IEC/PAS 61784-3-18

Edition 1.0 2009-08

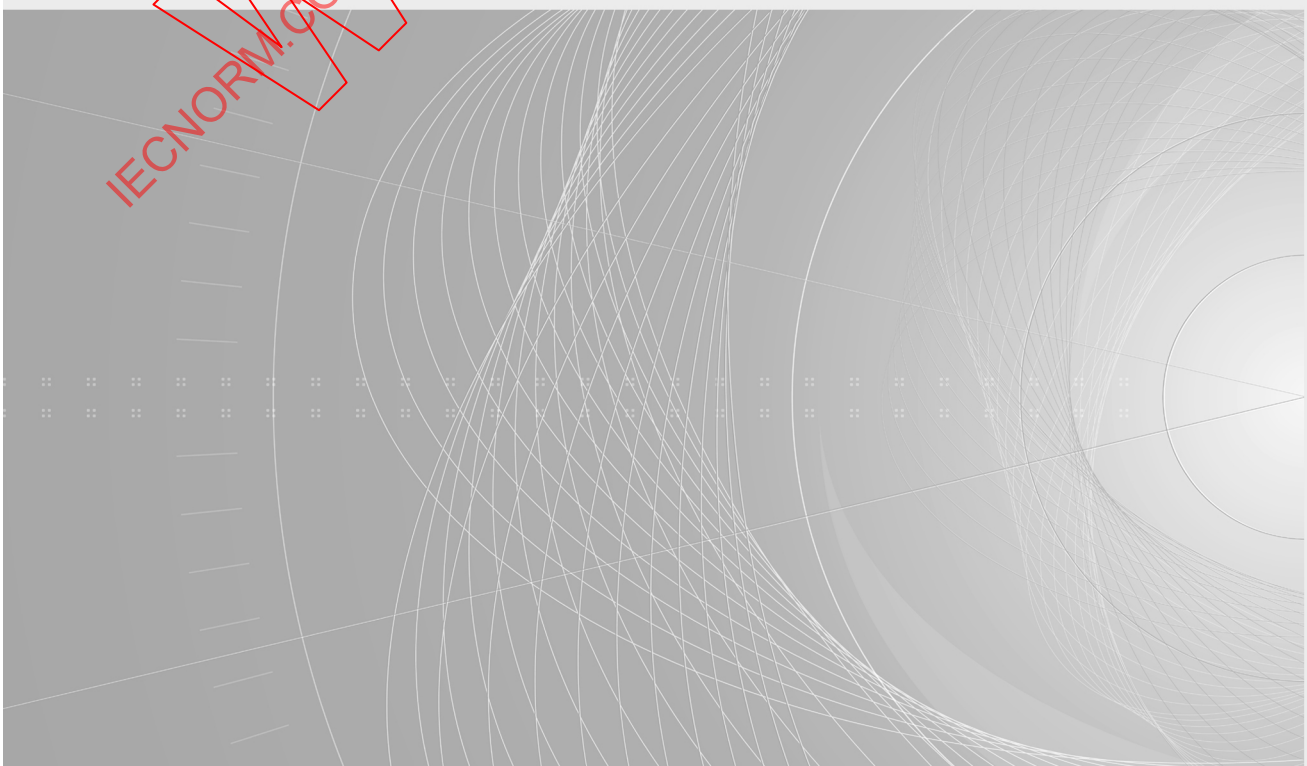
PUBLICLY AVAILABLE SPECIFICATION

PRE-STANDARD

colour inside

IECNORM.COM : Click to view the full PDF of IEC PAS 61784-3-18:2009
Withdrawn

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



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2009 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester.

If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland
Email: inmail@iec.ch
Web: 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.

- Catalogue of IEC publications: www.iec.ch/searchpub
The IEC on-line Catalogue enables you to search by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, withdrawn and replaced publications.

- IEC Just Published: www.iec.ch/online_news/justpub
Stay up to date on all new IEC publications. Just Published details twice a month all new publications released. Available on-line and also by email.

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

- Customer Service Centre: www.iec.ch/webstore/custserv
If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us:

Email: csc@iec.ch
Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00

IECNORM.COM : Click to view the full PDF of IEC PAS 61784-3-18:2009
Withdrawn

IEC/PAS 61784-3-18

Edition 1.0 2009-08

PUBLICLY AVAILABLE SPECIFICATION

PRE-STANDARD

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

IECNORM.COM : Click to view the full PDF of IEC PAS 61784-3-18:2009
Withdrawn

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

PRICE CODE XA

ICS 13.110; 25.040.40; 35.100.05

ISBN 978-2-88910-807-7

® Registered trademark of the International Electrotechnical Commission

CONTENTS

FOREWORD 5
INTRODUCTION 7
1 Scope 8
2 Normative references 8
3 Terms, definitions, symbols, abbreviated terms and conventions 9
3.1 Terms and definitions 9
3.1.1 Common terms and definitions 9
3.1.2 CPF X: Additional terms and definitions 13
3.2 Symbols and abbreviated terms 14
3.2.1 Common symbols and abbreviated terms 14
3.2.2 CPF SNpFAMILY: Additional abbreviated terms 15
3.2.3 CPF SNpFAMILY: Additional symbols 16
3.3 Conventions 16
4 Overview of FSCP SNpFAMILY/1 (SafetyNET p™) 17
5 General 18
5.1 External documents providing specifications for the profile 18
5.2 Safety functional requirements 19
5.3 Safety measures 19
5.4 Safety communication layer structure 20
5.5 Relationships with FAL (and DLL, PhL) 20
5.5.1 General 20
5.5.2 Data Types 20
6 Safety communication layer services 21
6.1 General elements 21
6.1.1 General 21
6.1.2 Safe object dictionary 21
6.1.3 Safe process data object (SPDO) 21
6.1.4 Safe heartbeat (SHB) 21
6.1.5 Safe delay monitoring (SDM) 21
6.2 Communication relation 21
7 Safety communication layer protocol 23
7.1 Safety PDU formats 23
7.1.1 Safe process data objects (SPDO) 23
7.1.2 Safe heartbeat (SHB) 24
7.1.3 Safety PDUs embedded in a Type SNpTYPE PDU 26
7.2 Safe application layer management (SALMT) 27
7.3 Safe process data communication 28
7.4 Safe heartbeat 29
7.5 Delay monitoring 30
8 Safety communication layer management 31
8.1 Parameter handling 31
8.2 Object dictionary 31
8.2.1 General 31
8.2.2 Communication profile section 32
8.2.3 Standardized device profile section 47
8.3 Device description 47

IECNORM.COM : Click to view the full PDF of IEC PAS 61784-3-18:2009
Withdrawn

9 System requirements 47
9.1 Indicators and switches 47
9.1.1 Indicator states and flash rates 47
9.1.2 Indicators 48
9.1.3 Switches 48
9.2 Installation guidelines 48
9.3 Safety function response time 48
9.3.1 General 48
9.3.2 Determination of FSCP SNpFAMILY time expectation behavior 50
9.3.3 Calculation of the worst case safety function response time 50
9.4 Duration of demands 51
9.5 Constraints for calculation of system characteristics 51
9.5.1 Safety related constraints 51
9.5.2 Probabilistic considerations 52
9.6 Maintenance 52
9.7 Safety manual 53
10 Certification 53
Bibliography 54

Figure 1 – FSCP SNpFAMILY/1 system 18
Figure 2 – FSCP SNpFAMILY/1 software architecture 20
Figure 3 – SPDO interaction model 22
Figure 4 – SHB interaction model 22
Figure 5 – Safe process data object frame 23
Figure 6 – Safe heartbeat request PDU 24
Figure 7 – Safe heartbeat response PDU 25
Figure 8 – Safety PDU for FSCP SNpFAMILY embedded in a Type SNpTYPE CDC data section 27
Figure 9 – Safe application layer management state machine 28
Figure 10 – RxSPDO state machine 29
Figure 11 – Heartbeat procedure 30
Figure 12 – Delay measurement principle 30
Figure 13 – Parameter handling 31
Figure 14 – Safety response time components 49
Figure 15 – Considered data fields for message size calculation 52
Figure 16 – Residual error rate 52

Table 1 – Object definition 17
Table 2 – Safety PDU element definition 17
Table 3 – Communication errors and detection measures 19
Table 4 – SPDO PDU structure 23
Table 5 – SHB request PDU structure 25
Table 6 – SHB response PDU structure 25
Table 7 – Safe heartbeat FS AL state encoding 26
Table 8 – Safe application layer management commands 27

