IEC 61784-3-18

Edition 1.1 2016-07

CONSOLIDATED VERSION

VERSION CONSOLIDÉE

colour inside

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 le CPF 18

IEC 61784-3-18:2011-04+AMD1:2016-07 CSV(en-fr)

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

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
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 corrigenda or an amendment might have been published.

IEC Catalogue - webstore.iec.ch/catalogue
The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

IEC publications search - www.iec.ch/searchpub
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 It also gives information on projects, replaced and withdrawn publications.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 also once a month by email.

Electropedia - www.electropedia.org
The world's leading online dictionary of electronic and electrical terms containing 20 000 terms and definitions in English and French, with equivalent terms in 15 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary
65 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

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: csc@iec.ch.

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.

Catalogue IEC - webstore.iec.ch/catalogue
Application autonome pour consulter tous les renseignements bibliographiques sur les Normes internationales, Spécifications techniques, Rapports techniques et autres documents de l'IEC. Disponible pour PC, Mac OS, tablettes Android et iPad.

Recherche de publications IEC - www.iec.ch/searchpub
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 aussi une fois par mois par email.

Electropedia - www.electropedia.org
Le premier dictionnaire en ligne de termes électroniques et électriques. Il contient 20 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans 15 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

Glossaire IEC - std.iec.ch/glossary
65 000 entrées terminologiques électrotechniques, en anglais et en français, extraites des articles Termes et Définitions des publications IEC parues depuis 2002. Plus certaines entrées antérieures extraites des publications des CE 37, 77, 86 et CISPR de l'IEC.

Service Clients - webstore.iec.ch/csc
Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: csc@iec.ch.

IEC 61784-3-18

Edition 1.1 2016-07

CONSOLIDATED VERSION

VERSION CONSOLIDÉE

colour inside

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 le CPF 18

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

ICS 13.110; 25.040.40, 35.100.05

ISBN 978-2-8322-3543-0

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.

IEC 61784-3-18

Edition 1.1 2016-07

REDLINE VERSION

VERSION REDLINE

colour inside

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 le CPF 18

IEC 61784-3-18:2011-04+AMD1:2016-07 CSV(en-fr)

CONTENTS

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.

DISCLAIMER
This Consolidated version is not an official IEC Standard and has been prepared for user convenience. Only the current versions of the standard and its amendment(s) are to be considered the official documents.

This Consolidated version of IEC 61784-3-18 bears the edition number 1.1. It consists of the first edition (2011-04) [documents 65C/639/FDIS and 65C/649/RVD] and its amendment 1 (2016-07) [documents 65C/851/FDIS and 65C/854/RVD]. The technical content is identical to the base edition and its amendment.

In this Redline version, a vertical line in the margin shows where the technical content is modified by amendment 1. 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 amendment 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.

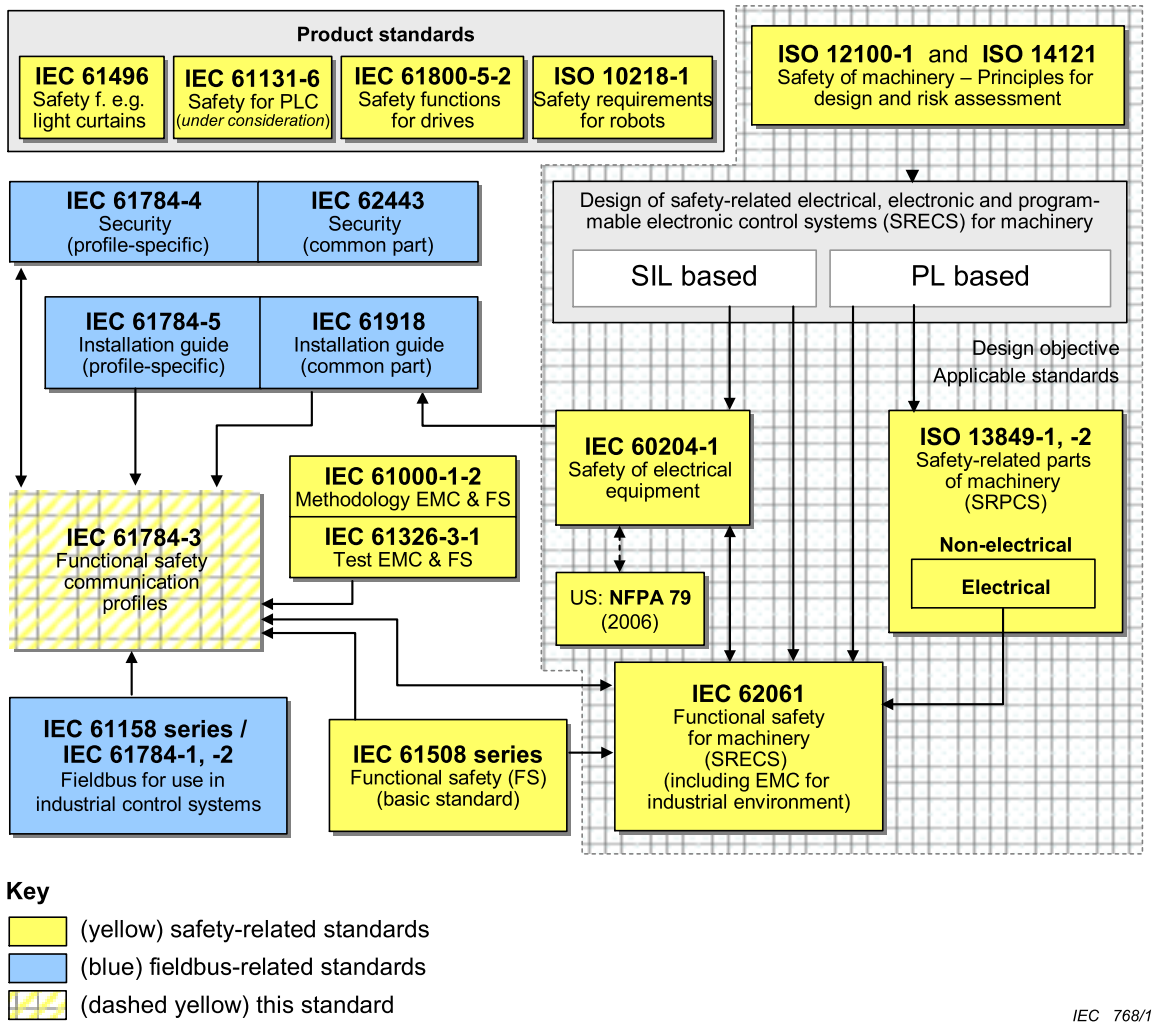
0 Introduction

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.

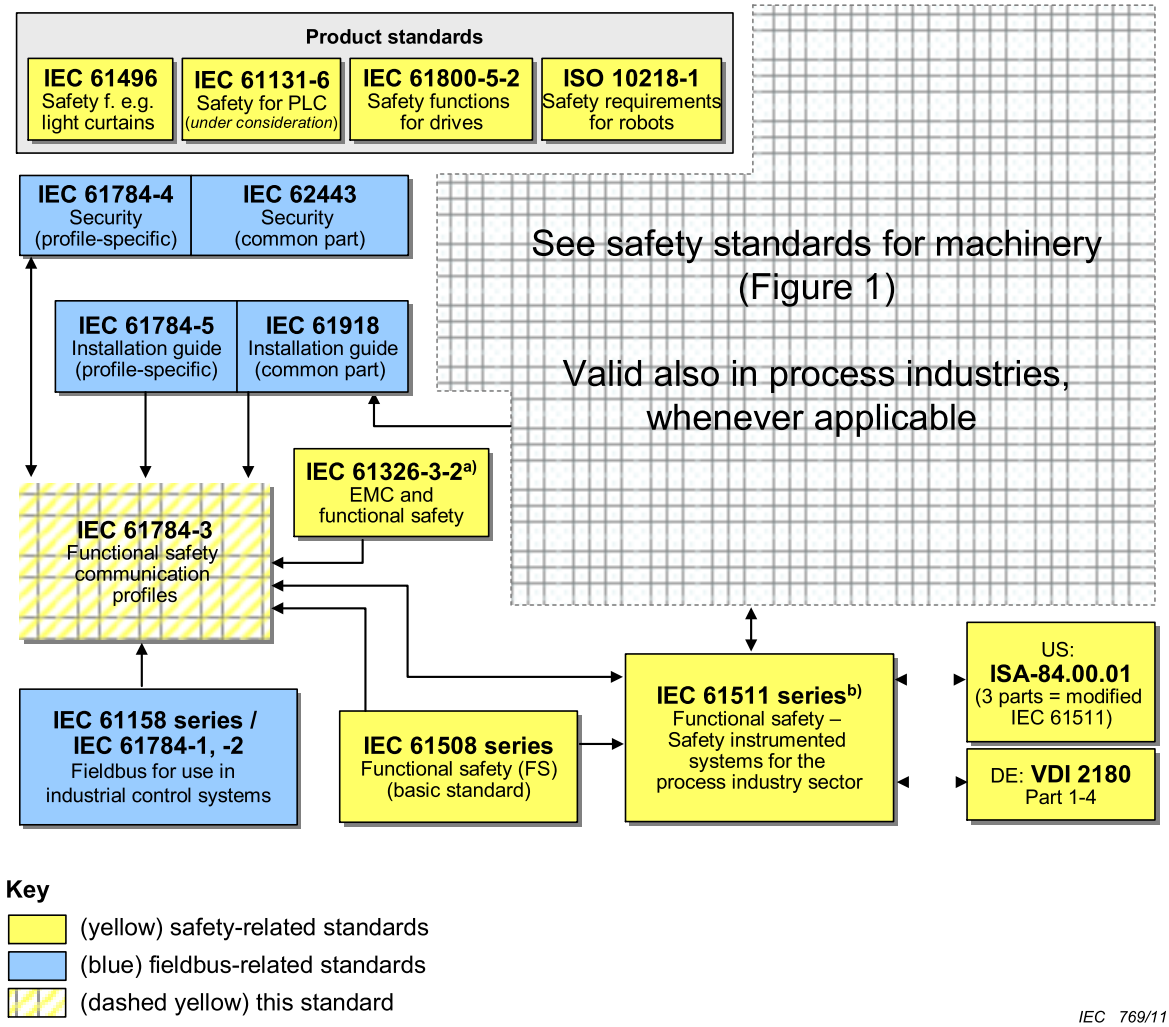
Figure 1 shows the relationships between this standard and relevant safety and fieldbus standards in a machinery environment.



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.

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

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



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

b EN ratified.

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

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

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

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

This standard describes:

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

0.2 Patent declaration

The International Electrotechnical Commission (IEC) draws attention to the fact that it is claimed that compliance with this document may involve the use of 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 part[1] 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 series[2] 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.

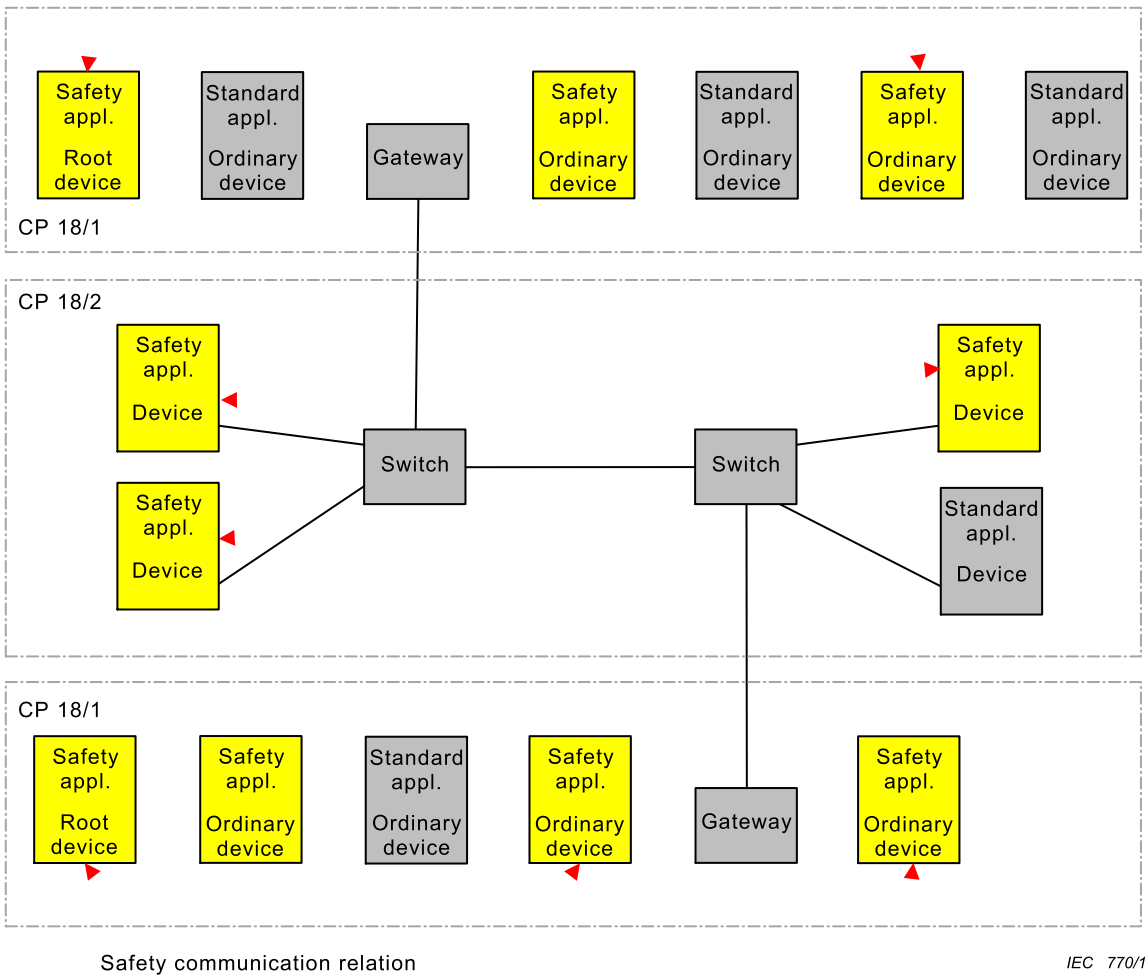


Figure 3 – FSCP 18/1 system

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]

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.

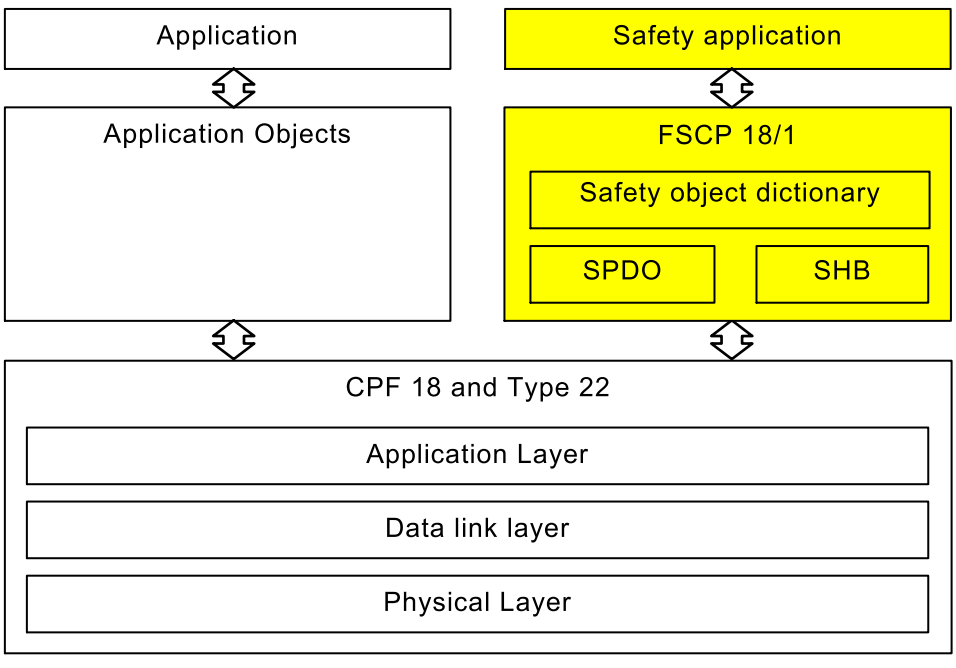


Figure 4 – FSCP 18/1 software architecture

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).

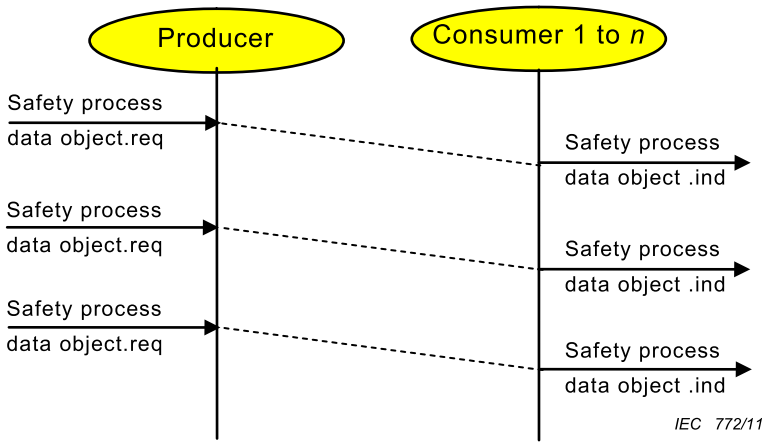


Figure 5 – SPDO interaction model

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.

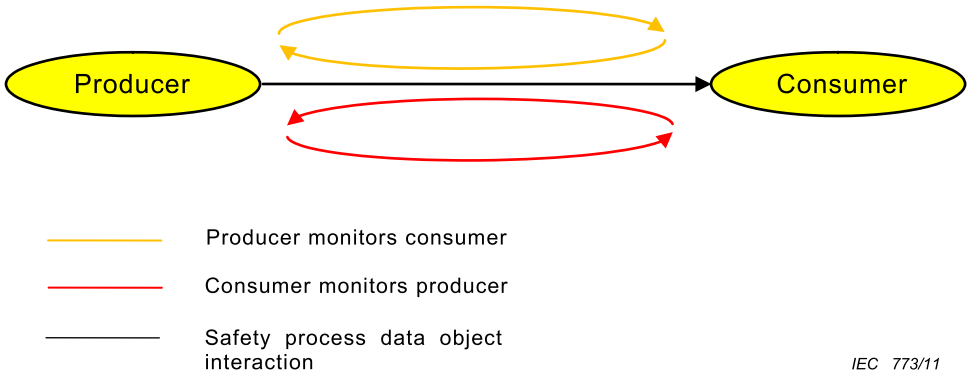


Figure 6 – SHB interaction model

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.

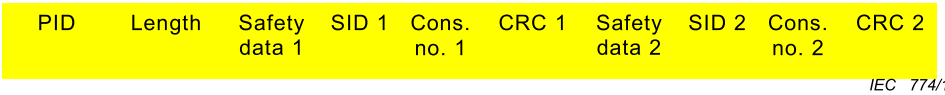


Figure 7 – Safety process data object structure

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+2*n*+*m* to 12+2*n*+*m*	SID 2	Copy of SID 1
13+2*n*+*m* to 13+2*n*+2*m*-1	Consecutive number 2	Copy of consecutive number 1
14+2*n*+2*m* to 17+2*n*+2*m*	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.

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 a~~n 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 is used for calculating the CRCs. For details see 7.1.2.4 and 9.5.2.

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+2*n*+*m*-1	Safety AP state 2	Copy of safety application process state 1
15+2*n*+*m* to 16+2*n*+*m*	SID 2	Copy of SID 1
17+2*n*+*m* to 17+2*n*+2*m*-1	Consecutive number 2	Copy of consecutive number 1
18+2*n*+2*m* to 21+2*n*+2*m*	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. 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.

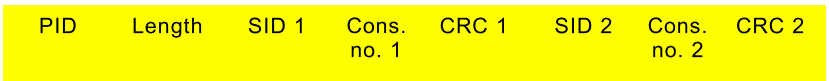


Figure 9 – Safety heartbeat response structure

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+2*m*-1	Consecutive number 2	Copy of consecutive number 1
14+2*m* to 17+2*m*	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 a~~n 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 is used for calculating the CRCs. For details see 7.1.3.5 and 9.5.2.

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.

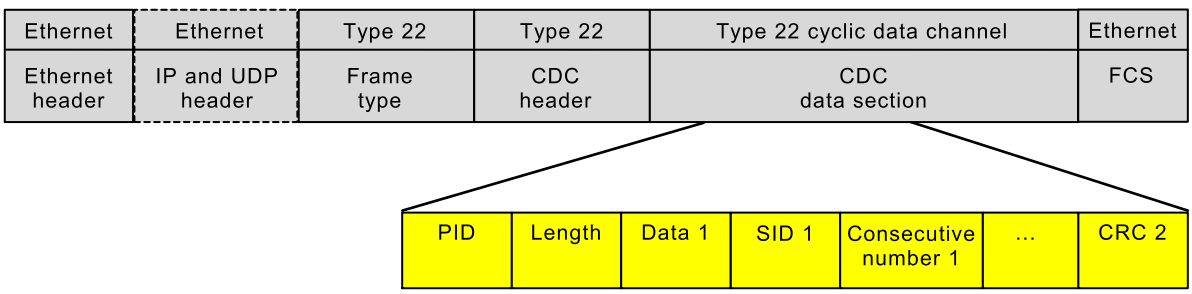


Figure 10 – Safety PDU for FSCP 18/1 embedded in a Type 22 CDC data section

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.

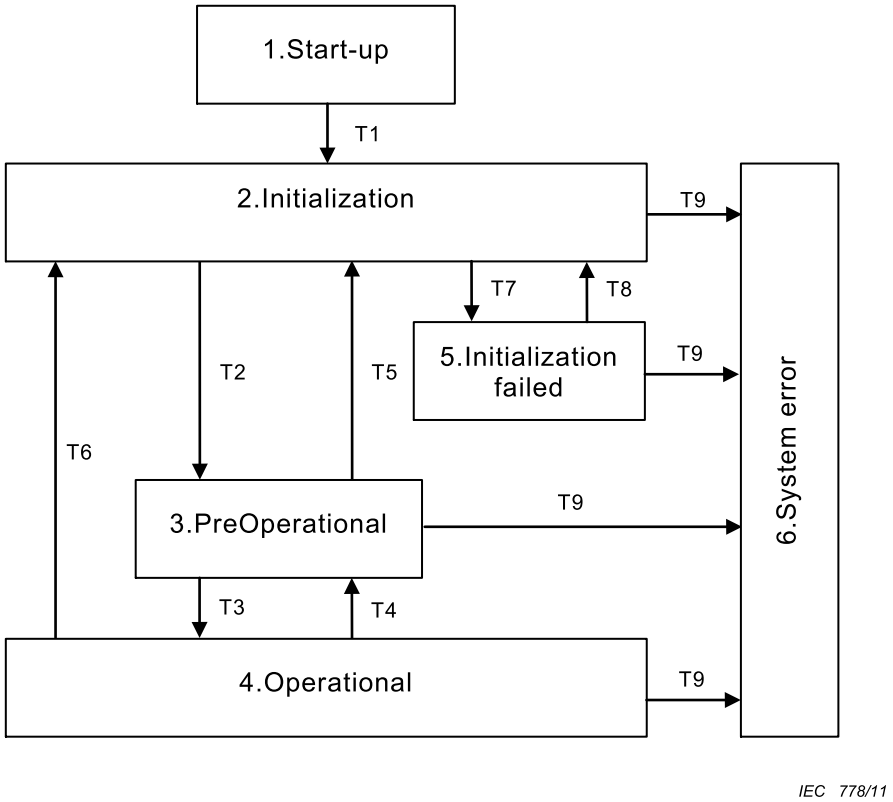


Figure 11 – SALMT state machine

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.

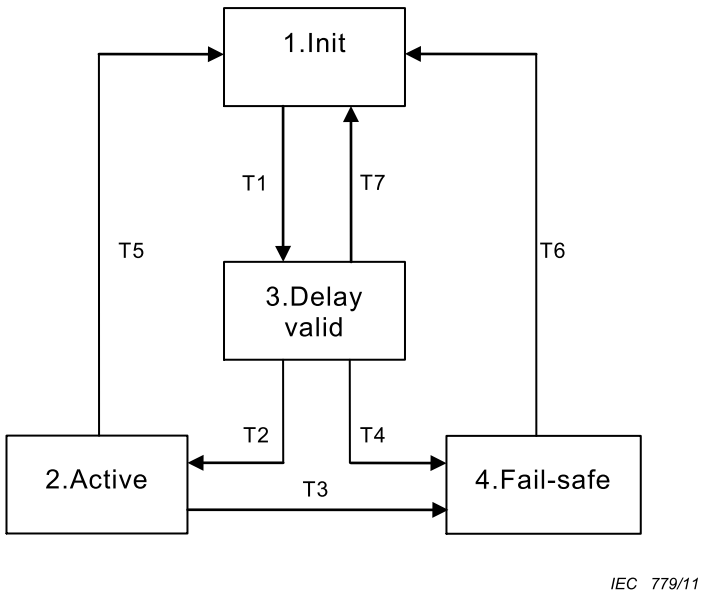


Figure 12 – RxSPDO state machine

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
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 timout multiplier cylces no SPDO has been received
SHB expected response	The SHB expected response timout 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 timout multiplier cycles no SHB from the consumer has been received
SHB timeout	SHB expected response timeout or SHB consumer timout

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.

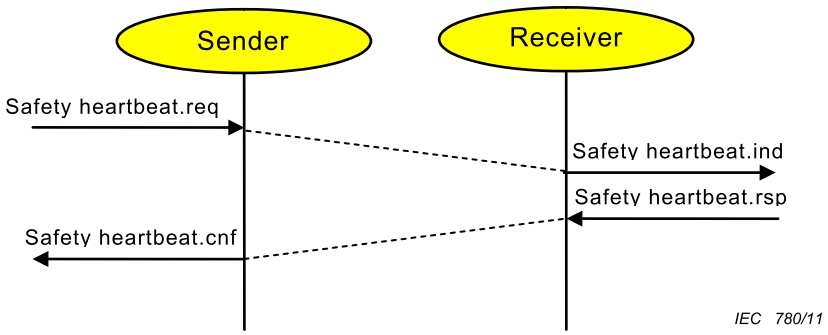


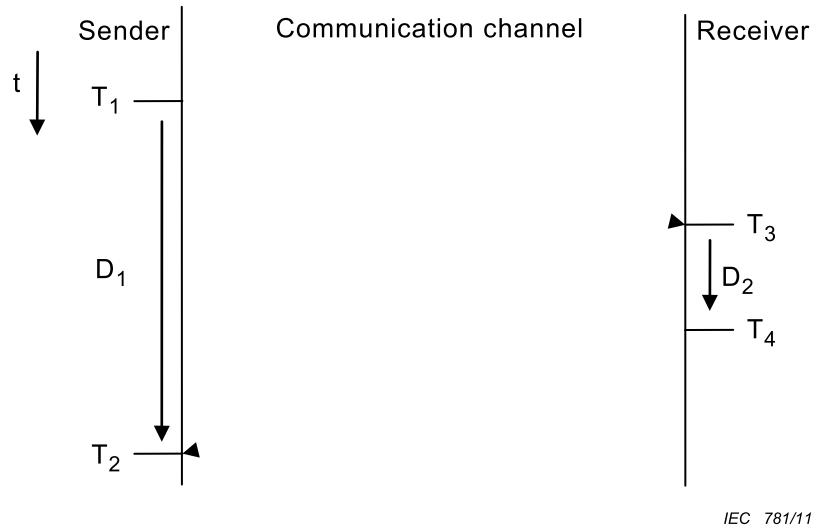
Figure 13 – Heartbeat procedure

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.



T_x Point in time x

D_x Resulting delay

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 1 ≤ T_{Timer} ≤ 0,1;
T_{TO}	Configurable tolerance for the RxSPDO timeout, index 0x121E per Table 15 with 0,01 ≤ T_{TO} ≤ 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.

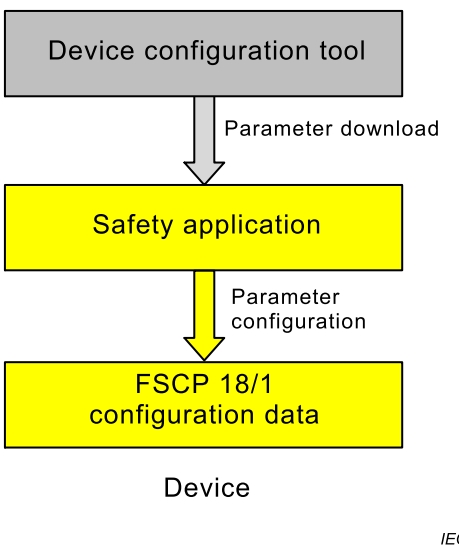


Figure 15 – Parameter handling

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	—	—
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.	Desription	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					

Index	Object	Name	Data type	Attr.	Desription	Cat.
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 communicati on parameter	PDO COM_PAR	FSF		M/O
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 μs 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

8.2.2.6 Safety bus cycle times

The safety bus cycle time object is specified in Table 21. The safety bus cycle times are used to compute the timeout values for safety packets.

Table 21 – Safety bus cycle times

Attribute	Value
Index	0x1218
Name	Safety bus cycle times
Object type	ARRAY
Data type	Unsigned32
Category	Mandatory
Sub-index	0x00
Name	Number of supported entries
Data type	Unsigned8
Category	Mandatory
Access attribute	RO
SPDO mapping	No
Value range	0x01 to 0x02
Value	No
Sub-index	0x01
Name	Safety RTFN base cycle time
Description	Base cycle time for CDCN in μs
Data type	Unsigned32
Category	Conditional
Access attribute	FSF
SPDO mapping	No
Value range	No
Value	No
Sub-index	0x02
Name	Safety RTFL base cycle time
Description	Base cycle time for CDCL in μs
Data-type	Unsigned32
Category	Conditional
Access attribute	FSF
SPDO mapping	No
Value range	No
Value	No

8.2.2.7 SPDO timeout tolerance

The SPDO timeout tolerance object is specified in Table 22.

Table 22 – SPDO timeout tolerance

Attribute	Value
Index	0x121E
Name	SPDO timeout tolerance
Description	Specifies how much the SPDU timeout may be exceeded. Given in percent
Object type	VAR
Data type	Unsigned8
Category	Conditional
Access attribute	FSF
SPDO mapping	No
Value range	0x00 to 0xFF
Value	No

8.2.2.8 RxSPDO communication parameter

The receive SPDO communication parameter object is specified in Table 23.

Table 23 – Receive SPDO communication parameter

Attribute	Value
Index	0x1C00 – 0x1CFF
Name	Receive SPDO communication parameter
Object type	RECORD
Data type	PDO COMMUNICATION PARAMETER
Category	Conditional; Mandatory for each supported RxSPDO
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 in case of CDCL transmission
Data type	Unsigned32
Category	Conditional
Access attribute	FSF
SPDO mapping	No
Value range	0x01 to 0xFFFFFFFF
Value	No
Sub-index	0x02
Name	RTFN PID
Description	Packet identifier in case of CDCN transmission

Attribute	Value
Data type	Unsigned32
Category	Conditional
Access attribute	FSF
SPDO mapping	No
Value range	0x01 to 0xFFFFFFFF
Value	No
Sub-index	0x03
Name	SID
Description	Unique id of communication partner
Data type	Unsigned16
Category	Mandatory
Access attribute	FSF
SPDO mapping	No
Value range	No
Value	No
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 specified as cyclic
Data type	Unsigned16
Category	Conditional
Access attribute	FSF
SPDO mapping	No
Value range	0x0000 to 0xFFFF
Value	No
Sub-index	0x06
Name	Timeout multiplier
Description	Specifies how often the packet is expected
Data type	Unsigned16
Category	Optional
Access attribute	FSF
SPDO mapping	No
Value range	0x0000 to 0xFFFF
Value	No
Sub-index	0x07
Name	Cycle multiplier

Attribute	Value
Description	Specifies how often CP18/1 to CP18/2 gateway may write the SPDU to the CDCL communication channel. Mandatory if CDCL is used for transmission and CP18/1 to CP18/2 gateways are present. For all other cases it is not used
Data type	Unsigned16
Category	Conditional
Access attribute	FSF
SPDO mapping	No
Value range	0x01 to 0xFFFF
Value	No
Sub-index	0x08
Name	Cycle offset
Description	Cycle Offset (when is the SPDU written to CDCL channel). Mandatory if CDCL is used for transmission and CP18/1 to CP18/2 gateways are present. For all other cases it is not used
Data type	Unsigned16
Category	Conditional
Access attribute	FSF
SPDO mapping	No
Value range	0x00 to 0xFFFE
Value	No
Sub-index	0x09
Name	Number of allowed receives
Description	Maximum number that SPDU may be received
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	0x00 to 0x200
Value	No
Sub-index	0x0B
Name	IPv4 address
Data type	Unsigned32
Category	Conditional
Access attribute	FSF
SPDO mapping	No

Attribute	Value
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

8.2.2.9 TxSPDO communication parameter

The transmit SPDO communication parameter object is specified in Table 24.

Table 24 – Transmit SPDO communication parameter

Attribute	Value
Index	0x1E00 – 0x1EFF
Name	Transmit SPDO communication 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 in case of CDCL transmission
Data type	Unsigned32
Category	Conditional
Access attribute	FSF
SPDO mapping	No
Value range	0x01 to 0xFFFFFFFF
Value	No
Sub-index	0x02
Name	RTFN PID
Description	Packet identifier in case of CDCN transmission
Data type	Unsigned32
Category	Conditional

Attribute	Value
Access attribute	FSF
SPDO mapping	No
Value range	0x01 to 0xFFFFFFFF
Value	No
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 specified as 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 specified as 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.
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
Name	Cycle offset
Description	In which cycles it is transmitted.

Attribute	Value
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	Specifies how often the packet 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	0x00 to 0x200
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

8.2.2.10 SPDO mapping

8.2.2.10.1 SPDO mapping principle

The SPDO mapping parameters define the contents of a SPDO. A valid SPDO contains at least one and at most 254 safety application objects. The encoding of a mapping entry is specified in Table 25.

Table 25 – Mapping format

Bit	Name	Meaning
0 to 7	Length	Length of safety application object in bits
8 to 15	Sub-index	Sub-index of the safety application object to be mapped. The safety object dictionary is organized as a table with key (index, sub-index). This mapping specifies the lookup key for this application object.
16 to 31	Index	Index of the safety application object to be mapped

8.2.2.10.2 RxSPDO mapping parameter

The receive SPDO mapping parameter object is specified in Table 26.

Table 26 – Receive SPDO mapping parameter

Attribute	Value
Index	0x1D00 to 0x1DFF
Name	Receive SPDO mapping parameter
Description	Maps object from safety PDU to safety object dictionary. See Table 25
Object type	RECORD
Data type	PDO_MAPPING
Category	Conditional; Mandatory for each supported RxSPDO
Sub-index	0x00
Name	Number of mapped safety application objects
Data type	Unsigned8
Category	Mandatory
Access attribute	FSF
SPDO mapping	No
Value range	0x00 to 0xFE
Value	No
Sub-index	0x01 to 0xFE
Name	SPDO mapping for the nth safety application object to be mapped
Description	Specified in Table 25
Data type	Unsigned32
Category	Conditional depending on the number and size of objects to be mapped
Access attribute	FSF
SPDO mapping	No
Value range	No
Value	No

8.2.2.10.3 TxSPDO mapping parameter

The transmit SPDO mapping parameter object is specified in Table 27.

Table 27 – Transmit SPDO mapping parameter

Attribute	Value
Index	0x1E00 to 0x1EFF
Name	Transmit SPDO mapping parameter
Description	Maps object from safety object dictionary to safety PDU. See Table 25
Object type	RECORD
Data type	PDO_MAPPING
Category	Conditional; Mandatory for each supported TxSPDO
Sub-index	0x00
Name	Number of mapped safety application objects
Data type	Unsigned8
Category	Mandatory
Access attribute	FSF
SPDO mapping	No
Value range	0x01 to 0xFE
Value	No
Sub-index	0x01 to 0xFE
Name	SPDO mapping for the nth safety application object to be mapped
Description	Specified in Table 25
Data type	Unsigned32
Category	Conditional depending on the number and size of objects to be mapped
Access attribute	FSF
SPDO mapping	No
Value range	No
Value	No

8.2.3 Standardized device profile section

Safety application objects can be mapped within SPDOs. Safety application objects are located in the safety object dictionary area from 0x8000 to 0x9FFF. These objects are manufacturer and application specific.

9 System requirements

9.1 Indicators and switches

9.1.1 Indicator states and flash rates

The indicator states and flash rates are defined in Table 28. The times listed shall be met with a tolerance of less than ± 25 %.

Table 28 – Indicator states definiton

Indicator state	Definition
OFF	The indicator shall be constantly off
ON	The indicator shall be constantly on
BLINKING 1 Hz	The indicator shall turn on and off with a frequency of 1 Hz
BLINKING 2 Hz	The indicator shall turn on and off with a frequency of 2 Hz

9.1.2 Indicators

Devices which support FSCP 18/1 protocol should have a STATUS indicator. This indicator, typically LED, assists troubleshooting, visual inspection, maintenance and diagnosis of problems. If a device supports the STATUS indicator, this indicator shall comply with this specification. Additional indicators may be implemented.

The STATUS indicator shall show the status of the FSCP 18/1 communication. A single bicolor indicator (green/red) shall be used.

The STATUS indicator shall be labeled with “FS SNp”.

The STATUS indicator states are specified in Table 29.

Table 29 – STATUS indicator states

Indicator state	Definition
OFF	No safety process data communication is active
GREEN ON	All configured safety process data communication (SPDO) is active
GREEN BLINKING 1 Hz	At least one SPDO is active and at least one SPDO is not active
RED ON	Configuration is invalid or inconsistent
RED BLINKING 2 Hz	Internal error

9.1.3 Switches

There are no switches for FSCP 18/1.

9.2 Installation guidelines

Relevant installation guidelines are specified by IEC 61918.

9.3 Safety function response time

9.3.1 General

A safety function may consist of several components. To determine the safety function response time, the safety function is decomposed into the different components shown in Figure 16.

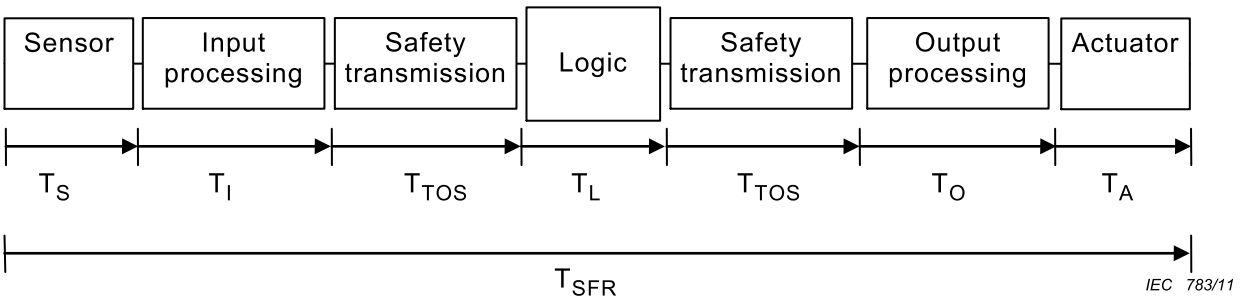


Figure 16 – Safety response time components

The safety function channel consists of a sensor (for example light curtain or emergency stop button) to detect the actuation of the safety function. This sensor converts the physical signal in an electrical signal. This electrical signal is connected to an input device (for example, functional safety input module), which converts the electrical signal in logical input information. The logical input information is transmitted to the safety logic controller via the safety communication system. Safety logic controller combines the logical input information to logical output information, which is transmitted to an output device (for example functional safety output module) via the safety communication system. Logical output information is converted to a physical output signal which is connected to an actuator. This actuator performs the physical reaction. Each component is described by a characteristic time behavior.

The following general assumptions are applied for further considerations.

- All components of the safety function channel work asynchronous.
- All components of the safety function channel are described by a worst case processing or response time which is gueranteed under non error conditions.
- For safety reasons, every component has its superposed timeout timer (T_{TOi}).
- In order to calculate the safety function response time one error or failure shall be assumed in that signal path, which contributes the maximum difference time between its timeout and its worst case processing or response time.

The characteristic times of the devices sensor, input, logic, output and actuator are outside the scope of this standard. Meaningful information for these characteristic values should be taken from component specifications. Each device shall provide these values as part of their device properties.

9.3.2 Determination of FSCP 18/1 time expectation behavior

FSCP 18/1 defines a configurable time expectation behavior (timeout) for the delivery of safety process data at the receiver side of a communication relation. This behavior is implemented by communication timeout T_{TOS}.

For the safety function channel two safety transmissions are necessary. The logic and the output processing component operate as a receiver and implement the time expectation behavior. The calculation of T_{TOS} is described in Equation (2).

$$T_{TOS} = T_{cycle} + \Delta T \qquad (2)$$

The SHB does not influence T_{TOS} as it is only required to synchronize the system clocks. In case the safety heart beat detects unacceptable delays, then the fail safe state is activated (see 7.3).

9.3.3 Calculation of the worst case safety function response time

The basic safety function channel for the calculation of the worst case safety function is shown in Figure 16.

The safety function response time can be calculated according to Equation (3).

To get the worst case for the safety function response time, one error or failure shall be assumed in the safety function channel. It contributes the maximum difference between its worst case delay time and its timeout time.

$$T_{SFR} = T_S + T_I + T_T + T_L + T_T + T_O + T_A + \max_{i=S,I,...A}(T_{TOi} - T_i) \quad (3)$$

NOTE Index “i” identifies components S, I, T, L, O and A in Equation (3).

System manufacturers shall provide their individual adapted calculation method if necessary.

9.4 Duration of demands

The duration of demand by the safety-related application to the safety communication layer may be present as long as or longer than the process safety time or the FSCP 18/1 timeout time (T_{TO}).

9.5 Constraints for calculation of system characteristics

9.5.1 Safety related constraints

9.5.1.1 General

The boundary conditions and constraints for the safety assessment of FSCP 18/1 and for the relevant calculations of residual error rate are described within the following clauses.

9.5.1.2 Number of information sinks

The number of producing and consuming devices for a FSCP 18/1 network is limited to 512 devices. The number of information sinks for a 1:*n* relationship is limited to 511 consuming devices.

9.5.1.3 Message rate limit

The message rate shall not exceed 1 000 safety messages per second. The number of producing devices and the cycle time has to be considered to not exceed the message rate limit as shown in Equation (4) to (6).

$$MR_{SPDO} = \sum_{I \in SPDO} \frac{1\,000\,000 \times NS_I}{CM_I \times T_{BC}} \quad (4)$$

$$MR_{SHB} = \sum_{D1 \in devices} \left[\sum_{\substack{D2 \in devices \\ D2 \neq D1}} \frac{1\,000\,000 \times NS_{D1} \times 2}{CM_{D1} \times T_{BC}} \right] \quad (5)$$

$$MR = MR_{SPDO} + MR_{SHB} \quad (6)$$

where

CM_{D1}	is the safety producer heartbeat parameter (Index: 0x1217, Sub-index: 0x07, cycle multiplier) sent by device D1 (see Table 20);
CM_{I}	is the Transmit SPDO communication parameter (Index: 0x1E00 - 0x1EFF, Sub-index: 0x07, Cycle multiplier) for SPDOI (see Table 24);
NS_{D1}	is the safety producer heartbeat parameter (Index: 0x1217, Sub-index: 0x09, Number of sends) sent by device D1 (see Table 20);
NS_{I}	is the Transmit SPDO communication parameter (Index: 0x1E00 - 0x1EFF, Sub-index: 0x09, Number of sends) for SPDOI (see Table 24);
MR	is the Total message rate;
MR_{SHB}	is the Message rate for SHBs;
MR_{SPDO}	is the Message rate for SPDOs;
T_{BC}	is the safety bus cycle times. The parameter is depending if CP 18/1 (Index: 0x1218, Sub-index 0x02, Safety RTFL base cycle time) or CP 18/2 (Index: 0x1218, Sub-index: 0x01, Safety RTFN base cycle time) is used (see Table 21).

9.5.1.4 Message size

The message size of one safety PDU consisting of data fields as shown in Figure 17 is restricted from 0 to 128 octets

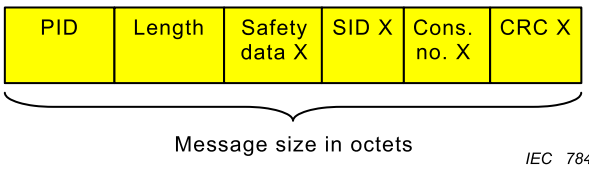


Figure 17 – Considered data fields for message size calculation

9.5.1.5 Bit error rate

The maximum bit error rate shall not exceed 0,01.

9.5.2 Probabilistic considerations

The data integrity checking mechanism of the FSCP 18/1 is totally independent from the mechanisms of the underlying communication system, which then is called a "black channel".

Figure 18 is showing the diagrams of residual error probabilities for the used 32-bit polynomial (minimum Hamming Distance 6). The diagram is for data lengths of 128 octets as specified in 9.5.1.4 including the CRC signature and incorporating the overall safety PDU structure as described in 7.1. The resulting PFH of the communication channel has been calculated to be less than or equal to 10^{-9}. This level equals to 5,43 x 10^{-19} for the residual error probability of one PDU as shown in Figure 18. In order to achieve these levels, the data integrity checking mechanism is mandatory (see 7.1.1.2)

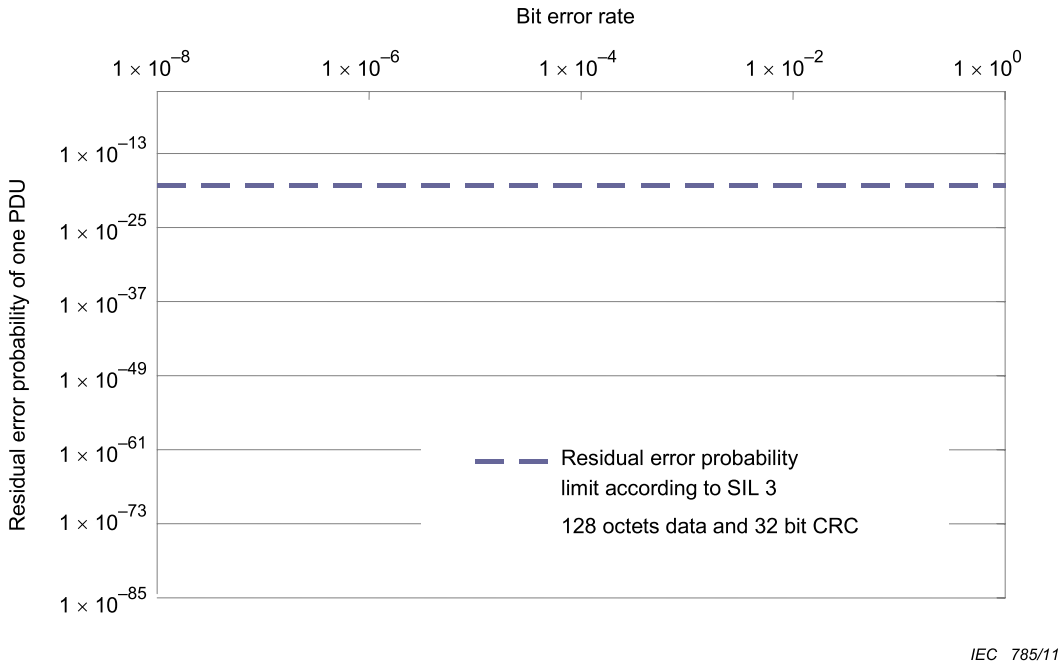


Figure 18 – Residual error rate

9.6 Maintenance

There are no special maintenance requirements for this protocol.

9.7 Safety manual

The manufacturer of the safety device shall provide a safety manual according to the requirements of IEC 61508-2 with the device. Besides the requirements listed in IEC 61508-2 the following information shall be given:

- Manufacturer name and adress;
- Worst case time T_i;
- Timeout time T_{TOi};
- Probability of failure on demand PFH;
- Safety integrity level SIL;
- Proof test interval T_1 (per IEC 61508-6) and/or Mission T_m (per ISO 13849-1);
- Supported protocol version(s) (see 7.1.3.4) unless only protocol version 1 is supported.

NOTE Times can depend on the individual safety functions and operating modes.

10 Assessment

It is highly recommended that implementers of FSCP 18/1 obtain verification from an independent competent body for all functional safety aspects of the product for both, the protocol and any application. It is highly recommended that implementers of FSCP 18/1 obtain proof that a suitable conformance test has been performed by an independent competent body.

The manufacturer of a safety product is responsible for the correct implementation of the safety communication layer technology, the correctness and completeness of the product documentation and information. The complete information is available in [46].

Annex A
(informative)

Additional information
for functional safety communication profiles of CPF 18

There is no additional information for this FSCP.

