

DIN EN 61784-3-14

ICS 35.160; 35.240.50

**Industrielle Kommunikationsnetze –
Profile –****Teil 3-14: Funktional sichere Übertragung bei Feldbussen – Zusätzliche
Festlegungen für die Kommunikationsprofilfamilie 14
(IEC 61784-3-14:2010);
Englische Fassung EN 61784-3-14:2010**

Industrial communication networks –

Profiles –

Part 3-14: Functional safety fieldbuses – Additional specifications for CPF 14

(IEC 61784-3-14:2010);

English version EN 61784-3-14:2010

Réseaux de communication industriels –

Partie 3-14: Bus de terrain à sécurité fonctionnelle –

Spécifications complémentaires pour le CPF 14

(CEI 61784-3-14:2010);

Version anglaise EN 61784-3-14:2010

Gesamtumfang 82 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 61784-3-14 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

Bridge (en: bridge)

abstraktes Gerät, das auf der Sicherungsebene mehrere Netzwerksegmente verbindet

3.1.1.4

Kommunikationskanal (en: communication channel)

logische Verbindung zwischen zwei Endpunkten in einem *Kommunikationssystem*

3.1.1.5

Kommunikationssystem (en: communication system)

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

3.1.1.6

Verbindung (en: connection)

logische Verbindung zwischen zwei Anwendungsobjekten in demselben oder in unterschiedlichen Geräten

3.1.1.7

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 [40], [41]¹⁾.

3.1.1.8

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]

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

²⁾ Noch zu veröffentlichen.

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*.

3.1.1.9

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).

3.1.1.10

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]

3.1.1.11

Feldbus (en: fieldbus)

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

3.1.1.12

Telegrammrahmen (en: frame)

veraltetes Synonym für DLPDU

3.1.1.13

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]

3.1.1.14

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

3.1.1.15

Nachricht (en: message)

geordnete Folge von Oktetts, bestimmt für die Übermittlung von Informationen

[ISO/IEC 2382-16.02.01, modifiziert]

3.1.1.16

Nachrichtensenke (en: message sink)

Teil eines *Kommunikationssystems*, der für den Empfang von *Nachrichten* gedacht ist

[ISO/IEC 2382-16.02.03]

3.1.1.17

Nachrichtenquelle (en: message source)

Teil eines *Kommunikationssystems*, der für den Versand von *Nachrichten* gedacht ist

[ISO/IEC 2382-16.02.02]

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

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]

3.1.1.20

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]

3.1.1.21

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]

3.1.1.22

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

3.1.1.23

Sicherheitsdaten (en: safety data)

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

³⁾ Noch zu veröffentlichen.

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

3.1.1.24

Sicherheitsgerät (en: safety device)

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

3.1.1.25

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]

3.1.1.26

Reaktionszeit einer Sicherheitsfunktion (en: safety function response time)

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 61784-3:2010, 5.2.4, eingeführt und von den in diesem Normteil aufgeführten funktional sicheren Kommunikationsprofilen verwendet.

3.1.1.27

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 61508-1:2010⁴⁾ 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]

3.1.1.28

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.

⁴⁾ Noch zu veröffentlichen.

3.1.1.29**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

3.1.1.30**sicherheitsbezogenes System (en: safety-related system)**

System, welches *Sicherheitsfunktionen* nach IEC 61508 ausführt

3.1.1.31**Zeitstempel (en: time stamp)**

Zeitinformation in einer *Nachricht*

3.1.2 CPF 14: Zusätzliche Begriffe**3.1.2.1****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 des funktional sicheren Verbindungsobjekts und des funktional sicheren Verwaltungsobjekts für sicherheitsbezogene Buseinheiten einer bestimmten sicherheitsbezogenen Anwendung.

