

INTERNATIONAL STANDARD



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

(<https://standards.iteh.ai>)

Document Preview

IEC 61784-3-3:2010

<https://standards.iteh.ai/catalog/standards/iec/3eccc5d6-59ce-4baa-ace0-5650cb656c38/iec-61784-3-3-2010>

Withhold



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 It also gives information on projects, withdrawn and replaced publications.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

IEC 61784-3-3:2010

<https://standards.iec.org/standards/iec/38/cb5d6-59ce-4baa-ace0-5650cb656c38/iec-61784-3-3-2010>



IEC 61784-3-3

Edition 2.0 2010-06

INTERNATIONAL STANDARD



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

Document Preview
[\(https://standards.iteh.ai/\)](https://standards.iteh.ai/)

IEC 61784-3-3:2010

<https://standards.iteh.ai/catalog/standards/iec/38cc5d6-59ce-4baa-ace0-5650cb656c38/iec-61784-3-3-2010>

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

PRICE CODE **XF**

ICS 25.040.40; 35.100.05

ISBN 978-2-88910-978-4

CONTENTS

FOREWORD.....	8
0 Introduction.....	10
0.1 General.....	10
0.2 Patent declaration.....	12
1 Scope.....	13
2 Normative references.....	13
3 Terms, definitions, symbols, abbreviated terms and conventions.....	15
3.1 Terms and definitions.....	15
3.1.1 Common terms and definitions.....	15
3.1.2 CPF 3: Additional terms and definitions.....	20
3.2 Symbols and abbreviated terms.....	23
3.2.1 Common symbols and abbreviated terms.....	23
3.2.2 CPF 3: Additional symbols and abbreviated terms.....	24
3.3 Conventions.....	25
4 Overview of FSCP 3/1 (PROFIsafe™).....	25
5 General.....	28
5.1 External documents providing specifications for the profile.....	28
5.2 Safety functional requirements.....	28
5.3 Safety measures.....	29
5.4 Safety communication layer structure.....	30
5.4.1 Principle of FSCP 3/1 safety communications.....	30
5.4.2 CPF 3 communication structures.....	31
5.5 Relationships with FAL (and DLL, PhL).....	34
5.5.1 Device model.....	34
5.5.2 Application and communication relationships.....	34
5.5.3 Message format.....	36
5.5.4 Data types.....	36
6 Safety communication layer services.....	37
6.1 F-Host services.....	37
6.2 F-Device services.....	39
6.3 Diagnosis.....	41
6.3.1 Safety alarm generation.....	41
6.3.2 F-Device safety layer diagnosis including the iPar-Server.....	41
7 Safety communication layer protocol.....	42
7.1 Safety PDU format.....	42
7.1.1 Safety PDU structure.....	42
7.1.2 Safety I/O data.....	43
7.1.3 Status and Control Byte.....	43
7.1.4 (Virtual) Consecutive Number.....	44
7.1.5 CRC2 Signature.....	46
7.1.6 Appended standard I/O data.....	47
7.2 FSCP 3/1 behavior.....	47
7.2.1 General.....	47
7.2.2 F-Host state diagram.....	47
7.2.3 F-Device state diagram.....	51
7.2.4 Sequence diagrams.....	55

7.2.5	Timing diagram for a counter reset	61
7.2.6	Monitoring of safety times.....	61
7.3	Reaction in the event of a malfunction.....	64
7.3.1	Repetition.....	64
7.3.2	Loss	65
7.3.3	Insertion	65
7.3.4	Incorrect sequence	65
7.3.5	Corruption of safety data	65
7.3.6	Delay.....	66
7.3.7	Masquerade	66
7.3.8	Memory failures within switches	66
7.3.9	Network boundaries and router.....	67
7.4	F-Startup and change coordination.....	68
7.4.1	Standard startup procedure	68
7.4.2	iParameter assignment deblocking	68
8	Safety communication layer management.....	69
8.1	F-Parameter	69
8.1.1	Summary.....	69
8.1.2	F_Source/Destination_Address (codename).....	69
8.1.3	F_WD_Time (F-Watchdog time).....	69
8.1.4	F_WD_Time_2 (secondary F-Watchdog time).....	70
8.1.5	F_Prm_Flag1 (Parameters for the safety layer management)	70
8.1.6	F_Prm_Flag2 (Parameters for the safety layer management)	72
8.1.7	F_iPar_CRC (value of iPar_CRC across iParameters).....	73
8.1.8	F_Par_CRC (CRC1 across F-Parameters).....	73
8.1.9	Structure of the F-Parameter record data object	74
8.1.10	F-Data fraction	74
8.2	iParameter and iPar_CRC.....	74
8.3	Safety parameterization.....	75
8.3.1	Objectives	75
8.3.2	GSDL and GSDML safety extensions.....	76
8.3.3	Securing safety parameters and GSD data	77
8.4	Safety configuration	80
8.4.1	Securing the safety I/O data description (CRC7).....	80
8.4.2	DataItem data type section examples	81
8.5	Data type information usage.....	84
8.5.1	F-Channel driver.....	84
8.5.2	Rules for standard F-Channel drivers	85
8.5.3	Recommendations for F-Channel drivers	86
8.6	Safety parameter assignment mechanisms.....	87
8.6.1	F-Parameter assignment	87
8.6.2	General iParameter assignment.....	87
8.6.3	System integration requirements for iParameterization tools.....	88
8.6.4	iPar-Server	90
9	System requirements.....	99
9.1	Indicators and switches	99
9.2	Installation guidelines.....	99
9.3	Safety function response time	99
9.3.1	Model	99