IECNORM.COM : Click to view the full PDF of IEC PAS 61784-3-18:2009
Withdrawn

Table 9 – State transitions SALMT state machine 28
Table 10 – State transitions RxSPDO state machine 29
Table 11 – Object dictionary structure 32
Table 12 – Objects of communication section 33
Table 13 – Device type 34
Table 14 – Safe ID 34
Table 15 – Fail-safe consumer heartbeat list entry encoding 35
Table 16 – Fail-safe consumer heartbeat 36
Table 17 – Fail-safe producer heartbeat parameter 36
Table 18 – Fail-safe bus cycle times 39
Table 19 – SPDO timeout tolerance 40
Table 20 – Receive SPDO communication parameter 40
Table 21 – Transmit SPDO communication parameter 43
Table 22 – Mapping format 45
Table 23 – Receive SPDO mapping parameter 46
Table 24 – Transmit SPDO mapping parameter 47
Table 25 – Indicator states definiton 48
Table 26 – STATUS indicator states 48
Table 27 – Definition of terms 49
Table 28 – Definition of terms for time expectation behavior 50
Table 29 – Definition of terms for SFR calculation 51

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC PAS 61784-3-18:2009

INTERNATIONAL ELECTROTECHNICAL COMMISSION

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES –

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

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 provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with an IEC Publication.
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.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

A PAS is a technical specification not fulfilling the requirements for a standard, but made available to the public.

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

The text of this PAS is based on the following document:	This PAS was approved for publication by the P-members of the committee concerned as indicated in the following document
Draft PAS	**Report on voting**
65C/530/PAS	65C/534/RVD

Following publication of this PAS, which is a pre-standard publication, the technical committee or subcommittee concerned may transform it into an International Standard.

IECNORM.COM : Click to view the full PDF of IEC PAS 61784-3-18:2009
Withdrawn

This PAS shall remain valid for an initial maximum period of 3 years starting from the publication date. The validity may be extended for a single 3-year period, following which it shall be revised to become another type of normative document, or shall be withdrawn.

The list of all the parts of the IEC 61784 series, under the general title *Industrial communication networks – Profiles*, can be found on the IEC web site.

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 publication using a colour printer.

IECNORM.COM : Click to view the full PDF of IEC PAS 61784-3-18:2009
Withdrawn

INTRODUCTION

This PAS contains an additional profile – SNpTYPE – which may be integrated into a future new edition of IEC 61784-3.

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC PAS 61784-3-18:2009

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES –

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

IECNORM.COM : Click to view the full PDF of IEC PAS 61784-3-18:2009
Withdrawn

1 Scope

This part of the IEC 61784-3 series specifies a safety communication layer (services and protocol) based on CPF SNpFAMILY of IEC/PAS 62633 and IEC/PAS 61158 Type SNpTYPE. 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 of the IEC 61784-3 series 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 for functional safety. These mechanisms may be used in various industrial applications such as process control, manufacturing automation and machinery.

This part of the IEC 61784-3 series 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 of the IEC 61784-3 series in a standard device is not sufficient to qualify it as a safety device.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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

IEC/PAS 61158-3-22, *Industrial communication networks – Fieldbus specifications – Part 3-22: Data-link layer service definition – Type SNpType elements*

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

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

IEC/PAS 61158-6-22, *Industrial communication networks – Fieldbus specifications – Part 6-22: Application layer protocol specification – Type SNpType elements*

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

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

IEC 61784-3, *Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions*

IEC/PAS 62633, *Industrial communication networks – Profiles – Additional fieldbus profiles for real-time networks based on ISO/IEC 8802-3 - SNpTYPE*

3 Terms, definitions, symbols, abbreviated terms and conventions

3.1 Terms and definitions

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

NOTE Availability depends on MTBF (mean time between failure) and MDT (mean down time): Availability = MTBF / (MTBF + MDT).

3.1.1.2
black channel
communication channel without available evidence of design or validation according to IEC 61508 series

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 See also [2], [3][1].

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

NOTE 1 An error can be caused by a faulty item, for example a computing error made by faulty computer equipment.

[IEV 191-05-24], [IEC 61508-4:1998], [IEC 61158]

---

1 Figures in square brackets refer to the bibliography.

IECNORM.COM : Click to view the full PDF of IEC PAS 61784-3-18:2009
Withdrawn

NOTE 2 Errors may be due to design mistakes within hardware/software and/or corrupted information due to electromagnetic interference and/or other effects.

NOTE 3 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

NOTE 1 The definition in IEV 191-04-01 is the same, with additional notes.

[IEC 61508-4:1998], [ISO/IEC 2382-14.01.11]

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 preventative maintenance or other planned actions, or due to lack of external resources.

[IEC 61508-4:1998], [ISO/IEC 2382-14.01.10]

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 [2], [3].

3.1.1.13
hash function
(mathematical) function that maps values from a (possibly very) large set of values into a (usually) smaller range of values

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

NOTE 2 Common hash functions include parity, checksum or CRC.

[IEC 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

IECNORM.COM : Click to view the full PDF of IEC PAS 61784-3-18:2009
Withdrawn

[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
proof test
periodic test performed to detect failures in a safety-related system so that, if necessary, the system can be restored to an “as new” condition or as close as practical to this condition

NOTE A proof test is intended to confirm that the safety-related system is in a condition that assures the specified safety integrity.

[IEC 61508-4 and IEC 62061, modified]

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

EXAMPLE Duplicated functional components and the addition of parity bits are both instances of redundancy.

NOTE 1 Redundancy is used primarily to improve reliability or availability.

NOTE 2 The definition in IEV 191-15-01 is less complete.

[IEC 61508-4:1998], [ISO/IEC 2382-14.01.12]

3.1.1.21
reliability
probability that an automated system can perform a required function under given conditions for a given time interval (t1,t2)

NOTE 1 It is generally assumed that the automated system is in a state to perform this required function at the beginning of the time interval.

NOTE 2 The term "reliability" is also used to denote the reliability performance quantified by this probability.

NOTE 3 Within the MTBF or MTTF period of time, the probability that an automated system will perform a required function under given conditions is decreasing.

NOTE 4 Reliability differs from availability.

[IEC 62059-11, modified]

3.1.1.22
risk
combination of the probability of occurrence of harm and the severity of that harm

IECNORM.COM : Click to view the full PDF of IEC PAS 61784-3-18:2009
Withdrawn

[IEC 61508-4:1998]

3.1.1.23
safety communication layer (SCL)
communication layer that includes all the necessary measures to ensure safe transmission of data in accordance with the requirements of IEC 61508

3.1.1.24
safety data
data transmitted across a safety network using a safety protocol

NOTE The Safety Communication Layer does not ensure safety of the data itself, only that the data is transmitted safely.

3.1.1.25
safety device
device designed in accordance with IEC 61508 and which implements the functional safety communication profile

3.1.1.26
safety function
function to be implemented by an E/E/PE safety-related system, other technology safety-related system or external risk reduction facilities, which is intended to achieve or maintain a safe state for the EUC, in respect of a specific hazardous event

[IEC 61508-4:1998]

3.1.1.27
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, 5.2.4 and addressed by the functional safety communication profiles defined in this part of the IEC 61784-3 series .

3.1.1.28
safety integrity level (SIL)
discrete level (one out of a possible four) for specifying the safety integrity requirements of the safety functions to be allocated to the E/E/PE safety-related systems, where safety integrity level four has the highest level of safety integrity and safety integrity level one has the lowest

NOTE The target failure measures for the four safety integrity levels are specified in Tables 2 and 3 of IEC 61508-1.

[IEC 61508-4:1998]

3.1.1.29
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, 5.3 and 5.4.