3.1.2.2**Kreuzvergleich (en: cross-check)**

Bestätigung, dass die redundant übertragenen Daten identisch sind

3.1.2.3**Makrozyklus (en: macro-cycle)**

einmalige Wiederholung des Link-Level-Schedules

3.1.2.4**Maskerade (en: masquerade)**

Fehler aufgrund irrtümlicher Identifizierungsinformationen

3.1.2.5**Herausgeber (en: publisher)**

Nachrichtenquelle, die Nachrichten auf einer regelmäßig wiederkehrenden Basis überträgt

3.1.2.6**Teilnehmer (en: subscriber)**

Nachrichtensenke, die Nachrichten von einem Herausgeber empfängt

– Leerseite –

**Industrial communication networks -
Profiles -
Part 3-14: Functional safety fieldbuses -
Additional specifications for CPF 14
(IEC 61784-3-14:2010)**

Réseaux de communication industriels -
Partie 3-14: Bus de terrain à sécurité
fonctionnelle -
Spécifications complémentaires
pour le CPF 14
(CEI 61784-3-14:2010)

Industrielle Kommunikationsnetze -
Profile -
Teil 3-14: Funktional sichere Übertragung
bei Feldbussen -
Zusätzliche Festlegungen
für die Kommunikationsprofilfamilie 14
(IEC 61784-3-14:2010)

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 61784-3-14, 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 61784-3-14 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 61784-3-14:2010 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 60204-1	NOTE	Harmonized as EN 60204-1.
IEC 61131-2	NOTE	Harmonized as EN 61131-2.
IEC 61158-2	NOTE	Harmonized as EN 61158-2.
IEC 61326-3-1	NOTE	Harmonized as EN 61326-3-1.
IEC 61326-3-2	NOTE	Harmonized as EN 61326-3-2.
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 61784-1	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 61918	NOTE	Harmonized as EN 61918.
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	8
0.1	General	8
0.2	Patent declaration	10
1	Scope	11
2	Normative references	11
3	Terms, definitions, symbols, abbreviated terms and conventions	12
3.1	Terms and definitions	12
3.1.1	Common terms and definitions	12
3.1.2	CPF 14: Additional terms and definitions	16
3.2	Symbols and abbreviated terms	16
3.2.1	Common symbols and abbreviated terms	16
3.2.2	CPF 14: Additional symbols and abbreviated terms	17
3.3	Conventions	17
4	Overview of FSCP 14/1 (EPASafety®)	17
4.1	EPASafety®	17
4.2	Principle of EPA safety communications	18
4.3	Safety function processing	18
5	General	19
5.1	External documents providing specifications for the profile	19
5.2	Safety functional requirements	19
5.3	Safety measures	20
5.4	Safety communication layer structure	21
5.4.1	Combination of standard communication and safety communication systems	21
5.4.2	CP 14/1 safety communication structure	22
5.5	Relationships with FAL (and DLL, PhL)	23
5.5.1	Overview	23
5.5.2	Data types	23
6	Safety communication layer services	24
6.1	Overview	24
6.2	FSCP 14/1 object extensions	24
6.2.1	General	24
6.2.2	Functional safety communication management object	25
6.2.3	Functional Safety Link Object	26
6.2.4	Functional safety communication alert object	29
6.3	Extended services	30
6.3.1	General	30
6.3.2	SafetyCommunicationOpen	31
6.3.3	SafetyCommunicationClose	33
7	Safety communication layer protocol	34
7.1	Safety PDU format	34
7.1.1	General	34
7.1.2	APDU header structure	34
7.1.3	Functional safety PDU	35
7.2	Safety communication operation	36

7.2.1	Sequence number	36
7.2.2	RelationKey	36
7.2.3	Feedback message	37
7.2.4	CRC-cross-check	37
7.2.5	Scheduling number	38
7.2.6	Time stamp	39
7.2.7	Time expectation	39
7.2.8	Time synchronization monitoring	39
7.2.9	Communication scheduling precision monitoring	39
7.3	Safety communication behaviour	39
7.3.1	Protocol state description of periodic data transmission	39
7.3.2	Protocol state description of non-periodic data transmission	41
7.3.3	Protocol state description of alert report for communication fault	46
7.3.4	Function description	49
7.4	Code	51
7.4.1	Object code	51
7.4.2	Service code	53
8	Safety communication layer management	59
8.1	Time synchronization diagnostics	59
8.1.1	Time synchronization process	59
8.1.2	Time synchronization management	60
8.2	CSME diagnostics	60
8.2.1	General	60
8.2.2	CSME diagnostics management	60
8.3	Communication fault management	61
8.3.1	Configuration management	61
8.3.2	Communication fault report process	61
9	System requirements	64
9.1	Indicators and switches	64
9.2	Installation guidelines	64
9.3	Safety function response time	64
9.3.1	General	64
9.3.2	Calculation of the network reaction time	65
9.4	Duration of demands	66
9.5	Constraints for calculation of system characteristics	66
9.6	Maintenance	67
9.7	Safety manual	67
10	Assessment	67
Annex A (informative) Additional information for functional safety communication profiles of CPF 14		68
A.1 Hash function calculation		68
A.2		69
Annex B (informative) Information for assessment of the functional safety communication profiles of CPF 14		70
Bibliography		71
Annex ZA (normative) Normative references to international publications with their corresponding European publications		74
Table 1 – Relationships between errors and safety measures		21

