6-2: Application layer protocol specification - Type 2 elements	EN IEC 61158-6-2	-
IEC 61158-6-19	-	Industrial communication networks - Fieldbus specifications - Part 6-19: Application layer protocol specification - Type 19 elements	EN IEC 61158-6-19	-

Documents
Document Sharing Hub
Full document details: DIN EN IEC 61784-3-2:2023-04

Publication	Year	Title	EN/HD	Year
IEC 61326-3-1	-	Electrical equipment for measurement, control and laboratory use - EMC requirements - Part 3-1: Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety) - General industrial applications	EN 61326-3-1	-
IEC 61326-3-2	-	Electrical equipment for measurement, control and laboratory use - EMC requirements - Part 3-2: Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety) - Industrial applications with specified electromagnetic environment	EN IEC 61326-3-2	-
IEC 61508	series	Functional safety of electrical/electronic/programmable electronic safety-related systems	EN 61508	series
IEC 61784-1	-	Industrial communication networks - Profiles Part 1: Fieldbus profiles	EN IEC 61784-1	-
IEC 61784-2	-	Industrial communication networks - Profiles - Part 2: Additional fieldbus profiles for real-time networks based on ISO/IEC/IEEE 8802-3	EN IEC 61784-2	-
IEC 61784-3	2021	Industrial communication networks - Profiles - Part 3: Functional safety fieldbuses - General rules and profile definitions	EN IEC 61784-3	2021
IEC 61784-5-2	-	Industrial communication networks - Profiles - Part 5-2: Installation of fieldbuses - Installation profiles for CPF 2	EN IEC 61784-5-2	-
IEC 61918	-	Industrial communication networks - Installation of communication networks in industrial premises	EN IEC 61918	-
IEC 62026-3	-	Low-voltage switchgear and controlgear - Controller-device interfaces (CDIs) - Part 3: DeviceNet	-	-
ISO 13849-1	2015	Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design	EN ISO 13849-1	2015
ISO 15745-2	2003	Industrial automation systems and integration - Open systems application integration framework - Part 2: Reference description for ISO 11898-based control systems	-	-
ISO 15745-3	2003	Industrial automation systems and integration - Open systems application integration framework - Part 3: Reference description for IEC 61158 based control systems	-	-
ISO 15745-4	2003	Industrial automation systems and integration - Open systems application integration framework - Part 4: Reference description for Ethernet-based control systems	-	-

Documents
Document Sharing Hub

Full document details: DIN EN IEC 61784-3-2:2023-04

CONTENTS

page

European foreword 20

Annex ZA (normative) Normative references to international publications with their corresponding European publications 21

0 Introduction 34

0.1 General 34

0.2 Patent declaration 36

1 Scope 36

2 Normative references 36

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 2: Additional terms and definitions 43

3.2 Symbols and abbreviated terms 44

3.2.1 Common symbols and abbreviated terms 44

3.2.2 CPF 2: Additional symbols and abbreviated terms 44

3.3 Conventions 45

4 Overview of FSCP 2/1 (CIP Safety™) 46

4.1 General 46

4.2 FSCP 2/1 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 48

5.5 Relationships with FAL (and DLL, PhL) 49

5.5.1 General 49

5.5.2 Data types 49

6 Safety communication layer services 49

6.1 General 49

6.2 Connection object 50

6.2.1 General 50

6.2.2 Class attribute extensions 50

6.2.3 Service extensions 50

6.2.4 Explicit message response format for SafetyOpen and SafetyClose 51

6.3 Connection Manager object 51

6.3.1 General 51

6.3.2 ForwardOpen for safety 52

6.3.3 Safety network segment 54

Documents
Document Sharing Hub

Full document details: DIN EN IEC 61784-3-2:2023-04

6.3.4 Originator rules for calculating the connection parameter CRC 57
6.3.5 SafetyOpen processing flowcharts 57
6.3.6 Checks required by Multipoint producers with existing connections 60
6.3.7 Electronic key usage for safety 61
6.3.8 RPI vs. API in safety connections 61
6.3.9 Application path construction rules for safety connections 61
6.3.10 Safety Validator connection types 63
6.3.11 Application reply data in a successful SafetyOpen response 66
6.3.12 Unsuccessful SafetyOpen response 68
6.3.13 ForwardClose for safety 70
6.4 Identity object 71
6.4.1 General 71
6.4.2 Changes to common services 71
6.4.3 Extensions for CP 16/3 devices 71
6.5 Link objects 72
6.5.1 DeviceNet object changes 72
6.5.2 TCP/IP Interface object changes 72
6.5.3 SERCOS III Link object 73
6.6 Safety Supervisor object 74
6.6.1 General 74
6.6.2 Safety Supervisor class attributes 75
6.6.3 Subclasses 75
6.6.4 Safety Supervisor instance attributes 75
6.6.5 Semantics 79
6.6.6 Subclasses 85
6.6.7 Safety Supervisor common services 85
6.6.8 Safety Supervisor behavior 98
6.7 Safety Validator object 105
6.7.1 General 105
6.7.2 Class attributes 106
6.7.3 Instance attributes 106
6.7.4 Class services 112
6.7.5 Instance services 112
6.7.6 Object behavior 113
6.8 Connection Configuration Object 116
6.8.1 General 116
6.8.2 Class attribute extensions 116
6.8.3 Instance attributes, additions and extensions. 116
6.8.4 Instance attribute semantics extensions or restrictions for safety 119

Documents
Document Sharing Hub
Full document details: DIN EN IEC 61784-3-2:2023-04

6.8.5 Special Safety Related Parameters – (Attribute 13) 124
6.8.6 Object-specific services 129
6.8.7 Common service extensions for safety 129
6.8.8 Object behavior 131
7 Safety communication layer protocol 133
7.1 Safety PDU format 133
7.1.1 Safety PDU encoding 133
7.1.2 Safety CRC 145
7.2 Communication protocol behavior 146
7.2.1 Sequence of safety checks 146
7.2.2 Connection termination 146
7.2.3 Cross checking error 147
7.3 Time stamp operation 147
7.4 Rollover counts in the EF 148
7.5 Protocol sequence diagrams 148
7.5.1 General 148
7.5.2 Normal safety transmission 148
7.5.3 Lost, corrupted and delayed message transmission 149
7.5.4 Lost, corrupted or delayed message transmission with production repeated 152
7.5.5 Point-to-point ping 154
7.5.6 Multipoint ping on CP 2/3 Safety 155
7.5.7 Multipoint ping on CP 2/2 safety networks 157
7.5.8 Multipoint ping – retry with success 157
7.5.9 Multipoint ping – retry with timeout 158
7.6 Safety protocol definition 159
7.6.1 General 159
7.6.2 High level view of a safety device 159
7.6.3 Safety Validator object 160
7.6.4 Relationship between SafetyValidatorServer and SafetyValidatorClient 160
7.6.5 Extended Format time stamp rollover handling 161
7.6.6 SafetyValidatorClient function definition 166
7.6.7 SafetyValidatorServer function definition 174
7.7 Safety message and protocol data specifications 187
7.7.1 Mode octet 187
7.7.2 Time Stamp Section 188
7.7.3 Time Coordination Message 188
7.7.4 Time correction message 189
7.7.5 Safety data production 189
7.7.6 Producer dynamic variables 196