3.1.1.30
safety-related application
programs designed in accordance with IEC 61508 to meet the SIL requirements of the application

IECNORM.COM : Click to view the full PDF of PAS 61784-3-18:2009
Withdrawn

3.1.1.31
safety-related system
system performing safety functions according to IEC 61508

3.1.1.32
spurious trip
trip caused by the safety system without a process demand

3.1.2 CPF X: Additional terms and definitions

3.1.2.1
consecutive number
means to ensure completeness and the right order of transmitted safety PDUs

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

3.1.2.2
cycle
interval at which a list of instructions or an activity is repetitively and continuously executed

3.1.2.3
delay
transmission time of PDUs which is dynamically caused by network properties like traffic, switching devices and topology

3.1.2.4
fail-safe
ability of a system that by adequate technical or organizational measures prevents from hazards either deterministically or by reducing the risk to a tolerable measure

3.1.2.5
gateway
device acting as a linking element between different protocols

3.1.2.6
real time frame line (RTFL)
communication model for communication with high real time requirements

3.1.2.7
real time frame network (RTFN)
communication model for communication with low real time requirements

3.1.2.8
safe application layer management (SALMT)
mechanism to control the safe application layer sate of safe devices

3.1.2.9
safe delay monitoring (SDM)
safe mechanism to cyclically monitor the delay of transmitted PDUs

3.1.2.10
safe heartbeat (SHB)
mechanism to cyclically monitor the state of safe devices

3.1.2.11
safe process data object (SPDO)
mechanism to cyclically exchange safe process data between devices

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC PAS 61784-3-18:2009

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	
EMI	Electro-magnetic interference	
EUC	Equipment under control	[IEC 61508-4:1998]
FAL	Fieldbus application layer	[IEC 61158-5]
FCS	Frame check sequence	
FSCP	Functional safety communication profile	
HD	Hamming distance	
E/E/PE	Electrical/Electronic/Programmable electronic	[IEC 61508-4:1998]
NSR	Non safety relevant	
PDU	Protocol data unit	[ISO/IEC 7498-1]
PELV	Protective extra low voltage	
PES	Programmable electronic system	[IEC 61508-4:1998]
PFD	Average probability of failure on demand	[IEC 61508-6:2000]
PFH	Probability of failure per hour	[IEC 61508-6:2000]
PhL	Physical layer	[ISO/IEC 7498-1]
PLC	Programmable logic controller	
SCL	Safety communication layer	
SELV	Safety extra low voltage	
SFRT	Safety function response time	
SIL	Safety integrity level	[IEC 61508-4:1998]
SR	Safety relevant	

IECNORM.COM : Click to view the full PDF of IEC PAS 61784-3-18:2009
Withdrawn

3.2.2 CPF SNpFAMILY: Additional abbreviated terms

AL	Application layer
AP	Application process
FS	Fail-safe
ID	Identification
MSB	Most significant bit
OS	Operating system
PDO-ID	Process data object ID
PID	Packet ID
RTFL	Real time frame line
RTFN	Real time frame network
SALMT	Safe application layer management
SDM	Safe delay monitoring
SHB	Safe heartbeat
SID	Safe-ID
SPDO	Safe process data object

IECNORM.COM : Click to view the full PDF of IEC PAS 61784-3-18:2009
Withdrawn

3.2.3 CPF SNpFAMILY: Additional symbols

Symbol	Definition	Unit
T_A	Actuator time	µs
T_{Awc}	Worst case actuator time	µs
T_{cycle}	Cycle time of communication	µs
T_I	Input time	µs
T_{Iwc}	Worst case input time	µs
T_L	Logic processing time	µs
T_{Lwc}	Worst case logic processing time	µs
T_O	Output time	µs
T_{Owc}	Worst case output time	µs
T_S	Sensor time	µs
T_{SFR}	Safety function response time	µs
T_{Swc}	Worst case sensor time	µs
T_T	Transmission time	µs
T_{TOi}	Timeout time of component	µs
T_{TOS}	FSCP SNpFAMILY timeout time	µs
T_{Twc}	Worst case transmission time	µs
ΔT	Timeout margin	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 object dictionary of an object.
- Sub-index describes a single element of the object.
- Name denotes a name string for this attribute.
- Object type denotes the characterizing type for each object as specified in IEC/PAS 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 FS denotes no access rights except for the safety application and optional read access by SDO services as specified in IEC/PAS 61158-5-22 and IEC/PAS 61158-6-22.
- SPDO mapping denotes the possibility to map this attribute to TxSPDO or RxSPDO or to indicate that this parameter is not mappable.
- Value range contains the value range of a dedicated element or “No” for no pre-defined value range.
- Value contains the constant value(s) and/or the meaning of the parameter or “No” for no pre-defined value.

IECNORM.COM : Click to view the full PDF of IEC PAS 61784-3-18:2009
Withdrawn

Table 1 – Object definition

Attribute	Value
Index	
Sub-index	
Name	
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 frame 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 SNpFAMILY/1 (SafetyNET p™)

Communication Profile Family SNpFAMILY (commonly known as SafetyNET p™[2]) defines communication profiles based on IEC/PAS 61158-3-22, IEC/PAS 61158-4-22, IEC/PAS 61158-5-22 and IEC/PAS 61158-6-22. The basic profile(s) CP SNpFAMILY/1 and CP SNpFAMILY/2 are defined in IEC/PAS 62633. The CPF SNpFAMILY functional safety communication profile FSCP SNpFAMILY/1 is based on the CPF SNpFAMILY basic profiles in IEC/PAS 62633 and the safety communication layer specifications defined in this part of the IEC 61784-3 series.

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

FSCP SNpFAMILY/1 uses a dedicated 1:n producer-consumer interaction model for safe process data communication and a 1:1 interaction model for the purpose of safety device monitoring. Figure 1 depicts possible communication relationships based on a CP

2 SafetyNET p is a trade name of the 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 profile does not require use of the trade name SafetyNET p. Use of the trade name SafetyNET p requires permission of the trade name holder.

IECNORM.COM : Click to view the full PDF of IEC PAS 61784-3-18:2009

SNpFAMILY/1 and CP SNpFAMILY/2 network. Safety-related communication within cells is possible as well as inter-cell communication.

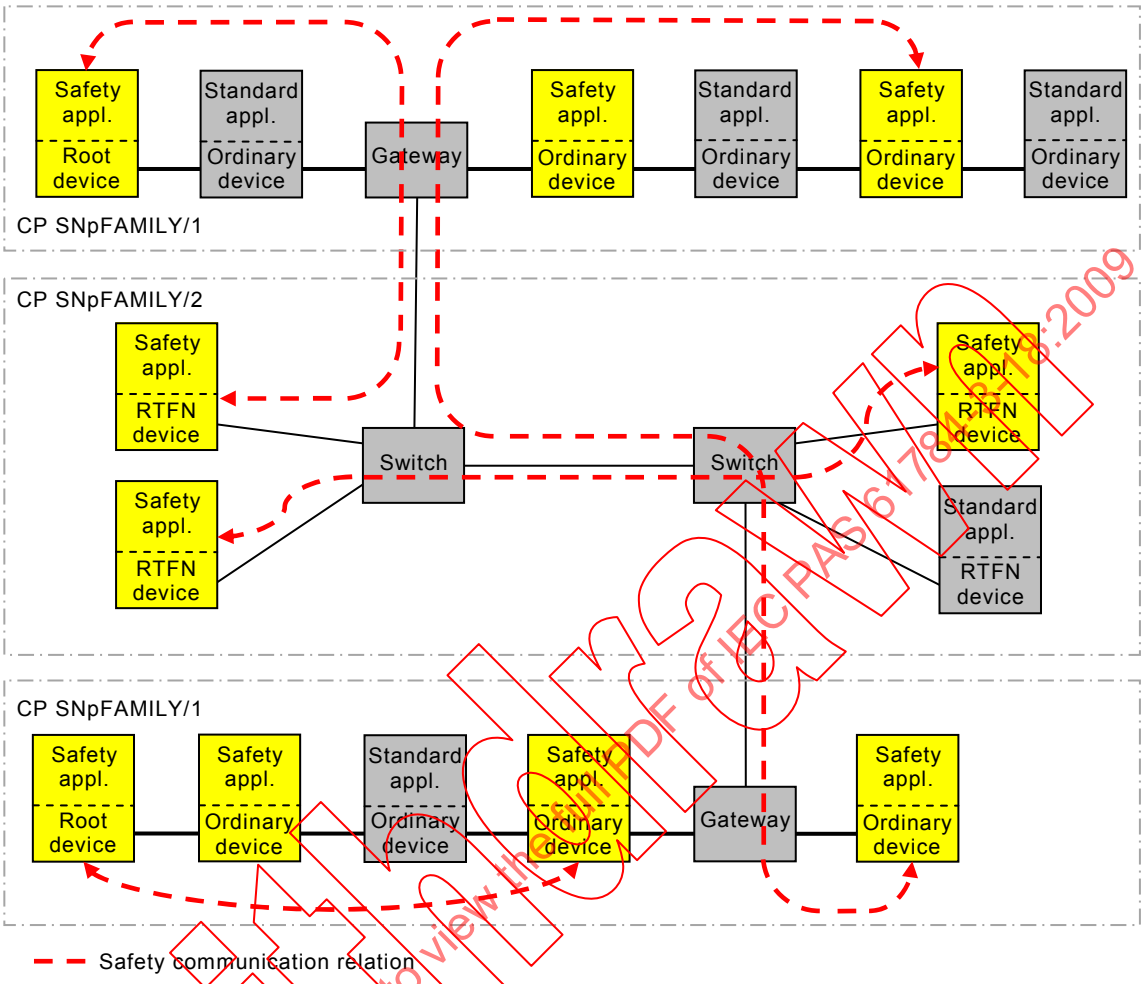


Figure 1 – FSCP SNpFAMILY/1 system

For the realization of FSCP SNpFAMILY/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 safe and non-safe communication.
- Packet delay monitoring for dedicated communication relationships.

