

INTERNATIONAL STANDARD

NORME INTERNATIONALE



**Industrial communication networks – Profiles –
Part 3-18: Functional safety fieldbuses – Additional specifications for CPF 18**

**Réseaux de communication industriels – Profils –
Partie 3-18: Bus de terrain de sécurité fonctionnelle – Spécifications
supplémentaires pour CPF 18**



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2021 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'IEC ou du Comité national de l'IEC du pays du demandeur. Si vous avez des questions sur le copyright de l'IEC ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de l'IEC de votre pays de résidence.

IEC Central Office
3, rue de Varembe
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigendum or an amendment might have been published.

IEC publications search - webstore.iec.ch/advsearchform

The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee, ...). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

IEC Customer Service Centre - webstore.iec.ch/csc

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

IEC online collection - oc.iec.ch

Discover our powerful search engine and read freely all the publications previews. With a subscription you will always have access to up to date content tailored to your needs.

Electropedia - www.electropedia.org

The world's leading online dictionary on electrotechnology, containing more than 22 000 terminological entries in English and French, with equivalent terms in 18 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

A propos de l'IEC

La Commission Electrotechnique Internationale (IEC) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications IEC

Le contenu technique des publications IEC est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Recherche de publications IEC -

webstore.iec.ch/advsearchform

La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études, ...). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

IEC Just Published - webstore.iec.ch/justpublished

Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et une fois par mois par email.

Service Clients - webstore.iec.ch/csc

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: sales@iec.ch.

IEC online collection - oc.iec.ch

Découvrez notre puissant moteur de recherche et consultez gratuitement tous les aperçus des publications. Avec un abonnement, vous aurez toujours accès à un contenu à jour adapté à vos besoins.

Electropedia - www.electropedia.org

Le premier dictionnaire d'électrotechnologie en ligne au monde, avec plus de 22 000 articles terminologiques en anglais et en français, ainsi que les termes équivalents dans 16 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.



IEC 61784-3-18

Edition 1.2 2021-04
CONSOLIDATED VERSION

INTERNATIONAL STANDARD

NORME INTERNATIONALE



**Industrial communication networks – Profiles –
Part 3-18: Functional safety fieldbuses – Additional specifications for CPF 18**

**Réseaux de communication industriels – Profils –
Partie 3-18: Bus de terrain de sécurité fonctionnelle – Spécifications
supplémentaires pour CPF 18**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 25.040.40; 35.100.05

ISBN 978-2-8322-9767-4

**Warning! Make sure that you obtained this publication from an authorized distributor.
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.**

REDLINE VERSION

VERSION REDLINE



**Industrial communication networks – Profiles –
Part 3-18: Functional safety fieldbuses – Additional specifications for CPF 18**

**Réseaux de communication industriels – Profils –
Partie 3-18: Bus de terrain de sécurité fonctionnelle – Spécifications
supplémentaires pour CPF 18**

CONTENTS

FOREWORD	5
0 Introduction	7
0.1 General	7
0.2 Patent declaration	11
INTRODUCTION to Amendment 2	11
1 Scope	12
2 Normative references	12
3 Terms, definitions, symbols, abbreviated terms and conventions	13
3.1 Terms and definitions	13
3.1.1 Common terms and definitions	13
3.1.2 CPF 18: Additional terms and definitions	17
3.2 Symbols and abbreviated terms.....	18
3.2.1 Common symbols and abbreviated terms	18
3.2.2 CPF 18: Additional symbols and abbreviated terms	19
3.3 Conventions	19
4 Overview of FSCP 18/1 (SafetyNET p™)	21
4.1 General	21
4.2 FSCP 18/1	21
5 General	22
5.1 External documents providing specifications for the profile	22
5.2 Safety functional requirements	22
5.3 Safety measures	23
5.4 Safety communication layer structure	23
5.5 Relationships with FAL (and DLL, PhL)	24
5.5.1 General	24
5.5.2 Data Types	24
6 Safety communication layer services	24
6.1 General elements	24
6.1.1 General	24
6.1.2 Safety object dictionary	25
6.1.3 Safety process data object (SPDO)	25
6.1.4 Safety heartbeat (SHB).....	25
6.1.5 Safety delay monitoring (SDM)	25
6.2 Communication relation	25
7 Safety communication layer protocol	27
7.1 Safety PDU format	27
7.1.1 General	27
7.1.2 Safety process data objects (SPDO).....	27
7.1.3 Safety heartbeat (SHB).....	29
7.1.4 Safety PDUs embedded in a Type 22 PDU	31
7.2 Safety communication layer management (SALMT)	32
7.3 Safety process data communication	34
7.4 Safety heartbeat.....	36
7.5 Delay monitoring	37
8 Safety communication layer management.....	38

8.1	Parameter handling	38
8.2	Safety object dictionary	38
8.2.1	General	38
8.2.2	Communication profile section	39
8.2.3	Standardized device profile section	55
9	System requirements	55
9.1	Indicators and switches	55
9.1.1	Indicator states and flash rates	55
9.1.2	Indicators	56
9.1.3	Switches	56
9.2	Installation guidelines	56
9.3	Safety function response time	56
9.3.1	General	56
9.3.2	Determination of FSCP 18/1 time expectation behavior	57
9.3.3	Calculation of the worst case safety function response time	58
9.4	Duration of demands	58
9.5	Constraints for calculation of system characteristics	58
9.5.1	Safety related constraints	58
~~9.5.2~~	~~Probabilistic considerations~~	~~58~~
9.6	Maintenance	60
9.7	Safety manual	60
10	Assessment	61
Annex A (informative) Additional information for functional safety communication profiles of CPF 18		62
A.1	Hash function calculation	62
A.2	Void	65
Annex B (informative) Information for assessment of the functional safety communication profiles of CPF 18		66
Bibliography		67
Figure 1 – Relationships of IEC 61784-3 with other standards (machinery)		8
Figure 2 – Relationships of IEC 61784-3 with other standards (process)		10
Figure 3 – FSCP 18/1 system		21
Figure 4 – FSCP 18/1 software architecture		24
Figure 5 – SPDO interaction model		26
Figure 6 – SHB interaction model		26
Figure 7 – Safety process data object structure		27
Figure 8 – Safety heartbeat request structure		29
Figure 9 – Safety heartbeat response structure		30
Figure 10 – Safety PDU for FSCP 18/1 embedded in a Type 22 CDC data section		32
Figure 11 – SALMT state machine		33
Figure 12 – RxSPDO state machine		35
Figure 13 – Heartbeat procedure		36
Figure 14 – Delay measurement principle		37
Figure 15 – Parameter handling		38
Figure 16 – Safety response time components		57

Figure 17 – Considered data fields for message size calculation..... 59

~~Figure 18 – Residual error rate~~

Table 1 – Object definition	20
Table 2 – Safety PDU element definition.....	20
Table 3 – Communication errors and detection measures	23
Table 4 – SPDO PDU structure	28
Table 5 – SHB request PDU structure	29
Table 6 – SHB response PDU structure	30
Table 7 – SHB safety communication layer state encoding	31
Table 8 – SALMT commands	32
Table 9 – System states of SALMT state machine.....	33
Table 10 – State transitions SALMT state machine	34
Table 11 – System states of RxSPDO state machine	35
Table 12 – State transitions RxSPDO state machine.....	35
Table 13 – Timeouts	36
Table 14 – Safety object dictionary structure	38
Table 15 – Objects of communication section	39
Table 16 – Device type	40
Table 17 – Safety ID	41
Table 18 – Safety consumer heartbeat entry.....	42
Table 19 – Safety consumer heartbeat.....	43
Table 20 – Safety producer heartbeat parameter	44
Table 21 – Safety bus cycle times.....	47
Table 22 – SPDO timeout tolerance	48
Table 23 – Receive SPDO communication parameter	48
Table 24 – Transmit SPDO communication parameter	51
Table 25 – Mapping format	54
Table 26 – Receive SPDO mapping parameter	54
Table 27 – Transmit SPDO mapping parameter	55
Table 28 – Indicator states definiton	56
Table 29 – STATUS indicator states	56

INTERNATIONAL ELECTROTECHNICAL COMMISSION

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES

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

FOREWORD

- 1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as “IEC Publication(s)”). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
- 2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
- 3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
- 4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
- 5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
- 6) All users should ensure that they have the latest edition of this publication.
- 7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
- 8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.

This consolidated version of the official IEC Standard and its amendments has been prepared for user convenience.

IEC 61784-3-18 edition 1.2 contains the first edition (2011-04) [documents 65C/639/FDIS and 65C/649/RVD], its amendment 1 (2016-07) [documents 65C/851/FDIS and 65C/854/RVD] and its amendment 2 (2021-04) [documents 65C/1083/FDIS and 65C/1087/RVD].

In this Redline version, a vertical line in the margin shows where the technical content is modified by amendments 1 and 2. Additions are in green text, deletions are in strikethrough red text. A separate Final version with all changes accepted is available in this publication.

International Standard IEC 61784-3-18 has been prepared by subcommittee 65C: Industrial networks, of IEC technical committee 65: Industrial process measurement, control and automation.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

A list of all parts of the IEC 61784-3 series, published under the general title *Industrial communication networks – Profiles – Functional safety fieldbuses*, can be found on the IEC website.