Annex B
(informative)

Information for assessment of the functional safety communication profiles of CPF 18

Information about test laboratories which test and validate the conformance of FSCP 18/1 products with IEC 61784-3-18 can be obtained from the National Committees of the IEC or from the following organization:

Safety Network International e.V.
Robert-Bosch-Str.30
73760 Ostfildern
GERMANY

Phone: +49 711 3409 118
Fax: +49 711 3409 449
e-mail: info@safety-network.de
URL: www.safety-network.de

Bibliography

[1] IEC 60050 (all parts), *International Electrotechnical Vocabulary*

NOTE See also the IEC Multilingual Dictionary – Electricity, Electronics and Telecommunications (available on CD-ROM and at <http://www.electropedia.org>).

[2] IEC 60204-1, *Safety of machinery – Electrical equipment of machines – Part 1: General requirements*

[3] IEC/TS 61000-1-2, *Electromagnetic compatibility (EMC) – Part 1-2: General – Methodology for the achievement of the functional safety of electrical and electronic equipment with regard to electromagnetic phenomena*

[4] IEC 61131-6[5], *Programmable controllers – Part 6: Functional safety*

[5] IEC 61158 (all parts), *Industrial communication networks – Fieldbus specifications*

[6] IEC 61326-3-1, *Electrical equipment for measurement, control and laboratory use – EMC requirements – Part 3-1: Immunity requirements for safety-related systems and for equipment intended to perform safety related functions (functional safety) – General industrial applications*

[7] IEC 61326-3-2, *Electrical equipment for measurement, control and laboratory use – EMC requirements – Part 3-2: Immunity requirements for safety-related systems and for equipment intended to perform safety related functions (functional safety) – Industrial applications with specified electromagnetic environment*

[8] IEC 61496 (all parts), *Safety of machinery – Electro-sensitive protective equipment*

[9] IEC 61508-1:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements*

[10] IEC 61508-4:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations*

[11] IEC 61508-5:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 5: Examples of methods for the determination of safety integrity levels*

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

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

[14] IEC/PWI 61784-4[6], *Industrial communication networks – Profiles – Part 4: Secure communications for fieldbuses*

[15] IEC 61784-5 (all parts), *Industrial communication networks – Profiles – Part 5: Installation of fieldbuses – Installation profiles for CPF x*

[16] IEC 61800-5-2, *Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional*

[17] IEC/TR 62059-11, *Electricity metering equipment – Dependability – Part 11: General concepts*

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

[19] IEC/TR 62210, *Power system control and associated communications – Data and communication security*

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

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

[22] IEC 62443 (all parts), *Industrial communication networks – Network and system security*

---

5 In preparation.

6 Under consideration.

[23] ISO/IEC Guide 51:1999, *Safety aspects – Guidelines for their inclusion in standards*

[24] ISO/IEC 2382-14, *Information technology – Vocabulary – Part 14: Reliability, maintainability and availability*

[25] ISO/IEC 2382-16, *Information technology – Vocabulary – Part 16: Information theory*

[26] ISO/IEC 7498 (all parts), *Information technology – Open Systems Interconnection – Basic Reference Model*

[27] ISO 10218-1, *Robots for industrial environments – Safety requirements – Part 1: Robot*

[28] ISO 12100-1, *Safety of machinery – Basic concepts, general principles for design – Part 1: Basic terminology, methodology*

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

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

[31] ISO 14121, *Safety of machinery – Principles of risk assessment*

[32] ANSI/ISA-84.00.01-2004 (all parts), *Functional Safety: Safety Instrumented Systems for the Process Industry Sector*

[33] VDI/VDE 2180 (all parts), *Safeguarding of industrial process plants by means of process control engineering*

[34] GS-ET-26[7], *Grundsatz für die Prüfung und Zertifizierung von Bussystemen für die Übertragung sicherheitsrelevanter Nachrichten*, May 2002. HVBG, Gustav-Heinemann-Ufer 130, D-50968 Köln ("*Principles for Test and Certification of Bus Systems for Safety relevant Communication*")

[35] ANDREW S. TANENBAUM, *Computer Networks*, 4th Edition, Prentice Hall, N.J., ISBN-10:0130661023, ISBN-13: 978-0130661029

[36] W. WESLEY PETERSON, *Error-Correcting Codes*, 2nd Edition 1981, MIT-Press, ISBN 0-262-16-039-0

[37] BRUCE P. DOUGLASS, *Doing Hard Time*, 1999, Addison-Wesley, ISBN 0-201-49837-5

[38] *New concepts for safety-related bus systems*, 3rd International Symposium "Programmable Electronic Systems in Safety Related Applications ", May 1998, from Dr. Michael Schäfer, BG-Institute for Occupational Safety and Health.

[39] DIETER CONRADS, *Datenkommunikation*, 3rd Edition 1996, Vieweg, ISBN 3-528-245891

[40] German IEC subgroup DKE AK 767.0.4: *EMC and Functional Safety*, Spring 2002

[41] NFPA79 (2002), *Electrical Standard for Industrial Machinery*

[42] GUY E. CASTAGNOLI, *On the Minimum Distance of Long Cyclic Codes and Cyclic Redundancy-Check Codes*, 1989, Dissertation No. 8979 of ETH Zurich, Switzerland

[43] GUY E. CASTAGNOLI, STEFAN BRÄUER, and MARTIN HERRMANN, *Optimization of Cyclic Redundancy-Check Codes with 24 and 32 Parity Bits*, June 1993, IEEE Transactions On Communications, Volume 41, No. 6

[44] SCHILLER F and MATTES T: *An Efficient Method to Evaluate CRC-Polynomials for Safety-Critical Industrial Communication*, Journal of Applied Computer Science, Vol. 14, No 1, pp. 57-80, Technical University Press, Łódź,Poland, 2006

[45] SCHILLER F and MATTES T: *Analysis of CRC-polynomials for Safety-critical Communication by Deterministic and Stochastic Automata*, 6th IFAC Symposium on Fault Detection, Supervision and Safety for Technical Processes, SAFEPROCESS 2006, pp. 1003-1008, Beijing, China, 2006

[46] *Technical Guideline Integration*, V2.0, December 2008, Safety Network International e. V. Ostfildern, Germany

---

7 GS-ET-26 has served as one of the starting points for this part. It is currently undergoing a major revision.

[47] *CANopen Application Layer and Communication Profile, CiA Draft Standard 301*, Version 4.02, 13 February 2002, CAN in Automation e.V., Nürnberg, Germany

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

RÉSEAUX DE COMMUNICATION INDUSTRIELS – PROFILS

Partie 3-18: Bus de terrain de sécurité fonctionnelle – Spécifications supplémentaires pour le CPF 18

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.

DÉGAGEMENT DE RESPONSABILITÉ
Cette version consolidée n'est pas une Norme IEC officielle, elle a été préparée par commodité pour l'utilisateur. Seules les versions courantes de cette norme et de son(ses) amendement(s) doivent être considérées comme les documents officiels.

Cette version consolidée de l'IEC 61784-3-18 porte le numéro d'édition 1.1. Elle comprend la première édition (2011-04) [documents 65C/639/FDIS et 65C/649/RVD] et son amendement 1 (2016-07) [documents 65C/851/FDIS et 65C/854/RVD]. Le contenu technique est identique à celui de l'édition de base et à son amendement.

Dans cette version Redline, une ligne verticale dans la marge indique où le contenu technique est modifié par l'amendement 1. Les ajouts sont en vert, les suppressions sont en rouge, barrées. Une version Finale avec toutes les modifications acceptées est disponible dans cette publication.

La Norme internationale IEC 61784-3-18 a été établie par le sous-comité 65C: Réseaux de communication industriels, du comité d'études 65 de l'IEC: Mesure, commande et automation dans les processus industriels.

Cette publication a été rédigée selon les Directives ISO/IEC, Partie 2.

Une liste de toutes les parties de la série IEC 61784-3, publiée sous le titre général *Réseaux de communication industriels – Profils – Bus de terrain de sécurité fonctionnelle*, est disponible sur le site Web de l'IEC.

Le comité a décidé que le contenu de la publication de base et de son amendement ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous "http://webstore.iec.ch" dans les données relatives à la publication recherchée. A cette date, la publication sera

- reconduite,
- supprimée,
- remplacée par une édition révisée, ou
- amendée.

IMPORTANT – Le logo *"colour inside"* qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

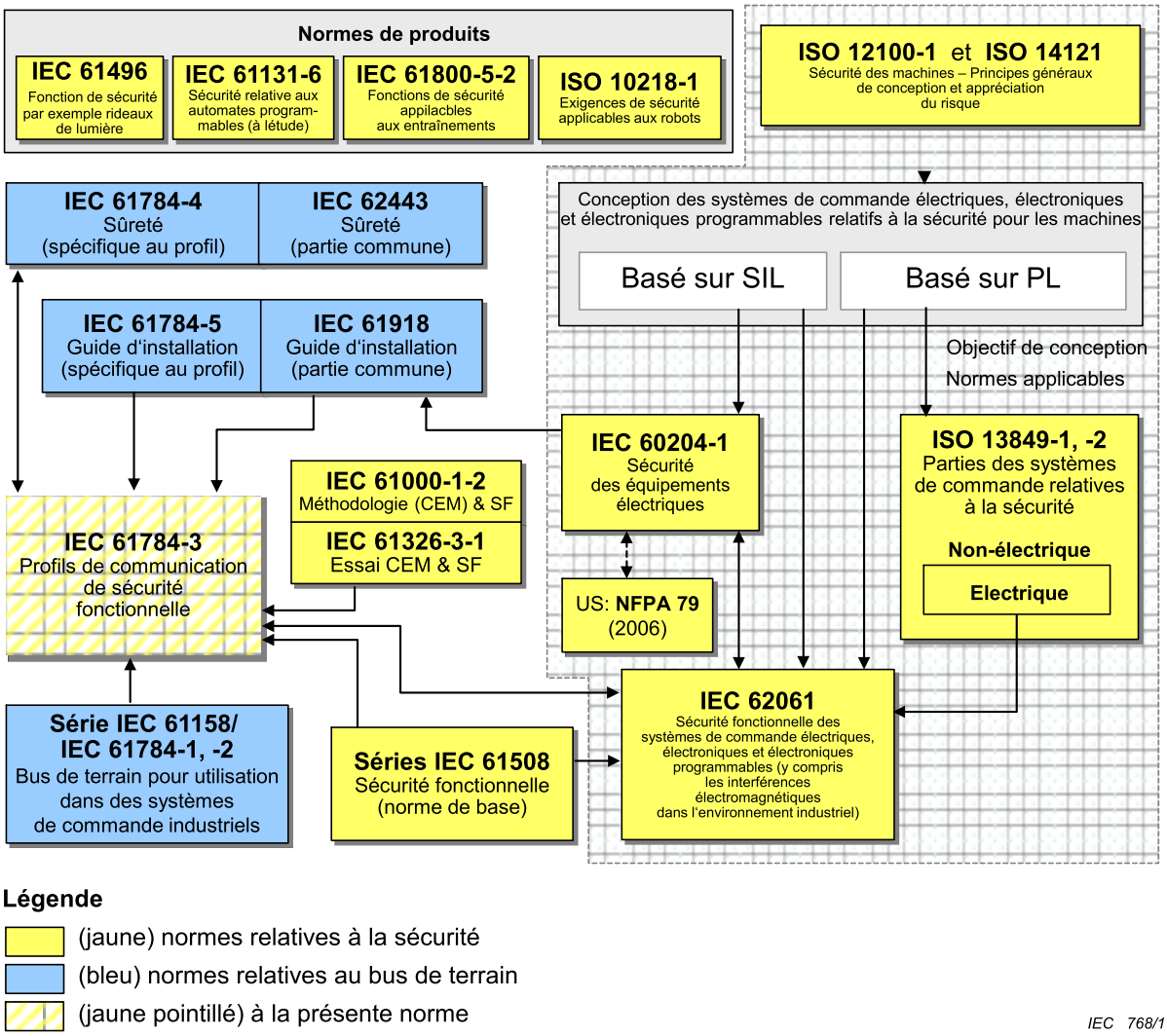
0 Introduction

0.1 Généralités

La norme IEC 61158 relative aux bus de terrain, ainsi que ses normes associées IEC 61784-1 et IEC 61784-2, définissent un ensemble de protocoles de communication qui assurent la commande répartie d'applications automatisées. La technologie de bus de terrain est désormais reconnue et bien éprouvée. Ainsi de nombreuses améliorations des bus de terrain se développent pour traiter de domaines non encore normalisés tels que les applications en temps réel relatives à la sécurité et à la sûreté.

La présente norme définit les principes pertinents applicables aux communications en termes de sécurité fonctionnelle en référence à la série IEC 61508, et spécifie plusieurs couches de communication de sécurité (profils et protocoles correspondants) basés sur les profils de communication et les couches de protocoles de l'IEC 61784-1, l'IEC 61784-2 et la série IEC 61158. Elle ne couvre pas les aspects relatifs à la sécurité électrique et à la sécurité intrinsèque.

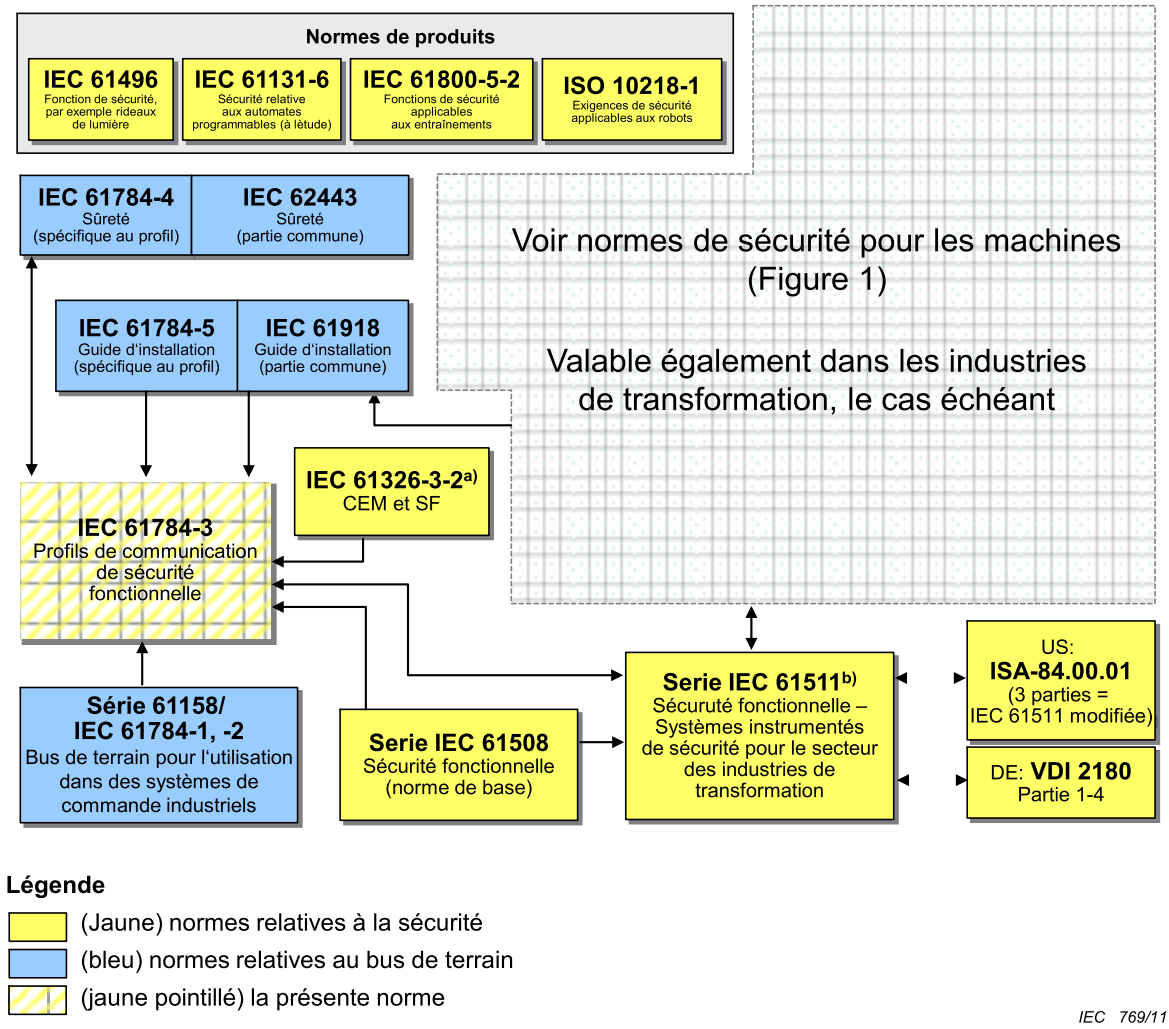
La Figure 1 illustre les relations entre la présente norme et les normes pertinentes relatives à la sécurité et au bus de terrain dans un environnement de machines.



NOTE Les paragraphes 6.7.6.4 (haute complexité) et 6.7.8.1.6 (faible complexité) de l'IEC 62061 spécifient la relation entre PL (catégorie) et SIL.

Figure 1 – Relations entre l'IEC 61784-3 et d'autres normes (machines)

La Figure 2 illustre les relations entre la présente norme et les normes pertinentes relatives à la sécurité et au bus de terrain dans un environnement de transformation.



a Pour des environnements électromagnétiques spécifiés, sinon IEC 61326-3-1.

b EN ratifiée.

Figure 2 – Relations entre l'IEC 61784-3 et d'autres normes (transformation)

Les couches de communication de sécurité mises en œuvre dans le cadre de systèmes relatifs à la sécurité conformément à la série IEC 61508, assurent la confiance nécessaire à accorder à la transmission de messages (information) entre deux participants ou plus sur un bus de terrain dans un système relatif à la sécurité, ou une fiabilité suffisante dans le comportement de sécurité en cas d'erreurs ou de défaillances du bus de terrain.

Les couches de communication de sécurité spécifiées dans la présente norme permettent de garantir cette assurance en utilisant un bus de terrain dans des applications nécessitant une sécurité fonctionnelle jusqu'au niveau d'intégrité de sécurité (SIL) spécifié par son profil de communication de sécurité fonctionnelle correspondant.

La revendication du SIL qui en résulte pour un système dépend de la mise en œuvre du profil de communication de sécurité fonctionnelle retenu au sein du système – la mise en œuvre du profil de communication de sécurité fonctionnelle dans un appareil normal ne suffit pas à le qualifier d'appareil de sécurité.

La présente norme décrit:

– les principes de base de mise en œuvre des exigences de la série IEC 61508 pour les communications de données relatives à la sécurité, y compris les défauts de transmission potentiels, les mesures correctives et les considérations concernant l'intégrité des données;
– la description individuelle des profils de sécurité fonctionnelle pour plusieurs familles de profils de communication dans les IEC 61784-1 et IEC 61784-2;
– les extensions de la couche de sécurité aux sections relatives au service et aux protocoles de communication de la série IEC 61158.

0.2 Déclaration de propriété

La Commission Electrotechnique Internationale (IEC) attire l'attention sur le fait qu'il est déclaré que la conformité avec les dispositions du présent document peut impliquer l'utilisation de brevets concernant les profils de communication de sécurité fonctionnelle pour la famille 18 comme suit, où la notation [xx] désigne le détenteur des droits de propriété:

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

L'IEC ne prend pas position quant à la preuve, la validité et la portée de ces droits de propriété.

Le détenteur de ces droits de propriété a donné l'assurance à l'IEC qu'il consent à négocier des licences avec des demandeurs du monde entier, soit sans frais soit à des termes conditions raisonnables et non discriminatoires. A ce propos, la déclaration du détenteur des droit de propriété est enregistrée à l'IEC.

Des informations peuvent être obtenues auprès de:

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

L'attention est d'autre part attirée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété autres que ceux mentionnés ci-dessus. L'IEC ne saurait être tenue pour responsable de l'identification de ces droits de propriété en tout ou en partie.

L'ISO (www.iso.org/patents) et l'IEC (http://www.iec.ch/tctools/patent_decl.htm) maintiennent des bases des données, consultables en ligne, des droits de propriété pertinents à leurs normes. Les utilisateurs sont encourages à consulter ces bases de données pour obtenir l'information la plus récente concernant les droits de propriété.

RÉSEAUX DE COMMUNICATION INDUSTRIELS – PROFILS

Partie 3-18: Bus de terrain de sécurité fonctionnelle – Spécifications supplémentaires pour le CPF 18

1 Domaine d'application

La présente partie de la série IEC 61784-3 spécifie une couche de communication relative à la sécurité (services et protocole) fondée sur le CPF 18 de l'IEC 61784-2 et le type 22 de l'IEC 61158. Elle identifie les principes applicables aux communications de sécurité fonctionnelle définies dans l'IEC 61784-3, et appropriés à cette couche de communication de sécurité.

NOTE 1 Elle ne couvre pas les aspects relatifs à la sécurité électrique et à la sécurité intrinsèque. La sécurité électrique concerne les dangers tels que les chocs électriques. La sécurité intrinsèque concerne les dangers associés aux atmosphères explosibles.

La présente partie[1] définit les mécanismes de transmission des messages propres à la sécurité entre les participants d'un réseau réparti, en utilisant la technologie de bus de terrain conformément aux exigences de la série IEC 61508[2] concernant la sécurité fonctionnelle. Ces mécanismes peuvent être utilisés dans diverses applications industrielles, telles que la commande de processus, l'usinage automatique et les machines.

La présente partie fournit des lignes directrices tant pour les développeurs que pour les évaluateurs d'appareils et systèmes conformes.

NOTE 2 La revendication du SIL qui résulte pour un système dépend de la mise en œuvre du profil de communication de sécurité fonctionnelle retenu au sein du système – la mise en œuvre du profil de communication de sécurité fonctionnelle, conforme à la présente partie, dans un appareil normal ne suffit pas à le qualifier de appareil de sécurité.

2 Références normatives

Les documents de référence suivants sont indispensables pour l'application du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

IEC 61158-3-22, *Industrial communication networks – Fieldbus specifications – Part 3-22: Data-link layer service definition – Type 22 elements* (disponible uniquement en anglais)

IEC 61158-4-22, *Industrial communication networks – Fieldbus specifications – Part 4-22: Data-link layer protocol specification – Type 22 elements* (disponible uniquement en anglais)

IEC 61158-5-22, *Industrial communication networks – Fieldbus specifications – Part 5-22: Application layer service definition – Type 22 elements* (disponible uniquement en anglais)

---

1 Dans les pages suivantes de la présente norme, "la présente partie" se substitue à "cette partie de la série IEC 61784-3".

2 Dans les pages suivantes de la présente norme, "IEC 61508" se substitue à "série IEC 61508".

IEC 61158-6-22, *Industrial communication networks – Fieldbus specifications – Part 6-22: Application layer protocol specification – Type 22 elements* (disponible uniquement en anglais)

IEC 61508 (toutes parties), *Sécurité fonctionnelle des systèmes électriques/électroniques/ électroniques programmables relatifs à la sécurité*

IEC 61508-2:2010, *Sécurité fonctionnelle des systèmes électriques/électroniques/ électroniques programmables relatifs à la sécurité – Partie 2: Exigences pour les systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité*

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

IEC 61784-3:2010, *Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions* (disponible uniquement en anglais)

IEC 61918, *Industrial communication networks – Installation of communication networks in industrial premises* (disponible uniquement en anglais)

ISO/IEC 10731, *Technologies de l'information – Interconnexion de systèmes ouverts – Modèle de référence de base – Conventions pour la définition des services OSI*

3 Termes, définitions, symboles, abréviations et conventions

3.1 Termes et définitions

Pour les besoins du présent document, les termes et définitions suivants s'appliquent.

3.1.1 Termes et définitions communs

3.1.1.1
disponibilité
probabilité, pour un système automatisé, qu'il ne se produise pas de conditions opérationnelles non satisfaisantes, telles que la perte de production, pendant une période donnée

3.1.1.2
canal noir
canal de communication sans preuve existante de conception ou de validation conformément à l'IEC 61508

3.1.1.3
canal de communication
connexion logique entre deux points limites d'un *système de communication*

3.1.1.4
système de communication
disposition de matériels, logiciels et vecteurs de propagation destinée à permettre la transmission de *messages* (couche d'application définie dans l'ISO/IEC 7498) d'une application à une autre

3.1.1.5
connexion
liaison logique entre deux objets d'application d'appareils identiques ou différents

3.1.1.6
contrôle de redondance cyclique (CRC)
<valeur> donnée redondante déduite, et enregistrée ou transmise simultanément, d'un bloc de données afin de détecter toute corruption des données

<méthode> procédure utilisée pour calculer les données redondantes

NOTE 1 Les termes « code CRC » et « signature CRC », et les étiquettes telles que CRC1, CRC2, peuvent également être utilisés dans la présente norme pour se référer aux données redondantes.

NOTE 2 Voir également [35], [36]]3.

3.1.1.7
erreur
écart ou discordance entre une valeur ou une condition calculée, observée ou mesurée, et la valeur ou la condition vraie, prescrite ou théoriquement correcte

[IEC 61508-4:2010], [IEC 61158]

NOTE 1 Les erreurs peuvent être causées par des erreurs de conception du matériel/logiciel et/ou des informations altérées du fait de perturbations électromagnétiques et/ou autres effets.

NOTE 2 Les erreurs ne produisent nécessairement pas une *défaillance* ou une *panne*.

3.1.1.8
défaillance
cessation de l'aptitude d'une unité fonctionnelle à accomplir une fonction requise ou fonctionnement d'une unité fonctionnelle d'une toute autre manière que celle requise

NOTE 1 La définition de l'IEC 61508-4 est identique avec des notes complémentaires.

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

NOTE 2 Une défaillance peut être causée par une *erreur* (par exemple, problème de conception matérielle/logicielle ou rupture de message).

3.1.1.9
panne
condition anormale susceptible de provoquer la réduction, ou la perte, de capacité d'une unité fonctionnelle à accomplir une fonction requise

NOTE Le VEI 191-05-01 définit la « panne » comme un état caractérisé par l'incapacité à accomplir une fonction requise, à l'exclusion de l'incapacité au cours de la période de maintenance préventive ou autres actions planifiées, ou du fait de l'absence de ressources externes.

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

3.1.1.10
bus de terrain
système de communication basé sur le transfert de données en série et utilisé dans des applications d'automatisation industrielle ou de commande de processus

3.1.1.11
trame
synonyme discrédité de DLPDU

3.1.1.12
séquence de contrôle de trame (FCS)
données redondantes issues d'un bloc de données d'une DLPDU (trame), utilisant une fonction de hachage, et enregistrées ou transmises avec le bloc de données, afin de déterminer l'altération des données

---

3 Les chiffres entre crochets font référence à la Bibliographie.

NOTE 1 Il est possible de calculer une FCS à l'aide, par exemple, d'un CRC ou d'une autre fonction de hachage.

NOTE 2 Voir également [35], [36].

3.1.1.13
fonction de hachage
fonction (mathématique) de mise en correspondance des valeurs d'un ensemble (éventuellement) très grand de valeurs en une plage de valeurs (habituellement) plus petite

NOTE 1 Les fonctions de hachage peuvent être utilisées pour déterminer l'altération des données.

NOTE 2 Les fonctions de hachage courantes incluent la parité, la somme de contrôle ou le CRC.

[IEC/TR 62210, modifiée]

3.1.1.14
danger
état ou ensemble de conditions d'un système qui, avec d'autres conditions associées, entraîne inévitablement un préjudice pour les personnes, les biens ou l'environnement

3.1.1.15
message
série ordonnée d'octets destinée à communiquer des informations

[ISO/IEC 2382-16.02.01, modifiée]

3.1.1.16
collecteur de messages
partie d'un *système de communication* destiné à recevoir des *messages*

[ISO/IEC 2382-16.02.03]

3.1.1.17
source de messages
partie d'un *système de communication* destiné à envoyer des *messages*

[ISO/IEC 2382-16.02.02]

3.1.1.18
déclenchement de nuisance
déclenchement parasite sans effet préjudiciable

NOTE Les erreurs anormales internes peuvent être générées dans des systèmes de communication tels que des systèmes de transmission par ondes radioélectriques, par exemple, du fait d'un trop grand nombre de nouvelles tentatives en présence de perturbations.

3.1.1.19
niveau de performance (PL)
niveau discret utilisé pour spécifier la capacité des parties relatives à la sécurité des systèmes de commande à accomplir une fonction de sécurité dans des conditions prévisibles

[ISO 13849-1]

3.1.1.20
redondance
existence de moyens, outre les moyens qui se révèleraient suffisants pour qu'une unité fonctionnelle accomplisse une fonction requise ou que des données représentent une information

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

3.1.1.21
risque
combinaison de la probabilité d'un dommage et de sa gravité

NOTE Pour plus d'informations sur ce concept, se reporter à l'Annexe A de l'IEC 61508-5:2010.

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

3.1.1.22
couche de communication de sécurité (SCL)
couche de communication qui comprend toutes les mesures nécessaires permettant d'assurer la transmission de données en toute sécurité conformément aux exigences de l'IEC 61508

3.1.1.23
données de sécurité
données transmises par un réseau de sécurité utilisant un protocole de sécurité

NOTE La couche de communication de sécurité ne garantit pas la sécurité des données proprement dites, mais uniquement la transmission en toute sécurité de ces dernières.

3.1.1.24
appareil de sécurité
appareil conçu conformément à l'IEC 61508 et qui met en oeuvre le profil de communication de sécurité fonctionnelle

3.1.1.25
fonction de sécurité
fonction à réaliser par un système E/E/PE relatif à la sécurité ou par un appareil externe de réduction de risque, prévue pour assurer ou maintenir un état de sécurité de l'EUC par rapport à un événement dangereux spécifique

NOTE La définition de l'IEC 61508-4 est identique, avec un exemple et des références supplémentaires.

[IEC 61508-4:2210, modifiée]

3.1.1.26
temps de réponse de la fonction de sécurité
temps écoulé du cas le plus défavorable suite à l'activation d'un capteur de sécurité relié à un bus de terrain, avant que ne soit atteint l'état de sécurité correspondant de son (ses) actionneur(s) de sécurité, du fait d'erreurs ou de défaillances avérées dans le canal de fonction de sécurité

NOTE Ce concept est introduit dans l'IEC 61784-3:2010, 5.2.4, et traité par les profils de communication de sécurité fonctionnelle définis dans la présente partie.

3.1.1.27
niveau d'intégrité de sécurité (SIL)
niveau discret (parmi quatre possibles), correspondant à une gamme de valeurs d'intégrité de sécurité où le niveau 4 d'intégrité de sécurité possède le plus haut degré d'intégrité et le niveau 1 possède le plus bas

NOTE 1 Les objectifs chiffrés de défaillance (voir l'IEC 61508-4:2010, 3.5.17) pour les quatre niveaux d'intégrité de sécurité sont indiqués dans les Tableaux 2 et 3 de l'IEC 61508-1:2010.

NOTE 2 Les niveaux d'intégrité de sécurité sont utilisés pour spécifier les exigences concernant l'intégrité de sécurité des fonctions de sécurité à allouer aux systèmes E/E/PE relatifs à la sécurité.

NOTE 3 Le niveau d'intégrité de sécurité (SIL) ne constitue pas une propriété d'un système, sous-système, élément ou composant. L'interprétation correcte de l'expression « système relatif à la sécurité à SIL*n* » (où *n* est 1, 2, 3 ou 4) signifie que le système est potentiellement capable de prendre en charge des fonctions de sécurité avec un niveau d'intégrité de sécurité jusqu'à *n*.

[IEC 61508-4:2010]

3.1.1.28
mesure de sécurité
<la présente norme> mesure permettant de contrôler les *erreurs* de communication éventuelles, qui est conçue et mise en œuvre conformément aux exigences de l'IEC 61508

NOTE 1 Dans la pratique, plusieurs mesures de sécurité sont combinées pour atteindre le niveau d'intégrité de sécurité requis.

NOTE 2 Les *erreurs* de communication et les mesures de sécurité associées sont détaillées dans l'IEC 61784-3:2010, 5.3 et 5.4.

3.1.1.29
application relative à la sécurité
programmes conçus conformément à l'IEC 61508 pour satisfaire aux exigences SIL de l'application

3.1.1.30
système relatif à la sécurité
système qui exécute les *fonctions de sécurité* conformément à l'IEC 61508

3.1.1.31
déclenchement parasite
déclenchement provoqué par le système de sécurité sans injonction du processus

3.1.2 CPF 18: Termes et définitions supplémentaires

3.1.2.1
relation client/serveur
relation dans laquelle le client envoie des données au serveur qui transmet en retour les données demandées

3.1.2.2
numéro consécutif
entier sans signe comportant un retour à zéro en cas de débordement, utilisé comme moyen permettant de s'assurer de l'exhaustivité et du bon ordre des PDU de sécurité transmises

NOTE Instance de « numéro de séquence » tel que décrit dans l'IEC 61784-3.

3.1.2.3
cycle
intervalle auquel une liste d'instructions ou une activité est exécutée de manière répétitive et continue

3.1.2.4
retard
temps de transmission des PDU ayant pour origine dynamique les propriétés du réseau, telles que le trafic, les appareils de commutation et la topologie

3.1.2.5
à sécurité intégrée
capacité d'un système qui, par l'adoption de mesures techniques ou organisationnelles appropriées, évite les dangers de manière déterministe, ou par réduction du risque potentiel à une mesure tolérable

3.1.2.6
passerelle
appareil qui intervient comme élément de liaison entre des protocoles différents

3.1.2.7
double ligne logique
séquence de l'appareil racine et de tous les appareils ordinaires prenant en charge le traitement de la trame de communication dans les directions avant et arrière

3.1.2.8
relation producteur/consommateur
relation dans laquelle le producteur envoie des données au consommateur sans aucune demande spécifique

3.1.2.9
ligne de trame en temps réel (RTFL)
modèle de communication dont les appareils constitutifs communiquent dans une double ligne logique (voir CP 18/2)

3.1.2.10
réseau de trames en temps réel (RTFN)
modèle de communication dont les appareils constitutifs communiquent dans un réseau commuté (voir CP 18/1)

3.1.2.11
gestion SCL (SALMT)

mécanisme de commande de l'état SCL des appareils de sécurité

3.1.2.12
contrôle de retard de sécurité (SDM)
mécanisme de sécurité permettant le contrôle cyclique du retard des PDU transmises

3.1.2.13
cadence (impulsions) de sécurité (SHB)
mécanisme de contrôle cyclique de l'état des appareils de sécurité

3.1.2.14
objet de données de processus de sécurité (SPDO)
mécanisme d'échange cyclique de données de processus de sécurité entre appareils

3.1.2.15
relation émetteur/récepteur
relation dans laquelle l'émetteur envoie des données au récepteur

3.1.2.16
relation 1:1
relation de communication comportant exactement un émetteur et un récepteur

3.1.2.17
relation 1:n
relation de communication comportant exactement un émetteur et un ou plusieurs récepteurs

3.2 Symboles et abréviations

3.2.1 Symboles et abréviations communs

CEM	Compatibilité électromagnétique	
CP	Profil de communication (*communication profile*)	[IEC 61784-1]
CPF	Famille de profils de communication (*Communication Profile Family*)	[IEC 61784-1]
CRC	Contrôle de redondance cyclique (*Cyclic Redundancy Check*)	
DLL	Couche de liaison de données (*Data Link Layer*)	[ISO/IEC 7498-1]

DLPDU	Unité de données de protocole de liaison de données (*Data Link Protocol Data Unit*)	
EUC	Equipement commandé (*Equipment Under Control*)	[IEC 61508-4:2010]
E/E/PE	Electrique/électronique/électronique programmable (*Electrical/Electronic/Programmable Electronic*)	[IEC 61508-4:2010]
FAL	Couche Application de bus de terrain (*Fieldbus Application Layer*)	[IEC 61158-5]
FCS	Séquence de contrôle de trame (*Frame Check Sequence*)	
FS	Sécurité fonctionnelle (*Functional Safety*)	
FSCP	Profil de communication de sécurité fonctionnelle (*Functional Safety Communication Profile*)	
PDU	Unité de données de protocole (*Protocol Data Unit*)	[ISO/IEC 7498-1]
PFH	Fréquence moyenne de défaillance dangereuse par heure (*Average frequency of dangerous failure*) [h-1]	[IEC 61508-4]
PhL	Couche physique (*Physical Layer*)	[ISO/IEC 7498-1]
PL	Niveau de performance (*Performance Level*)	[ISO 13849-1]
PLC	Automate programmable (*Programmable Logic Controller*)	
SCL	Couche de communication de sécurité (*Safety Communication Layer*)	
SIL	Niveau d'intégrité de sécurité (*Safety Integrity Level*)	[IEC 61508-4:2010]

3.2.2 CPF 18: Symboles et abréviations supplémentaires

3.2.2.1 Abréviations supplémentaires

AL	Couche Application (*Application layer*)
AP	Processus d'Application (*Application process*)
CDC	Canal de données cycliques (*Cyclic data channel*)
FSF	A sécurité intégrée (*Fail-safe*)
ID	Indicatif (*Identification*)
PDO	Objet de données de processus (*Process data object*)
PDO-ID	Indicatif d'objet de données de processus (*Process data object ID*)
PID	Indicatif de paquet (*Packet ID*)
RTFL	Ligne de trame en temps réel (*Real time frame line*)
RTFN	Réseau de trames en temps réel (*Real time frame network*)
SALMT	Gestion SCL (*SCL management*)
SDM	Contrôle de retard de sécurité (*Safety delay monitoring*)
SHB	Cadence (impulsions) de sécurité (*Safety heartbeat*)
SID	Indicatif de sécurité (*Safety ID*)
SPDO	Objet de données de processus de sécurité (*Safety process data object*)

3.2.2.2 Symboles supplémentaires

Symbole	Définition	Description	Unité
T_A	Temps d'activation	Temps de réponse le plus défavorable de l'actionneur pour conversion et réaction selon la fonction de sécurité	µs
T_{cycle}	Temps de cycle	Temps de cycle de communication	µs
T_I	Temps d'entrée	Temps de traitement le plus défavorable de l'appareil d'entrée	µs
T_L	Temps de traitement logique	Temps de traitement le plus défavorable de l'automate logique de sécurité	µs
T_O	Temps de sortie	Temps de traitement le plus défavorable de l'appareil de sortie	µs

Symbole	Définition	Description	Unité
T_S	Temps de détection	Temps de réponse le plus défavorable du détecteur de la constatation du changement d'un signal physique au résultat de conversion valide	µs
T_{SFR}	Temps de réponse de la fonction de sécurité	Temps de réponse de la fonction de sécurité du signal d'entrée physique à la réaction effective de l'actionneur	µs
T_{TOi}	Durée de temporisation de composant	Durée de temporisation du composant de sécurité i	µs
T_{TOS}	Temps de transmission	Temps de transmission le plus défavorable du réseau de communication. Temps de temporisation pour FSCP 18/1	µs
ΔT	Marge de temporisation	Marge supplémentaire applicable au temps de cycle de transmission. Cette valeur est définie par l'utilisateur sur la base des exigences de l'application. La plage typique est comprise entre 0 % et 15%	µs

3.3 Conventions

Les attributs d'un objet sont décrits sous la forme indiquée dans le Tableau 1. La signification des attributs est décrite dans la liste suivante.

- L'attribut « Index» décrit la position d'un objet dans le dictionnaire d'objets de sécurité.
- L'attribut «Sous-index» décrit un élément unique de l'objet contenant les données suivantes. Le sous-index est répété pour chaque élément de l'objet.
  - L'attribut « Nom » désigne une chaîne de noms applicable à cet attribut.
  - L'attribut « Description » est utilisé pour les informations supplémentaires concernant la méthode selon laquelle l'objet doit être utilisé.
  - L'attribut «Type d'objet » désigne le type de caractérisation de chaque objet, tel que spécifié dans l'IEC 61158-6-22..
  - L'attribut «Type de données » désigne le type de données de cet élément.
  - L'attribut « Catégorie » indique si l'élément est obligatoire (M), facultatif (O) ou dépend de l'établissement d'autres attributs (C).
  - L'attribut «Attribut d'accès » montre l'accès direct à cet élément. RO signifie droit d'accès en lecture, RW signifie droit d'accès en lecture-écriture, WO signifie droit d'accès en écriture, tandis que FSF désigne l'absence de droits d'accès, à l'exception de l'application de sécurité et de l'accès en lecture facultatif par les services SDO, tel que spécifié dans l'IEC 61158-5-22 et l'IEC 61158-6-22.
  - L'attribut « Mise en correspondance SPDO » désigne la possibilité de faire correspondre cet attribut à TxSPDO ou RxSPDO, ou d'indiquer que ce paramètre ne peut être mis en correspondance.
  - L'attribut « Plage de valeurs» contient la plage de valeurs d'un élément dédié ou l'attribut «Aucune » pour indiquer l'absence de plage de valeurs prédéfinie.
  - L'attribut « Valeur » contient la (les) valeur(s) constante(s) et/ou la signification du paramètre ou l'attribut «Aucune » pour indiquer l'absence de valeur prédéfinie.

Tableau 1 – Définition des objets

Attribut	Valeur
Index	
Sous-index	
Nom	
Description	
Type d'objet	
Type de données	
Catégorie	
Attribut d'accès	
Mise en correspondance SPDO	
Plage de valeurs	
Valeur	

Les éléments de la syntaxe FSCP associés à la structure PDU sont décrits tel qu'indiqué dans le Tableau 2. La signification des colonnes du tableau est décrite dans la liste suivante.

- La colonne « Décalage d'octet » désigne le décalage de l'élément DLPDU par rapport au début de la PDU de sécurité.
- La colonne « Champ de données » est le nom de l'élément.
- La colonne « Valeur/Description » contient la valeur constante ou la signification du paramètre.

Tableau 2 – Définition des éléments PDU de sécurité

Décalage d'octet	Champ de données	Description

4 Présentation de FSCP 18/1 (SafetyNET p™)

4.1 Généralités

La famille de profils de communication 18 (communément appelée SafetyNET p™[4]) définit des profils de communication sur la base des IEC 61158-3-22 IEC 61158-4-22, IEC 61158-5-22 et IEC 61158-6-22.

Les profils de base CP 18/1 et CP 18/2 sont définis dans l'IEC 61784-2:2010. Le profil de communication de sécurité fonctionnelle FSCP 18/1 (SafetyNET p™) est basé sur les profils de base de CPF 18 spécifiés dans l'IEC 61784-2 et les spécifications de la couche de communication de sécurité définies dans la présente partie.

---

4 SafetyNET p est l'appellation commerciale de Pilz GmbH & Co. KG. Cette information est donnée à l'intention des utilisateurs de la présente norme internationale et ne signifie nullement que l'IEC approuve ou recommande le détenteur de la marque ou l'un quelconque de ses produits. La conformité à la présente partie n'exige aucunement l'utilisation de la marque SafetyNET p, ladite utilisation nécessitant l'accord de Pilz GmbH & Co. KG.

4.2 FSCP 18/1

Le protocole FSCP 18/1 décrit un protocole de sécurité qui permet le transfert de données de processus de sécurité jusqu'au niveau SIL 3 entre les appareils de type FSCP 18/1. Un bus de terrain subordonné non pris en compte dans les considérations de sécurité (méthode du canal noir) est utilisé pour le transfert du protocole de sécurité. Les données de sécurité échangées entre des partenaires de communication sont considérées comme des données de processus cyclique échangées entre eux par le bus de terrain subordonné.

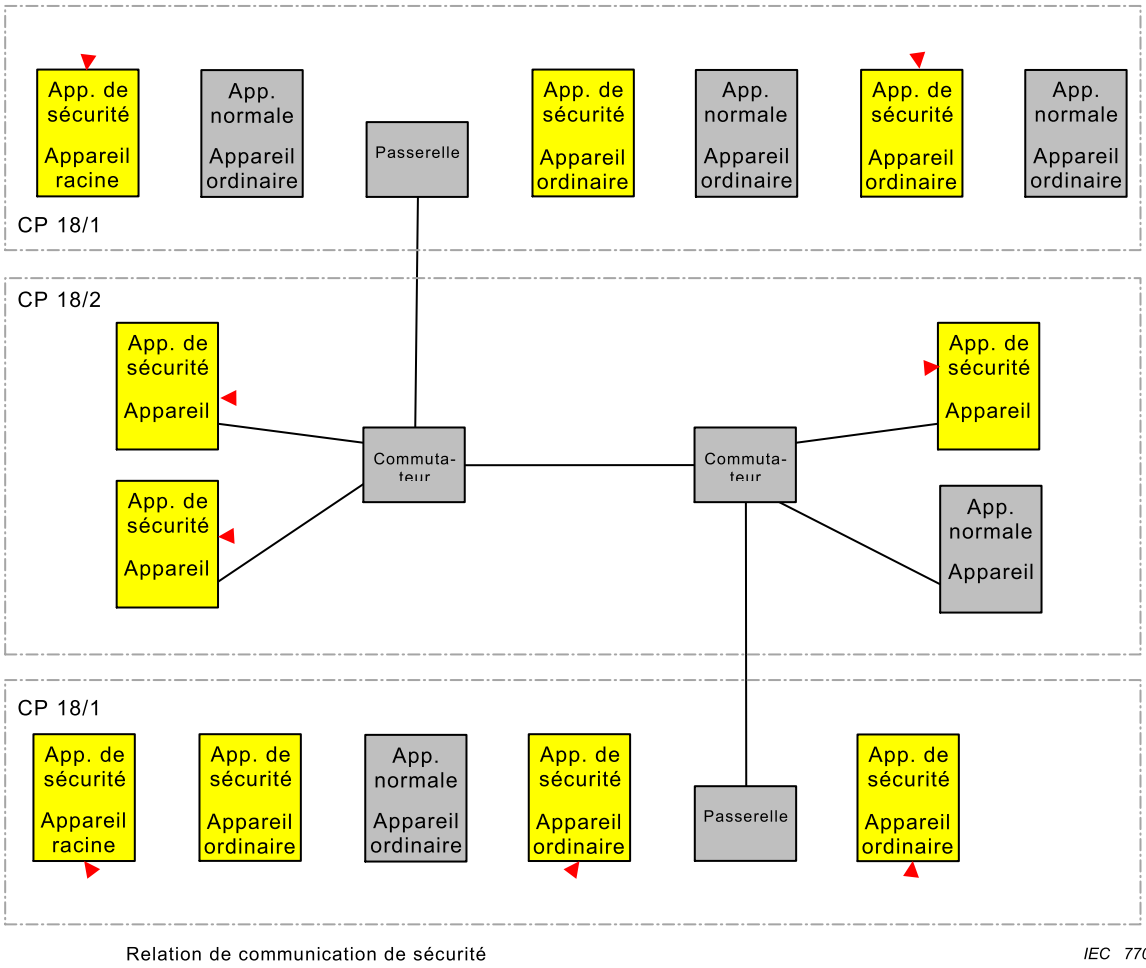


Figure 3 – Système FSCP 18/1

Le système FSCP 18/1 utilise une relation 1:n dédiée du type relation producteur/consommateur pour la communication de données de processus de sécurité et une relation 1:1 à des fins de contrôle des appareils de sécurité. La Figure 3 montre les relations de communication potentielles fondées sur un réseau CP 18/1 et CP 18/2.

Les mesures de sécurité suivantes ont été retenues pour réaliser le système FSCP 18/1:

- numéro de session (numéro consécutif);
- délai de contrôle de communication;
- identification unique des émetteurs;
- contrôle de redondance cyclique pour l'intégrité des données;

- différents systèmes d'assurance d'intégrité des données pour les communications de sécurité et de non sécurité;
- contrôle de retard des paquets pour les relations de communication dédiées.

Chaque appareil maintient un automate fini à couche de communication de sécurité, dont la coordination s'effectue par l'application de sécurité. La sécurité est assurée sur la base de la commutation SCL en état d'erreur système (c'est-à-dire état de sécurité) dès la détection d'une erreur.

5 Généralités

5.1 Documents externes de spécifications applicables au profil

Le document suivant est utile pour bien comprendre la conception du protocole FSCP 18/1:

- GS-ET-26 [34]

5.2 Exigences fonctionnelles de sécurité

Les exigences suivantes doivent s'appliquer au développement d'appareils qui mettent en oeuvre le protocole FSCP 18/1. Les mêmes exigences ont été appliquées pour le développement de ce protocole.

- Les exigences de l'IEC 61508 doivent être satisfaites.
- Le protocole FSCP 18/1 est conçu de manière à prendre en charge le niveau d'intégrité de sécurité 3 (SIL 3) (voir IEC 61508).
- Le protocole FSCP 18/1 est mis en œuvre en appliquant la méthode du canal noir; aucune dépendance relative à la sécurité ne s'applique aux profils de communication CPF 18 normaux. Le matériel de transmission ne doit pas être modifié.
- Les communications de sécurité et normale doivent être indépendantes. Les appareils de sécurité et normaux doivent être capables d'utiliser le même canal de communication.
- Une relation 1:1 doit toujours exister entre les appareils de communication à des fins de contrôle des appareils.
- La communication de sécurité doit utiliser un système de communication mono-canal. La redondance peut uniquement être utilisée, le cas échéant, pour une plus grande disponibilité.
- La mise en œuvre du protocole de sécurité doit être limitée aux appareils terminaux de communication.
- La durée de transmission doit être contrôlée.
- Les documents propres aux appareils doivent indiquer le niveau d'intégrité de sécurité (SIL) pour lequel ces derniers sont conçus.
- Pour les appareils qui utilisent la version 2 du protocole (voir 7.1.3.4), il est exigé d'ajouter 10^{-9} à la PFH du matériel de l'appareil pour tenir compte du canal de communication.

