

DIN EN 61784-3-12

ICS 35.160; 35.240.50

**Industrielle Kommunikationsnetze –
Profile –****Teil 3-12: Funktional sichere Übertragung bei Feldbussen – Zusätzliche
Festlegungen für die Kommunikationsprofilfamilie 12
(IEC 61784-3-12:2010);
Englische Fassung EN 61784-3-12:2010**

Industrial communication networks –

Profiles –

Part 3-12: Functional safety fieldbuses – Additional specifications for CPF 12

(IEC 61784-3-12:2010);

English version EN 61784-3-12:2010

Réseaux de communication industriels –

Partie 3-12: Bus de terrain à sécurité fonctionnelle –

Spécifications complémentaires pour le CPF 12

(CEI 61784-3-12:2010);

Version anglaise EN 61784-3-12:2010

Gesamtumfang 106 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.

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 61784-3-12 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.

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 [34], [35]¹⁾.

3.1.1.7

Fehler (en: 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.

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

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

²⁾ Noch zu veröffentlichen.

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 (en: 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 [34], [35].

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**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]

3.1.1.19**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]

3.1.1.20**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]

3.1.1.21**Zuverlässigkeit (en: reliability)**

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

ANMERKUNG 1 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]

3.1.1.22**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]

3.1.1.23

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

3.1.1.24

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.

3.1.1.25

Sicherheitsgerät (en: safety device)

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

3.1.1.26

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]

3.1.1.27

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]

3.1.1.28

Reaktionszeit einer Sicherheitsfunktion (en: safety function response time)

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

3.1.1.29

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

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

³⁾ Noch zu veröffentlichen.

⁴⁾ In Bearbeitung.

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]

3.1.1.30

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.

3.1.1.31

sicherheitsbezogene Anwendung (en: safety-related application)

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

3.1.1.32

sicherheitsbezogenes System (en: safety-related system)

System, welches *Sicherheitsfunktionen* nach IEC 61508 ausführt

3.1.1.33

Slave (en: slave)

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

3.1.2 CPF 12: Zusätzliche Begriffe

3.1.2.1

ausfallsichere Daten (en: fail-safe data)

Ausdruck für Daten, die für den Fall der Initialisierung oder eines Fehlers auf einen vorgegeben Wert festgelegt werden

ANMERKUNG In diesem Teil sollte der Wert der ausfallsicheren Daten immer auf „0“ festgelegt werden.

3.1.2.2

FSoE-Verbindung (en: FSoE Connection)

eindeutige Beziehung zwischen dem FSoE-Master und einem FSoE-Slave

3.1.2.3

FSoE-Zyklus (en: FSoE Cycle)

Kommunikationszyklus mit einer Sicherheits-PDU eines Masters und der entsprechenden Sicherheits-PDU eines Slaves

⁵⁾ Noch zu veröffentlichen.

3.1.2.4

Sicherheitseingabe (en: SafeInput)

Sicherheitprozessdaten, die vom FSoE-Slave an den FSoE-Master übertragen werden

3.1.2.5

Sicherheitsausgabe (en: SafeOutput)

Sicherheitsprozessdaten, die vom FSoE-Master an den FSoE-Slave übertragen werden

3.1.2.6

Sicherheits-PDU des Masters (en: Safety Master PDU)

Sicherheits-PDU, die vom FSoE-Master an den FSoE-Slave übertragen wird

3.1.2.7

Sicherheits-PDU des Slaves (en: Safety Slave PDU)

Sicherheits-PDU, die vom FSoE-Slave an den FSoE-Master übertragen wird

**Industrial communication networks -
Profiles -
Part 3-12: Functional safety fieldbuses -
Additional specifications for CPF 12
(IEC 61784-3-12:2010)**

Réseaux de communication industriels -
Partie 3-12: Bus de terrain à sécurité
fonctionnelle -
Spécifications complémentaires
pour le CPF 12
(CEI 61784-3-12:2010)

Industrielle Kommunikationsnetze -
Profile -
Teil 3-12: Funktional sichere Übertragung
bei Feldbussen -
Zusätzliche Festlegungen
für die Kommunikationsprofilfamilie 12
(IEC 61784-3-12:2010)

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 1 of IEC 61784-3-12, 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 61784-3-12 on 2010-07-01.

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 61784-3-12:2010 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 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 61511 series	NOTE	Harmonized in EN 61511 series (not modified).
IEC 61784-1	NOTE	Harmonized as EN 61784-1.
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 62061	NOTE	Harmonized as EN 62061.
ISO 10218-1	NOTE	Harmonized as EN ISO 10218-1.
ISO 12100-1	NOTE	Harmonized as EN ISO 12100-1.
ISO 13849-1	NOTE	Harmonized as EN ISO 13849-1.
ISO 13849-2	NOTE	Harmonized as EN ISO 13849-2.