AVA Documents
Document Sharing Hub

Full document details: DIN EN IEC 61784-3-2:2023-04

7.7.7 Producer per consumer dynamic variables 198
7.7.8 Consumer data variables 200
7.7.9 Consumer input static variables 201
7.7.10 Consumer dynamic variables 202
8 Safety communication layer management 204
8.1 Overview 204
8.2 Definition of the measures used during connection establishment 205
8.3 Originator-Target relationship validation 208
8.4 Detection of mis-routed connection requests 208
8.5 SafetyOpen processing 208
8.6 Ownership management 209
8.7 Bridging different physical layers 210
8.8 Safety connection establishment 211
8.8.1 Overview 211
8.8.2 Basic facts for connection establishment 211
8.8.3 Configuring safety connections 212
8.8.4 Network time expectation multiplier 213
8.8.5 Establishing connections 215
8.8.6 Recommendations for consumer number allocation 218
8.8.7 Recommendations for connection establishment 218
8.8.8 Ownership establishment 218
8.8.9 Ownership use cases 219
8.8.10 PID/CID usage and establishment 222
8.8.11 Proper PID/CID usage in multipoint and point-to-point connections 222
8.8.12 Network supported services 224
8.8.13 FSCP 2/1 safety device type 225
8.9 Safety configuration process 228
8.9.1 Introduction to safety configuration 228
8.9.2 Configuration goals 228
8.9.3 Configuration overview 229
8.9.4 User configuration guidelines 230
8.9.5 Configuration process justification 231
8.9.6 Device functions for tool configuration 232
8.9.7 Password security 232
8.9.8 SNCT interface services 232
8.9.9 Configuration lock 233
8.9.10 Effect of configuration lock on device behavior 233
8.9.11 Configuration ownership 235
8.9.12 Configuration mode 235

Documents
Document Sharing Hub
Full document details: DIN EN IEC 61784-3-2:2023-04

8.9.13 Measures used to ensure integrity of configuration process 235
8.9.14 Download process 237
8.9.15 Verification process 240
8.9.16 Configuration error analysis 243
8.10 Electronic Data Sheets extensions for safety 247
8.10.1 General rules for EDS based safety devices 247
8.10.2 EDS extensions for safety 248
8.11 Requirements for CP 2/2 253
8.11.1 EPI rules for safety messages that travel over CP 2/2 253
8.11.2 Default safety I/O service 253
8.11.3 Duplicate IP detection 253
8.11.4 Priority for safety connections 253
8.12 Requirements for CP 2/3 254
8.12.1 Allocation of CP 2/3 identifiers 254
8.12.2 Additional requirements 256
8.13 CP 16/3 requirements 256
8.13.1 General architecture for CPF 2 on CP 16/3 256
8.13.2 Baseline FSCP 2/1 on CP 16/3 device 257
8.13.3 Supported objects and services in CP 16/3 devices 257
8.13.4 Transport layer requirements 258
8.13.5 FSCP 2/1 and the CP 16/3 device model 260
8.13.6 UNID assignment on CP 16/3 261
9 System requirements 264
9.1 Indicators and switches 264
9.1.1 General indicator requirements 264
9.1.2 LED indications for setting the device UNID 264
9.1.3 Module Status LED 264
9.1.4 Indicator warning 265
9.1.5 Network Status LED 265
9.1.6 Switches 266
9.2 Installation guidelines 268
9.3 Safety function response time 269
9.3.1 Overview 269
9.3.2 Network time expectation 269
9.3.3 Equations for calculating network reaction times 270
9.4 Duration of demands 272
9.5 Constraints for calculation of system characteristics 272
9.5.1 Number of nodes 272
9.5.2 Network PFH of Extended Format 272

Documents
Document Sharing Hub
Full document details: DIN EN IEC 61784-3-2:2023-04

9.5.3 Bit Error Rate (BER) 273
9.6 Maintenance 274
9.7 Safety manual 274
10 Assessment 274
Annex B (informative) Additional information for functional safety communication profiles of CPF 2 275
B.1 Hash function example code 275
B.2 Void 289
Annex B (informative) Information for assessment of the functional safety communication profiles of CPF 2 290
Bibliography 291

Figures

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 – Relationship of Safety Validators 46
Figure 4 – Communication layers 49
Figure 5 – ForwardOpen with safety network segment 53
Figure 6 – Safety network target format 55
Figure 7 – Target Processing SafetyOpen with no configuration data (Type 2 SafetyOpen) 58
Figure 8 – Target Processing for SafetyOpen with configuration data (Type 1 SafetyOpen) 59
Figure 9 – Originator logic to determine which format to use 60
Figure 10 – Applying device configuration 90
Figure 11 – Configure and Validate processing flowcharts 91
Figure 12– UNID handling during "Waiting for TUNID" 97
Figure 13 – Safety Supervisor state diagram 99
Figure 14 – Configuration, testing and locked relationships 103
Figure 15 – Safety connection types 110
Figure 16 – Safety Validator state transition diagram 114
Figure 17 – Logic for Auto-detecting format type 128
Figure 18 – Connection Configuration Object state diagram 132
Figure 19 – Connection Configuration Object data flow 132
Figure 20 – Format of the mode octet 134
Figure 21 – 1 or 2 octet data section, Base Format 135
Figure 22 – 1 or 2 octet data section, Extended Format 136
Figure 23 – 3 to 250 octet data section format, Base Format 136
Figure 24 – 3 to 250 octet data section format, Extended Format 137
Figure 25 – Time Stamp section format, Base Format 138
Figure 26 – BF Time Coordination message encoding 139
Figure 27 – EF Time Coordination message encoding 139
Figure 28 – BF Time Correction message encoding 140

Documents
Document Sharing Hub
Full document details: DIN EN IEC 61784-3-2:2023-04