  NOTE De cette manière, l'utilisateur de l'appareil n'aura pas à tenir compte du nombre de connexions logiques dans une fonction de sécurité.
- L'utilisation des mécanismes de correction d'erreurs dans le canal noir est admise.

5.3 Mesures de sécurité

Les mesures de sécurité appliquées dans le protocole FSCP 18/1 pour détecter les erreurs de communication sont énumérées dans le Tableau 3. Toutes les mesures de sécurité doivent être appliquées et contrôlées dans chaque appareil de sécurité.

Tableau 3 – Erreurs de communication et mesures de détection

Erreurs de communication	Mesures de sécurité				
	Numéro de séquence	Délai [a]	Authentification de connexion [b]	Assurance d'intégrité des données	Différents systèmes d'assurance d'intégrité des données
Corruption	—	—	—	X	—
Répétition non prévue	X	—	—	—	—
Séquence incorrecte	X	—	—	—	—
Perte	X	X	—	—	—
Retard inacceptable	—	X	—	—	—
Insertion	X	—	X	—	—
Déguisement	X	—	X	—	X
Adressage	X	—	X	—	—
Défaillances de mémoire tournante des commutateurs	X	X	X	X	—

[a] « T_{TOS} » dans la présente norme.

b Réalisé par "SID" et "PID" dans la présente norme.

5.4 Structure de la couche de communication de sécurité

La Figure 4 montre la relation entre le protocole, CPF 18 et le type 22. La couche de communication de sécurité du protocole FSCP 18/1 se situe au sommet des couches d'application de CPF 18 et du type 22 et des couches de liaison de données, et utilise les services de non-sécurité de CPF 18 et du type 22 pour transférer les PDU de sécurité.

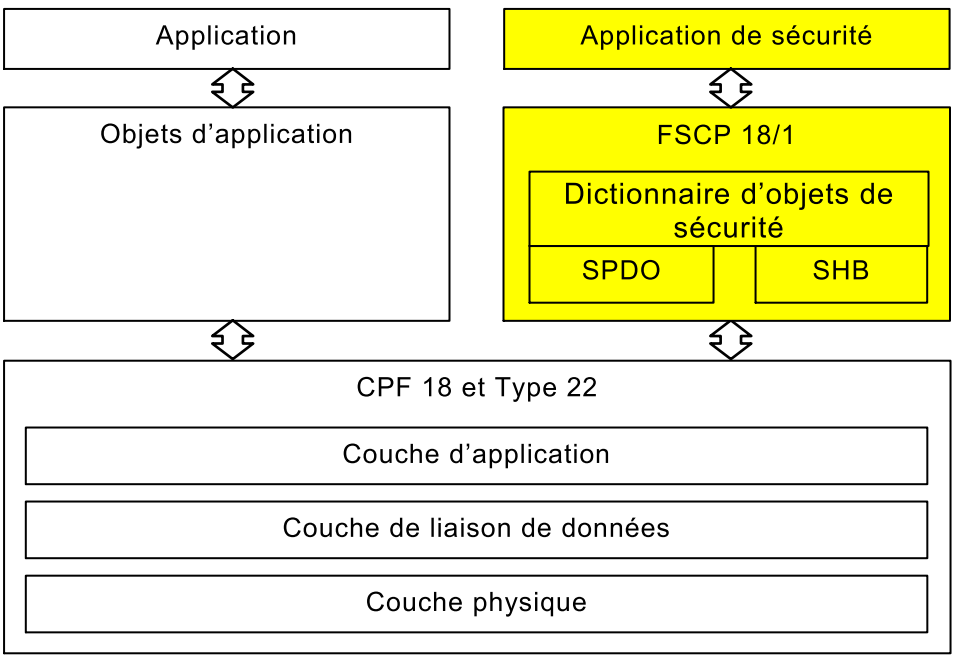


Figure 4 – Architecture logicielle du protocole FSCP 18/1

Les objets de données de processus de type 22 comprennent un objet de données de processus de sécurité (SPDO) contenant les données de processus de sécurité, les informations d'identification et les mesures de détection d'erreurs requises. La mise en

correspondance des données de processus de sécurité avec les SPDO s'effectue par les entrées du dictionnaire d'objets de sécurité.

Un service de cadence de sécurité (SHB) permet de contrôler la synchronisation temporelle de l'application de sécurité.

Le calcul de la probabilité d'erreur résiduelle propre au protocole FSCP 18/1 ne bénéficie pas des mécanismes de détection d'erreurs du système de communication. Le protocole peut également être transféré par l'intermédiaire d'autres systèmes de communication.

5.5 Relations avec la FAL (et DLL, PhL)

5.5.1 Généralités

Cette couche de communication de sécurité est conçue pour être utilisée avec les profils de communication CPF 18. Elle ne se limite toutefois pas à ce profil de communication.

5.5.2 Types de données

Les profils définis dans la présente partie prennent en charge tous les types de données CPF 18 définis dans l'IEC 61158-5-22. Le codage de ces types de données suit les règles de codage définies dans l'IEC 61158-6-22.

6 Services de la couche de communication de sécurité

6.1 Eléments généraux

6.1.1 Généralités

Le protocole FSCP 18/1 fournit les éléments suivants:

- dictionnaire d'objets de sécurité;
- objet de données de processus de sécurité (SPDO);
- cadence (impulsions) de sécurité (SHB);
- contrôle de retard de sécurité (SDM).

6.1.2 Dictionnaire d'objets de sécurité

Le dictionnaire d'objets de sécurité constitue l'interface entre l'application de sécurité et le système de communication. Il consiste en un regroupement d'objets et spécifie des paramètres de communication et d'appareil uniformes pour la fonctionnalité relative à la sécurité. L'organisation des objets est adaptée à l'organisation de CP 18/1 et CP 18/2. L'accès aux entrées des dictionnaires d'objets de sécurité peut le cas échéant s'effectuer par les services SDO tels que définis dans l'IEC 61158-5-22 et l'IEC 61158-6-22. Cet accès doit être limité à l'accès en lecture seulement (RO).

6.1.3 Objet de données de processus de sécurité (SPDO)

Les objets de données de processus de sécurité doivent fournir les services requis pour l'échange de données de processus relatif à la sécurité entre certains appareils de communication. La communication des données de processus de sécurité avec le protocole FSCP 18/1 s'effectue de manière cyclique en utilisant les objets de données de processus de sécurité (SPDO). La communication des données de processus est répartie en objets de données de processus de transmission et de réception de sécurité (TxSPDOs ou RxSPDO).

6.1.4 Cadence (impulsions) de sécurité (SHB)

Les appareils qui mettent en œuvre le protocole FSCP 18/1 SCL utilisent le service SHB pour le contrôle des couches application et le contrôle d'application. Ce service est indépendant de tout autre service de cadence (impulsions) que les appareils pourraient mettre en œuvre de façon parallèle. Les messages SHB sont des messages cycliques confirmés échangés entre les appareils de communication et établissent par ailleurs une relation 1:1 entre les appareils. Le mécanisme SHB permet la synchronisation des horloges système des appareils de communication.

6.1.5 Contrôle de retard de sécurité (SDM)

Le service de contrôle de retard de sécurité sert à contrôler le retard des paquets dans le cadre d'une relation de communication des appareils de même nature. Ce mécanisme est basé sur une relation de service confirmée entre les appareils. Le service s'assure que le temps qui s'écoule entre l'émission de la demande de service et la réception de la confirmation du service ne dépasse pas un retard maximal configurable. De plus, le service contrôle la durée entre deux mesures abouties du retard. Cette durée ne doit pas être supérieure à une durée fonction de la configuration au cours de laquelle il serait possible que le retard dépasse le retard maximal autorisé.

6.2 Relation de communication

Le protocole FSCP 18/1 définit une relation 1:*n* avec la relation producteur/consommateur pour la communication de données de processus de sécurité. Les producteurs doivent transmettre, de manière cyclique, des objets de données de processus de sécurité identifiés par un PDO-ID unique destiné à l'identification des paquets et par un indicatif de sécurité unique destiné à l'identification du producteur. L'interaction des objets de données de processus de sécurité n'est pas confirmée. La Figure 5 illustre le modèle d'interaction des objets de données de processus de sécurité (voir ISO/IEC 10731 pour une explication de l'organigramme séquentiel).

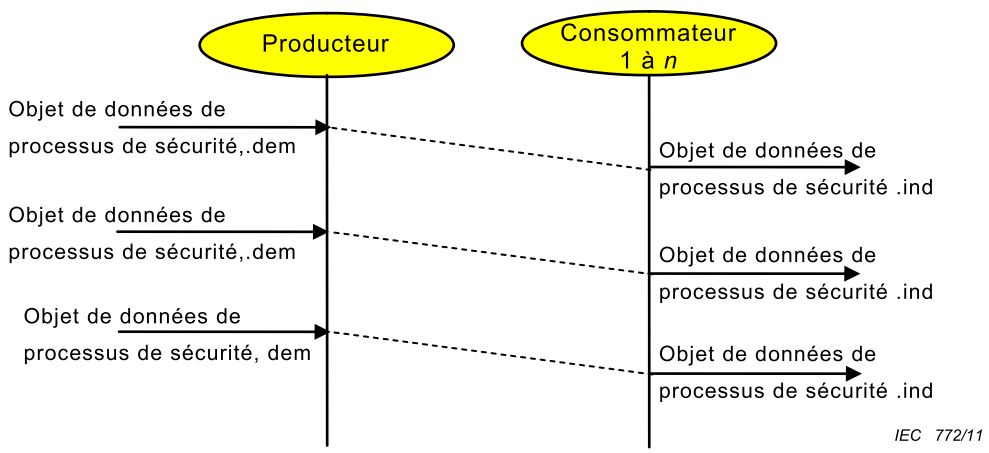


Figure 5 – Modèle d'interaction SPDO

L'état et la présence des partenaires de communication (c'est-à-dire les producteurs et les consommateurs) dans le protocole FSCP 18/1 font l'objet d'un contrôle indépendant par chaque appareil participant. Une relation de cadence (impulsions) est utilisée pour toutes les relations de communication d'un appareil dédié à un autre. Il existe ainsi une relation 1:1 entre les partenaires de communication. La communication de cadence de sécurité suit la relation client/serveur confirmée. La Figure 6 illustre les interactions de cadence (impulsions) pour une relation d'objets de données de processus de sécurité. Le temps de cycle du service de cadence (impulsions) est indépendant des autres temps de cycle de communication et

dépend du temps de réponse de la fonction de sécurité, ainsi que de l'augmentation maximale autorisée du temps de remise des messages.

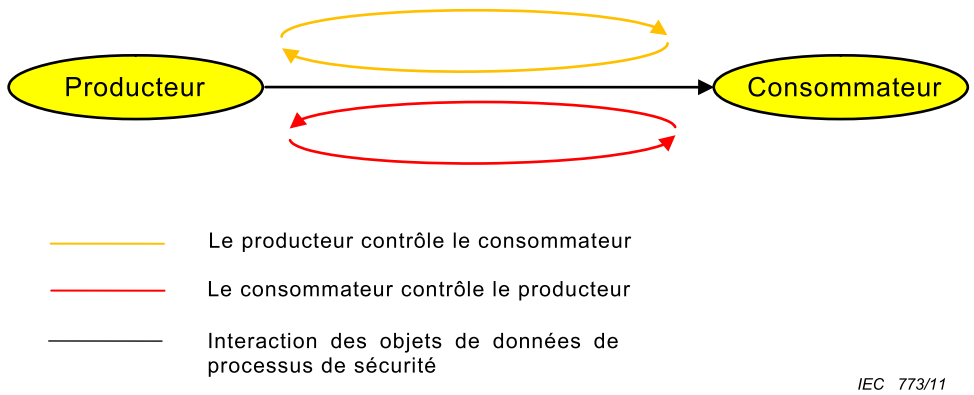


Figure 6 – Modèle d'interaction SHB

La communication de données de processus relative à la sécurité utilisant le protocole FSCP 18/1 est basée sur les deux composants essentiels suivants:

- objets de données de processus de sécurité (SPDO);
- cadence (impulsions) de sécurité (SHB).

Le cycle de communication FSCP 18/1 consiste principalement en un échange cyclique non confirmé d'objets de données de processus de sécurité. Le côté consommateur fait appel à un comportement de délai pour contrôler l'échange de données de processus de sécurité et détecter les défaillances de communication. L'application du modèle d'interaction non confirmé impose un mécanisme supplémentaire qui permet de détecter un appareil défaillant et qui permet également de détecter tout retard de remise de messages PDU accru au-delà du délai normal du consommateur. Le service de cadence (impulsions) de sécurité prend en charge cette réalisation. Les deux mécanismes combinés définissent et appliquent un cycle de communication.

7 Protocole de couche de communication de sécurité

7.1 Format PDU de sécurité

7.1.1 Généralités

7.1.1.1 Structure PDU

Un PDU de sécurité consiste soit en un objet de données de processus de sécurité (SPDO), soit en une cadence (impulsions) de sécurité (SHB). Tandis que le SPDO permet de communiquer les données d'application de sécurité, la SHB permet de synchroniser les appareils de communication.

7.1.1.2 Intégrité des données

Le récepteur d'un PDU de sécurité doit vérifier l'intégrité de sécurité des données en procédant au contrôle des deux copies de données (SPDO ou SHB) par rapport à leurs CRC, et en comparant les CRC de ces deux copies.

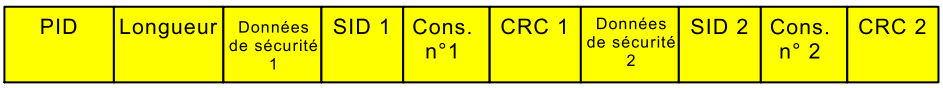
En cas de configuration avérée des répétitions de transmission, chaque réception doit alors faire l'objet d'une vérification tel que spécifié ci-dessus. La réception de la PDU de sécurité

doit être considérée comme non aboutie si toutes les répétitions n'ont pas satisfait au contrôle d'intégrité des données.

7.1.2 Objets de données de processus de sécurité (SPDO)

7.1.2.1 Structure SPDO

La Figure 7 définit la structure d'un objet de données de processus de sécurité et ses champs de données.



IEC 774/11

Figure 7 – Structure des objets de données de processus de sécurité

Le transfert des SPDO s'effectue de manière cyclique via le bus de terrain subordonné. Le contenu d'un SPDO consiste en un ou plusieurs objets d'application de sécurité parmi les objets du dictionnaire d'objets de sécurité. La mise en correspondance de l'élément du dictionnaire d'objets de sécurité avec le SPDO s'effectue par les entrées de mise en correspondance SPDO indiquées dans les Tableaux 25 et 26. Le Tableau 23 permet d'identifier l'index de la table de mise en correspondance du Tableau 26 sur la base du PID du SPDO.

La structure générale d'un SPDO est présentée dans le Tableau 4.

Tableau 4 – Structure du PDU du SPDO

Décalage d'octet	Champ de données	Description
0 à 2	PID	Indicatif de paquet
3	Longueur	Longueur du paquet complet en octets.
4 à 4+~~(~~*n*-1~~)~~	Données de sécurité 1	Données de processus d'application de sécurité mises en correspondance
4+*n* à 5+*n*	SID 1	ID de sécurité de l'émetteur
6+*n* à 6+*n*+*m*-1	numéro consécutif 1	Numéro consécutif pour ordonnancement et contrôle d'application, où : *m* = 1 pour la version 1 du protocole *m* = 3 pour la version 2 du protocole
7+*n*+*m* à 10+*n*+*m*	CRC 1	Contrôle de redondance cyclique de 32 bits couvrant les champs de données PID, ~~longueur,~~ données de sécurité 1, SID 1 et numéro consécutif 1
11+*n*+*m* à 11+2~~(~~*n*-1~~)~~+*m*	Données de sécurité 2	Copie des données de processus d'application de sécurité mises en correspondance
11+2*n*+*m* à 12+2*n*+*m*	SID 2	Copie de SID 1
13+2*n*+*m* à 13+2*n*+2*m*-1	Numéro consécutif 2	Copie du numéro consécutif 1
14+2*n*+2*m* à 17+2*n*+2*m*	CRC 2	Contrôle de redondance cyclique de 32 bits couvrant les champs de données PID, ~~longueur,~~ données de sécurité 2, SID 2 et numéro consécutif 2
NOTE 1 *n* est la longueur en octets du champ de données « données de sécurité 1 » (« données de sécurité 2 »). NOTE 2 *m* est la longueur du nombre consécutif en fonction de la version du protocole (voir 7.1.3.4).		

7.1.2.2 PID du SPDO

Ce champ de données constitue un numéro d'identification du paquet qui, associé au champ SID, identifie de manière unique le paquet.

7.1.2.3 Longueur du SPDO

Ce champ de données doit contenir la longueur en octet du paquet complet.

7.1.2.4 Données de sécurité

Ce champ de données doit contenir les objets d'application de sécurité selon la configuration de mise en correspondance.

Le nombre de données est limité de 0 à 115 octets pour la version 2 du protocole ou respectivement 117 octets pour la version 1 du protocole afin de permettre la transmission du PDU de sécurité via un canal noir dont les caractéristiques de transfert ne sont pas prises en compte dans les considérations de sécurité. Le taux d'erreur résiduelle par heure ne dépasse pas $10^{-9,}$ tel que démontré en 9.5.2, pour le système d'assurance d'intégrité des données.

7.1.2.5 SID du SPDO

Ce champ de données est un identifiant de 16 bits de l'émetteur. Cette valeur doit être unique sur tout le réseau. Chaque appareil FSCP 18/1 participant obtient un SID. Le SID d'un appareil est enregistré dans l'entrée du dictionnaire d'objets de sécurité correspondant avec l'index 0x1200. Le SID ne doit pas être égal à 0. Le numéro est généré par l'outil de configuration de réseau qui doit garantir le caractère unique du SID du SPDO.

7.1.2.6 Numéro consécutif du SPDO

Ce champ de données est un numéro consécutif ~~de 8 bits~~ (compteur cyclique) pour le contrôle du signe du cycle de vie et l'ordonnancement des paquets de la couche application. Ce numéro est généré par l'émetteur du SPDO. La taille du numéro consécutif dépend de la version du protocole (voir 7.1.3.4) et elle est de 1 octet pour la version 1 du protocole et de 3 octets pour la version 2 du protocole.

7.1.2.7 CRC du SPDO

Ce champ de données contient le CRC de 32 bits couvrant les champs de données « PID », ~~« longueur »,~~ « données », « SID » et « numéro consécutif».

Le polynôme 0x20044009 est utilisé pour calculer les CRC. Pour de plus amples informations, voir 7.1.2.4 et 9.5.2.

7.1.3 Cadence (impulsions) de sécurité (SHB)

7.1.3.1 Structure SHB

7.1.3.1.1 PDU de demande SHB

La Figure 8 illustre la structure du PDU d'une demande de cadence (impulsions) de sécurité.

PID	Longueur	SCL état 1	AP de sécurité état 1	SID 1	Cons. n°1	CRC 1	SCL état 2	AP de sécurité état 2	SID 2	Cons. n°2	CRC 2

IEC 775/11

Figure 8 – Structure de demande de cadence (impulsions) de sécurité

Le Tableau 5 répertorie la structure générale du PDU.

Tableau 5 – Structure du PDU de demande SHB

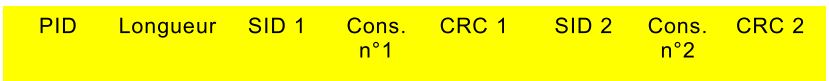
Décalage d'octet	Champ de données	Description
0 à 2	PID	Indicatif de paquet
3	Longueur	Longueur du paquet complet en octets
4	Etat 1 de la SCL	Etat SALMT (voir Tableau 7)
~~5 à 6+(*n*-1)~~ 5 à 5+*n*-1	Etat 1 du processus d'application de sécurité	Etat du processus d'application de sécurité (spécifique à la mise en œuvre)
6+*n* à 7+*n*	SID 1	ID de sécurité de l'émetteur
8+*n* à 8+*n*+*m*-1	Numéro consécutif 1	Numéro consécutif pour ordonnancement et contrôle d'application où : *m* = 1 pour la version 1 du protocole *m* = 3 pour la version 2 du protocole
9+*n*+*m* à 12+*n*+*m*	CRC 1	Contrôle de redondance cyclique de 32 bits couvrant les champs de données PID, ~~longueur,~~ état 1 de la SCL, état 1 du processus d'application de sécurité, SID 1 et numéro consécutif 1
13+*n*+*m*	Etat 2 de la SCL	Copie de l'état 1 de SALMT
~~14 à 15+(*n*-1)~~ 14+*n*+*m* to 14+2*n*+*m*-1	Etat 2 du processus d'application de sécurité	Copie de l'état 1 du processus d'application de sécurité
15+2*n*+*m* à 16+2*n*+*m*	SID 2	Copie de SID 1
17+2*n*+*m* à 17+2*n*+2*m*-1	Numéro consécutif 2	Copie du numéro consécutif 1
18+2*n*+2*m* à 21+2*n*+2*m*	CRC 2	Contrôle de redondance cyclique de 32 bits couvrant les champs de données PID, ~~longueur,~~ état 2 de la SCL, état 2 du processus d'application de sécurité, SID 2 et numéro consécutif 2

NOTE 1 *n* est la longueur en octets du champ de données « Etat du processus d'application de sécurité ».

NOTE 2 *m* est la longueur du numéro consécutif, en fonction de la version du protocole (voir 7.1.3.4)

7.1.3.1.2 PDU de réponse de SHB

La Figure 9 illustre la structure du PDU d'une réponse de cadence (impulsions) de sécurité.



IEC 776/11

Figure 9 – Structure de réponse de cadence (impulsions) de sécurité

Le Tableau 6 répertorie la structure générale de ce PDU.

Tableau 6 – Structure du PDU de réponse SHB

Décalage d'octet	Champ de données	Description
0 à 2	PID	Indicatif de paquet
3	Longueur	Longueur du paquet complet en octets
4 à 5	SID 1	ID de sécurité de l'émetteur
6 à 6+*m*-1	Numéro consécutif 1	Numéro consécutif pour ordonnancement et contrôle d'application où : *m* = 1 pour la version 1 du protocole *m* = 3 pour la version 2 du protocole
7+*m* à 10+*m*	CRC 1	Contrôle de redondance cyclique de 32 bits couvrant les champs de données PID, ~~longueur,~~ SID 1 et numéro consécutif 1
11+*m* à 12+*m*	SID 2	Copie de SID 1
13+*m* à 13+2*m*-1	Numéro consécutif 2	Copie du numéro consécutif 1
14+2*m* à 17+2*m*	CRC 2	Contrôle de redondance cyclique de 32 bits couvrant les champs de données PID, ~~longueur,~~ SID 2 et numéro consécutif 2
NOTE *m* est la longueur du numéro consécutif, en fonction de la version du protocole (voir 7.1.3.4).		

7.1.3.2 PID de SHB

Ce champ de données constitue un numéro d'identification du paquet qui, associé au champ SID, identifie de manière unique le paquet.

7.1.3.3 Longueur SHB

Ce champ de données doit contenir la longueur en octet du paquet complet.

7.1.3.4 Etat de la couche de communication de sécurité SHB

Ce champ de données doit contenir les informations d'état concernant la SCL. Ces informations sont interprétées par les récepteurs SHB. Le Tableau 7 spécifie le codage du contenu de ce champ de données.

Tableau 7 – Codage de l'état de la couche de communication de sécurité SHB

Valeur	Description	Protocole
0x00	FS FAL est à l'état BOOTUP	Version 1
0x04	FS FAL est à l'état STOPPED	Version 1
0x05	FS FAL est à l'état OPERATIONAL	Version 1
0x7F	FS FAL est à l'état PRE-OPERATIONAL	Version 1
0x10	FS FAL est à l'état BOOTUP	Version 2
0x14	FS FAL est à l'état STOPPED	Version 2
0x15	FS FAL est à l'état OPERATIONAL	Version 2
0x1F	FS FAL est à l'état PRE-OPERATIONAL	Version 2

L'appareil doit prendre en charge au moins une version du protocole. L'état FS FAL doit être codé conformément au Tableau 7 en fonction de la version du protocole utilisée. Il est recommandé qu'il prenne en charge toutes les versions du protocole.

7.1.3.5 Etat du processus d'application de sécurité SHB

Ce champ de données doit contenir les informations d'état concernant l'application de sécurité. Le contenu et le codage de ce champ de données dépendent de l'application et ne relèvent pas du domaine d'application de la présente norme internationale. La longueur est limitée de 0 à 114 octets pour la version 2 du protocole ou respectivement 116 octets pour la version 1 du protocole.

7.1.3.6 SID de SHB

Ce champ de données est l'indicatif de 16 bits de l'émetteur. Cette valeur doit être unique sur tout le réseau. Chaque appareil FSCP 18/1 participant obtient un SID. Le SID d'un appareil est enregistré dans l'entrée du dictionnaire d'objets de sécurité correspondant avec l'index 0x1200. Le SID ne doit pas être égal à 0. Le numéro est généré par l'outil de configuration de réseau qui doit garantir le caractère unique du SID de SHB.

7.1.3.7 Numéro consécutif de SHB

Ce champ de données est un numéro consécutif ~~de 8 bits~~ (compteur cyclique) pour le contrôle du signe de vie et l'ordonnancement des paquets de la couche application. Dans le cas d'un PDU de réponse, ce champ de données contient le numéro consécutif du PDU confirmé par cette réponse. Ce numéro est généré par l'émetteur de la SHB. La taille du numéro consécutif dépend de la version du protocole (voir 7.1.3.4) et elle est de 1 octet pour la version 1 du protocole et de 3 octets pour la version 2 du protocole.

7.1.3.8 CRC de SHB

Ce champ de données contient le CRC de 32 bits couvrant les champs de données « PID », ~~« longueur »,~~ « données », « SID » et « numéro consécutif».

Le polynôme 0x20044009 est utilisé pour calculer les CRC. Pour de plus amples informations, voir 7.1.3.5 et 9.5.2.

7.1.4 PDU de sécurité intégrées dans un PDU de type 22

La Figure 10 illustre la structure d'un PDU de sécurité FSCP 18/1 intégrée dans un DLPDU CDC de type 22. La présence de renseignements d'en-tête IP et UDP dépend du profil de communication utilisé. Pour de plus amples informations concernant le DLPDU de type 22, se reporter à l'IEC 61158-4-22.

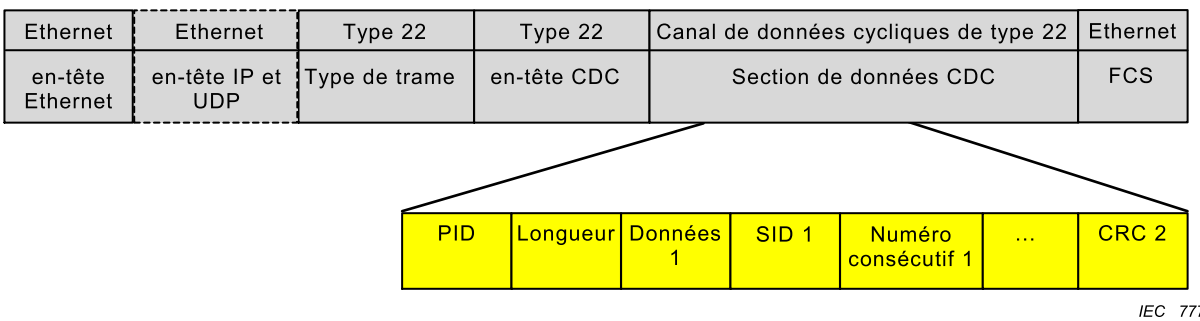


Figure 10 – PDU de sécurité pour le protocole FSCP 18/1 intégrée dans une section de données CDC de type 22

7.2 Gestion de la couche de communication de sécurité (SALMT)

Le service SALMT local permet de déclencher l'automate fini de la SCL, et ainsi de contrôler le comportement de la partie sécurité d'un appareil.

Les commandes SALMT spécifiées dans le Tableau 8 sont disponibles.

Tableau 8 – Commandes SALMT

Commande	Description
0x01	Initialisation de la communication
0x02	Initialisation de nœud
0x03	Arrêt de nœud distant
0x04	Démarrage de nœud distant
0x05	Saisie état pré-opérationnel

La Figure 11 illustre le diagramme d'états SALMT. Tous les états du diagramme d'états doivent être pris en charge.

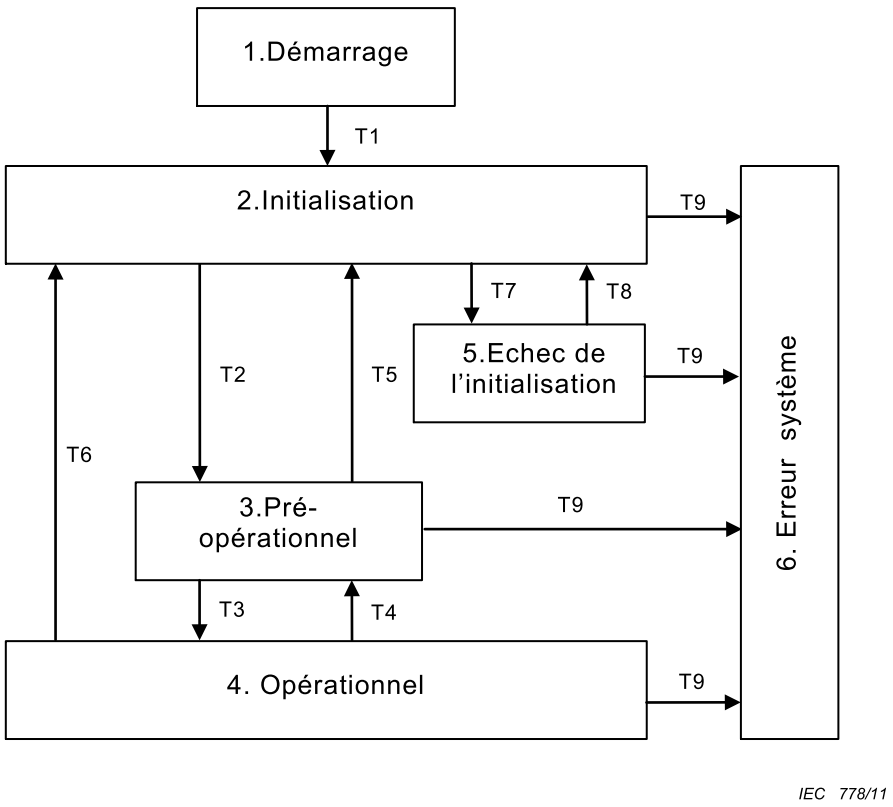


Figure 11 – Diagramme d'états SALMT

Les commandes de gestion locale sont associées aux transitions et états du diagramme d'états SALMT, tels que spécifiés dans les Tableaux 9 et 10.

Tableau 9 – Etats du diagramme d'états SALMT

Numéro d'état	Etat	Description
1	Démarrage	Etat virtuel après démarrage de l'appareil. L'émission et la réception des PDU SPDO et SHB ne sont pas admises.
2	Initialisation	Initialisation fonction du système. L'émission et la réception des PDU SPDO et SHB ne sont pas admises.
3	Pré-opérationnel	Exécution de la configuration ou attente de la demande par le système pour initialiser l'état opérationnel. L'émission et la réception des PDU SHB sont admises. Les PDU SPDO ne sont pas admises.
4	Opérationnel	Etat opérationnel. L'émission et la réception des PDU SPDO et SHB sont admises.
5	Echec de l'initialisation	Occurrence d'une erreur non relative à la sécurité pendant l'initialisation. L'émission et la réception des PDU SHB sont admises. Les PDU SPDO ne sont pas admises.
6	Erreur système	Détection d'une erreur relative à la sécurité. L'émission et la réception des PDU SPDO et SHB ne sont pas admises.

Tableau 10 – Transitions du diagramme d'états SALMT

Transition d'état	Numéro d'état d'origine	Numéro d'état destinataire	Description	Action
T1	1	2	Transition automatique après démarrage de l'appareil	Désactiver l'émission et la réception des PDU SPDO et SHB
T2	2	3	Transition déclenchée par la commande SALMT entrée dans l'état « Pré-opérationnel »	Activer l'émission et la réception des PDU SHB. Désactiver l'émission et la réception des PDU SPDO
T3	3	4	Transition déclenchée par la commande SALMT, démarrage du nœud distant	Activer l'émission et la réception des PDU SPDO et SHB
T4	4	3	Transition déclenchée par la commande SALMT, arrêt du nœud distant	Activer l'émission et la réception des PDU SHB. Désactiver l'émission et la réception des PDU SPDO
T5	3	2	Transition déclenchée par la commande SALMT, initialisation de nœud ou initialisation de la communication	Désactiver l'émission et la réception des PDU SPDO et SHB
T6	4	2	Transition déclenchée par la commande SALMT, initialisation de nœud ou initialisation de la communication	Désactiver l'émission et la réception des PDU SPDO et SHB
T7	2	5	Transition déclenchée par une défaillance ou une panne pendant l'initialisation	Activer l'émission et la réception des PDU SHB. Désactiver l'émission et la réception des PDU SPDO
T8	5	2	Transition déclenchée par la commande SALMT, initialisation de nœud	Désactiver l'émission et la réception des PDU SPDO et SHB
T9	2 3, 4 ou 5	6	Transition déclenchée par une erreur système	Désactiver l'émission et la réception des PDU SPDO et SHB

7.3 Communication de données de processus de sécurité

La communication de données de processus de sécurité est basée sur une relation 1:*n* du type relation producteur/consommateur. Aucun message de confirmation n'est utilisé. Les relations de communication sont configurées au cours de la phase de configuration du système. Aucune autre gestion de connexion en ligne n'est prévue.

Le côté consommateur fait appel à un comportement de délai pour contrôler l'échange de données de processus de sécurité et détecter les défaillances de communication. Le temps de cycle SPDO est contrôlé à l'aide d'un mécanisme de temporisation approprié. De plus, le producteur et le consommateur contrôlent le retard des paquets afin d'identifier toute augmentation inacceptable.

La Figure 12 illustre le diagramme d'états RxSPDO. Le diagramme d'états est appliqué pour chaque RxSPDO configuré. Tous les états doivent être pris en charge.

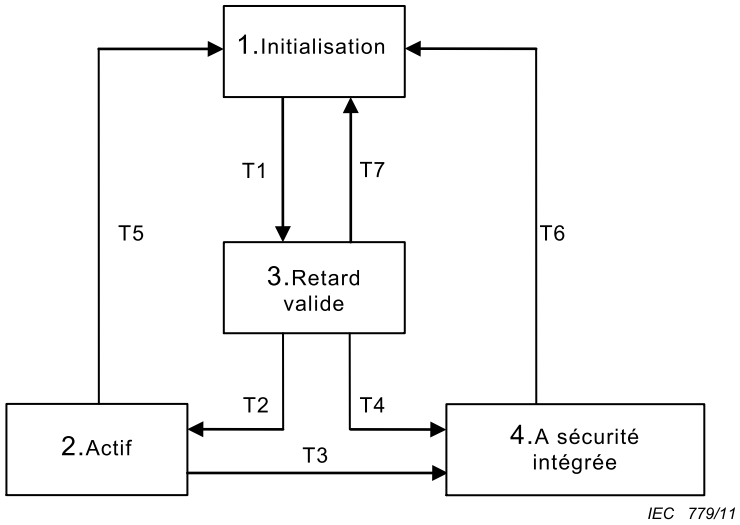


Figure 12 – Diagramme d'états RxSPDO

Les Tableaux 11 à 13 décrivent les transitions d'état et les événements et actions associés.

Tableau 11 – Etats du diagramme d'états RxSPDO

Numéro d'état	Transition d'état	Description
1	Initialisation	Démarrage ou temporisation SHB (aucune temporisation RxSPDO) en état non « Actif ». Aucune donnée générée
2	Actif	Réception RxSPDO et mesure de retard valide. Production de données. Etat SALMT « Opérationnel »
3	Retard valide	Mesure de retard satisfaisante, connexion avec le partenaire de communication dans les délais spécifiés, RxSPDO non « Actif » dans la mesure où aucun SPDO n'a encore été reçu. Aucune donnée n'est générée
4	A sécurité intégrée	Temporisation de RxSPDO ou SHB en état RxSPDO « Actif ». Mise à zéro et production unique des données. Réactivation admise uniquement par transition SALMT

Tableau 12 – Transitions du diagramme d'état RxSPDO

Transition d'état	Numéro d'état d'origine	Numéro d'état destinataire	Description	Action
T1	1	3	Pour les états SALMT « Pré-opérationnel » et « Opérationnel » si la mesure de retard (SHB) était satisfaisante	Aucune
T2	3	2	Pour l'état SALMT « Opérationnel » si réception de RxSPDO	Démarrage de la production de données et réglage de SALMT sur « Opérationnel »
T3	2	4	Pour l'état SALMT « Opérationnel » si la mesure de retard (SHB) n'est pas satisfaisante ou temporisation de RxSPDO. ou Echec du contrôle d'intégrité de sécurité de la PDU reçue (voir 7.1.1.2)	Mise à zéro et production unique des données. Puis arrêt de la production de données

Transition d'état	Numéro d'état d'origine	Numéro d'état destinataire	Description	Action
T4	3	4	Pour l'état SALMT « Opérationnel » si la mesure de retard (SHB) n'est pas satisfaisante (expiration de la temporisation SHB sans réponse du partenaire de communication à la SHB) ou Echec du contrôle d'intégrité de sécurité de la PDU reçue. (Voir 7.1.1.2)	Mise à zéro et production unique des données. Puis arrêt de la production de données
T5, T6, T7	2,3 ou 4	1	Sur changement de l'état SALMT d'« Opérationnel » en « Pré-opérationnel »	Arrêt de la production de données

Tableau 13 – Temporisations

Temporisation	Description
RxSPDO	Temporisation RxSPDO si aucun SPDO n'a été reçu après configuration du nombre de cycles multiplicateurs de temporisation
Réponse attendue SHB	Temporisation de la réponse attendue SHB si aucune réponse n'a été reçue au cours de la période de configuration après l'envoi d'un message SHB
Consommateur SHB	Temporisation du consommateur SHB si aucune SHB n'a été émise par le consommateur pendant la configuration du nombre de cycles multiplicateurs de temporisation
Temporisation SHB	Temporisation de la réponse attendue SHB ou du consommateur SHB

Plusieurs copies d'une PDU SPDO peuvent être transmises par un émetteur afin d'améliorer la disponibilité du service. Ce comportement dépend de la configuration du service. Le récepteur contrôle le nombre de copies d'un SPDO reçues. La réception d'un trop grand nombre de copies entraîne la transition vers l'état « erreur système » afin de signifier une configuration défectueuse du réseau. Le mécanisme de temporisation du récepteur n'est pas influencé par la réception de plusieurs copies. Le mécanisme est déclenché par le premier PDU reçu.

7.4 Cadence (impulsions) de sécurité

Les appareils de mise en oeuvre d'une SCL doivent prendre en charge la cadence (impulsions) de sécurité. Ce mécanisme de cadence (impulsions) est indépendant des messages de cadence (impulsions) CP 18/1 et CP 18/2 et doit faire l'objet d'une configuration indépendante.

Les messages de cadence (impulsions) de sécurité sont transmis tel que spécifié à la Figure 13. Chaque message de cadence (impulsions) contient l'état de la SCL et le processus d'application de sécurité.

La procédure de cadence (impulsions) est illustrée à la Figure 13.

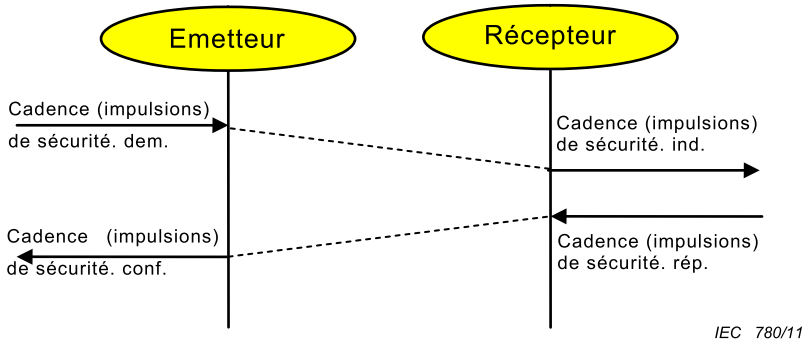


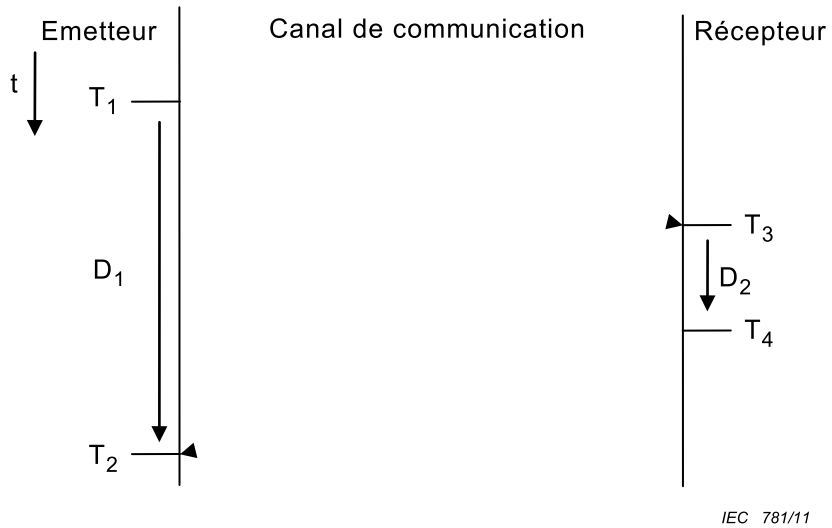
Figure 13 – Procédure de cadence (impulsions)

7.5 Contrôle de retard

La procédure de mesure de retard doit être exécutée par l'ensemble des appareils de mesure afin de déterminer le retard réel de remise des PDU, et ainsi de déterminer la validité des informations reçues.

Le service de cadence (impulsions) de sécurité permet de contrôler le retard des paquets. Le récepteur accuse réception de chaque PDU de cadence (impulsions) de sécurité. L'émetteur contrôle le temps qui s'écoule entre la génération de la demande de cadence (impulsions) et la réception de la réponse. Cette durée ne doit pas dépasser un retard maximal configuré.

La Figure 14 illustre le principe général de mesure du retard observé au niveau de l'émetteur et du récepteur.



T_x Point au temps x

D_x Retard résultant

Figure 14 – Principe de mesure du retard

Les appareils d'émission déterminent les temps T_1 et T_2. Les temps D_2, T_3 et T_4 ne font l'objet d'aucune analyse ultérieure. L'émetteur des PDU de demande de cadence (impulsions) doit, sur la base de ces informations, déterminer une estimation du retard de remise des paquets. Le résultat du contrôle de retard doit être comparé à une valeur de seuil configurée. Lorsque l'augmentation du retard déterminé est supérieure à la valeur de seuil configurée, la SCL doit déclencher une transition vers l'état SPDO « A sécurité intégrée » et l'application doit passer à l'état de sécurité.

La détermination de la fréquence de répétition applicable à la procédure de contrôle de retard (c'est-à-dire le temps de cycle SHB) doit être déduite du retard maximal autorisé (fonction du temps de réponse de la fonction de sécurité), du retard réel et des temps de cycle SPDO configurés.

De plus, l'émetteur contrôle la durée entre deux mesures du retard satisfaisantes. Cette durée ne doit pas être supérieure à la durée au cours de laquelle il est possible que le retard soit supérieur au seuil de retard configuré.

La durée maximale qui s'écoule jusqu'à la mesure suivante du retard est calculée selon l'Equation (1).

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

où

T_{Max} Temps maximal autorisé jusqu'à la mesure suivante du retard;

D_{Max} Retard maximal autorisé;

D_{Act} Retard réel (selon la dernière mesure du retard);

T_{Timer} Tolérance relative du temporisateur avec $0{,}000\,1 \leq T_{Timer} \leq 0{,}1$;

T_{TO} Tolérance configurable pour la temporisation RxSPDO, index 0x121E selon le Tableau 15 avec $0{,}01 \leq T_{TO} \leq 1$:

8 Gestion de la couche de communication de sécurité

8.1 Traitement des paramètres

La configuration des paramètres des appareils PFSCP 18/1 fait partie intégrante de la configuration de l'application de sécurité. Tous les paramètres relatifs à la sécurité sont téléchargés sur l'appareil à l'aide d'un outil de configuration approprié. Le mécanisme de téléchargement des paramètres ne relève pas du domaine d'application de la présente norme internationale et dépend de l'application de sécurité. La Figure 15 illustre la séquence de configuration des appareils.

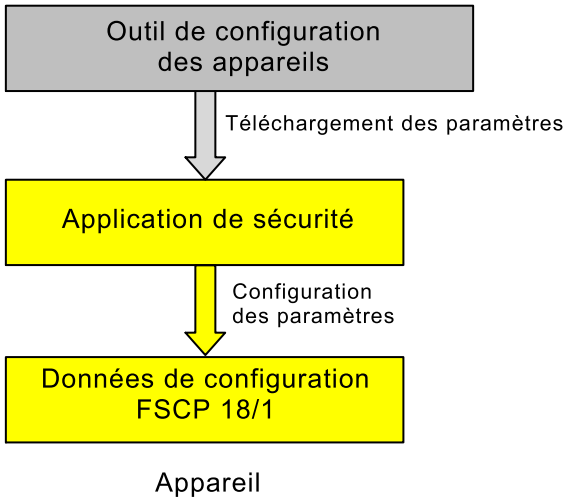


Figure 15 – Traitement des paramètres

8.2 Dictionnaire d'objets de sécurité

8.2.1 Généralités

Le dictionnaire d'objets de sécurité utilise la même structure que le dictionnaire d'objets employé dans les protocoles CP 18/1 et CP 18/2. Il contient les espaces objets énumérés dans le Tableau 14.

Tableau 14 – Structure du dictionnaire d'objets de sécurité

Index	Section	Sous-section	Contenu
0x0001 à 0x001F	Type de données	Types de données de base	Définition des types de données de base
0x0020 à 0x003F	—	Types de données complexes	Définition des types de données complexes
0x0040 à 0x005F	—	Types de données spécifiques au fabricant	Définition des types de données spécifiques au fabricant
0x0060 à 0x007F	—	Types de données de base spécifiques au profil de l'appareil	Définition des types de données de base spécifiques au profil de l'appareil
0x0080 à 0x009F	—	Types de données complexes spécifiques au profil de l'appareil	Définition des types de données complexes spécifiques au profil de l'appareil
0x00A0 à 0x0FFF	Réservé	—	—
0x1000 à 0x1FFF	Profil de communication	—	Définition des paramètres utilisés à des fins de configuration de communication et de communication dédiée
0x2000 à 0x5FFF	Profil défini par le fabricant	—	Définition des paramètres spécifiques au fabricant
0x6000 à 0x9FFF	Profil de l'appareil normalisé	—	Définition des paramètres définis dans un profil de l'appareil normalisé
0xA000 à 0xBFFF	Profil d'interface normalisée	—	Définition des paramètres spécifiés dans un profil d'interface normalisée
0xC000 à 0xC8FF	Profil d'interface CP 18/2	—	Définition des paramètres spécifiés dans un profil d'interface CP 18/2
0xC900 à 0xFFFF	Réservé	—	—

8.2.2 Section de profil de communication

8.2.2.1 Généralités

Les objets associés à l'application de sécurité énumérés dans le Tableau 15 doivent être pris en charge.