CONTENTS

0	Introduction.....	7
0.1	General.....	7
0.2	Patent declaration	9
1	Scope.....	10
2	Normative references.....	10
3	Terms, definitions, symbols, abbreviated terms and conventions	11
3.1	Terms and definitions	11
3.1.1	Common terms and definitions	11
3.1.2	CPF 12: Additional terms and definitions	15
3.2	Symbols and abbreviated terms.....	16
3.2.1	Common symbols and abbreviated terms.....	16
3.2.2	CPF 12: Additional symbols and abbreviated terms	17
3.3	Conventions	17
4	Overview of FSCP 12/1 (Safety-over-EtherCAT™)	17
5	General	18
5.1	External document providing specifications for the profile.....	18
5.2	Safety functional requirements	18
5.3	Safety measures	19
5.4	Safety communication layer structure.....	19
5.5	Relationships with FAL (and DLL, PhL)	20
5.5.1	General.....	20
5.5.2	Data types.....	20
6	Safety communication layer services	20
6.1	FSoE Connection	20
6.2	FSoE Cycle	21
6.3	FSoE services	21
7	Safety communication layer protocol	22
7.1	Safety PDU format	22
7.1.1	Safety PDU structure.....	22
7.1.2	Safety PDU command.....	23
7.1.3	Safety PDU CRC.....	24
7.2	FSCP 12/1 communication procedure.....	27
7.2.1	Message cycle.....	27
7.2.2	FSCP 12/1 node states.....	28
7.3	Reaction on communication errors.....	37
7.4	State table for FSoE Master	38
7.4.1	FSoE Master state machine	38
7.4.2	Reset state.....	42
7.4.3	Session state.....	43
7.4.4	Connection state.....	46
7.4.5	Parameter state	50
7.4.6	Data state	53
7.5	State table for FSoE Slave.....	56
7.5.1	FSoE Slave state machine	56

7.5.2	Reset state	60
7.5.3	Session state	62
7.5.4	Connection state	66
7.5.5	Parameter state	71
7.5.6	Data state	76
8	Safety communication layer management	79
8.1	FSCP 12/1 parameter handling	79
8.2	FSoE communication parameters	79
9	System requirements	80
9.1	Indicators and switches	80
9.1.1	Indicator states and flash rates	80
9.1.2	Indicators	81
9.2	Installation guidelines	82
9.3	Safety function response time	82
9.3.1	General	82
9.3.2	Determination of FSoE Watchdog time	83
9.3.3	Calculation of the worst case safety function response time	84
9.4	Duration of demands	85
9.5	Constraints for calculation of system characteristics	85
9.5.1	General	85
9.5.2	Probabilistic considerations	85
9.6	Maintenance	87
9.7	Safety manual	87
10	Assessment	87
Annex A (informative) Additional information for functional safety communication profiles of CPF 12		88
A.1	Hash function calculation	88
A.2		92
Annex B (informative) Information for assessment of the functional safety communication profiles of CPF 12		93
Bibliography		94
Annex ZA (normative) Normative references to international publications with their corresponding European publications		97
Table 1 – State machine description elements		17
Table 2 – Communication errors and detection measures		19
Table 3 – General Safety PDU		23
Table 4 – Shortest Safety PDU		23
Table 5 – Safety PDU command		24
Table 6 – CRC_0 calculation sequence		24
Table 7 – CRC_i calculation sequence (i>0)		25
Table 8 – Example for CRC_0 inheritance		26
Table 9 – Example for 4 octets of safety data with interchanging of octets 1-4 with 5-8		27
Table 10 – Safety Master PDU for 4 octets of safety data with command = Reset after restart (reset connection) or error		29
Table 11 – Safety Slave PDU for 4 octets of safety data with command = Reset for acknowledging a Reset command from the FSoE Master		29

Table 12 – Safety Slave PDU for 4 octets of safety data with command = Reset after restart (reset connection) or error.....	30
Table 13 – Safety Master PDU for 4 octets of safety data with command = Session.....	30
Table 14 – Safety Slave PDU for 4 octets of safety data with command = Session	31
Table 15 – Safety data transferred in the connection state.....	32
Table 16 – Safety Master PDU for 4 octets of safety data in Connection state.....	32
Table 17 – Safety Slave PDU for 4 octets of safety data in Connection state	32
Table 18 – Safety data transferred in the parameter state.....	33
Table 19 – First Safety Master PDU for 4 octets of safety data in parameter state.....	33
Table 20 – First Safety Slave PDU for 4 octets of safety data in parameter state.....	34
Table 21 – Second Safety Master PDU for 4 octets of safety data in parameter state	34
Table 22 – Second Safety Slave PDU for 4 octets of safety data in parameter state	35
Table 23 – Safety Master PDU for 4 octets of ProcessData in data state	35
Table 24 – Safety Slave PDU for 4 octets of ProcessData in data state.....	36
Table 25 – Safety Master PDU for 4 octets of fail-safe data in data state.....	36
Table 26 – Safety Slave PDU for 4 octets of fail-safe data in data state	37
Table 27 – FSoE communication error	37
Table 28 – FSoE communication error codes.....	38
Table 29 – States of the FSoE Master	38
Table 30 – Events in the FSoE Master state table.....	40
Table 31 – Functions in the FSoE Master state table.....	40
Table 32 – Variables in the FSoE Master state table	41
Table 33 – Macros in the FSoE Master state table	41
Table 34 – States of the FSoE Slave	56
Table 35 – Events in the FSoE Slave state table.....	58
Table 36 – Functions in the FSoE Slave state table.....	58
Table 37 – Variables in the FSoE Slave state table	59
Table 38 – Macros in the FSoE Slave state table	59
Table 39 – FSoE Communication parameters	80
Table 40 – Indicator States.....	80
Table 41 – FSoE STATUS indicator states	81
Table 42 – Definition of times	83
Figure 1 – Relationships of IEC 61784-3 with other standards (machinery).....	7
Figure 2 – Relationships of IEC 61784-3 with other standards (process)	8
Figure 3 – Basic FSCP 12/1 system	18
Figure 4 – FSCP 12/1 software architecture	20
Figure 5 – FSoE Cycle	21
Figure 6 – FSCP 12/1 communication structure	22
Figure 7 – Safety PDU for CPF 12 embedded in Type 12 PDU	22
Figure 8 – FSCP 12/1 node states.....	28
Figure 9 – State diagram for FSoE Master	39