Figure 29 – EF Time Correction message encoding 140
Figure 30 – 1 or 2 octet point-to-point PDU encoding 142
Figure 31 – 1 or 2 Octet multipoint PDU encoding 142
Figure 32 – 1 or 2 Octet, multipoint, Format 2 safety connection format 143
Figure 33 – 3 to 250 Octet Point-to-point PDU encoding 143
Figure 34 – 3 to 248 Octet Multipoint PDU encoding 144
Figure 35 – 3 to 248 Octet, Multipoint, safety connection format 144
Figure 36 – CRC Calculation order for Extended Format messages 145
Figure 37 – Time stamp sequence 147
Figure 38 – Sequence diagram of a normal producer/consumer safety sequence 148
Figure 39 – Sequence diagram of a normal producer/consumer safety sequence (production repeated) 149
Figure 40 – Sequence diagram of a corrupted producer to consumer message 150
Figure 41 – Sequence diagram of a lost producer to consumer message 151
Figure 42 – Sequence diagram of a delayed message 152
Figure 43 – Sequence diagram of a corrupted producer to consumer message with production repeated 153
Figure 44 – Sequence diagram of a connection terminated due to delays 153
Figure 45 – Sequence diagram of a failure of safety CRC check 154
Figure 46 – Sequence diagram of a point-to-point ping – normal response 154
Figure 47 – Sequence diagram of a successful multipoint ping, CP 2/3 safety 156
Figure 48 – Sequence diagram of a successful multipoint ping, CP 2/2 safety 157
Figure 49 – Sequence diagram of a multipoint ping retry 158
Figure 50 – Sequence diagram of a multipoint ping timeout 158
Figure 51 – Possible safety architectures for FSCP 2/1 159
Figure 52 – Safety device reference model entity relation diagram 160
Figure 53 – Two devices interchanging safety data via a SafetyValidatorClient and a SafetyValidatorServer 161
Figure 54 – Point-to-point, originating consumer. target producer 162
Figure 55 – Point-to-point, originator producer, target consumer 164
Figure 56 – Multi-point, originator consumer, target producer 165
Figure 57 – Safety production data flow 166
Figure 58 – Consumer safety data monitoring 175
Figure 59 – SafetyValidatorServer – application triggered 176
Figure 60 – Target ownership 208
Figure 61 – SafetyOpen forms 209
Figure 62 – Connection ownership state chart 209
Figure 63 – SafetyOpen UNID mapping 210
Figure 64 – Common CPF 2 application layer 210
Figure 65 – End-to-End routing example 211

Documents
Document Sharing Hub
Full document details: DIN EN IEC 61784-3-2:2023-04

Figure 66 – Sources for safety related connection parameters 214
Figure 67 – Parameter mapping between originator and target 215
Figure 68 – CP 2/3 Safety connection establishment in targets for Type 2a SafetyOpen 217
Figure 69 – General sequence to detect configuration is required 217
Figure 70 – PID/CID exchanges for two originator scenarios 222
Figure 71 – Seed generation for multipoint connections 223
Figure 72 – PID/CID runtime handling 224
Figure 73 – Connection categories and supported services 226
Figure 74 – Recommended connection types 227
Figure 75 – Logic-to-logic supported services 227
Figure 76 – Recommended connection types for logic to logic 228
Figure 77 – Configuration data transfers 229
Figure 78 – Protection measures in safety devices 231
Figure 79 – Configuration, testing and locked relationships 234
Figure 80 – Originator's configuration data 236
Figure 81 – SNCT to device download process 238
Figure 82 – SNCT Downloads to originators that perform Type 1 configuration 239
Figure 83 – Protection from locking and ownership 241
Figure 84 – Verification process including all alternatives 243
Figure 85 – Baseline FSCP 2/1 on CP 16/3 device 257
Figure 86 – FSCP 2/1 Adaptation Layer and SMP interaction 259
Figure 87 – FSCP 2/1 Adaptation 260
Figure 88 – CP 16/3 device model 261
Figure 89 – Adding a standard module to a modular device 263
Figure 90 – Safety device NodeID processing logic 268
Figure 91 – Safety function response time 269
Figure 92 – Safety function response time components 271
Figure 93 – Network protocol reliability block diagram (RBD) 272

Tables

Table 1 – Communications errors and detection measures matrix 48
Table 2 – New class attributes 50
Table 3 – Service extensions 51
Table 4 – SafetyOpen and SafetyClose response format 51
Table 5 – Safety network segment identifier 54
Table 6 – Safety network segment definition 54
Table 7 – Safety network segment router format 56
Table 8 – Safety Network Segment Extended Format 56
Table 9 – Multipoint producer parameter evaluation rules 61

Documents
Document Sharing Hub
Full document details: DIN EN IEC 61784-3-2:2023-04

Table 10 – ForwardOpen setting options for safety connections with object-based application paths 64
Table 11 – ForwardOpen setting options for safety connections with ANSI Extended symbol segment application path 65
Table 12 – Network connection parameters for safety connections 66
Table 13 – SafetyOpen target application reply (size: 10 octets) 67
Table 14 – EF CP 2/2 or CP 16/3 SafetyOpen target application reply (size: 14 octets) 67
Table 15 – BF CP 2/3 SafetyOpen target application reply (size: 18 octets) 68
Table 16 – EF CP 2/3 SafetyOpen target application reply (size: 22 octets) 68
Table 17 – New and extended error codes for safety 69
Table 18 – SafetyOpen error event guidance table 70
Table 19 – Identity object common service changes 71
Table 20 – Identity object extensions for CP 16/3 devices 71
Table 21 – New DeviceNet object instance attribute 72
Table 22 – New TCP/IP Interface object instance attribute 73
Table 23 – SERCOS III Link object class attributes 73
Table 24 – SERCOS III Link object instance attributes 73
Table 25 – SERCOS III Link Object Common Services 74
Table 26 – Safety Supervisor class attributes 75
Table 27 – Safety Supervisor instance attributes 75
Table 28 – Device status attribute state values 79
Table 29 – Exception status attribute format 80
Table 30 – Common exception detail attribute values 81
Table 31 – Exception detail format summary 82
Table 32 – Summary of device behavior for various CFUNID values 84
Table 33 – Safety Supervisor common services 86
Table 34 – Safety Supervisor object specific services 86
Table 35 – Configure_Request message structure 88
Table 36 – Validate_Configuration message structure 88
Table 37 – Validate_Configuration success message structure 89
Table 38 – Validate_Configuration error code 89
Table 39 – Validate_Configuration extended codes 89
Table 40 – Set_Password message structure 92
Table 41 – Reset_Password message structure 92
Table 42 – Configuration_Lock/Unlock message structure 93
Table 43 – Mode_Change message structure 93
Table 44 – Safety_Reset message structure 94
Table 45 – Safety Supervisor safety reset types 94
Table 46 – Attribute bit map parameter 94
Table 47 – Reset processing rules for reset types 95
Table 48 – Propose_TUNID service 95

AVA Documents
Document Sharing Hub
Full document details: DIN EN IEC 61784-3-2:2023-04