The committee has decided that the contents of the base publication and its amendments will remain unchanged until the stability date indicated on the IEC web site under "<http://webstore.iec.ch>" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

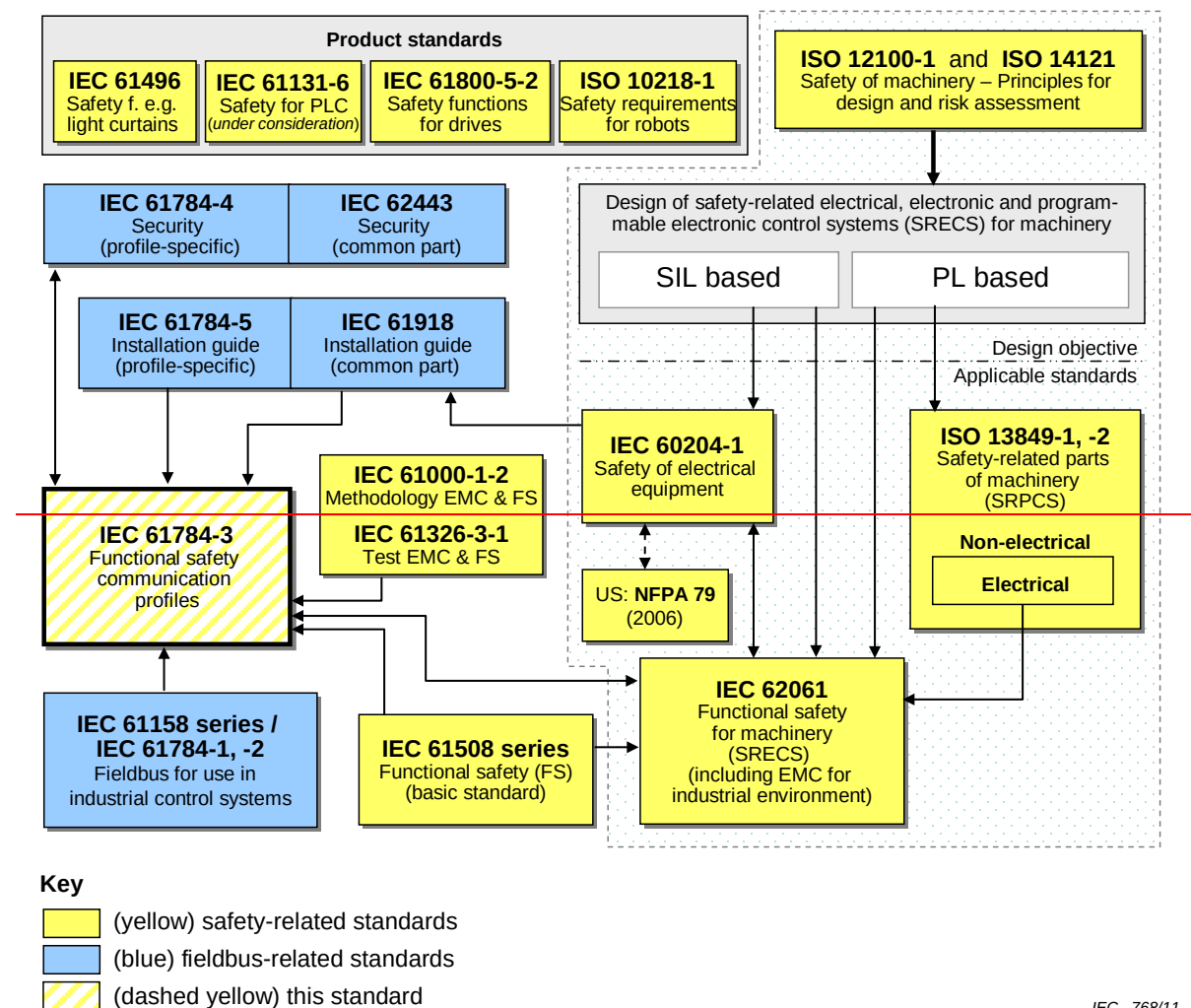
0 Introduction

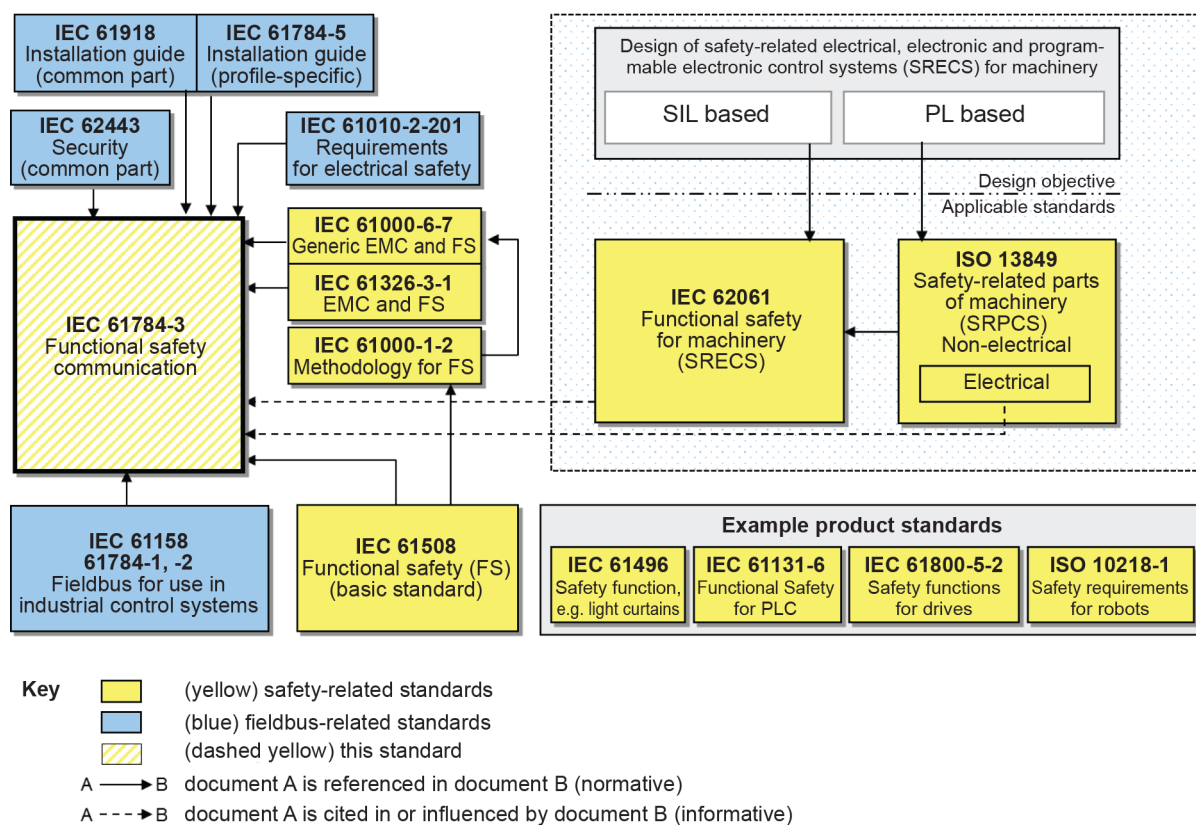
0.1 General

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.

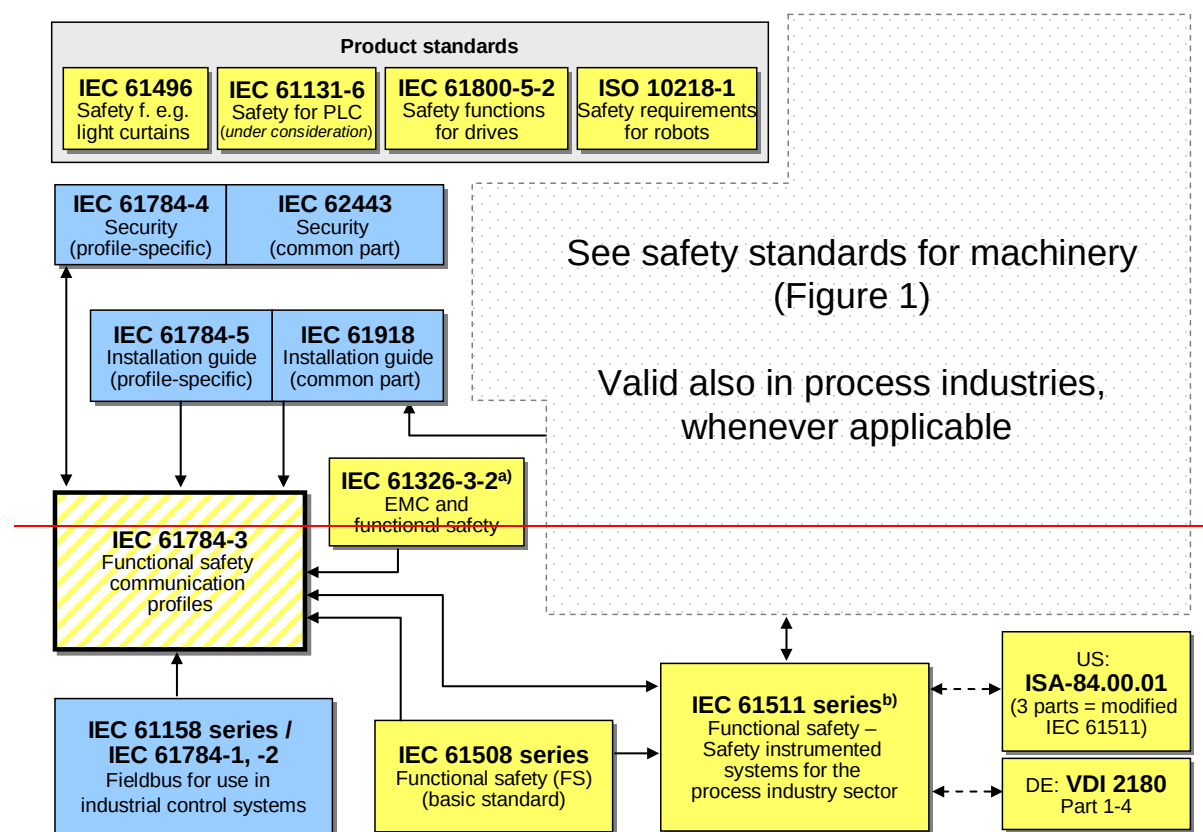




~~NOTE Subclauses 6.7.6.4 (high complexity) and 6.7.8.1.6 (low complexity) of IEC 62061 specify the relationship between PL (Category) and SIL. IEC 62061 specifies the relationship between PL (Category) and SIL.~~