Figure 10 – State diagram for FSoE Slave.....57

Figure 11 – Indicator flash rates 81

Figure 12 – Components of a safety function 82

Figure 13 – Calculation of the FSoE Watchdog times for input and output connections 83

Figure 14 – Calculation of the worst case safety function response time.....84

Figure 15 – Safety PDU embedded in standard PDU 86

Figure 16 – Residual error rate for 8/16/24 bit safety data and up to 12 144 bit standard data87

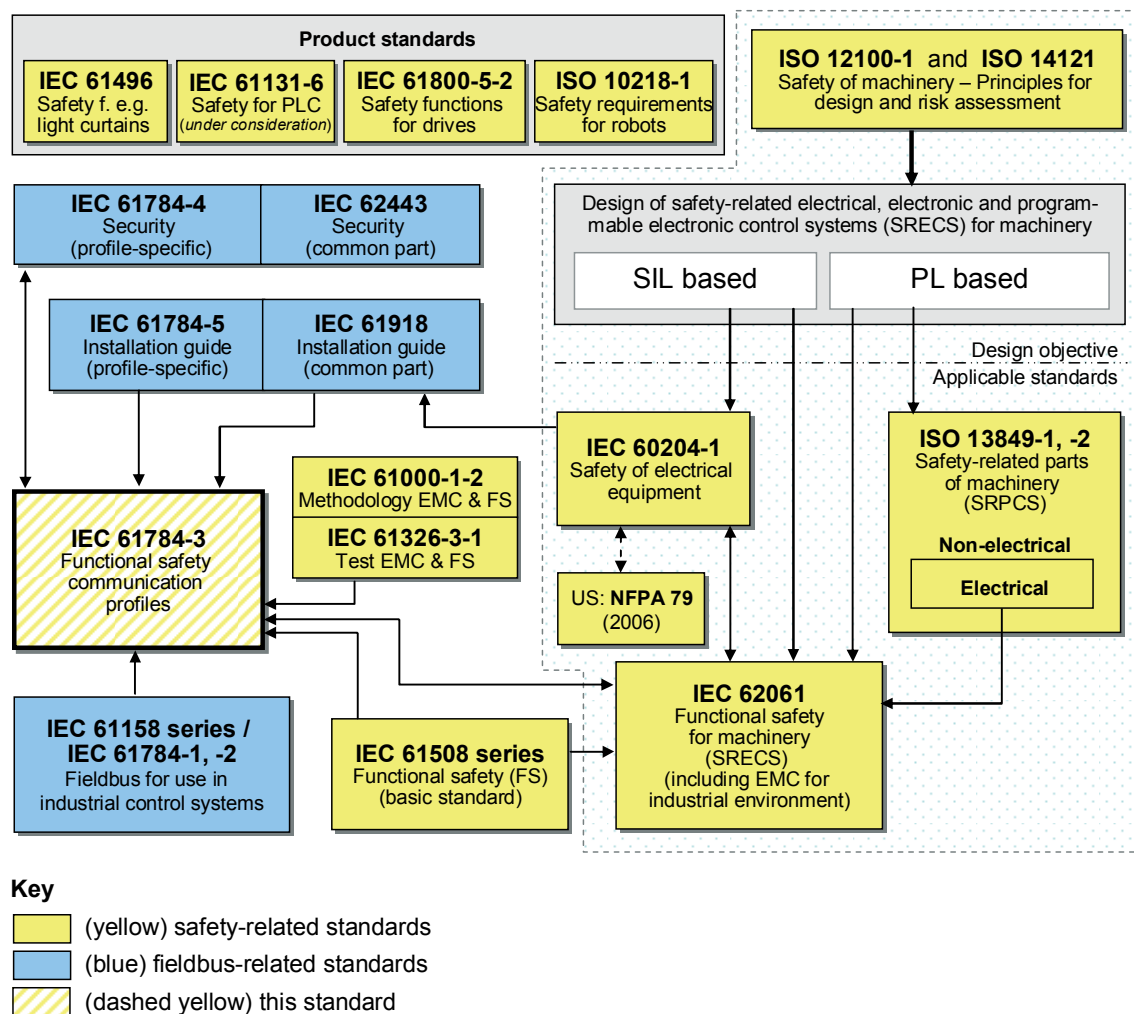
0 Introduction

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.