Each device maintains a safety layer state machine, which is coordinated by the safe application. Safety is ensured based on the fail-safe application layer 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 documents are useful in understanding the design of FSCP SNpFAMILY/1 protocol:

IECNORM.COM : Click to view the full PDF of IEC PAS 61784-3-18:2009
Withdrawn

- GS-ET-26 [1]

5.2 Safety functional requirements

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

- Requirements of IEC 61508 (see IEC 61508) shall be fulfilled to meet the Safety Integrity Level of the device.
- The FSCP SNpFAMILY/1 protocol is designed to support Safety Integrity Level 3 (SIL 3) (see IEC 61508).
- FSCP SNpFAMILY/1 protocol is implemented using a black channel approach; there is no safety related dependency on the standard CPF SNpTYPE 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 communication 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 safe 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.

5.3 Safety measures

The safety measures used in the FSCP SNpFAMILY/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 ID [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	—

[a] In this standard called "T_{TOS}".

[b] In this standard realized by "SID" and "PID".

IECNORM.COM : Click to view the full PDF of IEC PAS 61784-3-18:2009
Withdrawn

5.4 Safety communication layer structure

The FSCP SNpFAMILY/1 protocol is layered on top of the data link layer protocol. Figure 2 shows how the protocol is related to the CPF SNpFAMILY layer. The safety-related functionality is implemented within the application layer for safety and utilizes the non-safe data link layer services to transfer safe PDUs. The safety-related application uses the FSCP SNpFAMILY/1 to transfer safety-related data. The safety layer is designed to work in parallel with application layer from CP SNpFAMILY/1 and SNpFAMILY/2.

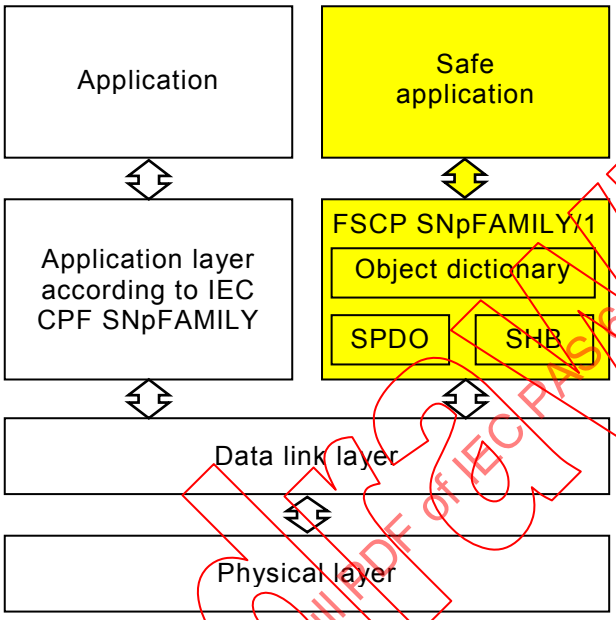


Figure 2 – FSCP SNpFAMILY/1 software architecture

A safety PDU (SPDO) containing the safe process data, the identification information and the required error detection measures is included in the process data objects of the data link layer protocol. The mapping within the process data of the communication system is described within different object dictionary entries within the application layer for safety.

Safe application layer monitoring is realized using a safe heartbeat service (SHB).

The calculation of the residual error probability for the FSCP SNpFAMILY/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 SNpFAMILY communication profiles. But it is not restricted to this communication profile.

5.5.2 Data Types

Profiles defined in this part of the IEC 61784-3 series support all the CPF SNpFAMILY data types as defined in IEC/PAS 61158-5-22. The encoding of these data types follows the encoding rules defined in IEC/PAS 61158-6-22.

IECNORM.COM : Click to view the full PDF of IEC PAS 61784-3-18:2009
Withdrawn

6 Safety communication layer services

6.1 General elements

6.1.1 General

The FSCP SNpFAMILY/1 provides the following elements.

- Safe object dictionary.
- Safe process data object (SPDO).
- Safe heartbeat (SHB).
- Safe delay monitoring (SDM).

6.1.2 Safe object dictionary

The safe object dictionary is the interface between the safe 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 SNpFAMILY/1 and SNpFAMILY/2. Access to safe object dictionary entries can optionally be realized by SDO services as defined in IEC/PAS 61158-5-22 and IEC/PAS 61158-6-22. This access shall be restricted to read only (RO) access.

6.1.3 Safe process data object (SPDO)

Safe process data objects shall provide the required services for safety related process data exchange between certain communicating devices. Safe process data communication in FSCP SNpFAMILY/1 is cyclic using safe process data objects (SPDOs). Inter-cell communication in the sense of CPF SNpFAMILY is possible. The process data communication is split into safe transmit and receive process data objects (TxSPDOs or RxSPDO).

6.1.4 Safe heartbeat (SHB)

Devices which implement FSCP SNpFAMILY/1 safe application layer use safe heartbeat service for application layer monitoring and application monitoring. This service is independent of any other heartbeat services devices could implement in parallel. Safe heartbeat messages are confirmed cyclic messages exchanged between communicating devices and realize a 1:1 communication relation between devices.

6.1.5 Safe delay monitoring (SDM)

The safe 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 SNpFAMILY/1 defines a 1:n producer-consumer interaction model for safe process data communication. Producers shall cyclically send safe process data objects identified by a unique PDO-ID for packet identification and a unique safety ID for producer identification. Safe process data object interaction is unconfirmed. Figure 3 shows the safe process data object interaction model.

IECNORM.COM : Click to view the full PDF of IEC PAS 61784-3-18:2009
Withdrawn

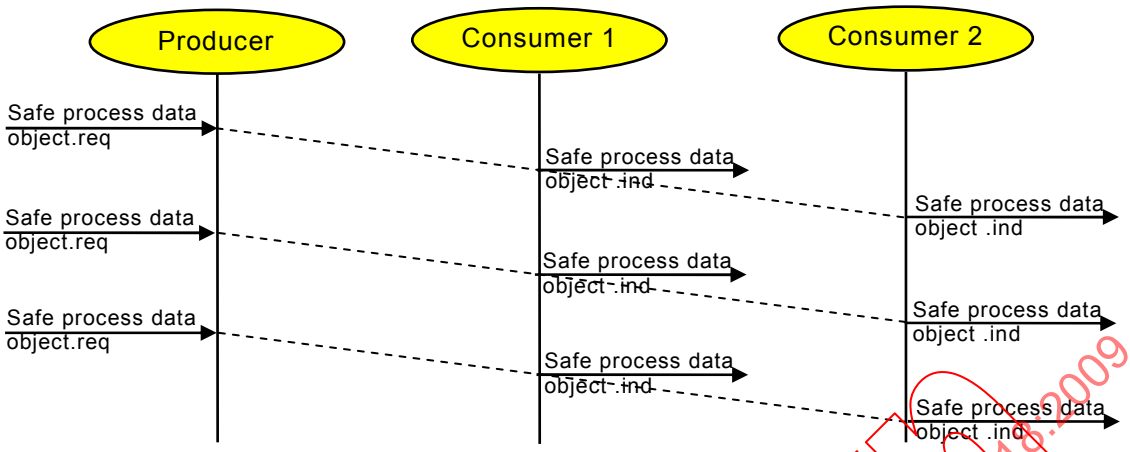


Figure 3 – SPDO interaction model

The state and presence of communication partners (i.e. producers and consumers) in FSCP SNpFAMILY/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 communication between communication partners exists. Safe heartbeat communication follows the confirmed client-server interaction model. Figure 4 depicts heartbeat interactions for a safe 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.

