

DIN EN 61784-3-3

ICS 35.160; 35.240.50

Ersatz für
DIN EN 61784-3-3:2008-11
Siehe Anwendungsbeginn

**Industrielle Kommunikationsnetze - Profile –
Teil 3-3: Funktional sichere Übertragung bei Feldbussen –
Zusätzliche Festlegungen für die Kommunikationsprofilfamilie 3
(IEC 61784-3-3:2010);
Englische Fassung EN 61784-3-3:2010**

Industrial communication networks - Profiles –
Part 3-3: Functional safety fieldbuses –
Additional specifications for CPF 3
(IEC 61784-3-3:2010);
English version EN 61784-3-3:2010

Réseaux de communication industriels –
Partie 3-3: Bus de terrain à sécurité fonctionnelle –
Spécifications complémentaires pour le CPF 3
(CEI 61784-3-3:2010);
Version anglaise EN 61784-3-3:2010

Gesamtumfang 141 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE

Anwendungsbeginn

Anwendungsbeginn für die von CENELEC am 2010-07-01 angenommene Europäische Norm als DIN-Norm ist 2012-03-01.

Für DIN EN 61784-3-3:2008-11 gilt eine Übergangsfrist bis zum 2013-07-01.

Nationales Vorwort

Zu diesem Dokument wurde ein Kurzverfahren in den DIN-Mitteilungen veröffentlicht.

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

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

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

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

DIN EN 61784-3 (VDE 0803-500-3) erläutert die Grundsätze für funktional sichere Kommunikation, bezogen auf die Normen der Reihe DIN EN 61508 (VDE 0803). Für sie ist eine deutsche Sprachfassung verfügbar.

Die Normen der Reihe DIN EN 61784-3 legen mehrere Sicherheitskommunikationsschichten (Profile und entsprechende Protokolle) basierend auf den Kommunikationsprofilen und Protokollschichten der DIN EN 61784-1, der DIN EN 61784-2 und der Reihe DIN EN 61158 fest. Für diese Kommunikationsnormen ist keine deutsche Sprachfassung verfügbar. Sie allein sind nicht ausreichend zur Auslegung eines sicherheitsbezogenen Systems nach DIN EN 61508 (VDE 0803), stets ist die Beachtung der letztgenannten Normenreihe und der DIN EN 61784-3 erforderlich.

Die Kommunikationsnormen der Reihe DIN EN 61784-3 weisen alle die gleiche Gliederung auf, sie ist in DIN EN 61784-3 (VDE 0803-500), Anhang C, in deutscher und englischer Sprache wiedergegeben, so dass ein Bezug zwischen der deutschsprachigen DIN EN 61784-3 (VDE 0803-500) und der englischsprachigen Reihe DIN EN 61784-3-x jederzeit möglich ist. Darüber hinaus sind in ersterer alle Begriffe und Abkürzungen jeweils in Deutsch und Englisch wiedergegeben.

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

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

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

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

Da sich die Benutzer der vorliegenden Norm der englischen Sprache als Fachsprache bedienen, wird die Englische Fassung der EN 61784-3-3 veröffentlicht. Zu deren Abschnitt 3, der die Begriffe festlegt, wurde eine Übersetzung angefertigt und als Nationaler Anhang NA der vorliegenden Norm hinzugefügt. Für die

meisten der verwendeten Begriffe existieren keine gebräuchlichen deutschen Benennungen, da sich die deutschen Anwender in der Regel ebenfalls der englischen Benennungen bedienen. Diese Norm steht nicht in unmittelbarem Zusammenhang mit Rechtsvorschriften und ist nicht als Sicherheitsnorm anzusehen.

Änderungen

Gegenüber DIN EN 61784-3-3:2008-11 wurden folgende Änderungen vorgenommen:

- a) Änderungen, die sich aus DIN EN 61784-3 (VDE 0803-500):2011-02 ergeben, eingearbeitet;
- b) Einführung eines sekundären Watchdog-Timers (F_WD_Time_2), um die Anwendungsfälle „configuration-in-run“, „maintenance of fault tolerance systems“ oder beide (7.1.3, 7.2.3, 7.2.6, 8.1.1, 8.1.4, 8.1.6.2) abzudecken;
- c) fehlende GSDL-Festlegungen eingefügt (8.3.2.1);
- d) fehlende Berechnung der CRC-Signatur einer GSD eingefügt (8.3.3.3);
- e) Beschränkungen für die Zuweisung von Parameterwerten des primären Watchdog-Timers „F_WD_Time“ eingefügt (9.3.3);
- f) Feststellung des Zustandes „Sicherheitsparametrierung“ eines F-Gerätes oder F-Moduls mit Hilfe des Feldes IM4 (Signatur) innerhalb der I&M-Funktion (9.6.2);
- g) Literaturverweise auf den neuesten Stand gebracht.

Frühere Ausgaben

DIN EN 61784-3-3: 2008-11

Nationaler Anhang NA (informativ)

3.1 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

3.1.1 Allgemeine Begriffe

3.1.1.1

Verfügbarkeit (en: availability)

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

3.1.1.2

Black Channel (en: black channel)

Kommunikationskanal ohne verfügbaren Nachweis des Entwurfs oder der Validierung nach IEC 61508

3.1.1.3

Kommunikationskanal (en: communication channel)

logische Verbindung zwischen zwei Endpunkten in einem *Kommunikationssystem*

3.1.1.4

Kommunikationssystem (en: communication system)

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

3.1.1.5

Verbindung (en: connection)

logische Verbindung zwischen zwei Anwendungsobjekten in demselben oder in unterschiedlichen Geräten

3.1.1.6

CRC (en: Cyclic Redundancy Check (CRC))

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

<Methode> Prozedur zur Berechnung der redundanten Daten

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

ANMERKUNG 2 Siehe auch [32], [33]¹⁾.

3.1.1.7

Fehler (error)

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

[IEC 61508-4:2010²⁾], [IEC 61158]

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

¹⁾ Zahlen in rechteckigen Klammern beziehen sich auf die Literaturhinweise.

²⁾ Noch zu veröffentlichen.

ANMERKUNG 2 Fehler führen nicht notwendigerweise zu einem *Ausfall* oder einem *Fehlzustand*.

3.1.1.8

Ausfall (en: failure)

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

ANMERKUNG 1 Die Definition in IEC 61508-4 ist die gleiche, jedoch mit zusätzlichen Anmerkungen.

[IEC 61508-4:2010, modifiziert], [ISO/IEC 2382-14.01.11, modifiziert]

ANMERKUNG 2 Ein Ausfall kann auf einen *Fehler* zurückzuführen sein (z. B. ein Problem des Hardware-/Software-entwurfs oder eine Nachrichtenstörung).

3.1.1.9

Fehlzustand (en: fault)

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

ANMERKUNG IEC 191-05-01 definiert „fault“ als einen Zustand, der durch das Unvermögen gekennzeichnet ist, eine geforderte Funktion auszuführen, jedoch nicht ein Unvermögen während vorbeugender Instandhaltung, anderer geplanter Aktionen oder aufgrund fehlender externer Betriebsmittel.

[IEC 61508-4:2010, modifiziert], [ISO/IEC 2382-14.01.10, modifiziert]

3.1.1.10

Feldbus (en: fieldbus)

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

3.1.1.11

Feldbussystem (en: fieldbus system)

System mit einem *Feldbus* und angeschlossenen Geräten

3.1.1.12

Telegrammrahmen (frame)

veraltetes Synonym für DLPDU

3.1.1.13

Blockprüfzeichenfolge (en: Frame Check Sequence (FCS))

redundante Daten, mittels Hash-Funktion aus einem Block von Daten in einer DLPDU (Telegrammrahmen) abgeleitet und mit diesen zusammen zur Aufdeckung von Datenverfälschungen gespeichert oder übertragen

ANMERKUNG 1 Eine FCS kann z. B. mittels einer CRC oder einer anderen Hash-Funktion abgeleitet werden.

ANMERKUNG 2 Siehe auch [32], [33].

3.1.1.14

Hash-Funktion (en: hash function)

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

ANMERKUNG 1 Hash-Funktionen können zur Aufdeckung von Datenverfälschung eingesetzt werden.

ANMERKUNG 2 Gebräuchliche Hash-Funktionen schließen Parity-Bit, Quersummen oder CRC mit ein.

[IEC/TR 62210, modifiziert]

3.1.1.15

Gefährdung (en: hazard)

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

3.1.1.16

Master (en: master)

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

3.1.1.17

Nachricht (en: message)

geordnete Folge von Oktetts, bestimmt für die Übermittlung von Informationen

[ISO/IEC 2382-16.02.01, modifiziert]

3.1.1.18

Fehlauslösung (en: nuisance trip)

unberechtigte Auslösung ohne schädliche Wirkung

ANMERKUNG Interne außergewöhnliche Fehler können z. B. in Kommunikationssystemen wie Funkübertragung durch zu viele Wiederholungen unter Störeinfluss auftreten.

3.1.1.19

Wiederholungsprüfung (en: proof test)

wiederkehrende Prüfung zur Aufdeckung von Ausfällen in einem *sicherheitsbezogenen System*, sodass nötigenfalls eine Reparatur das System in einen „Wie-Neu“-Zustand bringen oder so nah wie unter praktischen Gesichtspunkten möglich an diesen Zustand heranbringen kann

ANMERKUNG Eine Wiederholungsprüfung ist zur Bestätigung vorgesehen, dass sich das sicherheitsbezogene System in einem Zustand befindet, der die festgelegte Sicherheitsintegrität garantiert.

[IEC 61508-4 und IEC 62061, modifiziert]

3.1.1.20

Performance Level (PL) (en: performance level (PL))

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

[ISO 13849-1]

3.1.1.21

Schutzkleinspannung (en: protective extra-low-voltage (PELV))

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

ANMERKUNG Ein PELV-Stromkreis ist wie ein SELV-Stromkreis, der mit Schutz Erde verbunden ist.

[IEC 61131-2]

3.1.1.22

Redundanz (en: redundancy)

Vorhandensein von mehr als den notwendigen Mitteln, damit eine Funktionseinheit eine geforderte Funktion ausführt oder damit Daten eine Information darstellen können

ANMERKUNG Die Definition in IEC 61508-4 ist die gleiche, jedoch mit zusätzlichen Beispielen und Anmerkungen.

[IEC 61508-4:2010, modifiziert], [ISO/IEC 2382-14.01.12, modifiziert]

3.1.1.23**Zuverlässigkeit (en: reliability)**

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

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

ANMERKUNG 2 Der Begriff „Zuverlässigkeit“ wird ebenfalls zur Kennzeichnung der Überlebenswahrscheinlichkeit (en: Reliability Performance) genutzt und durch die Wahrscheinlichkeit bemessen.

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

ANMERKUNG 4 Zuverlässigkeit unterscheidet sich von Verfügbarkeit.

[IEC 62059-11, modifiziert]

3.1.1.24**Risiko (en: risk)**

Kombination aus der Wahrscheinlichkeit, mit der ein Schaden auftritt, und dem Ausmaß dieses Schadens

ANMERKUNG Für die weitere Diskussion dieses Konzepts siehe IEC 61508-5:2010³⁾, Anhang A.

