IEC/PAS 61784-3-18

Edition 1.0 2009-08

PUBLICLY AVAILABLE SPECIFICATION

PRE-STANDARD

colour inside

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

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 It also gives information on projects, withdrawn and replaced publications.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

IEC/PAS 61784-3-18

Edition 1.0 2009-08

PUBLICLY AVAILABLE SPECIFICATION

PRE-STANDARD

colour inside

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

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

PRICE CODE XA

ICS 13.110; 25.040.40; 35.100.05

ISBN 978-2-88910-807-7

CONTENTS

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.

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.

INTRODUCTION

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

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES –

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

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.

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

[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

[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