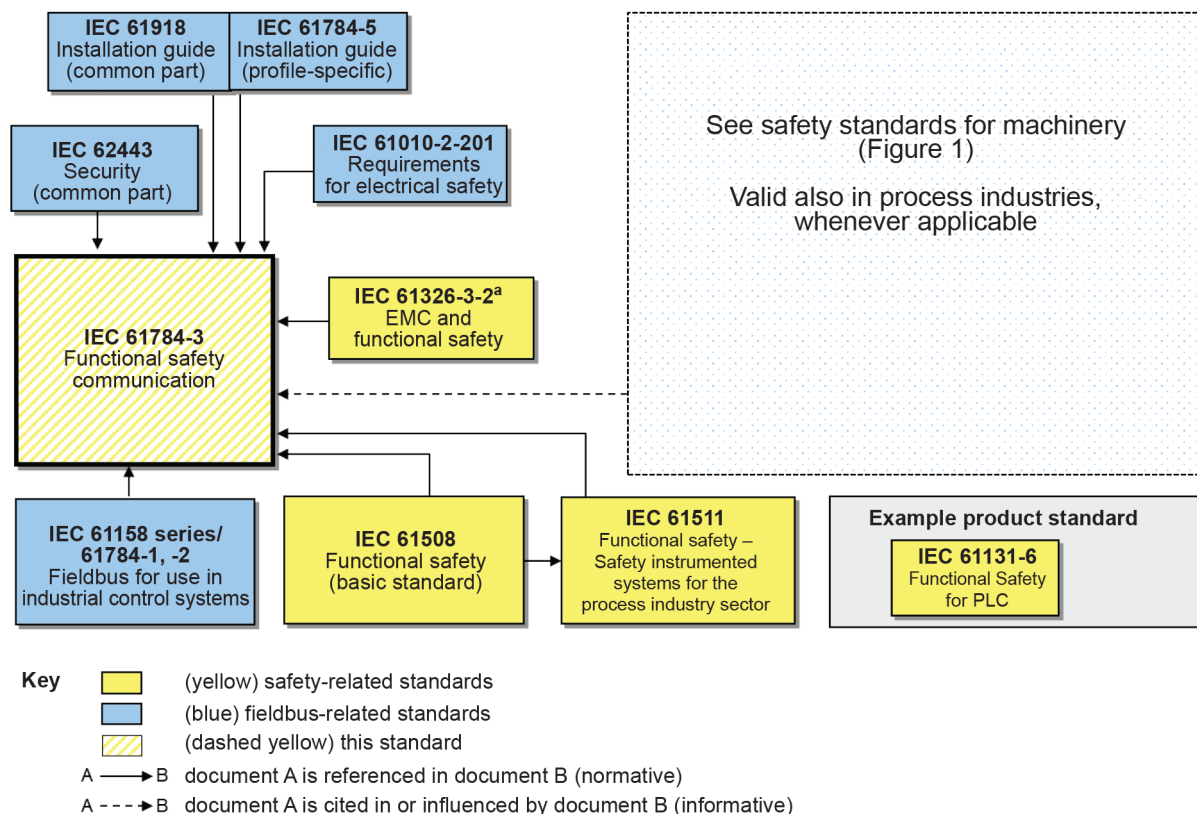
Figure 1 – Relationships of IEC 61784-3 with other standards (machinery)

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_{IEC}

^a For specified electromagnetic environments; otherwise IEC 61326-3-1 or IEC 61000-6-7.

^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.

INTRODUCTION to Amendment 2

This Amendment 2 introduces several editorial and informational corrections in the context of Edition 4 of IEC 61784-3.

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

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

³ Figures in square brackets refer to the Bibliography.

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 mapable.
- 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

4 Overview of FSCP 18/1 (SafetyNET p™)

4.1 General

Communication Profile Family 18 (commonly known as SafetyNET p™⁴) defines communication profiles based on IEC 61158-3-22, IEC 61158-4-22, IEC 61158-5-22 and IEC 61158-6-22.

The basic profiles CP 18/1 and CP 18/2 are defined in IEC 61784-2:2010. The functional safety communication profile FSCP 18/1 (SafetyNET p™) is based on the CPF 18 basic profiles in IEC 61784-2 and the safety communication layer specifications defined in this part.

4.2 FSCP 18/1

FSCP 18/1 describes a safety protocol for transferring safety process data up to SIL 3 between FSCP 18/1 devices. For the transfer of the safety protocol, a subordinated fieldbus is used that is not included in the safety considerations (black channel approach). Safety data exchanged between communicating partners is regarded as cyclic process data exchanged between them by the subordinated fieldbus.

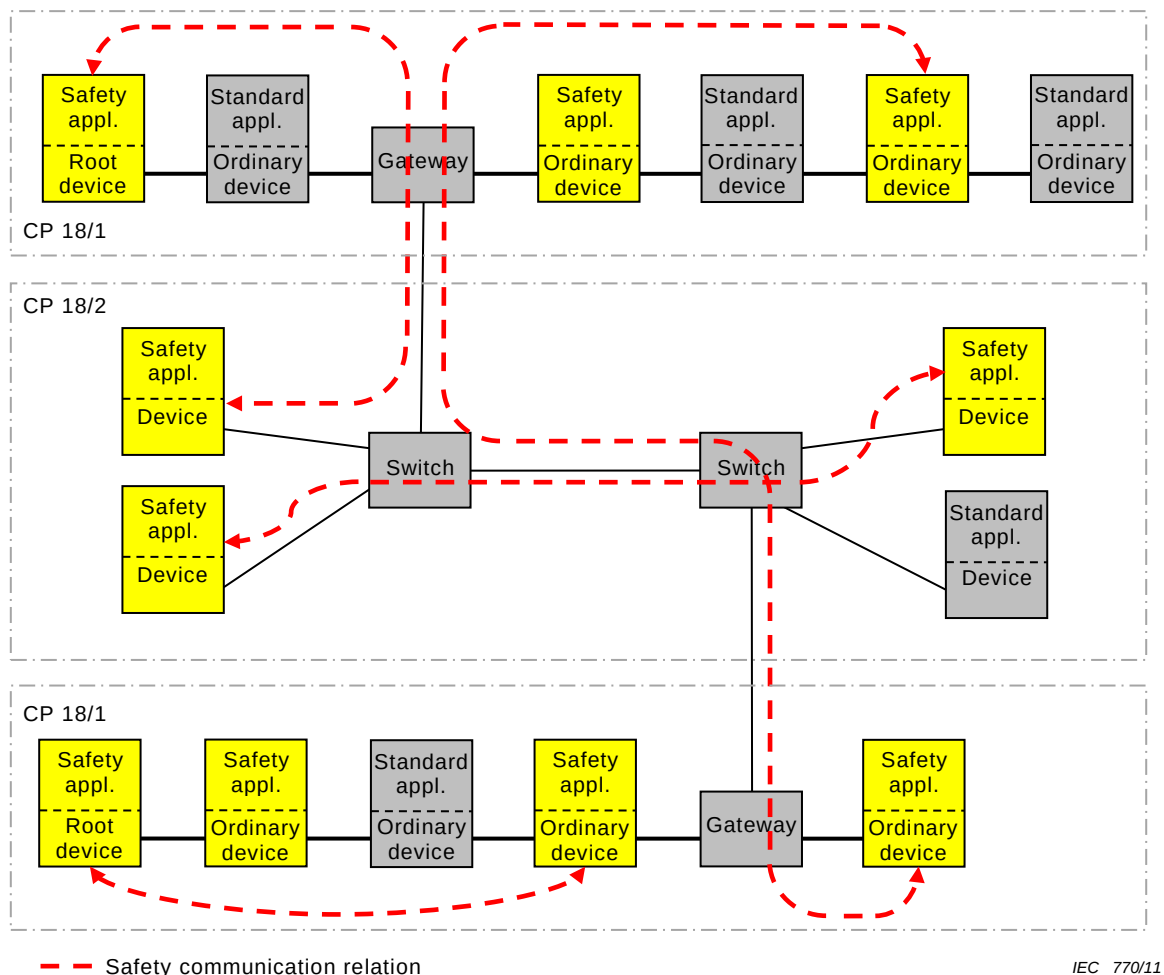


Figure 3 – FSCP 18/1 system

⁴ SafetyNET p is a trade name of Pilz GmbH & Co. KG. 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 part does not require use of the trade name SafetyNET p. Use of the trade name SafetyNET p requires permission of Pilz GmbH & Co. KG.

FSCP 18/1 uses a dedicated 1:n relationship of the producer/consumer relationship type for safety process data communication and a 1:1 relationship for the purpose of safety device monitoring. Figure 3 shows possible communication relationships based on a CP 18/1 and CP 18/2 network.

For the realization of FSCP 18/1, the following safety measures have been chosen:

- session number (consecutive number);
- time expectation for communication monitoring;
- unique identification of senders;
- cyclic redundancy checking for data integrity;
- different data integrity assurance systems for safety and non-safety communication;
- packet delay monitoring for dedicated communication relationships.

Each device maintains a safety communication layer state machine, which is coordinated by the safety application. Safety is ensured based on the SCL switching to the system error state (i.e. safe state) as soon as an error is detected.

5 General

5.1 External documents providing specifications for the profile

~~The following document is useful in understanding the design of FSCP 18/1 protocol:~~

- ~~• GS-ET-26 [34]~~

There is no additional external document used for FSCP 18/1.

5.2 Safety functional requirements

The following requirements shall apply to the development of devices that implement the FSCP 18/1 protocol. The same requirements were used in the development of FSCP 18/1.

- Requirements of IEC 61508 shall be fulfilled.
- The FSCP 18/1 protocol is designed to support Safety Integrity Level 3 (SIL 3) (see IEC 61508).
- FSCP 18/1 protocol is implemented using a black channel approach; there is no safety related dependency on the standard CPF 18 communication profiles. Transmission equipment shall remain unmodified.
- Safety communication and standard communication shall be independent. Safety devices and standard devices shall be able to use the same communication channel.
- There shall always be a 1:1 relationship between communicating devices for device monitoring purpose.
- Safety communication shall use a single-channel communication system. Redundancy may only be used optionally for increased availability.
- Implementation of the safety protocol shall be restricted to the communication end devices.
- The transmission duration time shall be monitored.
- Devices documentations shall indicate the Safety Integrity Level (SIL) they are designed for.
- For devices using protocol version 2 (see 7.1.3.4) it is required to add 10^{-9} to the PFH of the device hardware to account for the communication channel.