[IEC 61508-4:2010], [ISO/IEC Guide 51:1999, Definition 3.2]

3.1.1.25**Sicherheitskommunikationsschicht (en: safety communication layer (SCL))**

Kommunikationsschicht, die sämtliche notwendigen Mittel beinhaltet, um die sichere Übertragung von Daten entsprechend den Anforderungen in IEC 61508 zu gewährleisten

3.1.1.26**sichere Verbindung (en: safety connection)**

Verbindung, welche das Sicherheitsprotokoll für Kommunikationstätigkeiten nutzt

3.1.1.27**Sicherheitsdaten (en: safety data)**

Daten, die in einem Sicherheitsnetzwerk unter Nutzung eines Sicherheitsprotokolls übertragen wurden

ANMERKUNG Die Sicherheitskommunikationsschicht garantiert nicht sichere Daten an sich, sondern nur den gesicherten Transport.

3.1.1.28**Sicherheitsgerät (en: safety device)**

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

3.1.1.29**Sicherheitskleinspannung (en: safety extra-low-voltage (SELV))**

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

ANMERKUNG Ein SELV-Stromkreis ist nicht mit Schutz Erde verbunden.

[IEC 61131-2]

³⁾ Noch zu veröffentlichen.

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

ANMERKUNG Die Definition in IEC 61508-4 ist die gleiche, jedoch mit einem zusätzlichen Beispiel und einer Referenz.
[IEC 61508-4:2010, modifiziert]

3.1.1.31 Reaktionszeit einer Sicherheitsfunktion (en: safety function response time (SFRT))

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

ANMERKUNG Dieses Konzept wird in IEC 61784-3:2010⁴⁾, 5.2.4, eingeführt und von den in diesem Normteil aufgeführten funktional sicheren Kommunikationsprofilen verwendet.

3.1.1.32

Sicherheits-Integritätslevel (en: safety integrity level (SIL))

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

ANMERKUNG 1 Die Ausfallgrenzwerte (siehe IEC 61508-4:2010, 3.5.17) für die vier Sicherheits-Integritätslevel sind in den Tabellen 2 und 3 in IEC 61508-1:2010⁵⁾ festgelegt.

ANMERKUNG 2 Sicherheits-Integritätslevel werden zur Festlegung der Anforderungen an die Sicherheitsintegrität der Sicherheitsfunktionen verwendet, die den sicherheitsbezogenen E/E/PE-Systemen zugeordnet werden.

ANMERKUNG 3 Ein Sicherheits-Integritätslevel (SIL) ist keine Eigenschaft eines Systems, Teilsystems, Elements oder Bauteils. Die korrekte Deutung des Ausdrucks „sicherheitsbezogenes System mit SIL n“ (wobei „n“ 1, 2, 3 oder 4 ist) ist, dass das System potentiell in der Lage ist, Sicherheitsfunktionen mit einem Sicherheits-Integritätslevel bis zu „n“ zu unterstützen.

[IEC 61508-4:2010]

3.1.1.33

Sicherheitsmaßnahme (en: safety measure)

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

ANMERKUNG 1 In der Praxis werden mehrere Sicherheitsmaßnahmen kombiniert, um den geforderten Sicherheits-Integritätslevel zu erzielen.

ANMERKUNG 2 Kommunikationsfehler und zugehörige Sicherheitsmaßnahmen sind ausführlich in IEC 61784-3:2010, 5.3 und 5.4, beschrieben.

3.1.1.34

sicherheitsbezogene Anwendung (safety-related application)

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

3.1.1.35

sicherheitsbezogenes System (en: safety-related system)

System, welches *Sicherheitsfunktionen* nach IEC 61508 ausführt

⁴⁾ In Bearbeitung.

⁵⁾ Noch zu veröffentlichen.

3.1.1.36**Slave (en: slave)**

passive Kommunikationseinheit, die Nachrichten empfangen und sie als Antwort an andere Kommunikationseinheiten, seien es Master oder Slaves, senden kann

3.1.1.37**unberechtigte Auslösung (en: spurious trip)**

Auslösung in einem Sicherheitssystem ohne Prozessanforderung

3.1.2 CPF 3: Zusätzliche Begriffe**3.1.2.1****Bit (Binärziffer) (en: bit (Binary Digit))**

verschlüsselte Binärinformation ohne eine technische Einheit

3.1.2.2**Codename (en: codename)**

eindeutige Identifikation zwischen sicheren Kommunikations-Peers

ANMERKUNG Beispiel für die *Verbindungsauthentizität*, wie in IEC 61784-3 beschrieben.

3.1.2.3**Konfiguration (en: configuration)**

Festlegung der standardmäßigen Kommunikationsverbindungen und Kommunikationsparameter für Bus-einheiten einer bestimmten Anwendung

ANMERKUNG Die Konfiguration für eine sichere Kommunikation umfasst die Festlegung der sicheren Verbindungen und F-Parameter für sicherheitsbezogene Buseinheiten einer bestimmten sicherheitsbezogenen Anwendung.

3.1.2.4**fortlaufende Nummer (en: consecutive number)**

Mittel, um die Vollständigkeit und richtige Reihenfolge der übertragenen Sicherheits-PDUs zu gewährleisten

ANMERKUNG 1 Beispiel für eine *Laufnummer* wie in IEC 61784-3 beschrieben.

ANMERKUNG 2 Die fortlaufende Nummer kann mit jeder Sicherheits-PDU (V1-Modus) oder nur über eine übertragene CRC-Signatur gesichert übertragen werden.

3.1.2.5**CPD-Tool (en: CPD-Tool)**

zugehöriges Programm in Service-Rechnern, das mit dem Feldbus zum Zweck der Konfiguration, Parametrisierung und Diagnose bestimmter Feldgeräte verbunden ist

3.1.2.6**Zyklus (en: cycle)**

Intervall, in dem eine Liste von Anweisungen oder eine Aktivität wiederholt und ununterbrochen ausgeführt wird

3.1.2.7**Gerätezugangspunkt (en: device access point (DAP))**

Element, das verwendet wird, um ein modulares E/A-Gerät als Einheit zu adressieren

ANMERKUNG Üblicherweise als Kopfstation bezeichnet.

3.1.2.8**Geräterückmeldungszeit (en: device acknowledgement time (DAT))**

benötigte Zeit in einem F-Gerät für das Starten des Empfangs einer Sicherheits-PDU mit einer laufenden Nummer im DAP bis zu dem Zeitpunkt, an dem die entsprechende Sicherheits-PDU als Antwort generiert und an den DAP zurückgegeben wurde

3.1.2.9

Treiber (en: driver)

Softwaremodul, das für die Abstraktion der Hardware in Bezug auf die restliche Anwendungssoftware verwendet wird

3.1.2.10

ausfallsicher (en: fail-safe (F))

Fähigkeit eines Systems, Gefährdungen bei entsprechenden technischen oder organisatorischen Maßnahmen entweder deterministisch oder indem das Risiko auf ein toleriertes Maß verringert wird, zu verhindern

3.1.2.11

ausfallsichere Werte (en: fail-safe values (FV))

Werte, die anstelle von Prozesswerten ausgegeben werden, wenn die Sicherheitsfunktion auf einen ausfallsicheren Zustand festgelegt wurde

ANMERKUNG In diesem Normteil müssen die ausfallsicheren Werte (FV) immer auf „0“ festgelegt werden.

3.1.2.12

ausfallsicherer Zustand (en: fail-safe state)

Betriebsmodus einer Sicherheitsfunktion oder eines Endelements (Aktor), in dem Gefährdungen bei entsprechenden technischen Maßnahmen entweder deterministisch oder indem das Risiko auf ein toleriertes Maß verringert wird, verhindert werden

ANMERKUNG In Abhängigkeit von der bestimmten Sicherheitsfunktion stellt das Abschalten möglicherweise nicht die einzige Möglichkeit für einen ausfallsicheren Zustand dar.

3.1.2.13

F-Gerät (en: F-Device)

passiver CP 3/RTE-Kommunikations-Peer, der das FSCP 3/1-Protokoll ausführen kann und der üblicherweise von dem F-Host für den Datenaustausch aktiviert wird

3.1.2.14

F-Treiber (en: F-Driver)

Software zur Verwaltung der Sicherheits-PDUs in F-Hosts und F-Geräten entsprechend der FSCP 3/1-Spezifikationen

3.1.2.15

F-Host (en: F-Host)

Datenverarbeitungseinheit, die das FSCP 3/1-Protokoll ausführen kann und die den Black Channel bedient

ANMERKUNG Hierbei handelt es sich üblicherweise um einen PLC oder einen IPC mit einem entsprechenden Betriebssystem.

3.1.2.16

F-Modul (en: F-Module)

passiver Kommunikations-Peer in einem modularen F-Gerät oder F-Slave, der das FSCP 3/1-Protokoll ausführen kann und der üblicherweise von dem F-Host für den Datenaustausch aktiviert wird

ANMERKUNG Hierbei handelt es sich üblicherweise um ein sicherheitsbezogenes Eingabe- oder Ausgabemodul.

3.1.2.17

F-Slave (en: F-Slave)

passiver CP 3/1- oder CP 3/2-Kommunikations-Peer, der das FSCP 3/1-Protokoll ausführen kann und der üblicherweise von dem F-Host für den Datenaustausch aktiviert wird

3.1.2.18

Fehlreaktion (en: fault reaction)

Angabe einer Kommunikationsfehlfunktion durch Setzen der Fehlerbits im Status-Byte und einer entsprechenden automatischen sicheren Reaktion innerhalb der Komponenten

ANMERKUNG

Innerhalb einer F-Ausgabe: Abschalten der Ausgabegeräte und/oder automatische sichere Reaktion der Aktoreinheit.

Innerhalb einer F-CPU: Entsprechende Reaktion des Benutzerprogramms möglich. F-E/A-Daten sind auf ausfallsichere Werte festzulegen.

Innerhalb einer F-Eingabe: Bei Kommunikationsfehlern, die durch die F-Eingabe ermittelt wurden: Fehlerbits werden im Status-Byte gesetzt.

Bei Kommunikationsfehlern, die durch den F-Host ermittelt wurden: F-Eingabedaten sind auf ausfallsichere Werte festzulegen.

3.1.2.19**Funktionsblock (FB) (en: function block (FB))**

eigenständiger Programmteil mit besonderer Funktionalität

3.1.2.20**Hostrückmeldungszeit (en: host acknowledgement time (HAT))**

Zeit, die in einem F-Host für das Starten des Empfangs einer Sicherheits-PDU mit einer bestimmten laufenden Nummer bis zu dem Zeitpunkt, an dem die entsprechende Sicherheits-PDU mit einer inkrementierten laufenden Nummer generiert und an den Master bzw. E/A-Controller zurückgegeben wurde, benötigt wird

3.1.2.21**E/A-Controller (en: IO-Controller)**

aktive Kommunikationseinheit, die CP 3/RTE-Kommunikationsaktivitäten anderer Einheiten, seien es E/A-Controller oder E/A-Geräte, einrichten und festlegen kann

ANMERKUNG Im CP 3/1 entspricht diese Task einem Master Klasse 1.

3.1.2.22**E/A-Gerät (en: IO-Device)**

passive Kommunikationseinheit, die Nachrichten empfangen und sie als Antwort an eine andere CP 3/RTE-Kommunikationseinheit, sei es ein E/A-Controller oder ein anderes E/A-Gerät, senden kann

ANMERKUNG Im CP 3/1 entspricht diese Task einem Slave.

