

BS EN 61784-3-18:2011+A1:2017



BSI Standards Publication

Industrial communication networks — Profiles

Part 3-18: Functional safety fieldbuses
— Additional specifications for CPF 18
(IEC 61784-3-18:2011)



National foreword

This British Standard is the UK implementation of EN 61784-3-18:2011+A1:2017. It is identical to IEC 61784-3-18:2011 incorporating amendment 1:2016. It supersedes BS EN 61784-3-18:2011, which is withdrawn.

The start and finish of text introduced or altered by amendment is indicated in the text by tags. Tags indicating changes to IEC text carry the number of the IEC amendment. For example, text altered by IEC amendment 1 is indicated by A1 A1.

The UK participation in its preparation was entrusted to Technical Committee AMT/7, Industrial communications: process measurement and control, including fieldbus.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2017.

Published by BSI Standards Limited 2017

ISBN 978 0 580 94721 6

ICS 13.110, 25.040.40, 35.100.05

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 July 2011.

Amendments issued since publication

Date	Text affected
31 March 2017	Implementation of IEC amendment 1:2016 with CENELEC endorsement A1:2017

**Industrial communication networks -
Profiles -
Part 3-18: Functional safety fieldbuses -
Additional specifications for CPF 18
(IEC 61784-3-18:2011)**

Réseaux de communication industriels -
Profils -
Partie 3-18: Bus de terrain à sécurité
fonctionnelle -
Spécifications supplémentaires pour le
CPF 18
(CEI 61784-3-18:2011)

Industrielle Kommunikationsnetze -
Profile -
Teil 3-18: Funktional sichere Übertragung
bei Feldbussen -
Zusätzliche Festlegungen für die
Kommunikationsprofilfamilie 18
(IEC 61784-3-18:2011)

This European Standard was approved by CENELEC on 2011-05-25. 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/639/FDIS, future edition 1 of IEC 61784-3-18, 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 61784-3-18 on 2011-05-25.

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) 2012-02-25
- latest date by which the national standards conflicting
with the EN have to be withdrawn (dow) 2014-05-25

Annex ZA has been added by CENELEC.

Endorsement notice

The text of the International Standard IEC 61784-3-18:2011 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 61131-6	NOTE	Harmonized as EN 61131-6 ¹⁾ .
IEC 61158 series	NOTE	Harmonized in EN 61158 series.
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.
IEC 61508-1:2010	NOTE	Harmonized as EN 61508-1:2010.
IEC 61508-4:2010	NOTE	Harmonized as EN 61508-4:2010.
IEC 61508-5:2010	NOTE	Harmonized as EN 61508-5:2010.
IEC 61511 series	NOTE	Harmonized in EN 61511 series.
IEC 61784-1	NOTE	Harmonized as EN 61784-1.
IEC 61784-5 series	NOTE	Harmonized in EN 61784-5 series.
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.

¹⁾ At draft stage.

ISO 13849-2	NOTE Harmonized as EN ISO 13849-2.
ISO 14121	NOTE Harmonized as EN ISO 14121.

Foreword to amendment A1

This document (EN 61784-3-18:2011/A1:2017) consists of the text of IEC 61784-3-18:2011/A1:2016 prepared by SC 65C “Industrial networks” of IEC/TC 65 “Industrial process measurement, control and automation”.

The following dates are fixed:

- latest date by which the document has to be implemented (dop) 2018-01-16
at national level by publication of an identical national standard or by endorsement
- latest date by which the national standards conflicting (dow) 2020-01-16
with the document have to be withdrawn

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

Endorsement notice

The text of the International Standard IEC 61784-3-18:2011/A1:2016 was approved by CENELEC as a European Standard without any modification.

Annex ZA (normative)

Normative references to international publications with their corresponding European publications

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.