Tableau 15 – Objets de la section de communication

Index	Objet	Nom	Type de données	Attribut	Description	Catégorie
0x1000	VAR	Type d'appareil	Unsigned32	RO	Classification de l'appareil: 16 bits de poids faible correspondent au « Numéro de profil de l'appareil », décrivant le profil utilisé. 16 bits de poids fort correspondent aux « Informations supplémentaires ».	M
0x1200	VAR	Indicatif de sécurité	Unsigned16	FSF	Indicatif unique de l'appareil de sécurité, ne doit pas être égal à zéro	M/O
0x1216	ARRAY	Liste de cadence (impulsions) du consommateur de sécurité	Unsigned256	FSF	Liste des appareils distants qui doivent être contrôlés par l'appareil.	M/O
0x1217	RECORD	Paramètre de cadence (impulsions) du producteur de sécurité	PDO COM_PAR	FSF	Même configuration que la transmission SPDO. Doit être configurée comme la transmission cyclique.	M/O
0x1218	ARRAY	Temps de cycle de bus de sécurité	Unsigned32	FSF	Sous-index 0: nombre d'entrées Sous-index 1: Temps de cycle de base RTFN Sous-index 2: Temps de cycle de base RTFL	M/O
0x121B vers 0x121D	Réservé pour d'autres paramètres de sécurité					
0x121E	VAR	Tolérance T_{TO} de temporisation SPDO	Unsigned8	FSF	Définit le niveau de dépassement de temporisation RxSPDO acceptable. Nombre sans unité, interprété en pourcentage.	M/O
0x121F vers 0x127F	Réservé pour d'autres paramètres de sécurité					
0x1C00 vers 0x1CFF	RECORD	Paramètre de communication RxSPDO	PDO COM_PAR	FSF		M/O
0x1D00 vers 0x1DFF	RECORD	Paramètre de mise en correspondance RxSPDO	Mise en correspondance PDO	FSF		M/O

Index	Objet	Nom	Type de données	Attribut	Description	Catégorie
0x1E00 vers 0x1EFF	RECORD	Paramètre de communication TxSPDO	PDO COM_PAR	FSF		M/O
0x1F00 vers 0x1FFF	RECORD	Paramètre de mise en correspondance TxSPDO	Mise en correspondance PDO	FSF		M/O

8.2.2.2 Type d'appareil

L'objet de type d'appareil indique le profil de l'appareil mis en œuvre, ainsi que sa fonction, et est spécifié dans le Tableau 16. Il comprend deux champs de 16 bits. Le premier champ est le numéro de profil de l'appareil, qui décrit le profil de l'appareil employé. Le second champ de 16 bits fournit des informations supplémentaires concernant les fonctions de l'appareil facultatives et fait partie intégrante du profil de l'appareil ou de la spécification du produit. La valeur 0x0000 désigne un appareil qui ne suit pas un profil normalisé. Pour les modules d'appareils multiples, le paramètre d'informations supplémentaires contient 0xFFFF et le numéro de profil d'appareil référencé par l'objet 0x1000 est le profil du premier appareil dans le dictionnaire d'objets de sécurité. Tous les autres appareils d'un module d'appareil multiple identifient leurs profils aux objets 0x67FF + (N x 0x800) avec N = numéro interne de l'appareil (compris entre 0 et 7). Ces entrées décrivent le type d'appareil de l'appareil précédent. Les appareils utilisent des numéros de profil compris entre quatre et sept pour les fonctions de sécurité, de sorte que les premiers objets d'application de sécurité commencent à 0x8000.

Tableau 16 – Type d'appareil

Attribut	Valeur
Index	0x1000
Nom	Type d'appareil
Description	Classification des appareils conforme à CANopen. D'autres informations sont données en [47]
Type d'objet	VAR
Type de données	Unsigned32
Catégorie	Obligatoire
Attribut d'accès	RO
Mise en correspondance PDO	Non
Plage de valeurs	Non
Valeur	Bits 0 à 15: Numéro de profil de l'appareil Bits 16 à 31: Information supplémentaire selon le profil d'appareil employé

8.2.2.3 Indicatif de sécurité (SID)

L'objet d'indicatif de sécurité est spécifié dans le Tableau 17. L'objet spécifie l'indicatif de sécurité d'un appareil de même nature. Il est obligatoire pour les appareils de sécurité.

Tableau 17 – Indicatif de sécurité

Attribut	Valeur
Index	0x1200
Nom	Indicatif de sécurité
Description	Indicatif unique de l'appareil
Type d'objet	VAR
Type de données	Unsigned16
Catégorie	Obligatoire
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	0x0001 à 0xFFFF
Valeur	Non

8.2.2.4 Liste de cadence (impulsions) du consommateur de sécurité

L'objet de cadence (impulsions) du consommateur de sécurité est spécifié dans le Tableau 19. La cadence (impulsions) du consommateur de sécurité définit tous les appareils de sécurité que l'appareil concerné doit contrôler. De plus, les paramètres des réponses de cadence (impulsions) sont configurés, ainsi que les paramètres relatifs aux réponses attendues. Le codage d'une entrée de cadence (impulsions) d'un consommateur de sécurité dans les limites d'une valeur OCTET_STRING est spécifié dans le Tableau 18.

Tableau 18 – Entrée de cadence (impulsions) d'un consommateur de sécurité

Octet	Type de données	Signification
0 à 3	Unsigned32	Adresse IPv4 du partenaire de communication. Pour le consommateur de cadence (impulsions) et la réponse attendue
4 à 19	Unsigned128	Adresse IPv6 du partenaire de communication. Pour le consommateur de cadence (impulsions) et la réponse attendue
20 à 21	Unsigned16	Le SID du partenaire de communication est l'indicatif unique de l'appareil. Pour le consommateur de cadence (impulsions) et la réponse attendue
22	Unsigned8	Type de transmission Pour le consommateur de cadence (impulsions), la réponse attendue et la réponse propre Description: Bit 7 (bit le plus significatif): Activation 0, non actif; 1 actif. Bits 6,5: Canal de communication 00 pour CDCL; 01 pour CDCN; 10 Réservé pour une utilisation future; 11 Réservé pour une utilisation future. Bit 4: Acheminé par une passerelle CP 18/1 – CP 18/2. 0 par défaut – aucune passerelle existante, 1 pour la passerelle. Ne doit pas être réglé pour PDO/cadence (impulsions) lorsque le canal de transmission est CDCN. Bit 3: Type de trame 0 pour la trame MAC, est utilisé uniquement pour RxSPDO sur le CDCN 1 pour la trame UDP. Bits 2,1,0 (bits les moins significatifs): Mode de transmission 001: Cyclique, autre: Réservé pour une utilisation future.

Octet	Type de données	Signification
23	Unsigned8	Réservé
24 à 27	Unsigned32	Le PID de cadence (impulsions) consommée est l'indicatif des paquets, utilisé pour vérifier l'émetteur approprié Pour le consommateur de cadence (impulsions)
28 à 29	Unsigned16	La temporisation de cadence (impulsions) spécifie le nombre de fréquences d'occurrence d'une cadence produite par le partenaire de communication. Les valeurs admises sont des multiples entiers du temps de cycle de base. Pour le consommateur de cadence (impulsions)
30 à 31	Unsigned16	Le multiplicateur de cycles pour la cadence (impulsions) consommée est obligatoire pour les réseaux comportant les passerelles CP 18/1 à CP 18/2. Il précise la fréquence d'écriture potentielle de la SPDU dans le canal de communication CDCL par la passerelle CDCN/CDCL. Pour le consommateur de cadence (impulsions) Valeurs admises: 0x0001, 0x0002, 0x0004, 0x0008, 0x0010, 0x0020, 0x0040, 0x0080, 0x0100, 0x0200, 0x0400, 0x0800, 0x1000, 0x2000, 0x4000, 0x8000
32 à 33	Unsigned16	Le décalage de cycle pour la cadence (impulsions) consommée est obligatoire pour les réseaux comportant les passerelles CP18/1 à CP 18/2. Il spécifie le décalage de la SPDU lors d'une transmission sur la CDCL. Pour le consommateur de cadence (impulsions) La plage valide est comprise entre 0 et (multiplicateur de cycles – 1)
34	Unsigned8	Le numéro de seuil de réception spécifie le nombre maximal de réceptions acceptable du même paquet. Pour le consommateur de cadence (impulsions)
35	Unsigned8	Réservé
36 à 39	Unsigned32	Le PID de la réponse attendue est l'indicatif des paquets, utilisé pour vérifier l'émetteur approprié Pour la réponse attendue
40 à 41	Unsigned16	Multiplicateur de cycles de la réponse attendue pour les réseaux comportant les passerelles CP18/1 à CP18/2. Pour la réponse attendue
42 à 43	Unsigned16	Décalage de cycle de la réponse attendue pour les réseaux comportant les passerelles CP18/1 à CP 18/2. Pour la réponse attendue
44 à 47	Unsigned32	PID de la réponse transmise. Pour la réponse propre
48 à 49	Unsigned16	Multiplicateur de cycles de la réponse transmise. Pour la réponse propre. Valeurs admises: 0x0001, 0x0002, 0x0004, 0x0008, 0x0010, 0x0020, 0x0040, 0x0080, 0x0100, 0x0200, 0x0400, 0x0800, 0x1000, 0x2000, 0x4000, 0x8000
50 à 51	Unsigned16	Décalage de cycles de la réponse transmise utilisé pour la CDCL uniquement. Pour la réponse propre. Plage 0 à (multiplicateur de cycles – 1)
52 à 55	Unsigned32	Retard maximal acceptable en µs de la réponse attendue, de l'envoi de la cadence (impulsions) à la réception de la réponse. Pour la réponse attendue
56	Unsigned8	Nombre d'envois de la réponse transmise. Pour la réponse propre
57	Unsigned8	Réservé

Tableau 19 – Cadence (impulsions) du consommateur de sécurité

Attribut	Valeur
Index	0x1216
Nom	Liste de la cadence (impulsions) du consommateur de sécurité
Type d'objet	ARRAY
Type de données	OCTET_STRING
Catégorie	Facultatif
Sous-index	0x00
Nom	Nombre d'entrées prises en charge
Description	Nombre de cadences (impulsions) de consommation (une pour chaque partenaire de communication)
Type de données	Unsigned8
Catégorie	Obligatoire
Attribut d'accès	RO
Mise en correspondance SPDO	Non
Plage de valeurs	0x01 à 0xFF
Valeur	Non
Sous-index	0x01
Nom	Cadence (impulsions) du consommateur
Description	Il doit y avoir au moins un partenaire de communication, une entrée est par conséquent obligatoire. Format décrit dans le Tableau 18
Type de données	OCTET_STRING
Catégorie	Obligatoire
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	Non
Valeur	Non
Sous-index	0x02 à 0xFE
Nom	Cadence (impulsions) du consommateur
Description	Entrées supplémentaires. Format décrit dans le Tableau 18
Type de données	OCTET_STRING
Catégorie	Facultatif
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	Non
Valeur	Non

8.2.2.5 Paramètre de cadence (impulsions) du producteur de sécurité

L'objet « Paramètre de cadence (impulsions) du producteur de sécurité » est spécifié dans le Tableau 20.

Tableau 20 – Paramètre de cadence (impulsions) du producteur de sécurité

Attribut	Valeur
Index	0x1217
Nom	Paramètre de cadence (impulsions) du producteur de sécurité
Type d'objet	RECORD
Type de données	PDO COMMUNICATION PARAMETER
Catégorie	Sous condition; obligatoire pour chaque TxSPDO pris en charge
Sous-index	0x00
Nom	Nombre d'entrées
Type de données	Unsigned8
Catégorie	Obligatoire
Attribut d'accès	RO
Mise en correspondance SPDO	Non
Plage de valeurs	0x01 à 0x0C
Valeur	Non
Sous-index	0x01
Nom	RTFL PID
Description	Indicatif de paquets si transmis sur la CDCL
Type de données	Unsigned32
Catégorie	Sous condition
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	0x01 à 0x00FFFFFF
Valeur	Non
Sous-index	0x02
Nom	RTFN PID
Description	Indicatif de paquets si transmis sur le CDCN
Type de données	Unsigned32
Catégorie	Sous condition
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	0x01 à 0x00FFFFFF
Valeur	Non
Sous-index	0x03
Nom	Réservé
Type de données	Unsigned32
Sous-index	0x04
Nom	Type de transmission
Description	Spécifie le mode de transmission (voir Tableau 18). Doit être mis au mode cyclique
Type de données	Unsigned8
Catégorie	Obligatoire
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	Non

Attribut	Valeur
Valeur	Non
Sous-index	0x05
Nom	ID de synchronisation temporelle
Description	Non utilisé, car le type de transmission est cyclique.
Type de données	Unsigned16
Catégorie	Sous condition
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	0x00 à 0xFF
Valeur	Non
Sous-index	0x06
Nom	Durée d'événement
Description	Non utilisé, car le type de transmission est cyclique
Type de données	Unsigned16
Catégorie	Sous condition
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	Non
Valeur	Non
Sous-index	0x07
Nom	Multiplicateur de cycles
Description	Spécifie la fréquence de transmission (multiple du temps de cycle de base)
Type de données	Unsigned16
Catégorie	Sous condition
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	0x0001, 0x0002, 0x0004, 0x0008, 0x0010, 0x0020, 0x0040, 0x0080, 0x0100, 0x0200, 0x0400, 0x0800, 0x1000, 0x2000, 0x4000, 0x8000
Valeur	Non
Sous-index	0x08
Nom	Décalage de cycle
Description	Spécifie les cycles effectifs de transmission
Type de données	Unsigned16
Catégorie	Sous condition
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	0 à (multiplicateur de cycles – 1)
Valeur	Non
Sous-index	0x09
Nom	Nombre d'envois
Description	Nombre d'occurrences de transmission
Type de données	Unsigned8
Catégorie	Obligatoire
Attribut d'accès	FSF

Attribut	Valeur
Mise en correspondance SPDO	Non
Plage de valeurs	Non
Valeur	2
Sous-index	0x0A
Nom	Adresse de l'appareil
Description	Non utilisé, car la transmission s'effectue sur le CDCN ou la CDCL
Type de données	Unsigned16
Catégorie	Sous condition
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	0x0000 à 0x0200
Valeur	Non
Sous-index	0x0B
Nom	adresse IPv4
Type de données	Unsigned32
Catégorie	Sous condition
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	Non
Valeur	Non
Sous-index	0x0C
Nom	adresse IPv6
Type de données	Unsigned128
Catégorie	Sous condition
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	Non
Valeur	Non

8.2.2.6 Durées de cycle des bus de sécurité

L'objet « Durée de cycle des bus de sécurité » est spécifié dans le Tableau 21. Les durées de cycle des bus de sécurité permettent de calculer les valeurs de temporisation pour les paquets de sécurité.

Tableau 21 – Durées de cycle des bus de sécurité

Attribut	Valeur
Index	0x1218
Nom	Durées de cycle des bus de sécurité
Type d'objet	ARRAY
Type de données	Unsigned32
Catégorie	Obligatoire
Sous-index	0x00
Nom	Nombre d'entrées prises en charge
Type de données	Unsigned8

Attribut	Valeur
Catégorie	Obligatoire
Attribut d'accès	RO
Mise en correspondance SPDO	Non
Plage de valeurs	0x01 à 0x02
Valeur	Non
Sous-index	0x01
Nom	Durée de cycle de base du RTFN de sécurité
Description	Durée de cycle de base pour le CDCN en µs
Type de données	Unsigned32
Catégorie	Sous condition
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	Non
Valeur	Non
Sous-index	0x02
Nom	Durée de cycle de base de la RTFL de sécurité
Description	Durée de cycle de base pour la CDCL en µs
Type de données	Unsigned32
Catégorie	Sous condition
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	Non
Valeur	Non

8.2.2.7 Tolérance de temporisation SPDO

L'objet « Tolérance de temporisation SPDO » est spécifié dans le Tableau 22.

Tableau 22 – Tolérance de temporisation SPDO

Attribut	Valeur
Index	0x121E
Nom	Tolérance de temporisation SPDO
Description	Spécifie le niveau de dépassement potentiel de la temporisation SPDU Donné en pourcentage
Type d'objet	VAR
Type de données	Unsigned8
Catégorie	Sous condition
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	0x00 à 0xFF
Valeur	Non

8.2.2.8 Paramètre de communication RxSPDO

L'objet « Paramètre de communication SPDO de réception » est spécifié dans le Tableau 23.

Tableau 23 – Paramètre de communication SPDO de réception

Attribut	Valeur
Index	0x1C00 – 0x1CFF
Nom	Paramètre de communication SPDO de réception
Type d'objet	RECORD
Type de données	PDO COMMUNICATION PARAMETER
Catégorie	Sous condition; obligatoire pour chaque RxSPDO pris en charge
Sous-index	0x00
Nom	Nombre d'entrées
Type de données	Unsigned8
Catégorie	Obligatoire
Attribut d'accès	RO
Mise en correspondance SPDO	Non
Plage de valeurs	0x01 à 0x0C
Valeur	Non
Sous-index	0x01
Nom	RTFL PID
Description	Indicatif de paquets en cas de transmission CDCL
Type de données	Unsigned32
Catégorie	Sous condition
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	0x01 à 0xFFFFFFFF
Valeur	Non
Sous-index	0x02
Nom	RTFN PID
Description	Indicatif de paquets en cas de transmission CDCN
Type de données	Unsigned32
Catégorie	Sous condition
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	0x01 à 0xFFFFFFFF
Valeur	Non
Sous-index	0x03
Nom	SID
Description	Indicatif unique du partenaire de communication
Type de données	Unsigned16
Catégorie	Obligatoire
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	Non
Valeur	Non
Sous-index	0x04
Nom	Type de transmission

Attribut	Valeur
Description	Spécifie le mode de transmission (voir Tableau 18). Doit être mis au mode cyclique
Type de données	Unsigned8
Catégorie	Obligatoire
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	Non
Valeur	Non
Sous-index	0x05
Nom	ID de synchronisation temporelle
Description	Non utilisé, car le type de transmission est spécifié comme cyclique
Type de données	Unsigned16
Catégorie	Sous condition
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	0x0000 à 0xFFFF
Valeur	Non
Sous-index	0x06
Nom	Multiplicateur de temporisation
Description	Spécifie la fréquence prévue du paquet
Type de données	Unsigned16
Catégorie	Facultatif
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	0x0000 à 0xFFFF
Valeur	Non
Sous-index	0x07
Nom	Multiplicateur de cycles
Description	Spécifie la fréquence d'écriture de la SPDU dans le canal de communication CDCL par les passerelles CP18/1 à CP18/2. Obligatoire si la CDCL est utilisée pour transmission et si les passerelles CP18/1 à CP18/2 sont présentes. Non utilisé pour tous les autres cas
Type de données	Unsigned16
Catégorie	Sous condition
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	0x01 à 0xFFFF
Valeur	Non
Sous-index	0x08
Nom	Décalage de cycle
Description	Décalage de cycle (écriture de la SPDU dans le canal CDCL). Obligatoire si la CDCL est utilisée pour transmission et si les passerelles CP18/1 à CP18/2 sont présentes. Non utilisé pour tous les autres cas
Type de données	Unsigned16

Attribut	Valeur
Catégorie	Sous condition
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	0x00 à 0xFFFE
Valeur	Non
Sous-index	0x09
Nom	Nombre de réceptions admises
Description	Nombre maximal de réceptions potentielles de la SPDU
Type de données	Unsigned8
Catégorie	Obligatoire
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	Non
Valeur	2
Sous-index	0x0A
Nom	Adresse de l'appareil
Description	Non utilisé, car la transmission s'effectue sur le CDCN ou la CDCL
Type de données	Unsigned16
Catégorie	Sous condition
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	0x00 à 0x200
Valeur	Non
Sous-index	0x0B
Nom	adresse IPv4
Type de données	Unsigned32
Catégorie	Sous condition
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	Non
Valeur	Non
Sous-index	0x0C
Nom	adresse IPv6
Type de données	Unsigned128
Catégorie	Sous condition
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	Non
Valeur	Non

8.2.2.9 Paramètre de communication TxSPDO

L'objet « Paramètre de communication SPDO de transmission » est spécifié dans le Tableau 24.

Tableau 24 – Paramètre de communication SPDO de transmission

Attribut	Valeur
Index	0x1E00 – 0x1EFF
Nom	Paramètre de communication SPDO de transmission
Type d'objet	RECORD
Type de données	PDO COMMUNICATION PARAMETER
Catégorie	Sous condition; obligatoire pour chaque TxSPDO pris en charge
Sous-index	0x00
Nom	Nombre d'entrées
Type de données	Unsigned8
Catégorie	Obligatoire
Attribut d'accès	RO
Mise en correspondance SPDO	Non
Plage de valeurs	0x01 à 0x0C
Valeur	Non
Sous-index	0x01
Nom	RTFL PID
Description	Indicatif de paquets en cas de transmission CDCL
Type de données	Unsigned32
Catégorie	Sous condition
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	0x01 à 0xFFFFFFFF
Valeur	Non
Sous-index	0x02
Nom	RTFN PID
Description	Indicatif de paquets en cas de transmission CDCN
Type de données	Unsigned32
Catégorie	Sous condition
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	0x01 à 0xFFFFFFFF
Valeur	Non
Sous-index	0x04
Nom	Type de transmission
Description	Spécifie le mode de transmission (voir Tableau 18). Doit être mis au mode cyclique
Type de données	Unsigned8
Catégorie	Obligatoire
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	Non
Valeur	Non
Sous-index	0x05
Nom	ID de synchronisation temporelle

Attribut	Valeur
Description	Non utilisé, car le type de transmission est spécifié comme cyclique
Type de données	Unsigned16
Catégorie	Sous condition
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	0x00 à 0xFF
Valeur	Non
Sous-index	0x06
Nom	Durée d'événement
Description	Non utilisé, car le type de transmission est spécifié comme cyclique
Type de données	Unsigned16
Catégorie	Sous condition
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	Non
Valeur	Non
Sous-index	0x07
Nom	Multiplicateur de cycles
Description	Spécifie la fréquence de transmission.
Type de données	Unsigned16
Catégorie	Sous condition
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	0x0001, 0x0002, 0x0004, 0x0008, 0x0010, 0x0020, 0x0040, 0x0080, 0x0100, 0x0200, 0x0400, 0x0800, 0x1000, 0x2000, 0x4000, 0x8000
Valeur	Non
Sous-index	0x08
Nom	Décalage de cycle
Description	Cycles de transmission effectifs.
Type de données	Unsigned16
Catégorie	Sous condition
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	0 à (multiplicateur de cycles – 1)
Valeur	Non
Sous-index	0x09
Nom	Nombre d'envois
Description	Spécifie la fréquence de transmission du paquet.
Type de données	Unsigned8
Catégorie	Obligatoire
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	Non
Valeur	2

Attribut	Valeur
Sous-index	0x0A
Nom	Adresse de l'appareil
Description	Non utilisé, car la transmission s'effectue sur le CDCN ou la CDCL
Type de données	Unsigned16
Catégorie	Sous condition
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	0x00 à 0x200
Valeur	Non
Sous-index	0x0B
Nom	adresse IPv4
Type de données	Unsigned32
Catégorie	Sous condition
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	Non
Valeur	Non
Sous-index	0x0C
Nom	adresse IPv6
Type de données	Unsigned128
Catégorie	Sous condition
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	Non
Valeur	Non

8.2.2.10 Mise en correspondance SPDO

8.2.2.10.1 Principe de mise en correspondance SPDO

Les paramètres de mise en correspondance SPDO définissent le contenu d'un SPDO. Un SPDO valide contient au moins un objet d'application de sécurité et au plus 254. Le codage d'une entrée de mise en correspondance est spécifié dans le Tableau 25.

Tableau 25 – Format de mise en correspondance

Bit	Nom	Signification
0 à 7	Longueur	Longueur de l'objet d'application de sécurité en bits
8 à 15	Sous-index	Sous-index de l'objet d'application de sécurité à mettre en correspondance. Le dictionnaire d'objets de sécurité est organisé sous forme de tableau avec éléments clés (index, sous-index). Cette mise en correspondance spécifie la clé de consultation pour cet objet d'application.
16 à 31	Index	Index de l'objet d'application de sécurité à mettre en correspondance

8.2.2.10.2 Paramètre de mise en correspondance RxSPDO

L'objet « Paramètre de mise en correspondance SPDO de réception » est spécifié dans le Tableau 26.

Tableau 26 – Paramètre de mise en correspondance SPDO de réception

Attribut	Valeur
Index	0x1D00 à 0x1DFF
Nom	Paramètre de mise en correspondance SPDO de réception
Description	Mise en correspondance de l'objet de la PDU de sécurité au dictionnaire d'objets de sécurité. Voir Tableau 25
Type d'objet	RECORD
Type de données	PDO_MAPPING
Catégorie	Sous condition; obligatoire pour chaque RxSPDO pris en charge
Sous-index	0x00
Nom	Nombre d'objets d'application de sécurité mis en correspondance
Type de données	Unsigned8
Catégorie	Obligatoire
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	0x00 à 0xFE
Valeur	Non
Sous-index	0x01 à 0xFE
Nom	Mise en correspondance SPDO pour le nème objet d'application de sécurité à mettre en correspondance
Description	Spécifié dans le Tableau 25
Type de données	Unsigned32
Catégorie	Sous condition selon le nombre et la taille des objets à mettre en correspondance
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	Non
Valeur	Non

8.2.2.10.3 Paramètre de mise en correspondance TxSPDO

L'objet « Paramètre de mise en correspondance SPDO de transmission » est spécifié dans le Tableau 27.

Tableau 27 – Paramètre de mise en correspondance SPDO de transmission

Attribut	Valeur
Index	0x1E00 à 0x1EFF
Nom	Paramètre de mise en correspondance SPDO de transmission
Description	Mise en correspondance de l'objet du dictionnaire d'objets de sécurité à la PDU de sécurité. Voir Tableau 25
Type d'objet	RECORD
Type de données	PDO_MAPPING
Catégorie	Sous condition; obligatoire pour chaque TxSPDO pris en charge
Sous-index	0x00
Nom	Nombre d'objets d'application de sécurité mis en correspondance
Type de données	Unsigned8
Catégorie	Obligatoire

Attribut	Valeur
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	0x01 à 0xFE
Valeur	Non
Sous-index	0x01 à 0xFE
Nom	Mise en correspondance SPDO pour le nème objet d'application de sécurité à mettre en correspondance
Description	Spécifié dans le Tableau 25
Type de données	Unsigned32
Catégorie	Sous condition selon le nombre et la taille des objets à mettre en correspondance
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	Non
Valeur	Non

8.2.3 Section de profil d'appareil normalisé

Les objets d'application de sécurité peuvent être mis en correspondance dans les SPDO. Les objets d'application de sécurité sont situés dans la zone de dictionnaire d'objets de sécurité de 0x8000 à 0x9FFF. Ces objets sont spécifiques au fabricant et à l'application.

9 Exigences relatives au système

9.1 Voyants et commutateurs

9.1.1 Etats des voyants et fréquences de clignotement

Les états des voyants et les fréquences de clignotement sont définis dans le Tableau 28. Les durées énumérées doivent être respectées avec une tolérance de moins de ± 25%.

Tableau 28 – Définition des états des voyants

Etat du voyant	Définition
OFF	Le voyant doit être éteint de manière constante
ON	Le voyant doit être allumé de manière constante
BLINKING 1 Hz	Le voyant doit s'allumer et s'éteindre avec une fréquence de 1 Hz
BLINKING 2 Hz	Le voyant doit s'allumer et s'éteindre avec une fréquence de 2 Hz

9.1.2 Voyants

Il convient que les appareils qui prennent en charge le protocole FSCP 18/1 comportent un voyant STATUS. Ce voyant, généralement une DEL, participe à la recherche de pannes, à l'examen visuel, aux opérations de maintenance et au diagnostic des problèmes constatés. Si un appareil prend en charge le voyant STATUS, ce dernier doit satisfaire à cette spécification. D'autres voyants peuvent être mis en oeuvre.

Le voyant STATUS doit indiquer l'état de la communication FSCP 18/1. Un voyant bicolore unique (vert/rouge) doit être utilisé.

Une étiquette « FS SNp » doit être apposée sur le voyant STATUS.

Les états du voyant STATUS sont spécifiés dans le Tableau 29.

Tableau 29 – Etats du voyant STATUS

Etat du voyant	Définition
OFF	Aucune communication de données de processus de sécurité n'est active
GREEN ON	Toutes les communications de données de processus de sécurité configurées (SPDO) sont actives
GREEN BLINKING 1 Hz	Au moins un SPDO est actif et au moins un SPDO est inactif
RED ON	Configuration non valide ou incompatible
RED BLINKING 2 Hz	Erreur interne

9.1.3 Commutateurs

Il n'existe aucun commutateur pour le protocole FSP 18/1.

9.2 Lignes directrices d'installation

Les lignes directrices d'installation appropriées sont spécifiées par l'IEC 61918.

9.3 Temps de réponse de la fonction de sécurité

9.3.1 Généralités

Une fonction de sécurité peut être constituée de plusieurs composantes. Afin de pouvoir déterminer le temps de réponse de la fonction de sécurité, ladite fonction est décomposée dans les différentes composantes illustrées à la Figure 16.

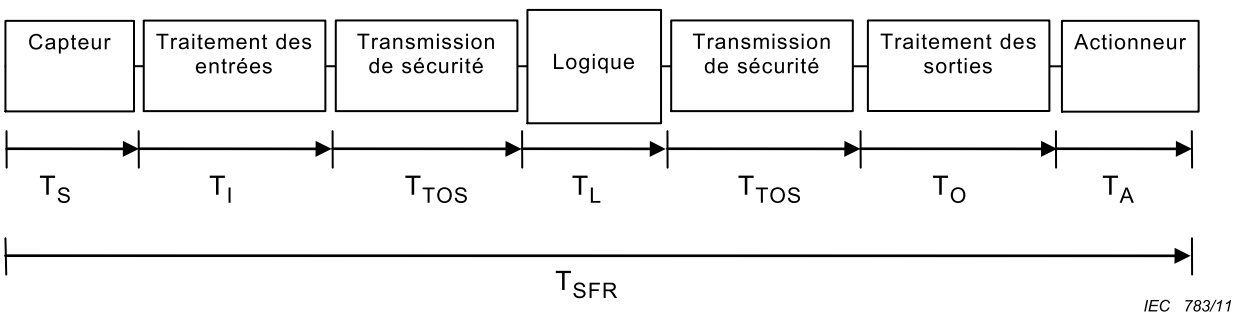


Figure 16 – Composantes du temps de réponse de la fonction de sécurité

Le canal de la fonction de sécurité se compose d'un capteur (par exemple, rideau de lumière ou bouton d'arrêt d'urgence) qui permet de détecter l'activation de la fonction de sécurité. Ce capteur convertit le signal physique en un signal électrique. Ce signal électrique est relié à un appareil d'entrée (par exemple, un module d'entrée de sécurité fonctionnelle) qui convertit le signal électrique en une information d'entrée logique. Le système de communication de sécurité permet de transmettre l'information d'entrée logique au contrôleur logique de sécurité. Ce dernier compile l'information d'entrée logique en information de sortie logique, qui est transmise à un appareil de sortie (par exemple, un module de sortie de sécurité fonctionnelle) par l'intermédiaire du système de communication de sécurité. L'information de sortie logique est convertie en un signal de sortie physique relié à un actionneur. Ce dernier exécute la réaction physique. Chaque composante est décrite par un comportement temporel caractéristique.

Les hypothèses générales suivantes s'appliquent à d'autres prises en considération.

- Le fonctionnement de toutes les composantes du canal de la fonction de sécurité est asynchrone.
- Toutes les composantes du canal de la fonction de sécurité sont décrites par un temps de traitement ou de réponse le plus défavorable garanti dans des conditions autres que des conditions d'erreur.
- Un temporisateur superposé (T_{TOi}) est associé à chaque composante pour des raisons de sécurité.
- Il doit être supposé, afin de calculer le temps de réponse de la fonction de sécurité, que le parcours de signal concerné comporte une erreur ou une défaillance, qui contribue au temps de différence maximal entre sa temporisation et son temps de traitement ou de réponse le plus défavorable.

Les temps caractéristiques du capteur, des entrées, de la logique, des sorties et de l'actionneur des appareils ne relèvent pas du domaine d'application de la présente norme. Il convient que les informations cohérentes pour ces valeurs caractéristiques proviennent des spécifications des composantes. Chaque appareil doit fournir ces valeurs comme partie intégrante de ses propriétés intrinsèques.

9.3.2 Détermination de la procédure de contrôle de retard FSCP 18/1

Le protocole FSCP 18/1 définit une procédure de contrôle de retard configurable (temporisation) pour la remise de données de processus de sécurité côté récepteur d'une relation de communication. Cette procédure de contrôle est mise en œuvre par la temporisation de communication T_{TOS}.

Deux transmissions de sécurité sont nécessaires pour le canal de la fonction de sécurité. Les composantes logique et de traitement de sortie fonctionnent comme un récepteur et mettent en œuvre la procédure de contrôle de retard. L'Equation (2) décrit le calcul de T_{TOS}.

$$T_{TOS} = T_{cycle} + \Delta T \qquad (2)$$

La SHB n'influence pas T_{TOS} dans la mesure où seule la synchronisation des horloges système est requise. Lorsque la cadence (impulsion) à de sécurité détecte des retards inacceptables, l'état de sécurité intrinsèque est alors activé (voir 7.3).

9.3.3 Calcul du temps de réponse de la fonction de sécurité le plus défavorable

Le canal de la fonction de sécurité de base utilisé pour calculer la fonction de sécurité la plus défavorable est illustré à la Figure 16.

Le temps de réponse de la fonction de sécurité peut être calculé selon l'Equation (3).

Il doit être supposé que le canal de la fonction de sécurité comporte une erreur ou une défaillance pour obtenir le temps de réponse de la fonction de sécurité le plus défavorable. Cette erreur ou défaillance contribue à la différence maximale observée entre son temps de retard le plus défavorable et son temps de temporisation.

$$T_{SFR} = T_S + T_I + T_T + T_L + T_T + T_O + T_A + \max_{i=S,I,...A}(T_{TOi} - T_i) \qquad (3)$$

NOTE L'index « i » identifie les composantes S, I, T, L, O et A dans l'Equation (3).

Les fabricants de systèmes doivent fournir, si nécessaire, leur propre méthode de calcul adaptée.

9.4 Durée des demandes

La durée de la demande émise par l'application relative à la sécurité à la couche de communication de sécurité peut être équivalente ou supérieure au temps de sécurité de processus ou au temps de temporisation FSCP 18/1 (T_{TO}).

9.5 Contraintes liées au calcul des caractéristiques du système

9.5.1 Contraintes relatives à la sécurité

9.5.1.1 Généralités

Les conditions aux limites et les contraintes relatives à l'évaluation de la sécurité du protocole FSCP 18/1, et applicables aux calculs appropriés du taux d'erreur résiduel sont décrites dans les articles suivants.

9.5.1.2 Nombre de collecteurs d'information

Le nombre de appareils de production et de consommation pour un réseau FSCP 18/1 est limité à 512. Le nombre de collecteurs d'information est limité à 511 appareils de consommation dans le cas d'une relation 1:*n*.

9.5.1.3 Limite de fréquence des messages

La fréquence des messages ne doit pas dépasser 1 000 messages de sécurité à la seconde. Il doit être tenu compte du nombre d'appareils de production et du temps de cycle afin qu'ils ne dépassent pas la limite de taux de messages, tel qu'indiqué dans les Equations (4) à (6).

$$MR_{SPDO} = \sum_{I \in SPDO} \frac{1\,000\,000 \times NS_I}{CM_I \times T_{BC}} \tag{4}$$

$$MR_{SHB} = \sum_{D1 \in devices} \left[\sum_{\substack{D2 \in devices \\ D2 \neq D1}} \frac{1\ 000\,000 \times NS_{D1} \times 2}{CM_{D1} \times T_{BC}} \right] \tag{5}$$

$$MR = MR_{SPDO} + MR_{SHB} \tag{6}$$

où

CM_{D1} est le paramètre de cadence (impulsions) du producteur de sécurité (Index: 0x1217, Sous-index: 0x07, multiplicateur de cycles) transmis par l'appareil D1 (voir le Tableau 20);

CM_I est le paramètre de communication SPDO de transmission (Index: 0x1E00 - 0x1EFF, Sous-index: 0x07, multiplicateur de cycles) pour SPDOI (voir le Tableau 24);

NS_{D1} est le paramètre de cadence (impulsions) du producteur de sécurité (Index: 0x1217, Sous-index: 0x09, Nombre d'envois) transmis par l'appareil D1 (voir le Tableau 20);

NS_I est le paramètre de communication SPDO de transmission (Index: 0x1E00 - 0x1EFF, Sous-index: 0x09, Nombre d'envois) pour SPDOI (voir le Tableau 24);

MR est le taux de message total;

MR_{SHB} est le taux de messages pour les SHB;

MR_{SPDO} est le taux de messages pour les SPDO;

T_{BC} est les temps de cycle de bus de sécurité. Paramètre dépendant si CP 18/1 (Index: 0x1218, Sous-index 0x02, temps de cycle de base RTFL de sécurité) ou CP 18/2 (Index: 0x1218, Sous-index: 0x01, temps de cycle de base RTFN de sécurité) est utilisé (voir le Tableau 21).

9.5.1.4 Taille des messages

La taille de message d'une PDU de sécurité constituée des champs de données illustrés à la Figure 17 est limitée de 0 à 128 octets.

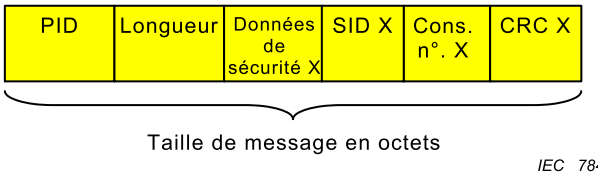


Figure 17 – Champs de données pris en compte pour le calcul de la taille des messages

9.5.1.5 Taux d'erreurs sur les bits

Le taux maximal d'erreurs sur les bits ne doit pas dépasser 0,01.

9.5.2 Considérations d'ordre probabiliste

Le mécanisme de contrôle de l'intégrité des données du protocole FSCP 18/1 est totalement indépendant des mécanismes du système de communication sous-jacent, qui est alors appelé « canal noir ».

La Figure 18 illustre les diagrammes des probabilités d'erreurs résiduelles applicables au polynôme de 32 bits utilisé (distance de Hamming minimale de 6). Les diagrammes s'appliquent pour des longueurs de données de 128 octets tel que spécifié en 9.5.1.4, incluant la signature CRC et intégrant la structure du PDU de sécurité global tel que décrit au 7.1. Il a été calculé que la PFH résultante du canal de communication est inférieure ou égale à 10^{-9}. Ce niveau équivaut à $5{,}43 \times 10^{-19}$ pour la probabilité d'erreur résiduelle d'une PDU telle qu'illustrée à la Figure 18. Le mécanisme de contrôle d'intégrité des données doit être obligatoirement utilisé pour atteindre ces niveaux (voir 7.1.1.2)

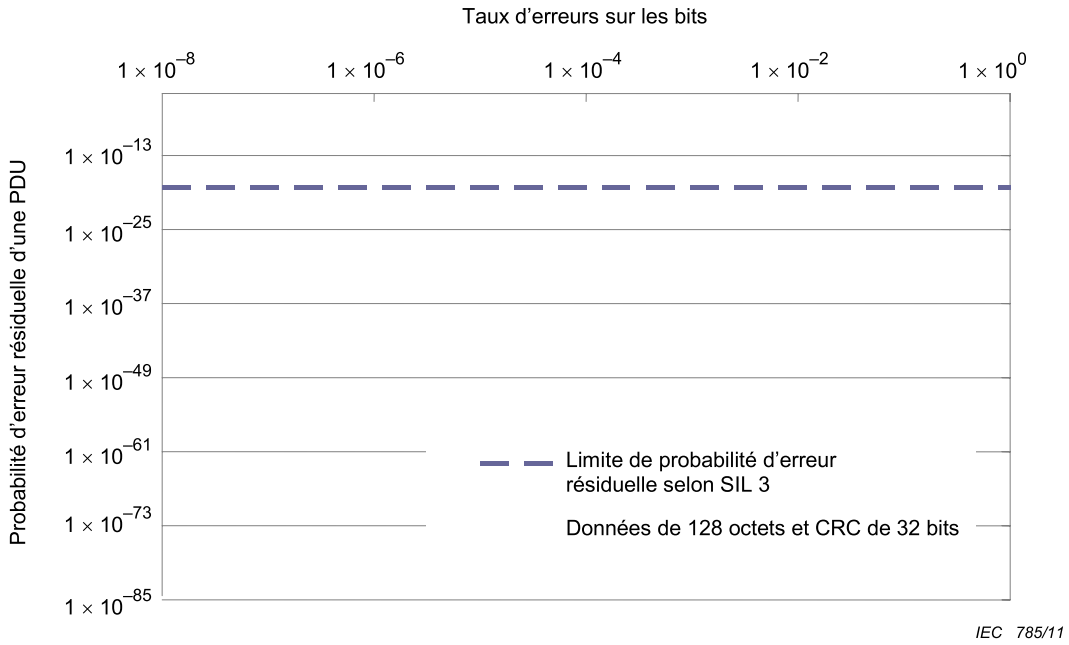


Figure 18 – Taux d'erreurs résiduelles

9.6 Maintenance

Ce protocole ne fait l'objet d'aucune exigence de maintenance particulière.

9.7 Manuel de sécurité

Le fabricant de l'appareil de sécurité doit fournir avec l'appareil un manuel de sécurité conforme aux exigences de l'IEC 61508-2 Outre les exigences énumérées dans l'IEC 61508-2, les informations suivantes doivent être fournies:

- le nom et l'adresse du fabricant;
- le temps T_i le plus défavorable;
- le temps de temporisation T_{TOi};
- Probabilité de défaillance à la demande PFH;
- Niveau d'intégrité de sécurité SIL;
- Intervalle de l'essai périodique T_1 (selon IEC 61508-6) et/ou Mission T_m (selon ISO 13849-1);
- Version(s) du protocole prise(s) en charge (voir 7.1.3.4) sauf dans le cas où seule la version 1 du protocole est prise en charge.

NOTE Les temps peuvent dépendre des fonctions de sécurité et des modes de fonctionnement individuels.

10 Evaluation

Il est fortement recommandé aux ingénieurs d'application du FSCP 18/1 d'obtenir la vérification auprès d'un organisme compétent indépendant pour tous les aspects de sécurité fonctionnelle du produit, tant du protocole que de toute application. Il est fortement recommandé aux ingénieurs d'application du FSCP 18/1 d'obtenir la preuve qu'un organisme compétent indépendant a réalisé un essai de conformité approprié.

Le fabricant d'un produit de sécurité est responsable de la mise en œuvre correcte de la technologie de couche de communication de sécurité, ainsi que de l'exactitude et de l'exhaustivité de l'information orientée produit et des renseignements sur le produit. Les informations complètes sont fournies en [46].

Annex A
(informative)

Informations supplémentaires pour les profils de communication de sécurité fonctionnelle de protocole CPF 18

Il n'existe aucune information supplémentaire concernant ce FSCP.

Annex B
(informative)

Information pour l'évaluation des profils de communication de sécurité fonctionnelle de protocole CPF 18

Des informations sur les laboratoires d'essai qui vérifient et valident la conformité des produits FSCP 18/1 avec l'IEC 61784-3-18 peuvent être obtenues auprès des comités nationaux de l'IEC ou de l'institution suivante:

Safety Network International e.V.
Robert-Bosch-Str.30
73760 Ostfildern
ALLEMAGNE

Téléphone: +49 711 3409 118
Télécopie: +49 711 3409 449
e-mail: info@safety-network.de
URL: www.safety-network.de

Bibliographie

[1] IEC 60050 (toutes parties), *Vocabulaire Electrotechnique International*

NOTE Voir également le dictionnaire multilingue de l'IEC – Electricité, électronique et télécommunications (disponible sur CD-ROM et à l'adresse http://www.electropedia.org).

[2] IEC 60204-1, *Sécurité des machines – Équipement électrique des machines – Partie 1: Règles générales*

[3] IEC/TS 61000-1-2, *Electromagnetic compatibility (EMC) – Part 1-2: General – Methodology for the achievement of the functional safety of electrical and electronic equipment with regard to electromagnetic phenomena* (disponible uniquement en anglais)

[4] IEC 61131-6[5], *Programmable controllers – Part 6: Functional safety* (disponible uniquement en anglais)

[5] IEC 61158 (toutes parties), *Industrial communication networks – Fieldbus specifications* (disponible uniquement en anglais)

[6] IEC 61326-3-1, *Matériel électrique de mesure, de commande et de laboratoire – Exigences relatives à la CEM – Partie 3-1: Exigences d'immunité pour les systèmes relatifs à la sécurité et pour les matériels destinés à réaliser des fonctions relatives à la sécurité (sécurité fonctionnelle) – Applications industrielles générales*

[7] IEC 61326-3-2, *Matériel électrique de mesure, de commande et de laboratoire – Exigences relatives à la CEM – Partie 3-2: Exigences d'immunité pour les systèmes relatifs à la sécurité et pour les matériels destinés à réaliser des fonctions relatives à la sécurité (sécurité fonctionnelle) – Applications industrielles dont l'environnement électromagnétique est spécifié*

[8] IEC 61496 (toutes parties), *Sécurité des machines – Equipements de protection électro-sensibles*

[9] IEC 61508-1:2010, *Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité – Partie 1: Exigences générales*

[10] IEC 61508-4:2010, *Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité – Partie 4: Définitions et abréviations*

[11] IEC 61508-5:2010, *Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité – Partie 5: Exemples de méthodes de détermination des niveaux d'intégrité de sécurité*

[12] IEC 61511 (toutes parties), *Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur des industries de transformation*

[13]

[14] IEC/PWI 61784-4[6], *Industrial communication networks – Profiles – Part 4: Secure communications for fieldbuses* (disponible uniquement en anglais)

[15] IEC 61784-5 (toutes parties), *Industrial communication networks – Profiles – Part 5: Installation of fieldbuses – Installation profiles for CPF x* (disponible uniquement en anglais)

[16] IEC 61800-5-2, *Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional* (disponible uniquement en anglais)

[17] IEC/TR 62059-11, *Equipements de comptage de l'électricité – Sûreté de fonctionnement – Partie 11: Concepts généraux*

[18] IEC 62061, *Sécurité des machines - Sécurité fonctionnelle des systèmes de commande électriques, électroniques et électroniques programmables relatifs à la sécurité*

[19] IEC/TR 62210, *Power system control and associated communications – Data and communication security* (disponible uniquement en anglais)

---

5 En cours d'élaboration.

6 A l'étude.

[20] IEC 62280-1, *Applications ferroviaires – Systèmes de signalisation, de télécommunication et de traitement – Partie 1: Communication de sécurité sur des systèmes de transmission fermés*

[21] IEC 62280-2, *Applications ferroviaires – Systèmes de signalisation, de télécommunication et de traitement – Partie 2: Communication de sécurité sur des systèmes de transmission ouverts*

[22] IEC 62443 (toutes parties), *Industrial communication networks – Network and system security* (disponible uniquement en anglais)

[23] ISO/IEC Guide 51:1999, *Aspects liés à la sécurité – Principes directeurs pour les inclure dans les normes*

[24] ISO/IEC 2382-14, *Technologies de l'information – Vocabulaire – Partie 14: Fiabilité, maintenabilité et disponibilité*

[25] ISO/IEC 2382-16, *Technologies de l'information – Vocabulaire – Partie 16: Théorie de l'information*

[26] ISO/IEC 7498 (toutes parties), *Technologies de l'information – Interconnexion de systèmes ouverts (OSI) – Modèle de référence de base*

[27] ISO 10218-1, *Robots pour environnements industriels – Exigences de sécurité – Partie 1: Robot*

[28] ISO 12100-1, *Sécurité des machines – Notions fondamentales, principes généraux de conception – Partie 1: terminologie de base, méthodologie*

[29] ISO 13849-1, *Sécurité des machines – Parties des systèmes de commande relatives à la sécurité – Partie 1: principes généraux de conception*

[30] ISO 13849-2, *Sécurité des machines – Parties des systèmes de commande relatives à la sécurité – Partie 2: Validation*

[31] ISO 14121, *Sécurité des machines – Principes pour l'appréciation du risque*

[32] ANSI/ISA-84.00.01-2004 (all parts), *Functional Safety: Safety Instrumented Systems for the Process Industry Sector*

[33] VDI/VDE 2180 (toutes parties), *Safeguarding of industrial process plants by means of process control engineering*

[34] GS-ET-26[7], *Grundsatz für die Prüfung und Zertifizierung von Bussystemen für die Übertragung sicherheitsrelevanter Nachrichten*, May 2002. HVBG, Gustav-Heinemann-Ufer 130, D-50968 Köln ("*Principles for Test and Certification of Bus Systems for Safety relevant Communication*")

[35] ANDREW S. TANENBAUM, *Computer Networks*, 4th Edition, Prentice Hall, N.J., ISBN-10:0130661023, ISBN-13: 978-0130661029

[36] W. WESLEY PETERSON, *Error-Correcting Codes*, 2nd Edition 1981, MIT-Press, ISBN 0-262-16-039-0

[37] BRUCE P. DOUGLASS, *Doing Hard Time*, 1999, Addison-Wesley, ISBN 0-201-49837-5

[38] *New concepts for safety-related bus systems*, 3rd International Symposium "Programmable Electronic Systems in Safety Related Applications ", May 1998, from Dr. Michael Schäfer, BG-Institute for Occupational Safety and Health.

[39] DIETER CONRADS, *Datenkommunikation*, 3rd Edition 1996, Vieweg, ISBN 3-528-245891

[40] German IEC subgroup DKE AK 767.0.4: *EMC and Functional Safety*, Spring 2002

[41] NFPA79 (2002), *Electrical Standard for Industrial Machinery*

[42] GUY E. CASTAGNOLI, *On the Minimum Distance of Long Cyclic Codes and Cyclic Redundancy-Check Codes*, 1989, Dissertation No. 8979 of ETH Zurich, Switzerland

---

7 GS-ET-26 constitue l'un des points de départ de l'élaboration de la présente partie. Il fait actuellement l'objet d'une révision importante.