3.1.2.23**E/A-Modul (en: IO-Module)**

adressierbare untergeordnete Eingabe/Ausgabe-Einheit in einem modularen E/A-Gerät

3.1.2.24**E/A-Supervisor (en: IO-Supervisor)**

Engineering-Station, die Daten aus einem E/A-Gerät lesen und auf ein E/A-Gerät schreiben kann

ANMERKUNG Ein E/A-Supervisor wird zu Installations- und Diagnosezwecken verwendet. Im Gegensatz zu einem E/A-Controller übernimmt der E/A-Supervisor keine aktive Rolle während des Hochfahrens eines E/A-Systems. Ein E/A-Supervisor ist nicht Teil des E/A-Systems.

3.1.2.25**E/A-System (en: IO-System)**

E/A-Controller und die zugehörigen E/A-Geräte

3.1.2.26**iParameter (en: iParameter)**

individuelle oder technologiespezifische Parameter für F-Geräte

ANMERKUNG Typische iParameter sind die Koordinaten der Schutzzone eines Laserscanners.

3.1.2.27

iPar-Server (en: iPar-Server)

genormter Mechanismus, mit dem individuelle oder technologiespezifische Parameter für F-Geräte im Standardteil eines F-Hosts oder seines gesteuerten Teilsystems gespeichert und abgerufen werden können

3.1.2.28

Master (Klasse 1) (en: master (class 1))

aktiver CP 3/1-Kommunikations-Peer, der Slaves für den Datenaustausch aktiviert

3.1.2.29

Prozesswerte (en: process values (PV))

Eingabe- und Ausgabedaten (in einer Sicherheits-PDU), die für die Steuerung eines automatisierten Prozesses erforderlich sind

3.1.2.30

Wertstatus (en: qualifier)

zusätzliche kennzeichnende Bits in *Prozesswerten*, die den Status jeder individuellen Eingabe angeben

3.1.2.31

gemeinsame E/A (en: shared I/O)

Eingaben und Ausgaben in Feldgeräten, auf die über mehrere Controller zugegriffen werden kann

ANMERKUNG Obwohl gemeinsame E/A im CP 3/RTE zulässig ist, ist sie im FSCP 3/1 nicht erlaubt.

3.1.2.32

Toggle-Bit (en: toggle bit)

ein Bit des Control- und Status-Bytes, das die (virtuellen) laufenden Zähler sowohl im F-Host als auch im F-Gerät synchronisiert

3.1.2.33

USB (en: universal serial bus (USB))

externer Busstandard, der Datenübertragungsraten von bis zu 480 Mbit/s unterstützt

ANMERKUNG USB ersetzt serielle und parallele Computerports und wird für schnelle Direktverbindungen zwischen Service-Rechnern und Feldgeräten verwendet.

3.1.2.34

V1-Modus (en: V1-mode)

FSCP 3/1-Dienste und Protokoll nach [48]

3.1.2.35

V2-Modus (en: V2-mode)

FSCP 3/1-Dienste und Protokoll nach diesem Normteil

3.1.2.36

VLAN-Tag (en: VLAN tag)

Erweiterung innerhalb Ethernet-Nachrichten, die es bestimmten Benutzergruppen in großen Netzwerken ermöglicht, ihre eigenen virtuellen Netzwerke über Prioritäten und VLAN-IDs unter Verwendung geeigneter Switches auszuführen, ohne sich gegenseitig zu beeinflussen

English version

**Industrial communication networks -
Profiles -
Part 3-3: Functional safety fieldbuses -
Additional specifications for CPF 3
(IEC 61784-3-3:2010)**

Réseaux de communication industriels -
Partie 3-3: Bus de terrain à sécurité
fonctionnelle -
Spécifications complémentaires
pour le CPF 3
(CEI 61784-3-3:2010)

Industrielle Kommunikationsnetze -
Profile -
Teil 3-3: Funktional sichere Übertragung
bei Feldbussen -
Zusätzliche Festlegungen
für die Kommunikationsprofilfamilie 3
(IEC 61784-3-3:2010)

This European Standard was approved by CENELEC on 2010-07-01. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the Central Secretariat 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 Central Secretariat 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, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and the United Kingdom.

CENELEC

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

Management Centre: Avenue Marnix 17, B - 1000 Brussels

Foreword

The text of document 65C/591A/FDIS, future edition 2 of IEC 61784-3-3, 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 was approved by CENELEC as EN 61784-3-3 on 2010-07-01.

This European Standard supersedes EN 61784-3-3:2008.

The main technical changes with respect to EN 61784-3-3:2008 are listed below:

- updates in relation with changes in EN 61784-3;
- introduction of a secondary watchdog timer (F_WD_Time_2) to cover the use cases 'configuration-in-run', or 'maintenance of fault tolerance systems', or both (7.1.3, 7.2.3, 7.2.6, 8.1.1, 8.1.4, 8.1.6.2);
- missing GSDL definitions conveyed from other approved documents (8.3.2.1);
- missing CRC signature calculation for a GSD conveyed from other approved documents (8.3.3.3);
- constraints for the parameter value assignment of the primary watchdog timer 'F_WD_Time' (9.3.3);
- identification of the safety parameterization state of an F-Device or F-Module via field IM4 (signature) within the I&M functions (9.6.2);
- updated documents in bibliography.

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

The following dates were fixed:

- | | | |
|--|-------|------------|
| – latest date by which the EN has to be implemented
at national level by publication of an identical
national standard or by endorsement | (dop) | 2011-04-01 |
| – latest date by which the national standards conflicting
with the EN have to be withdrawn | (dow) | 2013-07-01 |

Annex ZA has been added by CENELEC.

Endorsement notice

The text of the International Standard IEC 61784-3-3:2010 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 60870-5-1	NOTE	Harmonized as EN 60870-5-1.
IEC 61158 series	NOTE	Harmonized in EN 61158 series (not modified).
IEC 61496 series	NOTE	Harmonized in EN 61496 series (partially modified).
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 61508-6:2010	NOTE	Harmonized as EN 61508-6:2010 (not modified).
IEC 61784-5 series	NOTE	Harmonized in EN 61784-5 series (not modified).
IEC 61800-5-2	NOTE	Harmonized as EN 61800-5-2.
IEC 61804 series	NOTE	Harmonized in EN 61804 series (not modified).
ISO 10218-1	NOTE	Harmonized as EN ISO 10218-1.
ISO 12100-1	NOTE	Harmonized as EN ISO 12100-1.

CONTENTS

0	Introduction	10
0.1	General	10
0.2	Patent declaration	12
1	Scope	13
2	Normative references	13
3	Terms, definitions, symbols, abbreviated terms and conventions	15
3.1	Terms and definitions	15
3.1.1	Common terms and definitions	15
3.1.2	CPF 3: Additional terms and definitions	20
3.2	Symbols and abbreviated terms	23
3.2.1	Common symbols and abbreviated terms	23
3.2.2	CPF 3: Additional symbols and abbreviated terms	24
3.3	Conventions	25
4	Overview of FSCP 3/1 (PROFIsafe™)	25
5	General	28
5.1	External documents providing specifications for the profile	28
5.2	Safety functional requirements	28
5.3	Safety measures	29
5.4	Safety communication layer structure	30
5.4.1	Principle of FSCP 3/1 safety communications	30
5.4.2	CPF 3 communication structures	31
5.5	Relationships with FAL (and DLL, PhL)	34
5.5.1	Device model	34
5.5.2	Application and communication relationships	34
5.5.3	Message format	36
5.5.4	Data types	36
6	Safety communication layer services	37
6.1	F-Host services	37
6.2	F-Device services	39
6.3	Diagnosis	41
6.3.1	Safety alarm generation	41
6.3.2	F-Device safety layer diagnosis including the iPar-Server	41
7	Safety communication layer protocol	42
7.1	Safety PDU format	42
7.1.1	Safety PDU structure	42
7.1.2	Safety I/O data	43
7.1.3	Status and Control Byte	43
7.1.4	(Virtual) Consecutive Number	44
7.1.5	CRC2 Signature	46
7.1.6	Appended standard I/O data	47
7.2	FSCP 3/1 behavior	47
7.2.1	General	47
7.2.2	F-Host state diagram	47
7.2.3	F-Device state diagram	51

7.2.4	Sequence diagrams.....	55
7.2.5	Timing diagram for a counter reset.....	61
7.2.6	Monitoring of safety times	61
7.3	Reaction in the event of a malfunction.....	64
7.3.1	Repetition.....	64
7.3.2	Loss	65
7.3.3	Insertion.....	65
7.3.4	Incorrect sequence.....	65
7.3.5	Corruption of safety data.....	65
7.3.6	Delay	66
7.3.7	Masquerade	66
7.3.8	Memory failures within switches.....	66
7.3.9	Network boundaries and router.....	67
7.4	F-Startup and change coordination	68
7.4.1	Standard startup procedure.....	68
7.4.2	iParameter assignment deblocking.....	68
8	Safety communication layer management	69
8.1	F-Parameter	69
8.1.1	Summary.....	69
8.1.2	F_Source/Destination_Address (codename).....	69
8.1.3	F_WD_Time (F-Watchdog time).....	69
8.1.4	F_WD_Time_2 (secondary F-Watchdog time).....	70
8.1.5	F_Prm_Flag1 (Parameters for the safety layer management).....	70
8.1.6	F_Prm_Flag2 (Parameters for the safety layer management).....	72
8.1.7	F_iPar_CRC (value of iPar_CRC across iParameters).....	73
8.1.8	F_Par_CRC (CRC1 across F-Parameters)	73
8.1.9	Structure of the F-Parameter record data object	74
8.1.10	F-Data fraction.....	74
8.2	iParameter and iPar_CRC.....	74
8.3	Safety parameterization	75
8.3.1	Objectives	75
8.3.2	GSDL and GSDML safety extensions	76
8.3.3	Securing safety parameters and GSD data	77
8.4	Safety configuration	80
8.4.1	Securing the safety I/O data description (CRC7).....	80
8.4.2	Dataltem data type section examples	81
8.5	Data type information usage.....	84
8.5.1	F-Channel driver	84
8.5.2	Rules for standard F-Channel drivers	85
8.5.3	Recommendations for F-Channel drivers	86
8.6	Safety parameter assignment mechanisms	87
8.6.1	F-Parameter assignment.....	87
8.6.2	General iParameter assignment.....	87
8.6.3	System integration requirements for iParameterization tools.....	88
8.6.4	iPar-Server.....	90
9	System requirements	99
9.1	Indicators and switches	99
9.2	Installation guidelines	99

