

INTERNATIONAL STANDARD



Industrial communication networks – Profiles –
Part 3-1: Functional safety fieldbuses – Additional specifications for CPF 1
(standards.iteh.ai)

IEC 61784-3-1:2010

<https://standards.iteh.ai/catalog/standards/sist/abdbb12b-56ab-429b-b40d-6b3af25aa3c7/iec-61784-3-1-2010>



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2010 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 Varembe
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 It also gives information on projects, withdrawn and replaced publications.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

INTERNATIONAL STANDARD



**Industrial communication networks – Profiles –
Part 3-1: Functional safety fieldbuses – Additional specifications for CPF 1**

<https://standards.iteh.ai/catalog/standards/sist/abdbb12b-56ab-429b-b40d-6b3af25aa3c7/iec-61784-3-1-2010>

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

PRICE CODE **XB**

ICS 25.040.40; 35.100.05

ISBN 978-2-88910-973-9

CONTENTS

FOREWORD.....	7
0 Introduction	9
0.1 General.....	9
0.2 Patent declaration	11
1 Scope.....	12
2 Normative references	12
3 Terms, definitions, symbols, abbreviated terms and conventions	13
3.1 Terms and definitions	13
3.1.1 Common terms and definitions	14
3.1.2 CPF 1: Additional terms and definitions	18
3.2 Symbols and abbreviated terms.....	19
3.2.1 Common symbols and abbreviated terms	19
3.2.2 CPF 1: Additional symbols and abbreviated terms	19
3.3 Conventions	20
3.3.1 State diagrams	20
3.3.2 Use of colors in figures.....	21
4 Overview of FSCP 1/1 (FOUNDATION Fieldbus™ SIS).....	21
4.1 General.....	21
4.2 Key concepts of FSCP 1/1.....	22
4.2.1 Black channel.....	22
4.2.2 Connection key.....	22
4.2.3 Cross-check	23
4.2.4 FSCP 1/1.....	23
4.2.5 Programmable electronic system.....	23
4.2.6 Queuing delays	23
4.2.7 Redundancy	23
4.2.8 SIL environment	23
4.3 Key components of FSCP 1/1.....	23
4.3.1 Overview	23
4.3.2 Black channel.....	24
4.4 Relationship to the ISO OSI basic reference model	25
5 General	25
5.1 External documents providing specifications for the profile.....	25
5.2 Safety functional requirements	25
5.2.1 Requirements for functional safety.....	25
5.2.2 Functional constraints.....	26
5.2.3 Device manufacturer requirements	26
5.3 Safety measures	26
5.3.1 Sequence number	26
5.3.2 Time stamp	26
5.3.3 Time expectation	26
5.3.4 Connection authentication	26
5.3.5 Data integrity assurance.....	26
5.3.6 Redundancy with cross checking	27
5.3.7 Different data integrity assurance systems	27
5.3.8 Relationships between errors and safety measures	27

5.4	Safety communication layer structure	27
5.4.1	Network topology and device connectivity	27
5.4.2	Device architecture	28
5.5	Relationships with FAL (and DLL, PhL)	29
5.5.1	General	29
5.5.2	Data types	29
6	Safety communication layer services	30
6.1	Application Process (AP)	30
6.1.1	Overview	30
6.1.2	Network visible objects	30
6.1.3	Application layer interface	30
6.1.4	Object dictionary	30
6.1.5	Application program directory	30
6.2	Function block application processes	31
6.2.1	General	31
6.2.2	Function block model	31
6.2.3	Application process	33
6.3	Device to device communications	36
6.3.1	General	36
6.3.2	Client/server	36
6.3.3	Publisher/subscriber	37
6.3.4	Report distribution	37
6.3.5	FBAP operation in a linking device	37
6.3.6	System management kernel protocol (SMKP) communications	37
6.4	Profiles	37
6.4.1	General	37
6.4.2	FSCP 1/1 profile	37
6.5	Device descriptions	38
6.6	Common file formats	38
6.7	Configuration information	39
6.7.1	Overview	39
6.7.2	Level 1 configuration: manufacturer device definition	39
6.7.3	Level 2 configuration: network definition	39
6.7.4	Level 3 configuration: distributed application definition	39
6.7.5	Level 4 configuration: device configuration	39
7	Safety communication layer protocol	39
7.1	Safety PDU format	39
7.1.1	General	39
7.1.2	Safety communication layer CRC	39
7.1.3	Black channel time synchronization monitoring	40
7.1.4	Sequence number	40
7.1.5	Virtual header	41
7.1.6	Connection key	41
7.1.7	Redundancy and cross-check	41
7.2	Protocol extensions for use in safety-related systems	42
7.2.1	Overview	42
7.2.2	Publisher-subscriber interactions	42
7.2.3	Client-server interactions	47
7.2.4	Time synchronization	53