NOTE In this way, the user of the device will not have to account for the number of logical connections within a safety function.

- The use of error correction mechanisms in the black channel is permitted.

5.3 Safety measures

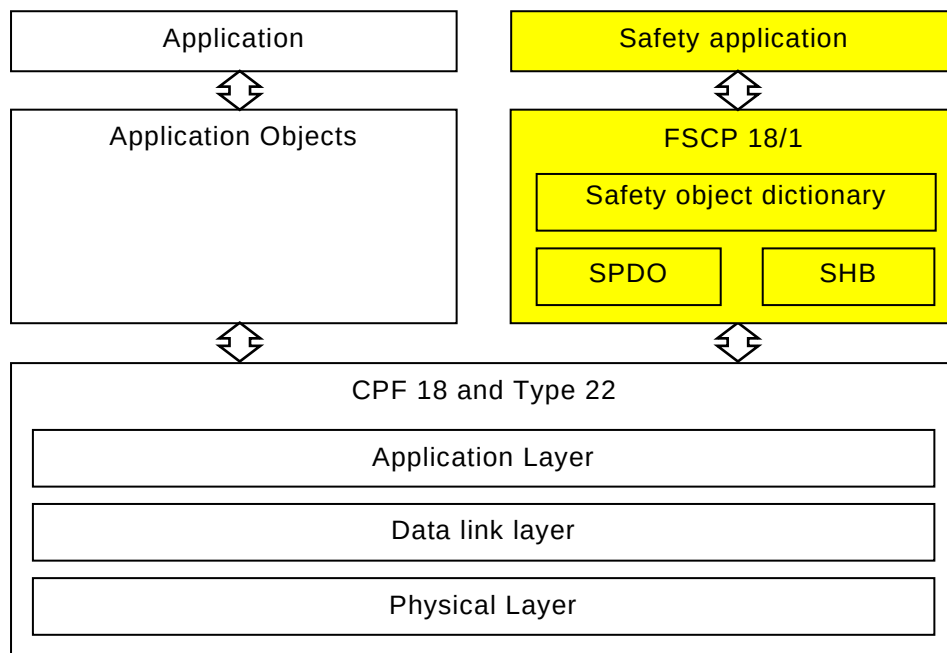
The safety measures used in the FSCP 18/1 to detect communication errors are listed in Table 3. All safety measures shall be applied and monitored within each safety device.

Table 3 – Communication errors and detection measures

Communication errors	Safety measures				
	Sequence number	Time expectation ^a	Connection authentication ^b	Data integrity assurance	Diff. data integrity assurance systems
Corruption	—	—	—	X	—
Unintended repetition	X	—	—	—	—
Incorrect sequence	X	—	—	—	—
Loss	X	X	—	—	—
Unacceptable delay	—	X	—	—	—
Insertion	X	—	X	—	—
Masquerade	X	—	X	—	X
Addressing	X	—	X	—	—
Revolving memory failures within switches	X	X	X	X	—
^a In this standard called “T _{TOS} ”.					
^b In this standard realized by “SID” and “PID”.					

5.4 Safety communication layer structure

Figure 4 shows how the protocol is related to CPF 18 and Type 22. The FSCP 18/1 safety communication layer is located on top of the CPF 18 and Type 22 application and data link layers and utilizes the non-safety services of CPF 18 and Type 22 to transfer safety PDUs.



IEC 771/11

Figure 4 – FSCP 18/1 software architecture

A safety process data object (SPDO) containing the safety process data, the identification information and the required error detection measures is included in the Type 22 process data objects. The mapping of the safety process data to SPDOs is done by entries in the safety object dictionary.

Monitoring of the time synchronization of the safety application is realized using a safety heartbeat service (SHB).

The calculation of the residual error probability for the FSCP 18/1 protocol takes no credit of the error detection mechanisms of the communication system. The protocol can also be transferred via other communication systems.

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 18 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 18 data types as defined in IEC 61158-5-22. The encoding of these data types follows the encoding rules defined in IEC 61158-6-22.

6 Safety communication layer services

6.1 General elements

6.1.1 General

The FSCP 18/1 provides the following elements:

- safety object dictionary;
- safety process data object (SPDO);

- safety heartbeat (SHB);
- safety delay monitoring (SDM).

6.1.2 Safety object dictionary

The safety object dictionary is the interface between the safety application and the communication system. It is a grouping of objects and specifies uniform communication and device parameters for the safety-related functionality. The organization of objects is adjusted with the organization of CP 18/1 and CP 18/2. Access to safety object dictionary entries can optionally be realized by SDO services as defined in IEC 61158-5-22 and IEC 61158-6-22. This access shall be restricted to read only (RO) access.

6.1.3 Safety process data object (SPDO)

Safety process data objects shall provide the required services for safety related process data exchange between certain communicating devices. Safety process data communication in FSCP 18/1 is cyclic, using safety process data objects (SPDOs). The process data communication is split into safety transmit and receive process data objects (TxSPDOs or RxSPDO).

6.1.4 Safety heartbeat (SHB)

Devices which implement FSCP 18/1 SCL use SHB service for application layer monitoring and application monitoring. This service is independent of any other heartbeat services that devices could implement in parallel. SHB messages are confirmed cyclic messages exchanged between communicating devices and realize a 1:1 relationship between devices. The SHB mechanism is used to synchronize the system clocks of the communicating devices.

6.1.5 Safety delay monitoring (SDM)

The safety delay monitoring service is used to monitor the delay of packets within a communication relationship of communicating devices. This mechanism is based on a confirmed service relation between devices. The service monitors that the time between producing the service request and receiving the service confirmation does not exceed a configurable maximum delay. Further on, the service monitors the time between two successful delay measurements. This time shall not exceed a configuration dependent time in which it would be possible that the delay arises over the maximum allowed delay.

6.2 Communication relation

FSCP 18/1 defines a 1:n relationship with producer/consumer relationship for safety process data communication. Producers shall cyclically send safety process data objects identified by a unique PDO-ID for packet identification and a unique safety ID for producer identification. Safety process data object interaction is unconfirmed. Figure 5 shows the safety process data object interaction model (see ISO/IEC 10731 for explanation of sequence chart).

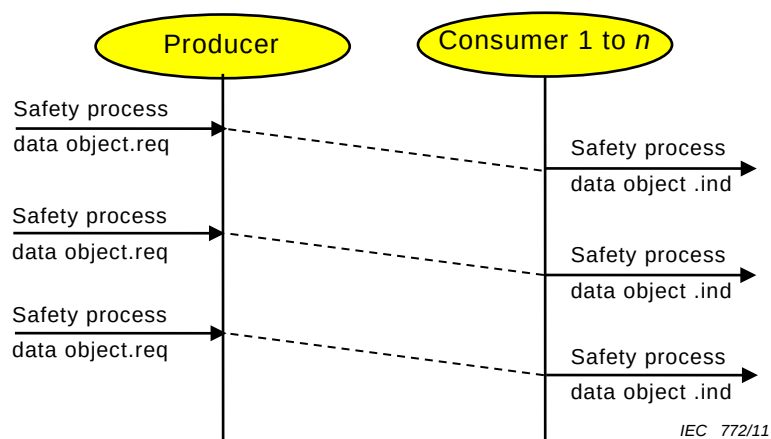


Figure 5 – SPDO interaction model

The state and presence of communication partners (i.e. producers and consumers) in FSCP 18/1 is monitored independently by each participating device. For all communication relations from one dedicated device to one other dedicated device one heartbeat relationship is executed. Thus, a 1:1 relationship between communication partners exists. Safety heartbeat communication follows the confirmed client/server relationship. Figure 6 shows heartbeat interactions for a safety process data object relationship. The cycle time of the heartbeat service is independent from other communication cycle times and depends on the safety function response time as well as from the maximum allowed growth of message delivery time.

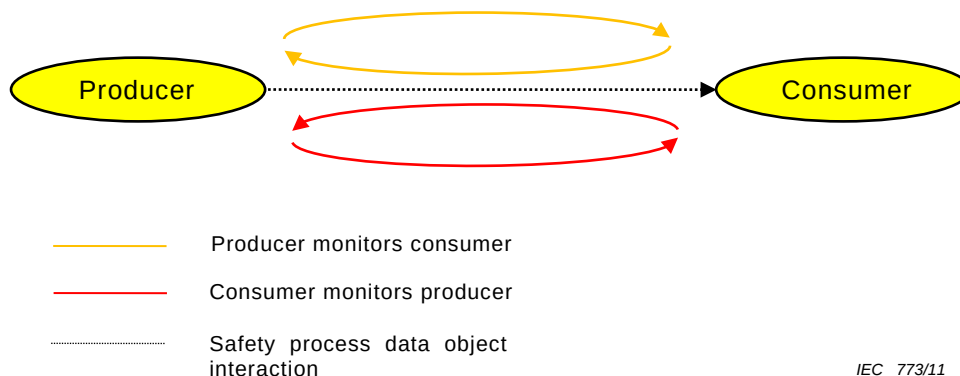


Figure 6 – SHB interaction model

Safety related process data communication using FSCP 18/1 is based on the following two essential components:

- safety process data objects (SPDO);
- safety heartbeat (SHB).

The FSCP 18/1 communication cycle mainly consists of cyclic unconfirmed exchange of safety process data objects. A time expectation behavior is used on the consumer-side to monitor safety process data exchange and to detect communication failures. Because of the unconfirmed interaction model an additional mechanism is required which enables the detection of a failed device and which also enables the detection of an increased PDU delivery delay besides the time expectation of the consumer. This is realized by safety heartbeat service. Both mechanisms in combination define and observe a communication cycle.