NOTE When an international publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
IEC 61158-3-22	-	Industrial communication networks - Fieldbus - specifications - Part 3-22: Data-link layer service definition - Type 22 elements	-	-
IEC 61158-4-22	-	Industrial communication networks - Fieldbus - specifications - Part 4-22: Data-link layer protocol specification - Type 22 elements	-	-
IEC 61158-5-22	-	Industrial communication networks - Fieldbus - specifications - Part 5-22: Application layer service definition - Type 22 elements	-	-
IEC 61158-6-22	-	Industrial communication networks - Fieldbus - specifications - Part 6-22: Application layer protocol specification - Type 22 elements	-	-
IEC 61508	Series	Functional safety of electrical/electronic/programmable electronic safety-related systems	EN 61508	Series
IEC 61508-2	2010	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems	EN 61508-2	2010
IEC 61784-2	2010	Industrial communication networks - Profiles - Part 2: Additional fieldbus profiles for real-time networks based on ISO/IEC 8802-3	EN 61784-2	2010
IEC 61784-3	2010	Industrial communication networks - Profiles - Part 3: Functional safety fieldbuses - General rules and profile definitions	EN 61784-3	2010
IEC 61918	-	Industrial communication networks - Installation of communication networks in industrial premises	EN 61918	-
ISO/IEC 10731	-	Information technology - Open Systems Interconnection - Basic reference model - Conventions for the definition of OSI services	-	-

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 18: Additional terms and definitions	16
3.2	Symbols and abbreviated terms	17
3.2.1	Common symbols and abbreviated terms	17
3.2.2	CPF 18: Additional symbols and abbreviated terms	18
3.3	Conventions	18
4	Overview of FSCP 18/1 (SafetyNET p™)	20
4.1	General	20
4.2	FSCP 18/1	20
5	General	21
5.1	External documents providing specifications for the profile	21
5.2	Safety functional requirements	21
5.3	Safety measures	22
5.4	Safety communication layer structure	22
5.5	Relationships with FAL (and DLL, PhL)	23
5.5.1	General	23
5.5.2	Data Types	23
6	Safety communication layer services	23
6.1	General elements	23
6.1.1	General	23
6.1.2	Safety object dictionary	23
6.1.3	Safety process data object (SPDO)	23
6.1.4	Safety heartbeat (SHB)	23
6.1.5	Safety delay monitoring (SDM)	24
6.2	Communication relation	24
7	Safety communication layer protocol	25
7.1	Safety PDU format	25
7.1.1	General	25
7.1.2	Safety process data objects (SPDO)	25
7.1.3	Safety heartbeat (SHB)	27
7.1.4	Safety PDUs embedded in a Type 22 PDU	29
7.2	Safety communication layer management (SALMT)	30
7.3	Safety process data communication	32
7.4	Safety heartbeat	34
7.5	Delay monitoring	35
8	Safety communication layer management	36
8.1	Parameter handling	36
8.2	Safety object dictionary	36

8.2.1	General	36
8.2.2	Communication profile section	37
8.2.3	Standardized device profile section	53
9	System requirements	53
9.1	Indicators and switches	53
9.1.1	Indicator states and flash rates	53
9.1.2	Indicators	53
9.1.3	Switches	54
9.2	Installation guidelines	54
9.3	Safety function response time	54
9.3.1	General	54
9.3.2	Determination of FSCP 18/1 time expectation behavior	55
9.3.3	Calculation of the worst case safety function response time	55
9.4	Duration of demands	55
9.5	Constraints for calculation of system characteristics	55
9.5.1	Safety related constraints	55
9.5.2	Probabilistic considerations	57
9.6	Maintenance	57
9.7	Safety manual	57
10	Assessment	58
Annex A (informative) Additional information for functional safety communication profiles of CPF 18		59
Annex B (informative) Information for assessment of the functional safety communication profiles of CPF 18		60
Bibliography		61
Table 1 – Object definition		19
Table 2 – Safety PDU element definition		19
Table 3 – Communication errors and detection measures		22
Table 4 – SPDO PDU structure		26
Table 5 – SHB request PDU structure		27
Table 6 – SHB response PDU structure		28
Table 7 – SHB safety communication layer state encoding		29
Table 8 – SALMT commands		30
Table 9 – System states of SALMT state machine		31
Table 10 – State transitions SALMT state machine		32
Table 11 – System states of RxSPDO state machine		33
Table 12 – State transitions RxSPDO state machine		33
Table 13 – Timeouts		34
Table 14 – Safety object dictionary structure		36
Table 15 – Objects of communication section		37
Table 16 – Device type		38
Table 17 – Safety ID		39
Table 18 – Safety consumer heartbeat entry		39
Table 19 – Safety consumer heartbeat		40
Table 20 – Safety producer heartbeat parameter		41