9.3	Safety function response time	99
9.3.1	Model	99
9.3.2	Calculation and optimization	101
9.3.3	Adjustment of watchdog times for FSCP 3/1	103
9.3.4	Engineering tool support	104
9.3.5	Retries (repetition of messages)	104
9.4	Duration of demands.....	105
9.5	Constraints for the calculation of system characteristics	106
9.5.1	Probabilistic considerations	106
9.5.2	Safety related constraints.....	108
9.5.3	Non safety related constraints (availability)	109
9.6	Maintenance	109
9.6.1	F-Module commissioning / replacement	109
9.6.2	Identification and maintenance functions.....	109
9.7	Safety manual.....	110
9.8	Wireless transmission channels	111
9.8.1	Black channel approach	111
9.8.2	Availability	111
9.8.3	Security measures.....	111
9.8.4	Stationary and mobile applications	114
9.9	Conformance classes.....	114
10	Assessment	115
10.1	Safety policy	115
10.2	Obligations	115
Annex A (informative) Additional information for functional safety communication profiles of CPF 3.....		116
A.1	Hash function calculation.....	116
A.2	Response time measurements	118
Annex B (informative) Information for assessment of the functional safety communication profiles of CPF 3.....		122
Bibliography		123
Annex ZA (normative) Normative references to international publications with their corresponding European publications		127
Table 1 – Deployed measures to master errors		29
Table 2 – Data types used for FSCP 3/1		36
Table 3 – Safety layer diagnosis messages		41
Table 4 – F-Host states and transitions		49
Table 5 – F-Device states and transitions.....		53
Table 6 – SIL monitor times		64
Table 7 – Remedies for switch failures.....		67
Table 8 – Safety network boundaries		68
Table 9 – GSDL keywords for F-Parameters and F-I/O structures.....		76
Table 10 – I/O data structure items (Version 2).....		81
Table 11 – Sample F-Channel drivers		85
Table 12 – Requirements for iParameterization.....		88
Table 13 – Specifier for the iPar-Server Request.....		93

Table 14 – Structure of the Read_RES_PDU ("read record")	94
Table 15 – Structure of the Write_REQ_PDU ("write record")	95
Table 16 – Structure of the Pull_RES_PDU ("Pull")	95
Table 17 – Structure of the Push_REQ_PDU ("Push")	95
Table 18 – iPar-Server states and transitions	97
Table 19 – iPar-Server management measures	98
Table 20 – Information to be included in the safety manual	110
Table 21 – Security measures for WLAN (IEEE 802.11i)	112
Table 22 – Security measures for Bluetooth (IEEE 802.15.1)	113
Table 23 – F-Host conformance class requirements	114
Table A.1 – The table "Crctab24" for 24 bit CRC signature calculations.....	117
Table A.2 – The table "Crctab32" for 32 bit CRC signature calculations.....	118
Figure 1 – Relationships of IEC 61784-3 with other standards (machinery).....	10
Figure 2 – Relationships of IEC 61784-3 with other standards (process)	11
Figure 3 – Basic communication preconditions for FSCP 3/1	26
Figure 4 – Structure of an FSCP 3/1 safety PDU.....	27
Figure 5 – Safety communication modes.....	28
Figure 6 – Standard CPF 3 transmission system.....	30
Figure 7 – Safety layer architecture.....	31
Figure 8 – Basic communication layers.....	31
Figure 9 – Multiport switch bus structure.....	32
Figure 10 – Linear bus structure	32
Figure 11 – Crossing network borders with routers.....	33
Figure 12 – Complete safety transmission paths	33
Figure 13 – Device model.....	34
Figure 14 – Application relationships of a modular device	35
Figure 15 – Application and communication relationships (AR/CR)	35
Figure 16 – Message format	36
Figure 17 – FSCP 3/1 communication structure	37
Figure 18 – F user interface of F-Host driver instances.....	38
Figure 19 – F-Device driver interfaces	40
Figure 20 – Safety PDU for CPF 3.....	42
Figure 21 – Status Byte.....	43
Figure 22 – Control Byte	44
Figure 23 – The Toggle Bit function.....	45
Figure 24 – F-Device Consecutive Number	45
Figure 25 – CRC2 generation (F-Host output).....	46
Figure 26 – Details of the CRC2 calculation (reverse order).....	47
Figure 27 – Safety layer communication relationship.....	47
Figure 28 – F-Host state diagram	48
Figure 29 – F-Device state diagram.....	52

Figure 30 – Interaction F-Host / F-Device during start-up	55
Figure 31 – Interaction F-Host / F-Device during F-Host power off → on.....	56
Figure 32 – Interaction F-Host / F-Device with delayed power on.....	57
Figure 33 – Interaction F-Host / F-Device during power off → on	58
Figure 34 – Interaction F-Host / F-Device while host recognizes CRC error	59
Figure 35 – Interaction F-Host / F-Device while device recognizes CRC error	60
Figure 36 – Impact of the counter reset signal	61
Figure 37 – Monitoring the message transit time F-Host ↔ F-Output.....	62
Figure 38 – Monitoring the message transit time F-Input ↔ F-Host	62
Figure 39 – Extended watchdog time on request.....	64
Figure 40 – F-Parameter data and CRC	65
Figure 41 – iParameter assignment deblocking by the F-Host.....	68
Figure 42 – Effect of F_WD_Time_2	70
Figure 43 – F_Prm_Flag1	70
Figure 44 – F_Check_SeqNr	71
Figure 45 – F_Check_iPar	71
Figure 46 – F_SIL.....	71
Figure 47 – F_CRC_Length	72
Figure 48 – F_Prm_Flag2	72
Figure 49 – F_Block_ID.....	72
Figure 50 – F_Par_Version	73
Figure 51 – F-Parameter	74
Figure 52 – iParameter block	75
Figure 53 – F-Parameter extension within the GSDML specification	77
Figure 54 – CRC1 including iPar_CRC.....	78
Figure 55 – Algorithm to build CRC0 (GSDL)	79
Figure 56 – Algorithm to build CRC0 (GSDML)	80
Figure 57 – Dataltem section for F_IN_OUT_1.....	82
Figure 58 – Dataltem section for F_IN_OUT_2.....	83
Figure 59 – Dataltem section for F_IN_OUT_5.....	83
Figure 60 – Dataltem section for F_IN_OUT_6.....	84
Figure 61 – F-Channel driver as "glue" between F-Device and user program	85
Figure 62 – Layout example of an F-Channel driver.....	86
Figure 63 – F-Parameter assignment for simple F-Devices and F-Slaves.....	87
Figure 64 – F and iParameter assignment for complex F-Devices	88
Figure 65 – System integration of CPD-Tools	89
Figure 66 – iPar-Server mechanism (commissioning)	90
Figure 67 – iPar-Server mechanism (for example F-Device replacement)	91
Figure 68 – iPar-Server request coding ("status model")	92
Figure 69 – Coding of SR_Type	93
Figure 70 – iPar-Server request coding ("alarm model").....	94
Figure 71 – iPar-Server state diagram.....	96
Figure 72 – Example safety function with a critical response time path	100

Figure 73 – Simplified typical response time model	100
Figure 74 – Frequency distributions of typical response times of the model	101
Figure 75 – Context of delay times and watchdog times.....	102
Figure 76 – Timing sections forming the FSCP 3/1 F_WD_Time	103
Figure 77 – Frequency distribution of response times with message retries	104
Figure 78 – Retries with CP 3/1	105
Figure 79 – Retries with CP 3/RTE	105
Figure 80 – Residual error probabilities for the 24-bit polynomial.....	106
Figure 81 – Properness of the 32-bit polynomial for 52 octets	107
Figure 82 – Properness of the 32-bit polynomial for 132 octets.....	107
Figure 83 – Monitoring of corrupted messages	108
Figure 84 – Security for WLAN networks.....	111
Figure 85 – Security for Bluetooth networks	113
Figure A.1 – Typical "C" procedure of a cyclic redundancy check	116
Figure A.2 – Comparison of the response time model and a real application.....	119
Figure A.3 – Frequency distribution of measured response times	120
Figure A.4 – F-Host with standard and safety-related application programs	121

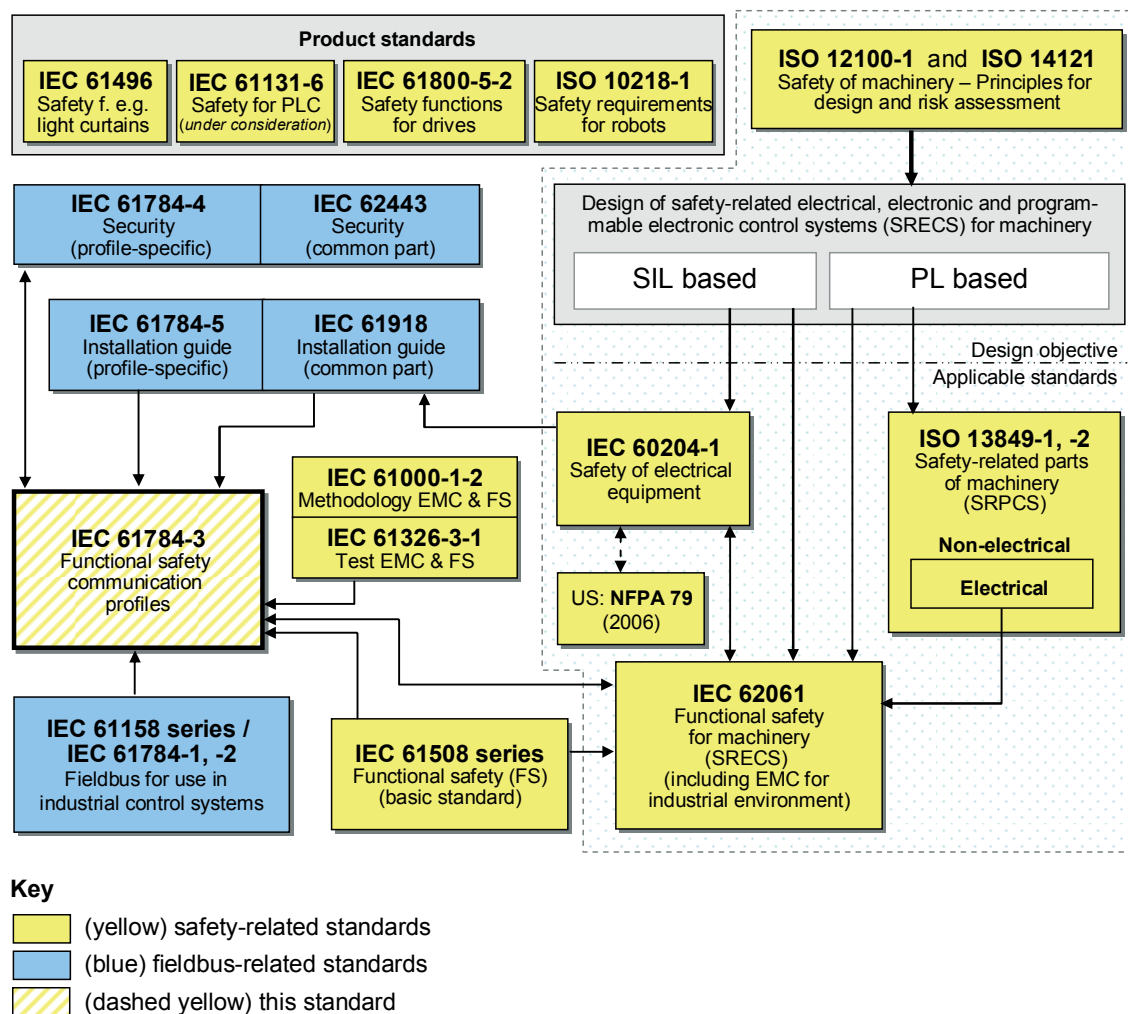
0 Introduction

0.1 General

The IEC 61158 fieldbus standard together with its companion standards IEC 61784-1 and IEC 61784-2 defines a set of communication protocols that enable distributed control of automation applications. Fieldbus technology is now considered well accepted and well proven. Thus many fieldbus enhancements are emerging, addressing not yet standardized areas such as real time, safety-related and security-related applications.