7 Safety communication layer protocol

7.1 Safety PDU format

7.1.1 General

7.1.1.1 PDU structure

A safety PDU consists of either a safety process data object (SPDO) or a safety heartbeat (SHB). While the SPDO is used to communicate the safety application data, the SHB is used to synchronise the communicating devices.

7.1.1.2 Data integrity

The receiver of a safety PDU shall verify the safety integrity of the data by checking both copies of the data (SPDO or SHB) against their CRCs and by comparing the CRCs of the two copies of the data.

If transmissions repetitions are configured, then each reception shall be checked as specified above. The reception of the safety PDU shall be treated as failed if all repetitions failed the data integrity check.

7.1.2 Safety process data objects (SPDO)

7.1.2.1 SPDO structure

Figure 7 defines the structure of a safety process data object and its data fields.

PID	Length	Safety data 1	SID 1	Cons. no. 1	CRC 1	Safety data 2	SID 2	Cons. no. 2	CRC 2
-----	--------	---------------	-------	-------------	-------	---------------	-------	-------------	-------

IEC 774/11

Figure 7 – Safety process data object structure

The SPDO is cyclically transferred via the subordinate fieldbus. The content of one SPDO consists of one or several safety application objects out of the safety object dictionary. The mapping from the safety object dictionary element to the SPDO is done by the SPDO mapping entries in Table 25 and Table 26. Table 23 is used to identify the mapping table index of Table 26 based on the PID of the SPDO.

In Table 4 the general structure of a SPDO is listed.

Table 4 – SPDO PDU structure

Octet offset	Data field	Description
0 to 2	PID	Packet ID
3	Length	Length of the complete packet in octets
4 to 4+(~~$n-1$~~)	Safety data 1	Mapped safety application process data
4+n to 5+n	SID 1	Safety ID of the sender
6+n to 6+n+m-1	Consecutive number 1	Consecutive number for sequencing and application monitoring where: $m = 1$ for protocol version 1 $m = 3$ for protocol version 2
7+n+m to 10+n+m	CRC 1	32 bit cyclic redundancy check covering data fields PID, ~~length~~ , safety data 1, SID 1 and consecutive number 1
11+n+m to 11+2(~~$n-1$~~)+m	Safety data 2	Copy of mapped safety application process data
11+2n+m to 12+2n+m	SID 2	Copy of SID 1
13+2n+m to 13+2n+2m-1	Consecutive number 2	Copy of consecutive number 1
14+2n+2m to 17+2n+2m	CRC 2	32 bit cyclic redundancy check covering data fields PID, ~~length~~ , safety data 2, SID 2 and consecutive number 2
NOTE 1 n is the length in octets of the data field safety data 1 (safety data 2).		
NOTE 2 m is the length of the consecutive number depending on the protocol version (see 7.1.3.4).		

7.1.2.2 SPDO PID

This data field is an identification number of the packet which, in conjunction with the SID field uniquely identifies the packet.

7.1.2.3 SPDO length

This data field shall contain the complete packet length in octets.

7.1.2.4 Safety data

This data field shall contain the safety application objects according to the mapping configuration.

In order to allow the safety PDU to be transported via a black channel whose transfer characteristics are not included in the safety considerations, the amount of data is restricted from 0 to 115 octets for protocol version 2 or respectively 117 octets for protocol version 1. For the data integrity assurance system applied by this FSCP the residual error rate per hour does not exceed 10^{-9} ~~as proven in 9.5.2.~~

7.1.2.5 SPDO SID

This data field is a 16 bit identifier of the sender. This value shall be unique across the network. Each participating FSCP 18/1 device obtains one SID. The SID of a device is stored within the corresponding safety object dictionary entry with index 0x1200. The SID shall not be 0. The number is generated by the network configuration tool which shall ensure the uniqueness of the SPDO SID.

7.1.2.6 SPDO consecutive number

This data field is an ~~8-bit~~ consecutive number (cyclic counter) for application layer life-sign monitoring and packet sequencing. This number is generated by the sender of the SPDO. The

size of the consecutive number depends on the protocol version (see 7.1.3.4) and is 1 octet for protocol version 1 and 3 octets for protocol version 2.

7.1.2.7 SPDO CRC

This data field contains the 32 bit CRC covering the data fields PID, ~~length~~, data, SID and consecutive number.

The polynomial ~~0x20044009~~ 0x120044009 is used for calculating the CRCs. For details see 7.1.2.4 and ~~9.5.2~~ Clause A.1.

7.1.3 Safety heartbeat (SHB)

7.1.3.1 SHB structure

7.1.3.1.1 SHB request PDU

Figure 8 shows the structure of a safety heartbeat request PDU.

PID	Length	SCL state 1	Safety AP state 1	SID 1	Cons. No.1	CRC 1	SCL state 2	Safety AP state 2	SID 2	Cons. No.2	CRC 2
-----	--------	-------------	-------------------	-------	------------	-------	-------------	-------------------	-------	------------	-------

IEC 775/11

Figure 8 – Safety heartbeat request structure

Table 5 lists the general structure of this PDU.

Table 5 – SHB request PDU structure

Octet offset	Data field	Description
0 to 2	PID	Packet ID
3	Length	Length of the complete packet in octets
4	SCL state 1	SALMT state (see Table 7)
~~5 to 6+(n-1)~~ 5 to 5+n-1	Safety AP state 1	Safety application process state (implementation specific)
6+n to 7+n	SID 1	Safety ID of the sender
8+n to 8+n+m-1	Consecutive number 1	Consecutive number for sequencing and application monitoring where: $m = 1$ for protocol version 1 $m = 3$ for protocol version 2
9+n+m to 12+n+m	CRC 1	32 bit cyclic redundancy check covering data fields PID, ~~length~~ , SCL state 1, Safety AP state 1, SID 1 and consecutive number 1
13+n+m	SCL state 2	Copy of SALMT state 1
~~14 to 15+(n-1)~~ 14+n+m to 14+2n+m-1	Safety AP state 2	Copy of safety application process state 1
15+2n+m to 16+2n+m	SID 2	Copy of SID 1
17+2n+m to 17+2n+2m-1	Consecutive number 2	Copy of consecutive number 1
18+2n+2m to 21+2n+2m	CRC 2	32 bit cyclic redundancy check covering data fields PID, ~~length~~ , SCL state 2, Safety AP state 2, SID 2 and consecutive number 2

NOTE 1 n is the length in octets of the data field Safety AP state.

Octet offset	Data field	Description
NOTE 2 m is the length of the consecutive number, depending on the protocol version (see 7.1.3.4).		

7.1.3.1.2 SHB response PDU

Figure 9 shows the structure of a safety heartbeat response PDU.

PID	Length	SID 1	Cons. no. 1	CRC 1	SID 2	Cons. no. 2	CRC 2
-----	--------	-------	----------------	-------	-------	----------------	-------

Figure 9 – Safety heartbeat response structure

Table 6 lists the general structure of this PDU.

Table 6 – SHB response PDU structure

Octet offset	Data field	Description
0 to 2	PID	Packet ID
3	Length	Length of the complete packet in octets
4 to 5	SID 1	Safety ID of the sender
6 to 6+m-1	Consecutive number 1	Consecutive number for sequencing and application monitoring where: $m = 1$ for protocol version 1 $m = 3$ for protocol version 2
7+m to 10+m	CRC 1	32 bit cyclic redundancy check covering data fields PID, ~~length~~ , SID 1 and consecutive number 1
11+m to 12+m	SID 2	Copy of SID 1
13+m to 13+2m-1	Consecutive number 2	Copy of consecutive number 1
14+2m to 17+2m	CRC 2	32 bit cyclic redundancy check covering data fields PID, ~~length~~ , SID 2 and consecutive number 2
NOTE m is the length of the consecutive number, depending on the protocol version (see 7.1.3.4).		

7.1.3.2 SHB PID

This data field is an identification number of the packet which, in conjunction with the SID field uniquely identifies the packet.

7.1.3.3 SHB length

This data field shall contain the complete packet length in octets.

7.1.3.4 SHB safety communication layer state

This data field shall contain state information about the SCL. This information is interpreted by SHB receivers. Table 7 specifies the encoding of the content of this data field.

Table 7 – SHB safety communication layer state encoding

Value	Description	Protocol
0x00	FS FAL is in BOOTUP state	Version 1
0x04	FS FAL is in STOPPED state	Version 1
0x05	FS FAL is in OPERATIONAL state	Version 1
0x7F	FS FAL is in PRE-OPERATIONAL state	Version 1
0x10	FS FAL is in BOOTUP state	Version 2
0x14	FS FAL is in STOPPED state	Version 2
0x15	FS FAL is in OPERATIONAL state	Version 2
0x1F	FS FAL is in OPERATIONAL state	Version 2

The device shall support at least one protocol version. The FS FAL state shall be encoded according to Table 7 depending on the used protocol version. It is recommended to support all protocol versions.

7.1.3.5 SHB safety AP state

This data field shall contain state information about the safety application. The content and encoding of this data field are application dependent and are outside the scope of this international standard. The length is restricted from 0 to 114 octets for protocol version 2 or respectively 116 octets for protocol version 1.

7.1.3.6 SHB SID

This data field is the 16 bit identifier of the sender. This value shall be unique across the network. Each participating FSCP 18/1 device obtains a SID. The SID of a device is stored within the corresponding safety object dictionary entry with index 0x1200. The SID shall not be 0. The number is generated by the network configuration tool which shall ensure the uniqueness of the SHB SID.

7.1.3.7 SHB consecutive number

This data field is an ~~8-bit~~ consecutive number (cyclic counter) for application layer life-sign monitoring and packet sequencing. In the event of a response PDU this data field contains the consecutive number of the PDU confirmed by this response. This number is generated by the sender of the SHB. The size of the consecutive number depends on the protocol version (see 7.1.3.4) and is 1 octet for protocol version 1 and 3 octets for protocol version 2.