7.2.5	Device start-up	54
7.3	Communications entity	54
7.3.1	General	54
7.3.2	Network management	54
7.3.3	FMS	54
7.3.4	H1 stack	54
8	Safety communication layer management.....	55
8.1	Overview	55
8.2	SMK communications	55
8.3	FMS services	55
8.4	SMK services	55
8.4.1	General	55
8.4.2	Address assignment	55
8.4.3	Time synchronization.....	55
8.5	Safety communication layer configuration and start-up.....	55
8.5.1	H1 configuration and start-up	55
8.5.2	FSCP 1/1 FBAP	56
8.5.3	Testing	56
9	System requirements.....	56
9.1	Indicators and switches	56
9.2	Installation guidelines.....	56
9.3	Safety function response time	56
9.3.1	Overview	56
9.3.2	Safety Sensor.....	56
9.3.3	Input Function Block	57
9.3.4	Safe Transmission	57
9.3.5	Logic Solver	57
9.3.6	Discrete Output Function Block	57
9.3.7	Safety Actuator.....	57
9.4	Duration of demands	57
9.5	Constraints for calculation of system characteristics.....	57
9.5.1	System characteristics.....	57
9.5.2	Message rate.....	57
9.5.3	SIL level	58
9.5.4	Mixing FSCP 1/1 devices and CP 1/1 devices.....	58
9.5.5	Devices on a segment	58
9.5.6	Residual error rate calculations	58
9.6	Maintenance.....	59
9.7	Safety manual	59
10	Assessment.....	59
Annex A (informative)	Additional information for functional safety communication profiles of CPF 1	60
A.1	Hash function calculation.....	60
A.2	Fault conditions arising from locations beyond the output function block.....	62
Annex B (informative)	Information for assessment of the functional safety communication profiles of CPF 1	64
Bibliography.....		65

Table 1 – Example state transition table	21
Table 2 – Safety measures and possible communication errors	27
Table 3 – Data types used within FSCP 1/1	30
Table 4 – Fault state behaviour.....	33
Table 5 – Publisher states	43
Table 6 – Publisher state table - Received transitions.....	44
Table 7 – Publisher state table - Internal transitions.....	44
Table 8 – Subscriber states	45
Table 9 – Subscriber state table - Received transitions.....	46
Table 10 – Subscriber state table - Internal transitions.....	47
Table 11 – Server states during read operations	48
Table 12 – Received transitions for a FSCP 1/1 Server during read operations.....	49
Table 13 – States of a FSCP 1/1 server during write operations.....	51
Table 14 – Received transitions for a FSCP 1/1 Server during write operations	51
Table 15 – Values used for calculation of residual error rate.....	58
Table 16 – Values of R_{SL} (P_e) for different values of n	58
Table A.1 – Fault conditions arising from locations beyond the output function block	63

iTeh STANDARD PREVIEW

Figure 1 – Relationships of IEC 61784-3 with other standards (machinery)	9
Figure 2 – Relationships of IEC 61784-3 with other standards (process).....	10
Figure 3 – Example state diagram..... IEC 61784-3-1:2010	20
Figure 4 – Use of colors in figures.....	21
Figure 5 – Scope of FSCP 1/1	22
Figure 6 – FSCP 1/1 architecture (H1)	24
Figure 7 – Black channel	24
Figure 8 – FSCP 1/1 in system architecture	28
Figure 9 – FSCP 1/1 H1 device.....	28
Figure 10 – FSCP 1/1 protocol layers	29
Figure 11 – Relationship between FSCP 1/1 and the other layers of IEC 61158 Type 1	29
Figure 12 – Key write-lock	32
Figure 13 – Password write-lock	32
Figure 14 – Example of FSCP 1/1 communication.....	36
Figure 15 – Example of device description.....	38
Figure 16 – Safety PDU showing virtual content.....	43
Figure 17 – Safety PDU showing duplication of data and addition of CRC.....	43
Figure 18 – State transition diagram for a FSCP 1/1 Publisher.....	43
Figure 19 – Safety PDU showing duplication of data and addition of CRC.....	45
Figure 20 – Safety PDU showing virtual content.....	45
Figure 21 – State transition diagram for a FSCP 1/1 subscriber	46
Figure 22 – Safety PDU showing virtual content.....	48
Figure 23 – Safety PDU showing virtual content with sub index	48
Figure 24 – Safety PDU showing duplication of data, addition of sequence number and CRC	48