Table 49 – Apply_TUNID service 96
Table 50 – Propose_TUNID_List service 98
Table 51 – Apply_TUNID_List service 98
Table 52 – Safety Supervisor events 99
Table 53 – State event matrix for Safety Supervisor 100
Table 54 – Configuration owner control vs. device state 104
Table 55 – State mapping of Safety Supervisor to Identity object 104
Table 56 – Safety Supervisor object event mapping 104
Table 57 – Identity object event mapping 105
Table 58 – Safety Validator class attributes 106
Table 59 – Safety Validator instance attributes 106
Table 60 – Safety Validator state assignments 109
Table 61 – Safety Validator type, bit field assignments 109
Table 62 – Multipoint producer SafetyOpen parameter evaluation rules 111
Table 63 – Safety Validator class services 112
Table 64 – Safety Validator instance services 113
Table 65 – Safety Validator Get_Attributes_All service data 113
Table 66 – Safety Validator state event matrix 115
Table 67 – State mapping between Safety Supervisor and Safety Validator objects 115
Table 68 – Connection configuration object class attribute extensions 116
Table 69 – Connection Configuration Object instance attribute additions/extensions 117
Table 70 – Connection flag bit definitions 119
Table 71 – O-to-T connection parameters 121
Table 72 – T-to-O connection parameters 121
Table 73 – Data map formats 123
Table 74 – Data map format 0 123
Table 75 – Data map format 1 124
Table 76 – Target device's SCCRC values 126
Table 77 – Target device's SCTS values 126
Table 78 – Time correction connection parameters for multipoint connection 127
Table 79 – Format Type attribute meaning 127
Table 80 – Format Status attribute meaning 128
Table 81 – Connection Configuration Object-specific services 129
Table 82 – Get_Attributes_All Response service data (added attributes) 130
Table 83 – Get_Attributes_All Response service data (added parameters) 130
Table 84 – Set_Attributes_All Request service data (added attributes) 131
Table 85 – Set_Attributes_All Response service data (added parameters) 131
Table 86 – State Mapping between Safety Supervisor and the CCO objects 132
Table 87 – Connection sections and PDU formats 134

Documents
Document Sharing Hub
Full document details: DIN EN IEC 61784-3-2:2023-04

Table 88 – Connection sections and message format 134
Table 89 – Mode octet variables 135
Table 90 – Time Stamp variables 138
Table 91 – Time Coordination message variables 139
Table 92 – Time Correction Message variables 141
Table 93 – CRC polynomials used 145
Table 94 – CRC usage for connection and configuration 146
Table 95 – Data reception – Link triggered 177
Table 96 – Time_Correction reception – Link triggered 177
Table 97 – Data reception – Application triggered 177
Table 98 – Time_Correction reception – Application triggered 178
Table 99 – Consuming application – Safety data monitoring 178
Table 100 – Producer connection status determination 190
Table 101 – Consuming safety connection status 200
Table 102 – Connection establishment errors and measures to detect errors 204
Table 103 – SNN Date/Time allocations 205
Table 104 – SNN legal range of time values 205
Table 105 – Safety connection parameters 213
Table 106 – SafetyOpen summary 216
Table 107 – Originator/Target service mapping 225
Table 108 – Unsupported originator/target service types 226
Table 109 – Configuration goals 229
Table 110 – Configuration owner control vs. device state 234
Table 111 – Errors and detection measures 244
Table 112 – Object Class section keywords 248
Table 113 – Safety Classx entry format 249
Table 114 – Parameter class keywords 249
Table 115 – New Connection Manager section keywords for safety 250
Table 116 – Connection Manager field usage for safety 251
Table 117 – Connection parameter field settings for safety 252
Table 118 – CP 2/3 ID assignment rules 254
Table 119 – LED indications for setting UNID 264
Table 120 – Module Status LED 265
Table 121 – Network status LED states 265
Table 122 – Connection reaction time type – producing/consuming applications 270

AVA Documents
Document Sharing Hub
Full document details: DIN EN IEC 61784-3-2:2023-04

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES –

Part 3-2: Functional safety fieldbuses – Additional specifications for CPF 2

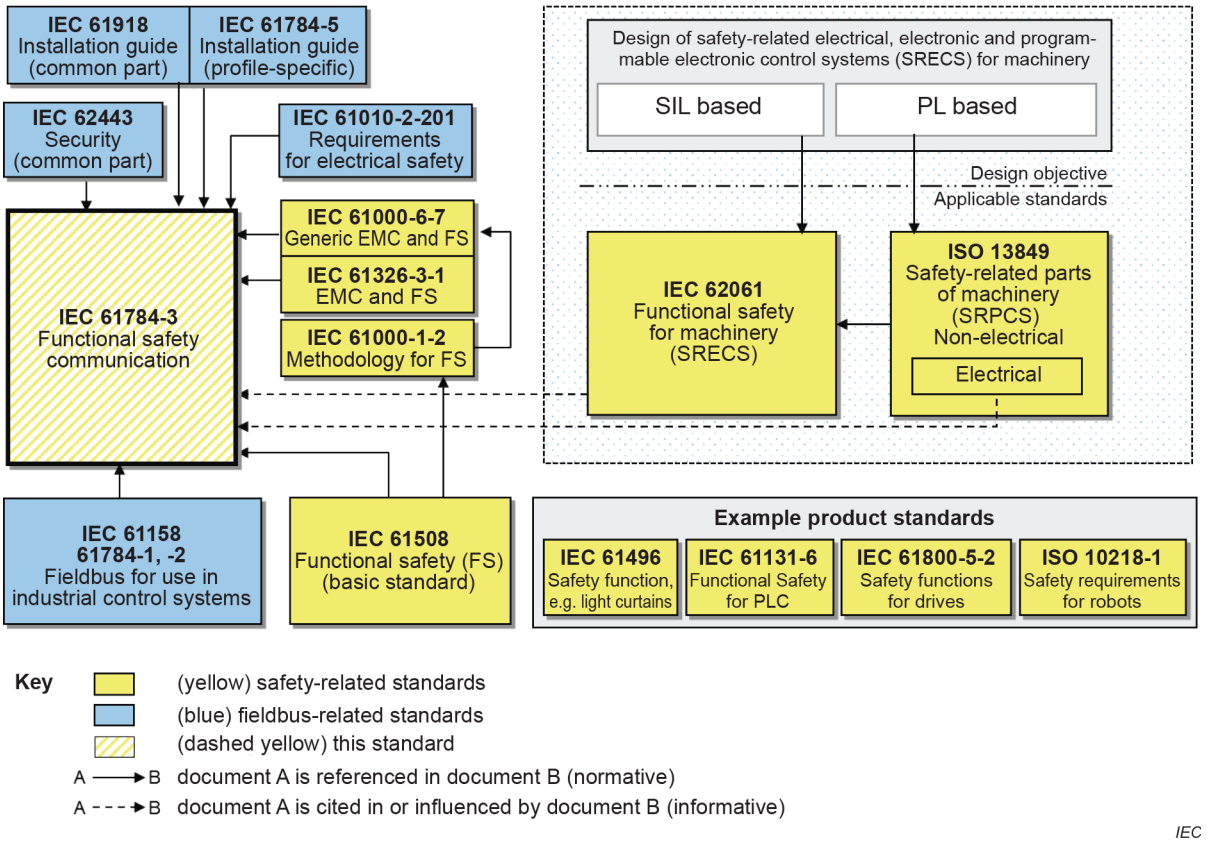
0 Introduction

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.