[43] GUY E. CASTAGNOLI, STEFAN BRÄUER, and MARTIN HERRMANN, *Optimization of Cyclic Redundancy-Check Codes with 24 and 32 Parity Bits*, June 1993, IEEE Transactions On Communications, Volume 41, No. 6

[44] SCHILLER F and MATTES T: *An Efficient Method to Evaluate CRC-Polynomials for Safety-Critical Industrial Communication*, Journal of Applied Computer Science, Vol. 14, No 1, pp. 57-80, Technical University Press, Łódź,Poland, 2006

[45] SCHILLER F and MATTES T: *Analysis of CRC-polynomials for Safety-critical Communication by Deterministic and Stochastic Automata*, 6th IFAC Symposium on Fault Detection, Supervision and Safety for Technical Processes, SAFEPROCESS 2006, pp. 1003-1008, Beijing, China, 2006

[46] *Technical Guideline Integration*, V2.0, December 2008, Safety Network International e. V. Ostfildern, Germany

[47] *CANopen Application Layer and Communication Profile, CiA Draft Standard 301*, Version 4.02, 13 February 2002, CAN in Automation e.V., Nürnberg, Germany

———————

IEC 61784-3-18

Edition 1.1 2016-07

FINAL VERSION

VERSION FINALE

colour inside

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 le CPF 18

IEC 61784-3-18:2011-04+AMD1:2016-07 CSV(en-fr)

CONTENTS

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 IEC 61784-3-18 bears the edition number 1.1. It consists of the first edition (2011-04) [documents 65C/639/FDIS and 65C/649/RVD] and its amendment 1 (2016-07) [documents 65C/851/FDIS and 65C/854/RVD]. The technical content is identical to the base edition and its amendment.

This Final version does not show where the technical content is modified by amendment 1. A separate Redline version with all changes highlighted 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 amendment 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.

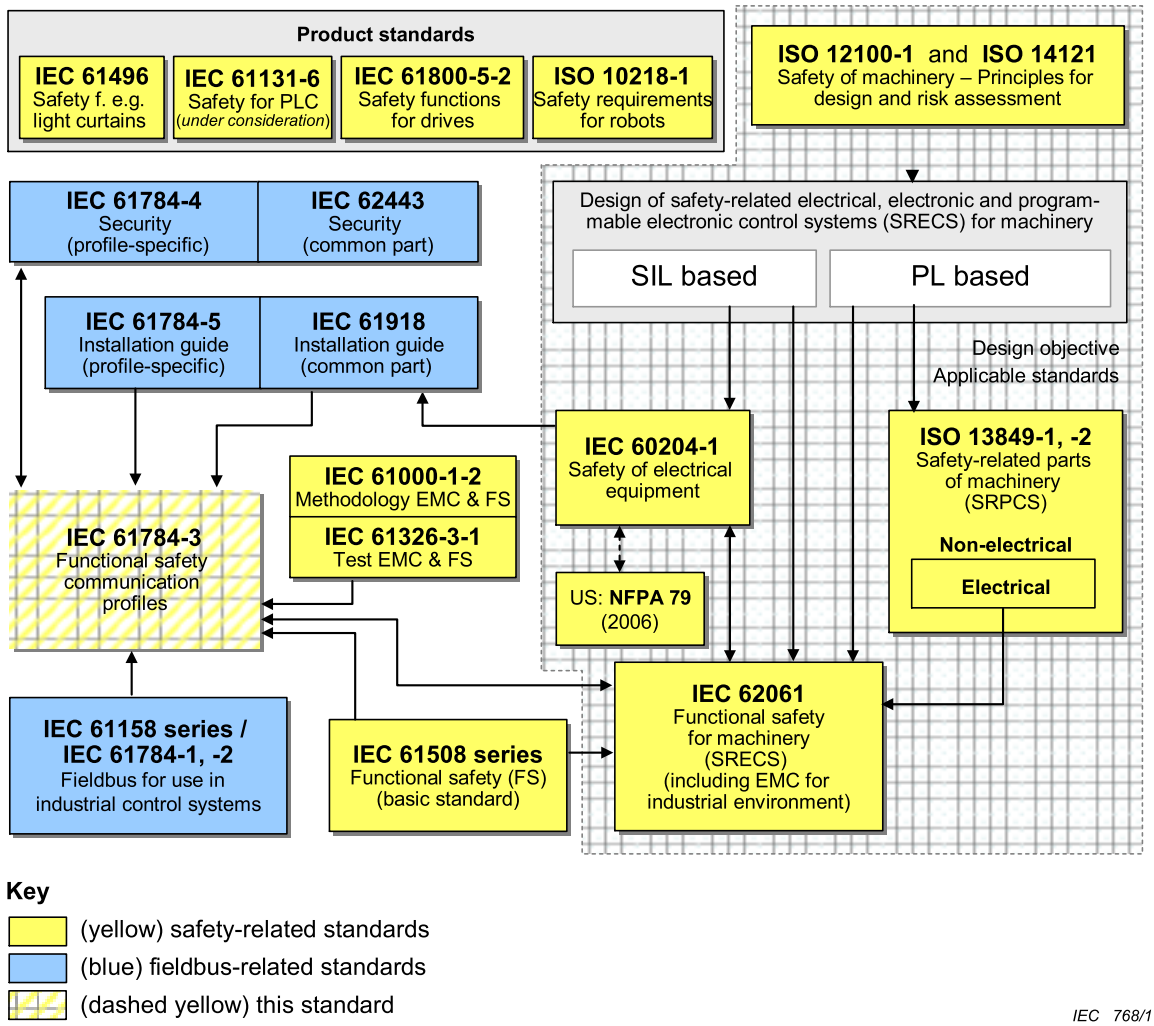
0 Introduction

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.

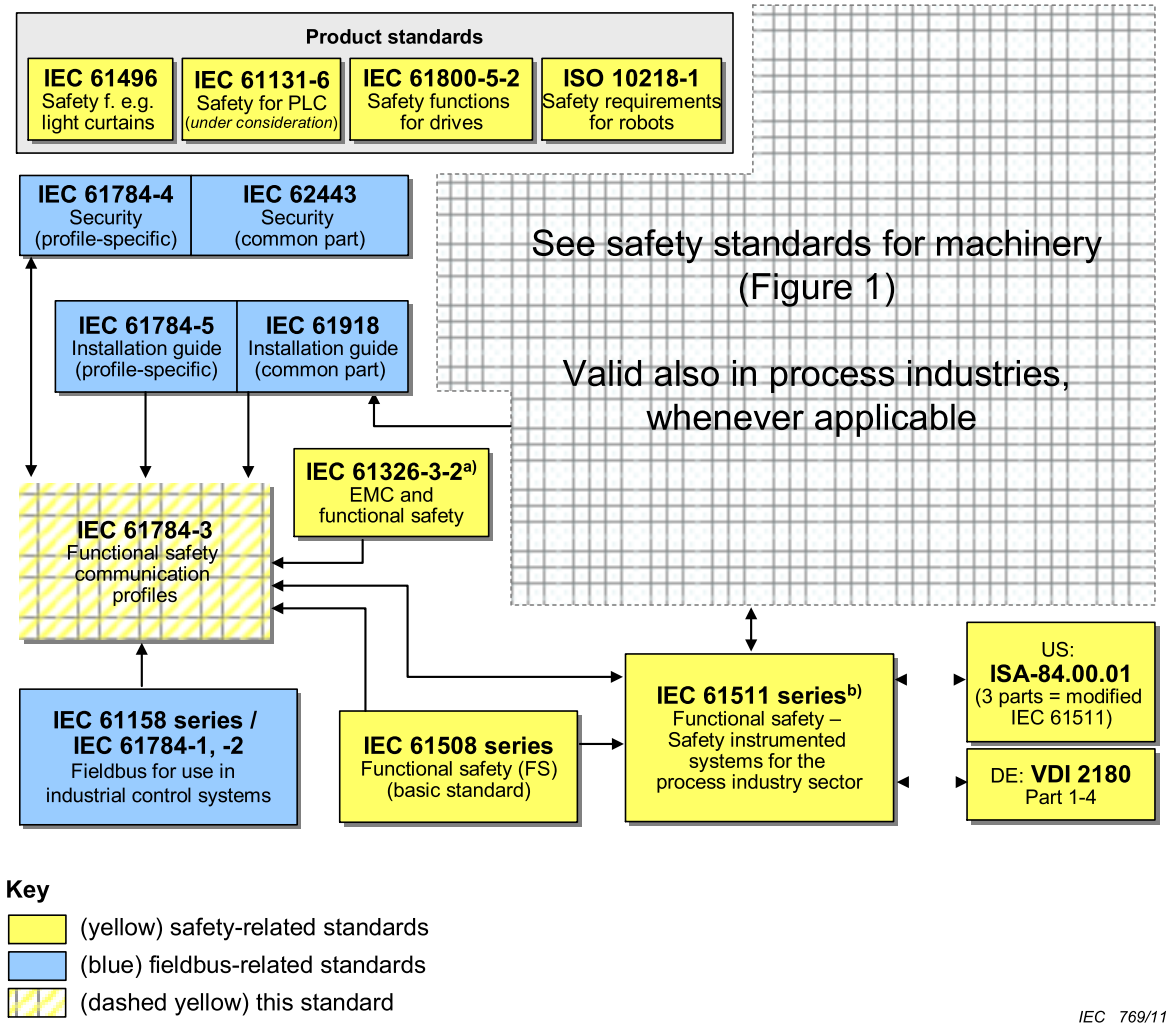
Figure 1 shows the relationships between this standard and relevant safety and fieldbus standards in a machinery environment.



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.

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

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



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

b EN ratified.

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

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

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

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

This standard describes:

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

0.2 Patent declaration

The International Electrotechnical Commission (IEC) draws attention to the fact that it is claimed that compliance with this document may involve the use of 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 part[1] 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 series[2] 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.

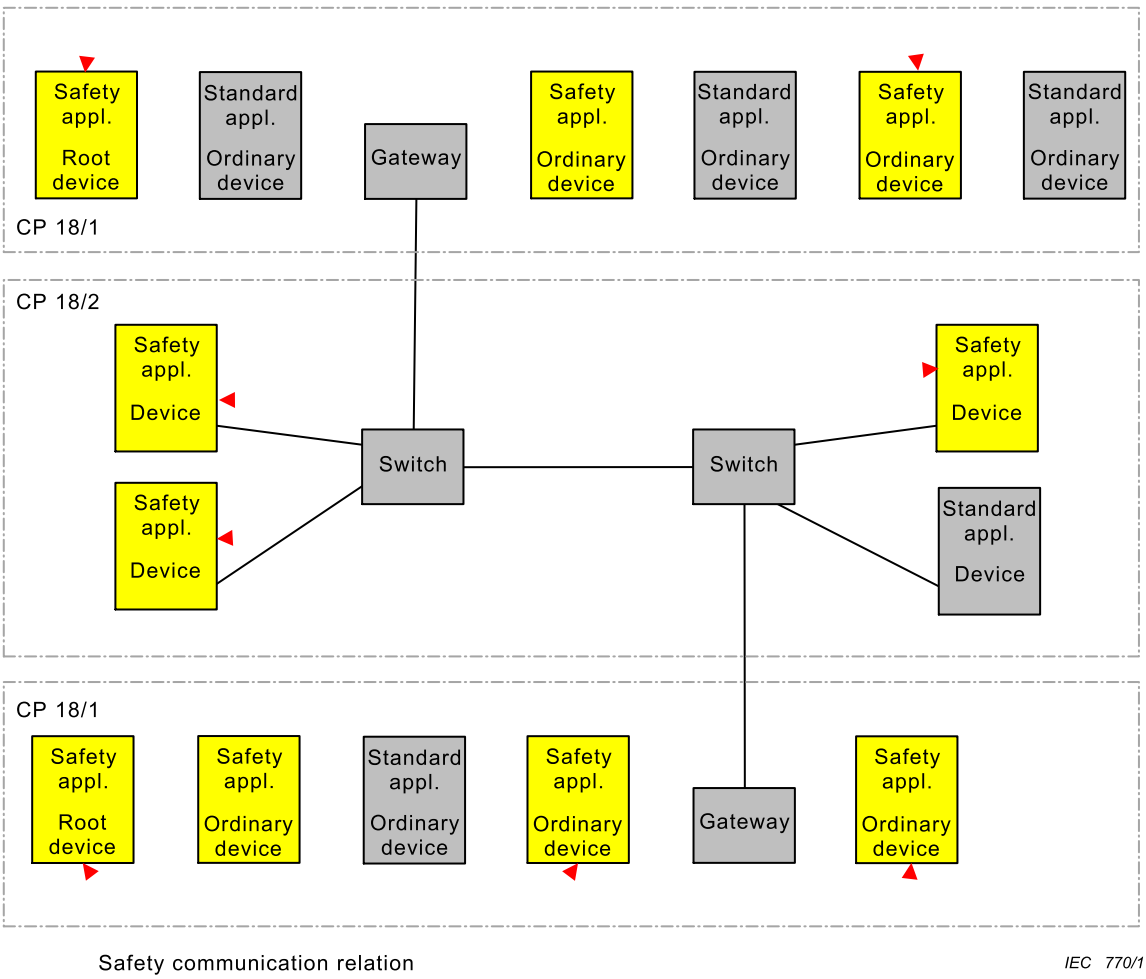


Figure 3 – FSCP 18/1 system

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]

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.

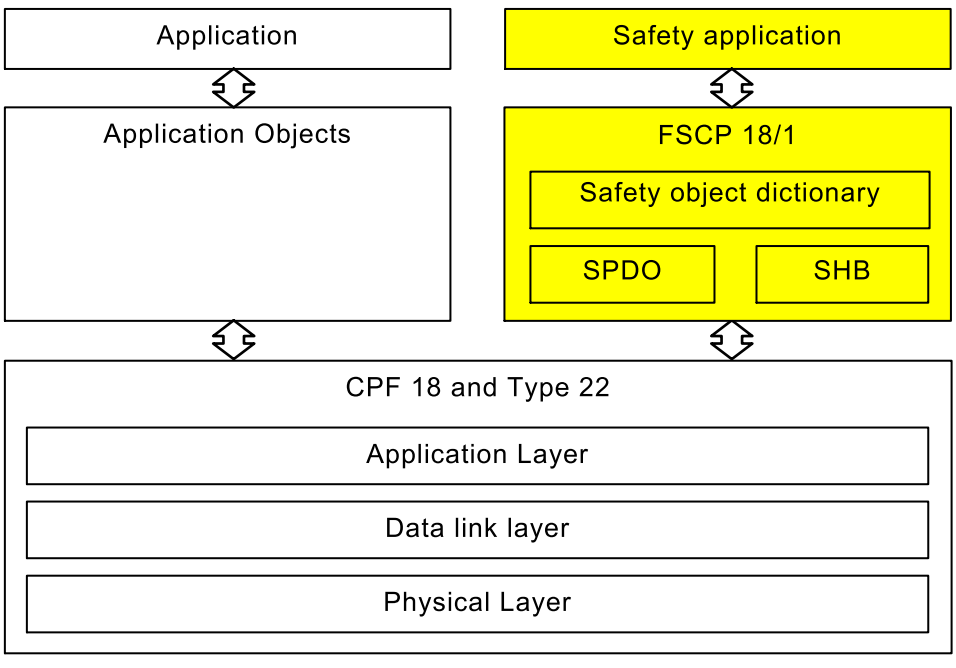


Figure 4 – FSCP 18/1 software architecture

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).

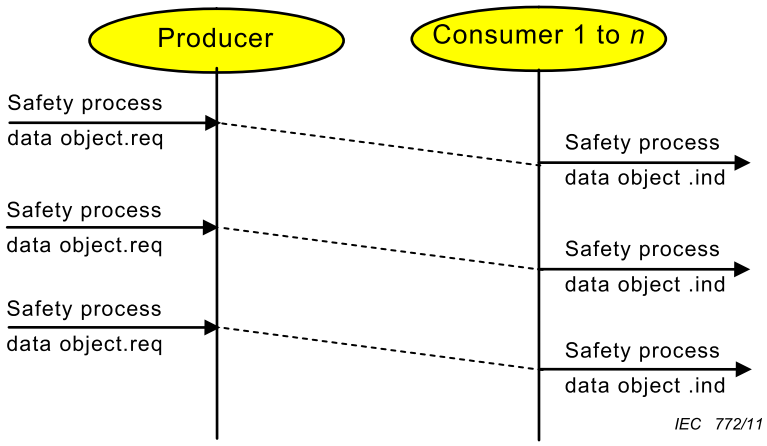


Figure 5 – SPDO interaction model

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.

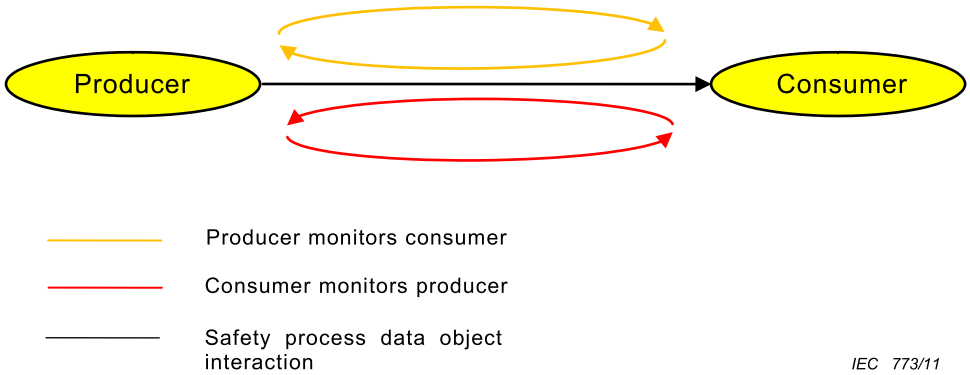


Figure 6 – SHB interaction model

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.

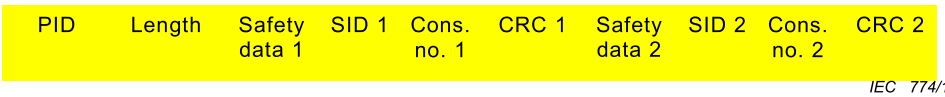


Figure 7 – Safety process data object structure

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, 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+2*n*+*m* to 12+2*n*+*m*	SID 2	Copy of SID 1
13+2*n*+*m* to 13+2*n*+2*m*-1	Consecutive number 2	Copy of consecutive number 1
14+2*n*+2*m* to 17+2*n*+2*m*	CRC 2	32 bit cyclic redundancy check covering data fields PID, 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 a 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, data, SID and consecutive number.

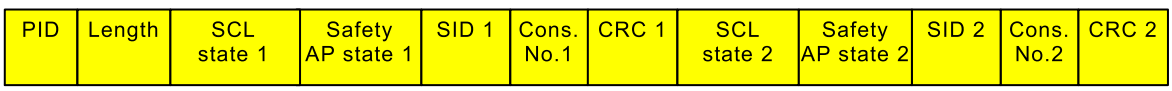
The polynomial 0x20044009 is used for calculating the CRCs. For details see 7.1.2.4 and 9.5.2.

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.



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 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, 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+*n*+*m* to 14+2*n*+*m*-1	Safety AP state 2	Copy of safety application process state 1
15+2*n*+*m* to 16+2*n*+*m*	SID 2	Copy of SID 1
17+2*n*+*m* to 17+2*n*+2*m*-1	Consecutive number 2	Copy of consecutive number 1
18+2*n*+2*m* to 21+2*n*+2*m*	CRC 2	32 bit cyclic redundancy check covering data fields PID, 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. 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.

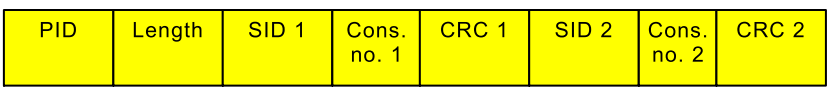


Figure 9 – Safety heartbeat response structure

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, SID 1 and consecutive number 1
11+*m* to 12+*m*	SID 2	Copy of SID 1
13+*m* to 13+2*m*-1	Consecutive number 2	Copy of consecutive number 1
14+2*m* to 17+2*m*	CRC 2	32 bit cyclic redundancy check covering data fields PID, 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 a 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, data, SID and consecutive number.

The polynomial 0x20044009 is used for calculating the CRCs. For details see 7.1.3.5 and 9.5.2.

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.

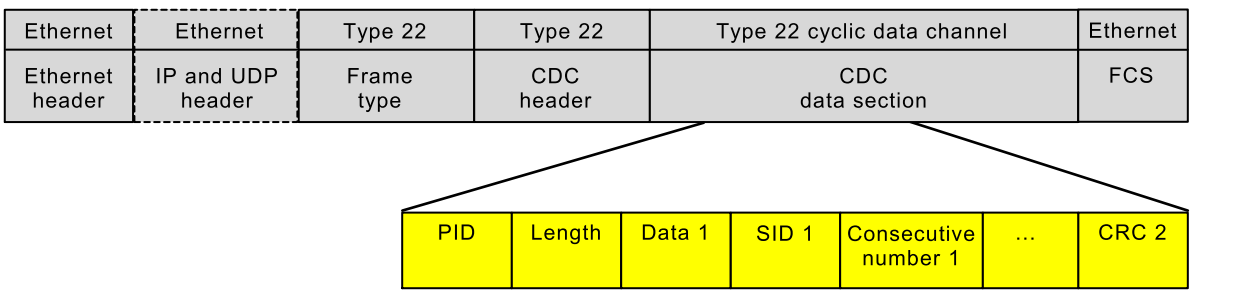


Figure 10 – Safety PDU for FSCP 18/1 embedded in a Type 22 CDC data section

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.

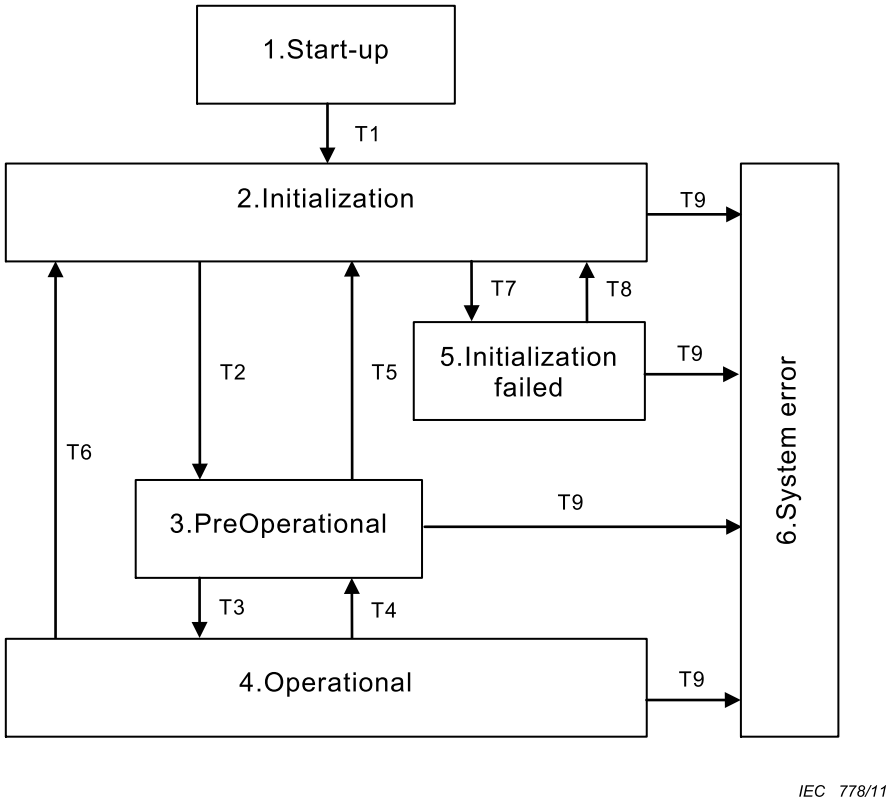


Figure 11 – SALMT state machine

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.

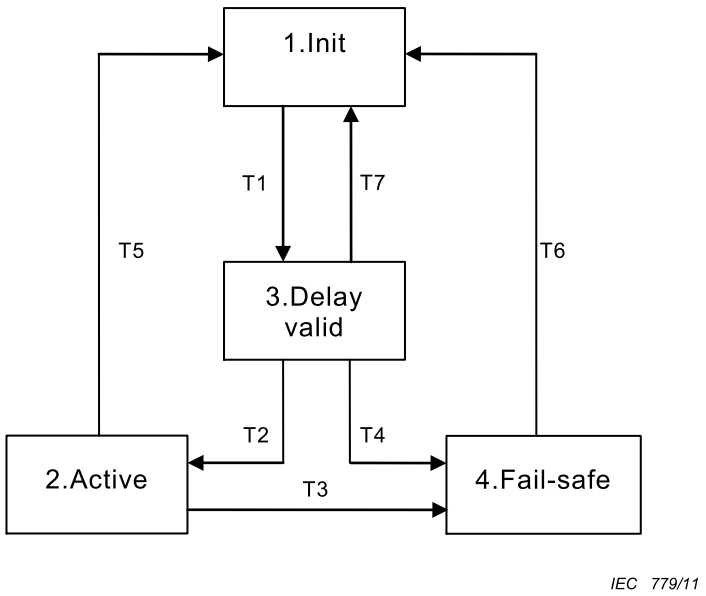


Figure 12 – RxSPDO state machine

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
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 timout multiplier cylces no SPDO has been received
SHB expected response	The SHB expected response timout 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 timout multiplier cycles no SHB from the consumer has been received
SHB timeout	SHB expected response timeout or SHB consumer timout

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.

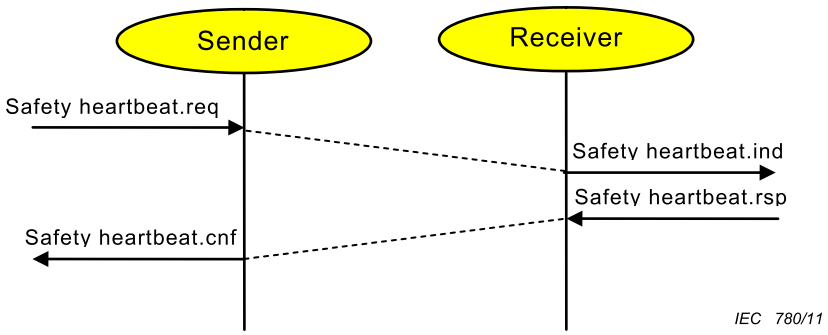


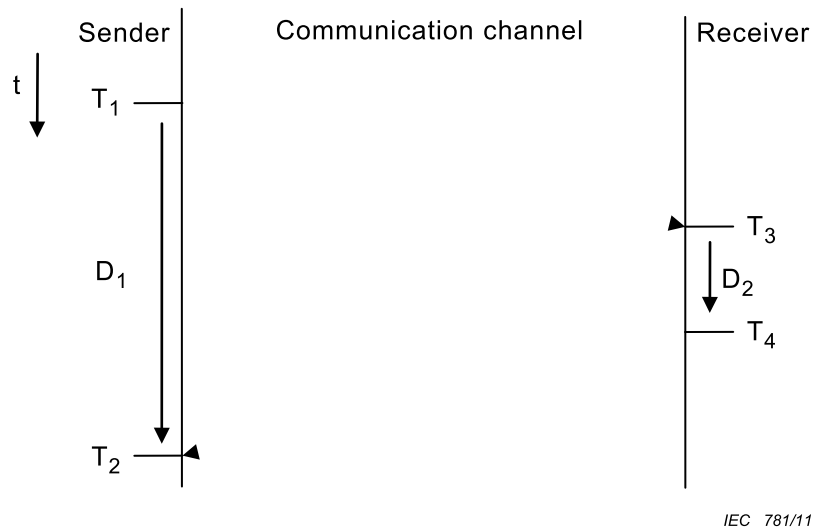
Figure 13 – Heartbeat procedure

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.



T_x Point in time x

D_x Resulting delay

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 1 ≤ T_{Timer} ≤ 0,1;
T_{TO}	Configurable tolerance for the RxSPDO timeout, index 0x121E per Table 15 with 0,01 ≤ T_{TO} ≤ 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.

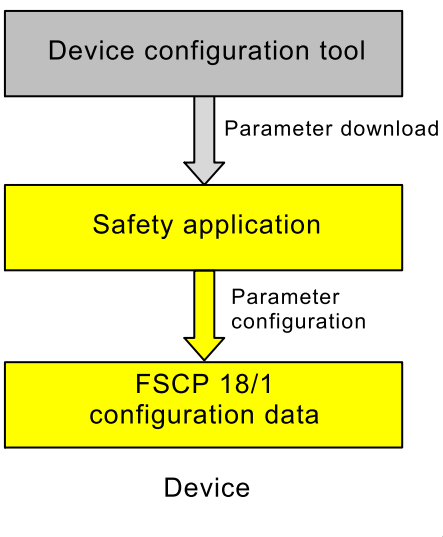


Figure 15 – Parameter handling

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	—	—
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.	Desription	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					

Index	Object	Name	Data type	Attr.	Desription	Cat.
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
0x1D00 to 0x1DFF	RECORD	RxSPDO mapping parameter	PDO MAPPING	FSF		M/O
0x1E00 to 0x1EFF	RECORD	TxSPDO communication 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 μs 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

8.2.2.6 Safety bus cycle times

The safety bus cycle time object is specified in Table 21. The safety bus cycle times are used to compute the timeout values for safety packets.

Table 21 – Safety bus cycle times

Attribute	Value
Index	0x1218
Name	Safety bus cycle times
Object type	ARRAY
Data type	Unsigned32
Category	Mandatory
Sub-index	0x00
Name	Number of supported entries
Data type	Unsigned8
Category	Mandatory
Access attribute	RO
SPDO mapping	No
Value range	0x01 to 0x02
Value	No
Sub-index	0x01
Name	Safety RTFN base cycle time
Description	Base cycle time for CDCN in μs
Data type	Unsigned32
Category	Conditional
Access attribute	FSF
SPDO mapping	No
Value range	No
Value	No
Sub-index	0x02
Name	Safety RTFL base cycle time
Description	Base cycle time for CDCL in μs
Data-type	Unsigned32
Category	Conditional
Access attribute	FSF
SPDO mapping	No
Value range	No
Value	No

8.2.2.7 SPDO timeout tolerance

The SPDO timeout tolerance object is specified in Table 22.

Table 22 – SPDO timeout tolerance

Attribute	Value
Index	0x121E
Name	SPDO timeout tolerance
Description	Specifies how much the SPDU timeout may be exceeded. Given in percent
Object type	VAR
Data type	Unsigned8
Category	Conditional
Access attribute	FSF
SPDO mapping	No
Value range	0x00 to 0xFF
Value	No

8.2.2.8 RxSPDO communication parameter

The receive SPDO communication parameter object is specified in Table 23.

Table 23 – Receive SPDO communication parameter

Attribute	Value
Index	0x1C00 – 0x1CFF
Name	Receive SPDO communication parameter
Object type	RECORD
Data type	PDO COMMUNICATION PARAMETER
Category	Conditional; Mandatory for each supported RxSPDO
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 in case of CDCL transmission
Data type	Unsigned32
Category	Conditional
Access attribute	FSF
SPDO mapping	No
Value range	0x01 to 0xFFFFFFFF
Value	No
Sub-index	0x02
Name	RTFN PID
Description	Packet identifier in case of CDCN transmission

Attribute	Value
Data type	Unsigned32
Category	Conditional
Access attribute	FSF
SPDO mapping	No
Value range	0x01 to 0xFFFFFFFF
Value	No
Sub-index	0x03
Name	SID
Description	Unique id of communication partner
Data type	Unsigned16
Category	Mandatory
Access attribute	FSF
SPDO mapping	No
Value range	No
Value	No
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 specified as cyclic
Data type	Unsigned16
Category	Conditional
Access attribute	FSF
SPDO mapping	No
Value range	0x0000 to 0xFFFF
Value	No
Sub-index	0x06
Name	Timeout multiplier
Description	Specifies how often the packet is expected
Data type	Unsigned16
Category	Optional
Access attribute	FSF
SPDO mapping	No
Value range	0x0000 to 0xFFFF
Value	No
Sub-index	0x07
Name	Cycle multiplier

Attribute	Value
Description	Specifies how often CP18/1 to CP18/2 gateway may write the SPDU to the CDCL communication channel. Mandatory if CDCL is used for transmission and CP18/1 to CP18/2 gateways are present. For all other cases it is not used
Data type	Unsigned16
Category	Conditional
Access attribute	FSF
SPDO mapping	No
Value range	0x01 to 0xFFFF
Value	No
Sub-index	0x08
Name	Cycle offset
Description	Cycle Offset (when is the SPDU written to CDCL channel). Mandatory if CDCL is used for transmission and CP18/1 to CP18/2 gateways are present. For all other cases it is not used
Data type	Unsigned16
Category	Conditional
Access attribute	FSF
SPDO mapping	No
Value range	0x00 to 0xFFFE
Value	No
Sub-index	0x09
Name	Number of allowed receives
Description	Maximum number that SPDU may be received
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	0x00 to 0x200
Value	No
Sub-index	0x0B
Name	IPv4 address
Data type	Unsigned32
Category	Conditional
Access attribute	FSF
SPDO mapping	No

Attribute	Value
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

8.2.2.9 TxSPDO communication parameter

The transmit SPDO communication parameter object is specified in Table 24.

Table 24 – Transmit SPDO communication parameter

Attribute	Value
Index	0x1E00 – 0x1EFF
Name	Transmit SPDO communication 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 in case of CDCL transmission
Data type	Unsigned32
Category	Conditional
Access attribute	FSF
SPDO mapping	No
Value range	0x01 to 0xFFFFFFFF
Value	No
Sub-index	0x02
Name	RTFN PID
Description	Packet identifier in case of CDCN transmission
Data type	Unsigned32
Category	Conditional

Attribute	Value
Access attribute	FSF
SPDO mapping	No
Value range	0x01 to 0xFFFFFFFF
Value	No
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 specified as 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 specified as 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.
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
Name	Cycle offset
Description	In which cycles it is transmitted.

Attribute	Value
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	Specifies how often the packet 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	0x00 to 0x200
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

8.2.2.10 SPDO mapping

8.2.2.10.1 SPDO mapping principle

The SPDO mapping parameters define the contents of a SPDO. A valid SPDO contains at least one and at most 254 safety application objects. The encoding of a mapping entry is specified in Table 25.

Table 25 – Mapping format

Bit	Name	Meaning
0 to 7	Length	Length of safety application object in bits
8 to 15	Sub-index	Sub-index of the safety application object to be mapped. The safety object dictionary is organized as a table with key (index, sub-index). This mapping specifies the lookup key for this application object.
16 to 31	Index	Index of the safety application object to be mapped

8.2.2.10.2 RxSPDO mapping parameter

The receive SPDO mapping parameter object is specified in Table 26.

Table 26 – Receive SPDO mapping parameter

Attribute	Value
Index	0x1D00 to 0x1DFF
Name	Receive SPDO mapping parameter
Description	Maps object from safety PDU to safety object dictionary. See Table 25
Object type	RECORD
Data type	PDO_MAPPING
Category	Conditional; Mandatory for each supported RxSPDO
Sub-index	0x00
Name	Number of mapped safety application objects
Data type	Unsigned8
Category	Mandatory
Access attribute	FSF
SPDO mapping	No
Value range	0x00 to 0xFE
Value	No
Sub-index	0x01 to 0xFE
Name	SPDO mapping for the nth safety application object to be mapped
Description	Specified in Table 25
Data type	Unsigned32
Category	Conditional depending on the number and size of objects to be mapped
Access attribute	FSF
SPDO mapping	No
Value range	No
Value	No

8.2.2.10.3 TxSPDO mapping parameter

The transmit SPDO mapping parameter object is specified in Table 27.

Table 27 – Transmit SPDO mapping parameter

Attribute	Value
Index	0x1E00 to 0x1EFF
Name	Transmit SPDO mapping parameter
Description	Maps object from safety object dictionary to safety PDU. See Table 25
Object type	RECORD
Data type	PDO_MAPPING
Category	Conditional; Mandatory for each supported TxSPDO
Sub-index	0x00
Name	Number of mapped safety application objects
Data type	Unsigned8
Category	Mandatory
Access attribute	FSF
SPDO mapping	No
Value range	0x01 to 0xFE
Value	No
Sub-index	0x01 to 0xFE
Name	SPDO mapping for the nth safety application object to be mapped
Description	Specified in Table 25
Data type	Unsigned32
Category	Conditional depending on the number and size of objects to be mapped
Access attribute	FSF
SPDO mapping	No
Value range	No
Value	No

8.2.3 Standardized device profile section

Safety application objects can be mapped within SPDOs. Safety application objects are located in the safety object dictionary area from 0x8000 to 0x9FFF. These objects are manufacturer and application specific.

9 System requirements

9.1 Indicators and switches

9.1.1 Indicator states and flash rates

The indicator states and flash rates are defined in Table 28. The times listed shall be met with a tolerance of less than ± 25 %.

Table 28 – Indicator states definiton

Indicator state	Definition
OFF	The indicator shall be constantly off
ON	The indicator shall be constantly on
BLINKING 1 Hz	The indicator shall turn on and off with a frequency of 1 Hz
BLINKING 2 Hz	The indicator shall turn on and off with a frequency of 2 Hz

9.1.2 Indicators

Devices which support FSCP 18/1 protocol should have a STATUS indicator. This indicator, typically LED, assists troubleshooting, visual inspection, maintenance and diagnosis of problems. If a device supports the STATUS indicator, this indicator shall comply with this specification. Additional indicators may be implemented.

The STATUS indicator shall show the status of the FSCP 18/1 communication. A single bicolor indicator (green/red) shall be used.

The STATUS indicator shall be labeled with “FS SNp”.

The STATUS indicator states are specified in Table 29.

Table 29 – STATUS indicator states

Indicator state	Definition
OFF	No safety process data communication is active
GREEN ON	All configured safety process data communication (SPDO) is active
GREEN BLINKING 1 Hz	At least one SPDO is active and at least one SPDO is not active
RED ON	Configuration is invalid or inconsistent
RED BLINKING 2 Hz	Internal error

9.1.3 Switches

There are no switches for FSCP 18/1.

9.2 Installation guidelines

Relevant installation guidelines are specified by IEC 61918.

9.3 Safety function response time

9.3.1 General

A safety function may consist of several components. To determine the safety function response time, the safety function is decomposed into the different components shown in Figure 16.

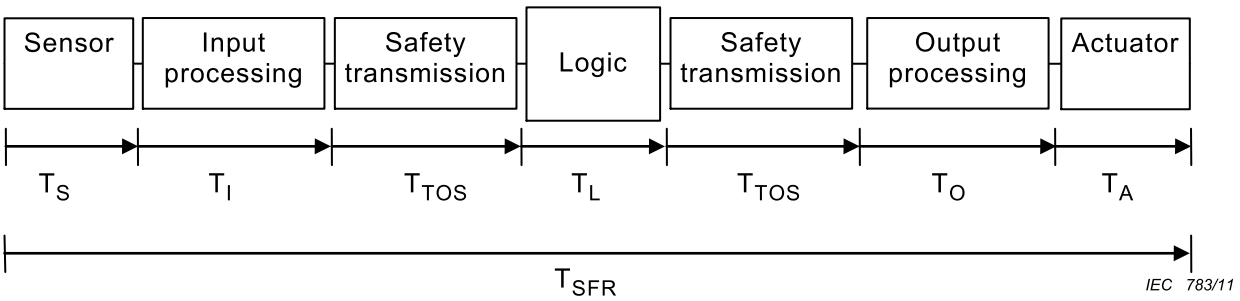


Figure 16 – Safety response time components

The safety function channel consists of a sensor (for example light curtain or emergency stop button) to detect the actuation of the safety function. This sensor converts the physical signal in an electrical signal. This electrical signal is connected to an input device (for example, functional safety input module), which converts the electrical signal in logical input information. The logical input information is transmitted to the safety logic controller via the safety communication system. Safety logic controller combines the logical input information to logical output information, which is transmitted to an output device (for example functional safety output module) via the safety communication system. Logical output information is converted to a physical output signal which is connected to an actuator. This actuator performs the physical reaction. Each component is described by a characteristic time behavior.

The following general assumptions are applied for further considerations.

- All components of the safety function channel work asynchronous.
- All components of the safety function channel are described by a worst case processing or response time which is gueranteed under non error conditions.
- For safety reasons, every component has its superposed timeout timer (T_{TOi}).
- In order to calculate the safety function response time one error or failure shall be assumed in that signal path, which contributes the maximum difference time between its timeout and its worst case processing or response time.

The characteristic times of the devices sensor, input, logic, output and actuator are outside the scope of this standard. Meaningful information for these characteristic values should be taken from component specifications. Each device shall provide these values as part of their device properties.

9.3.2 Determination of FSCP 18/1 time expectation behavior

FSCP 18/1 defines a configurable time expectation behavior (timeout) for the delivery of safety process data at the receiver side of a communication relation. This behavior is implemented by communication timeout T_{TOS}.

For the safety function channel two safety transmissions are necessary. The logic and the output processing component operate as a receiver and implement the time expectation behavior. The calculation of T_{TOS} is described in Equation (2).

$$T_{TOS} = T_{cycle} + \Delta T \qquad (2)$$

The SHB does not influence T_{TOS} as it is only required to synchronize the system clocks. In case the safety heart beat detects unacceptable delays, then the fail safe state is activated (see 7.3).

9.3.3 Calculation of the worst case safety function response time

The basic safety function channel for the calculation of the worst case safety function is shown in Figure 16.

The safety function response time can be calculated according to Equation (3).

To get the worst case for the safety function response time, one error or failure shall be assumed in the safety function channel. It contributes the maximum difference between its worst case delay time and its timeout time.

$$T_{SFR} = T_S + T_I + T_T + T_L + T_T + T_O + T_A + \max_{i=S,I,...A}(T_{TOi} - T_i) \quad (3)$$

NOTE Index “i” identifies components S, I, T, L, O and A in Equation (3).

System manufacturers shall provide their individual adapted calculation method if necessary.

9.4 Duration of demands

The duration of demand by the safety-related application to the safety communication layer may be present as long as or longer than the process safety time or the FSCP 18/1 timeout time (T_{TO}).

9.5 Constraints for calculation of system characteristics

9.5.1 Safety related constraints

9.5.1.1 General

The boundary conditions and constraints for the safety assessment of FSCP 18/1 and for the relevant calculations of residual error rate are described within the following clauses.

9.5.1.2 Number of information sinks

The number of producing and consuming devices for a FSCP 18/1 network is limited to 512 devices. The number of information sinks for a 1:*n* relationship is limited to 511 consuming devices.

9.5.1.3 Message rate limit

The message rate shall not exceed 1 000 safety messages per second. The number of producing devices and the cycle time has to be considered to not exceed the message rate limit as shown in Equation (4) to (6).

$$MR_{SPDO} = \sum_{I \in SPDO} \frac{1\,000\,000 \times NS_I}{CM_I \times T_{BC}} \quad (4)$$

$$MR_{SHB} = \sum_{D1 \in devices} \left[\sum_{\substack{D2 \in devices \\ D2 \neq D1}} \frac{1\,000\,000 \times NS_{D1} \times 2}{CM_{D1} \times T_{BC}} \right] \quad (5)$$

$$MR = MR_{SPDO} + MR_{SHB} \quad (6)$$

where

CM_{D1}	is the safety producer heartbeat parameter (Index: 0x1217, Sub-index: 0x07, cycle multiplier) sent by device D1 (see Table 20);
CM_{I}	is the Transmit SPDO communication parameter (Index: 0x1E00 - 0x1EFF, Sub-index: 0x07, Cycle multiplier) for SPDOI (see Table 24);
NS_{D1}	is the safety producer heartbeat parameter (Index: 0x1217, Sub-index: 0x09, Number of sends) sent by device D1 (see Table 20);
NS_{I}	is the Transmit SPDO communication parameter (Index: 0x1E00 - 0x1EFF, Sub-index: 0x09, Number of sends) for SPDOI (see Table 24);
MR	is the Total message rate;
MR_{SHB}	is the Message rate for SHBs;
MR_{SPDO}	is the Message rate for SPDOs;
T_{BC}	is the safety bus cycle times. The parameter is depending if CP 18/1 (Index: 0x1218, Sub-index 0x02, Safety RTFL base cycle time) or CP 18/2 (Index: 0x1218, Sub-index: 0x01, Safety RTFN base cycle time) is used (see Table 21).

9.5.1.4 Message size

The message size of one safety PDU consisting of data fields as shown in Figure 17 is restricted from 0 to 128 octets

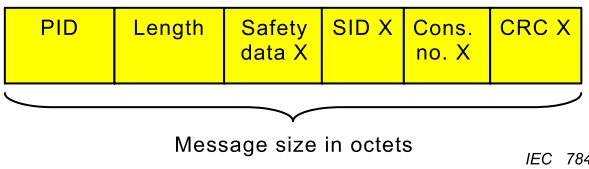


Figure 17 – Considered data fields for message size calculation

9.5.1.5 Bit error rate

The maximum bit error rate shall not exceed 0,01.

9.5.2 Probabilistic considerations

The data integrity checking mechanism of the FSCP 18/1 is totally independent from the mechanisms of the underlying communication system, which then is called a "black channel".

Figure 18 is showing the diagrams of residual error probabilities for the used 32-bit polynomial (minimum Hamming Distance 6). The diagram is for data lengths of 128 octets as specified in 9.5.1.4 including the CRC signature and incorporating the overall safety PDU structure as described in 7.1. The resulting PFH of the communication channel has been calculated to be less than or equal to 10^{-9}. This level equals to 5,43 x 10^{-19} for the residual error probability of one PDU as shown in Figure 18. In order to achieve these levels, the data integrity checking mechanism is mandatory (see 7.1.1.2)

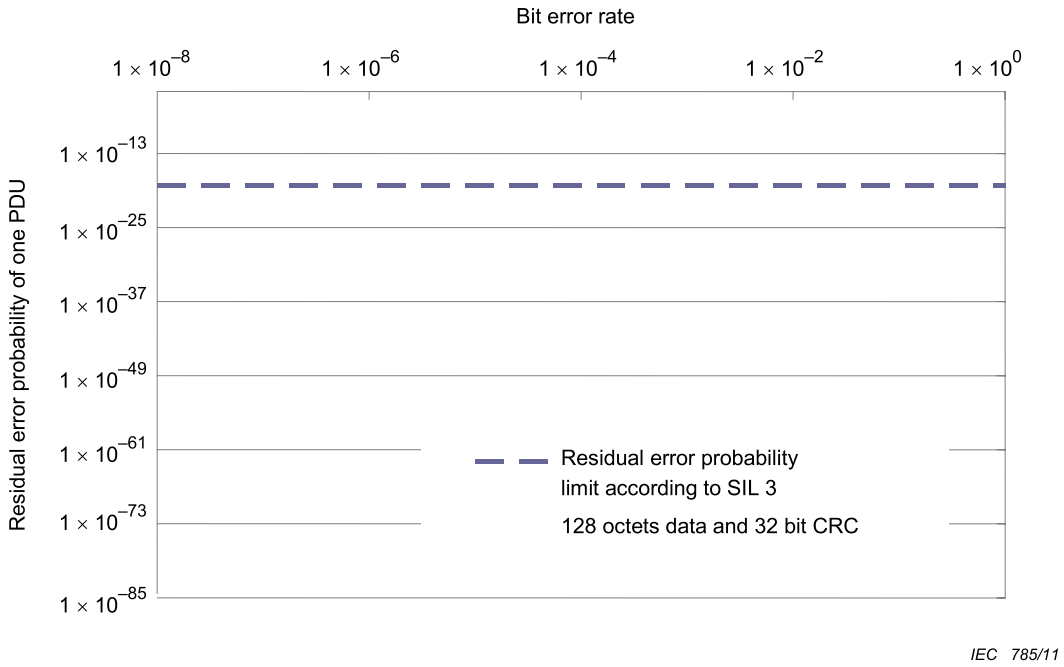


Figure 18 – Residual error rate

9.6 Maintenance

There are no special maintenance requirements for this protocol.

9.7 Safety manual

The manufacturer of the safety device shall provide a safety manual according to the requirements of IEC 61508-2 with the device. Besides the requirements listed in IEC 61508-2 the following information shall be given:

- Manufacturer name and adress;
- Worst case time T_i;
- Timeout time T_{TOi};
- Probability of failure on demand PFH;
- Safety integrity level SIL;
- Proof test interval T_1 (per IEC 61508-6) and/or Mission T_m (per ISO 13849-1);
- Supported protocol version(s) (see 7.1.3.4) unless only protocol version 1 is supported.

NOTE Times can depend on the individual safety functions and operating modes.

10 Assessment

It is highly recommended that implementers of FSCP 18/1 obtain verification from an independent competent body for all functional safety aspects of the product for both, the protocol and any application. It is highly recommended that implementers of FSCP 18/1 obtain proof that a suitable conformance test has been performed by an independent competent body.

The manufacturer of a safety product is responsible for the correct implementation of the safety communication layer technology, the correctness and completeness of the product documentation and information. The complete information is available in [46].

Annex A
(informative)

Additional information
for functional safety communication profiles of CPF 18

There is no additional information for this FSCP.

Annex B
(informative)

Information for assessment of the functional safety communication profiles of CPF 18

Information about test laboratories which test and validate the conformance of FSCP 18/1 products with IEC 61784-3-18 can be obtained from the National Committees of the IEC or from the following organization:

Safety Network International e.V.
Robert-Bosch-Str.30
73760 Ostfildern
GERMANY

Phone: +49 711 3409 118
Fax: +49 711 3409 449
e-mail: info@safety-network.de
URL: www.safety-network.de

Bibliography

[1] IEC 60050 (all parts), *International Electrotechnical Vocabulary*

NOTE See also the IEC Multilingual Dictionary – Electricity, Electronics and Telecommunications (available on CD-ROM and at <http://www.electropedia.org>).