Figure 25 – State transition diagram for a FSCP 1/1 Server during read operations 49

Figure 26 – Safety PDU showing duplication of data and addition of sequence number and CRC..... 50

Figure 27 – Example of FSCP 1/1 write 50

Figure 28 – Example of FSCP 1/1 write with sub index 50

Figure 29 – State transition diagram for a FSCP 1/1 Server during write operations..... 51

Figure 30 – Safety PDU showing duplication of data and CRC 52

Figure 31 – Example of safety function response time components..... 56

Figure 32 – Example FSCP 1/1 network topology..... 57

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[IEC 61784-3-1:2010](https://standards.iteh.ai/catalog/standards/sist/abdbb12b-56ab-429b-b40d-6b3af25aa3c7/iec-61784-3-1-2010)

<https://standards.iteh.ai/catalog/standards/sist/abdbb12b-56ab-429b-b40d-6b3af25aa3c7/iec-61784-3-1-2010>

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**INDUSTRIAL COMMUNICATION NETWORKS –
PROFILES –**
**Part 3-1: Functional safety fieldbuses –
Additional specifications for CPF 1**

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.

International Standard IEC 61784-3-1 has been prepared by subcommittee 65C: Industrial networks, of IEC technical committee 65: Industrial process measurement, control and automation.

This second edition cancels and replaces the first edition published in 2007. This edition constitutes a technical revision. The main changes with respect to the previous edition are listed below:

- updates in relation with changes in IEC 61784-3;
- adjustment of Figure 5;
- change of sequence number from two octets to four octets in 7.2.2 to match the final protocol from the consortium.
- addition of details for time synchronization in 7.2.4;
- addition of information for safety response time in 9.3;
- addition of information in constraints for calculation of system characteristics in 9.5.

The text of this standard is based on the following documents:

FDIS	Report on voting
65C/591A/FDIS	65C/603/RVD

Full information on the voting for the approval of this standard can be found in the report on voting indicated in the above table.

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 this publication 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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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.