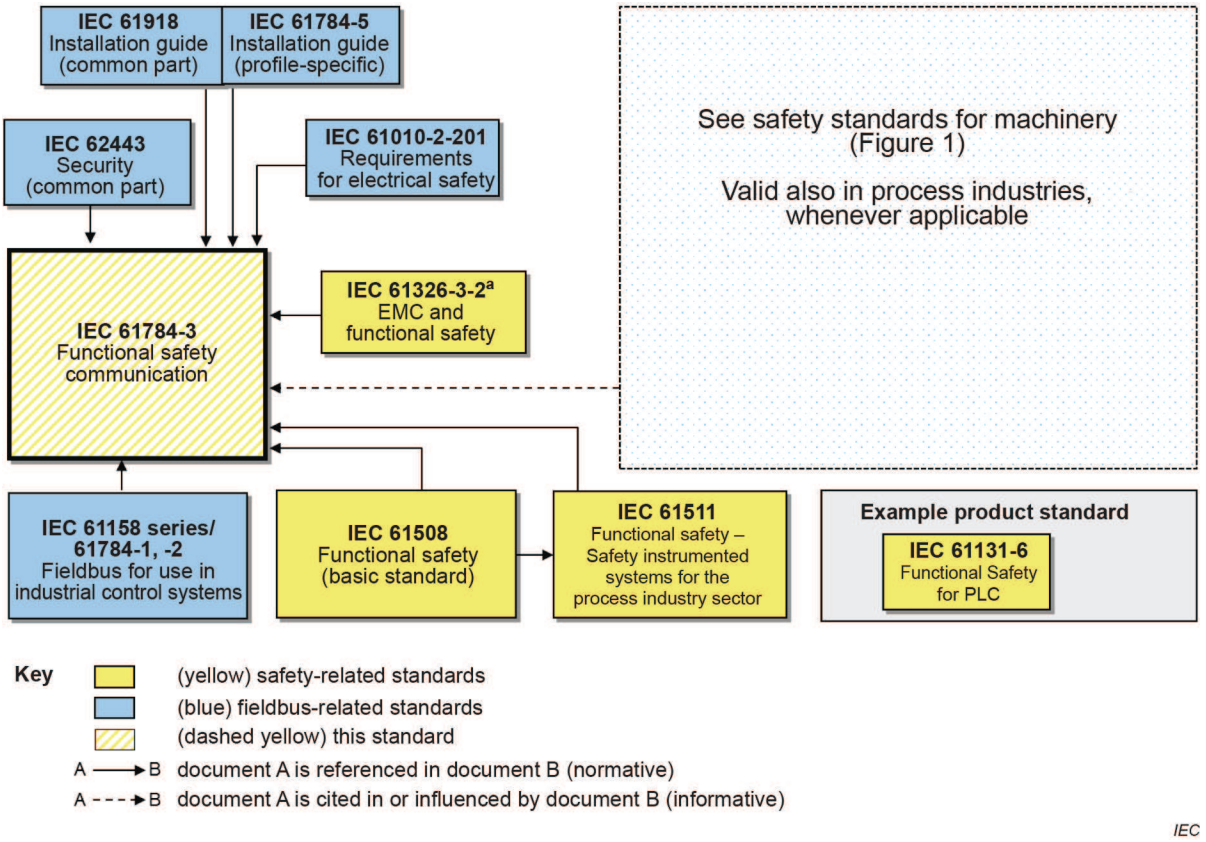


NOTE IEC 62061 specifies the relationship between PL (Category) and SIL.

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

Documents
Document Sharing Hub
Full document details: DIN EN IEC 61784-3-2:2023-04

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 61784-3-2:2023-04

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 2. 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.

1 Scope

This part of IEC 61784-3 (all parts) specifies a safety communication layer (services and protocol) based on CPF 2 of IEC 61784-1, IEC 61784-2 and IEC 61158 Type 2. 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)[1] for functional safety. These mechanisms may be used in various industrial applications such as process control, manufacturing automation and machinery.

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

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

2 Normative references

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

IEC 61131-2, *Industrial-process measurement and control – Programmable controllers – Part 2: Equipment requirements and tests*

IEC 61131-3, *Programmable controllers – Part 3: Programming languages*

IEC 61158-2:2014, *Industrial communication networks – Fieldbus specifications – Part 2: Physical layer specification and service definition*

IEC 61158-3-2, *Industrial communication networks – Fieldbus specifications – Part 3-2: Data-link layer service definition – Type 2 elements*

IEC 61158-3-19, *Industrial communication networks – Fieldbus specifications – Part 3-19: Data-link layer service definition – Type 19 elements*

[1] 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 61784-3-2:2023-04

IEC 61158-4-2:2019, *Industrial communication networks – Fieldbus specifications – Part 4-2: Data-link layer protocol specification – Type 2 elements*

IEC 61158-4-19, *Industrial communication networks – Fieldbus specifications – Part 4-19: Data-link layer protocol specification – Type 19 elements*

IEC 61158-5-2, *Industrial communication networks – Fieldbus specifications – Part 5-2: Application layer service definition – Type 2 elements*

IEC 61158-5-19, *Industrial communication networks – Fieldbus specifications – Part 5-19: Application layer service definition – Type 19 elements*

IEC 61158-6-2, *Industrial communication networks – Fieldbus specifications – Part 6-2: Application layer protocol specification – Type 2 elements*

IEC 61158-6-19, *Industrial communication networks – Fieldbus specifications – Part 6-19: Application layer protocol specification – Type 19 elements*

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

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

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

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

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

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

IEC 61784-5-2, *Industrial communication networks – Profiles – Part 5-2: Installation of fieldbuses – Installation profiles for CPF 2*

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

IEC 62026-3, *Low-voltage switchgear and controlgear – Controller-device interfaces (CDIs) – Part 3: DeviceNet*

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

ISO 15745-2:2003, *Industrial automation systems and integration – Open systems application integration framework – Part 2: Reference description for ISO 11898-based control systems*

ISO 15745-3:2003, *Industrial automation systems and integration – Open systems application integration framework – Part 3: Reference description for IEC 61158-based control systems*

ISO 15745-4:2003, *Industrial automation systems and integration – Open systems application integration framework – Part 4: Reference description for Ethernet-based control systems*

Documents
Document Sharing Hub
Full document details: DIN EN IEC 61784-3-2:2023-04

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

3.1.1.4
closed communication system
fixed number or fixed maximum number of participants linked by a *communication system* with well-known and fixed properties, and where the *risk* of unauthorized access is considered negligible

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

3.1.1.5
communication channel
logical *connection* between two end-points within a *communication system*

3.1.1.6
communication system
arrangement of hardware, software and propagation media to allow the transfer of *messages* (ISO/IEC 7498-1 application layer) from one application to another

3.1.1.7
connection
logical binding between two application objects within the same or different devices

Documents
Document Sharing Hub
Full document details: DIN EN IEC 61784-3-2:2023-04

3.1.1.8
Cyclic Redundancy Check
CRC
<value> redundant data derived from, and stored or transmitted together with, a block of data in order to detect data corruption
<method> procedure used to calculate the redundant data

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

Note 2 to entry: See also [26], [27][2].