[2] IEC 60204-1, *Safety of machinery – Electrical equipment of machines – Part 1: General requirements*

[3] IEC/TS 61000-1-2, *Electromagnetic compatibility (EMC) – Part 1-2: General – Methodology for the achievement of the functional safety of electrical and electronic equipment with regard to electromagnetic phenomena*

[4] IEC 61131-6[5], *Programmable controllers – Part 6: Functional safety*

[5] IEC 61158 (all parts), *Industrial communication networks – Fieldbus specifications*

[6] IEC 61326-3-1, *Electrical equipment for measurement, control and laboratory use – EMC requirements – Part 3-1: Immunity requirements for safety-related systems and for equipment intended to perform safety related functions (functional safety) – General industrial applications*

[7] IEC 61326-3-2, *Electrical equipment for measurement, control and laboratory use – EMC requirements – Part 3-2: Immunity requirements for safety-related systems and for equipment intended to perform safety related functions (functional safety) – Industrial applications with specified electromagnetic environment*

[8] IEC 61496 (all parts), *Safety of machinery – Electro-sensitive protective equipment*

[9] IEC 61508-1:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements*

[10] IEC 61508-4:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations*

[11] IEC 61508-5:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 5: Examples of methods for the determination of safety integrity levels*

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

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

[14] IEC/PWI 61784-4[6], *Industrial communication networks – Profiles – Part 4: Secure communications for fieldbuses*

[15] IEC 61784-5 (all parts), *Industrial communication networks – Profiles – Part 5: Installation of fieldbuses – Installation profiles for CPF x*

[16] IEC 61800-5-2, *Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional*

[17] IEC/TR 62059-11, *Electricity metering equipment – Dependability – Part 11: General concepts*

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

[19] IEC/TR 62210, *Power system control and associated communications – Data and communication security*

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

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

[22] IEC 62443 (all parts), *Industrial communication networks – Network and system security*

---

5 In preparation.

6 Under consideration.

[23] ISO/IEC Guide 51:1999, *Safety aspects – Guidelines for their inclusion in standards*

[24] ISO/IEC 2382-14, *Information technology – Vocabulary – Part 14: Reliability, maintainability and availability*

[25] ISO/IEC 2382-16, *Information technology – Vocabulary – Part 16: Information theory*

[26] ISO/IEC 7498 (all parts), *Information technology – Open Systems Interconnection – Basic Reference Model*

[27] ISO 10218-1, *Robots for industrial environments – Safety requirements – Part 1: Robot*

[28] ISO 12100-1, *Safety of machinery – Basic concepts, general principles for design – Part 1: Basic terminology, methodology*

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

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

[31] ISO 14121, *Safety of machinery – Principles of risk assessment*

[32] ANSI/ISA-84.00.01-2004 (all parts), *Functional Safety: Safety Instrumented Systems for the Process Industry Sector*

[33] VDI/VDE 2180 (all parts), *Safeguarding of industrial process plants by means of process control engineering*

[34] GS-ET-26[7], *Grundsatz für die Prüfung und Zertifizierung von Bussystemen für die Übertragung sicherheitsrelevanter Nachrichten*, May 2002. HVBG, Gustav-Heinemann-Ufer 130, D-50968 Köln ("*Principles for Test and Certification of Bus Systems for Safety relevant Communication*")

[35] ANDREW S. TANENBAUM, *Computer Networks*, 4th Edition, Prentice Hall, N.J., ISBN-10:0130661023, ISBN-13: 978-0130661029

[36] W. WESLEY PETERSON, *Error-Correcting Codes*, 2nd Edition 1981, MIT-Press, ISBN 0-262-16-039-0

[37] BRUCE P. DOUGLASS, *Doing Hard Time*, 1999, Addison-Wesley, ISBN 0-201-49837-5

[38] *New concepts for safety-related bus systems*, 3rd International Symposium "Programmable Electronic Systems in Safety Related Applications ", May 1998, from Dr. Michael Schäfer, BG-Institute for Occupational Safety and Health.

[39] DIETER CONRADS, *Datenkommunikation*, 3rd Edition 1996, Vieweg, ISBN 3-528-245891

[40] German IEC subgroup DKE AK 767.0.4: *EMC and Functional Safety*, Spring 2002

[41] NFPA79 (2002), *Electrical Standard for Industrial Machinery*

[42] GUY E. CASTAGNOLI, *On the Minimum Distance of Long Cyclic Codes and Cyclic Redundancy-Check Codes*, 1989, Dissertation No. 8979 of ETH Zurich, Switzerland

[43] GUY E. CASTAGNOLI, STEFAN BRÄUER, and MARTIN HERRMANN, *Optimization of Cyclic Redundancy-Check Codes with 24 and 32 Parity Bits*, June 1993, IEEE Transactions On Communications, Volume 41, No. 6

[44] SCHILLER F and MATTES T: *An Efficient Method to Evaluate CRC-Polynomials for Safety-Critical Industrial Communication*, Journal of Applied Computer Science, Vol. 14, No 1, pp. 57-80, Technical University Press, Łódź,Poland, 2006

[45] SCHILLER F and MATTES T: *Analysis of CRC-polynomials for Safety-critical Communication by Deterministic and Stochastic Automata*, 6th IFAC Symposium on Fault Detection, Supervision and Safety for Technical Processes, SAFEPROCESS 2006, pp. 1003-1008, Beijing, China, 2006

[46] *Technical Guideline Integration*, V2.0, December 2008, Safety Network International e. V. Ostfildern, Germany

---

7 GS-ET-26 has served as one of the starting points for this part. It is currently undergoing a major revision.

[47] *CANopen Application Layer and Communication Profile, CiA Draft Standard 301*, Version 4.02, 13 February 2002, CAN in Automation e.V., Nürnberg, Germany

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

RÉSEAUX DE COMMUNICATION INDUSTRIELS – PROFILS

Partie 3-18: Bus de terrain de sécurité fonctionnelle – Spécifications supplémentaires pour le CPF 18

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.

DÉGAGEMENT DE RESPONSABILITÉ
Cette version consolidée n'est pas une Norme IEC officielle, elle a été préparée par commodité pour l'utilisateur. Seules les versions courantes de cette norme et de son(ses) amendement(s) doivent être considérées comme les documents officiels.

Cette version consolidée de l'IEC 61784-3-18 porte le numéro d'édition 1.1. Elle comprend la première édition (2011-04) [documents 65C/639/FDIS et 65C/649/RVD] et son amendement 1 (2016-07) [documents 65C/851/FDIS et 65C/854/RVD]. Le contenu technique est identique à celui de l'édition de base et à son amendement.

Cette version Finale ne montre pas les modifications apportées au contenu technique par l'amendement 1. Une version Redline montrant toutes les modifications est disponible dans cette publication.

La Norme internationale IEC 61784-3-18 a été établie par le sous-comité 65C: Réseaux de communication industriels, du comité d'études 65 de l'IEC: Mesure, commande et automation dans les processus industriels.

Cette publication a été rédigée selon les Directives ISO/IEC, Partie 2.

Une liste de toutes les parties de la série IEC 61784-3, publiée sous le titre général *Réseaux de communication industriels – Profils – Bus de terrain de sécurité fonctionnelle*, est disponible sur le site Web de l'IEC.

Le comité a décidé que le contenu de la publication de base et de son amendement ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous "http://webstore.iec.ch" dans les données relatives à la publication recherchée. A cette date, la publication sera

- reconduite,
- supprimée,
- remplacée par une édition révisée, ou
- amendée.

IMPORTANT – Le logo *"colour inside"* qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

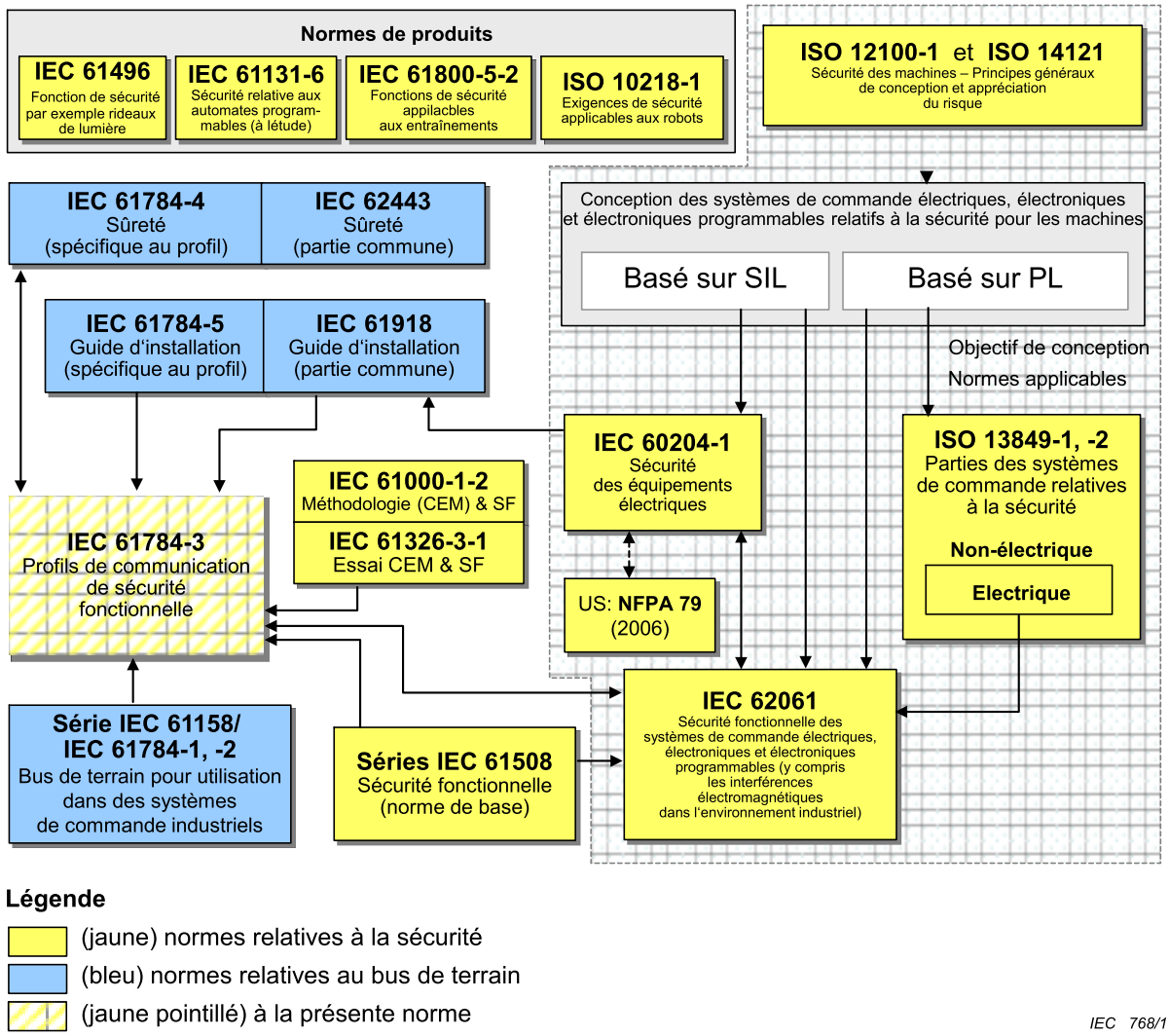
0 Introduction

0.1 Généralités

La norme IEC 61158 relative aux bus de terrain, ainsi que ses normes associées IEC 61784-1 et IEC 61784-2, définissent un ensemble de protocoles de communication qui assurent la commande répartie d'applications automatisées. La technologie de bus de terrain est désormais reconnue et bien éprouvée. Ainsi de nombreuses améliorations des bus de terrain se développent pour traiter de domaines non encore normalisés tels que les applications en temps réel relatives à la sécurité et à la sûreté.

La présente norme définit les principes pertinents applicables aux communications en termes de sécurité fonctionnelle en référence à la série IEC 61508, et spécifie plusieurs couches de communication de sécurité (profils et protocoles correspondants) basés sur les profils de communication et les couches de protocoles de l'IEC 61784-1, l'IEC 61784-2 et la série IEC 61158. Elle ne couvre pas les aspects relatifs à la sécurité électrique et à la sécurité intrinsèque.

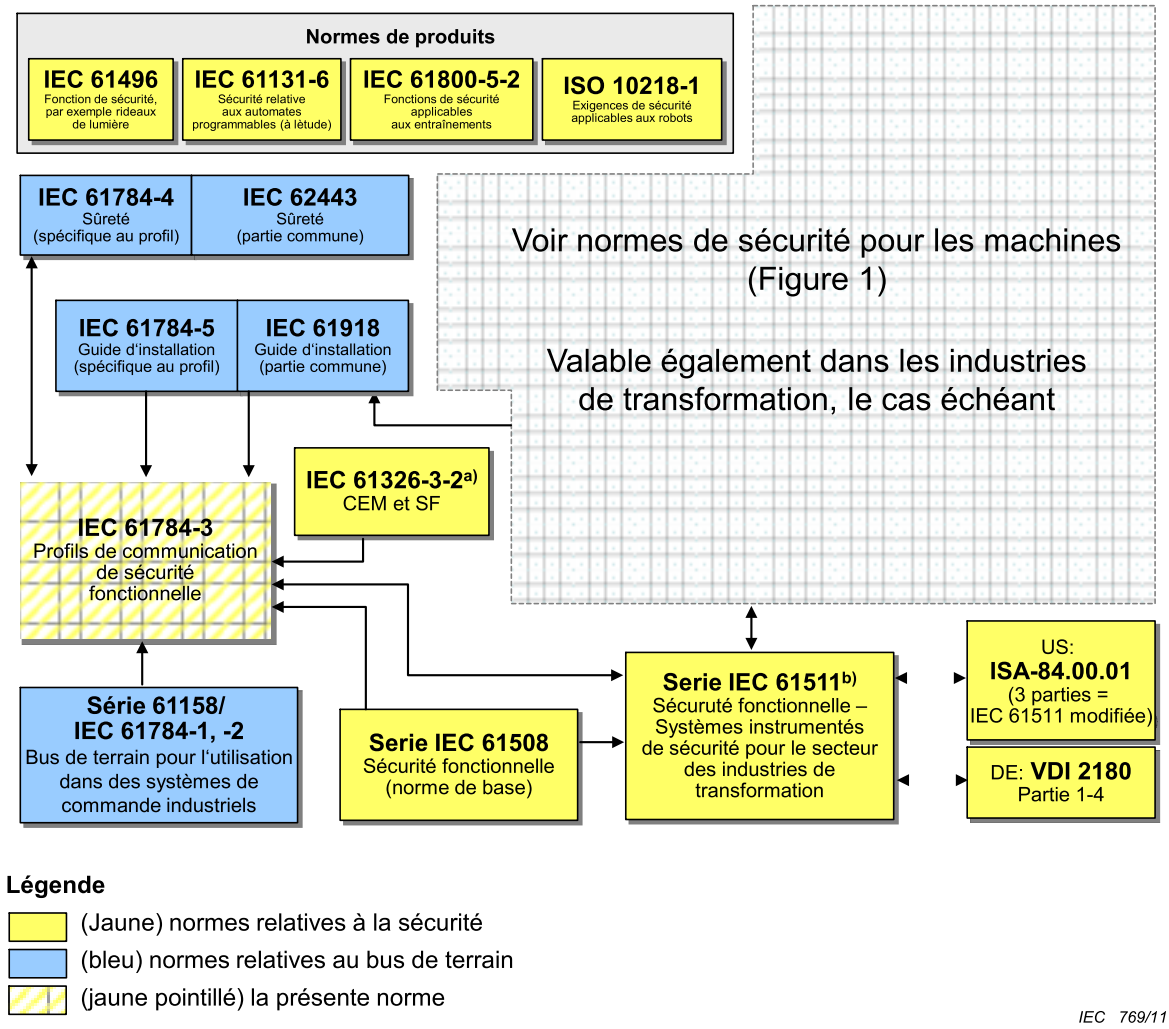
La Figure 1 illustre les relations entre la présente norme et les normes pertinentes relatives à la sécurité et au bus de terrain dans un environnement de machines.



NOTE Les paragraphes 6.7.6.4 (haute complexité) et 6.7.8.1.6 (faible complexité) de l'IEC 62061 spécifient la relation entre PL (catégorie) et SIL.

Figure 1 – Relations entre l'IEC 61784-3 et d'autres normes (machines)

La Figure 2 illustre les relations entre la présente norme et les normes pertinentes relatives à la sécurité et au bus de terrain dans un environnement de transformation.



a Pour des environnements électromagnétiques spécifiés, sinon IEC 61326-3-1.

b EN ratifiée.

Figure 2 – Relations entre l'IEC 61784-3 et d'autres normes (transformation)

Les couches de communication de sécurité mises en œuvre dans le cadre de systèmes relatifs à la sécurité conformément à la série IEC 61508, assurent la confiance nécessaire à accorder à la transmission de messages (information) entre deux participants ou plus sur un bus de terrain dans un système relatif à la sécurité, ou une fiabilité suffisante dans le comportement de sécurité en cas d'erreurs ou de défaillances du bus de terrain.

Les couches de communication de sécurité spécifiées dans la présente norme permettent de garantir cette assurance en utilisant un bus de terrain dans des applications nécessitant une sécurité fonctionnelle jusqu'au niveau d'intégrité de sécurité (SIL) spécifié par son profil de communication de sécurité fonctionnelle correspondant.

La revendication du SIL qui en résulte pour un système dépend de la mise en œuvre du profil de communication de sécurité fonctionnelle retenu au sein du système – la mise en œuvre du profil de communication de sécurité fonctionnelle dans un appareil normal ne suffit pas à le qualifier d'appareil de sécurité.

La présente norme décrit:

– les principes de base de mise en œuvre des exigences de la série IEC 61508 pour les communications de données relatives à la sécurité, y compris les défauts de transmission potentiels, les mesures correctives et les considérations concernant l'intégrité des données;
– la description individuelle des profils de sécurité fonctionnelle pour plusieurs familles de profils de communication dans les IEC 61784-1 et IEC 61784-2;
– les extensions de la couche de sécurité aux sections relatives au service et aux protocoles de communication de la série IEC 61158.

0.2 Déclaration de propriété

La Commission Electrotechnique Internationale (IEC) attire l'attention sur le fait qu'il est déclaré que la conformité avec les dispositions du présent document peut impliquer l'utilisation de brevets concernant les profils de communication de sécurité fonctionnelle pour la famille 18 comme suit, où la notation [xx] désigne le détenteur des droits de propriété:

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

L'IEC ne prend pas position quant à la preuve, la validité et la portée de ces droits de propriété.

Le détenteur de ces droits de propriété a donné l'assurance à l'IEC qu'il consent à négocier des licences avec des demandeurs du monde entier, soit sans frais soit à des termes conditions raisonnables et non discriminatoires. A ce propos, la déclaration du détenteur des droit de propriété est enregistrée à l'IEC.

Des informations peuvent être obtenues auprès de:

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

L'attention est d'autre part attirée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété autres que ceux mentionnés ci-dessus. L'IEC ne saurait être tenue pour responsable de l'identification de ces droits de propriété en tout ou en partie.

L'ISO (www.iso.org/patents) et l'IEC (http://www.iec.ch/tctools/patent_decl.htm) maintiennent des bases des données, consultables en ligne, des droits de propriété pertinents à leurs normes. Les utilisateurs sont encourages à consulter ces bases de données pour obtenir l'information la plus récente concernant les droits de propriété.

RÉSEAUX DE COMMUNICATION INDUSTRIELS – PROFILS

Partie 3-18: Bus de terrain de sécurité fonctionnelle – Spécifications supplémentaires pour le CPF 18

1 Domaine d'application

La présente partie de la série IEC 61784-3 spécifie une couche de communication relative à la sécurité (services et protocole) fondée sur le CPF 18 de l'IEC 61784-2 et le type 22 de l'IEC 61158. Elle identifie les principes applicables aux communications de sécurité fonctionnelle définies dans l'IEC 61784-3, et appropriés à cette couche de communication de sécurité.

NOTE 1 Elle ne couvre pas les aspects relatifs à la sécurité électrique et à la sécurité intrinsèque. La sécurité électrique concerne les dangers tels que les chocs électriques. La sécurité intrinsèque concerne les dangers associés aux atmosphères explosibles.

La présente partie[1] définit les mécanismes de transmission des messages propres à la sécurité entre les participants d'un réseau réparti, en utilisant la technologie de bus de terrain conformément aux exigences de la série IEC 61508[2] concernant la sécurité fonctionnelle. Ces mécanismes peuvent être utilisés dans diverses applications industrielles, telles que la commande de processus, l'usinage automatique et les machines.

La présente partie fournit des lignes directrices tant pour les développeurs que pour les évaluateurs d'appareils et systèmes conformes.

NOTE 2 La revendication du SIL qui résulte pour un système dépend de la mise en œuvre du profil de communication de sécurité fonctionnelle retenu au sein du système – la mise en œuvre du profil de communication de sécurité fonctionnelle, conforme à la présente partie, dans un appareil normal ne suffit pas à le qualifier de appareil de sécurité.

2 Références normatives

Les documents de référence suivants sont indispensables pour l'application du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

IEC 61158-3-22, *Industrial communication networks – Fieldbus specifications – Part 3-22: Data-link layer service definition – Type 22 elements* (disponible uniquement en anglais)

IEC 61158-4-22, *Industrial communication networks – Fieldbus specifications – Part 4-22: Data-link layer protocol specification – Type 22 elements* (disponible uniquement en anglais)

IEC 61158-5-22, *Industrial communication networks – Fieldbus specifications – Part 5-22: Application layer service definition – Type 22 elements* (disponible uniquement en anglais)

---

1 Dans les pages suivantes de la présente norme, "la présente partie" se substitue à "cette partie de la série IEC 61784-3".

2 Dans les pages suivantes de la présente norme, "IEC 61508" se substitue à "série IEC 61508".

IEC 61158-6-22, *Industrial communication networks – Fieldbus specifications – Part 6-22: Application layer protocol specification – Type 22 elements* (disponible uniquement en anglais)

IEC 61508 (toutes parties), *Sécurité fonctionnelle des systèmes électriques/électroniques/ électroniques programmables relatifs à la sécurité*

IEC 61508-2:2010, *Sécurité fonctionnelle des systèmes électriques/électroniques/ électroniques programmables relatifs à la sécurité – Partie 2: Exigences pour les systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité*

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

IEC 61784-3:2010, *Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions* (disponible uniquement en anglais)

IEC 61918, *Industrial communication networks – Installation of communication networks in industrial premises* (disponible uniquement en anglais)

ISO/IEC 10731, *Technologies de l'information – Interconnexion de systèmes ouverts – Modèle de référence de base – Conventions pour la définition des services OSI*

3 Termes, définitions, symboles, abréviations et conventions

3.1 Termes et définitions

Pour les besoins du présent document, les termes et définitions suivants s'appliquent.

3.1.1 Termes et définitions communs

3.1.1.1
disponibilité
probabilité, pour un système automatisé, qu'il ne se produise pas de conditions opérationnelles non satisfaisantes, telles que la perte de production, pendant une période donnée

3.1.1.2
canal noir
canal de communication sans preuve existante de conception ou de validation conformément à l'IEC 61508

3.1.1.3
canal de communication
connexion logique entre deux points limites d'un *système de communication*

3.1.1.4
système de communication
disposition de matériels, logiciels et vecteurs de propagation destinée à permettre la transmission de *messages* (couche d'application définie dans l'ISO/IEC 7498) d'une application à une autre

3.1.1.5
connexion
liaison logique entre deux objets d'application d'appareils identiques ou différents

3.1.1.6
contrôle de redondance cyclique (CRC)
<valeur> donnée redondante déduite, et enregistrée ou transmise simultanément, d'un bloc de données afin de détecter toute corruption des données

<méthode> procédure utilisée pour calculer les données redondantes

NOTE 1 Les termes « code CRC » et « signature CRC », et les étiquettes telles que CRC1, CRC2, peuvent également être utilisés dans la présente norme pour se référer aux données redondantes.

NOTE 2 Voir également [35], [36]]3.

3.1.1.7
erreur
écart ou discordance entre une valeur ou une condition calculée, observée ou mesurée, et la valeur ou la condition vraie, prescrite ou théoriquement correcte

[IEC 61508-4:2010], [IEC 61158]

NOTE 1 Les erreurs peuvent être causées par des erreurs de conception du matériel/logiciel et/ou des informations altérées du fait de perturbations électromagnétiques et/ou autres effets.

NOTE 2 Les erreurs ne produisent nécessairement pas une *défaillance* ou une *panne*.

3.1.1.8
défaillance
cessation de l'aptitude d'une unité fonctionnelle à accomplir une fonction requise ou fonctionnement d'une unité fonctionnelle d'une toute autre manière que celle requise

NOTE 1 La définition de l'IEC 61508-4 est identique avec des notes complémentaires.

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

NOTE 2 Une défaillance peut être causée par une *erreur* (par exemple, problème de conception matérielle/logicielle ou rupture de message).

3.1.1.9
panne
condition anormale susceptible de provoquer la réduction, ou la perte, de capacité d'une unité fonctionnelle à accomplir une fonction requise

NOTE Le VEI 191-05-01 définit la « panne » comme un état caractérisé par l'incapacité à accomplir une fonction requise, à l'exclusion de l'incapacité au cours de la période de maintenance préventive ou autres actions planifiées, ou du fait de l'absence de ressources externes.

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

3.1.1.10
bus de terrain
système de communication basé sur le transfert de données en série et utilisé dans des applications d'automatisation industrielle ou de commande de processus

3.1.1.11
trame
synonyme discrédité de DLPDU

3.1.1.12
séquence de contrôle de trame (FCS)
données redondantes issues d'un bloc de données d'une DLPDU (trame), utilisant une fonction de hachage, et enregistrées ou transmises avec le bloc de données, afin de déterminer l'altération des données

---

3 Les chiffres entre crochets font référence à la Bibliographie.

NOTE 1 Il est possible de calculer une FCS à l'aide, par exemple, d'un CRC ou d'une autre fonction de hachage.

NOTE 2 Voir également [35], [36].

3.1.1.13
fonction de hachage
fonction (mathématique) de mise en correspondance des valeurs d'un ensemble (éventuellement) très grand de valeurs en une plage de valeurs (habituellement) plus petite

NOTE 1 Les fonctions de hachage peuvent être utilisées pour déterminer l'altération des données.

NOTE 2 Les fonctions de hachage courantes incluent la parité, la somme de contrôle ou le CRC.

[IEC/TR 62210, modifiée]

3.1.1.14
danger
état ou ensemble de conditions d'un système qui, avec d'autres conditions associées, entraîne inévitablement un préjudice pour les personnes, les biens ou l'environnement

3.1.1.15
message
série ordonnée d'octets destinée à communiquer des informations

[ISO/IEC 2382-16.02.01, modifiée]

3.1.1.16
collecteur de messages
partie d'un *système de communication* destiné à recevoir des *messages*

[ISO/IEC 2382-16.02.03]

3.1.1.17
source de messages
partie d'un *système de communication* destiné à envoyer des *messages*

[ISO/IEC 2382-16.02.02]

3.1.1.18
déclenchement de nuisance
déclenchement parasite sans effet préjudiciable

NOTE Les erreurs anormales internes peuvent être générées dans des systèmes de communication tels que des systèmes de transmission par ondes radioélectriques, par exemple, du fait d'un trop grand nombre de nouvelles tentatives en présence de perturbations.

3.1.1.19
niveau de performance (PL)
niveau discret utilisé pour spécifier la capacité des parties relatives à la sécurité des systèmes de commande à accomplir une fonction de sécurité dans des conditions prévisibles

[ISO 13849-1]

3.1.1.20
redondance
existence de moyens, outre les moyens qui se révèleraient suffisants pour qu'une unité fonctionnelle accomplisse une fonction requise ou que des données représentent une information

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

3.1.1.21
risque
combinaison de la probabilité d'un dommage et de sa gravité

NOTE Pour plus d'informations sur ce concept, se reporter à l'Annexe A de l'IEC 61508-5:2010.

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

3.1.1.22
couche de communication de sécurité (SCL)
couche de communication qui comprend toutes les mesures nécessaires permettant d'assurer la transmission de données en toute sécurité conformément aux exigences de l'IEC 61508

3.1.1.23
données de sécurité
données transmises par un réseau de sécurité utilisant un protocole de sécurité

NOTE La couche de communication de sécurité ne garantit pas la sécurité des données proprement dites, mais uniquement la transmission en toute sécurité de ces dernières.

3.1.1.24
appareil de sécurité
appareil conçu conformément à l'IEC 61508 et qui met en oeuvre le profil de communication de sécurité fonctionnelle

3.1.1.25
fonction de sécurité
fonction à réaliser par un système E/E/PE relatif à la sécurité ou par un appareil externe de réduction de risque, prévue pour assurer ou maintenir un état de sécurité de l'EUC par rapport à un événement dangereux spécifique

NOTE La définition de l'IEC 61508-4 est identique, avec un exemple et des références supplémentaires.

[IEC 61508-4:2210, modifiée]

3.1.1.26
temps de réponse de la fonction de sécurité
temps écoulé du cas le plus défavorable suite à l'activation d'un capteur de sécurité relié à un bus de terrain, avant que ne soit atteint l'état de sécurité correspondant de son (ses) actionneur(s) de sécurité, du fait d'erreurs ou de défaillances avérées dans le canal de fonction de sécurité

NOTE Ce concept est introduit dans l'IEC 61784-3:2010, 5.2.4, et traité par les profils de communication de sécurité fonctionnelle définis dans la présente partie.

3.1.1.27
niveau d'intégrité de sécurité (SIL)
niveau discret (parmi quatre possibles), correspondant à une gamme de valeurs d'intégrité de sécurité où le niveau 4 d'intégrité de sécurité possède le plus haut degré d'intégrité et le niveau 1 possède le plus bas

NOTE 1 Les objectifs chiffrés de défaillance (voir l'IEC 61508-4:2010, 3.5.17) pour les quatre niveaux d'intégrité de sécurité sont indiqués dans les Tableaux 2 et 3 de l'IEC 61508-1:2010.

NOTE 2 Les niveaux d'intégrité de sécurité sont utilisés pour spécifier les exigences concernant l'intégrité de sécurité des fonctions de sécurité à allouer aux systèmes E/E/PE relatifs à la sécurité.

NOTE 3 Le niveau d'intégrité de sécurité (SIL) ne constitue pas une propriété d'un système, sous-système, élément ou composant. L'interprétation correcte de l'expression « système relatif à la sécurité à SIL*n* » (où *n* est 1, 2, 3 ou 4) signifie que le système est potentiellement capable de prendre en charge des fonctions de sécurité avec un niveau d'intégrité de sécurité jusqu'à *n*.

[IEC 61508-4:2010]

3.1.1.28
mesure de sécurité
<la présente norme> mesure permettant de contrôler les *erreurs* de communication éventuelles, qui est conçue et mise en œuvre conformément aux exigences de l'IEC 61508

NOTE 1 Dans la pratique, plusieurs mesures de sécurité sont combinées pour atteindre le niveau d'intégrité de sécurité requis.

NOTE 2 Les *erreurs* de communication et les mesures de sécurité associées sont détaillées dans l'IEC 61784-3:2010, 5.3 et 5.4.

3.1.1.29
application relative à la sécurité
programmes conçus conformément à l'IEC 61508 pour satisfaire aux exigences SIL de l'application

3.1.1.30
système relatif à la sécurité
système qui exécute les *fonctions de sécurité* conformément à l'IEC 61508

3.1.1.31
déclenchement parasite
déclenchement provoqué par le système de sécurité sans injonction du processus

3.1.2 CPF 18: Termes et définitions supplémentaires

3.1.2.1
relation client/serveur
relation dans laquelle le client envoie des données au serveur qui transmet en retour les données demandées

3.1.2.2
numéro consécutif
entier sans signe comportant un retour à zéro en cas de débordement, utilisé comme moyen permettant de s'assurer de l'exhaustivité et du bon ordre des PDU de sécurité transmises

NOTE Instance de « numéro de séquence » tel que décrit dans l'IEC 61784-3.

3.1.2.3
cycle
intervalle auquel une liste d'instructions ou une activité est exécutée de manière répétitive et continue

3.1.2.4
retard
temps de transmission des PDU ayant pour origine dynamique les propriétés du réseau, telles que le trafic, les appareils de commutation et la topologie

3.1.2.5
à sécurité intégrée
capacité d'un système qui, par l'adoption de mesures techniques ou organisationnelles appropriées, évite les dangers de manière déterministe, ou par réduction du risque potentiel à une mesure tolérable

3.1.2.6
passerelle
appareil qui intervient comme élément de liaison entre des protocoles différents

3.1.2.7
double ligne logique
séquence de l'appareil racine et de tous les appareils ordinaires prenant en charge le traitement de la trame de communication dans les directions avant et arrière

3.1.2.8
relation producteur/consommateur
relation dans laquelle le producteur envoie des données au consommateur sans aucune demande spécifique

3.1.2.9
ligne de trame en temps réel (RTFL)
modèle de communication dont les appareils constitutifs communiquent dans une double ligne logique (voir CP 18/2)

3.1.2.10
réseau de trames en temps réel (RTFN)
modèle de communication dont les appareils constitutifs communiquent dans un réseau commuté (voir CP 18/1)

3.1.2.11
gestion SCL (SALMT)

mécanisme de commande de l'état SCL des appareils de sécurité

3.1.2.12
contrôle de retard de sécurité (SDM)
mécanisme de sécurité permettant le contrôle cyclique du retard des PDU transmises

3.1.2.13
cadence (impulsions) de sécurité (SHB)
mécanisme de contrôle cyclique de l'état des appareils de sécurité

3.1.2.14
objet de données de processus de sécurité (SPDO)
mécanisme d'échange cyclique de données de processus de sécurité entre appareils

3.1.2.15
relation émetteur/récepteur
relation dans laquelle l'émetteur envoie des données au récepteur

3.1.2.16
relation 1:1
relation de communication comportant exactement un émetteur et un récepteur

3.1.2.17
relation 1:n
relation de communication comportant exactement un émetteur et un ou plusieurs récepteurs

3.2 Symboles et abréviations

3.2.1 Symboles et abréviations communs

CEM	Compatibilité électromagnétique	
CP	Profil de communication (*communication profile*)	[IEC 61784-1]
CPF	Famille de profils de communication (*Communication Profile Family*)	[IEC 61784-1]
CRC	Contrôle de redondance cyclique (*Cyclic Redundancy Check*)	
DLL	Couche de liaison de données (*Data Link Layer*)	[ISO/IEC 7498-1]

DLPDU	Unité de données de protocole de liaison de données (*Data Link Protocol Data Unit*)	
EUC	Equipement commandé (*Equipment Under Control*)	[IEC 61508-4:2010]
E/E/PE	Electrique/électronique/électronique programmable (*Electrical/Electronic/Programmable Electronic*)	[IEC 61508-4:2010]
FAL	Couche Application de bus de terrain (*Fieldbus Application Layer*)	[IEC 61158-5]
FCS	Séquence de contrôle de trame (*Frame Check Sequence*)	
FS	Sécurité fonctionnelle (*Functional Safety*)	
FSCP	Profil de communication de sécurité fonctionnelle (*Functional Safety Communication Profile*)	
PDU	Unité de données de protocole (*Protocol Data Unit*)	[ISO/IEC 7498-1]
PFH	Fréquence moyenne de défaillance dangereuse par heure (*Average frequency of dangerous failure*) [h-1]	[IEC 61508-4]
PhL	Couche physique (*Physical Layer*)	[ISO/IEC 7498-1]
PL	Niveau de performance (*Performance Level*)	[ISO 13849-1]
PLC	Automate programmable (*Programmable Logic Controller*)	
SCL	Couche de communication de sécurité (*Safety Communication Layer*)	
SIL	Niveau d'intégrité de sécurité (*Safety Integrity Level*)	[IEC 61508-4:2010]

3.2.2 CPF 18: Symboles et abréviations supplémentaires

3.2.2.1 Abréviations supplémentaires

AL	Couche Application (*Application layer*)
AP	Processus d'Application (*Application process*)
CDC	Canal de données cycliques (*Cyclic data channel*)
FSF	A sécurité intégrée (*Fail-safe*)
ID	Indicatif (*Identification*)
PDO	Objet de données de processus (*Process data object*)
PDO-ID	Indicatif d'objet de données de processus (*Process data object ID*)
PID	Indicatif de paquet (*Packet ID*)
RTFL	Ligne de trame en temps réel (*Real time frame line*)
RTFN	Réseau de trames en temps réel (*Real time frame network*)
SALMT	Gestion SCL (*SCL management*)
SDM	Contrôle de retard de sécurité (*Safety delay monitoring*)
SHB	Cadence (impulsions) de sécurité (*Safety heartbeat*)
SID	Indicatif de sécurité (*Safety ID*)
SPDO	Objet de données de processus de sécurité (*Safety process data object*)

3.2.2.2 Symboles supplémentaires

Symbole	Définition	Description	Unité
T_A	Temps d'activation	Temps de réponse le plus défavorable de l'actionneur pour conversion et réaction selon la fonction de sécurité	µs
T_{cycle}	Temps de cycle	Temps de cycle de communication	µs
T_I	Temps d'entrée	Temps de traitement le plus défavorable de l'appareil d'entrée	µs
T_L	Temps de traitement logique	Temps de traitement le plus défavorable de l'automate logique de sécurité	µs
T_O	Temps de sortie	Temps de traitement le plus défavorable de l'appareil de sortie	µs

Symbole	Définition	Description	Unité
T_S	Temps de détection	Temps de réponse le plus défavorable du détecteur de la constatation du changement d'un signal physique au résultat de conversion valide	µs
T_{SFR}	Temps de réponse de la fonction de sécurité	Temps de réponse de la fonction de sécurité du signal d'entrée physique à la réaction effective de l'actionneur	µs
T_{TOi}	Durée de temporisation de composant	Durée de temporisation du composant de sécurité i	µs
T_{TOS}	Temps de transmission	Temps de transmission le plus défavorable du réseau de communication. Temps de temporisation pour FSCP 18/1	µs
ΔT	Marge de temporisation	Marge supplémentaire applicable au temps de cycle de transmission. Cette valeur est définie par l'utilisateur sur la base des exigences de l'application. La plage typique est comprise entre 0 % et 15%	µs

3.3 Conventions

Les attributs d'un objet sont décrits sous la forme indiquée dans le Tableau 1. La signification des attributs est décrite dans la liste suivante.

- L'attribut « Index» décrit la position d'un objet dans le dictionnaire d'objets de sécurité.
- L'attribut «Sous-index» décrit un élément unique de l'objet contenant les données suivantes. Le sous-index est répété pour chaque élément de l'objet.
  - L'attribut « Nom » désigne une chaîne de noms applicable à cet attribut.
  - L'attribut « Description » est utilisé pour les informations supplémentaires concernant la méthode selon laquelle l'objet doit être utilisé.
  - L'attribut «Type d'objet » désigne le type de caractérisation de chaque objet, tel que spécifié dans l'IEC 61158-6-22..
  - L'attribut «Type de données » désigne le type de données de cet élément.
  - L'attribut « Catégorie » indique si l'élément est obligatoire (M), facultatif (O) ou dépend de l'établissement d'autres attributs (C).
  - L'attribut «Attribut d'accès » montre l'accès direct à cet élément. RO signifie droit d'accès en lecture, RW signifie droit d'accès en lecture-écriture, WO signifie droit d'accès en écriture, tandis que FSF désigne l'absence de droits d'accès, à l'exception de l'application de sécurité et de l'accès en lecture facultatif par les services SDO, tel que spécifié dans l'IEC 61158-5-22 et l'IEC 61158-6-22.
  - L'attribut « Mise en correspondance SPDO » désigne la possibilité de faire correspondre cet attribut à TxSPDO ou RxSPDO, ou d'indiquer que ce paramètre ne peut être mis en correspondance.
  - L'attribut « Plage de valeurs» contient la plage de valeurs d'un élément dédié ou l'attribut «Aucune » pour indiquer l'absence de plage de valeurs prédéfinie.
  - L'attribut « Valeur » contient la (les) valeur(s) constante(s) et/ou la signification du paramètre ou l'attribut «Aucune » pour indiquer l'absence de valeur prédéfinie.

Tableau 1 – Définition des objets

Attribut	Valeur
Index	
Sous-index	
Nom	
Description	
Type d'objet	
Type de données	
Catégorie	
Attribut d'accès	
Mise en correspondance SPDO	
Plage de valeurs	
Valeur	

Les éléments de la syntaxe FSCP associés à la structure PDU sont décrits tel qu'indiqué dans le Tableau 2. La signification des colonnes du tableau est décrite dans la liste suivante.

- La colonne « Décalage d'octet » désigne le décalage de l'élément DLPDU par rapport au début de la PDU de sécurité.
- La colonne « Champ de données » est le nom de l'élément.
- La colonne « Valeur/Description » contient la valeur constante ou la signification du paramètre.

Tableau 2 – Définition des éléments PDU de sécurité

Décalage d'octet	Champ de données	Description

4 Présentation de FSCP 18/1 (SafetyNET p™)

4.1 Généralités

La famille de profils de communication 18 (communément appelée SafetyNET p™[4]) définit des profils de communication sur la base des IEC 61158-3-22 IEC 61158-4-22, IEC 61158-5-22 et IEC 61158-6-22.

Les profils de base CP 18/1 et CP 18/2 sont définis dans l'IEC 61784-2:2010. Le profil de communication de sécurité fonctionnelle FSCP 18/1 (SafetyNET p™) est basé sur les profils de base de CPF 18 spécifiés dans l'IEC 61784-2 et les spécifications de la couche de communication de sécurité définies dans la présente partie.

---

4 SafetyNET p est l'appellation commerciale de Pilz GmbH & Co. KG. Cette information est donnée à l'intention des utilisateurs de la présente norme internationale et ne signifie nullement que l'IEC approuve ou recommande le détenteur de la marque ou l'un quelconque de ses produits. La conformité à la présente partie n'exige aucunement l'utilisation de la marque SafetyNET p, ladite utilisation nécessitant l'accord de Pilz GmbH & Co. KG.

4.2 FSCP 18/1

Le protocole FSCP 18/1 décrit un protocole de sécurité qui permet le transfert de données de processus de sécurité jusqu'au niveau SIL 3 entre les appareils de type FSCP 18/1. Un bus de terrain subordonné non pris en compte dans les considérations de sécurité (méthode du canal noir) est utilisé pour le transfert du protocole de sécurité. Les données de sécurité échangées entre des partenaires de communication sont considérées comme des données de processus cyclique échangées entre eux par le bus de terrain subordonné.

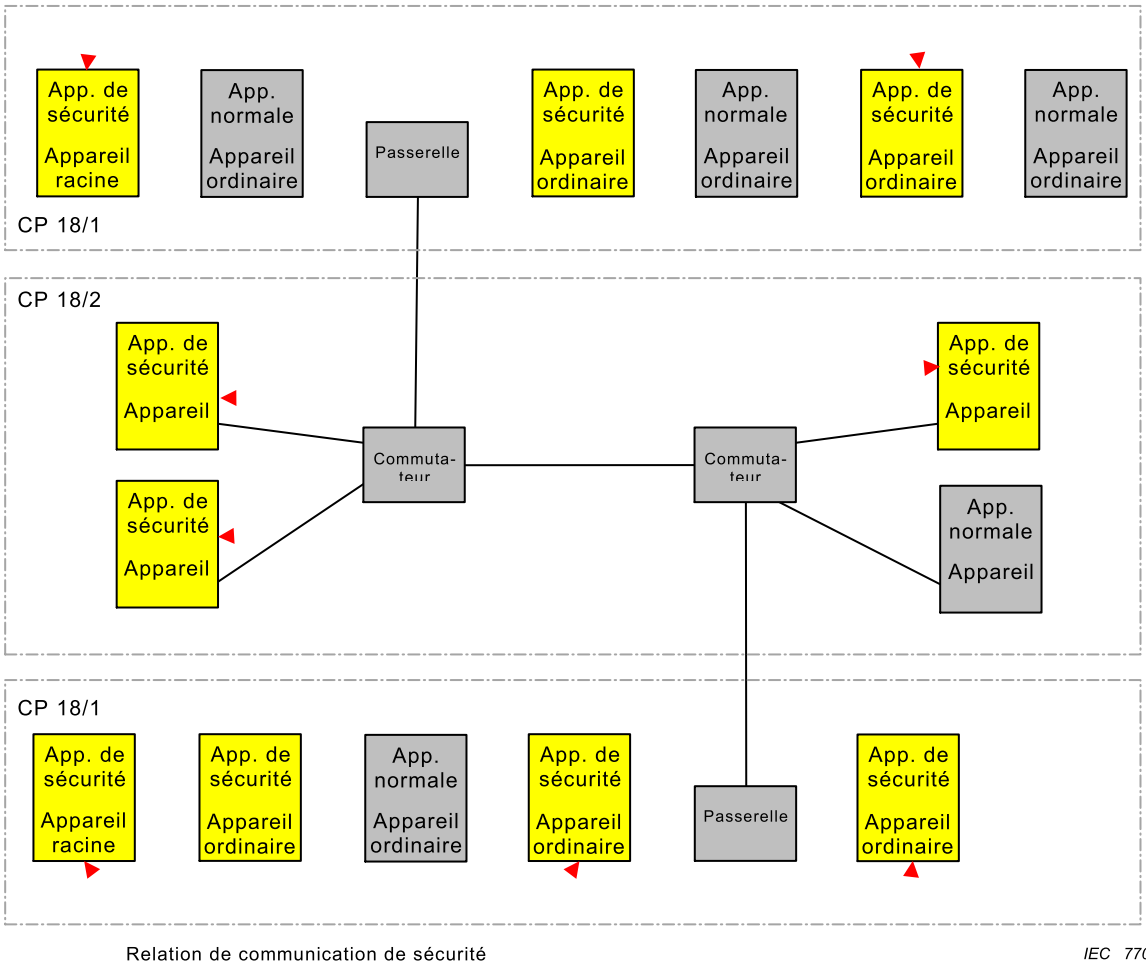


Figure 3 – Système FSCP 18/1

Le système FSCP 18/1 utilise une relation 1:n dédiée du type relation producteur/consommateur pour la communication de données de processus de sécurité et une relation 1:1 à des fins de contrôle des appareils de sécurité. La Figure 3 montre les relations de communication potentielles fondées sur un réseau CP 18/1 et CP 18/2.

Les mesures de sécurité suivantes ont été retenues pour réaliser le système FSCP 18/1:

- numéro de session (numéro consécutif);
- délai de contrôle de communication;
- identification unique des émetteurs;
- contrôle de redondance cyclique pour l'intégrité des données;

- différents systèmes d'assurance d'intégrité des données pour les communications de sécurité et de non sécurité;
- contrôle de retard des paquets pour les relations de communication dédiées.

Chaque appareil maintient un automate fini à couche de communication de sécurité, dont la coordination s'effectue par l'application de sécurité. La sécurité est assurée sur la base de la commutation SCL en état d'erreur système (c'est-à-dire état de sécurité) dès la détection d'une erreur.

5 Généralités

5.1 Documents externes de spécifications applicables au profil

Le document suivant est utile pour bien comprendre la conception du protocole FSCP 18/1:

- GS-ET-26 [34]

5.2 Exigences fonctionnelles de sécurité

Les exigences suivantes doivent s'appliquer au développement d'appareils qui mettent en oeuvre le protocole FSCP 18/1. Les mêmes exigences ont été appliquées pour le développement de ce protocole.

- Les exigences de l'IEC 61508 doivent être satisfaites.
- Le protocole FSCP 18/1 est conçu de manière à prendre en charge le niveau d'intégrité de sécurité 3 (SIL 3) (voir IEC 61508).
- Le protocole FSCP 18/1 est mis en œuvre en appliquant la méthode du canal noir; aucune dépendance relative à la sécurité ne s'applique aux profils de communication CPF 18 normaux. Le matériel de transmission ne doit pas être modifié.
- Les communications de sécurité et normale doivent être indépendantes. Les appareils de sécurité et normaux doivent être capables d'utiliser le même canal de communication.
- Une relation 1:1 doit toujours exister entre les appareils de communication à des fins de contrôle des appareils.
- La communication de sécurité doit utiliser un système de communication mono-canal. La redondance peut uniquement être utilisée, le cas échéant, pour une plus grande disponibilité.
- La mise en œuvre du protocole de sécurité doit être limitée aux appareils terminaux de communication.
- La durée de transmission doit être contrôlée.
- Les documents propres aux appareils doivent indiquer le niveau d'intégrité de sécurité (SIL) pour lequel ces derniers sont conçus.
- Pour les appareils qui utilisent la version 2 du protocole (voir 7.1.3.4), il est exigé d'ajouter 10^{-9} à la PFH du matériel de l'appareil pour tenir compte du canal de communication.

  NOTE De cette manière, l'utilisateur de l'appareil n'aura pas à tenir compte du nombre de connexions logiques dans une fonction de sécurité.

- L'utilisation des mécanismes de correction d'erreurs dans le canal noir est admise.