This standard explains the relevant principles for functional safety communications with reference to IEC 61508 series and specifies several safety communication layers (profiles and corresponding protocols) based on the communication profiles and protocol layers of IEC 61784-1, IEC 61784-2 and the IEC 61158 series. It does not cover electrical safety and intrinsic safety aspects.

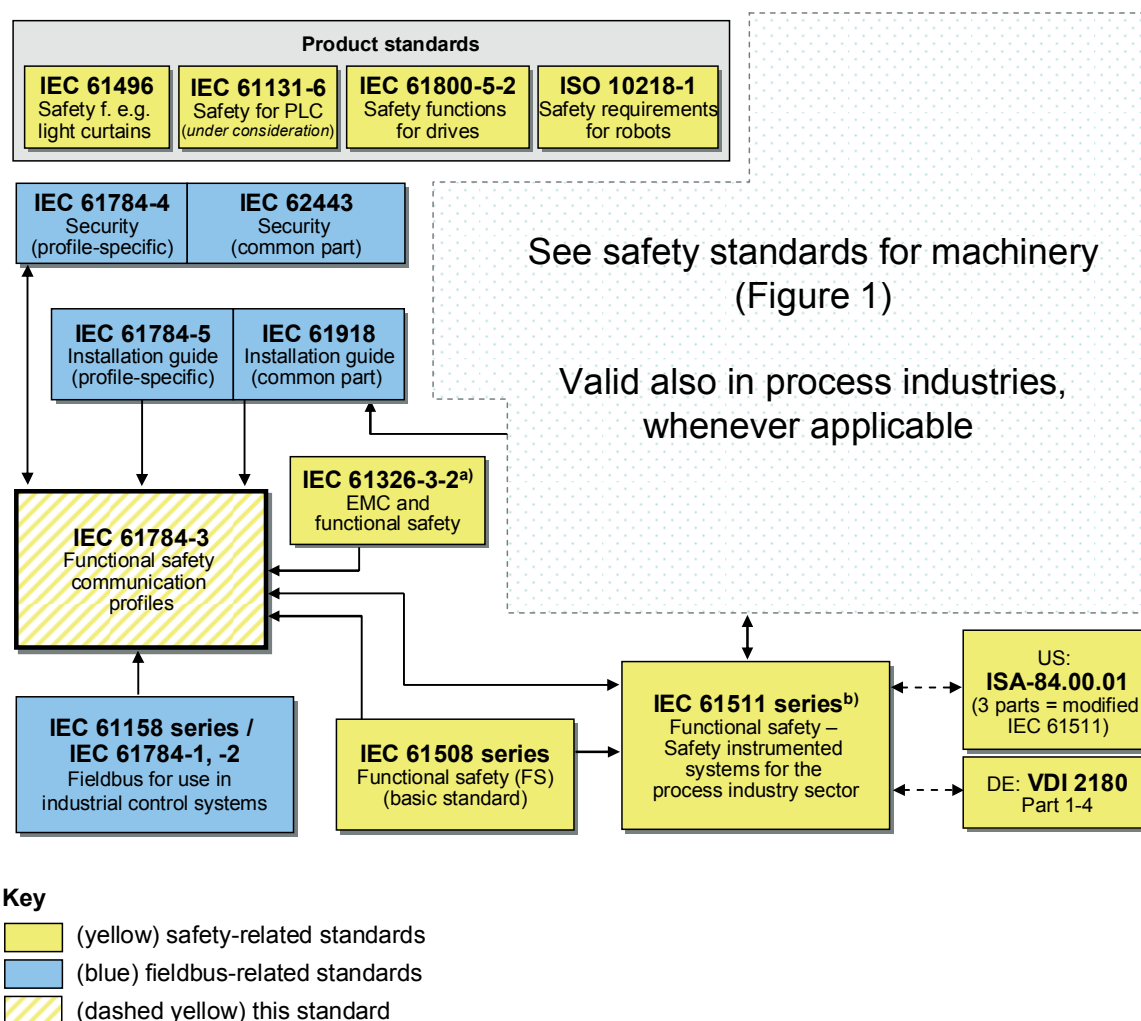
Figure 1 shows the relationships between this standard and relevant safety and fieldbus standards in a machinery environment.



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

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

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



^a For specified electromagnetic environments; otherwise IEC 61326-3-1.

^b EN ratified.

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

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

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

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

This standard describes:

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

0.2 Patent declaration

The International Electrotechnical Commission (IEC) draws attention to the fact that it is claimed that compliance with this document may involve the use of patents concerning the functional safety communication profiles for family 3 as follows, where the [xx] notation indicates the holder of the patent right:

EP1267270-A2	[SI]	Method for data transfer
WO00/045562-A1	[SI]	Method and device for determining the reliability of data carriers
WO99/049373-A1	[SI]	Shortened data message of an automation system
EP1686732	[SI]	Method and system for transmitting protocol data units
EP1802019	[SI]	Identification of errors in data transmission
EP1921525-A1	[SI]	Method for operation of a safety-related system

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

The holders of these patents rights have assured the IEC that they are willing to negotiate licences under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statement of the holders of these patent rights are registered with IEC.

Information may be obtained from:

[SI]	Siemens AG I IA AS FA TC 76187 Karlsruhe GERMANY
------	---

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

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES –

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

1 Scope

This part of the IEC 61784-3 series specifies a safety communication layer (services and protocol) based on CPF 3 of IEC 61784-1, IEC 61784-2 (CP 3/1, CP 3/2, CP 3/4, CP 3/5 and CP 3/6) and IEC 61158 Types 3 and 10. It identifies the principles for functional safety communications defined in IEC 61784-3 that are relevant for this safety communication layer.

NOTE 1 It does not cover electrical safety and intrinsic safety aspects. Electrical safety relates to hazards such as electrical shock. Intrinsic safety relates to hazards associated with potentially explosive atmospheres.

This part¹ defines mechanisms for the transmission of safety-relevant messages among participants within a distributed network using fieldbus technology in accordance with the requirements of IEC 61508 series² for functional safety. These mechanisms may be used in various industrial applications such as process control, manufacturing automation and machinery.

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

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

2 Normative references

The following referenced documents are indispensable for the application 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 60204-1, *Safety of machinery – Electrical equipment of machines – Part 1: General requirements*

IEC 61000-6-2, *Electromagnetic compatibility (EMC) – Part 6-2: Generic standards – Immunity for industrial environments*

IEC 61010-1, *Safety requirements for electrical equipment for measurement, control, and laboratory use – Part 1: General requirements*

IEC 61131-2, *Programmable controllers – Part 2: Equipment requirements and tests*

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

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

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

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

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

IEC 61158-4-3, *Industrial communication networks – Fieldbus specifications – Part 4-3: Data-link layer protocol specification – Type 3 elements*

IEC 61158-5-3, *Industrial communication networks – Fieldbus specifications – Part 5-3: Application layer service definition – Type 3 elements*

IEC 61158-5-10, *Industrial communication networks – Fieldbus specifications – Part 5-10: Application layer service definition – Type 10 elements*

IEC 61158-6-3, *Industrial communication networks – Fieldbus specifications – Part 6-3: Application layer protocol specification – Type 3 elements*

IEC 61158-6-10, *Industrial communication networks – Fieldbus specifications – Part 6-10: Application layer protocol specification – Type 10 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 61508-2, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*

IEC 61511 (all parts), *Functional safety – Safety instrumented systems for the process industry sector*

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

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

IEC 61784-3:2010³, *Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions*

IEC 61784-5-3, *Industrial communication networks – Profiles – Part 5: Installation of fieldbuses – Installation profiles for CPF 3*

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

IEC 62061, *Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems*

³ In preparation.

IEC 62280-1:2002, *Railway applications – Communication, signalling and processing systems – Part 1: Safety-related communication in closed transmission systems*

IEC 62280-2, *Railway applications – Communication, signalling and processing systems – Part 2: Safety-related communication in open transmission systems*

IEC/TR 62390, *Common automation device – Profile guideline*

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

ISO 13849-2, *Safety of machinery – Safety-related parts of control systems – Part 2: Validation*

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

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

3 Terms, definitions, symbols, abbreviated terms and conventions

3.1 Terms and definitions

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

3.1.1 Common terms and definitions

3.1.1.1

availability

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

3.1.1.2

black channel

communication channel without available evidence of design or validation according to IEC 61508

3.1.1.3

communication channel

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

3.1.1.4

communication system

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

3.1.1.5

connection

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

3.1.1.6

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

NOTE 2 See also [32], [33]⁴.

3.1.1.7

error

discrepancy between a computed, observed or measured value or condition and the true, specified or theoretically correct value or condition

[IEC 61508-4:2010⁵], [IEC 61158]

NOTE 1 Errors may be due to design mistakes within hardware/software and/or corrupted information due to electromagnetic interference and/or other effects.

NOTE 2 Errors do not necessarily result in a *failure* or a *fault*.

3.1.1.8

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 The definition in IEC 61508-4 is the same, with additional notes.

[IEC 61508-4:2010, modified], [ISO/IEC 2382-14.01.11, modified]

NOTE 2 Failure may be due to an *error* (for example, problem with hardware/software design or message disruption)

3.1.1.9

fault

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

NOTE IEC 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.

[IEC 61508-4:2010, modified], [ISO/IEC 2382-14.01.10, modified]

3.1.1.10

fieldbus

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

3.1.1.11

fieldbus system

system using a *fieldbus* with connected devices

3.1.1.12

frame

denigrated synonym for DLPDU

3.1.1.13

Frame Check Sequence (FCS)

redundant data derived from a block of data within a DLPDU (frame), using a hash function, and stored or transmitted together with the block of data, in order to detect data corruption

NOTE 1 An FCS can be derived using for example a CRC or other hash function.

NOTE 2 See also [32], [33].

⁴ Figures in square brackets refer to the bibliography.

⁵ To be published.

3.1.1.14

hash function

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

NOTE 1 Hash functions can be used to detect data corruption.

NOTE 2 Common hash functions include parity, checksum or CRC.
[IEC/TR 62210, modified]

3.1.1.15

hazard

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

3.1.1.16

master

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

3.1.1.17

message

ordered series of octets intended to convey information
[ISO/IEC 2382-16.02.01, modified]

3.1.1.18

nuisance trip

spurious trip with no harmful effect

NOTE Internal abnormal errors can be caused in communication systems such as wireless transmission, for example by too many retries in the presence of interferences.

3.1.1.19

proof test

periodic test performed to detect failures in a *safety-related system* so that, if necessary, the system can be restored to an “as new” condition or as close as practical to this condition

NOTE A proof test is intended to confirm that the safety-related system is in a condition that assures the specified safety integrity.

[IEC 61508-4 and IEC 62061, modified]

3.1.1.20

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
[ISO 13849-1]

3.1.1.21

protective extra-low-voltage (PELV)

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

NOTE A PELV circuit is similar to an SELV circuit that is connected to protective earth.

[IEC 61131-2]

3.1.1.22

redundancy

existence of means, in addition to the means which would be sufficient for a functional unit to perform a required function or for data to represent information

NOTE The definition in IEC 61508-4 is the same, with additional example and notes.