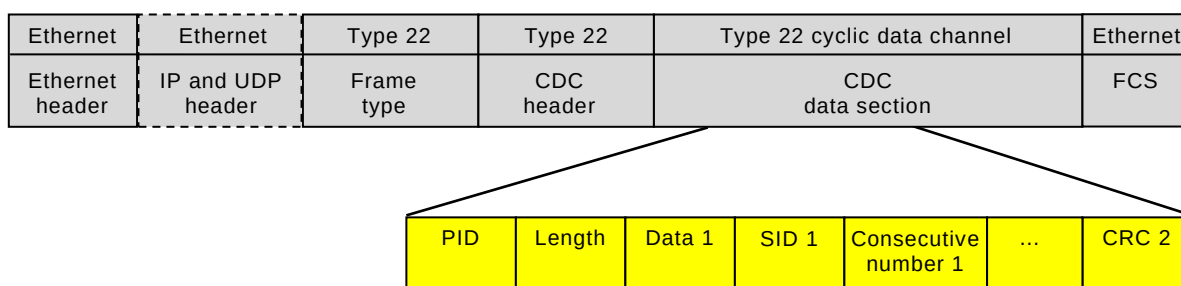
7.1.3.8 SHB CRC

This data field contains the 32 bit CRC covering the data fields PID, ~~length~~, data, SID and consecutive number.

The polynomial ~~0x20044009~~ 0x120044009 is used for calculating the CRCs. For details see 7.1.3.5 and ~~9.5.2~~ Clause A.1.

7.1.4 Safety PDUs embedded in a Type 22 PDU

Figure 10 shows the structure of a FSCP 18/1 safety PDU embedded in a Type 22 CDC DLPDU. The presence of IP and UDP header information depends on the used communication profile. For details about the Type 22 DLPDU refer to IEC 61158-4-22.



IEC 777/11

Figure 10 – Safety PDU for FSCP 18/1 embedded in a Type 22 CDC data section

7.2 Safety communication layer management (SALMT)

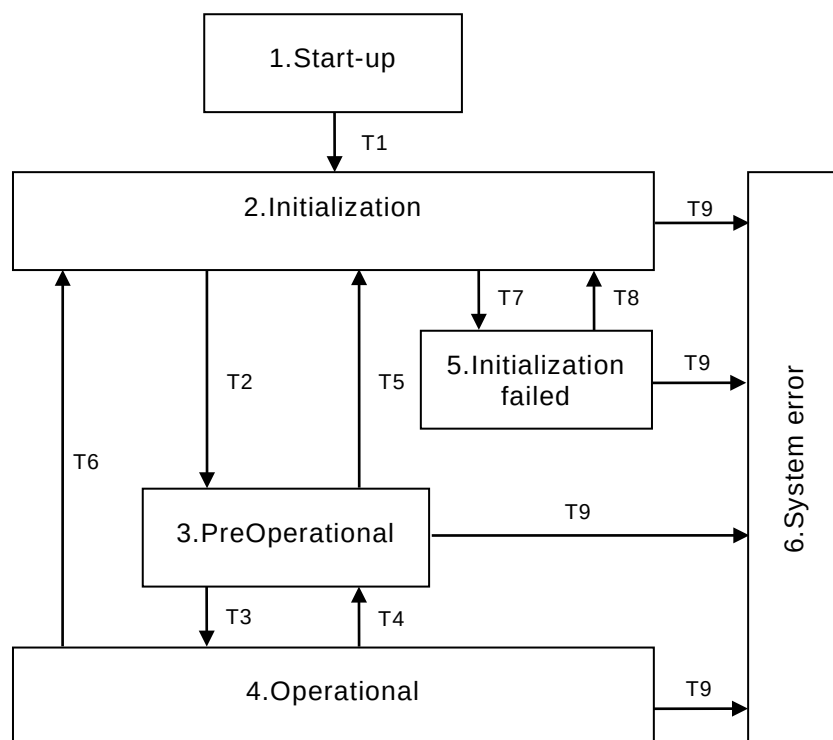
By the local SALMT service it is possible to trigger the state machine of the SCL and thus to control the behavior of the safety part of a device.

The SALMT commands as specified in Table 8 are available.

Table 8 – SALMT commands

Command	Description
0x01	Reset communication
0x02	Reset node
0x03	Stop remote node
0x04	Start remote node
0x05	Enter preoperational

Figure 11 shows the SALMT state machine. All states of the state machine shall be supported.



IEC 778/11

Figure 11 – SALMT state machine

The local management commands are related to the transitions and states in the SALMT state machine, as specified in Table 9 and Table 10.

Table 9 – System states of SALMT state machine

State number	State	Description
1	Start up	Virtual state after device start-up. Sending and receiving of SPDO and SHB PDUs are not allowed.
2	Initialization	System dependant initialisation. Sending and receiving of SPDO and SHB PDUs are not allowed.
3	PreOperational	Configuration is being performed or system awaits request to start operational state. Sending and receiving of SHB PDUs are allowed. SPDO PDUs are not allowed.
4	Operational	Operational state. Sending and receiving of SPDO and SHB PDUs are allowed.
5	Initialisation failed	A non safety relevant error occurred during initialisation. Sending and receiving of SHB PDUs are allowed. SPDO PDUs are not allowed.
6	System error	Safety relevant error has been detected. Sending and receiving of SPDO and SHB PDUs are not allowed.

Table 10 – State transitions SALMT state machine

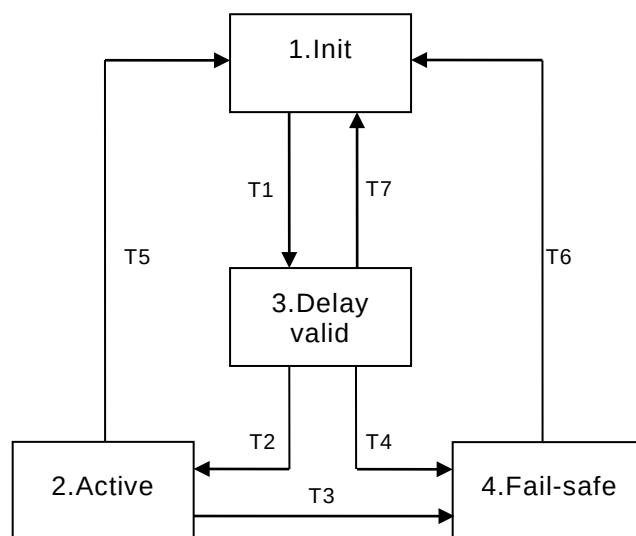
State transition	From state number	To state number	Description	Action
T1	1	2	Automatic state transition after device start-up	Disable sending and receiving of SPDO and SHB PDUs
T2	2	3	Transition is initiated by SALMT command enter "PreOperational" state	Enable sending and receiving of SHB PDUs. Disable sending and receiving of SPDO PDUs
T3	3	4	Transition is initiated by SALMT command start remote node	Enable sending and receiving of SPDO and SHB PDUs
T4	4	3	Transition is initiated by SALMT command stop remote node	Enable sending and receiving of SHB PDUs. Disable sending and receiving of SPDO PDUs
T5	3	2	Transition is initiated by SALMT command reset node or reset communication	Disable sending and receiving of SPDO and SHB PDUs
T6	4	2	Transition is initiated by SALMT command reset node or reset communication	Disable sending and receiving of SPDO and SHB PDUs
T7	2	5	Transition is initiated by a failure or fault during initialization	Enable sending and receiving of SHB PDUs. Disable sending and receiving of SPDO PDUs
T8	5	2	Transition is initiated by SALMT command reset node	Disable sending and receiving of SPDO and SHB PDUs
T9	2, 3, 4 or 5	6	This transition is initiated by a system error	Disable sending and receiving of SPDO and SHB PDUs

7.3 Safety process data communication

Safety process data communication is based on a 1:*n* relationship of the producer/consumer relationship type. No confirmation messages are used. Communication relationships are configured during system configuration phase. There exists no further online connection management.

A time expectation behavior is used on the consumer-side to monitor safety process data exchange and to detect communication failures. The SPDO cycle time is monitored with an appropriate timeout mechanism. Furthermore, producer and consumer monitor the packet delay to identify an unacceptable increase.

Figure 12 shows the RxSPDO state machine. This state machine is applied for each configured RxSPDO. All states shall be supported.



IEC 779/11

Figure 12 – RxSPDO state machine

Table 11 to Table 13 describe the state transitions and the related events and actions.

Table 11 – System states of RxSPDO state machine

State number	State transition	Description
1	Init	Startup or SHB timeout occurred (no RxSPDO timeout) while not in “Active” state. No data is produced
2	Active	RxSPDO received and valid delay measurement. Data is produced. SALMT state is “Operational”
3	Delay valid	Delay measurement successful, connection to communication partner within time limits, RxSPDO not “Active” because no SPDO has not been received yet. No data is produced
4	Fail-safe	RxSPDO timeout or SHB timeout occurred while in RxSPDO state “Active”. Data is zeroed out and produced once. Reactivation is only allowed by SALMT transition

Table 12 – State transitions RxSPDO state machine

State transition	From state number	To state number	Description	Action
T1	1	3	For SALMT states “PreOperational” and “Operational” if delay measurement (SHB) was successful	None
T2	3	2	For SALMT state “Operational” if RxSPDO has been received	Start production of data and set SALMT to “Operational”
T3	2	4	For SALMT state “Operational” if delay measurement (SHB) is without success or RxSPDO timeout. or The safety integrity check of the received PDU failed (see 7.1.1.2)	Zero data and produce once. Then stop production of data

State transition	From state number	To state number	Description	Action
T4	3	4	For SALMT state "Operational" if delay measurement (SHB) is without success (SHB timeout has expired without communication partner answering the SHB) or The safety integrity check of the received PDU failed. (see 7.1.1.2)	Zero data and produce once. Then stop production of data
T5, T6, T7	2,3 or 4	1	On change of SALMT state "Operational" to "PreOperational"	Stop production of data

Table 13 – Timeouts

Timeout	Description
RxSPDO	A RxSPDO timeout happens if after the configured number of timeout multiplier cycles no SPDO has been received
SHB expected response	The SHB expected response timeout happens if after sending a SHB message no answer has been received in the configured time
SHB consumer	The SHB consumer timeout happens if within the configured number of timeout multiplier cycles no SHB from the consumer has been received
SHB timeout	SHB expected response timeout or SHB consumer timeout

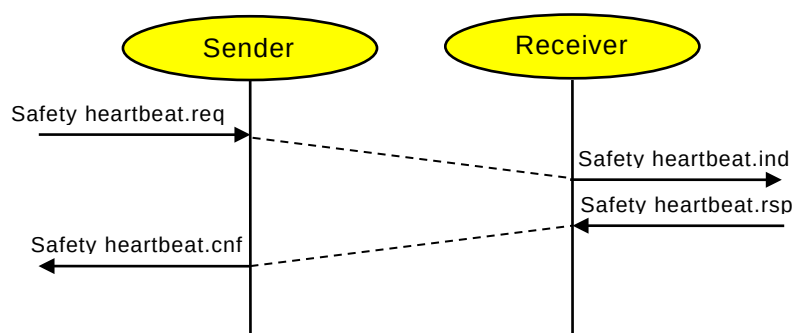
To enhance the availability of the service multiple copies of an SPDO PDU can be sent by a sender. This behavior depends on the configuration of the service. The receiver monitors the number of copies of an SPDO which are received. If too many copies are received a transition to system error state is issued to signal a faulty configuration of the network. The timeout mechanism at the receiver is not influenced by a receipt of multiple copies. The mechanism is triggered by the first received PDU.