5.3 Mesures de sécurité

Les mesures de sécurité appliquées dans le protocole FSCP 18/1 pour détecter les erreurs de communication sont énumérées dans le Tableau 3. Toutes les mesures de sécurité doivent être appliquées et contrôlées dans chaque appareil de sécurité.

Tableau 3 – Erreurs de communication et mesures de détection

Erreurs de communication	Mesures de sécurité				
	Numéro de séquence	Délai [a]	Authentification de connexion [b]	Assurance d'intégrité des données	Différents systèmes d'assurance d'intégrité des données
Corruption	—	—	—	X	—
Répétition non prévue	X	—	—	—	—
Séquence incorrecte	X	—	—	—	—
Perte	X	X	—	—	—
Retard inacceptable	—	X	—	—	—
Insertion	X	—	X	—	—
Déguisement	X	—	X	—	X
Adressage	X	—	X	—	—
Défaillances de mémoire tournante des commutateurs	X	X	X	X	—

[a] « T_{TOS} » dans la présente norme.

b Réalisé par "SID" et "PID" dans la présente norme.

5.4 Structure de la couche de communication de sécurité

La Figure 4 montre la relation entre le protocole, CPF 18 et le type 22. La couche de communication de sécurité du protocole FSCP 18/1 se situe au sommet des couches d'application de CPF 18 et du type 22 et des couches de liaison de données, et utilise les services de non-sécurité de CPF 18 et du type 22 pour transférer les PDU de sécurité.

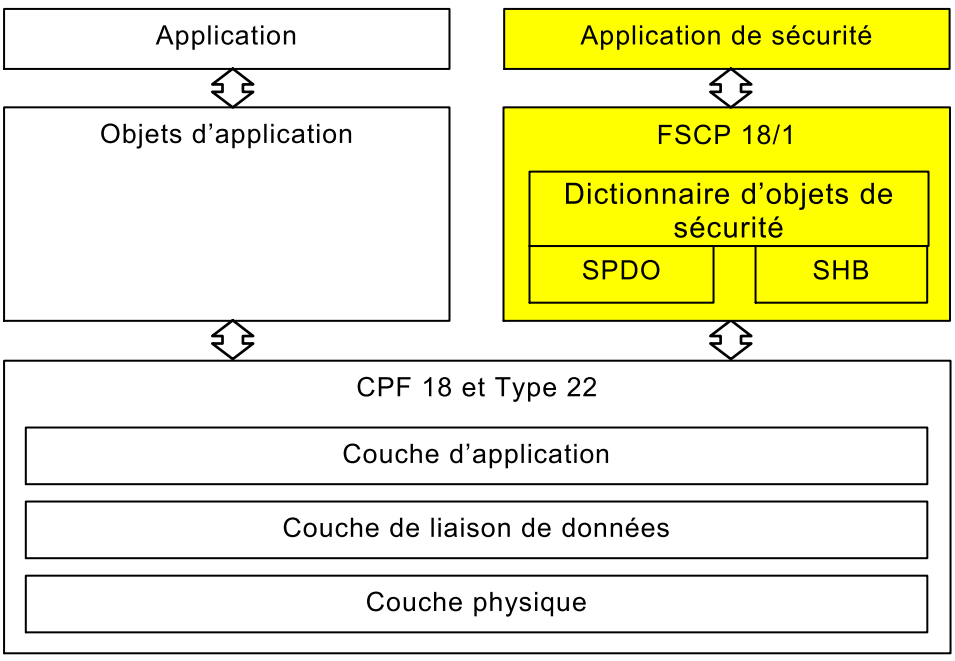


Figure 4 – Architecture logicielle du protocole FSCP 18/1

Les objets de données de processus de type 22 comprennent un objet de données de processus de sécurité (SPDO) contenant les données de processus de sécurité, les informations d'identification et les mesures de détection d'erreurs requises. La mise en

correspondance des données de processus de sécurité avec les SPDO s'effectue par les entrées du dictionnaire d'objets de sécurité.

Un service de cadence de sécurité (SHB) permet de contrôler la synchronisation temporelle de l'application de sécurité.

Le calcul de la probabilité d'erreur résiduelle propre au protocole FSCP 18/1 ne bénéficie pas des mécanismes de détection d'erreurs du système de communication. Le protocole peut également être transféré par l'intermédiaire d'autres systèmes de communication.

5.5 Relations avec la FAL (et DLL, PhL)

5.5.1 Généralités

Cette couche de communication de sécurité est conçue pour être utilisée avec les profils de communication CPF 18. Elle ne se limite toutefois pas à ce profil de communication.

5.5.2 Types de données

Les profils définis dans la présente partie prennent en charge tous les types de données CPF 18 définis dans l'IEC 61158-5-22. Le codage de ces types de données suit les règles de codage définies dans l'IEC 61158-6-22.

6 Services de la couche de communication de sécurité

6.1 Eléments généraux

6.1.1 Généralités

Le protocole FSCP 18/1 fournit les éléments suivants:

- dictionnaire d'objets de sécurité;
- objet de données de processus de sécurité (SPDO);
- cadence (impulsions) de sécurité (SHB);
- contrôle de retard de sécurité (SDM).

6.1.2 Dictionnaire d'objets de sécurité

Le dictionnaire d'objets de sécurité constitue l'interface entre l'application de sécurité et le système de communication. Il consiste en un regroupement d'objets et spécifie des paramètres de communication et d'appareil uniformes pour la fonctionnalité relative à la sécurité. L'organisation des objets est adaptée à l'organisation de CP 18/1 et CP 18/2. L'accès aux entrées des dictionnaires d'objets de sécurité peut le cas échéant s'effectuer par les services SDO tels que définis dans l'IEC 61158-5-22 et l'IEC 61158-6-22. Cet accès doit être limité à l'accès en lecture seulement (RO).

6.1.3 Objet de données de processus de sécurité (SPDO)

Les objets de données de processus de sécurité doivent fournir les services requis pour l'échange de données de processus relatif à la sécurité entre certains appareils de communication. La communication des données de processus de sécurité avec le protocole FSCP 18/1 s'effectue de manière cyclique en utilisant les objets de données de processus de sécurité (SPDO). La communication des données de processus est répartie en objets de données de processus de transmission et de réception de sécurité (TxSPDOs ou RxSPDO).

6.1.4 Cadence (impulsions) de sécurité (SHB)

Les appareils qui mettent en œuvre le protocole FSCP 18/1 SCL utilisent le service SHB pour le contrôle des couches application et le contrôle d'application. Ce service est indépendant de tout autre service de cadence (impulsions) que les appareils pourraient mettre en œuvre de façon parallèle. Les messages SHB sont des messages cycliques confirmés échangés entre les appareils de communication et établissent par ailleurs une relation 1:1 entre les appareils. Le mécanisme SHB permet la synchronisation des horloges système des appareils de communication.

6.1.5 Contrôle de retard de sécurité (SDM)

Le service de contrôle de retard de sécurité sert à contrôler le retard des paquets dans le cadre d'une relation de communication des appareils de même nature. Ce mécanisme est basé sur une relation de service confirmée entre les appareils. Le service s'assure que le temps qui s'écoule entre l'émission de la demande de service et la réception de la confirmation du service ne dépasse pas un retard maximal configurable. De plus, le service contrôle la durée entre deux mesures abouties du retard. Cette durée ne doit pas être supérieure à une durée fonction de la configuration au cours de laquelle il serait possible que le retard dépasse le retard maximal autorisé.

6.2 Relation de communication

Le protocole FSCP 18/1 définit une relation 1:*n* avec la relation producteur/consommateur pour la communication de données de processus de sécurité. Les producteurs doivent transmettre, de manière cyclique, des objets de données de processus de sécurité identifiés par un PDO-ID unique destiné à l'identification des paquets et par un indicatif de sécurité unique destiné à l'identification du producteur. L'interaction des objets de données de processus de sécurité n'est pas confirmée. La Figure 5 illustre le modèle d'interaction des objets de données de processus de sécurité (voir ISO/IEC 10731 pour une explication de l'organigramme séquentiel).

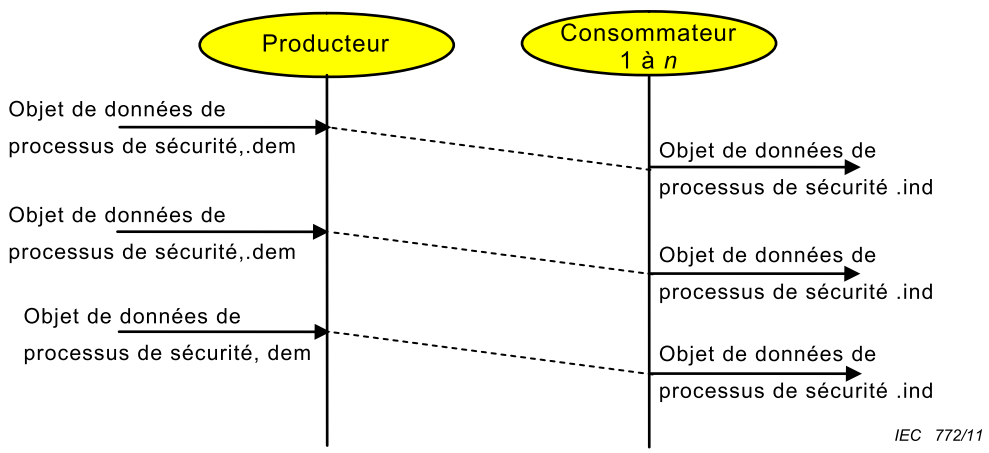


Figure 5 – Modèle d'interaction SPDO

L'état et la présence des partenaires de communication (c'est-à-dire les producteurs et les consommateurs) dans le protocole FSCP 18/1 font l'objet d'un contrôle indépendant par chaque appareil participant. Une relation de cadence (impulsions) est utilisée pour toutes les relations de communication d'un appareil dédié à un autre. Il existe ainsi une relation 1:1 entre les partenaires de communication. La communication de cadence de sécurité suit la relation client/serveur confirmée. La Figure 6 illustre les interactions de cadence (impulsions) pour une relation d'objets de données de processus de sécurité. Le temps de cycle du service de cadence (impulsions) est indépendant des autres temps de cycle de communication et

dépend du temps de réponse de la fonction de sécurité, ainsi que de l'augmentation maximale autorisée du temps de remise des messages.

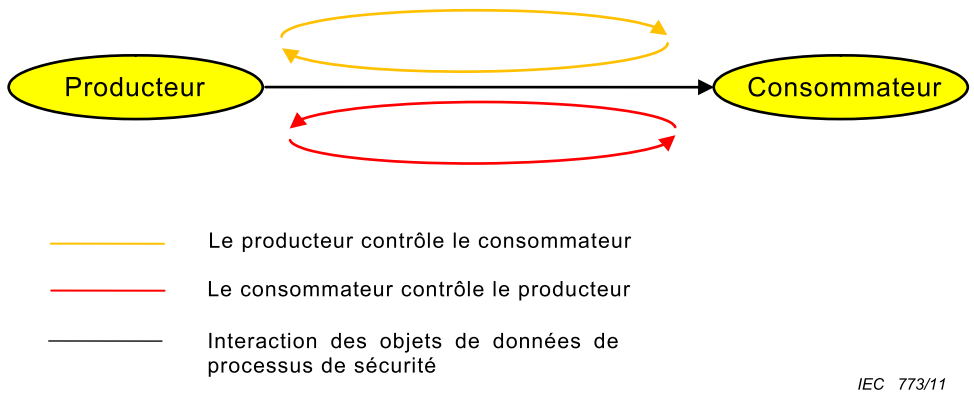


Figure 6 – Modèle d'interaction SHB

La communication de données de processus relative à la sécurité utilisant le protocole FSCP 18/1 est basée sur les deux composants essentiels suivants:

- objets de données de processus de sécurité (SPDO);
- cadence (impulsions) de sécurité (SHB).

Le cycle de communication FSCP 18/1 consiste principalement en un échange cyclique non confirmé d'objets de données de processus de sécurité. Le côté consommateur fait appel à un comportement de délai pour contrôler l'échange de données de processus de sécurité et détecter les défaillances de communication. L'application du modèle d'interaction non confirmé impose un mécanisme supplémentaire qui permet de détecter un appareil défaillant et qui permet également de détecter tout retard de remise de messages PDU accru au-delà du délai normal du consommateur. Le service de cadence (impulsions) de sécurité prend en charge cette réalisation. Les deux mécanismes combinés définissent et appliquent un cycle de communication.

7 Protocole de couche de communication de sécurité

7.1 Format PDU de sécurité

7.1.1 Généralités

7.1.1.1 Structure PDU

Un PDU de sécurité consiste soit en un objet de données de processus de sécurité (SPDO), soit en une cadence (impulsions) de sécurité (SHB). Tandis que le SPDO permet de communiquer les données d'application de sécurité, la SHB permet de synchroniser les appareils de communication.

7.1.1.2 Intégrité des données

Le récepteur d'un PDU de sécurité doit vérifier l'intégrité de sécurité des données en procédant au contrôle des deux copies de données (SPDO ou SHB) par rapport à leurs CRC, et en comparant les CRC de ces deux copies.

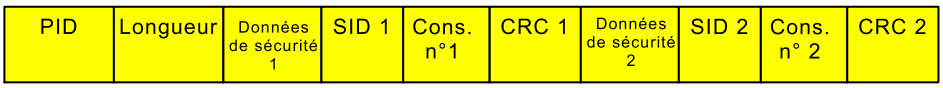
En cas de configuration avérée des répétitions de transmission, chaque réception doit alors faire l'objet d'une vérification tel que spécifié ci-dessus. La réception de la PDU de sécurité

doit être considérée comme non aboutie si toutes les répétitions n'ont pas satisfait au contrôle d'intégrité des données.

7.1.2 Objets de données de processus de sécurité (SPDO)

7.1.2.1 Structure SPDO

La Figure 7 définit la structure d'un objet de données de processus de sécurité et ses champs de données.



IEC 774/11

Figure 7 – Structure des objets de données de processus de sécurité

Le transfert des SPDO s'effectue de manière cyclique via le bus de terrain subordonné. Le contenu d'un SPDO consiste en un ou plusieurs objets d'application de sécurité parmi les objets du dictionnaire d'objets de sécurité. La mise en correspondance de l'élément du dictionnaire d'objets de sécurité avec le SPDO s'effectue par les entrées de mise en correspondance SPDO indiquées dans les Tableaux 25 et 26. Le Tableau 23 permet d'identifier l'index de la table de mise en correspondance du Tableau 26 sur la base du PID du SPDO.

La structure générale d'un SPDO est présentée dans le Tableau 4.

Tableau 4 – Structure du PDU du SPDO

Décalage d'octet	Champ de données	Description
0 à 2	PID	Indicatif de paquet
3	Longueur	Longueur du paquet complet en octets.
4 à 4+*n*-1	Données de sécurité 1	Données de processus d'application de sécurité mises en correspondance
4+*n* à 5+*n*	SID 1	ID de sécurité de l'émetteur
6+*n* à 6+*n*+*m*-1	numéro consécutif 1	Numéro consécutif pour ordonnancement et contrôle d'application, où : *m* = 1 pour la version 1 du protocole *m* = 3 pour la version 2 du protocole
7+*n*+*m* à 10+*n*+*m*	CRC 1	Contrôle de redondance cyclique de 32 bits couvrant les champs de données PID, données de sécurité 1, SID 1 et numéro consécutif 1
11+*n*+*m* à 11+2*n*-1+*m*	Données de sécurité 2	Copie des données de processus d'application de sécurité mises en correspondance
11+2*n*+*m* à 12+2*n*+*m*	SID 2	Copie de SID 1
13+2*n*+*m* à 13+2*n*+2*m*-1	Numéro consécutif 2	Copie du numéro consécutif 1
14+2*n*+2*m* à 17+2*n*+2*m*	CRC 2	Contrôle de redondance cyclique de 32 bits couvrant les champs de données PID, données de sécurité 2, SID 2 et numéro consécutif 2

NOTE 1 *n* est la longueur en octets du champ de données « données de sécurité 1 » (« données de sécurité 2 »).

NOTE 2 *m* est la longueur du nombre consécutif en fonction de la version du protocole (voir 7.1.3.4).

7.1.2.2 PID du SPDO

Ce champ de données constitue un numéro d'identification du paquet qui, associé au champ SID, identifie de manière unique le paquet.

7.1.2.3 Longueur du SPDO

Ce champ de données doit contenir la longueur en octet du paquet complet.

7.1.2.4 Données de sécurité

Ce champ de données doit contenir les objets d'application de sécurité selon la configuration de mise en correspondance.

Le nombre de données est limité de 0 à 115 octets pour la version 2 du protocole ou respectivement 117 octets pour la version 1 du protocole afin de permettre la transmission du PDU de sécurité via un canal noir dont les caractéristiques de transfert ne sont pas prises en compte dans les considérations de sécurité. Le taux d'erreur résiduelle par heure ne dépasse pas $10^{-9,}$ tel que démontré en 9.5.2, pour le système d'assurance d'intégrité des données.

7.1.2.5 SID du SPDO

Ce champ de données est un identifiant de 16 bits de l'émetteur. Cette valeur doit être unique sur tout le réseau. Chaque appareil FSCP 18/1 participant obtient un SID. Le SID d'un appareil est enregistré dans l'entrée du dictionnaire d'objets de sécurité correspondant avec l'index 0x1200. Le SID ne doit pas être égal à 0. Le numéro est généré par l'outil de configuration de réseau qui doit garantir le caractère unique du SID du SPDO.

7.1.2.6 Numéro consécutif du SPDO

Ce champ de données est un numéro consécutif (compteur cyclique) pour le contrôle du signe du cycle de vie et l'ordonnancement des paquets de la couche application. Ce numéro est généré par l'émetteur du SPDO. La taille du numéro consécutif dépend de la version du protocole (voir 7.1.3.4) et elle est de 1 octet pour la version 1 du protocole et de 3 octets pour la version 2 du protocole.

7.1.2.7 CRC du SPDO

Ce champ de données contient le CRC de 32 bits couvrant les champs de données « PID », « données », « SID » et « numéro consécutif».

Le polynôme 0x20044009 est utilisé pour calculer les CRC. Pour de plus amples informations, voir 7.1.2.4 et 9.5.2.

7.1.3 Cadence (impulsions) de sécurité (SHB)

7.1.3.1 Structure SHB

7.1.3.1.1 PDU de demande SHB

La Figure 8 illustre la structure du PDU d'une demande de cadence (impulsions) de sécurité.

PID	Longueur	SCL état 1	AP de sécurité état 1	SID 1	Cons. n°1	CRC 1	SCL état 2	AP de sécurité état 2	SID 2	Cons. n°2	CRC 2

IEC 775/11

Figure 8 – Structure de demande de cadence (impulsions) de sécurité

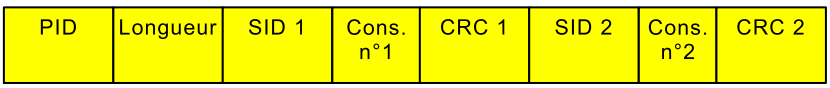
Le Tableau 5 répertorie la structure générale du PDU.

Tableau 5 – Structure du PDU de demande SHB

Décalage d'octet	Champ de données	Description
0 à 2	PID	Indicatif de paquet
3	Longueur	Longueur du paquet complet en octets
4	Etat 1 de la SCL	Etat SALMT (voir Tableau 7)
5 à 5+*n*-1	Etat 1 du processus d'application de sécurité	Etat du processus d'application de sécurité (spécifique à la mise en œuvre)
6+*n* à 7+*n*	SID 1	ID de sécurité de l'émetteur
8+*n* à 8+*n*+*m*-1	Numéro consécutif 1	Numéro consécutif pour ordonnancement et contrôle d'application où : *m* = 1 pour la version 1 du protocole *m* = 3 pour la version 2 du protocole
9+*n*+*m* à 12+*n*+*m*	CRC 1	Contrôle de redondance cyclique de 32 bits couvrant les champs de données PID, état 1 de la SCL, état 1 du processus d'application de sécurité, SID 1 et numéro consécutif 1
13+*n*+*m*	Etat 2 de la SCL	Copie de l'état 1 de SALMT
14+*n*+*m* to 14+2*n*+*m*-1	Etat 2 du processus d'application de sécurité	Copie de l'état 1 du processus d'application de sécurité
15+2*n*+*m* à 16+2*n*+*m*	SID 2	Copie de SID 1
17+2*n*+*m* à 17+2*n*+2*m*-1	Numéro consécutif 2	Copie du numéro consécutif 1
18+2*n*+2*m* à 21+2*n*+2*m*	CRC 2	Contrôle de redondance cyclique de 32 bits couvrant les champs de données PID, état 2 de la SCL, état 2 du processus d'application de sécurité, SID 2 et numéro consécutif 2
NOTE 1 *n* est la longueur en octets du champ de données « Etat du processus d'application de sécurité ». NOTE 2 *m* est la longueur du numéro consécutif, en fonction de la version du protocole (voir 7.1.3.4)		

7.1.3.1.2 PDU de réponse de SHB

La Figure 9 illustre la structure du PDU d'une réponse de cadence (impulsions) de sécurité.



IEC 776/11

Figure 9 – Structure de réponse de cadence (impulsions) de sécurité

Le Tableau 6 répertorie la structure générale de ce PDU.

Tableau 6 – Structure du PDU de réponse SHB

Décalage d'octet	Champ de données	Description
0 à 2	PID	Indicatif de paquet
3	Longueur	Longueur du paquet complet en octets
4 à 5	SID 1	ID de sécurité de l'émetteur
6 à 6+*m*-1	Numéro consécutif 1	Numéro consécutif pour ordonnancement et contrôle d'application où : *m* = 1 pour la version 1 du protocole *m* = 3 pour la version 2 du protocole
7+*m* à 10+*m*	CRC 1	Contrôle de redondance cyclique de 32 bits couvrant les champs de données PID, SID 1 et numéro consécutif 1
11+*m* à 12+*m*	SID 2	Copie de SID 1
13+*m* à 13+2*m*-1	Numéro consécutif 2	Copie du numéro consécutif 1
14+2*m* à 17+2*m*	CRC 2	Contrôle de redondance cyclique de 32 bits couvrant les champs de données PID, SID 2 et numéro consécutif 2
NOTE *m* est la longueur du numéro consécutif, en fonction de la version du protocole (voir 7.1.3.4).		

7.1.3.2 PID de SHB

Ce champ de données constitue un numéro d'identification du paquet qui, associé au champ SID, identifie de manière unique le paquet.

7.1.3.3 Longueur SHB

Ce champ de données doit contenir la longueur en octet du paquet complet.

7.1.3.4 Etat de la couche de communication de sécurité SHB

Ce champ de données doit contenir les informations d'état concernant la SCL. Ces informations sont interprétées par les récepteurs SHB. Le Tableau 7 spécifie le codage du contenu de ce champ de données.

Tableau 7 – Codage de l'état de la couche de communication de sécurité SHB

Valeur	Description	Protocole
0x00	FS FAL est à l'état BOOTUP	Version 1
0x04	FS FAL est à l'état STOPPED	Version 1
0x05	FS FAL est à l'état OPERATIONAL	Version 1
0x7F	FS FAL est à l'état PRE-OPERATIONAL	Version 1
0x10	FS FAL est à l'état BOOTUP	Version 2
0x14	FS FAL est à l'état STOPPED	Version 2
0x15	FS FAL est à l'état OPERATIONAL	Version 2
0x1F	FS FAL est à l'état PRE-OPERATIONAL	Version 2

L'appareil doit prendre en charge au moins une version du protocole. L'état FS FAL doit être codé conformément au Tableau 7 en fonction de la version du protocole utilisée. Il est recommandé qu'il prenne en charge toutes les versions du protocole.

7.1.3.5 Etat du processus d'application de sécurité SHB

Ce champ de données doit contenir les informations d'état concernant l'application de sécurité. Le contenu et le codage de ce champ de données dépendent de l'application et ne relèvent pas du domaine d'application de la présente norme internationale. La longueur est limitée de 0 à 114 octets pour la version 2 du protocole ou respectivement 116 octets pour la version 1 du protocole.

7.1.3.6 SID de SHB

Ce champ de données est l'indicatif de 16 bits de l'émetteur. Cette valeur doit être unique sur tout le réseau. Chaque appareil FSCP 18/1 participant obtient un SID. Le SID d'un appareil est enregistré dans l'entrée du dictionnaire d'objets de sécurité correspondant avec l'index 0x1200. Le SID ne doit pas être égal à 0. Le numéro est généré par l'outil de configuration de réseau qui doit garantir le caractère unique du SID de SHB.

7.1.3.7 Numéro consécutif de SHB

Ce champ de données est un numéro consécutif (compteur cyclique) pour le contrôle du signe de vie et l'ordonnancement des paquets de la couche application. Dans le cas d'un PDU de réponse, ce champ de données contient le numéro consécutif du PDU confirmé par cette réponse. Ce numéro est généré par l'émetteur de la SHB. La taille du numéro consécutif dépend de la version du protocole (voir 7.1.3.4) et elle est de 1 octet pour la version 1 du protocole et de 3 octets pour la version 2 du protocole.

7.1.3.8 CRC de SHB

Ce champ de données contient le CRC de 32 bits couvrant les champs de données « PID », « données », « SID » et « numéro consécutif».

Le polynôme 0x20044009 est utilisé pour calculer les CRC. Pour de plus amples informations, voir 7.1.3.5 et 9.5.2.

7.1.4 PDU de sécurité intégrées dans un PDU de type 22

La Figure 10 illustre la structure d'un PDU de sécurité FSCP 18/1 intégrée dans un DLPDU CDC de type 22. La présence de renseignements d'en-tête IP et UDP dépend du profil de communication utilisé. Pour de plus amples informations concernant le DLPDU de type 22, se reporter à l'IEC 61158-4-22.

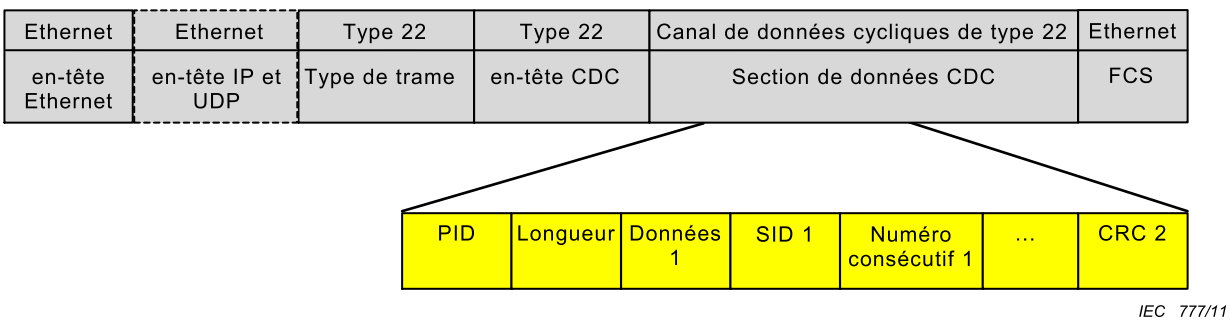


Figure 10 – PDU de sécurité pour le protocole FSCP 18/1 intégrée dans une section de données CDC de type 22

7.2 Gestion de la couche de communication de sécurité (SALMT)

Le service SALMT local permet de déclencher l'automate fini de la SCL, et ainsi de contrôler le comportement de la partie sécurité d'un appareil.

Les commandes SALMT spécifiées dans le Tableau 8 sont disponibles.

Tableau 8 – Commandes SALMT

Commande	Description
0x01	Initialisation de la communication
0x02	Initialisation de nœud
0x03	Arrêt de nœud distant
0x04	Démarrage de nœud distant
0x05	Saisie état pré-opérationnel

La Figure 11 illustre le diagramme d'états SALMT. Tous les états du diagramme d'états doivent être pris en charge.

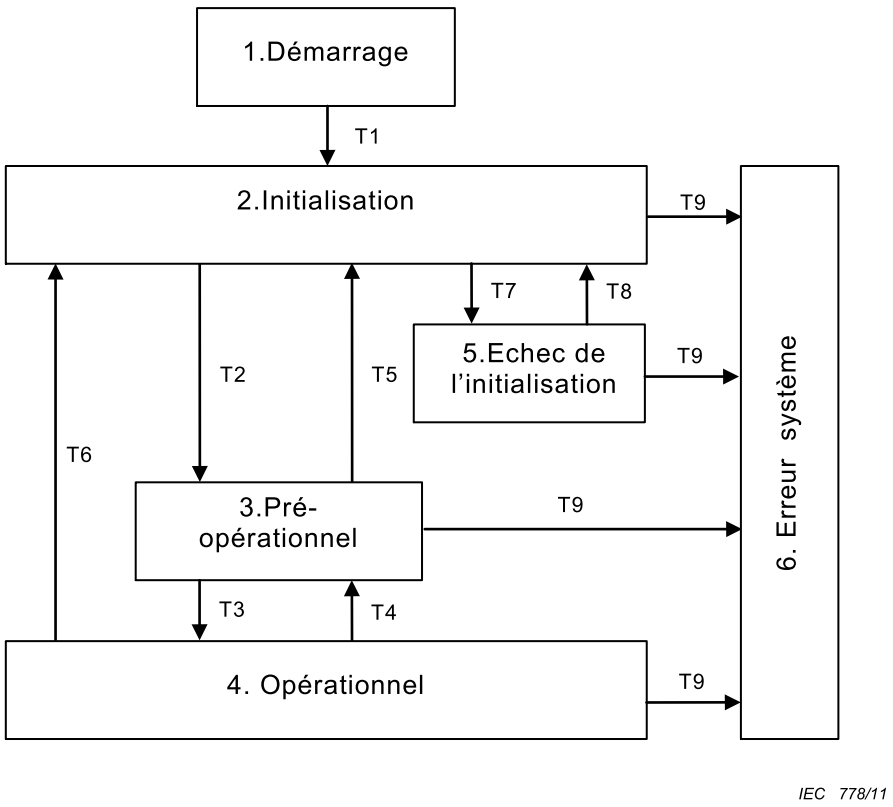


Figure 11 – Diagramme d'états SALMT

Les commandes de gestion locale sont associées aux transitions et états du diagramme d'états SALMT, tels que spécifiés dans les Tableaux 9 et 10.

Tableau 9 – Etats du diagramme d'états SALMT

Numéro d'état	Etat	Description
1	Démarrage	Etat virtuel après démarrage de l'appareil. L'émission et la réception des PDU SPDO et SHB ne sont pas admises.
2	Initialisation	Initialisation fonction du système. L'émission et la réception des PDU SPDO et SHB ne sont pas admises.
3	Pré-opérationnel	Exécution de la configuration ou attente de la demande par le système pour initialiser l'état opérationnel. L'émission et la réception des PDU SHB sont admises. Les PDU SPDO ne sont pas admises.
4	Opérationnel	Etat opérationnel. L'émission et la réception des PDU SPDO et SHB sont admises.
5	Echec de l'initialisation	Occurrence d'une erreur non relative à la sécurité pendant l'initialisation. L'émission et la réception des PDU SHB sont admises. Les PDU SPDO ne sont pas admises.
6	Erreur système	Détection d'une erreur relative à la sécurité. L'émission et la réception des PDU SPDO et SHB ne sont pas admises.

Tableau 10 – Transitions du diagramme d'états SALMT

Transition d'état	Numéro d'état d'origine	Numéro d'état destinataire	Description	Action
T1	1	2	Transition automatique après démarrage de l'appareil	Désactiver l'émission et la réception des PDU SPDO et SHB
T2	2	3	Transition déclenchée par la commande SALMT entrée dans l'état « Pré-opérationnel »	Activer l'émission et la réception des PDU SHB. Désactiver l'émission et la réception des PDU SPDO
T3	3	4	Transition déclenchée par la commande SALMT, démarrage du nœud distant	Activer l'émission et la réception des PDU SPDO et SHB
T4	4	3	Transition déclenchée par la commande SALMT, arrêt du nœud distant	Activer l'émission et la réception des PDU SHB. Désactiver l'émission et la réception des PDU SPDO
T5	3	2	Transition déclenchée par la commande SALMT, initialisation de nœud ou initialisation de la communication	Désactiver l'émission et la réception des PDU SPDO et SHB
T6	4	2	Transition déclenchée par la commande SALMT, initialisation de nœud ou initialisation de la communication	Désactiver l'émission et la réception des PDU SPDO et SHB
T7	2	5	Transition déclenchée par une défaillance ou une panne pendant l'initialisation	Activer l'émission et la réception des PDU SHB. Désactiver l'émission et la réception des PDU SPDO
T8	5	2	Transition déclenchée par la commande SALMT, initialisation de nœud	Désactiver l'émission et la réception des PDU SPDO et SHB
T9	2 3, 4 ou 5	6	Transition déclenchée par une erreur système	Désactiver l'émission et la réception des PDU SPDO et SHB

7.3 Communication de données de processus de sécurité

La communication de données de processus de sécurité est basée sur une relation 1:*n* du type relation producteur/consommateur. Aucun message de confirmation n'est utilisé. Les relations de communication sont configurées au cours de la phase de configuration du système. Aucune autre gestion de connexion en ligne n'est prévue.

Le côté consommateur fait appel à un comportement de délai pour contrôler l'échange de données de processus de sécurité et détecter les défaillances de communication. Le temps de cycle SPDO est contrôlé à l'aide d'un mécanisme de temporisation approprié. De plus, le producteur et le consommateur contrôlent le retard des paquets afin d'identifier toute augmentation inacceptable.

La Figure 12 illustre le diagramme d'états RxSPDO. Le diagramme d'états est appliqué pour chaque RxSPDO configuré. Tous les états doivent être pris en charge.

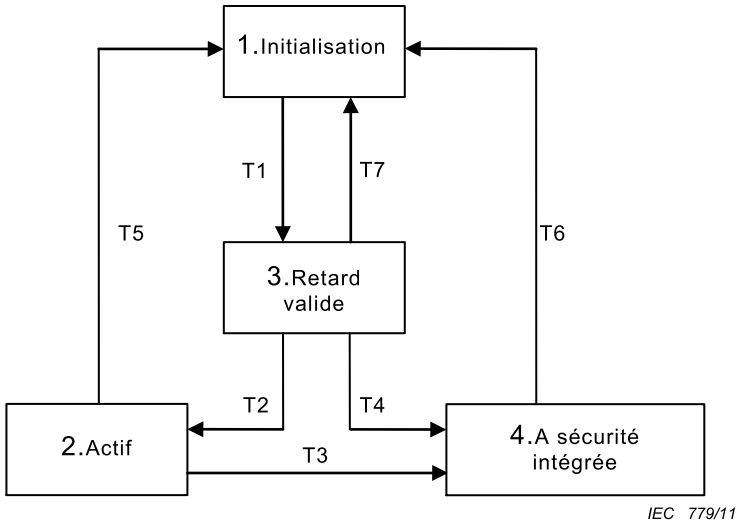


Figure 12 – Diagramme d'états RxSPDO

Les Tableaux 11 à 13 décrivent les transitions d'état et les événements et actions associés.

Tableau 11 – Etats du diagramme d'états RxSPDO

Numéro d'état	Transition d'état	Description
1	Initialisation	Démarrage ou temporisation SHB (aucune temporisation RxSPDO) en état non « Actif ». Aucune donnée générée
2	Actif	Réception RxSPDO et mesure de retard valide. Production de données. Etat SALMT « Opérationnel »
3	Retard valide	Mesure de retard satisfaisante, connexion avec le partenaire de communication dans les délais spécifiés, RxSPDO non « Actif » dans la mesure où aucun SPDO n'a encore été reçu. Aucune donnée n'est générée
4	A sécurité intégrée	Temporisation de RxSPDO ou SHB en état RxSPDO « Actif ». Mise à zéro et production unique des données. Réactivation admise uniquement par transition SALMT

Tableau 12 – Transitions du diagramme d'état RxSPDO

Transition d'état	Numéro d'état d'origine	Numéro d'état destinataire	Description	Action
T1	1	3	Pour les états SALMT « Pré-opérationnel » et « Opérationnel » si la mesure de retard (SHB) était satisfaisante	Aucune
T2	3	2	Pour l'état SALMT « Opérationnel » si réception de RxSPDO	Démarrage de la production de données et réglage de SALMT sur « Opérationnel »
T3	2	4	Pour l'état SALMT « Opérationnel » si la mesure de retard (SHB) n'est pas satisfaisante ou temporisation de RxSPDO. ou Echec du contrôle d'intégrité de sécurité de la PDU reçue (voir 7.1.1.2)	Mise à zéro et production unique des données. Puis arrêt de la production de données

Transition d'état	Numéro d'état d'origine	Numéro d'état destinataire	Description	Action
T4	3	4	Pour l'état SALMT « Opérationnel » si la mesure de retard (SHB) n'est pas satisfaisante (expiration de la temporisation SHB sans réponse du partenaire de communication à la SHB) ou Echec du contrôle d'intégrité de sécurité de la PDU reçue. (Voir 7.1.1.2)	Mise à zéro et production unique des données. Puis arrêt de la production de données
T5, T6, T7	2,3 ou 4	1	Sur changement de l'état SALMT d'« Opérationnel » en « Pré-opérationnel »	Arrêt de la production de données

Tableau 13 – Temporisations

Temporisation	Description
RxSPDO	Temporisation RxSPDO si aucun SPDO n'a été reçu après configuration du nombre de cycles multiplicateurs de temporisation
Réponse attendue SHB	Temporisation de la réponse attendue SHB si aucune réponse n'a été reçue au cours de la période de configuration après l'envoi d'un message SHB
Consommateur SHB	Temporisation du consommateur SHB si aucune SHB n'a été émise par le consommateur pendant la configuration du nombre de cycles multiplicateurs de temporisation
Temporisation SHB	Temporisation de la réponse attendue SHB ou du consommateur SHB

Plusieurs copies d'une PDU SPDO peuvent être transmises par un émetteur afin d'améliorer la disponibilité du service. Ce comportement dépend de la configuration du service. Le récepteur contrôle le nombre de copies d'un SPDO reçues. La réception d'un trop grand nombre de copies entraîne la transition vers l'état « erreur système » afin de signifier une configuration défectueuse du réseau. Le mécanisme de temporisation du récepteur n'est pas influencé par la réception de plusieurs copies. Le mécanisme est déclenché par le premier PDU reçu.

7.4 Cadence (impulsions) de sécurité

Les appareils de mise en oeuvre d'une SCL doivent prendre en charge la cadence (impulsions) de sécurité. Ce mécanisme de cadence (impulsions) est indépendant des messages de cadence (impulsions) CP 18/1 et CP 18/2 et doit faire l'objet d'une configuration indépendante.

Les messages de cadence (impulsions) de sécurité sont transmis tel que spécifié à la Figure 13. Chaque message de cadence (impulsions) contient l'état de la SCL et le processus d'application de sécurité.

La procédure de cadence (impulsions) est illustrée à la Figure 13.

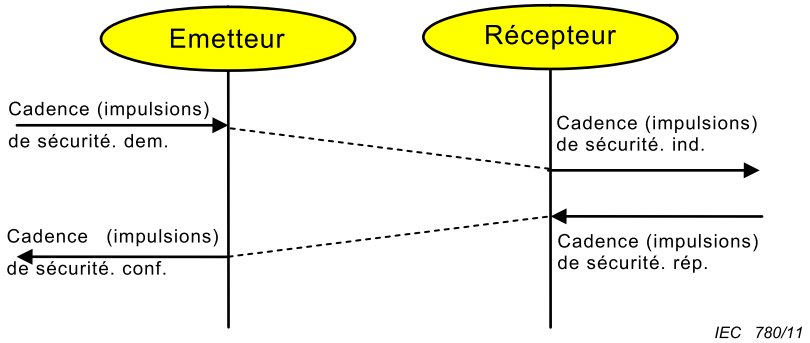


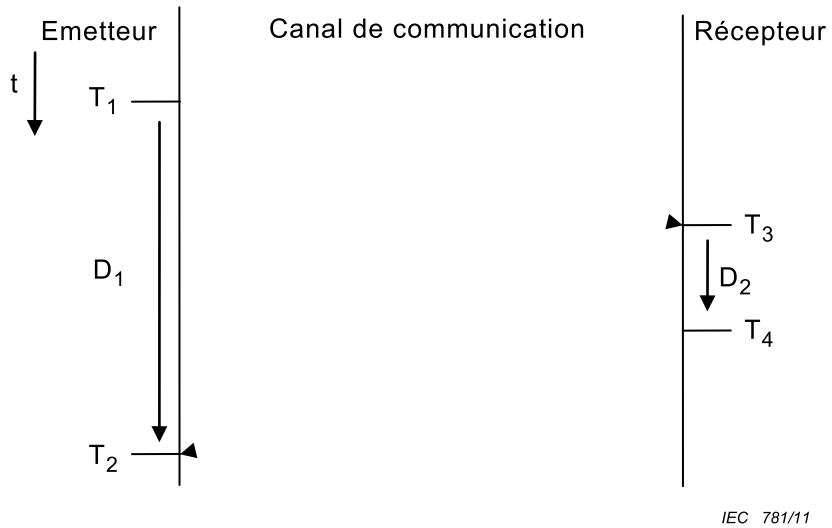
Figure 13 – Procédure de cadence (impulsions)

7.5 Contrôle de retard

La procédure de mesure de retard doit être exécutée par l'ensemble des appareils de mesure afin de déterminer le retard réel de remise des PDU, et ainsi de déterminer la validité des informations reçues.

Le service de cadence (impulsions) de sécurité permet de contrôler le retard des paquets. Le récepteur accuse réception de chaque PDU de cadence (impulsions) de sécurité. L'émetteur contrôle le temps qui s'écoule entre la génération de la demande de cadence (impulsions) et la réception de la réponse. Cette durée ne doit pas dépasser un retard maximal configuré.

La Figure 14 illustre le principe général de mesure du retard observé au niveau de l'émetteur et du récepteur.



T_x Point au temps x

D_x Retard résultant

Figure 14 – Principe de mesure du retard

Les appareils d'émission déterminent les temps T_1 et T_2. Les temps D_2, T_3 et T_4 ne font l'objet d'aucune analyse ultérieure. L'émetteur des PDU de demande de cadence (impulsions) doit, sur la base de ces informations, déterminer une estimation du retard de remise des paquets. Le résultat du contrôle de retard doit être comparé à une valeur de seuil configurée. Lorsque l'augmentation du retard déterminé est supérieure à la valeur de seuil configurée, la SCL doit déclencher une transition vers l'état SPDO « A sécurité intégrée » et l'application doit passer à l'état de sécurité.

La détermination de la fréquence de répétition applicable à la procédure de contrôle de retard (c'est-à-dire le temps de cycle SHB) doit être déduite du retard maximal autorisé (fonction du temps de réponse de la fonction de sécurité), du retard réel et des temps de cycle SPDO configurés.

De plus, l'émetteur contrôle la durée entre deux mesures du retard satisfaisantes. Cette durée ne doit pas être supérieure à la durée au cours de laquelle il est possible que le retard soit supérieur au seuil de retard configuré.

La durée maximale qui s'écoule jusqu'à la mesure suivante du retard est calculée selon l'Equation (1).

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

où

T_{Max} Temps maximal autorisé jusqu'à la mesure suivante du retard;

D_{Max} Retard maximal autorisé;

D_{Act} Retard réel (selon la dernière mesure du retard);

T_{Timer} Tolérance relative du temporisateur avec $0{,}000\ 1 \leq T_{Timer} \leq 0{,}1$;

T_{TO} Tolérance configurable pour la temporisation RxSPDO, index 0x121E selon le Tableau 15 avec $0{,}01 \leq T_{TO} \leq 1$:

8 Gestion de la couche de communication de sécurité

8.1 Traitement des paramètres

La configuration des paramètres des appareils PFSCP 18/1 fait partie intégrante de la configuration de l'application de sécurité. Tous les paramètres relatifs à la sécurité sont téléchargés sur l'appareil à l'aide d'un outil de configuration approprié. Le mécanisme de téléchargement des paramètres ne relève pas du domaine d'application de la présente norme internationale et dépend de l'application de sécurité. La Figure 15 illustre la séquence de configuration des appareils.

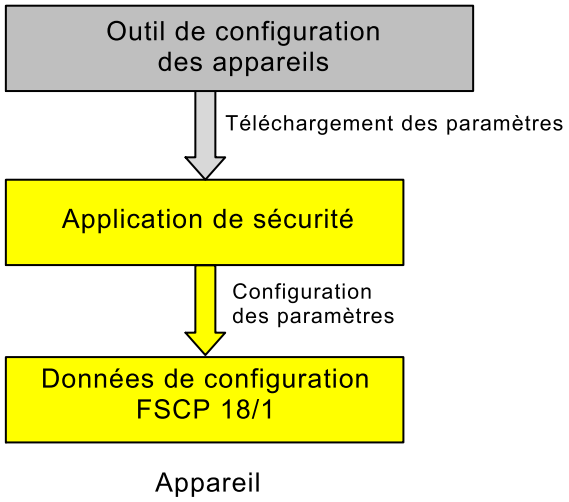


Figure 15 – Traitement des paramètres

8.2 Dictionnaire d'objets de sécurité

8.2.1 Généralités

Le dictionnaire d'objets de sécurité utilise la même structure que le dictionnaire d'objets employé dans les protocoles CP 18/1 et CP 18/2. Il contient les espaces objets énumérés dans le Tableau 14.

Tableau 14 – Structure du dictionnaire d'objets de sécurité

Index	Section	Sous-section	Contenu
0x0001 à 0x001F	Type de données	Types de données de base	Définition des types de données de base
0x0020 à 0x003F	—	Types de données complexes	Définition des types de données complexes
0x0040 à 0x005F	—	Types de données spécifiques au fabricant	Définition des types de données spécifiques au fabricant
0x0060 à 0x007F	—	Types de données de base spécifiques au profil de l'appareil	Définition des types de données de base spécifiques au profil de l'appareil
0x0080 à 0x009F	—	Types de données complexes spécifiques au profil de l'appareil	Définition des types de données complexes spécifiques au profil de l'appareil
0x00A0 à 0x0FFF	Réservé	—	—
0x1000 à 0x1FFF	Profil de communication	—	Définition des paramètres utilisés à des fins de configuration de communication et de communication dédiée
0x2000 à 0x5FFF	Profil défini par le fabricant	—	Définition des paramètres spécifiques au fabricant
0x6000 à 0x9FFF	Profil de l'appareil normalisé	—	Définition des paramètres définis dans un profil de l'appareil normalisé
0xA000 à 0xBFFF	Profil d'interface normalisée	—	Définition des paramètres spécifiés dans un profil d'interface normalisée
0xC000 à 0xC8FF	Profil d'interface CP 18/2	—	Définition des paramètres spécifiés dans un profil d'interface CP 18/2
0xC900 à 0xFFFF	Réservé	—	—

8.2.2 Section de profil de communication

8.2.2.1 Généralités

Les objets associés à l'application de sécurité énumérés dans le Tableau 15 doivent être pris en charge.

Tableau 15 – Objets de la section de communication

Index	Objet	Nom	Type de données	Attribut	Description	Catégorie
0x1000	VAR	Type d'appareil	Unsigned32	RO	Classification de l'appareil: 16 bits de poids faible correspondent au « Numéro de profil de l'appareil », décrivant le profil utilisé. 16 bits de poids fort correspondent aux « Informations supplémentaires ».	M
0x1200	VAR	Indicatif de sécurité	Unsigned16	FSF	Indicatif unique de l'appareil de sécurité, ne doit pas être égal à zéro	M/O
0x1216	ARRAY	Liste de cadence (impulsions) du consommateur de sécurité	Unsigned256	FSF	Liste des appareils distants qui doivent être contrôlés par l'appareil.	M/O
0x1217	RECORD	Paramètre de cadence (impulsions) du producteur de sécurité	PDO COM_PAR	FSF	Même configuration que la transmission SPDO. Doit être configurée comme la transmission cyclique.	M/O
0x1218	ARRAY	Temps de cycle de bus de sécurité	Unsigned32	FSF	Sous-index 0: nombre d'entrées Sous-index 1: Temps de cycle de base RTFN Sous-index 2: Temps de cycle de base RTFL	M/O
0x121B vers 0x121D	Réservé pour d'autres paramètres de sécurité					
0x121E	VAR	Tolérance T_{TO} de temporisation SPDO	Unsigned8	FSF	Définit le niveau de dépassement de temporisation RxSPDO acceptable. Nombre sans unité, interprété en pourcentage.	M/O
0x121F vers 0x127F	Réservé pour d'autres paramètres de sécurité					
0x1C00 vers 0x1CFF	RECORD	Paramètre de communication RxSPDO	PDO COM_PAR	FSF		M/O
0x1D00 vers 0x1DFF	RECORD	Paramètre de mise en correspondance RxSPDO	Mise en correspondance PDO	FSF		M/O

Index	Objet	Nom	Type de données	Attribut	Description	Catégorie
0x1E00 vers 0x1EFF	RECORD	Paramètre de communication TxSPDO	PDO COM_PAR	FSF		M/O
0x1F00 vers 0x1FFF	RECORD	Paramètre de mise en correspondance TxSPDO	Mise en correspondance PDO	FSF		M/O

8.2.2.2 Type d'appareil

L'objet de type d'appareil indique le profil de l'appareil mis en œuvre, ainsi que sa fonction, et est spécifié dans le Tableau 16. Il comprend deux champs de 16 bits. Le premier champ est le numéro de profil de l'appareil, qui décrit le profil de l'appareil employé. Le second champ de 16 bits fournit des informations supplémentaires concernant les fonctions de l'appareil facultatives et fait partie intégrante du profil de l'appareil ou de la spécification du produit. La valeur 0x0000 désigne un appareil qui ne suit pas un profil normalisé. Pour les modules d'appareils multiples, le paramètre d'informations supplémentaires contient 0xFFFF et le numéro de profil d'appareil référencé par l'objet 0x1000 est le profil du premier appareil dans le dictionnaire d'objets de sécurité. Tous les autres appareils d'un module d'appareil multiple identifient leurs profils aux objets 0x67FF + (N x 0x800) avec N = numéro interne de l'appareil (compris entre 0 et 7). Ces entrées décrivent le type d'appareil de l'appareil précédent. Les appareils utilisent des numéros de profil compris entre quatre et sept pour les fonctions de sécurité, de sorte que les premiers objets d'application de sécurité commencent à 0x8000.