Table 21 – Safety bus cycle times	44
Table 22 – SPDO timeout tolerance	45
Table 23 – Receive SPDO communication parameter	45
Table 24 – Transmit SPDO communication parameter	48
Table 25 – Mapping format	51
Table 26 – Receive SPDO mapping parameter	51
Table 27 – Transmit SPDO mapping parameter	52
Table 28 – Indicator states definiton	53
Table 29 – STATUS indicator states	53
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 – FSCP 18/1 system	20
Figure 4 – FSCP 18/1 software architecture	22
Figure 5 – SPDO interaction model	24
Figure 6 – SHB interaction model	24
Figure 7 – Safety process data object structure	25
Figure 8 – Safety heartbeat request structure	27
Figure 9 – Safety heartbeat response structure	28
Figure 10 – Safety PDU for FSCP 18/1 embedded in a Type 22 CDC data section	30
Figure 11 – SALMT state machine	31
Figure 12 – RxSPDO state machine	33
Figure 13 – Heartbeat procedure	34
Figure 14 – Delay measurement principle	35
Figure 15 – Parameter handling	36
Figure 16 – Safety response time components	54
Figure 17 – Considered data fields for message size calculation	56
Figure 18 – Residual error rate	57

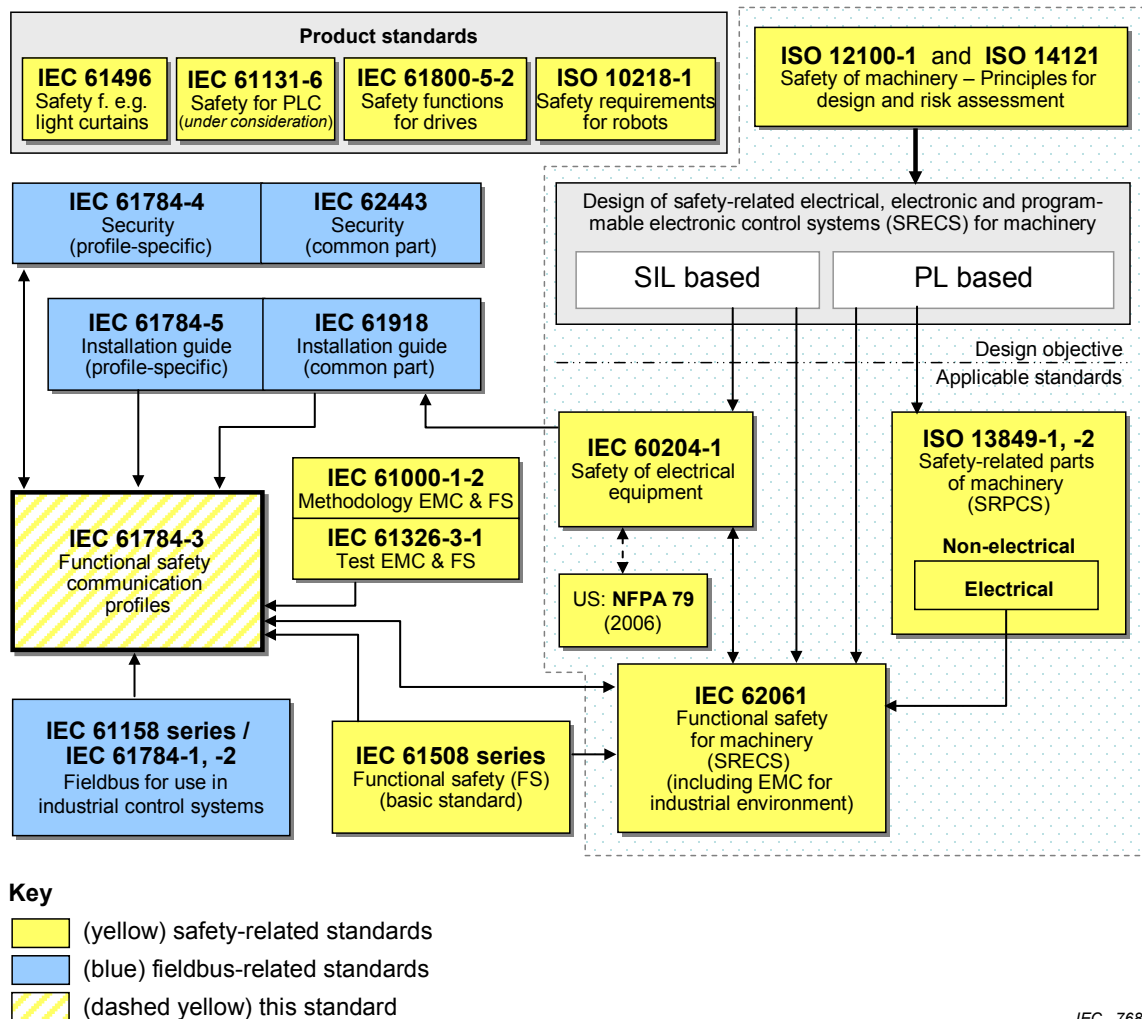
0 Introduction

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.

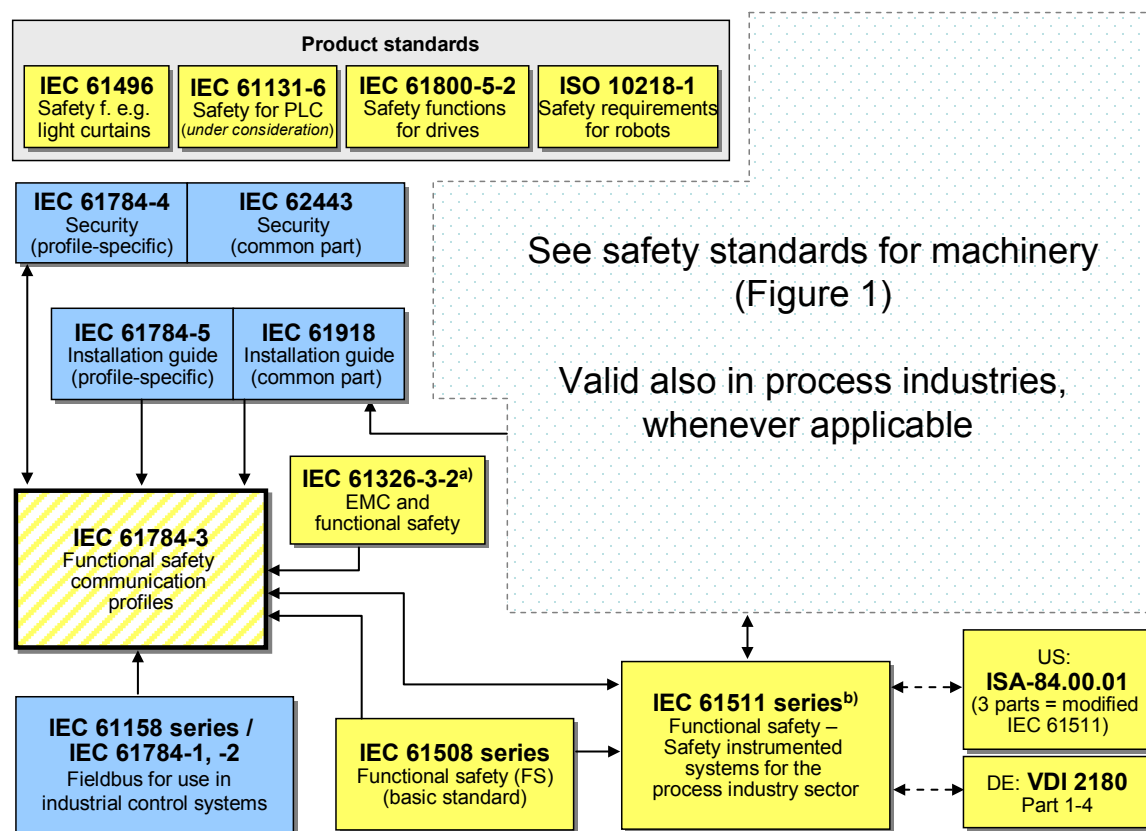
Figure 1 shows the relationships between this standard and relevant safety and fieldbus standards in a machinery environment.