3.1.1.9
defined communication system
defined channel
fixed number or fixed maximum number of participants linked by a *fieldbus* based *communication system* with well-known and fixed properties, such as installation conditions, electromagnetic immunity, industrial *(active) network elements*, and where the *risk* of unauthorized access is reduced to a tolerated level according to the lifecycle model of IEC 62443 (all parts), using for example zones and conduits

3.1.1.10
device
physical entity connected to the fieldbus composed of communication element and possibly other functional elements

[SOURCE: IEC 61158-2:2014, 3.1.13, modified – Note to entry and some details have been deleted.]

3.1.1.11
DLPDU
DEPRECATED: frame
Data Link Protocol Data Unit

3.1.1.12
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]

3.1.1.13
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]

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

Documents
Document Sharing Hub
Full document details: DIN EN IEC 61784-3-2:2023-04

3.1.1.14
fault
abnormal condition that may cause a reduction in, or loss of, the capability of a functional unit to perform a required function

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

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

3.1.1.15
fieldbus
communication system based on serial data transfer and used in industrial automation or process control applications

3.1.1.16
functional safety communication profile
FSCP
technology specification for the implementation of an SCL

3.1.1.17
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.

3.1.1.18
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]

3.1.1.19
master
communication entity able to initiate and schedule communication activities by other stations which may be masters or slaves

3.1.1.20
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]

3.1.1.21
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]

Documents
Document Sharing Hub
Full document details: DIN EN IEC 61784-3-2:2023-04

3.1.1.22
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]

3.1.1.23
residual error rate
statistical rate at which the SCL *safety measures* fail to detect *errors*

3.1.1.24
risk
combination of the probability of occurrence of harm and the severity of that harm

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

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

3.1.1.25
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*.

3.1.1.26
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

3.1.1.27
safety connection
connection that utilizes the safety protocol for communications transactions

3.1.1.28
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.

3.1.1.29
safety device
device designed in accordance with IEC 61508 and which implements the functional safety communication profile

3.1.1.30
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]

3.1.1.31
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.

Documents
Document Sharing Hub
Full document details: DIN EN IEC 61784-3-2:2023-04

3.1.1.32
safety integrity level
SIL
discrete level (one out of a possible four), corresponding to a range of safety integrity values, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest

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

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

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

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

3.1.1.33
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.

3.1.1.34
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*.

3.1.1.35
safety-related application
programs designed in accordance with IEC 61508 to meet the SIL requirements of the application

3.1.1.36
safety-related system
system performing *safety functions* according to IEC 61508

3.1.1.37
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

3.1.1.38
spurious trip
trip caused by the safety system without a process demand

3.1.1.39
time stamp
time information included in a *message*

Documents
Document Sharing Hub
Full document details: DIN EN IEC 61784-3-2:2023-04

3.1.2 CPF 2: Additional terms and definitions

3.1.2.1
base format
format used for connection RPIs of less than 100 ms or for applications where dropped connections can be tolerated

3.1.2.2
deprecate
action to withdraw official support for or discourage the use of (something, such as a software product) in favor of a newer or better alternative

3.1.2.3
extended format
format used for connection RPIs of more than 100 ms or for applications where there is a need to avoid dropped connections

3.1.2.4
ping
request for the consumer to acknowledge the reception of a message

3.1.2.5
ping response
response to a ping

3.1.2.6
originator
node that requests the creation of a connection

3.1.2.7
signature
method of uniquely identifying a set of data

Note 1 to entry: This could be by revision, checksum or some other method that is agreed upon by the originating and target devices.

3.1.2.8
single safety port device
originator, target, or mixed originator/target device that performs safety communications on one and only one CIP port

3.1.2.9
systematic capability
measure (expressed on a scale of SC 1 to SC 4) of the confidence that the systematic safety integrity of an element meets the requirements of the specified SIL, in respect of the specified element safety function, when the element is applied in accordance with the instructions specified in the compliant item safety manual for the element

[SOURCE: IEC 61508-4:2010, 3.5.9, modified – notes deleted]

3.1.2.10
systematic safety integrity
part of the safety integrity of a safety-related system relating to systematic failures in a dangerous mode of failure

[SOURCE: IEC 61508-4:2010, 3.5.6, modified – note deleted]

3.1.2.11
target
node that receives a connection creation request

Documents
Document Sharing Hub
Full document details: DIN EN IEC 61784-3-2:2023-04

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]
PFD	Probability of dangerous Failure on Demand	[IEC 61508-4:2010]
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]

3.2.2 CPF 2: Additional symbols and abbreviated terms

AIRS	Already In Requested Mode/State
BER	Bit Error Rate
BF	Base Format
CCO	Connection Configuration Object
CFUNID	Configuration UNID
CNP	Connection Point
CID	Consumer ID
CIP™[3]	Common Industrial Protocol (application framework shared among CPF 2 communication profiles)
CPCRC	Connection Parameter CRC
CTM	Connection Timeout Multiplier
EDS	Electronic Data Sheet

[3] For trade name declaration, see Clause 4.

Documents
Document Sharing Hub
Full document details: DIN EN IEC 61784-3-2:2023-04

EF	Extended Format	
EPI	Expected Packet Interval	
LED	Light Emitting Diode	
MACID	Device physical address (CP 2/3)	
MOD	Module	
NodeID	For CP 2/3 safety devices, this is the MACID of the device on the network. For CP 2/2 safety devices, this is the IP address of the device on the network. For CP 16/3 safety devices, this is the SDID of the device on the network.	
NV	Non-Volatile	
NVS	Non-Volatile Storage	
OCPUNID	Output Connection Owner UNID	
OSC	Object State Conflict	
O-to-T	Originator to Target	
OUNID	Originator UNID	
PID	Producer Identifier	
PS	Power Supply	
Res.	Reserved	
RPI	Requested Packet Interval	
SCCRC	Safety Configuration Data CRC	
SCID	Safety Configuration Identified	
SCTS	Safety Configuration Time Stamp	
SNCT	Safety Network Configuration Tool	
SNN	Safety Network Number	
T-to-O	Target to Originator	
TBD	To Be Defined	
TNS	TUNID Not Set	
TUNID	Target UNID	
UML	Universal Modeling Language	[ISO/IEC 19501]
UNID	Unique Network Identifier	

3.3 Conventions

The conventions used for the descriptions of objects, services and protocols are described in IEC 61158-3-2, IEC 61158-4-2, IEC 61158-5-2, and IEC 61158-6-2.

As appropriate this document uses flow charts, UML Sequence Diagrams and "C" pseudo-code to describe concepts.