Tableau 16 – Type d'appareil

Attribut	Valeur
Index	0x1000
Nom	Type d'appareil
Description	Classification des appareils conforme à CANopen. D'autres informations sont données en [47]
Type d'objet	VAR
Type de données	Unsigned32
Catégorie	Obligatoire
Attribut d'accès	RO
Mise en correspondance PDO	Non
Plage de valeurs	Non
Valeur	Bits 0 à 15: Numéro de profil de l'appareil Bits 16 à 31: Information supplémentaire selon le profil d'appareil employé

8.2.2.3 Indicatif de sécurité (SID)

L'objet d'indicatif de sécurité est spécifié dans le Tableau 17. L'objet spécifie l'indicatif de sécurité d'un appareil de même nature. Il est obligatoire pour les appareils de sécurité.

Tableau 17 – Indicatif de sécurité

Attribut	Valeur
Index	0x1200
Nom	Indicatif de sécurité
Description	Indicatif unique de l'appareil
Type d'objet	VAR
Type de données	Unsigned16
Catégorie	Obligatoire
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	0x0001 à 0xFFFF
Valeur	Non

8.2.2.4 Liste de cadence (impulsions) du consommateur de sécurité

L'objet de cadence (impulsions) du consommateur de sécurité est spécifié dans le Tableau 19. La cadence (impulsions) du consommateur de sécurité définit tous les appareils de sécurité que l'appareil concerné doit contrôler. De plus, les paramètres des réponses de cadence (impulsions) sont configurés, ainsi que les paramètres relatifs aux réponses attendues. Le codage d'une entrée de cadence (impulsions) d'un consommateur de sécurité dans les limites d'une valeur OCTET_STRING est spécifié dans le Tableau 18.

Tableau 18 – Entrée de cadence (impulsions) d'un consommateur de sécurité

Octet	Type de données	Signification
0 à 3	Unsigned32	Adresse IPv4 du partenaire de communication. Pour le consommateur de cadence (impulsions) et la réponse attendue
4 à 19	Unsigned128	Adresse IPv6 du partenaire de communication. Pour le consommateur de cadence (impulsions) et la réponse attendue
20 à 21	Unsigned16	Le SID du partenaire de communication est l'indicatif unique de l'appareil. Pour le consommateur de cadence (impulsions) et la réponse attendue
22	Unsigned8	Type de transmission Pour le consommateur de cadence (impulsions), la réponse attendue et la réponse propre Description: Bit 7 (bit le plus significatif): Activation 0, non actif; 1 actif. Bits 6,5: Canal de communication 00 pour CDCL; 01 pour CDCN; 10 Réservé pour une utilisation future; 11 Réservé pour une utilisation future. Bit 4: Acheminé par une passerelle CP 18/1 – CP 18/2. 0 par défaut – aucune passerelle existante, 1 pour la passerelle. Ne doit pas être réglé pour PDO/cadence (impulsions) lorsque le canal de transmission est CDCN. Bit 3: Type de trame 0 pour la trame MAC, est utilisé uniquement pour RxSPDO sur le CDCN 1 pour la trame UDP. Bits 2,1,0 (bits les moins significatifs): Mode de transmission 001: Cyclique, autre: Réservé pour une utilisation future.

Octet	Type de données	Signification
23	Unsigned8	Réservé
24 à 27	Unsigned32	Le PID de cadence (impulsions) consommée est l'indicatif des paquets, utilisé pour vérifier l'émetteur approprié Pour le consommateur de cadence (impulsions)
28 à 29	Unsigned16	La temporisation de cadence (impulsions) spécifie le nombre de fréquences d'occurrence d'une cadence produite par le partenaire de communication. Les valeurs admises sont des multiples entiers du temps de cycle de base. Pour le consommateur de cadence (impulsions)
30 à 31	Unsigned16	Le multiplicateur de cycles pour la cadence (impulsions) consommée est obligatoire pour les réseaux comportant les passerelles CP 18/1 à CP 18/2. Il précise la fréquence d'écriture potentielle de la SPDU dans le canal de communication CDCL par la passerelle CDCN/CDCL. Pour le consommateur de cadence (impulsions) Valeurs admises: 0x0001, 0x0002, 0x0004, 0x0008, 0x0010, 0x0020, 0x0040, 0x0080, 0x0100, 0x0200, 0x0400, 0x0800, 0x1000, 0x2000, 0x4000, 0x8000
32 à 33	Unsigned16	Le décalage de cycle pour la cadence (impulsions) consommée est obligatoire pour les réseaux comportant les passerelles CP18/1 à CP 18/2. Il spécifie le décalage de la SPDU lors d'une transmission sur la CDCL. Pour le consommateur de cadence (impulsions) La plage valide est comprise entre 0 et (multiplicateur de cycles – 1)
34	Unsigned8	Le numéro de seuil de réception spécifie le nombre maximal de réceptions acceptable du même paquet. Pour le consommateur de cadence (impulsions)
35	Unsigned8	Réservé
36 à 39	Unsigned32	Le PID de la réponse attendue est l'indicatif des paquets, utilisé pour vérifier l'émetteur approprié Pour la réponse attendue
40 à 41	Unsigned16	Multiplicateur de cycles de la réponse attendue pour les réseaux comportant les passerelles CP18/1 à CP18/2. Pour la réponse attendue
42 à 43	Unsigned16	Décalage de cycle de la réponse attendue pour les réseaux comportant les passerelles CP18/1 à CP 18/2. Pour la réponse attendue
44 à 47	Unsigned32	PID de la réponse transmise. Pour la réponse propre
48 à 49	Unsigned16	Multiplicateur de cycles de la réponse transmise. Pour la réponse propre. Valeurs admises: 0x0001, 0x0002, 0x0004, 0x0008, 0x0010, 0x0020, 0x0040, 0x0080, 0x0100, 0x0200, 0x0400, 0x0800, 0x1000, 0x2000, 0x4000, 0x8000
50 à 51	Unsigned16	Décalage de cycles de la réponse transmise utilisé pour la CDCL uniquement. Pour la réponse propre. Plage 0 à (multiplicateur de cycles – 1)
52 à 55	Unsigned32	Retard maximal acceptable en µs de la réponse attendue, de l'envoi de la cadence (impulsions) à la réception de la réponse. Pour la réponse attendue
56	Unsigned8	Nombre d'envois de la réponse transmise. Pour la réponse propre
57	Unsigned8	Réservé

Tableau 19 – Cadence (impulsions) du consommateur de sécurité

Attribut	Valeur
Index	0x1216
Nom	Liste de la cadence (impulsions) du consommateur de sécurité
Type d'objet	ARRAY
Type de données	OCTET_STRING
Catégorie	Facultatif
Sous-index	0x00
Nom	Nombre d'entrées prises en charge
Description	Nombre de cadences (impulsions) de consommation (une pour chaque partenaire de communication)
Type de données	Unsigned8
Catégorie	Obligatoire
Attribut d'accès	RO
Mise en correspondance SPDO	Non
Plage de valeurs	0x01 à 0xFF
Valeur	Non
Sous-index	0x01
Nom	Cadence (impulsions) du consommateur
Description	Il doit y avoir au moins un partenaire de communication, une entrée est par conséquent obligatoire. Format décrit dans le Tableau 18
Type de données	OCTET_STRING
Catégorie	Obligatoire
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	Non
Valeur	Non
Sous-index	0x02 à 0xFE
Nom	Cadence (impulsions) du consommateur
Description	Entrées supplémentaires. Format décrit dans le Tableau 18
Type de données	OCTET_STRING
Catégorie	Facultatif
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	Non
Valeur	Non

8.2.2.5 Paramètre de cadence (impulsions) du producteur de sécurité

L'objet « Paramètre de cadence (impulsions) du producteur de sécurité » est spécifié dans le Tableau 20.

Tableau 20 – Paramètre de cadence (impulsions) du producteur de sécurité

Attribut	Valeur
Index	0x1217
Nom	Paramètre de cadence (impulsions) du producteur de sécurité
Type d'objet	RECORD
Type de données	PDO COMMUNICATION PARAMETER
Catégorie	Sous condition; obligatoire pour chaque TxSPDO pris en charge
Sous-index	0x00
Nom	Nombre d'entrées
Type de données	Unsigned8
Catégorie	Obligatoire
Attribut d'accès	RO
Mise en correspondance SPDO	Non
Plage de valeurs	0x01 à 0x0C
Valeur	Non
Sous-index	0x01
Nom	RTFL PID
Description	Indicatif de paquets si transmis sur la CDCL
Type de données	Unsigned32
Catégorie	Sous condition
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	0x01 à 0x00FFFFFF
Valeur	Non
Sous-index	0x02
Nom	RTFN PID
Description	Indicatif de paquets si transmis sur le CDCN
Type de données	Unsigned32
Catégorie	Sous condition
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	0x01 à 0x00FFFFFF
Valeur	Non
Sous-index	0x03
Nom	Réservé
Type de données	Unsigned32
Sous-index	0x04
Nom	Type de transmission
Description	Spécifie le mode de transmission (voir Tableau 18). Doit être mis au mode cyclique
Type de données	Unsigned8
Catégorie	Obligatoire
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	Non

Attribut	Valeur
Valeur	Non
Sous-index	0x05
Nom	ID de synchronisation temporelle
Description	Non utilisé, car le type de transmission est cyclique.
Type de données	Unsigned16
Catégorie	Sous condition
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	0x00 à 0xFF
Valeur	Non
Sous-index	0x06
Nom	Durée d'événement
Description	Non utilisé, car le type de transmission est cyclique
Type de données	Unsigned16
Catégorie	Sous condition
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	Non
Valeur	Non
Sous-index	0x07
Nom	Multiplicateur de cycles
Description	Spécifie la fréquence de transmission (multiple du temps de cycle de base)
Type de données	Unsigned16
Catégorie	Sous condition
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	0x0001, 0x0002, 0x0004, 0x0008, 0x0010, 0x0020, 0x0040, 0x0080, 0x0100, 0x0200, 0x0400, 0x0800, 0x1000, 0x2000, 0x4000, 0x8000
Valeur	Non
Sous-index	0x08
Nom	Décalage de cycle
Description	Spécifie les cycles effectifs de transmission
Type de données	Unsigned16
Catégorie	Sous condition
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	0 à (multiplicateur de cycles – 1)
Valeur	Non
Sous-index	0x09
Nom	Nombre d'envois
Description	Nombre d'occurrences de transmission
Type de données	Unsigned8
Catégorie	Obligatoire
Attribut d'accès	FSF

Attribut	Valeur
Mise en correspondance SPDO	Non
Plage de valeurs	Non
Valeur	2
Sous-index	0x0A
Nom	Adresse de l'appareil
Description	Non utilisé, car la transmission s'effectue sur le CDCN ou la CDCL
Type de données	Unsigned16
Catégorie	Sous condition
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	0x0000 à 0x0200
Valeur	Non
Sous-index	0x0B
Nom	adresse IPv4
Type de données	Unsigned32
Catégorie	Sous condition
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	Non
Valeur	Non
Sous-index	0x0C
Nom	adresse IPv6
Type de données	Unsigned128
Catégorie	Sous condition
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	Non
Valeur	Non

8.2.2.6 Durées de cycle des bus de sécurité

L'objet « Durée de cycle des bus de sécurité » est spécifié dans le Tableau 21. Les durées de cycle des bus de sécurité permettent de calculer les valeurs de temporisation pour les paquets de sécurité.

Tableau 21 – Durées de cycle des bus de sécurité

Attribut	Valeur
Index	0x1218
Nom	Durées de cycle des bus de sécurité
Type d'objet	ARRAY
Type de données	Unsigned32
Catégorie	Obligatoire
Sous-index	0x00
Nom	Nombre d'entrées prises en charge
Type de données	Unsigned8

Attribut	Valeur
Catégorie	Obligatoire
Attribut d'accès	RO
Mise en correspondance SPDO	Non
Plage de valeurs	0x01 à 0x02
Valeur	Non
Sous-index	0x01
Nom	Durée de cycle de base du RTFN de sécurité
Description	Durée de cycle de base pour le CDCN en µs
Type de données	Unsigned32
Catégorie	Sous condition
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	Non
Valeur	Non
Sous-index	0x02
Nom	Durée de cycle de base de la RTFL de sécurité
Description	Durée de cycle de base pour la CDCL en µs
Type de données	Unsigned32
Catégorie	Sous condition
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	Non
Valeur	Non

8.2.2.7 Tolérance de temporisation SPDO

L'objet « Tolérance de temporisation SPDO » est spécifié dans le Tableau 22.

Tableau 22 – Tolérance de temporisation SPDO

Attribut	Valeur
Index	0x121E
Nom	Tolérance de temporisation SPDO
Description	Spécifie le niveau de dépassement potentiel de la temporisation SPDU Donné en pourcentage
Type d'objet	VAR
Type de données	Unsigned8
Catégorie	Sous condition
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	0x00 à 0xFF
Valeur	Non

8.2.2.8 Paramètre de communication RxSPDO

L'objet « Paramètre de communication SPDO de réception » est spécifié dans le Tableau 23.

Tableau 23 – Paramètre de communication SPDO de réception

Attribut	Valeur
Index	0x1C00 – 0x1CFF
Nom	Paramètre de communication SPDO de réception
Type d'objet	RECORD
Type de données	PDO COMMUNICATION PARAMETER
Catégorie	Sous condition; obligatoire pour chaque RxSPDO pris en charge
Sous-index	0x00
Nom	Nombre d'entrées
Type de données	Unsigned8
Catégorie	Obligatoire
Attribut d'accès	RO
Mise en correspondance SPDO	Non
Plage de valeurs	0x01 à 0x0C
Valeur	Non
Sous-index	0x01
Nom	RTFL PID
Description	Indicatif de paquets en cas de transmission CDCL
Type de données	Unsigned32
Catégorie	Sous condition
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	0x01 à 0xFFFFFFFF
Valeur	Non
Sous-index	0x02
Nom	RTFN PID
Description	Indicatif de paquets en cas de transmission CDCN
Type de données	Unsigned32
Catégorie	Sous condition
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	0x01 à 0xFFFFFFFF
Valeur	Non
Sous-index	0x03
Nom	SID
Description	Indicatif unique du partenaire de communication
Type de données	Unsigned16
Catégorie	Obligatoire
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	Non
Valeur	Non
Sous-index	0x04
Nom	Type de transmission

Attribut	Valeur
Description	Spécifie le mode de transmission (voir Tableau 18). Doit être mis au mode cyclique
Type de données	Unsigned8
Catégorie	Obligatoire
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	Non
Valeur	Non
Sous-index	0x05
Nom	ID de synchronisation temporelle
Description	Non utilisé, car le type de transmission est spécifié comme cyclique
Type de données	Unsigned16
Catégorie	Sous condition
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	0x0000 à 0xFFFF
Valeur	Non
Sous-index	0x06
Nom	Multiplicateur de temporisation
Description	Spécifie la fréquence prévue du paquet
Type de données	Unsigned16
Catégorie	Facultatif
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	0x0000 à 0xFFFF
Valeur	Non
Sous-index	0x07
Nom	Multiplicateur de cycles
Description	Spécifie la fréquence d'écriture de la SPDU dans le canal de communication CDCL par les passerelles CP18/1 à CP18/2. Obligatoire si la CDCL est utilisée pour transmission et si les passerelles CP18/1 à CP18/2 sont présentes. Non utilisé pour tous les autres cas
Type de données	Unsigned16
Catégorie	Sous condition
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	0x01 à 0xFFFF
Valeur	Non
Sous-index	0x08
Nom	Décalage de cycle
Description	Décalage de cycle (écriture de la SPDU dans le canal CDCL). Obligatoire si la CDCL est utilisée pour transmission et si les passerelles CP18/1 à CP18/2 sont présentes. Non utilisé pour tous les autres cas
Type de données	Unsigned16

Attribut	Valeur
Catégorie	Sous condition
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	0x00 à 0xFFFE
Valeur	Non
Sous-index	0x09
Nom	Nombre de réceptions admises
Description	Nombre maximal de réceptions potentielles de la SPDU
Type de données	Unsigned8
Catégorie	Obligatoire
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	Non
Valeur	2
Sous-index	0x0A
Nom	Adresse de l'appareil
Description	Non utilisé, car la transmission s'effectue sur le CDCN ou la CDCL
Type de données	Unsigned16
Catégorie	Sous condition
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	0x00 à 0x200
Valeur	Non
Sous-index	0x0B
Nom	adresse IPv4
Type de données	Unsigned32
Catégorie	Sous condition
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	Non
Valeur	Non
Sous-index	0x0C
Nom	adresse IPv6
Type de données	Unsigned128
Catégorie	Sous condition
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	Non
Valeur	Non

8.2.2.9 Paramètre de communication TxSPDO

L'objet « Paramètre de communication SPDO de transmission » est spécifié dans le Tableau 24.

Tableau 24 – Paramètre de communication SPDO de transmission

Attribut	Valeur
Index	0x1E00 – 0x1EFF
Nom	Paramètre de communication SPDO de transmission
Type d'objet	RECORD
Type de données	PDO COMMUNICATION PARAMETER
Catégorie	Sous condition; obligatoire pour chaque TxSPDO pris en charge
Sous-index	0x00
Nom	Nombre d'entrées
Type de données	Unsigned8
Catégorie	Obligatoire
Attribut d'accès	RO
Mise en correspondance SPDO	Non
Plage de valeurs	0x01 à 0x0C
Valeur	Non
Sous-index	0x01
Nom	RTFL PID
Description	Indicatif de paquets en cas de transmission CDCL
Type de données	Unsigned32
Catégorie	Sous condition
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	0x01 à 0xFFFFFFFF
Valeur	Non
Sous-index	0x02
Nom	RTFN PID
Description	Indicatif de paquets en cas de transmission CDCN
Type de données	Unsigned32
Catégorie	Sous condition
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	0x01 à 0xFFFFFFFF
Valeur	Non
Sous-index	0x04
Nom	Type de transmission
Description	Spécifie le mode de transmission (voir Tableau 18). Doit être mis au mode cyclique
Type de données	Unsigned8
Catégorie	Obligatoire
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	Non
Valeur	Non
Sous-index	0x05
Nom	ID de synchronisation temporelle

Attribut	Valeur
Description	Non utilisé, car le type de transmission est spécifié comme cyclique
Type de données	Unsigned16
Catégorie	Sous condition
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	0x00 à 0xFF
Valeur	Non
Sous-index	0x06
Nom	Durée d'événement
Description	Non utilisé, car le type de transmission est spécifié comme cyclique
Type de données	Unsigned16
Catégorie	Sous condition
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	Non
Valeur	Non
Sous-index	0x07
Nom	Multiplicateur de cycles
Description	Spécifie la fréquence de transmission.
Type de données	Unsigned16
Catégorie	Sous condition
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	0x0001, 0x0002, 0x0004, 0x0008, 0x0010, 0x0020, 0x0040, 0x0080, 0x0100, 0x0200, 0x0400, 0x0800, 0x1000, 0x2000, 0x4000, 0x8000
Valeur	Non
Sous-index	0x08
Nom	Décalage de cycle
Description	Cycles de transmission effectifs.
Type de données	Unsigned16
Catégorie	Sous condition
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	0 à (multiplicateur de cycles – 1)
Valeur	Non
Sous-index	0x09
Nom	Nombre d'envois
Description	Spécifie la fréquence de transmission du paquet.
Type de données	Unsigned8
Catégorie	Obligatoire
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	Non
Valeur	2

Attribut	Valeur
Sous-index	0x0A
Nom	Adresse de l'appareil
Description	Non utilisé, car la transmission s'effectue sur le CDCN ou la CDCL
Type de données	Unsigned16
Catégorie	Sous condition
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	0x00 à 0x200
Valeur	Non
Sous-index	0x0B
Nom	adresse IPv4
Type de données	Unsigned32
Catégorie	Sous condition
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	Non
Valeur	Non
Sous-index	0x0C
Nom	adresse IPv6
Type de données	Unsigned128
Catégorie	Sous condition
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	Non
Valeur	Non

8.2.2.10 Mise en correspondance SPDO

8.2.2.10.1 Principe de mise en correspondance SPDO

Les paramètres de mise en correspondance SPDO définissent le contenu d'un SPDO. Un SPDO valide contient au moins un objet d'application de sécurité et au plus 254. Le codage d'une entrée de mise en correspondance est spécifié dans le Tableau 25.

Tableau 25 – Format de mise en correspondance

Bit	Nom	Signification
0 à 7	Longueur	Longueur de l'objet d'application de sécurité en bits
8 à 15	Sous-index	Sous-index de l'objet d'application de sécurité à mettre en correspondance. Le dictionnaire d'objets de sécurité est organisé sous forme de tableau avec éléments clés (index, sous-index). Cette mise en correspondance spécifie la clé de consultation pour cet objet d'application.
16 à 31	Index	Index de l'objet d'application de sécurité à mettre en correspondance

8.2.2.10.2 Paramètre de mise en correspondance RxSPDO

L'objet « Paramètre de mise en correspondance SPDO de réception » est spécifié dans le Tableau 26.

Tableau 26 – Paramètre de mise en correspondance SPDO de réception

Attribut	Valeur
Index	0x1D00 à 0x1DFF
Nom	Paramètre de mise en correspondance SPDO de réception
Description	Mise en correspondance de l'objet de la PDU de sécurité au dictionnaire d'objets de sécurité. Voir Tableau 25
Type d'objet	RECORD
Type de données	PDO_MAPPING
Catégorie	Sous condition; obligatoire pour chaque RxSPDO pris en charge
Sous-index	0x00
Nom	Nombre d'objets d'application de sécurité mis en correspondance
Type de données	Unsigned8
Catégorie	Obligatoire
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	0x00 à 0xFE
Valeur	Non
Sous-index	0x01 à 0xFE
Nom	Mise en correspondance SPDO pour le nème objet d'application de sécurité à mettre en correspondance
Description	Spécifié dans le Tableau 25
Type de données	Unsigned32
Catégorie	Sous condition selon le nombre et la taille des objets à mettre en correspondance
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	Non
Valeur	Non

8.2.2.10.3 Paramètre de mise en correspondance TxSPDO

L'objet « Paramètre de mise en correspondance SPDO de transmission » est spécifié dans le Tableau 27.

Tableau 27 – Paramètre de mise en correspondance SPDO de transmission

Attribut	Valeur
Index	0x1E00 à 0x1EFF
Nom	Paramètre de mise en correspondance SPDO de transmission
Description	Mise en correspondance de l'objet du dictionnaire d'objets de sécurité à la PDU de sécurité. Voir Tableau 25
Type d'objet	RECORD
Type de données	PDO_MAPPING
Catégorie	Sous condition; obligatoire pour chaque TxSPDO pris en charge
Sous-index	0x00
Nom	Nombre d'objets d'application de sécurité mis en correspondance
Type de données	Unsigned8
Catégorie	Obligatoire

Attribut	Valeur
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	0x01 à 0xFE
Valeur	Non
Sous-index	0x01 à 0xFE
Nom	Mise en correspondance SPDO pour le nème objet d'application de sécurité à mettre en correspondance
Description	Spécifié dans le Tableau 25
Type de données	Unsigned32
Catégorie	Sous condition selon le nombre et la taille des objets à mettre en correspondance
Attribut d'accès	FSF
Mise en correspondance SPDO	Non
Plage de valeurs	Non
Valeur	Non

8.2.3 Section de profil d'appareil normalisé

Les objets d'application de sécurité peuvent être mis en correspondance dans les SPDO. Les objets d'application de sécurité sont situés dans la zone de dictionnaire d'objets de sécurité de 0x8000 à 0x9FFF. Ces objets sont spécifiques au fabricant et à l'application.

9 Exigences relatives au système

9.1 Voyants et commutateurs

9.1.1 Etats des voyants et fréquences de clignotement

Les états des voyants et les fréquences de clignotement sont définis dans le Tableau 28. Les durées énumérées doivent être respectées avec une tolérance de moins de ± 25%.

Tableau 28 – Définition des états des voyants

Etat du voyant	Définition
OFF	Le voyant doit être éteint de manière constante
ON	Le voyant doit être allumé de manière constante
BLINKING 1 Hz	Le voyant doit s'allumer et s'éteindre avec une fréquence de 1 Hz
BLINKING 2 Hz	Le voyant doit s'allumer et s'éteindre avec une fréquence de 2 Hz

9.1.2 Voyants

Il convient que les appareils qui prennent en charge le protocole FSCP 18/1 comportent un voyant STATUS. Ce voyant, généralement une DEL, participe à la recherche de pannes, à l'examen visuel, aux opérations de maintenance et au diagnostic des problèmes constatés. Si un appareil prend en charge le voyant STATUS, ce dernier doit satisfaire à cette spécification. D'autres voyants peuvent être mis en oeuvre.

Le voyant STATUS doit indiquer l'état de la communication FSCP 18/1. Un voyant bicolore unique (vert/rouge) doit être utilisé.

Une étiquette « FS SNp » doit être apposée sur le voyant STATUS.

Les états du voyant STATUS sont spécifiés dans le Tableau 29.

Tableau 29 – Etats du voyant STATUS

Etat du voyant	Définition
OFF	Aucune communication de données de processus de sécurité n'est active
GREEN ON	Toutes les communications de données de processus de sécurité configurées (SPDO) sont actives
GREEN BLINKING 1 Hz	Au moins un SPDO est actif et au moins un SPDO est inactif
RED ON	Configuration non valide ou incompatible
RED BLINKING 2 Hz	Erreur interne

9.1.3 Commutateurs

Il n'existe aucun commutateur pour le protocole FSP 18/1.

9.2 Lignes directrices d'installation

Les lignes directrices d'installation appropriées sont spécifiées par l'IEC 61918.

9.3 Temps de réponse de la fonction de sécurité

9.3.1 Généralités

Une fonction de sécurité peut être constituée de plusieurs composantes. Afin de pouvoir déterminer le temps de réponse de la fonction de sécurité, ladite fonction est décomposée dans les différentes composantes illustrées à la Figure 16.

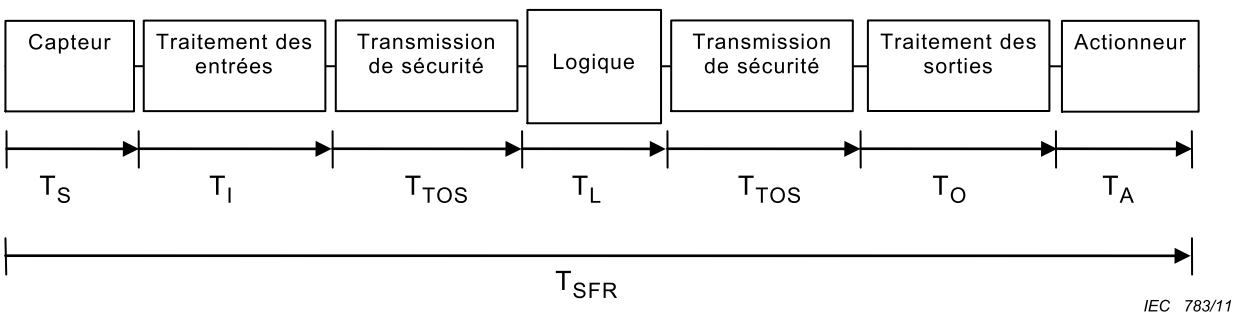


Figure 16 – Composantes du temps de réponse de la fonction de sécurité

Le canal de la fonction de sécurité se compose d'un capteur (par exemple, rideau de lumière ou bouton d'arrêt d'urgence) qui permet de détecter l'activation de la fonction de sécurité. Ce capteur convertit le signal physique en un signal électrique. Ce signal électrique est relié à un appareil d'entrée (par exemple, un module d'entrée de sécurité fonctionnelle) qui convertit le signal électrique en une information d'entrée logique. Le système de communication de sécurité permet de transmettre l'information d'entrée logique au contrôleur logique de sécurité. Ce dernier compile l'information d'entrée logique en information de sortie logique, qui est transmise à un appareil de sortie (par exemple, un module de sortie de sécurité fonctionnelle) par l'intermédiaire du système de communication de sécurité. L'information de sortie logique est convertie en un signal de sortie physique relié à un actionneur. Ce dernier exécute la réaction physique. Chaque composante est décrite par un comportement temporel caractéristique.

Les hypothèses générales suivantes s'appliquent à d'autres prises en considération.

- Le fonctionnement de toutes les composantes du canal de la fonction de sécurité est asynchrone.
- Toutes les composantes du canal de la fonction de sécurité sont décrites par un temps de traitement ou de réponse le plus défavorable garanti dans des conditions autres que des conditions d'erreur.
- Un temporisateur superposé (T_{TOi}) est associé à chaque composante pour des raisons de sécurité.
- Il doit être supposé, afin de calculer le temps de réponse de la fonction de sécurité, que le parcours de signal concerné comporte une erreur ou une défaillance, qui contribue au temps de différence maximal entre sa temporisation et son temps de traitement ou de réponse le plus défavorable.

Les temps caractéristiques du capteur, des entrées, de la logique, des sorties et de l'actionneur des appareils ne relèvent pas du domaine d'application de la présente norme. Il convient que les informations cohérentes pour ces valeurs caractéristiques proviennent des spécifications des composantes. Chaque appareil doit fournir ces valeurs comme partie intégrante de ses propriétés intrinsèques.

9.3.2 Détermination de la procédure de contrôle de retard FSCP 18/1

Le protocole FSCP 18/1 définit une procédure de contrôle de retard configurable (temporisation) pour la remise de données de processus de sécurité côté récepteur d'une relation de communication. Cette procédure de contrôle est mise en œuvre par la temporisation de communication T_{TOS}.

Deux transmissions de sécurité sont nécessaires pour le canal de la fonction de sécurité. Les composantes logique et de traitement de sortie fonctionnent comme un récepteur et mettent en œuvre la procédure de contrôle de retard. L'Equation (2) décrit le calcul de T_{TOS}.

$$T_{TOS} = T_{cycle} + \Delta T \qquad (2)$$

La SHB n'influence pas T_{TOS} dans la mesure où seule la synchronisation des horloges système est requise. Lorsque la cadence (impulsion) à de sécurité détecte des retards inacceptables, l'état de sécurité intrinsèque est alors activé (voir 7.3).

9.3.3 Calcul du temps de réponse de la fonction de sécurité le plus défavorable

Le canal de la fonction de sécurité de base utilisé pour calculer la fonction de sécurité la plus défavorable est illustré à la Figure 16.

Le temps de réponse de la fonction de sécurité peut être calculé selon l'Equation (3).

Il doit être supposé que le canal de la fonction de sécurité comporte une erreur ou une défaillance pour obtenir le temps de réponse de la fonction de sécurité le plus défavorable. Cette erreur ou défaillance contribue à la différence maximale observée entre son temps de retard le plus défavorable et son temps de temporisation.

$$T_{SFR} = T_S + T_I + T_T + T_L + T_T + T_O + T_A + \max_{i=S,I,...A}(T_{TOi} - T_i) \qquad (3)$$

NOTE L'index « i » identifie les composantes S, I, T, L, O et A dans l'Equation (3).

Les fabricants de systèmes doivent fournir, si nécessaire, leur propre méthode de calcul adaptée.

9.4 Durée des demandes

La durée de la demande émise par l'application relative à la sécurité à la couche de communication de sécurité peut être équivalente ou supérieure au temps de sécurité de processus ou au temps de temporisation FSCP 18/1 (T_{TO}).

9.5 Contraintes liées au calcul des caractéristiques du système

9.5.1 Contraintes relatives à la sécurité

9.5.1.1 Généralités

Les conditions aux limites et les contraintes relatives à l'évaluation de la sécurité du protocole FSCP 18/1, et applicables aux calculs appropriés du taux d'erreur résiduel sont décrites dans les articles suivants.

9.5.1.2 Nombre de collecteurs d'information

Le nombre de appareils de production et de consommation pour un réseau FSCP 18/1 est limité à 512. Le nombre de collecteurs d'information est limité à 511 appareils de consommation dans le cas d'une relation 1:*n*.

9.5.1.3 Limite de fréquence des messages

La fréquence des messages ne doit pas dépasser 1 000 messages de sécurité à la seconde. Il doit être tenu compte du nombre d'appareils de production et du temps de cycle afin qu'ils ne dépassent pas la limite de taux de messages, tel qu'indiqué dans les Equations (4) à (6).

$$MR_{SPDO} = \sum_{I \in SPDO} \frac{1\,000\,000 \times NS_I}{CM_I \times T_{BC}} \tag{4}$$

$$MR_{SHB} = \sum_{D1 \in devices} \left[\sum_{\substack{D2 \in devices \\ D2 \neq D1}} \frac{1\ 000\,000 \times NS_{D1} \times 2}{CM_{D1} \times T_{BC}} \right] \tag{5}$$

$$MR = MR_{SPDO} + MR_{SHB} \tag{6}$$

où

CM_{D1} est le paramètre de cadence (impulsions) du producteur de sécurité (Index: 0x1217, Sous-index: 0x07, multiplicateur de cycles) transmis par l'appareil D1 (voir le Tableau 20);

CM_I est le paramètre de communication SPDO de transmission (Index: 0x1E00 - 0x1EFF, Sous-index: 0x07, multiplicateur de cycles) pour SPDOI (voir le Tableau 24);

NS_{D1} est le paramètre de cadence (impulsions) du producteur de sécurité (Index: 0x1217, Sous-index: 0x09, Nombre d'envois) transmis par l'appareil D1 (voir le Tableau 20);

NS_I est le paramètre de communication SPDO de transmission (Index: 0x1E00 - 0x1EFF, Sous-index: 0x09, Nombre d'envois) pour SPDOI (voir le Tableau 24);

MR est le taux de message total;

MR_{SHB} est le taux de messages pour les SHB;

MR_{SPDO} est le taux de messages pour les SPDO;

T_{BC} est les temps de cycle de bus de sécurité. Paramètre dépendant si CP 18/1 (Index: 0x1218, Sous-index 0x02, temps de cycle de base RTFL de sécurité) ou CP 18/2 (Index: 0x1218, Sous-index: 0x01, temps de cycle de base RTFN de sécurité) est utilisé (voir le Tableau 21).

9.5.1.4 Taille des messages

La taille de message d'une PDU de sécurité constituée des champs de données illustrés à la Figure 17 est limitée de 0 à 128 octets.

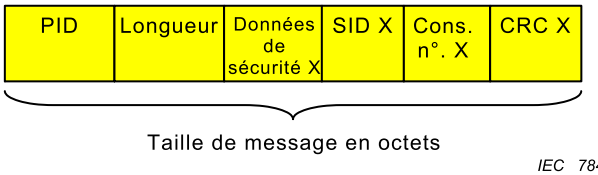


Figure 17 – Champs de données pris en compte pour le calcul de la taille des messages

9.5.1.5 Taux d'erreurs sur les bits

Le taux maximal d'erreurs sur les bits ne doit pas dépasser 0,01.

9.5.2 Considérations d'ordre probabiliste

Le mécanisme de contrôle de l'intégrité des données du protocole FSCP 18/1 est totalement indépendant des mécanismes du système de communication sous-jacent, qui est alors appelé « canal noir ».

La Figure 18 illustre les diagrammes des probabilités d'erreurs résiduelles applicables au polynôme de 32 bits utilisé (distance de Hamming minimale de 6). Les diagrammes s'appliquent pour des longueurs de données de 128 octets tel que spécifié en 9.5.1.4, incluant la signature CRC et intégrant la structure du PDU de sécurité global tel que décrit au 7.1. Il a été calculé que la PFH résultante du canal de communication est inférieure ou égale à 10^{-9}. Ce niveau équivaut à $5{,}43 \times 10^{-19}$ pour la probabilité d'erreur résiduelle d'une PDU telle qu'illustrée à la Figure 18. Le mécanisme de contrôle d'intégrité des données doit être obligatoirement utilisé pour atteindre ces niveaux (voir 7.1.1.2)

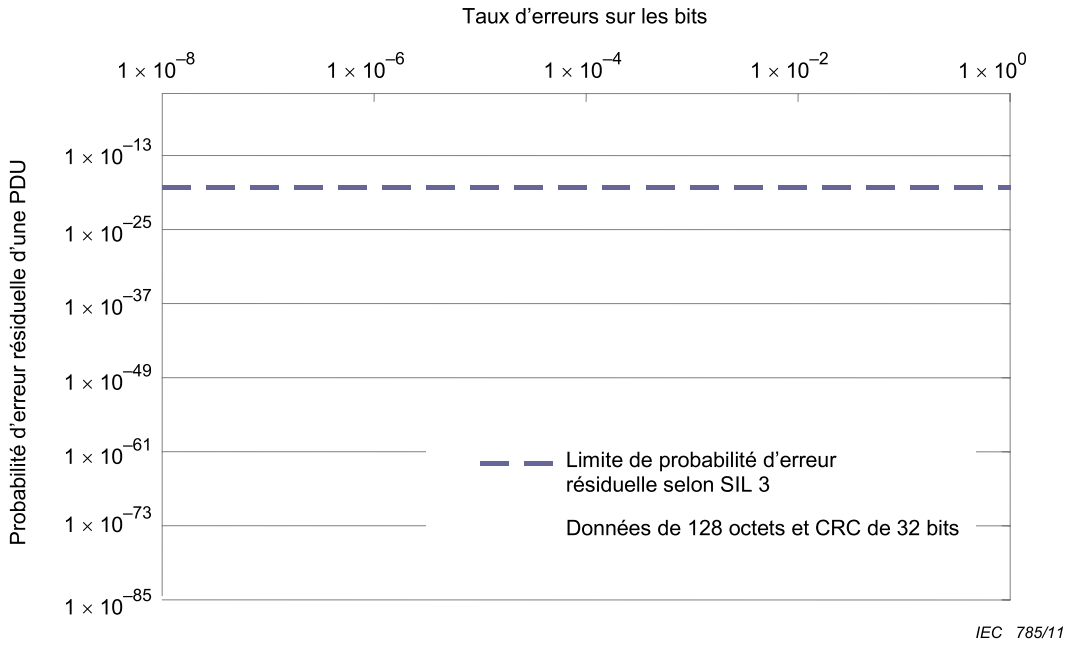


Figure 18 – Taux d'erreurs résiduelles

9.6 Maintenance

Ce protocole ne fait l'objet d'aucune exigence de maintenance particulière.

9.7 Manuel de sécurité

Le fabricant de l'appareil de sécurité doit fournir avec l'appareil un manuel de sécurité conforme aux exigences de l'IEC 61508-2 Outre les exigences énumérées dans l'IEC 61508-2, les informations suivantes doivent être fournies:

- le nom et l'adresse du fabricant;
- le temps T_i le plus défavorable;
- le temps de temporisation T_{TOi};
- Probabilité de défaillance à la demande PFH;
- Niveau d'intégrité de sécurité SIL;
- Intervalle de l'essai périodique T_1 (selon IEC 61508-6) et/ou Mission T_m (selon ISO 13849-1);
- Version(s) du protocole prise(s) en charge (voir 7.1.3.4) sauf dans le cas où seule la version 1 du protocole est prise en charge.

NOTE Les temps peuvent dépendre des fonctions de sécurité et des modes de fonctionnement individuels.

10 Evaluation

Il est fortement recommandé aux ingénieurs d'application du FSCP 18/1 d'obtenir la vérification auprès d'un organisme compétent indépendant pour tous les aspects de sécurité fonctionnelle du produit, tant du protocole que de toute application. Il est fortement recommandé aux ingénieurs d'application du FSCP 18/1 d'obtenir la preuve qu'un organisme compétent indépendant a réalisé un essai de conformité approprié.

Le fabricant d'un produit de sécurité est responsable de la mise en œuvre correcte de la technologie de couche de communication de sécurité, ainsi que de l'exactitude et de l'exhaustivité de l'information orientée produit et des renseignements sur le produit. Les informations complètes sont fournies en [46].

Annex A
(informative)

Informations supplémentaires pour les profils de communication de sécurité fonctionnelle de protocole CPF 18

Il n'existe aucune information supplémentaire concernant ce FSCP.

Annex B
(informative)

Information pour l'évaluation des profils de communication de sécurité fonctionnelle de protocole CPF 18

Des informations sur les laboratoires d'essai qui vérifient et valident la conformité des produits FSCP 18/1 avec l'IEC 61784-3-18 peuvent être obtenues auprès des comités nationaux de l'IEC ou de l'institution suivante:

Safety Network International e.V.
Robert-Bosch-Str.30
73760 Ostfildern
ALLEMAGNE

Téléphone: +49 711 3409 118
Télécopie: +49 711 3409 449
e-mail: info@safety-network.de
URL: www.safety-network.de

Bibliographie

[1] IEC 60050 (toutes parties), *Vocabulaire Electrotechnique International*

NOTE Voir également le dictionnaire multilingue de l'IEC – Electricité, électronique et télécommunications (disponible sur CD-ROM et à l'adresse http://www.electropedia.org).

[2] IEC 60204-1, *Sécurité des machines – Équipement électrique des machines – Partie 1: Règles générales*

[3] IEC/TS 61000-1-2, *Electromagnetic compatibility (EMC) – Part 1-2: General – Methodology for the achievement of the functional safety of electrical and electronic equipment with regard to electromagnetic phenomena* (disponible uniquement en anglais)

[4] IEC 61131-6[5], *Programmable controllers – Part 6: Functional safety* (disponible uniquement en anglais)

[5] IEC 61158 (toutes parties), *Industrial communication networks – Fieldbus specifications* (disponible uniquement en anglais)

[6] IEC 61326-3-1, *Matériel électrique de mesure, de commande et de laboratoire – Exigences relatives à la CEM – Partie 3-1: Exigences d'immunité pour les systèmes relatifs à la sécurité et pour les matériels destinés à réaliser des fonctions relatives à la sécurité (sécurité fonctionnelle) – Applications industrielles générales*

[7] IEC 61326-3-2, *Matériel électrique de mesure, de commande et de laboratoire – Exigences relatives à la CEM – Partie 3-2: Exigences d'immunité pour les systèmes relatifs à la sécurité et pour les matériels destinés à réaliser des fonctions relatives à la sécurité (sécurité fonctionnelle) – Applications industrielles dont l'environnement électromagnétique est spécifié*

[8] IEC 61496 (toutes parties), *Sécurité des machines – Equipements de protection électro-sensibles*

[9] IEC 61508-1:2010, *Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité – Partie 1: Exigences générales*

[10] IEC 61508-4:2010, *Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité – Partie 4: Définitions et abréviations*

[11] IEC 61508-5:2010, *Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité – Partie 5: Exemples de méthodes de détermination des niveaux d'intégrité de sécurité*

[12] IEC 61511 (toutes parties), *Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur des industries de transformation*

[13]

[14] IEC/PWI 61784-4[6], *Industrial communication networks – Profiles – Part 4: Secure communications for fieldbuses* (disponible uniquement en anglais)

[15] IEC 61784-5 (toutes parties), *Industrial communication networks – Profiles – Part 5: Installation of fieldbuses – Installation profiles for CPF x* (disponible uniquement en anglais)

[16] IEC 61800-5-2, *Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional* (disponible uniquement en anglais)

[17] IEC/TR 62059-11, *Equipements de comptage de l'électricité – Sûreté de fonctionnement – Partie 11: Concepts généraux*

[18] IEC 62061, *Sécurité des machines - Sécurité fonctionnelle des systèmes de commande électriques, électroniques et électroniques programmables relatifs à la sécurité*

[19] IEC/TR 62210, *Power system control and associated communications – Data and communication security* (disponible uniquement en anglais)

---

5 En cours d'élaboration.

6 A l'étude.

[20] IEC 62280-1, *Applications ferroviaires – Systèmes de signalisation, de télécommunication et de traitement – Partie 1: Communication de sécurité sur des systèmes de transmission fermés*

[21] IEC 62280-2, *Applications ferroviaires – Systèmes de signalisation, de télécommunication et de traitement – Partie 2: Communication de sécurité sur des systèmes de transmission ouverts*

[22] IEC 62443 (toutes parties), *Industrial communication networks – Network and system security* (disponible uniquement en anglais)

[23] ISO/IEC Guide 51:1999, *Aspects liés à la sécurité – Principes directeurs pour les inclure dans les normes*

[24] ISO/IEC 2382-14, *Technologies de l'information – Vocabulaire – Partie 14: Fiabilité, maintenabilité et disponibilité*

[25] ISO/IEC 2382-16, *Technologies de l'information – Vocabulaire – Partie 16: Théorie de l'information*

[26] ISO/IEC 7498 (toutes parties), *Technologies de l'information – Interconnexion de systèmes ouverts (OSI) – Modèle de référence de base*

[27] ISO 10218-1, *Robots pour environnements industriels – Exigences de sécurité – Partie 1: Robot*

[28] ISO 12100-1, *Sécurité des machines – Notions fondamentales, principes généraux de conception – Partie 1: terminologie de base, méthodologie*

[29] ISO 13849-1, *Sécurité des machines – Parties des systèmes de commande relatives à la sécurité – Partie 1: principes généraux de conception*

[30] ISO 13849-2, *Sécurité des machines – Parties des systèmes de commande relatives à la sécurité – Partie 2: Validation*

[31] ISO 14121, *Sécurité des machines – Principes pour l'appréciation du risque*

[32] ANSI/ISA-84.00.01-2004 (all parts), *Functional Safety: Safety Instrumented Systems for the Process Industry Sector*

[33] VDI/VDE 2180 (toutes parties), *Safeguarding of industrial process plants by means of process control engineering*

[34] GS-ET-26[7], *Grundsatz für die Prüfung und Zertifizierung von Bussystemen für die Übertragung sicherheitsrelevanter Nachrichten*, May 2002. HVBG, Gustav-Heinemann-Ufer 130, D-50968 Köln ("*Principles for Test and Certification of Bus Systems for Safety relevant Communication*")

[35] ANDREW S. TANENBAUM, *Computer Networks*, 4th Edition, Prentice Hall, N.J., ISBN-10:0130661023, ISBN-13: 978-0130661029

[36] W. WESLEY PETERSON, *Error-Correcting Codes*, 2nd Edition 1981, MIT-Press, ISBN 0-262-16-039-0

[37] BRUCE P. DOUGLASS, *Doing Hard Time*, 1999, Addison-Wesley, ISBN 0-201-49837-5

[38] *New concepts for safety-related bus systems*, 3rd International Symposium "Programmable Electronic Systems in Safety Related Applications ", May 1998, from Dr. Michael Schäfer, BG-Institute for Occupational Safety and Health.

[39] DIETER CONRADS, *Datenkommunikation*, 3rd Edition 1996, Vieweg, ISBN 3-528-245891

[40] German IEC subgroup DKE AK 767.0.4: *EMC and Functional Safety*, Spring 2002

[41] NFPA79 (2002), *Electrical Standard for Industrial Machinery*

[42] GUY E. CASTAGNOLI, *On the Minimum Distance of Long Cyclic Codes and Cyclic Redundancy-Check Codes*, 1989, Dissertation No. 8979 of ETH Zurich, Switzerland

---

7 GS-ET-26 constitue l'un des points de départ de l'élaboration de la présente partie. Il fait actuellement l'objet d'une révision importante.

[43] GUY E. CASTAGNOLI, STEFAN BRÄUER, and MARTIN HERRMANN, *Optimization of Cyclic Redundancy-Check Codes with 24 and 32 Parity Bits*, June 1993, IEEE Transactions On Communications, Volume 41, No. 6

[44] SCHILLER F and MATTES T: *An Efficient Method to Evaluate CRC-Polynomials for Safety-Critical Industrial Communication*, Journal of Applied Computer Science, Vol. 14, No 1, pp. 57-80, Technical University Press, Łódź,Poland, 2006

[45] SCHILLER F and MATTES T: *Analysis of CRC-polynomials for Safety-critical Communication by Deterministic and Stochastic Automata*, 6th IFAC Symposium on Fault Detection, Supervision and Safety for Technical Processes, SAFEPROCESS 2006, pp. 1003-1008, Beijing, China, 2006

[46] *Technical Guideline Integration*, V2.0, December 2008, Safety Network International e. V. Ostfildern, Germany

[47] *CANopen Application Layer and Communication Profile, CiA Draft Standard 301*, Version 4.02, 13 February 2002, CAN in Automation e.V., Nürnberg, Germany

———————

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

3, rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

Tel: + 41 22 919 02 11
Fax: + 41 22 919 03 00
info@iec.ch
www.iec.ch