7.4 Safety heartbeat

Devices which implement a SCL shall support safety heartbeat. This heartbeat mechanism is independent of the CP 18/1 and CP 18/2 heartbeat messages and shall be configured independent.

Safety heartbeat messages are transmitted as specified in Figure 13. Each heartbeat message contains the state of the SCL and the safety application process.

The heartbeat procedure is shown in Figure 13.



IEC 780/11

Figure 13 – Heartbeat procedure

7.5 Delay monitoring

The delay measurement procedure shall be executed by all safety devices to determine the actual delay in PDU delivery and thus to determine the validity of the received information.

It is possible to monitor the delay of packets based on the safety heartbeat service. Each safety heartbeat PDU is acknowledged by the receiver. The sender monitors the time between producing the heartbeat request and receiving the response. This time shall not exceed a configured maximum delay.

Figure 14 shows the general measurement principle for delay measurement at sender and receiver.

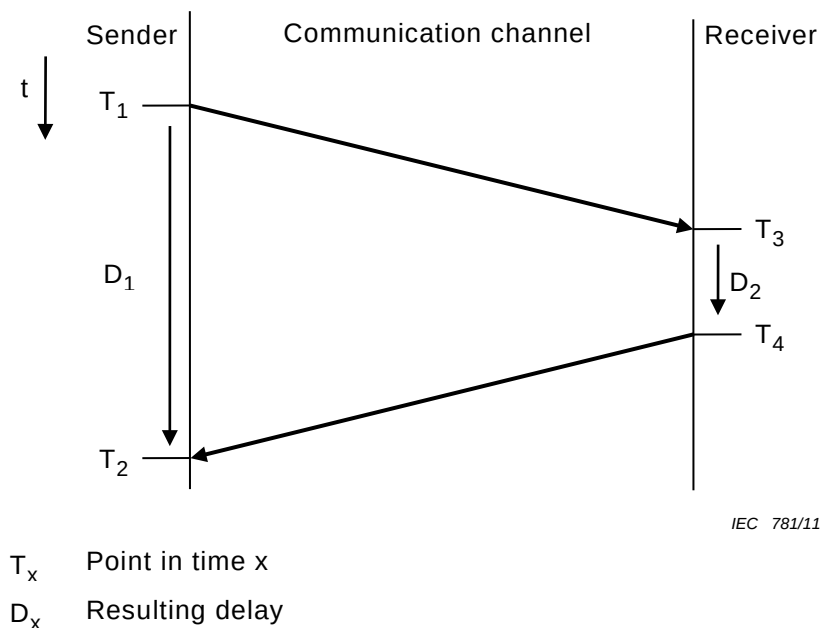


Figure 14 – Delay measurement principle

Sending devices determine the times T_1 and T_2 . Times D_2 , T_3 and T_4 are not further investigated. Based on this information, the sender of heartbeat request PDUs shall determine an estimation of the delay in packet delivery. The delay monitoring result shall be compared to a configured threshold value. Is an increase of the delay detected which exceeds the configured threshold value, the SCL shall initiate a transition to SPDO state “Fail-Safe” and the application shall enter a safe state.

The determination of the repetition rate for the delay monitoring procedure (i.e. the SHB cycle time) shall be derived out of the maximum allowed delay (depends on the safety function response time), the current delay and the configured SPDO cycle times.

Additionally, the sender monitors the time between two successful delay measurements. This time shall not exceed the time in which the possibility exists that the delay rises over the configured delay threshold.

The maximum time until the next delay measurement is calculated per Equation (1).

$$T_{Max} = \frac{(D_{Max} - D_{Act})}{2 * T_{Timer} + (T_{Timer} * T_{TO}) + T_{TO}} \quad (1)$$

where

T_{Max}	Maximum allowed time until the next delay measurement;
D_{Max}	Maximum allowed delay;
D_{Act}	Actual delay (per the last delay measurement);
T_{Timer}	Relative tolerance of the timer with $0,000 \leq T_{Timer} \leq 0,1$;
T_{TO}	Configurable tolerance for the RxSPDO timeout, index 0x121E per Table 15 with $0,01 \leq T_{TO} \leq 1$.

8 Safety communication layer management

8.1 Parameter handling

The parameter configuration of FSCP 18/1 devices is part of the configuration of the safety application. All safety-relevant parameters are downloaded to the device by an appropriate device configuration tool. The used mechanism for parameter download lies outside of the scope of this international standard and depends on the safety application. Figure 15 shows the device configuration sequence.

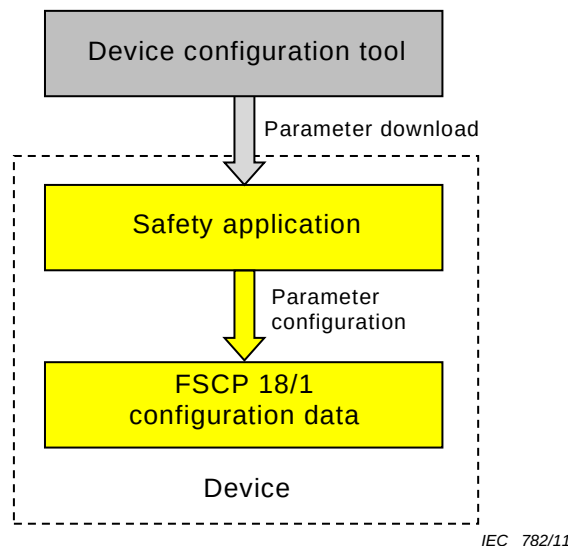


Figure 15 – Parameter handling

8.2 Safety object dictionary

8.2.1 General

The safety object dictionary uses the same structure as the object dictionary used in CP 18/1 and CP 18/2. It contains the object areas listed in Table 14.

Table 14 – Safety object dictionary structure

Index	Section	Sub-section	Content
0x0001 to 0x001F	Data type	Basic data types	Definition of basic data types
0x0020 to 0x003F	—	Complex data types	Definition of complex data types
0x0040 to 0x005F	—	Manufacturer specific data types	Definition of manufacturer specific data types
0x0060 to 0x007F	—	Device profile specific basic data types	Definition of device profile specific basic data types
0x0080 to 0x009F	—	Device profile specific complex data types	Definition of device profile specific complex data types
0x00A0 to 0x0FFF	Reserved	—	—

Index	Section	Sub-section	Content
0x1000 to 0x1FFF	Communication profile	—	Definition of the parameters which are used for communication configuration and dedicated communication purposes
0x2000 to 0x5FFF	Manufacturer defined profile	—	Definition of manufacturer specific parameters
0x6000 to 0x9FFF	Standardized device profile	—	Definition of the parameters defined in a standardized device profile
0xA000 to 0xBFFF	Standardized interface profile	—	Definition of the parameters defined in standardized interface profile
0xC000 to 0xC8FF	CP 18/2 interface profile	—	Definition of the parameters defined in CP 18/2 interface profile
0xC900 to 0xFFFF	Reserved	—	—

8.2.2 Communication profile section

8.2.2.1 General

The safety application related objects listed in Table 15 shall be supported.

Table 15 – Objects of communication section

Index	Object	Name	Data type	Attr.	Description	Cat.
0x1000	VAR	Device type	Unsigned32	RO	Device classification: Lower 16 bits are “Device Profile Number”, describing the used profile. Upper 16 bits are “Additional Information”.	M
0x1200	VAR	Safety ID	Unsigned16	FSF	Unique identifier for the safety device, shall be not zero	M/O
0x1216	ARRAY	Safety consumer heartbeat list	Unsigned256	FSF	List of remote devices that need to be monitored by the device.	M/O
0x1217	RECORD	Safety producer heartbeat parameter	PDO COM_PAR	FSF	Configured in same way as SPDO. transmission. Shall be configured as cyclic transmission.	M/O
0x1218	ARRAY	Safety bus cycle time	Unsigned32	FSF	Sub-Index 0: Number of entries Sub-Index 1: RTFN Base Cycle Time Sub-Index 2: RTFL Base Cycle Time	M/O
0x121B to 0x121D	Reserved for further safety parameters					
0x121E	VAR	SPDO Timeout tolerance T_{TO}	Unsigned8	FSF	Defines how much of an excession of a RxSPDO timeout is acceptable. Unitless number, interpreted as percentage.	M/O
0x121F to 0x127F	Reserved for further safety parameters					
0x1C00 to 0x1CFF	RECORD	RxSPDO communication parameter	PDO COM_PAR	FSF		M/O

Index	Object	Name	Data type	Attr.	Description	Cat.
0x1D00 to 0x1DFF	RECORD	RxSPDO mapping parameter	PDO MAPPING	FSF		M/O
0x1E00 to 0x1EFF	RECORD	TxSPDO communicati on parameter	PDO COM_PAR	FSF		M/O
0x1F00 to 0x1FFF	RECORD	TxSPDO mapping parameter	PDO MAPPING	FSF		M/O

8.2.2.2 Device type

The device type object indicates the implemented device profile and its function and is specified in Table 16. It comprises of two 16 bit fields. The first field is the device profile number and describes the used device profile. The second 16 bit field supplies additional information on optional device functions and is part of the device profile or product specification. The value 0x0000 indicates a device that does not follow a standardized device profile. For multiple device modules the additional information parameter contains 0xFFFF and the device profile number referenced by object 0x1000 is the device profile of the first device in the safety object dictionary. All other devices of a multiple device module identify their profiles at objects 0x67FF + (N x 0x800) with N = internal number of the device (0 to 7). These entries describe the device type of the preceding device. Devices use device profile numbers from four to seven for safety functions, so that the first safety application objects start at 0x8000.