Table 2 – Data types used within FSCP 14/1	24
Table 3 – FSCP 14/1 object extensions.....	24
Table 4 – Functional safety service extension.....	31
Table 5 – SafetyCommunicationOpen Service Parameters	31
Table 6 – SafetyCommunicationClose Service Parameters.....	33
Table 7 – Encoding of APDU Header	34
Table 8 – Structure of Functional Safety PDU (FSPDU) Header.....	35
Table 9 – CRC calculation polynomials	37
Table 10 – Functional safety communication state description	40
Table 11 – States and transitions of periodic data transmission	40
Table 12 – Functional safety communication states description	42
Table 13 – States and transitions of non-periodic data transmission.....	42
Table 14 – Communication alert state description	47
Table 15 – Communication alert states and transitions	47
Table 16 – LinkObjectType function description	49
Table 17 – CRCCheck function description.....	49
Table 18 – CrossCheck function description	50
Table 19 – TimeDelayCheck function description	50
Table 20 – PeriodUncomfrimedSNCheck function description.....	50
Table 21 – Non-periodicSNCheck function description.....	50
Table 22 – Functional safety communication management object encoding	51
Table 23 – Functional safety link object encoding.....	51
Table 24 – Functional safety communication alert object encoding.....	53
Table 25 – Encoding of SafetyCommunicationOpen request parameters.....	56
Table 26 – SafetyCommunicationOpen positive response parameters	56
Table 27 – SafetyCommunicationOpen negative response parameters.....	57
Table 28 – SafeCommunicationClose request parameters.....	57
Table 29 – SafeCommunicationClose positive response parameters	57
Table 30 – SafeCommunicationClose negative response parameters	57
Table 31 – Error class and code.....	58
Table 32 – Communication process of confirmed service between two devices	61
Table 33 – Settings for time expectation margin.....	65
Table 34 – Constraints for system characteristics at $\varepsilon = 10^{-2}$	67
Figure 1 – Relationships of IEC 61784-3 with other standards (machinery)	8
Figure 2 – Relationships of IEC 61784-3 with other standards (process).....	9
Figure 3 – Safety communication architecture.....	18
Figure 4 – Safety function processing	19
Figure 5 – Standard communication and safety communication	22
Figure 6 – CP 14/1 protocol hierarchy.....	23
Figure 7 – Relationship between the SCL and the other layers of CP 14/1	23
Figure 8 – Functional safety communication message structure.....	34
Figure 9 – Structure of Functional Safety PDU (FSPDU)	35

Figure 10 – Structure of Virtual Safety Check Message (VSCM)	35
Figure 11 – FSPDU mapping	36
Figure 12 – Time-sharing communication scheduling	38
Figure 13 – Format of EndofNonPeriodicDataSending PDU	38
Figure 14 – State transfer figure of periodic data transmission	39
Figure 15 – Functional safety communication state transfer	41
Figure 16 – Communication alert report state transfer figure	46
Figure 17 – CRC check for time synchronization process.....	59
Figure 18 – The process of communication fault report.....	63
Figure 19 – Example application for FSCP 14/1 communication	64
Figure 20 – Calculation of the network reaction time	65