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.



Key

- (yellow) safety-related standards
- (blue) fieldbus-related standards
- (dashed yellow) this standard

IEC 769/11

^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 a patent concerning the functional safety communication profiles for family 18 as follows, where the [xx] notation indicates the holder of the patent right:

DE 10 2008 007 672.4-31 [PI] Verfahren und Vorrichtung zum Übertragen von Daten in einem Netzwerk

IEC takes no position concerning the evidence, validity and scope of this patent right.

The holder of this patent right has assured the IEC that he/she is willing to negotiate licences either free of charge or under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statement of the holder of this patent right is registered with IEC. Information may be obtained from:

Information may be obtained from:

[PI] Pilz GmbH & Co. KG
Felix-Wankel-Str. 2
73760 Ostfildern
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.

ISO (www.iso.org/patents) and IEC (http://www.iec.ch/tctools/patent_decl.htm) maintain on-line data bases of patents relevant to their standards. Users are encouraged to consult the data bases for the most up to date information concerning patents.

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES

Part 3-18: Functional safety fieldbuses – Additional specifications for CPF 18

1 Scope

This part of the IEC 61784-3 series specifies a safety communication layer (services and protocol) based on CPF 18 of IEC 61784-2 and IEC 61158 Type 22. 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 61158-3-22, *Industrial communication networks – Fieldbus specifications – Part 3-22: Data-link layer service definition – Type 22 elements*

IEC 61158-4-22, *Industrial communication networks – Fieldbus specifications – Part 4-22: Data-link layer protocol specification – Type 22 elements*

IEC 61158-5-22, *Industrial communication networks – Fieldbus specifications – Part 5-22: Application layer service definition – Type 22 elements*

IEC 61158-6-22, *Industrial communication networks – Fieldbus specifications – Part 6-22: Application layer protocol specification – Type 22 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 61508-2:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*

IEC 61784-2:2010, *Industrial communication networks – Profiles – Part 2: Additional fieldbus profiles for real-time networks based on ISO/IEC 8802-3*

IEC 61784-3:2010, *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*

ISO/IEC 10731, *Information technology – Open system interconnection – Basic reference model – Conventions for the definition of OSI services*

3 Terms, definitions, symbols, abbreviated terms and conventions

3.1 Terms and definitions

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

3.1.1 Common terms and definitions

3.1.1.1

availability

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

3.1.1.2

black channel

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

3.1.1.3

communication channel

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

3.1.1.4

communication system

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

3.1.1.5

connection

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

3.1.1.6

Cyclic Redundancy Check (CRC)

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

<method> procedure used to calculate the redundant data

NOTE 1 Terms “CRC code” and “CRC signature”, and labels such as CRC1, CRC2, may also be used in this standard to refer to the redundant data.

NOTE 2 See also [35], [36]³.

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 61508-4:2010], [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 IEV 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

frame

denigrated synonym for DLPDU

3.1.1.12

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 [35], [36].

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

³ Figures in square brackets refer to the Bibliography.

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]

3.1.1.14

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

nuisance trip

spurious trip with no harmful effect

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

3.1.1.19

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]

3.1.1.20

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

[IEC 61508-4:2010, modified], [ISO/IEC 2382-14.01.12, 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 61508-5:2010.

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

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 61508-1:2010.

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 “SIL n 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.

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

spurious trip

trip caused by the safety system without a process demand

3.1.2 CPF 18: Additional terms and definitions

3.1.2.1

client/server relationship

relationship where the client sends data to the server, which replies with the requested data

3.1.2.2

consecutive number

unsigned integer with wrap to zero on overflow which is used as means to ensure completeness and the right order of transmitted safety PDUs

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

3.1.2.3

cycle

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

3.1.2.4

delay

transmission time of PDUs which is dynamically caused by network properties like traffic, switching devices and topology

3.1.2.5

fail-safe

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

3.1.2.6

gateway

device acting as a linking element between different protocols

3.1.2.7

logical double line

sequence of root device and all ordinary devices processing the communication frame in forward and backward direction

3.1.2.8

producer/consumer relationship

relationship where the producer sends data to the consumer without a specific request