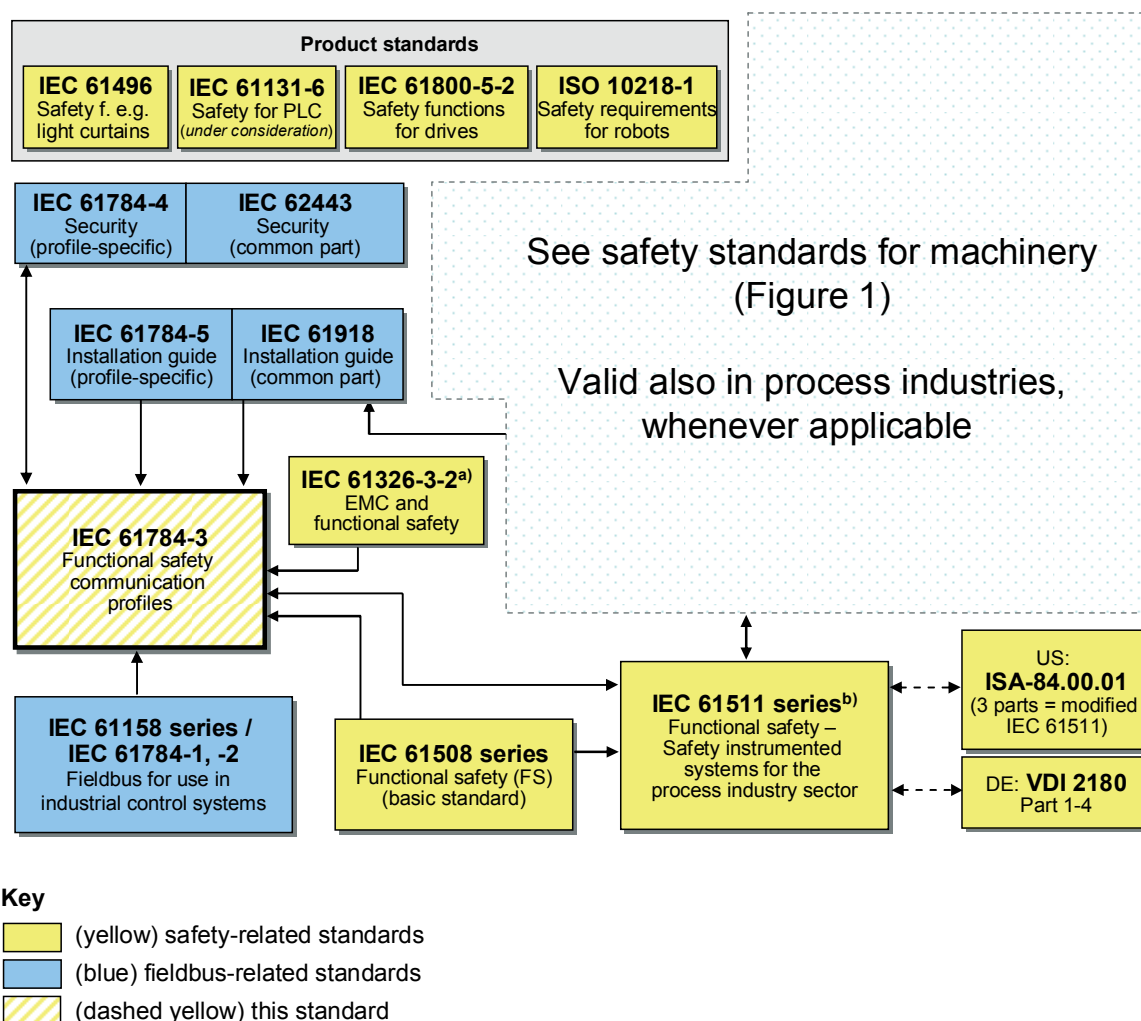
Figure 1 shows the relationships between this standard and relevant safety and fieldbus standards in a machinery environment.



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 12 as follows, where the [xx] notation indicates the holder of the patent right:

DE 10 2004 044 764.0 [BE] Datenübertragungsverfahren und Automatisierungssystem
zum Einsatz eines solchen Datenübertragungsverfahrens

EP 05 733 921.0 [BE] Sicherheitssteuerung

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:

[BE] Beckhoff Automation GmbH
Eiserstrasse 5, 33415 Verl
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 3-12: Functional safety fieldbuses – Additional specifications for CPF 12

1 Scope

This part of the IEC 61784-3 series specifies a safety communication layer (services and protocol) based on CPF 12 of IEC 61784-2 and IEC 61158 Type 12. 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 61131-2, *Programmable controllers – Part 2: Equipment requirements and tests*

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

IEC 61158-3-12, *Industrial communication networks – Fieldbus specifications – Part 3-12: Data-link layer service definition – Type 12 elements*

IEC 61158-4-12, *Industrial communication networks – Fieldbus specifications – Part 4-12: Data-link layer protocol specification – Type 12 elements*

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

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

IEC 61158-5-12, *Industrial communication networks – Fieldbus specifications – Part 5-12: Application layer service definition – Type 12 elements*

IEC 61158-6-12, *Industrial communication networks – Fieldbus specifications – Part 6-12: Application layer protocol specification – Type 12 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 61784-2, *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 61918, *Industrial communication networks – Installation of communication networks in industrial premises*

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 In preparation.

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 [34], [35]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

⁴ Figures in square brackets refer to the bibliography.

⁵ To be published.

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 [34], [35].

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

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]

3.1.1.19

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]

3.1.1.20

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]

3.1.1.21 **reliability**

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

NOTE 1 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]

3.1.1.22 **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]

3.1.1.23 **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

3.1.1.24 **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.

3.1.1.25 **safety device**

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

3.1.1.26 **safety extra-low-voltage (SELV)**

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

NOTE An SELV circuit is not connected to protective earth.

[IEC 61131-2]

3.1.1.27 **safety function**

function to be implemented by an E/E/PE safety-related system or other risk reduction measures, that is intended to achieve or maintain a safe state for the EUC, in respect of a specific hazardous event

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

⁶ To be published.

[IEC 61508-4:2010, modified]

3.1.1.28

safety function response time

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.

3.1.1.29

safety integrity level (SIL)

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

NOTE 1 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]

3.1.1.30

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.

3.1.1.31

safety-related application

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

3.1.1.32

safety-related system

system performing *safety functions* according to IEC 61508

3.1.1.33

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

3.1.2 CPF 12: Additional terms and definitions

3.1.2.1

fail-safe data

expression for data that are set to a predefined value in case of initialization or error

NOTE In this part, the value of the fail-safe data should always be set to "0".

⁷ In preparation.

⁸ To be published.