Table 16 – Device type

Attribute	Value
Index	0x1000
Name	Device type
Description	CANopen conformant device classification. Further information is found in [47]
Object type	VAR
Data type	Unsigned32
Category	Mandatory
Access attribute	RO
PDO mapping	No
Value range	No
Value	Bit 0 to 15: Device profile number Bit 16 to 31: Additional information depending on the used device profile

8.2.2.3 Safety ID (SID)

The safety ID object is specified in Table 17. The object specifies the safety ID of a safety device. It is mandatory for safety devices.

Table 17 – Safety ID

Attribute	Value
Index	0x1200
Name	Safety ID
Description	Unique identifier for device
Object type	VAR
Data type	Unsigned16
Category	Mandatory
Access attribute	FSF
SPDO mapping	No
Value range	0x0001 to 0xFFFF
Value	No

8.2.2.4 Safety consumer heartbeat list

The safety consumer heartbeat object is specified in Table 19. The safety consumer heartbeat defines all safety devices to be monitored by the device. Furthermore, the parameters of heartbeat responses are configured as well as parameters for expected responses. The encoding of a safety consumer heartbeat entry within an OCTET_STRING value is specified in Table 18.

Table 18 – Safety consumer heartbeat entry

Octet	Data type	Meaning
0 to 3	Unsigned32	IPv4 address of communication partner. For heartbeat consumer and expected response
4 to 19	Unsigned128	IPv6 address of communication partner. For heartbeat consumer and expected response
20 to 21	Unsigned16	SID of communication partner is unique identifier for the device. For heartbeat consumer and expected response
22	Unsigned8	Transmission type. For heartbeat consumer and expected response and own response Description: Bit 7 (MSB): Activation 0 not active; 1 active. Bits 6,5: Communication channel 00 for CDCL; 01 for CDCN; 10 Reserved for future use; 11 Reserved for future use. Bit 4: Routed by a CP 18/1 – CP 18/2 Gateway. 0 default – no gateway present, 1 for gateway. Shall not be set for PDO/Heartbeat where transmission channel is CDCN. Bit 3: Frame Type 0 for MAC frame, is only used for RxSPDO over CDCN 1 for UDP frame. Bits 2,1,0 (LSB): Transmission mode 001: Cyclic, else: Reserved for future use.
23	Unsigned8	Reserved
24 to 27	Unsigned32	PID of consumed heartbeat is the packet identifier, used to verify the correct sender For heartbeat consumer
28 to 29	Unsigned16	Heartbeat timeout specifies how often a heartbeat produced by the communication partner is expected. Allowed values are integer multiples of base cycle time. For heartbeat consumer
30 to 31	Unsigned16	Cycle multiplier for consumed heartbeat is mandatory for networks with CP18/1 to CP18/2 gateways. It specifies how often the CDCN/CDCL-gateway may write the SPDU into the CDCL communication channel. For heartbeat consumer Allowed values: 0x0001, 0x0002, 0x0004, 0x0008, 0x0010, 0x0020, 0x0040, 0x0080, 0x0100, 0x0200, 0x0400, 0x0800, 0x1000, 0x2000, 0x4000, 0x8000
32 to 33	Unsigned16	Cycle offset for consumed heartbeat is mandatory for networks with CP18/1 to CP18/2 gateways. It specifies the SPDU's offset when being sent over CDCL For heartbeat consumer Valid range is 0 to (Cycle multiplier - 1)
34	Unsigned8	Number of receives threshold specifies maximum number of receives of the same packet that is acceptable. For heartbeat consumer
35	Unsigned8	Reserved
36 to 39	Unsigned32	PID of expected response is packet identifier to verify correct sender For expected response
40 to 41	Unsigned16	Cycle multiplier of expected response for networks with CP18/1 to CP18/2 gateways. For expected response

Octet	Data type	Meaning
42 to 43	Unsigned16	Cycle offset of expected response for networks with CP18/1 to CP18/2 gateways. For expected response
44 to 47	Unsigned32	PID of transmitted response. For own response
48 to 49	Unsigned16	Cycle multiplier of transmitted response. For own response. Allowed values: 0x0001, 0x0002, 0x0004, 0x0008, 0x0010, 0x0020, 0x0040, 0x0080, 0x0100, 0x0200, 0x0400, 0x0800, 0x1000, 0x2000, 0x4000, 0x8000
50 to 51	Unsigned16	Cycle offset of transmitted response used for CDCL only. For own response. Range 0 to (Cycle multiplier - 1)
52 to 55	Unsigned32	Maximum acceptable delay in μ s of expected response from sending out the heartbeat to receiving the response. For expected response
56	Unsigned8	Number of sends of transmitted response. For own response
57	Unsigned8	Reserved

Table 19 – Safety consumer heartbeat

Attribute	Value
Index	0x1216
Name	Safety consumer heartbeat list
Object type	ARRAY
Data type	OCTET_STRING
Category	Optional
Sub-index	0x00
Name	Number of supported entries
Description	Number of heartbeats to consume (one for each communication partner)
Data type	Unsigned8
Category	Mandatory
Access attribute	RO
SPDO mapping	No
Value range	0x01 to 0xFF
Value	No
Sub-index	0x01
Name	Consumer heartbeat
Description	There shall be at least one communication partner, therefore one entry is mandatory. Format described in Table 18
Data type	OCTET_STRING
Category	Mandatory
Access attribute	FSF
SPDO mapping	No
Value range	No
Value	No

Attribute	Value
Sub-index	0x02 to 0xFE
Name	Consumer heartbeat
Description	Additional entries. Format described in Table 18
Data type	OCTET_STRING
Category	Optional
Access attribute	FSF
SPDO mapping	No
Value range	No
Value	No

8.2.2.5 Safety producer heartbeat parameter

The safety producer heartbeat parameter object is specified in Table 20.

Table 20 – Safety producer heartbeat parameter

Attribute	Value
Index	0x1217
Name	Safety producer heartbeat parameter
Object type	RECORD
Data type	PDO COMMUNICATION PARAMETER
Category	Conditional; Mandatory for each supported TxSPDO
Sub-index	0x00
Name	Number of entries
Data type	Unsigned8
Category	Mandatory
Access attribute	RO
SPDO mapping	No
Value range	0x01 to 0x0C
Value	No
Sub-index	0x01
Name	RTFL PID
Description	Packet identifier if sent over CDCL
Data type	Unsigned32
Category	Conditional
Access attribute	FSF
SPDO mapping	No
Value range	0x01 to 0x00FFFFFF
Value	No
Sub-index	0x02
Name	RTFN PID
Description	Packet identifier if sent over CDCN
Data type	Unsigned32
Category	Conditional
Access attribute	FSF

Attribute	Value
SPDO mapping	No
Value range	0x01 to 0x00FFFFFF
Value	No
Sub-Index	0x03
Name	Reserved
Data type	Unsigned32
Sub-index	0x04
Name	Transmission type
Description	Specifies transmission mode (see Table 18). Shall be set to cyclic
Data type	Unsigned8
Category	Mandatory
Access attribute	FSF
SPDO mapping	No
Value range	No
Value	No
Sub-index	0x05
Name	Time sync ID
Description	Not used, because transmission type is cyclic.
Data type	Unsigned16
Category	Conditional
Access attribute	FSF
SPDO mapping	No
Value range	0x00 to 0xFF
Value	No
Sub-index	0x06
Name	Event time
Description	Not used, because transmission type is cyclic
Data type	Unsigned16
Category	Conditional
Access attribute	FSF
SPDO mapping	No
Value range	No
Value	No
Sub-index	0x07
Name	Cycle multiplier
Description	Specifies how often it is transmitted (multiple of base cycle time)
Data type	Unsigned16
Category	Conditional
Access attribute	FSF
SPDO mapping	No
Value range	0x0001, 0x0002, 0x0004, 0x0008, 0x0010, 0x0020, 0x0040, 0x0080, 0x0100, 0x0200, 0x0400, 0x0800, 0x1000, 0x2000, 0x4000, 0x8000
Value	No
Sub-index	0x08

Attribute	Value
Name	Cycle offset
Description	Specifies in which cycles it is transmitted
Data type	Unsigned16
Category	Conditional
Access attribute	FSF
SPDO mapping	No
Value range	0 to (Cycle multiplier – 1)
Value	No
Sub-index	0x09
Name	Number of sends
Description	Number of times it is transmitted
Data type	Unsigned8
Category	Mandatory
Access attribute	FSF
SPDO mapping	No
Value range	No
Value	2
Sub-index	0x0A
Name	Device address
Description	Not used, because transmitted over CDCN or CDCL
Data type	Unsigned16
Category	Conditional
Access attribute	FSF
SPDO mapping	No
Value range	0x0000 to 0x0200
Value	No
Sub-index	0x0B
Name	IPv4 address
Data type	Unsigned32
Category	Conditional
Access attribute	FSF
SPDO mapping	No
Value range	No
Value	No
Sub-index	0x0C
Name	IPv6 address
Data type	Unsigned128
Category	Conditional
Access attribute	FSF
SPDO mapping	No
Value range	No
Value	No