[IEC 61508-4:2010, modified], [ISO/IEC 2382-14.01.12, modified]

3.1.1.23

reliability

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

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

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

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

NOTE 4 Reliability differs from availability.

[IEC 62059-11, modified]

3.1.1.24

risk

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

NOTE For more discussion on this concept see Annex A of IEC 61508-5:2010⁶.

[IEC 61508-4:2010], [ISO/IEC Guide 51:1999, definition 3.2]

3.1.1.25

safety communication layer (SCL)

communication layer that includes all the necessary measures to ensure safe transmission of data in accordance with the requirements of IEC 61508

3.1.1.26

safety connection

connection that utilizes the safety protocol for communications transactions

3.1.1.27

safety data

data transmitted across a safety network using a safety protocol

NOTE The Safety Communication Layer does not ensure safety of the data itself, only that the data is transmitted safely.

3.1.1.28

safety device

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

3.1.1.29

safety extra-low-voltage (SELV)

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

⁶ To be published.

NOTE An SELV circuit is not connected to protective earth.

[IEC 61131-2]

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

NOTE The definition in IEC 61508-4 is the same, with an additional example and reference.

[IEC 61508-4:2010, modified]

3.1.1.31 safety function response time (SFRT)

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

NOTE This concept is introduced in IEC 61784-3:2010⁷, 5.2.4 and addressed by the functional safety communication profiles defined in this part.

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 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 61508-1:2010⁸.

NOTE 2 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 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.

[IEC 61508-4:2010]

3.1.1.33 safety measure

<this standard> measure to control possible communication *errors* that is designed and implemented in compliance with the requirements of IEC 61508

NOTE 1 In practice, several safety measures are combined to achieve the required safety integrity level.

NOTE 2 Communication *errors* and related safety measures are detailed in IEC 61784-3:2010, 5.3 and 5.4.

3.1.1.34 safety-related application

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

3.1.1.35 safety-related system

system performing *safety functions* according to IEC 61508

⁷ In preparation.

⁸ To be published.

3.1.1.36

slave

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

3.1.1.37

spurious trip

trip caused by the safety system without a process demand

3.1.2 CPF 3: Additional terms and definitions

3.1.2.1

bit (Binary Digit)

encoded binary information without a technical unit

3.1.2.2

codename

unique identification between safety communication peers

NOTE Instance of *connection authentication* as described in IEC 61784-3.

3.1.2.3

configuration

definition of the standard communication connections and communication parameters for bus entities of a particular application

NOTE The configuration for safety communication comprises the definition of the safety connections and F-Parameters for safety-related bus entities of a particular safety-related application.

3.1.2.4

consecutive number

means to ensure completeness and the right order of transmitted safety PDUs

NOTE 1 Instance of *sequence number* as described in IEC 61784-3.

NOTE 2 The consecutive number can be transmitted with each safety PDU (V1-mode) or only secured via the transmitted CRC signature (V2-mode).

3.1.2.5

CPD-Tool

dedicated program in service computers connected to the fieldbus for the purpose of configuration, parameterization and diagnosis of particular field devices

3.1.2.6

cycle

interval at which a list of instructions or an activity is repetitively and continuously executed

3.1.2.7

device access point (DAP)

item used to address a modular IO device as an entity

NOTE Usually this is called a head station.

3.1.2.8

device acknowledgement time (DAT)

elapsed time in an F-Device starting with the reception of a safety PDU with a new consecutive number in the device access point until an appropriate response safety PDU has been generated and returned to the device access point

3.1.2.9

driver

software module used for abstracting the hardware with respect to the remaining application software

3.1.2.10

fail-safe (F)

ability of a system that, by adequate technical or organizational measures, prevents from hazards either deterministically or by reducing the risk to a tolerable measure

3.1.2.11

fail-safe values (FV)

values which are issued instead of process values when the safety function is set to a fail-safe state

NOTE In this part, the fail-safe values (FV) shall always be set to "0".

3.1.2.12

fail-safe state

operational mode of a safety function or final element (actuator) that by adequate technical measures prevents from hazards either deterministically or by reducing the risk to a tolerable measure

NOTE Depending on a particular safety function, de-energizing may not be the only possibility for a fail-safe state.

3.1.2.13

F-Device

passive CP 3/RTE communication peer that is able to perform the FSCP 3/1 protocol, usually triggered by the F-Host for data exchange

3.1.2.14

F-Driver

software administering safety PDUs within F-Hosts and F-Devices according to the FSCP 3/1 specifications

3.1.2.15

F-Host

data processing unit that is able to perform the FSCP 3/1 protocol and to service the black channel

NOTE This is usually a PLC or an IPC with an adequate operating system.

3.1.2.16

F-Module

passive communication peer within a modular F-Device or F-Slave that is able to perform the FSCP 3/1 protocol, usually triggered by the F-Host for data exchange

NOTE This is usually a safety-related input or output module.

3.1.2.17

F-Slave

passive CP 3/1 or CP 3/2 communication peer that is able to perform the FSCP 3/1 protocol, usually triggered by the F-Host for data exchange

3.1.2.18

fault reaction

indication of a communication malfunction by setting the fault bits in the Status Byte and a corresponding automatic safe reaction within the components

NOTE

Within F-Output: Shutting down the outputs, and/or automatic safe reaction of the actuator unit.

Within F-CPU: Corresponding user program reaction possible. F-I/O-Data to be set to fail-safe values.

Within F-Input: On communication faults detected from F-Input:
Fault bits set in the Status Byte.
On communication faults detected from F-Host:
F-Input data to be set to fail-safe values.

3.1.2.19

function block (FB)

self-contained program part possessing a specific functionality

3.1.2.20

host acknowledgement time (HAT)

elapsed time in an F-Host starting with the reception of a safety PDU with a certain consecutive number until an appropriate safety PDU with an incremented consecutive number has been generated and returned to the master/IO-controller

3.1.2.21

IO-Controller

active communication entity able to initiate and schedule CP 3/RTE communication activities by other entities which may be IO-Controllers or IO-Devices

NOTE Within CP 3/1 this task is corresponding to a master class 1.

3.1.2.22

IO-Device

passive communication entity able to receive messages and send them in response to another CP 3/RTE communication entity which may be an IO-Controller or other IO-Devices

NOTE Within CP 3/1 this task is corresponding to a slave.

3.1.2.23

IO-Module

addressable sub input/output unit within a modular IO-Device

3.1.2.24

IO-Supervisor

engineering station enabled to read and write data from and to an IO-Device

NOTE It is used for commissioning or diagnostics purposes. In contrast to an IO-Controller it does not take over an active role during the run-up of an IO-System. An IO-Supervisor is not part of the IO-System.

3.1.2.25

IO-System

IO-Controller and its associated IO-Devices

3.1.2.26

iParameter

individual or technology specific F-Device parameters

NOTE Typical iParameters are the protection zone coordinates of a laser scanner.

3.1.2.27

iPar-Server

standardised mechanism to store and retrieve individual or technology specific F-Device parameters within the standard part of an F-Host or its controlled subsystem

3.1.2.28

master (class 1)

active CP 3/1 communication peer triggering slaves for data exchange

3.1.2.29

process values (PV)

input and output data (in a safety PDU) that are required to control an automated process

3.1.2.30

qualifier

additional qualifying bits within *process values* indicating the status of each individual input

3.1.2.31

shared I/O

inputs and outputs in field devices that can be accessed by several controllers

NOTE Even though CP 3/RTE is permitting shared I/O it is not permitted with FSCP 3/1.

3.1.2.32

toggle bit

one bit of the Control and Status Byte to synchronize the (virtual) consecutive counters in both the F-Host and the F-Device

3.1.2.33

universal serial bus (USB)

external bus standard that supports data transfer rates up to 480 Mbit/s

NOTE USB is replacing serial and parallel computer ports and is used for fast direct connections between service computers and field devices.

3.1.2.34

V1-mode

FSCP 3/1 services and protocol according to [48]

3.1.2.35

V2-mode

FSCP 3/1 services and protocol according to this part

3.1.2.36

VLAN tag

extension within Ethernet messages that enables particular user groups on large networks to run their own virtual network via priorities and VLAN-IDs, using appropriate switches, without impacting other user groups and vice versa

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	
EMI	Electromagnetic Interference	
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]
FCS	Frame Check Sequence	
FS	Functional Safety	

FSCP	Functional Safety Communication Profile	
HD	Hamming Distance	
MTBF	Mean Time Between Failures	
MTTF	Mean Time To Failure	
PDU	Protocol Data Unit	[ISO/IEC 7498-1]
PELV	Protective Extra Low Voltage	
PFD	Probability of dangerous Failure on Demand	[IEC 61508-6:2010 ⁹]
PFH	Average frequency of dangerous failure [h ⁻¹] per hour	[IEC 61508-6:2010]
PhL	Physical Layer	[ISO/IEC 7498-1]
PL	Performance Level	[ISO 13849-1]
PLC	Programmable Logic Controller	
SCL	Safety Communication Layer	
SELV	Safety Extra Low Voltage	
SFRT	Safety Function Response Time	
SIL	Safety Integrity Level	[IEC 61508-4:2010]

3.2.2 CPF 3: Additional symbols and abbreviated terms

AES-CCMP	Advanced Encryption Standard - Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
AP	Application Process
API	Application Process Identifier
AR	Application Relationship
ASE	Application Service Element
ASIC	Application Specific Integrated Circuit
C	Coverage
CP 3/1	Communication profile commonly known as PROFIBUS DP ¹⁰
CP 3/2	Communication profile commonly known as PROFIBUS PA
CP 3/RTE	Communication profile commonly known as PROFINET IO
CPU	Central Processing Unit
CR	Communication Relationship
DAP	Device Access Point
DAT	Device Acknowledgement Time
DP	Decentralized Peripherals
F	Identifier for safety items (fail-safe, functional safe)
FB	Function Block
FV	Fail-safe Values
GSD	General Station Description (file associated with device)
GSDL	General Station Description Language (for CP 3/1 and CP 3/2 devices)
GSDML	General Station Description Markup Language (for CP 3/RTE devices)
HAT	Host Acknowledgement Time
I/O	Input/Output
LED	Light Emitting Diode

⁹ To be published.

¹⁰ For trade name declarations, see Clause 4.

PA	Process Automation	
PN IO	PROFINET IO = CP 3/4 to 3/6	
PSK	Pre-shared Key	
PV	Process Values	
RADIUS	Remote Authentication Dial In User Service	
S	Standard	
SR	(Functional) Safety-Related	
SSID	Service Set Identifier	
UML	Unified Modeling Language	[57]
USB	Universal Serial Bus	[62]
VLAN	Virtual Local Area Network	
WCDT	Worst Case Delay Time	
WTime	Watchdog Time	
WPA2	Wi-Fi Protected Access 2	[26]
XML	eXtensible Markup Language	[59], [60], [61]

3.3 Conventions

This part uses UML2 notation for the drawing of the state charts and a condensed form for sequence charts [57]. The transition tables are depicted following the recommendations of IEC 62390.

In this part the abbreviation "F" is an indication for safety related items, technologies, systems, and units (fail-safe, functional safe).

In this part the default data that shall be sent in case of unit failures or errors, are called fail-safe values (FV) and are set to "0".