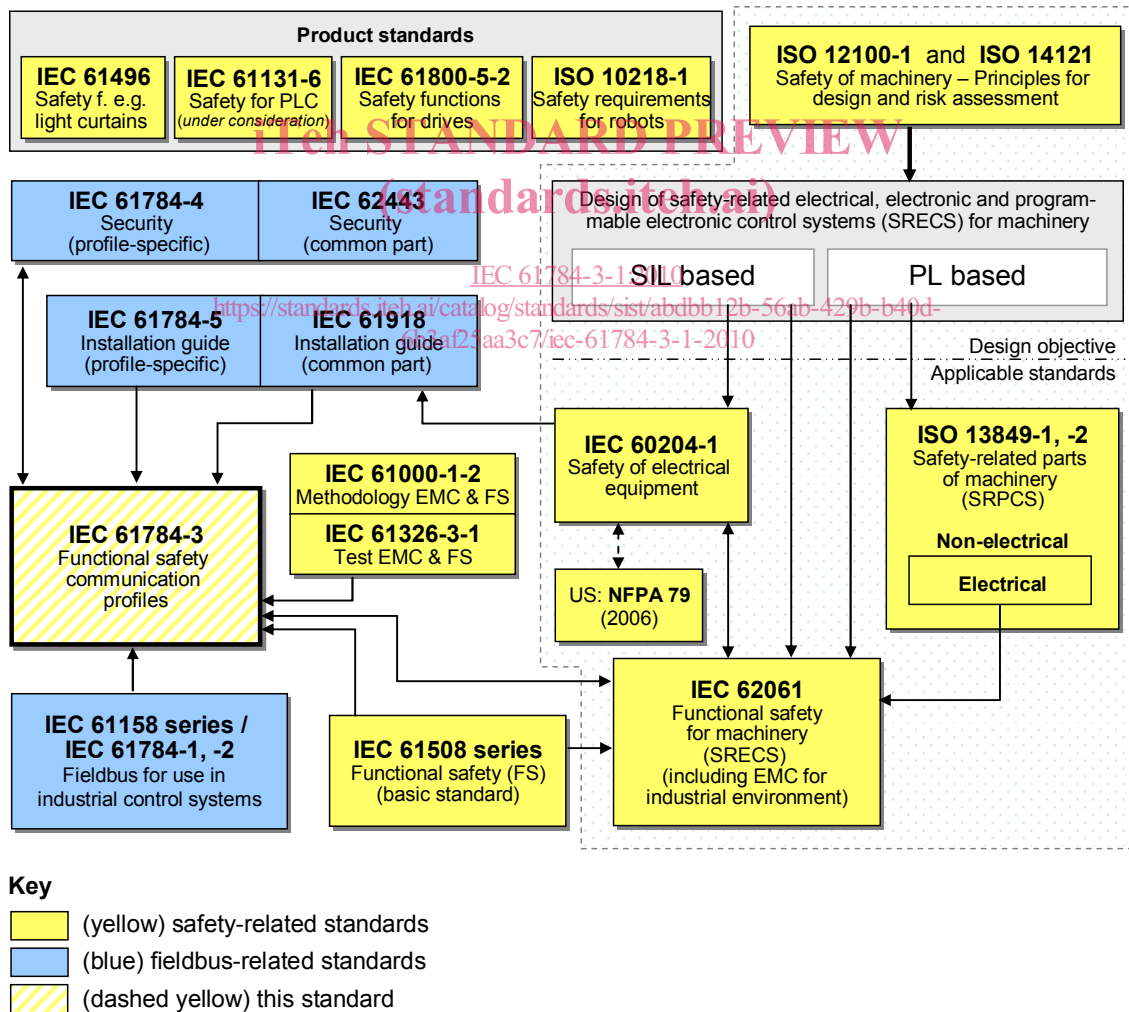
0 Introduction

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.

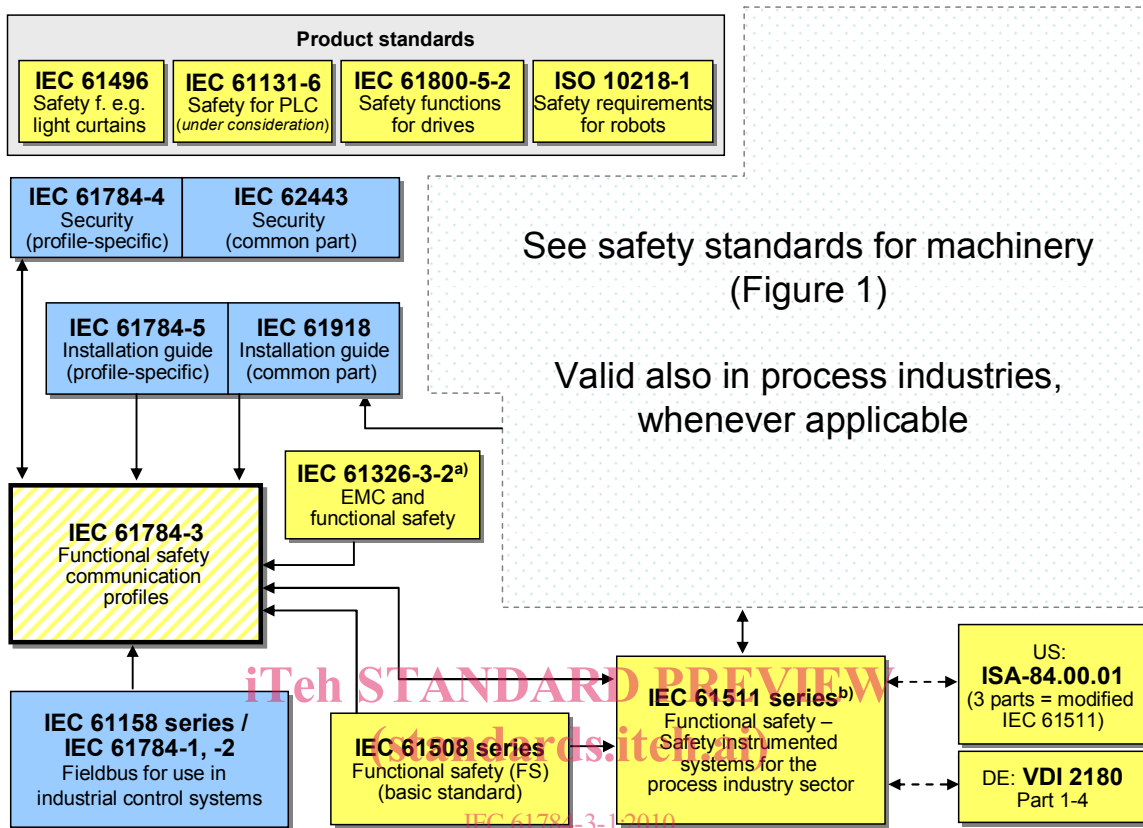
Figure 1 shows the relationships between this standard and relevant safety and fieldbus standards in a machinery environment.