3.1.2.2

FSoE Connection

unique relationship between the FSoE Master and an FSoE Slave

3.1.2.3

FSoE Cycle

communication cycle with one Safety Master PDU and the corresponding Safety Slave PDU

3.1.2.4

SafeInput

safety process data transferred from the FSoE Slave to the FSoE Master

3.1.2.5

SafeOutput

safety process data transferred from the FSoE Master to the FSoE Slave

3.1.2.6

Safety Master PDU

safety PDU transferred from the FSoE Master to the FSoE Slave

3.1.2.7

Safety Slave PDU

safety PDU transferred from the FSoE Slave to the FSoE Master

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]
FCS	Frame Check Sequence	
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]
PELV	Protective Extra Low Voltage	
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	
SIL	Safety Integrity Level	[IEC 61508-4:2010]

3.2.2 CPF 12: Additional symbols and abbreviated terms

ASIC	Application specific integrated circuit	
FSoE	Failsafe over CPF 12	
ID	Identifier	
UML	Unified Modeling Language	[ISO/IEC 19501]

3.3 Conventions

The conventions used for the descriptions of objects services and protocols are described in IEC 61158-3-12, IEC 61158-4-12, IEC 61158-5-12 and IEC 61118-6-12.

As appropriate, this part uses flow charts and UML Sequence Diagrams to describe concepts.

In state diagrams states are represented as boxes, state transitions are shown as arrows. Names of states and transitions of the state diagram correspond to the names in the textual listing of the state transitions.

The textual listing of the state transitions is structured as follows, see also Table 1.

The first row contains the name of the transition. The second row contains the condition for the transition. The third row contains the action(s) that shall take place. The last row contains the next state.

Table 1 – State machine description elements

Transition	Condition	Action	Next State

Each state with its transitions is described in a separate subclause. For each event that can occur in a state a separate subclause is inserted.

4 Overview of FSCP 12/1 (Safety-over-EtherCAT™)

Communication Profile Family 12 (commonly known as EtherCAT™⁹) defines communication profiles based on IEC 61158-2 Type 12, IEC 61158-3-12, IEC 61158-4-12, IEC 61158-5-12 and IEC 61158-6-12.

The basic profile(s) CP 12/1 and CP 12/2 are defined in IEC 61784-2. The CPF 12 functional safety communication profile FSCP 12/1 (Safety-over-EtherCAT™⁹) is based on the CPF 12 basic profiles in IEC 61784-2 and the safety communication layer specifications defined in this part.

FSCP 12/1 describes a protocol for transferring safety data up to SIL3 between FSCP 12/1 devices. Safety PDUs are transferred by a subordinate fieldbus that is not included in the safety considerations, since it can be regarded as a black channel. The Safety PDU exchanged between two communication partners is regarded by the subordinate fieldbus as process data that are exchanged cyclically.

⁹ EtherCAT™ and Safety-over-EtherCAT™ are trade names of Beckhoff, Verl. This information is given for the convenience of users of this International Standard and does not constitute an endorsement by IEC of the trade name holder or any of its products. Compliance to this standard does not require use of the trade names EtherCAT™ or Safety-over-EtherCAT™. Use of the trade names EtherCAT™ or Safety-over-EtherCAT™ requires permission of Beckhoff, Verl.

FSCP 12/1 uses a unique master/slave relationship between the FSoE Master and an FSoE Slave; it is called FSoE Connection (Figure 3). In the FSoE Connection, each device only returns its own new message once a new message has been received from the partner device. The complete transfer path between FSoE Master and FSoE Slave is monitored by a separate watchdog timer on both devices, in each FSoE Cycle.

The FSoE Master can handle more than one FSoE Connection to support several FSoE Slaves.

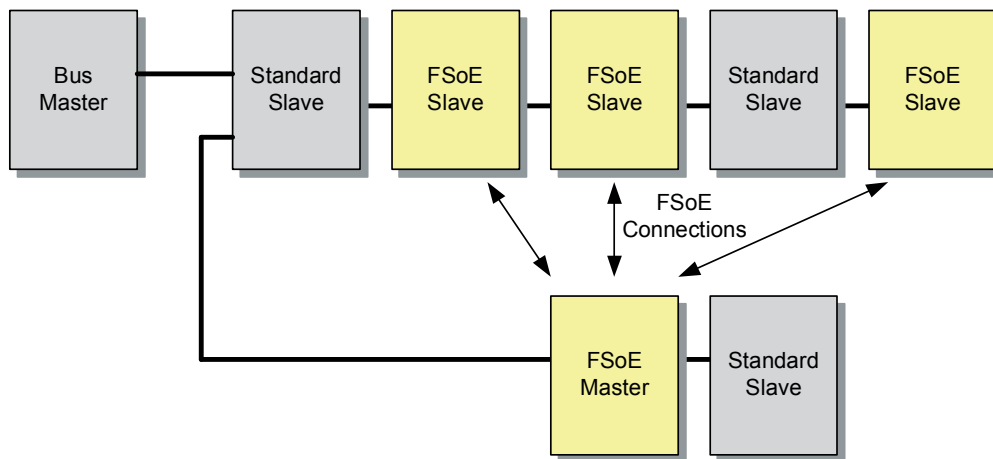


Figure 3 – Basic FSCP 12/1 system

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

- session-number for detecting buffering of a complete startup sequence;
- sequence number for detecting interchange, repetition, insertion or loss of whole messages;
- unique connection identification for safely detecting misrouted messages via a unique address relationship;
- watchdog monitoring for safely detecting delays not allowed on the communication path
- cyclic redundancy checking for data integrity for detecting message corruption from source to sink.

State transitions are initiated by the FSoE Master and acknowledged by the FSoE Slave. The FSoE state machine also involves exchange and checking of information for the communication relation.

5 General

5.1 External document providing specifications for the profile

The following document is useful in understanding the design of FSCP 12/1 protocol:

- GS-ET-26 [33]

5.2 Safety functional requirements

The following requirements shall apply to the development of devices that implement the FSCP 12/1 protocol. The same requirements were used in the development of FSCP 12/1.