In this part, any CRC signature calculation resulting in a "0" value, will use the value "1" instead.

In this part the abbreviation "CP 3/RTE" comprises the three communication profiles CP 3/4, CP 3/5, and CP 3/6. CP 3/RTE is commonly known as PROFINET IO.

4 Overview of FSCP 3/1 (PROFIsafe™)

Communication Profile Family 3 (commonly known as PROFIBUS™, PROFINET™¹¹) defines communication profiles based on IEC 61158-2 Type 3, IEC 61158-3-3, IEC 61158-4-3, IEC 61158-5-3, IEC 61158-5-10, IEC 61158-6-3, and IEC 61158-6-10.

The basic profiles CP 3/1 and CP 3/2 are defined in IEC 61784-1; CP 3/4, CP 3/5 and CP 3/6 are defined in IEC 61784-2. The CPF 3 functional safety communication profile FSCP 3/1 (PROFIsafe™¹¹) is based on the CPF 3 basic profiles in IEC 61784-1 and IEC 61784-2 and the safety communication layer specifications defined in this part.

FSCP 3/1 is based on the cyclic data exchange of a (bus) controller with its associated (field) devices using a one-to-one communication relationship (Figure 3). One controller can operate any mix of standard and safety devices connected to the network. Assigning safety tasks and standard

¹¹ PROFIBUS™, PROFINET™ and PROFIsafe™ are trade names of the non-profit organization PROFIBUS Nutzerorganisation e.V. (PNO). This information is given for the convenience of users of this International Standard and does not constitute an endorsement by IEC of the trade name holder or any of its products. Compliance to this standard does not require use of the registered logos for PROFIBUS™, PROFINET™ or PROFIsafe™. Use of the registered logos for PROFIBUS™, PROFINET™ or PROFIsafe™ requires permission of PNO.

tasks to different controllers also is possible. Any so-called acyclic communications between devices and controllers or supervisors such as programming devices are intended for configuration, parameterisation, diagnosis, and maintenance purposes.

For the realisation of FSCP 3/1, the following four measures have been chosen:

- (virtual) consecutive numbering;
- watchdog time monitoring with acknowledgement;
- codename per communication relationship;
- cyclic redundancy checking for data integrity.

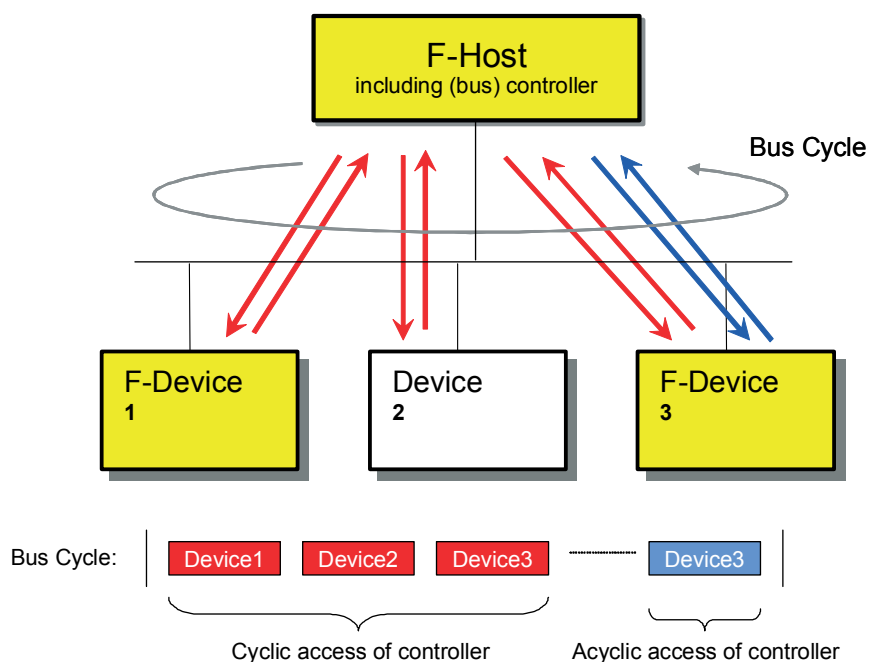


Figure 3 – Basic communication preconditions for FSCP 3/1

The consecutive numbering uses a range that is big enough to secure any malfunction caused by message storing network elements. Every safety device returns a message with a safety PDU for acknowledgement even if there are no process data. A separate watchdog timer on both the sender and the receiver side is used for each one-to-one communication relationship. The unique codename per communication relationship is established for authentication reasons and is encoded within an initial CRC signature value for the cyclically calculated and transmitted CRC2 signature (Figure 4).

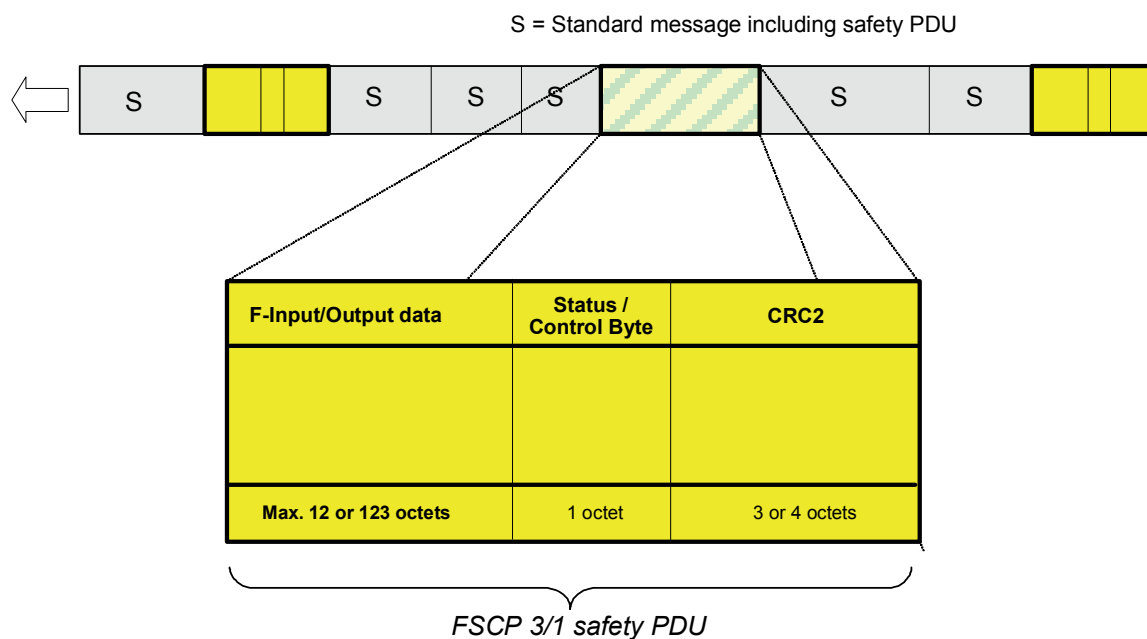


Figure 4 – Structure of an FSCP 3/1 safety PDU

FSCP 3/1 provides two operational modes: V1- and V2-mode. While the measures of the V1-mode are sufficient for the safety data transmission on pure CP 3/1 networks, the more "generous" features of Ethernet / CP 3/RTE such as wider address space and buffering switch components are requiring some extensions to the FSCP 3/1 protocol thus leading to the V2-mode. The V1-mode is restricted to CP 3/1 whereas the V2-mode is required for CP 3/4 to CP 3/6 and/or CP 3/1. This part only describes the details of the extended functionality of the so-called V2-mode. Safety communication between PROFINET CBA components (see CP 3/3) is not defined. Figure 5 provides an overview on FSCP 3/1 within the CP 3/1 and CP 3/RTE architectures.

While automation solutions with distributed I/O gained widely acceptance through PROFIBUS (CP 3/1 and CP 3/2) and the industrial Ethernet based PROFINET (CP 3/RTE), safety applications were still relying on a second layer of conventional electrical techniques or special busses thus limiting the seamless engineering and interoperability. Additionally, modern safety devices such as laser scanners or drives with integrated safety could not be fostered as needed due to missing system support. It is the purpose of this part and related documents to provide the corresponding enabling technologies.

After this introduction, subclause 5.1 holds additional references for the development of the FSCP 3/1 technology and 5.2 holds its functional requirements. The four safety measures of FSCP 3/1 are listed in 5.3. The network topologies within CP 3/RTE and their crossovers to CP 3/1 and CP 3/2 are mentioned in 5.4. A brief introduction into the communication relationships and objects of the fieldbus standard is following in 5.5.

For safety and efficiency reasons the list of possible fieldbus data types is reduced to a concise set and described in 5.5.4. Subclauses 6.1 to 6.3 are unveiling the F-Host and F-Device services as well as the possible diagnosis messages of the safety layer.

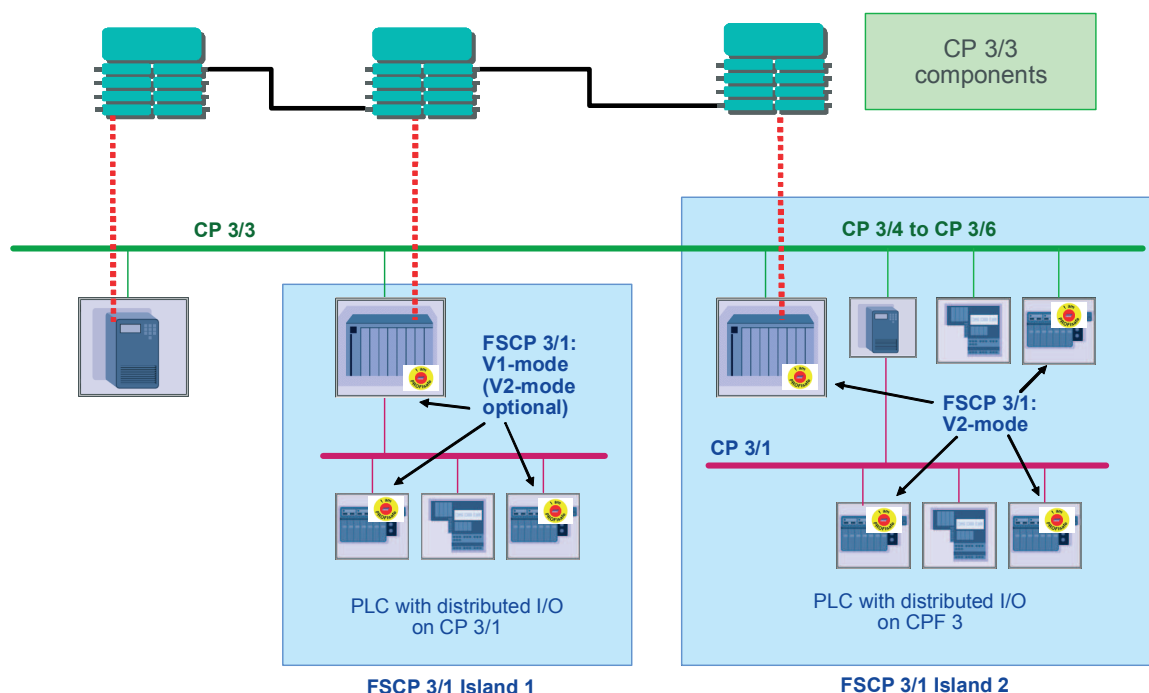


Figure 5 – Safety communication modes

Clause 7 starts with an overview on the safety PDU (7.1), continues with a description of the state machines in F-Host and F-Device and sequence diagrams in the Unified Modeling Language 2 format (7.2.2 to 7.2.4). Associated timing constraints are contained in 7.2.5 and 7.2.6. Following the format IEC 61784-3:2010 Annex D, subclause 7.3 illustrates the system reactions in the event of the possible malfunctions. Other system functions such as start-up of the safety layer are contained in 7.4. The layer management of safety devices is focusing on safety communication specific F-Parameters (8.1) and on device specific individual iParameters (8.2). The requirements for handling and supply of the F-Parameters are described in 8.3. Subclause 8.4 deals with securing the data structures that are to be exchanged between the communicating partners and that are representing the configuration of a device. Subclause 8.5 shows how the data structure information can be used to configure F-Channel drivers for more complex F-Devices to save programming effort. The requirements for the system integration of iParameterization means and tools are listed in 8.6. The aspects of response times, installation guidelines, and duration of demands, maintenance, safety manual, wireless transmission, and F-Host conformance classes are covered 9. The reasoning for assessment is pointed out in 10.1 and the details in 10.2. An informative annex contains examples for fast CRC signature calculations and a bibliography. Two additional FSCP 3/1 guidelines for electrical safety and assessment shall be observed ([44], [45]).