Documents
Document Sharing Hub

Full document details: DIN EN IEC 61784-3-2:2023-04

4 Overview of FSCP 2/1 (CIP Safety™)

4.1 General

Communication Profile Family 2 (commonly known as CIP™[4]) defines communication profiles based on IEC 61158-2 Type 2, IEC 61158-3-2, IEC 61158-4-2, IEC 61158-5-2, and IEC 61158-6-2.

Communication Profile Family 16 (commonly known as SERCOS®[5]) defines a communication profile CP 16/3 based on IEC 61158-3-19, IEC 61158-4-19, IEC 61158-5-19, and IEC 61158-6-19.

The basic profiles CP 2/1, CP 2/2, CP 2/3 and CP 16/3 are defined in IEC 61784-1 and IEC 61784-2. The CPF 2 functional safety communication profile FSCP 2/1 (CIP Safety™[4]) is based on the CPF 2 basic profiles in IEC 61784-1 and IEC 61784-2, the CP 16/3 basic profile in IEC 61784-2, and the safety communication layer specifications defined in this document.

4.2 FSCP 2/1

FSCP 2/1 is based on the producer/consumer model of CPF 2. The pairing of producers and consumers is an important part of the relationship that provides the high integrity needed for safety-related applications.

The FSCP 2/1 safety communication layer is specified using a Safety Validator object. This object is responsible for managing the FSCP 2/1 safety connections and serves as the interface between the safety-related application objects and the link layer connections, as shown in Figure 3. The Safety Validator ensures the integrity of the safety data transfers.

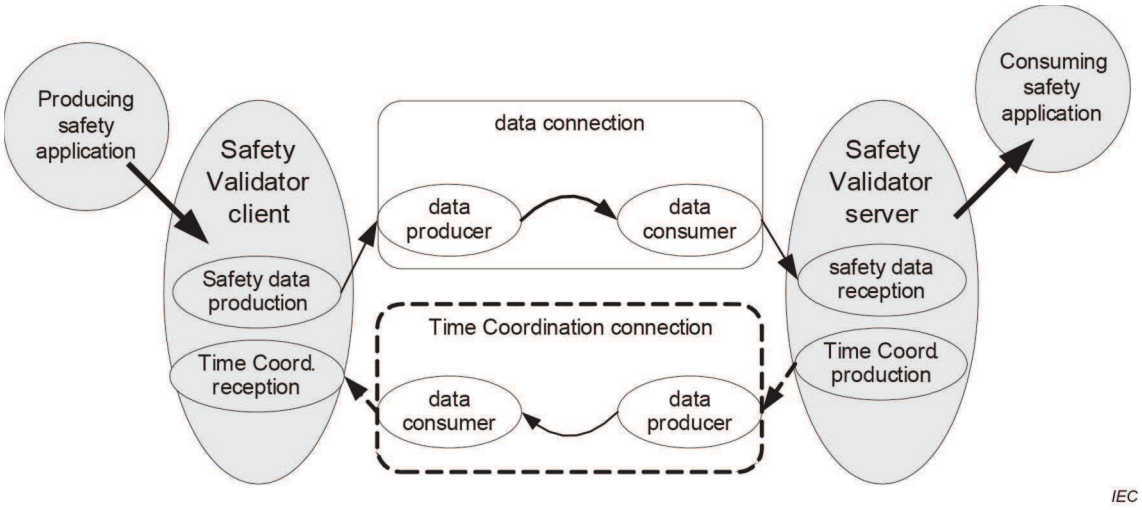


Figure 3 – Relationship of Safety Validators

The integrity of the safety data transfers is ensured as follows:

– the producing safety-related application uses an instance of a client Safety Validator to produce safety data and ensure time coordination;

4 CIP™ (Common Industrial Protocol) and CIP Safety™ are trade names of the non-profit organization ODVA, Inc. 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 CIP™ or CIP Safety™. Use of the trade names CIP™ or CIP Safety™ requires permission of ODVA and compliance with conditions for their use (such as testing and validation).

5 SERCOS® is a trade name of SERCOS International e.V. This information is given for the convenience of users of this document and does not constitute an endorsement by IEC of the trademark holder or any of its products. Compliance to this document does not require use of the trade name SERCOS®. Use of the trade name SERCOS® requires permission of the trade name holder and compliance with conditions for its use (such as testing and validation).

Documents
Document Sharing Hub
Full document details: DIN EN IEC 61784-3-2:2023-04

– the client uses a link data producer to transmit the data and a link consumer to receive time coordination messages;
– the consuming safety-related application uses a server Safety Validator to receive and check data;
– the server uses a link consumer to receive data and a link producer to transmit time coordination messages.

FSCP 2/1 utilizes the black channel concept. The link producers and consumers have no knowledge of the safety packet and implement no safety function. The responsibility for high-integrity transfer and checking of safety data lies within the Safety Validators.

FSCP 2/1 uses the following measures to ensure the integrity of safety messaging:

– time stamp;
– connection authentication;
– data integrity assurance;
– redundancy with cross checking;
– different data integrity assurance systems.

Messages are produced with a timestamp that allows the consumer to verify the age of data being sent. Identification is encoded into each safety-related message to ensure that the correct consumer is using the message. All safety-related messages use a unique CRC. Safety-related data is sent redundantly. Diverse measures for producing safety-related messages are used to ensure that standard CPF 2 messages are not interpreted as safety messages.

5 General

5.1 External documents providing specifications for the profile

Documents [30] and [31] provide additional specifications which are relevant when implementing the SCL defined in this document.

5.2 Safety functional requirements

The following requirements shall apply to the development of devices that implement the FSCP 2/1 protocol The same requirements were used in the development of FSCP 2/1.

- The FSCP 2/1 protocol is designed to support Safety Integrity Level 3 (SIL3) (see IEC 61508), and PLe/category 4 (see ISO 13849-1).
- The safety state for discrete data is the unenergized state (0). For analog values the unenergized state shall be defined by the safety-related application.
- The basic requirements for the development of the FSCP 2/1 protocol are in IEC 61784-3.
- FSCP 2/1 protocol is implemented using a black channel approach; there is no safety related dependency on the standard CPF 2 communication profiles.
- Implementations of FSCP 2/1 shall comply with IEC 61508.
- Environmental conditions shall be according to IEC 61131-2 for the basic levels and IEC 61326-3-1, IEC 61326-3-2 for the safety margin tests, unless there are specific product standards.
- Safety communication and standard communication shall be independent. However, standard devices and safety devices shall be able to use the same communication channel.
- Unless specified in this document, the CPF 2 requirements shall be unchanged for safety.

Documents
Document Sharing Hub
Full document details: DIN EN IEC 61784-3-2:2023-04

5.3 Safety measures

Table 1 contains the measures used to the detect communication errors and the coverage provided by each measure as used.