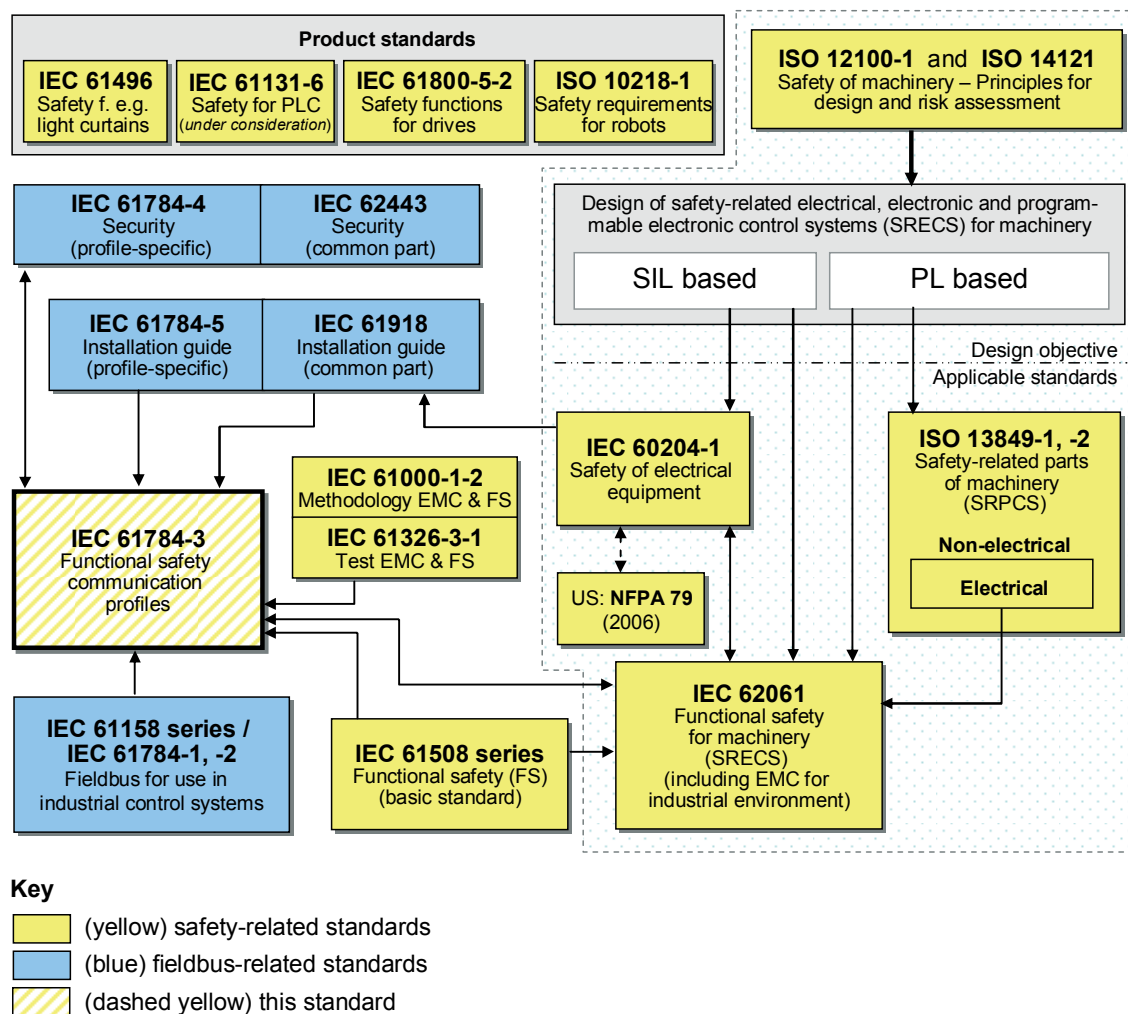
0 Introduction

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.