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.



<https://standards.iteh.ai/catalog/standards/sist/abdbb12b-56ab-429b-b40d-6b3af25aa3c7/iec-61784-3-1-2010>

Key

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

^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 patents concerning the functional safety communication profiles for family 1 as follows, where the [xx] notation indicates the holder of the patent right:

US 6,999,824	[FF]	System and method for implementing safety instrumented systems in a fieldbus architecture
--------------	------	---

IEC takes no position concerning the evidence, validity and scope of these patent rights.

The holders of these patents rights have assured the IEC that they are willing to negotiate licences under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statement of the holders of these patent rights are registered with IEC.

<https://standards.iteh.ai/catalog/standards/sist/abdbb12b-56ab-429b-b40d-6b3af25aa3c7/iec-61784-3-1-2010>

Information may be obtained from:

[FF]	Fieldbus Foundation
	9005 Mountain Ridge Drive
	Bowie Bldg. - Suite 190
	Austin, TX 78759-5316
	USA
	Tel: +1 512 794 8890

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.

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES –

Part 3-1: Functional safety fieldbuses – Additional specifications for CPF 1

1 Scope

This part of the IEC 61784-3 series specifies a safety communication layer (services and protocol) based on CPF 1 of IEC 61784-1 and IEC 61158 Types 1 and 9. It identifies the principles for functional safety communications defined in IEC 61784-3 that are relevant for this safety communication layer.

NOTE 1 It does not cover electrical safety and intrinsic safety aspects. Electrical safety relates to hazards such as electrical shock. Intrinsic safety relates to hazards associated with potentially explosive atmospheres.

This part¹ defines mechanisms for the transmission of safety-relevant messages among participants within a distributed network using fieldbus technology in accordance with the requirements of IEC 61508 series² for functional safety. These mechanisms may be used in various industrial applications such as process control, manufacturing automation and machinery.

This part provides guidelines for both developers and assessors of compliant devices and systems.

NOTE 2 The resulting SIL claim of a system depends on the implementation of the selected functional safety communication profile within this system – implementation of a functional safety communication profile according to this part in a standard device is not sufficient to qualify it as a safety device.

2 Normative references

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

IEC 61131-2, *Programmable controllers – Part 2: Equipment requirements and tests*

IEC 61158-2, *Industrial communication networks – Fieldbus specifications – Part 2: Physical layer specification and service definition*

IEC 61158-3-1, *Industrial communication networks – Fieldbus specifications – Part 3-1: Data-link layer service definition – Type 1 elements*

IEC 61158-4-1, *Industrial communication networks – Fieldbus specifications – Part 4-1: Data-link layer protocol specification – Type 1 elements*

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

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 61158-5-9, *Industrial communication networks – Fieldbus specifications – Part 5-9: Application layer service definition – Type 9 elements*

IEC 61158-6-5, *Industrial communication networks – Fieldbus specifications – Part 6-5: Application layer protocol specification – Type 5 elements*

IEC 61158-6-9, *Industrial communication networks – Fieldbus specifications – Part 6-9: Application layer protocol specification – Type 9 elements*

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

IEC 61508-1:2010³, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements*

IEC 61508-2:2010³, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*

IEC 61508-3:2010³, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements*

IEC 61508-4:2010³, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations*

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

standards.iteh.ai
IEC 61784-3-1:2010

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

standards.iteh.ai
6b3af25aa3c7/iec-61784-3-1-2010

IEC 61784-3:2010⁴, *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*

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

ISO/IEC 8802-3, *Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications*

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 To be published.

⁴ To be published.