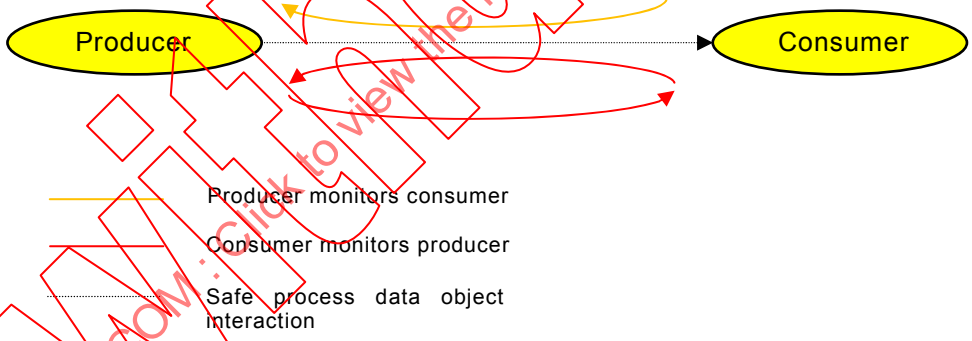


Figure 4 – SHB interaction model

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

- safe process data objects (SPDO); and
- safe heartbeat (SHB).

The FSCP SNpFAMILY/1 communication cycle mainly consists of cyclic unconfirmed exchange of safe process data objects. A time expectation behavior is used on the consumer-side to monitor safe 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 safe heartbeat service. Both mechanisms in combination define and observe a communication cycle.

IECNORM.COM : Click to view the full PDF of IEC PAS 61784-3-18:2009
Withdrawn

7 Safety communication layer protocol

7.1 Safety PDU formats

7.1.1 Safe process data objects (SPDO)

7.1.1.1 Safety PDU structure

Figure 5 defines the structure of a safe process data object and its data fields.

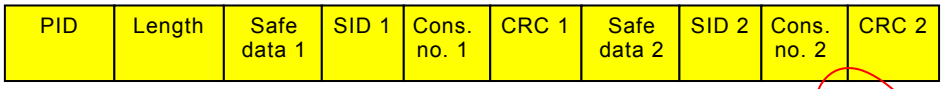


Figure 5 – Safe process data object frame

The safety PDU is cyclically transferred via the subordinate fieldbus. The content of the safe process data objects consists of fail-safe application objects out of the object dictionary. The content of a dedicated safety PDU is described by object mapping entries within the safe object dictionary.

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)	Safe data 1	Mapped safe application process data
4+n to 5+n	SID 1	Safe ID of the sender
6+n	Consecutive number 1	Consecutive number for sequencing and application monitoring
7+n to 10+n	CRC 1	32 bit cyclic redundancy check covering data fields PID, length, safe data 1, SID 1 and consecutive number 1
11 to 11+(n-1)	Safe data 2	Copy of mapped safe application process data
11+n to 12+n	SID 2	Copy of SID 1
13+n	Consecutive number 2	Copy of consecutive number 1
14+n to 17+n	CRC 2	32 bit cyclic redundancy check covering data fields PID, length, safe data 2, SID 2 and consecutive number 2
NOTE n depicts the length in octets of the data field safe data 1 (safe data 2).		

IECNORM.COM : Click to view the full PDF of IEC PAS 61784-3-18:2009
Withdrawn

7.1.1.2 SPDO PID

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

7.1.1.3 SPDO length

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

7.1.1.4 Safe data

This data field shall contain the fail-safe 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 maximum amount of data is restricted to 117 octets. For this data amount and the data integrity assurance system applied by this FSCP the residual error probability does not exceed 10^{-9} as proven in clause 9.5.2.

7.1.1.5 SPDO SID

This data field depicts a 16 bit identifier of the sender. This value shall be unique across the network. Each participating FSCP SNpFAMILY device obtains one SID. The SID of a device is stored within the corresponding object dictionary entry with index 0x1200. The SID shall not be 0.

7.1.1.6 SPDO consecutive number

This data field is an 8 bit consecutive number (cyclic counter) for application layer life-sign monitoring and packet sequencing.

7.1.1.7 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. The mathematical proof showing that the residual error probability with the polynomial for safe data up to 117 octets and a bit error rate of 0,5 does not exceed 10^{-9} is included in clause 9.5.2.

7.1.2 Safe heartbeat (SHB)

7.1.2.1 Safety PDU structure

7.1.2.1.1 SHB request PDU

Figure 6 shows the structure of a safe heartbeat request PDU.

PID	Length	Fail-safe AL state 1	Fail-safe AP state 1	SID 1	Cons. No.1	CRC 1	Fail-safe AL state 2	Fail-safe AP state 2	SID 2	Cons. No.2	CRC 2

Figure 6 – Safe heartbeat request PDU

Table 5 lists the general structure of this PDU.

IECNORM.COM : Click to view the full PDF of IEC PAS 61784-3-18:2009
Withdrawn

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	Fail-safe AL state 1	Fail-safe application layer state
5 to 6+(n-1)	Fail-safe AP state 1	Fail-safe application process state
6+n to 7+n	SID 1	Safe ID of the sender
8+n	Consecutive number 1	Consecutive number for sequencing and application monitoring
9+n to 12+n	CRC 1	32 bit cyclic redundancy check covering data fields PID, length, Fail-safe AL state 1, Fail-safe AP state 1, SID 1 and consecutive number 1
13	Fail-safe AL state 2	Copy of fail-safe application layer state 1
14 to 15+(n-1)	Fail-safe AP state 2	Copy of fail-safe application process state 1
15+n to 16+n	SID 2	Copy of SID 1
17+n	Consecutive number 2	Copy of consecutive number 1
18+n to 21+n	CRC 2	32 bit cyclic redundancy check covering data fields PID, length, Fail-safe AL state 2, Fail-safe AP state 2, SID 2 and consecutive number 2
NOTE n depicts the length in octets of the data field Fail-safe AP state.		

7.1.2.1.2 SHB response PDU

Figure 7 shows the structure of a safe heartbeat response PDU.

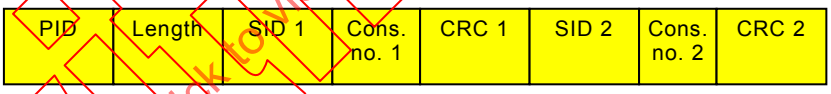


Figure 7 – Safe heartbeat response PDU

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	Safe ID of the sender
6	Consecutive number 1	Consecutive number for sequencing and application monitoring
7 to 10	CRC 1	32 bit cyclic redundancy check covering data fields PID, length, SID 1 and consecutive number 1
11 to 12	SID 2	Copy of SID 1
13	Consecutive number 2	Copy of consecutive number 1
14 to 17	CRC 2	32 bit cyclic redundancy check covering data fields PID, length, SID 2 and consecutive number 2

IECNORM.COM : Click to view the full PDF of IEC PAS 61784-3-18:2009

7.1.2.2 SHB PID

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

7.1.2.3 SHB length

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

7.1.2.4 SHB FS AL state

This data field shall contain state information about the fail-safe application layer. This information is interpreted by SHB receivers. Table 7 specifies the encoding of the content of this data field.

Table 7 – Safe heartbeat FS AL state encoding

Value	Description
0x00	FS AL is in BOOTUP state
0x04	FS AL is in STOPPED state
0x05	FS AL is in OPERATIONAL state
0x7F	FS AL is in PRE-OPERATIONAL state

7.1.2.5 SHB FS AP state

This data field shall contain state information about the fail-safe application. The content and encoding of this data field are application dependent and are outside the scope of this international standard. The length shall not exceed 116 octets.

7.1.2.6 SHB SID

This data field depicts a 16 bit identifier of the sender. This value shall be unique across the network. Each participating FSCP SNpFAMILY/1 device obtains a SID. The SID of a device is stored within the corresponding object dictionary entry with index 0x1200. The SID shall not be 0.

7.1.2.7 SHB consecutive number

This data field is an 8 bit consecutive number (cyclic counter) for application layer life-sign monitoring and packet sequencing. In the event of a response PDU this data field contains the consecutive number of the PDU confirmed by this response.