9.3.2	Calculation and optimization	101
9.3.3	Adjustment of watchdog times for FSCP 3/1	103
9.3.4	Engineering tool support.....	104
9.3.5	Retries (repetition of messages)	104
9.4	Duration of demands	105
9.5	Constraints for the calculation of system characteristics	106
9.5.1	Probabilistic considerations	106
9.5.2	Safety related constraints	108
9.5.3	Non safety related constraints (availability).....	109
9.6	Maintenance.....	109
9.6.1	F-Module commissioning / replacement	109
9.6.2	Identification and maintenance functions	109
9.7	Safety manual	110
9.8	Wireless transmission channels.....	111
9.8.1	Black channel approach	111
9.8.2	Availability	111
9.8.3	Security measures	111
9.8.4	Stationary and mobile applications	113
9.9	Conformance classes	113
10	Assessment.....	114
10.1	Safety policy	114
10.2	Obligations	115
Annex A (informative) Additional information for functional safety communication profiles of CPF 3.....		116
A.1	Hash function calculation.....	116
A.2	Response time measurements.....	118
Annex B (informative) Information for assessment of the functional safety communication profiles of CPF 3		122
Bibliography.....		123
Table 1 – Deployed measures to master errors		29
Table 2 – Data types used for FSCP 3/1		36
Table 3 – Safety layer diagnosis messages		41
Table 4 – F-Host states and transitions		49
Table 5 – F-Device states and transitions		53
Table 6 – SIL monitor times		64
Table 7 – Remedies for switch failures.....		67
Table 8 – Safety network boundaries		68
Table 9 – GSDL keywords for F-Parameters and F-I/O structures.....		76
Table 10 – I/O data structure items (Version 2).....		80
Table 11 – Sample F-Channel drivers		85
Table 12 – Requirements for iParameterization.....		88
Table 13 – Specifier for the iPar-Server Request		92
Table 14 – Structure of the Read_RES_PDU ("read record").....		94
Table 15 – Structure of the Write_REQ_PDU ("write record").....		95
Table 16 – Structure of the Pull_RES_PDU ("Pull").....		95

Table 17 – Structure of the Push_REQ_PDU ("Push")	95
Table 18 – iPar-Server states and transitions.....	97
Table 19 – iPar-Server management measures.....	98
Table 20 – Information to be included in the safety manual.....	110
Table 21 – Security measures for WLAN (IEEE 802.11i).....	112
Table 22 – Security measures for Bluetooth (IEEE 802.15.1).....	113
Table 23 – F-Host conformance class requirements.....	114
Table A.1 – The table "Crctab24" for 24 bit CRC signature calculations.....	117
Table A.2 – The table "Crctab32" for 32 bit CRC signature calculations.....	118
Figure 1 – Relationships of IEC 61784-3 with other standards (machinery).....	10
Figure 2 – Relationships of IEC 61784-3 with other standards (process).....	11
Figure 3 – Basic communication preconditions for FSCP 3/1.....	26
Figure 4 – Structure of an FSCP 3/1 safety PDU.....	27
Figure 5 – Safety communication modes.....	28
Figure 6 – Standard CPF 3 transmission system.....	30
Figure 7 – Safety layer architecture.....	31
Figure 8 – Basic communication layers.....	31
Figure 9 – Multiport switch bus structure.....	32
Figure 10 – Linear bus structure.....	32
Figure 11 – Crossing network borders with routers.....	33
Figure 12 – Complete safety transmission paths.....	33
Figure 13 – Device model.....	34
Figure 14 – Application relationships of a modular device.....	35
Figure 15 – Application and communication relationships (AR/CR).....	35
Figure 16 – Message format.....	36
Figure 17 – FSCP 3/1 communication structure.....	37
Figure 18 – F user interface of F-Host driver instances.....	38
Figure 19 – F-Device driver interfaces.....	40
Figure 20 – Safety PDU for CPF 3.....	42
Figure 21 – Status Byte.....	43
Figure 22 – Control Byte.....	44
Figure 23 – The Toggle Bit function.....	45
Figure 24 – F-Device Consecutive Number.....	45
Figure 25 – CRC2 generation (F-Host output).....	46
Figure 26 – Details of the CRC2 calculation (reverse order).....	47
Figure 27 – Safety layer communication relationship.....	47
Figure 28 – F-Host state diagram.....	48
Figure 29 – F-Device state diagram.....	52
Figure 30 – Interaction F-Host / F-Device during start-up.....	55
Figure 31 – Interaction F-Host / F-Device during F-Host power off → on.....	56
Figure 32 – Interaction F-Host / F-Device with delayed power on.....	57