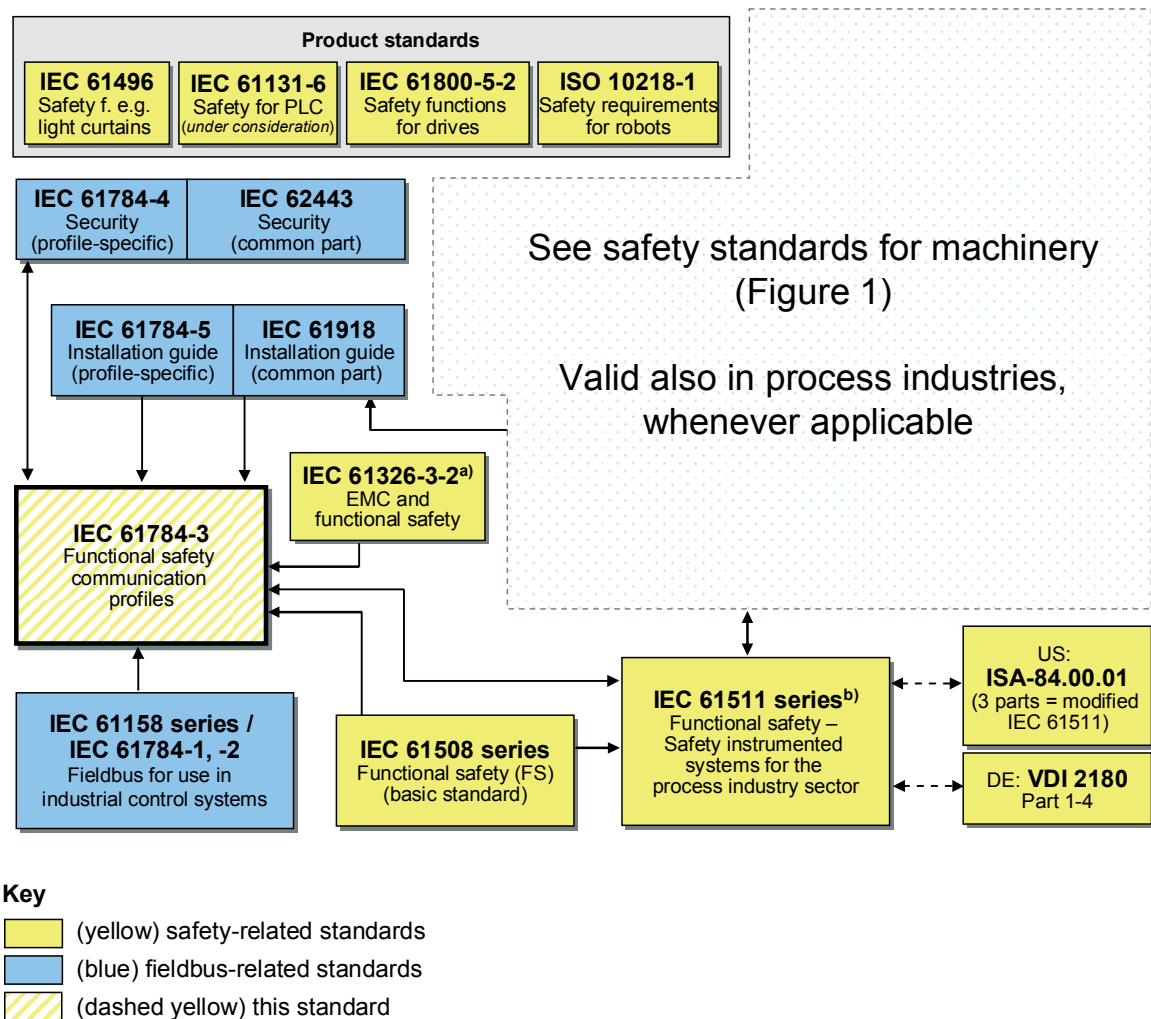
Figure 1 shows the relationships between this standard and relevant safety and fieldbus standards in a machinery environment.



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

CN1960247	[SxZ]	Method of Safety communication for industrial network
CN1929373	[SxZ]	The safety communication for the safety instrument system applied in industrial process.
CN101035030	[SxZ]	The diagnosis method and the equipment for monitoring the industrial Ethernet message.

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:

[SxZ]	SUPCON and Zhejiang university Dongqin FENG
	(1) Zhejiang SUPCON Technology Co., Ltd. Liuhe Road 309, Bingjiang District, Hangzhou, CHINA 310053
	(2) Zhejiang University Zheda Road 38, Hangzhou CHINA 310027

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 3-14: Functional safety fieldbuses – Additional specifications for CPF 14

1 Scope

This part of the IEC 61784-3 series specifies a safety communication layer (services and protocol) based on CPF 14 of IEC 61784-2 and IEC 61158 Type 14. 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 61158 (all parts), *Industrial communication networks – Fieldbus specifications*

IEC 61158-3-14, *Industrial communication networks – Fieldbus specifications – Part 3-14: Data-link layer service definition – Type 14 elements*

IEC 61158-4-14, *Industrial communication networks – Fieldbus specifications – Part 4-14: Data-link layer protocol specification – Type 14 elements*

IEC 61158-5-14, *Industrial communication networks – Fieldbus specifications – Part 5-14: Application layer service definition – Type 14 elements*

IEC 61158-6-14, *Industrial communication networks – Fieldbus specifications – Part 6-14: Application layer protocol specification – Type 14 elements*

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

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

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

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

IEC 61588, *Precision clock synchronization protocol for networked measurement and control 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*

ISO/IEC 8802-3, *Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications*

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

bridge

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

3.1.1.4

communication channel

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

3.1.1.5

communication system

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

3.1.1.6

connection

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

3.1.1.7

Cyclic Redundancy Check (CRC)

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

³ In preparation.