7.1.2.8 SHB CRC

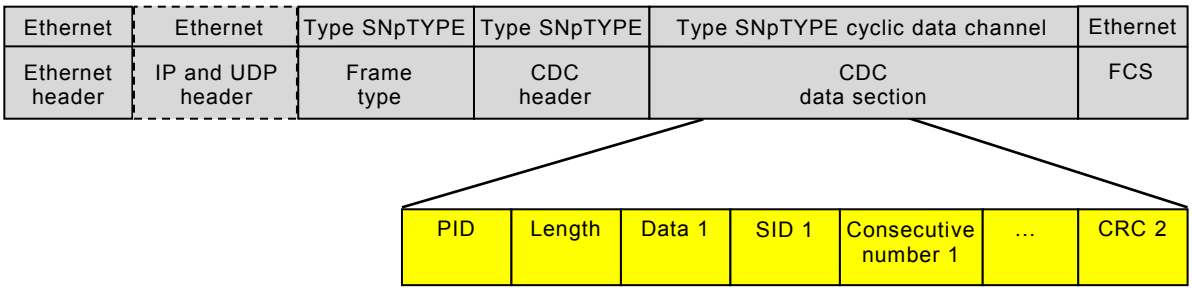
This data field contains the 32 bit CRC covering the data fields PID, length, data, SID and consecutive number.

The polynomial 0x20044009 is used for calculating the CRCs. The mathematical proof showing that the residual error probability with the polynomial for safe data up to 117 octets and a bit error rate of 0,5 does not exceed 10^{-9} is included in 9.5.2.

7.1.3 Safety PDUs embedded in a Type SNpTYPE PDU

Figure 8 shows the structure of a FSCP SNpFAMILY/1 safety PDU embedded in a Type SNpTYPE CDC DLPDU.

IECNORM.COM : Click to view the full PDF of IEC PAS 61784-3-18:2009
Withdrawn



NOTE The presence of IP and UDP header information depends on the used CP

Figure 8 – Safety PDU for FSCP SNpFAMILY embedded in a Type SNpTYPE CDC data section

7.2 Safe application layer management (SALMT)

By the local safe application layer management service it is possible to trigger the state machine of the fail-safe application layer and thus to control the behavior of the fail-safe part of a device.

The application layer management commands as specified in Table 8 are available.

Table 8 – Safe application layer management commands

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

Figure 9 shows the safe application layer management state machine. All depicted states of the state machine shall be supported.

IECNORM.COM : Click to view the full PDF of IEC PAS 61784-3-18:2009
Withdrawn

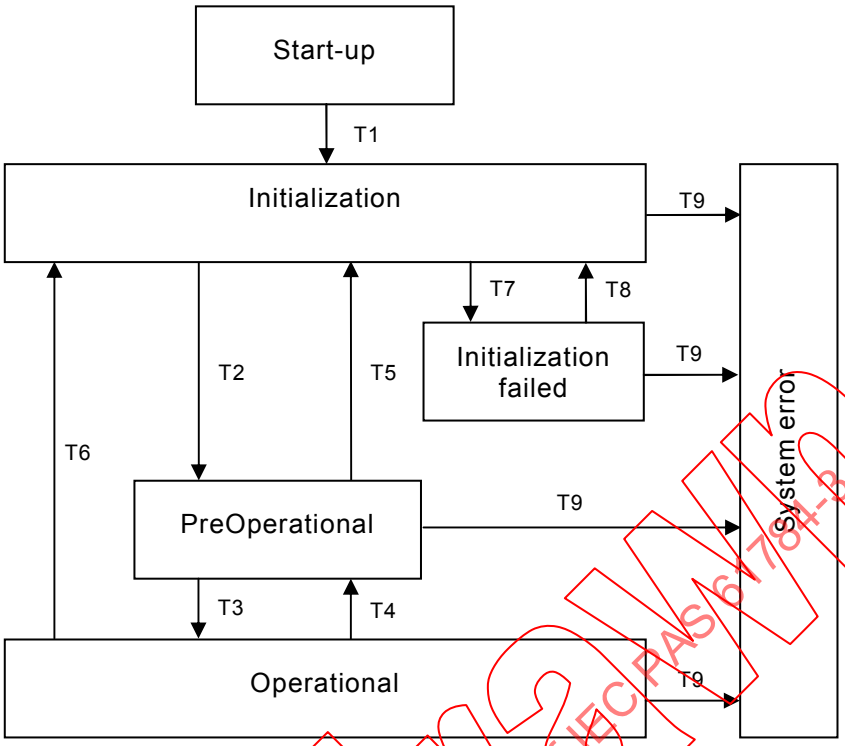


Figure 9 – Safe application layer management state machine

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

Table 9 – State transitions SALMT state machine

State transition	Description
T1	Automatic state transition after device start-up
T2	Transition is initiated by SALMT command enter preoperational. This transition enables the transmission of SHB PDUs
T3	Transition is initiated by SALMT command start remote node. This transition enables the transmission of SPDO PDUs
T4	Transition is initiated by SALMT command stop remote node. This transition disables the transmission of SPDO PDUs
T5	Transition is initiated by SALMT command reset node or reset communication. This transition disables the transmission of SHB PDUs
T6	Transition is initiated by SALMT command reset node or reset communication. This transition disables the transmission of SPDO and SHB PDUs
T7	Transition is initiated by a failure or fault during initialization
T8	Transition is initiated by SALMT command reset node
T9	This transition is initiated by a system error. No further PDUs are transmitted

IECNORM.COM : Click to view the full PDF of IEC PAS 61784-3-18:2009
Withdrawn

7.3 Safe process data communication

Safe process data communication is based on a 1:n producer-consumer interaction model. 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 safe 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 10 depicts the RxSPDO state machine. This state machine is applied for each configured RxSPDO. All depicted states shall be supported.

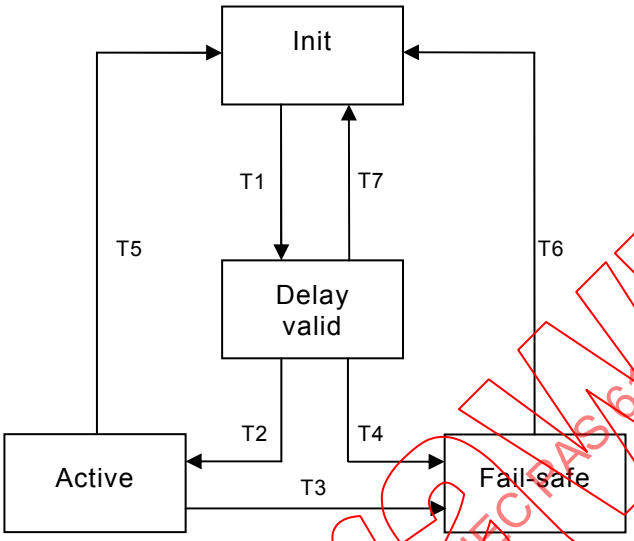


Figure 10 – RxSPDO state machine

Table 10 describes the state transitions and the related events and actions.

Table 10 – State transitions RxSPDO state machine

State transition	Description	SALMT state
T1	SDM was successfully executed	PreOperational or Operational
T2	SPDO communication is active	Operational
T3	SDM indicates unacceptable increase in PDU delivery delay or timeout time expired. Safe state is requested to safe application	Operational
T4	SDM indicates unacceptable increase in PDU delivery delay or timeout time expired. Safe state is requested to safe application	Operational
T5	SALMT command enter preoperational was received	Operational
T6	SALMT command enter preoperational was received	Operational
T7	SDM indicates unacceptable increase in PDU delivery delay	PreOperational

IECNORM.COM : Click to view the full PDF of IEC PAS 61784-3-18:2009
Withdrawn

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 Safe heartbeat

Devices which implement a safe application layer shall support safe heartbeat. This heartbeat mechanism is independent of the CPF SNpFAMILY/1 and SNpFAMILY/2 heartbeat messages and shall be configured independent.

Safe heartbeat messages are transmitted as specified in Figure 11. Each heartbeat message contains the state of the safe application layer and the safe application process.

The heartbeat procedure is depicted in Figure 11.