- The FSCP 12/1 protocol is designed to support Safety Integrity Level 3 (SIL 3) (see IEC 61508).
- Implementations of FSCP 12/1 shall comply with IEC 61508.
- The basic requirements for the development of the FSCP 12/1 protocol are defined in IEC 61784-3.

- FSCP 12/1 protocol is implemented using a black channel approach; there is no safety related dependency on the standard CPF 12 communication profiles. Transmission equipment such as controllers, ASICs, links, couplers, etc. shall remain unmodified.
- Environmental conditions shall be according to general automation requirements mainly IEC 61326-3-1 for the safety margin tests, unless there are specific product standards.
- Safety communication and non safety relevant communication shall be independent. However, non safety relevant devices and safety devices shall be able to use the same communication channel.
- Implementation of the FSCP 12/1 protocol shall be restricted to the communication end devices (FSoE Master and FSoE Slave).
- There shall always be a 1:1 communication relationship between an FSoE Slave and its FSoE Master.
- The safety communication shall not restrict the minimum cycle time of the communication system.

5.3 Safety measures

The safety measures used in the FSCP 12/1 to detect communication errors are listed in Table 2. The safety measures shall be processed and monitored within each safety device.

Table 2 – Communication errors and detection measures

Communication errors	Safety measures				
	Sequence number (see 7.1.3.4)	Time expectation (see 6.2) ^a	Connection authentication (see 7.2.2.4) ^b	Feedback Message (see 7.2.1)	Data integrity assurance (see 7.1.3)
Corruption					X
Unintended repetition	X				X
Incorrect sequence	X				X
Loss	X	X		X	X
Unacceptable delay		X		X	X
Insertion	X				X
Masquerade		X		X	X
Addressing			X		
Revolving memory failures within switches	X				X
^a In this standard the instance is called "FSoE Watchdog". ^b In this standard the instance is called "FSoE Connection ID".					

5.4 Safety communication layer structure

The FSCP 12/1 protocol is layered on top of the standard network protocol. Figure 4 shows how the protocol is related to the CPF 12 layer. The safety layer accept safety data from the safety-related application and transfers these data via the FSCP 12/1 protocol.

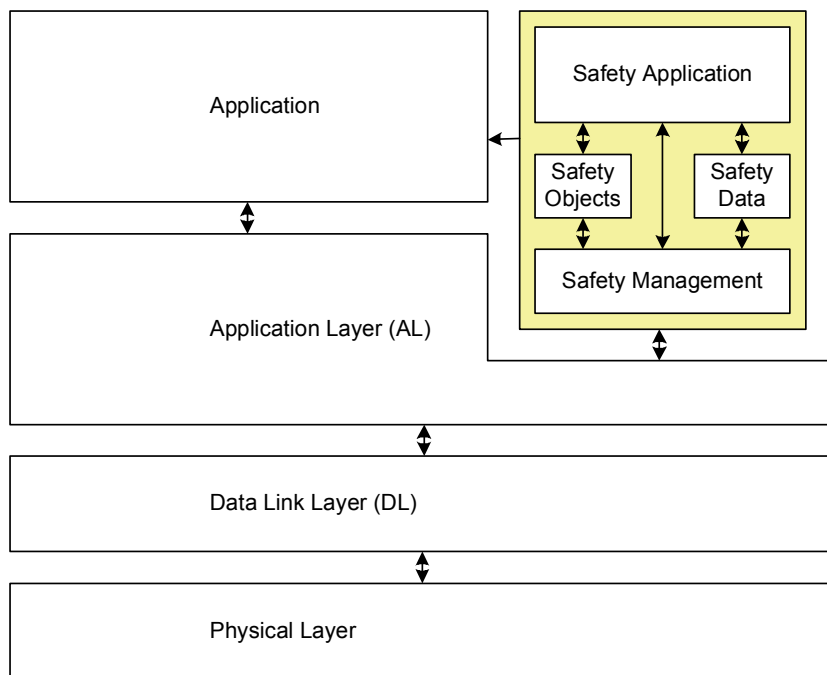


Figure 4 – FSCP 12/1 software architecture

A safety PDU containing the safety data and the required error detection measures is included in the communication process data objects (PDO). The mapping in the process data of the communication system and the start-up of the communication state machine is not part of the safety protocol.

The calculation of the residual error probability for the FSCP 12/1 protocol takes no credit of the error detection mechanisms of the communication system. This means that the protocol can also be transferred via other communication systems. Any transmission link can be used, including fieldbus systems, Ethernet or similar transfer routes, optical fibre cables, copper cables, or even radio links.

5.5 Relationships with FAL (and DLL, PhL)

5.5.1 General

This safety communication layer is designed to be used in conjunction with CPF 12 communication profiles. But it is not restricted to this communication profile.

5.5.2 Data types

Profiles defined in this part support all the CPF 12 data types as defined in IEC 61158-5-12.

6 Safety communication layer services

6.1 FSoE Connection

The connection between two FSCP 12/1 communication partners (FSCP 12/1 nodes) is referred to as FSoE Connection. In an FSoE Connection one communication partner is always the FSoE Master, the other one the FSoE Slave.

The FSoE Master initialises the FSoE Connection after power-on or after a communication fault, while the FSoE Slave is limited to responses. The FSoE Master sets the safety-related communication parameters and optionally the safety-related application parameters of the FSoE Slave.

The safety process data transferred from the FSoE Master to the FSoE Slave are referred to as SafeOutputs. The safety data transferred from the FSoE Slave to the FSoE Master are referred to as SafeInputs.

The Safety PDU transferred from the FSoE Master to the FSoE Slave is referred to as Safety Master PDU. The Safety PDU transferred from the FSoE Slave to the FSoE Master is referred to as Safety Slave PDU.