<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 [40], [41]⁴.

3.1.1.8

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*.

3.1.1.9

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)

3.1.1.10

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]

3.1.1.11

fieldbus

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

3.1.1.12

frame

denigrated synonym for DLPDU

3.1.1.13

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]

⁴ Figures in square brackets refer to the bibliography.

⁵ To be published.

3.1.1.14

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

3.1.1.15

message

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

3.1.1.16

message sink

part of a *communication system* in which *messages* are considered to be received
[ISO/IEC 2382-16.02.03]

3.1.1.17

message source

part of a *communication system* from which *messages* are considered to originate
[ISO/IEC 2382-16.02.02]

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

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]

3.1.1.20

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]

3.1.1.21

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]

⁶ To be published.

3.1.1.22

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

3.1.1.23

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.

3.1.1.24

safety device

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

3.1.1.25

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]

3.1.1.26

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 61784-3:2010, 5.2.4 and addressed by the functional safety communication profiles defined in this part.

3.1.1.27

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 61508-1:2010⁷.

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]

3.1.1.28

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.

⁷ To be published.

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

3.1.1.29

safety-related application

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

3.1.1.30

safety-related system

system performing *safety functions* according to IEC 61508

3.1.1.31

time stamp

time information included in a *message*

3.1.2 CPF 14: Additional terms and definitions

3.1.2.1

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 Functional Safety Link Object and Functional Safety Management Object for safety-related bus entities of a particular safety-related application.

3.1.2.2

cross-check

verification that the redundantly transmitted data are identical

3.1.2.3

macro-cycle

one iteration of the link level schedule

3.1.2.4

masquerade

error due to mistaken identification information

3.1.2.5

publisher

message source that transmits messages on a periodic basis

3.1.2.6

subscriber

message sink that receives messages from a publisher

3.2 Symbols and abbreviated terms

3.2.1 Common symbols and abbreviated terms

CP	Communication Profile	[IEC 61784-1]
CPF	Communication Profile Family	[IEC 61784-1]
CRC	Cyclic Redundancy Check	
DLL	Data Link Layer	[ISO/IEC 7498-1]
DLPDU	Data Link Protocol Data Unit	
EMC	Electromagnetic Compatibility	
EUC	Equipment Under Control	[IEC 61508-4:2010]
E/E/PE	Electrical/Electronic/Programmable Electronic	[IEC 61508-4:2010]
FAL	Fieldbus Application Layer	[IEC 61158-5]

FS	Functional Safety	
FSCP	Functional Safety Communication Profile	
MTBF	Mean Time Between Failures	
MTTF	Mean Time To Failure	
PDU	Protocol Data Unit	[ISO/IEC 7498-1]
PFD	Probability of dangerous Failure on Demand	[IEC 61508-6:2010 ⁸]
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	
SIL	Safety Integrity Level	[IEC 61508-4:2010]

3.2.2 CPF 14: Additional symbols and abbreviated terms

AP	Application Process	
APDU	Application Process Data Unit	
ASE	Application Service Element	
ASIC	Application Specific Integrated Circuit	
CSME	Communication Schedule Management Entity	
EPA	Ethernet for Plant Automation	
EPASafety	EPA Safety	
FB	Function Block	
FBAP	Function Block Application Process	
FSPDU	Functional Safety Protocol Data Unit	
IP	Internet Protocol	(RFC 791, see [37])
LED	Light Emitting Diode	
MAC	Medium Access Layer	
MIB	Management Information Base	
SN	Sequence Number	
TCP	Transport Control Protocol	(RFC 793, see [37])
UDP	User Datagram Protocol	(RFC 768, see [37])
VSCM	Virtual Safety Check Message	

3.3 Conventions

This part mainly uses flow charts as appropriate to describe definitions.

4 Overview of FSCP 14/1 (EPASafety®)

4.1 EPASafety®

Communication Profile Family 14 (commonly known as EPA^{®9}) defines communication profiles based on IEC 61158-3-14, IEC 61158-4-14, IEC 61158-5-14, and IEC 61158-6-14.

⁸ To be published.