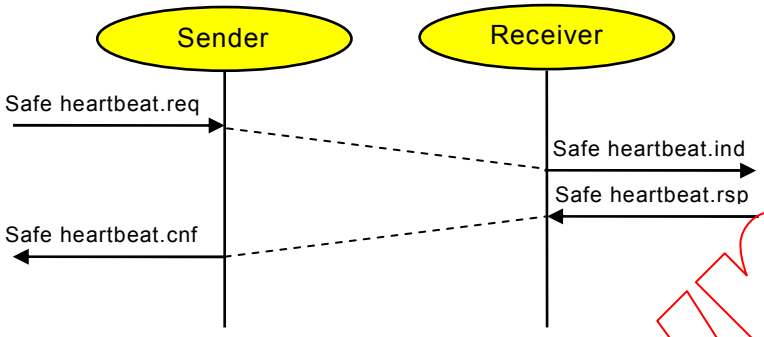
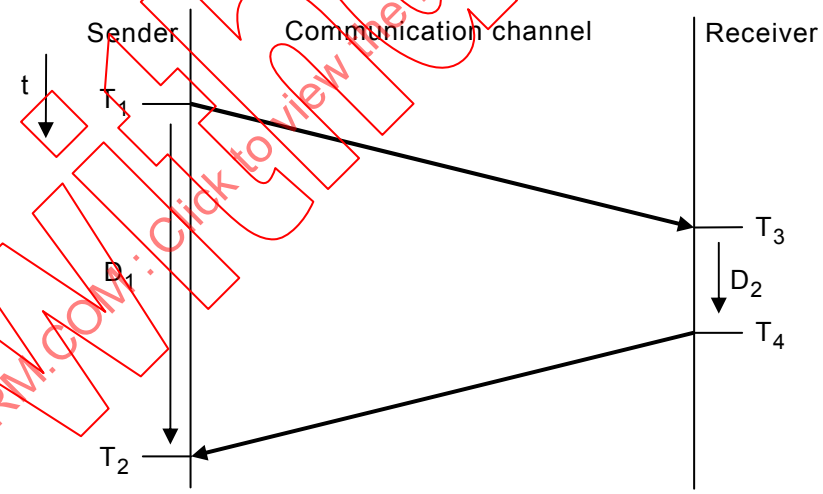


Figure 11 – Heartbeat procedure

7.5 Delay monitoring

It is possible to monitor the delay of packets based on the safe heartbeat service. Each safe 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 12 depicts the general measurement principle for delay measurement at sender and receiver.



T_x Point in time x

D_x Resulting delay

Figure 12 – 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 safe application layer shall initiate a transition to SPDO state FAIL-SAFE and the application shall enter a safe state.

IECNORM.COM : Click to view the full PDF of PAS 61784-3-18:2009
Withdrawn

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 arises over the configured delay threshold.

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

8 Safety communication layer management

8.1 Parameter handling

The parameter configuration of FSCP SNpFAMILY/1 devices is part of the configuration of the fail-safe 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 fail-safe application. Figure 13 depicts the device configuration sequence.

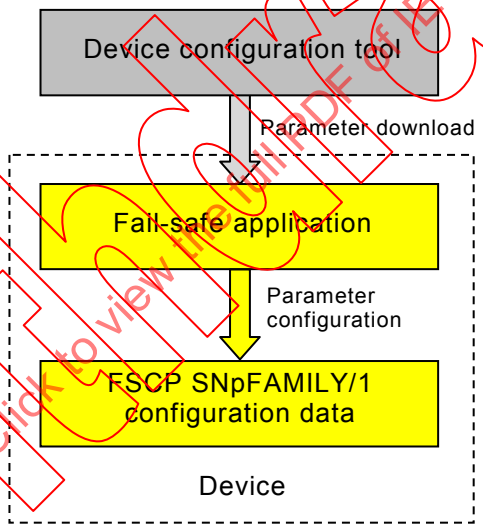


Figure 13 – Parameter handling

8.2 Object dictionary

8.2.1 General

The object dictionary according to CPF SNpFAMILY/1 and SNpFAMILY/2 contains the object areas listed in Table 11.

IECNORM.COM : Click to view the full PDF of IEC PAS 61784-3-18:2009
Withdrawn

Table 11 – 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	Type SNpTYPE RTFN interface profile	—	Definition of the parameters defined in Type SNpTYPE RTFN 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 12 shall be supported.

IECNORM.COM : Click to view the full PDF of IEC PAS 61784-3-18:2009
Withdrawn

Table 12 – Objects of communication section

Index	Object	Name	Data type	Attr.	Cat.
0x1000	VAR	Device type	Unsigned32	RO	M
0x1200	VAR	Safe ID	Unsigned16	FS	M/O
0x1216	ARRAY	Fail-safe consumer heartbeat list	Unsigned256	FS	M/O
0x1217	RECORD	Fail-safe producer heartbeat parameter	PDO COM_PAR	FS	M/O
0x1218	ARRAY	Fail-safe bus cycle time	Unsigned32	FS	M/O
0x121B to 0x121D	Reserved for further fail-safe parameters				
0x121E	VAR	SPDO Timeout tolerance	Unsigned8	FS	M/O
0x121F to 0x127F	Reserved for further fail-safe parameters				
0x1C00 to 0x1CFF	RECORD	RxSPDO communication parameter	PDO COM_PAR	FS	M/O
0x1D00 to 0x1DFF	RECORD	RxSPDO mapping parameter	PDO MAPPING	FS	M/O
0x1E00 to 0x1EFF	RECORD	TxSPDO communication parameter	PDO COM_PAR	FS	M/O
0x1F00 to 0x1FFF	RECORD	TxSPDO mapping parameter	PDO MAPPING	FS	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 13. It comprises of two 16 bit fields. The first field depicts 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 object dictionary. All other devices of a multiple device module identify their profiles at objects 0x67FF + X * 0x800 with X = 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 fail-safe functions, so that the first fail-safe application objects start at 0x8000.

IECNORM.COM : Click to view the full PDF of IEC PAS 61784-3-18:2009

Table 13 – Device type

Attribute	Value
Index	0x1000
Name	Device type
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 Safe ID (SID)

The safe ID object is specified in Table 14. The object specifies the safe ID of a fail-safe device. It is mandatory for fail-safe devices.

Table 14 – Safe ID

Attribute	Value
Index	0x1200
Name	Safe ID
Object type	VAR
Data type	Unsigned16
Category	Mandatory
Access attribute	FS
SPDO mapping	No
Value range	0x0001 to 0xFFFF
Value	No

8.2.2.4 Fail-safe consumer heartbeat list

The fail-safe consumer heartbeat list object is specified in Table 16. The fail-safe consumer heartbeat list defines all fail-safe 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 fail-safe consumer heartbeat list entry within an OCTET_STRING value is specified in Table 15.

IECNORM.COM : Click to view the full PDF of IEC PAS 61784-3-18:2009
Withdrawn

Table 15 – Fail-safe consumer heartbeat list entry encoding

Octet	Data type	Meaning
0 to 3	Unsigned32	IPv4 address of communication partner
4 to 19	Unsigned128	IPv6 address of communication partner
20 to 21	Unsigned26	SID of communication partner
22	Unsigned8	Transmission type
23	Unsigned8	Reserved
24 to 27	Unsigned32	PID of consumed heartbeat
28 to 29	Unsigned16	Heartbeat timeout
30 to 31	Unsigned16	Cycle multiplier for consumed heartbeat
32 to 33	Unsigned16	Cycle offset for consumed heartbeat
34	Unsigned8	Number of receives threshold
35	Unsigned8	Reserved
36 to 39	Unsigned32	PID of expected response
40 to 41	Unsigned16	Cycle multiplier of expected response
42 to 43	Unsigned16	Cycle offset of expected response
44 to 47	Unsigned32	PID of transmitted response
48 to 49	Unsigned16	Cycle multiplier of transmitted response
50 to 51	Unsigned16	Cycle offset of transmitted response
52 to 55	Unsigned32	Maximum delay in µs of expected response
56	Unsigned8	Number of repetitions of transmitted response
57	Unsigned8	Reserved

IECNORM.COM : Click to view the full PDF of IEC PAS 61784-3-18:2009
Withdrawn

Table 16 – Fail-safe consumer heartbeat

Attribute	Value
Index	0x1216
Name	Fail-safe consumer heartbeat list
Object type	ARRAY
Data type	OCTET_STRING
Category	Optional
Sub-index	0x00
Name	Number of supported entries
Data type	Unsigned8
Category	Mandatory
Access attribute	RO
SPDO mapping	No
Value range	0x01 to 0xFF
Value	No
Sub-index	0x01
Name	Consumer heartbeat
Data type	OCTET_STRING
Category	Mandatory
Access attribute	FS
SPDO mapping	No
Value range	No
Value	No
Sub-index	0x02 to 0xFE
Name	Consumer heartbeat
Data type	OCTET_STRING
Category	Optional
Access attribute	FS
SPDO mapping	No
Value range	No
Value	No

IECNORM.COM : Click to view the full PDF of IEC PAS 61784-3-18:2009
Withdrawn

8.2.2.5 Fail-safe producer heartbeat parameter

The fail-safe producer heartbeat parameter object is specified in Table 17.