5 General

5.1 External documents providing specifications for the profile

In addition to the normative references in Clause 2, the technology in this part has been approved according to GS-ET-26 [31].

FSCP 3/1 meets the requirements of NE97 [58].

5.2 Safety functional requirements

The following requirements apply for the development of the FSCP 3/1 technology.

- a) Safety communication and standard communication shall be independent. However, standard devices and safety devices shall be able to use the same communication channel.

- b) Safety communication shall be suitable for Safety Integrity Level SIL3 (see IEC 61508), control category 4 (see EN 954-1 [25]), and PL e (see ISO 13849-1).
- c) Safety communication shall use a single-channel communication system. Redundancy may only be used optionally for increased availability.
- d) Implementation of the safety transmission protocol shall be restricted to the communication end devices (F-Host or F-CPU – F-Device and /or F-I/O-Module).
- e) There shall always be a 1:1 communication relationship between an F-Device and its F-Host.
- f) The transmission duration times shall be monitored.
- g) Environmental conditions shall be according to general automation requirements, mainly IEC 61326-3-1 and IEC 61326-3-2, if there are no particular product standards.
- h) Transmission equipment such as controllers, ASICs, links, couplers, etc. shall remain unmodified (black channel). The safety functions shall be above OSI layer 7 (i.e. profile, no standard protocol changes or enhancements)
- i) The safety communication shall not reduce the permitted number of devices. Restrictions may occur during mapping in case of CP 3/2 applications due to message limitations (see CP 3/2 in IEC 61784-1).
- j) Safety communication shall be suitable for NE97 [58] and meet the requirements of IEC 61784-3:2010 Annex D.

5.3 Safety measures

The safety measures mentioned in Table 1 for mastering possible transmission errors are one significant component of the FSCP 3/1 profile. The selection in Table 1 of the generic safety measures listed in IEC 61784-3:2010, 5.5 is required for FSCP 3/1.

The safety measures shall be processed and monitored within one safety unit.

Table 1 – Deployed measures to master errors

Communication error	Safety measures			
	(virtual) Consecutive number ^a	Timeout with receipt ^b	Codename for sender and receiver ^c	Data consistency check ^d
Corruption				X
Unintended repetition	X			
Incorrect sequence	X			
Loss	X	X		
Unacceptable delay		X		
Insertion	X	X	X	
Masquerade		X	X	X
Addressing			X	
Revolving memory failures within switches	X			
^a Instance of "sequence number" of IEC 61784-3. ^b Instance of "time expectation" and "feedback message" of IEC 61784-3. ^c Instance of "connection authentication" of IEC 61784-3. ^d Instance of "data integrity assurance" of IEC 61784-3.				

5.4 Safety communication layer structure

5.4.1 Principle of FSCP 3/1 safety communications

FSCP 3/1's way of safety communication is based on the experience made in the railway signaling technique as it has been laid down in the IEC 62280-1 and IEC 62280-2.

On this basis, safety communication is performed by

- a standard transmission system (Figure 6), and
- an additional safety transmission protocol on top of this standard transmission system.

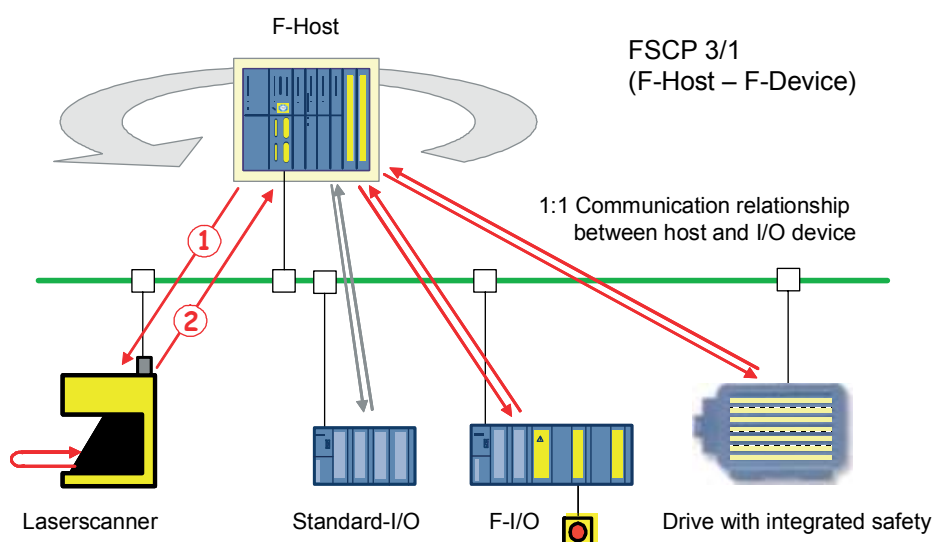


Figure 6 – Standard CPF 3 transmission system

The standard transmission system includes the entire hardware of the transmission system and the related protocol functions (i.e. OSI layers 1, 2 and 7 according to Figure 7).

Safety applications and standard applications are sharing the same standard CPF 3 communication systems at the same time. The safe transmission function comprises all measures to deterministically discover all possible faults / hazards that could be infiltrated by the standard transmission system or to keep the residual error (fault) probability under a certain limit. This includes

- Random malfunctions, for example due to EMI impact on the transmission channel
- Failures / faults of the standard hardware
- Systematic malfunctions of components within the standard hardware and software

This principle delimits the assessment effort to the "safe transmission functions". The "standard transmission system" (black channel) does not need any additional safety assessment.

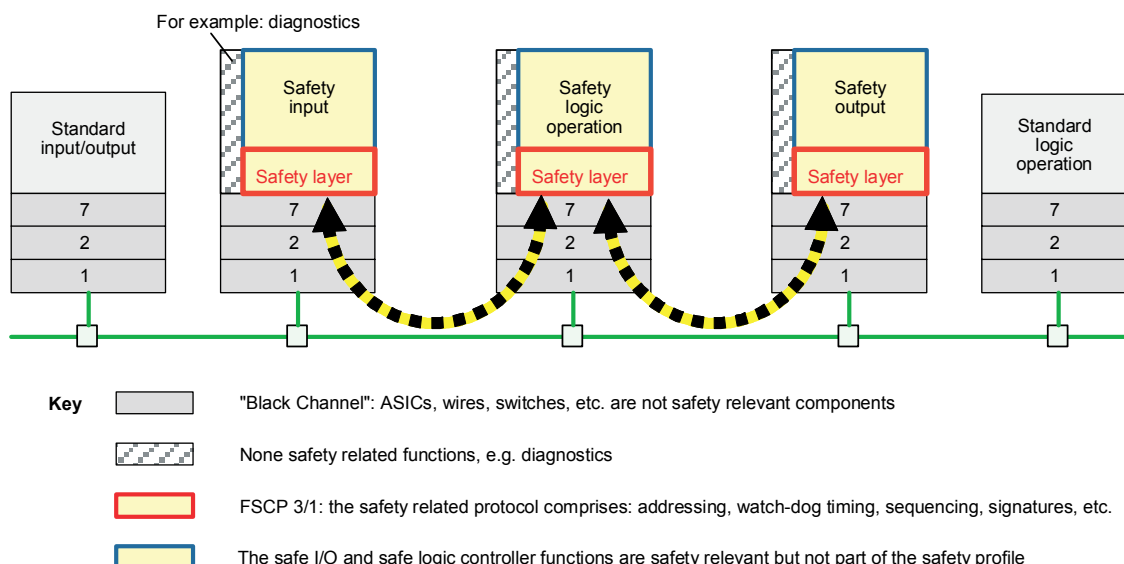


Figure 7 – Safety layer architecture

Transmission is performed via electrical or optical conductors. Permissible topologies and transmission features of the standard transmission system and the components of the "black channel" are described in 5.4.2.

5.4.2 CPF 3 communication structures

The basic communication layers of CP 3/RTE are shown in Figure 8. While the cyclic safety communication of FSCP 3/1 is using the realtime channels RT or IRT (CP 3/RTE of IEC 61784-2) the other services are using the so-called open channel via TCP/IP or UDP.

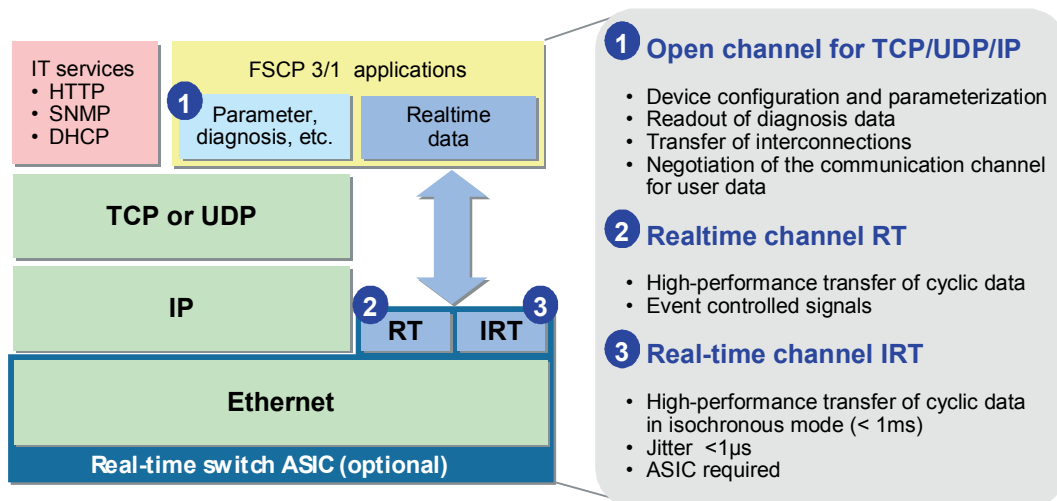


Figure 8 – Basic communication layers

Figure 9 shows the typical (star) topology of one possible CP 3/RTE wiring with multiport switches as hubs. One failing device will not shut down the whole network. However, the wiring effort may be unfavorable.