6.2 FSoE Cycle

The FSoE Master sends the Safety Master PDU to the FSoE Slave and starts the FSoE Watchdog.

After checking the integrity of the Safety PDU, the FSoE Slave transfers the SafeOutputs to the Safety Application. It calculates the Safety Slave PDU with the SafeInputs from the Safety Application and sends this PDU to the FSoE Master. The FSoE Slave also starts its FSoE watchdog. This is shown in Figure 5.

After receiving a valid Safety Slave PDU an FSoE Cycle is finished.

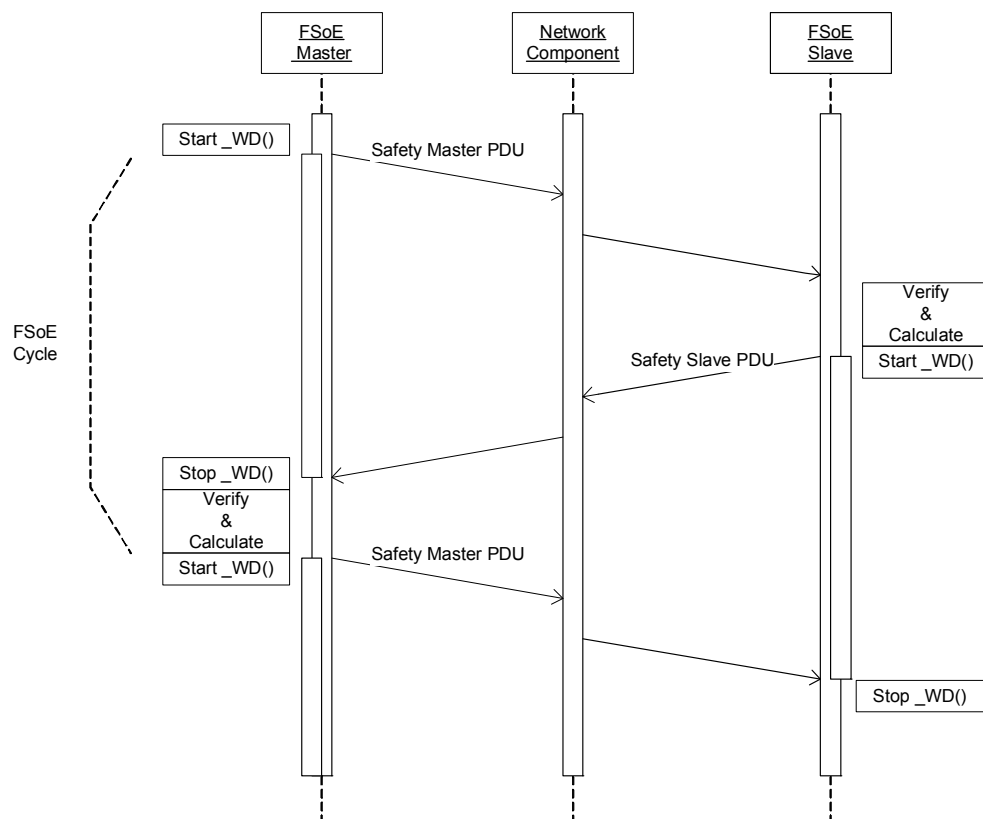


Figure 5 – FSoE Cycle

6.3 FSoE services

For each FSoE Connection, the FSoE Master shall support an FSoE Master handler to control the associated FSoE Slave.

For FSoE Master to FSoE Master Communication, the FSoE Master should support one or several FSoE Slave handler. Figure 6 shows the possible FSoE functionalities in the FSoE Master and FSoE Slave devices.

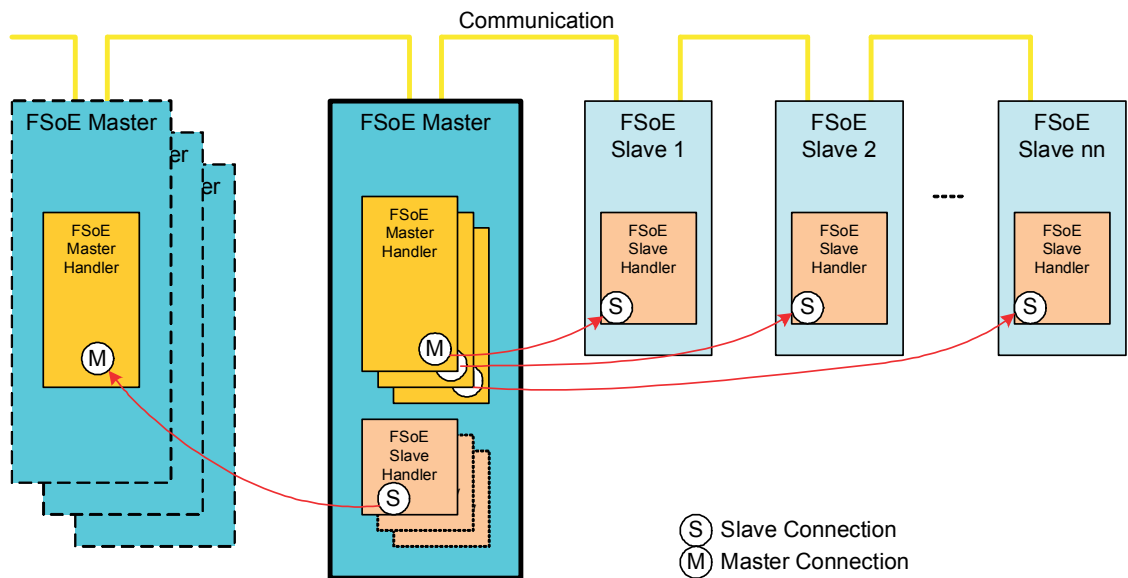


Figure 6 – FSCP 12/1 communication structure

7 Safety communication layer protocol

7.1 Safety PDU format

7.1.1 Safety PDU structure

Figure 7 shows the structure of one safety PDU embedded in a Type 12 PDU. In Table 3 the general structure of the Safety PDU is listed.