Table 17 – Fail-safe producer heartbeat parameter

Attribute	Value
Index	0x1217
Name	Fail-safe 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

Attribute	Value
Data type	Unsigned8
Category	Mandatory
Access attribute	RO
SPDO mapping	No
Value range	0x01 to 0x0C
Value	No
Sub-index	0x01
Name	RTFL PID
Data type	Unsigned32
Category	Conditional
Access attribute	FS
SPDO mapping	No
Value range	0x01 to 0x00FFFFFF
Value	No
Sub-index	0x02
Name	RTFN PID
Data type	Unsigned32
Category	Conditional
Access attribute	FS
SPDO mapping	No
Value range	0x01 to 0x00FFFFFF
Value	No
Sub-index	0x04
Name	Transmission type
Data type	Unsigned8
Category	Mandatory
Access attribute	FS
SPDO mapping	No
Value range	No
Value	No
Sub-index	0x05
Name	Time sync ID
Data type	Unsigned16
Category	Conditional
Access attribute	FS
SPDO mapping	No
Value range	0x00 to 0xFF
Value	No
Sub-index	0x06
Name	Event time
Data type	Unsigned16
Category	Conditional
Access attribute	FS
SPDO mapping	No

IECNORM.COM : Click to view the full PDF of IEC PAS 61784-3-18:2009
Withdrawn

Attribute	Value
Value range	No
Value	No
Sub-index	0x07
Name	Cycle multiplier
Data type	Unsigned16
Category	Conditional
Access attribute	FS
SPDO mapping	No
Value range	0x01 to 0xFFFF
Value	No
Sub-index	0x08
Name	Cycle offset
Data type	Unsigned16
Category	Conditional
Access attribute	FS
SPDO mapping	No
Value range	No
Value	No
Sub-index	0x09
Name	Number of repetitions
Data type	Unsigned8
Category	Mandatory
Access attribute	FS
SPDO mapping	No
Value range	No
Value	2
Sub-index	0x0A
Name	Device address
Data type	Unsigned16
Category	Conditional
Access attribute	FS
SPDO mapping	No
Value range	0x00 to 0x200
Value	No
Sub-index	0x0B
Name	IPv4 address
Data type	Unsigned32
Category	Conditional
Access attribute	FS
SPDO mapping	No
Value range	No
Value	No
Sub-index	0x0C
Name	IPv6 address

IECNORM.COM : Click to view the full PDF of IEC PAS 61784-3-18:2009
Withdrawn

Attribute	Value
Data type	Unsigned128
Category	Conditional
Access attribute	FS
SPDO mapping	No
Value range	No
Value	No

8.2.2.6 Fail-safe bus cycle times

The fail-safe bus cycle time object is specified in Table 18. The fail-safe bus cycle times are used to compute the timeout values for safe packets.

Table 18 – Fail-safe bus cycle times

Attribute	Value
Index	0x1218
Name	Fail-safe 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	Fail-safe RTFN base cycle time
Data type	Unsigned32
Category	Conditional
Access attribute	FS
SPDO mapping	No
Value range	No
Value	No
Sub-index	0x02
Name	Fail-safe RTFL base cycle time
Data-type	Unsigned32
Category	Conditional
Access attribute	FS
SPDO mapping	No
Value range	No
Value	No

IECNORM.COM : Click to view the full PDF of IEC PAS 61784-3-18:2009
Withdrawn

8.2.2.7 SPDO timeout tolerance

The SPDO timeout tolerance object is specified in Table 19.

Table 19 – SPDO timeout tolerance

Attribute	Value
Index	0x121E
Name	SPDO timeout tolerance
Object type	VAR
Data type	Unsigned8
Category	Conditional
Access attribute	FS
SPDO mapping	No
Value range	Unsigned8
Value	No

8.2.2.8 RxSPDO communication parameter

The receive SPDO communication parameter object is specified in Table 20.

Table 20 – 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
Data type	Unsigned32
Category	Conditional
Access attribute	FS
SPDO mapping	No
Value range	0x01 to 0x00FFFFFF
Value	No
Sub-index	0x02
Name	RTFN PID
Data type	Unsigned32

IECNORM.COM : Click to view the full PDF of IEC PAS 61784-3-18:2009
Withdrawn

Attribute	Value
Category	Conditional
Access attribute	FS
SPDO mapping	No
Value range	0x01 to 0x00FFFFFF
Value	No
Sub-index	0x03
Name	SID
Data type	Unsigned16
Category	Mandatory
Access attribute	FS
SPDO mapping	No
Value range	No
Value	No
Sub-index	0x04
Name	Transmission type
Data type	Unsigned8
Category	Mandatory
Access attribute	FS
SPDO mapping	No
Value range	No
Value	No
Sub-index	0x05
Name	Time sync ID
Data type	Unsigned16
Category	Conditional
Access attribute	FS
SPDO mapping	No
Value range	0x00 to 0xFF
Value	No
Sub-index	0x06
Name	Timeout
Data type	Unsigned16
Category	Optional
Access attribute	FS
SPDO mapping	No
Value range	No
Value	No
Sub-index	0x07
Name	Cycle multiplier
Data type	Unsigned16
Category	Conditional
Access attribute	FS
SPDO mapping	No
Value range	0x01 to 0xFFFF

IECNORM.COM : Click to view the full PDF of IEC PAS 61784-3-18:2009
Withdrawn

Attribute	Value
Value	No
Sub-index	0x08
Name	Cycle offset
Data type	Unsigned16
Category	Conditional
Access attribute	FS
SPDO mapping	No
Value range	0x00 to 0xFFFE
Value	No
Sub-index	0x09
Name	Number of allowed receives
Data type	Unsigned8
Category	Mandatory
Access Attribute	FS
SPDO mapping	No
Value range	No
Value	2
Sub-index	0x0A
Name	Device address
Data type	Unsigned16
Category	Conditional
Access attribute	FS
SPDO mapping	No
Value range	0x00 to 0x200
Value	No
Sub-index	0x0B
Name	IPv4 address
Data type	Unsigned32
Category	Conditional
Access attribute	FS
SPDO mapping	No
Value range	No
Value	No
Sub-index	0x0C
Name	IPv6 address
Data type	Unsigned128
Category	Conditional
Access attribute	FS
SPDO mapping	No
Value range	No
Value	No

IECNORM.COM : Click to view the full PDF of IEC PAS 61784-3-18:2009
Withdrawn

8.2.2.9 TxSPDO communication parameter

The transmit SPDO communication parameter object is specified in Table 21.

Table 21 – 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
Data type	Unsigned32
Category	Conditional
Access attribute	FS
SPDO mapping	No
Value range	0x01 to 0x00FFFFFF
Value	No
Sub-index	0x02
Name	RTFN PID
Data type	Unsigned32
Category	Conditional
Access attribute	FS
SPDO mapping	No
Value range	0x01 to 0x00FFFFFF
Value	No
Sub-index	0x04
Name	Transmission type
Data type	Unsigned8
Category	Mandatory
Access attribute	FS
SPDO mapping	No
Value range	No
Value	No
Sub-index	0x05
Name	Time sync ID

IECNORM.COM : Click to view the full PDF of IEC PAS 61784-3-18:2009
Withdrawn

Attribute	Value
Data type	Unsigned16
Category	Conditional
Access attribute	FS
SPDO mapping	No
Value range	0x00 to 0xFF
Value	No
Sub-index	0x06
Name	Event time
Data type	Unsigned16
Category	Conditional
Access attribute	FS
SPDO mapping	No
Value range	No
Value	No
Sub-index	0x07
Name	Cycle multiplier
Data type	Unsigned16
Category	Conditional
Access attribute	FS
SPDO mapping	No
Value range	0x01 to 0xFFFF
Value	No
Sub-index	0x08
Name	Cycle offset
Data type	Unsigned16
Category	Conditional
Access attribute	FS
SPDO mapping	No
Value range	No
Value	No
Sub-index	0x09
Name	Number of repetitions
Data type	Unsigned8
Category	Mandatory
Access attribute	FS
SPDO mapping	No
Value range	No
Value	2
Sub-index	0x0A
Name	Device address
Data type	Unsigned16
Category	Conditional
Access attribute	FS
SPDO mapping	No

IECNORM.COM : Click to view the full PDF of IEC PAS 61784-3-18:2009
Withdrawn