3.1.2.9

real time frame line (RTFL)

communication model with devices communicating in a logical double line (see CP 18/2)

3.1.2.10

real time frame network (RTFN)

communication model with devices communicating in a switched network (see CP 18/1)

3.1.2.11

SCL management (SALMT)

mechanism to control the SCL state of safety devices

3.1.2.12

safety delay monitoring (SDM)

safety mechanism to cyclically monitor the delay of transmitted PDUs

3.1.2.13

safety heartbeat (SHB)

mechanism to cyclically monitor the state of safety devices

3.1.2.14

safety process data object (SPDO)

mechanism to cyclically exchange safety process data between devices

3.1.2.15

sender/receiver relationship

relationship where the sender sends data to the receiver

3.1.2.16

1:1 relationship

communication relationship with exactly one sender and one receiver

3.1.2.17

1:n relationship

communication relationship with exactly one sender and one or many receivers

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	
PDU	Protocol Data Unit	[ISO/IEC 7498-1]
PFH	Average frequency of dangerous failure [h ⁻¹]	[IEC 61508-4]
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 18: Additional symbols and abbreviated terms

3.2.2.1 Additional abbreviated terms

AL	Application layer
AP	Application process
CDC	Cyclic data channel
FSF	Fail-safe
ID	Identification
PDO	Process data object
PDO-ID	Process data object ID
PID	Packet ID
RTFL	Real time frame line
RTFN	Real time frame network
SALMT	SCL management
SDM	Safety delay monitoring
SHB	Safety heartbeat
SID	Safety ID
SPDO	Safety process data object

3.2.2.2 Additional symbols

Symbol	Definition	Description	Unit
T_A	Actuator time	Worst case response time of the actuator for conversion and reaction according to the safety function	μs
T_{cycle}	Cycle time	Cycle time of communication	μs
T_I	Input time	Worst case processing time of the input device	μs
T_L	Logic processing time	Worst case processing time of the safety logic controller	μs
T_O	Output time	Worst case processing time of the output device	μs
T_S	Sensor time	Worst case response time of the sensor from the detection of a physical signal change to valid conversion result	μs
T_{SFR}	Safety function response time	Safety function response time from the physical input signal to the reaction on the actuator	μs
T_{TOi}	Timeout time of component	Timeout time for safety component i	μs
T_{TOS}	Transmission time	Worst case transmission time of the communication network. Timeout time for FSCP 18/1	μs
ΔT	Timeout margin	Additional margin on transmission cycle time. This value is defined by the user based on the application requirements. Typical range is 0 % to 15 %	μs

3.3 Conventions

The attributes of an object are described in the form as shown in Table 1. The meaning of the attributes is described in the following list.

- Index describes the position within the safety object dictionary of an object.
- Sub-index describes a single element of the object containing the following data. It will be repeated for each element of the object.
 - Name denotes a name string for this attribute.
 - Description is used for additional information on how the object shall be used.

- Object type denotes the characterizing type for each object as specified in IEC 61158-6-22.
- Data Type denotes the data type of this element.
- Category indicates whether the element is mandatory (M), optional (O) or depends upon setting of other attributes (C).
- Access attribute shows the access right to this element. RO means read access right, RW means read and write access right, WO means write access right, while FSF denotes no access rights except for the safety application and optional read access by SDO services as specified in IEC 61158-5-22 and IEC 61158-6-22.
- SPDO mapping denotes the possibility to map this attribute to TxSPDO or RxSPDO or to indicate that this parameter is not mappable.
- Value range contains the value range of a dedicated element or “No” for no pre-defined value range.
- Value contains the constant value(s) and/or the meaning of the parameter or “No” for no pre-defined value.

Table 1 – Object definition

Attribute	Value
Index	
Sub-index	
Name	
Description	
Object type	
Data type	
Category	
Access attribute	
SPDO mapping	
Value range	
Value	

The FSCP syntax elements related to PDU structure are described as shown in Table 2. The meaning of the table columns is described in the following list.

- Octet offset denotes the offset of the DLPDU part relative to the start of the safety PDU.
- Data field is the name of the element.
- Value/Description contains the constant value or the meaning of the parameter.

Table 2 – Safety PDU element definition

Octet offset	Data field	Description