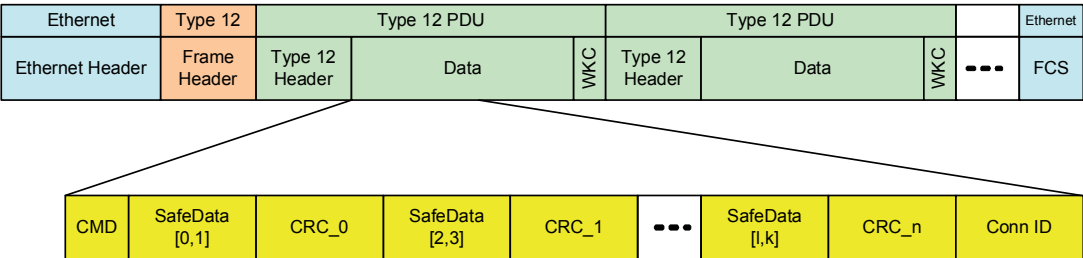


Figure 7 – Safety PDU for CPF 12 embedded in Type 12 PDU

The Safety PDU is cyclically transferred via the subordinate fieldbus. Each FSCP 12/1 node detects a new Safety PDU if at least one bit within the Safety PDU has changed.

The Safety PDU has a variable length specified in the device description of the FSoE Slave. The safety data length can be 1 octet or an even number of octets. The safety data length can be different in input and output direction.

The shorter of the two safety data lengths in the Safety Master PDU and the Safety Slave PDU determines how many safety data are used during the initialisation phase of the FSoE Connection with parameter information. In the longer of the two PDUs the remaining safety data are assigned zero.

Table 3 – General Safety PDU

Octet	Name	Description
0	Command	Command
1	SafeData[0]	safety data, octet 0
2	SafeData[1]	safety data, octet 1
3	CRC_0_Lo	low octet (bits 0-7) of the 16-bit CRC_0
4	CRC_0_Hi	high octet (bits 8-15) of the 16-bit CRC_0
5	SafeData[2]	safety data, octet 2
6	SafeData[3]	safety data, octet 3
7	CRC_1_Lo	low octet (bits 0-7) of the 16-bit CRC_1
8	CRC_1_Hi	high octet (bits 8-15) of the 16-bit CRC_1
...	...	...
$(n-1) \times 2-1$	SafeData[n-2]	safety data, octet n-2
$(n-1) \times 2$	SafeData[n-1]	safety data, octet n-1
$(n-1) \times 2+1$	CRC_(n-2)/2_Lo	low octet (bits 0-7) of the 16-bit CRC_(n-2)/2
$(n-1) \times 2+2$	CRC_(n-2)/2_Hi	high octet (bits 8-15) of the 16-bit CRC_(n-2)/2
$(n-1) \times 2+3$	Conn_Id_Lo	unique connection ID, low octet
$(n-1) \times 2+4$	Conn_Id_Hi	unique connection ID, high octet

The Safety PDU can transfer n safety data octets. Two octets of data are transferred by a 2-octet CRC.

The shortest Safety PDU consists of 6 octets, which can be used to transfer 1 octet of safety data, as shown in Table 4.

Table 4 – Shortest Safety PDU

Octet	Name	Description
0	Command	Command
1	SafeData[0]	safety data, octet 0
2	CRC_0_Lo	low octet (bits 0-7) of the 16-bit CRC_0
3	CRC_0_Hi	high octet (bits 8-15) of the 16-bit CRC_0
4	Conn_Id_Lo	unique connection ID, low octet
5	Conn_Id_Hi	unique connection ID, high octet

7.1.2 Safety PDU command

The Safety PDU command determines the meaning of the safety data based on the scheme shown in Table 5.

Table 5 – Safety PDU command

Command	Description
0x36	ProcessData
0x2A	Reset
0x4E	Session
0x64	Connection
0x52	Parameter
0x08	FailSafeData

7.1.3 Safety PDU CRC

7.1.3.1 CRC calculation

Two octets of safety data are transferred by a corresponding two octet CRC.

In addition to the transferred data (command, data, ConnID), the CRC_0 of the Safety PDU also includes a virtual sequence number, the CRC_0 of the last received Safety PDU and three additional zero octets. If only one octet safety data is transferred, the SafeData[1] is skipped in the calculation.

```
CRC_0 := f(received CRC_0, ConnID, Sequence_Number, command, SafeData[0],
           SafeData[1], 0x000000)
```

Table 6 shows the calculation sequence for CRC_0.

Table 6 – CRC_0 calculation sequence

Step	Argument
1	received CRC_0 (bit 0-7)
2	received CRC_0 (bit 8-15)
3	ConnID (bit 0-7)
4	ConnID (bit 8-15)
5	Sequence_Number (bit 0-7)
6	Sequence_Number (bit 8-15)
7	Command
8	SafeData[0]
9	SafeData[1]
10	0
11	0
12	0

The CRC_i ($0 < i \leq ((n-2)/2)$) of the Safety PDU additionally includes the index i of the CRC.

```
CRC_i := f(received CRC_0, ConnID, Sequence_Number, command, i,
           SafeData[i × 2], SafeData[i × 2 + 1], 0)
```