Table 1 – Communications errors and detection measures matrix

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				X[a]	(X)[e]	
Incorrect sequence		X				X[a]	(X)[e]	
Loss			X[c]			X[a]	(X)[e]	
Unacceptable delay		(X)[e]	X					
Insertion		X[d]		X		X[a]	(X)[e]	
Masquerade		X[d]		X		X[b]	X[f]	X
Addressing				X		X[b]		

[a] The safety related CRC provides additional protection for communication errors in messages.

[b] Encoding the unique identifier into the safety related CRC prevent masquerade and addressing errors.

[c] A message not received within the time expectation will be detected.

[d] Masquerade or inserted messages will not have the expected time stamp.

[e] Not claimed for FSCP 2/1.

[f] Masquerade will likely not have redundant data and will fail the cross-check.

5.4 Safety communication layer structure

The safety protocol is layered on top of the standard network protocol (the standard protocol stack is a black channel). Figure 4 shows how the safety communication layer is related to the existing CPF 2 layers.

The safety layers accept safety data from the safety-related application circuit. The safety layers then formulate a safety message, transmit the safety message, receive and decode the safety message. Once the safety message is decoded and verified, the data is presented to the receiving safety-related application circuit.

Documents
Document Sharing Hub
Full document details: DIN EN IEC 61784-3-2:2023-04

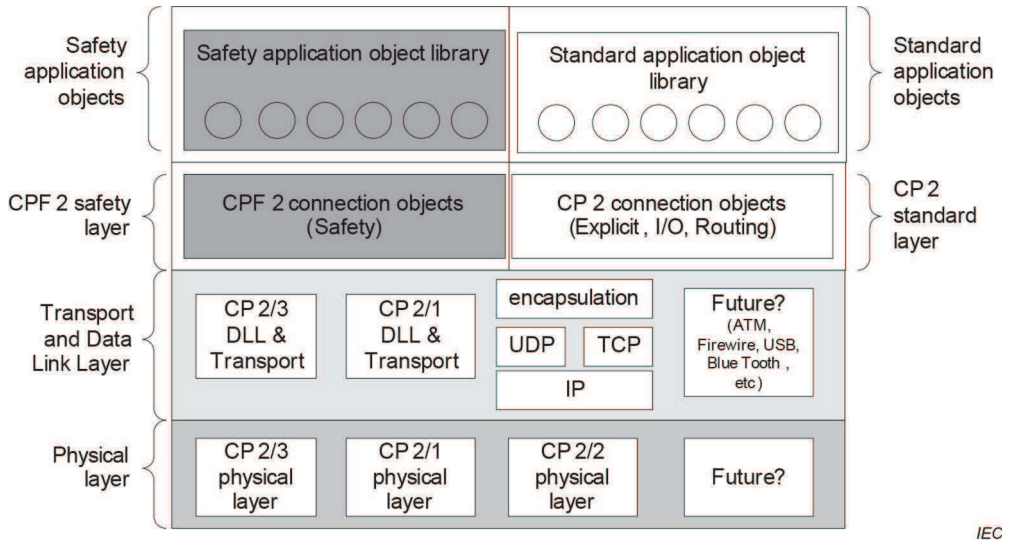


Figure 4 – Communication layers

5.5 Relationships with FAL (and DLL, PhL)

5.5.1 General

This safety communication layer shall only be used in conjunction with CPF 2 communication profiles (CP 2/3 (DeviceNet™[6]), CP 2/2 (EtherNet/IP™[7]), and CP 16/3 (SERCOS III™[8])). There are no requirements of CPF 2 communications profiles other than those defined in this document.

5.5.2 Data types

Profiles defined in this document support all the CPF 2 data types as defined in IEC 61158-5-2.

6 Safety communication layer services

6.1 General

This Clause 6 defines the extensions to existing CPF 2 objects and new objects for Safety. Safety connections use Class 0 connections for I/O messages. Standard Explicit message connections are used for the establishment of Safety I/O connections.

6 DeviceNet™ is a trade name of the non-profit organization ODVA, Inc. 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 name DeviceNet™. Use of the trade name DeviceNet™ requires permission of ODVA.

7 EtherNet/IP™ is a trade name of ODVA, Inc. 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 name EtherNet/IP™. Use of the trade name EtherNet/IP™ requires permission of ODVA.

8 SERCOS® and SERCOS® interface are trade names of SERCOS International e.V. This information is given for the convenience of users of this document and does not constitute an endorsement by IEC of the trademark holder or any of its products. Compliance to this profile does not require use of the trade name SERCOS®. Use of the trade name SERCOS® requires permission of the trade name holder.

Documents
Document Sharing Hub
Full document details: DIN EN IEC 61784-3-2:2023-04

6.2 Connection object

6.2.1 General

Several safety specific class attributes and services are defined to support safety. CP 2/3 Safety nodes which reside on FSCP 2/1 shall implement the SafetyOpen and SafetyClose services of the Connection object.

6.2.2 Class attribute extensions

Table 2 defines the class attributes used by safety devices.

Table 2 – New class attributes

Attrib ID	Need in implementation	Access rule	NV	Name	Date type	Description of attribute
8	Optional	Get	V	Connection request error count	UINT	Diagnostic Counter that is a running count of SafetyOpen or SafetyClose faults[a]
9	Optional	Get	V	Safety connection counters	STRUCT of:	Status counters
				SafetyOpen request suc-cess count	UINT	Count of successful SafetyOpen requests issued from this node to another target
				SafetyOpen request failure count	UINT	Count of unsuccessful SafetyOpen requests issued from this node to another target
				SafetyClose request success count	UINT	Count of successful SafetyClose requests issued from this node to another target
				SafetyClose request failure count[b]	UINT	Count of unsuccessful SafetyClose requests issued from this node to another target
				SafetyOpen indication success count	UINT	Count of successful SafetyOpen requests issued from an external originator to this node
				SafetyOpen indication failure count[b]	UINT	Count of unsuccessful SafetyOpen requests issued from an external originator to this node
				SafetyClose indication success count	UINT	Count of successful SafetyClose requests issued from an external originator to this node
				SafetyClose indication failure count[b]	UINT	Count of unsuccessful SafetyClose requests issued from an external originator to this node

[a] Attribute 8 is the sum of the 4 failure counters in attribute 9. Having this single attribute represent connection errors can be used in monitoring software to efficiently monitor errors without polling the additional attribute 9 structures. Once attribute 8 is non-zero then the monitoring software can examine attribute 9 for more details.

[b] Included in class attribute 8.

6.2.3 Service extensions

Table 3 defines services for use by CP 2/3 safety devices on FSCP 2/1. These services shall be supported by a target device on FSCP 2/1. The SafetyOpen and SafetyClose services, used in lieu of the ForwardOpen and ForwardClose services of the Connection Manager object, inherit the identical behavior from those Connection Manager services.

Documents
Document Sharing Hub
Full document details: DIN EN IEC 61784-3-2:2023-04