Figure 33 – Interaction F-Host / F-Device during power off → on	58
Figure 34 – Interaction F-Host / F-Device while host recognizes CRC error	59
Figure 35 – Interaction F-Host / F-Device while device recognizes CRC error	60
Figure 36 – Impact of the counter reset signal	61
Figure 37 – Monitoring the message transit time F-Host ↔ F-Output	62
Figure 38 – Monitoring the message transit time F-Input ↔ F-Host	62
Figure 39 – Extended watchdog time on request	64
Figure 40 – F-Parameter data and CRC	65
Figure 41 – iParameter assignment deblocking by the F-Host	68
Figure 42 – Effect of F_WD_Time_2	70
Figure 43 – F_Prm_Flag1	70
Figure 44 – F_Check_SeqNr	71
Figure 45 – F_Check_iPar	71
Figure 46 – F_SIL	71
Figure 47 – F_CRC_Length	72
Figure 48 – F_Prm_Flag2	72
Figure 49 – F_Block_ID	72
Figure 50 – F_Par_Version	73
Figure 51 – F-Parameter	74
Figure 52 – iParameter block	75
Figure 53 – F-Parameter extension within the GSDML specification	77
Figure 54 – CRC1 including iPar_CRC	78
Figure 55 – Algorithm to build CRC0 (GSDL)	79
Figure 56 – Algorithm to build CRC0 (GSDML)	80
Figure 57 – DataItem section for F_IN_OUT_1	82
Figure 58 – DataItem section for F_IN_OUT_2	83
Figure 59 – DataItem section for F_IN_OUT_5	83
Figure 60 – DataItem section for F_IN_OUT_6	84
Figure 61 – F-Channel driver as "glue" between F-Device and user program	85
Figure 62 – Layout example of an F-Channel driver	86
Figure 63 – F-Parameter assignment for simple F-Devices and F-Slaves	87
Figure 64 – F and iParameter assignment for complex F-Devices	88
Figure 65 – System integration of CPD-Tools	89
Figure 66 – iPar-Server mechanism (commissioning)	90
Figure 67 – iPar-Server mechanism (for example F-Device replacement)	91
Figure 68 – iPar-Server request coding ("status model")	92
Figure 69 – Coding of SR_Type	93
Figure 70 – iPar-Server request coding ("alarm model")	94
Figure 71 – iPar-Server state diagram	96
Figure 72 – Example safety function with a critical response time path	100
Figure 73 – Simplified typical response time model	100
Figure 74 – Frequency distributions of typical response times of the model	101
Figure 75 – Context of delay times and watchdog times	102

Figure 76 – Timing sections forming the FSCP 3/1 F_WD_Time	103
Figure 77 – Frequency distribution of response times with message retries	104
Figure 78 – Retries with CP 3/1	105
Figure 79 – Retries with CP 3/RTE	105
Figure 80 – Residual error probabilities for the 24-bit polynomial	106
Figure 81 – Properness of the 32-bit polynomial for 52 octets	107
Figure 82 – Properness of the 32-bit polynomial for 132 octets	107
Figure 83 – Monitoring of corrupted messages.....	108
Figure 84 – Security for WLAN networks.....	111
Figure 85 – Security for Bluetooth networks.....	112
Figure A.1 – Typical "C" procedure of a cyclic redundancy check.....	116
Figure A.2 – Comparison of the response time model and a real application.....	119
Figure A.3 – Frequency distribution of measured response times.....	120
Figure A.4 – F-Host with standard and safety-related application programs	121

iTech Standards
(<https://standards.itih.ai>)
Document Preview

[IEC 61784-3-3:2010](https://standards.itih.ai/catalog/standards/iec/36cc65d6-59ce-4baa-ace0-5650cb656c38/iec-61784-3-3-2010)

<https://standards.itih.ai/catalog/standards/iec/36cc65d6-59ce-4baa-ace0-5650cb656c38/iec-61784-3-3-2010>

INTERNATIONAL ELECTROTECHNICAL COMMISSION

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

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 61784-3-3 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;
- introduction of a secondary watchdog timer (F_WD_Time_2) to cover the use cases 'configuration-in-run', or 'maintenance of fault tolerance systems', or both (7.1.3, 7.2.3, 7.2.6, 8.1.1, 8.1.4, 8.1.6.2);
- missing GSDL definitions conveyed from other approved documents (8.3.2.1);
- missing CRC signature calculation for a GSD conveyed from other approved documents (8.3.3.3);

- constraints for the parameter value assignment of the primary watchdog timer 'F_WD_Time' (9.3.3);
- identification of the safety parameterization state of an F-Device or F-Module via field IM4 (signature) within the I&M functions (9.6.2);
- updated documents in bibliography.

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.

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.

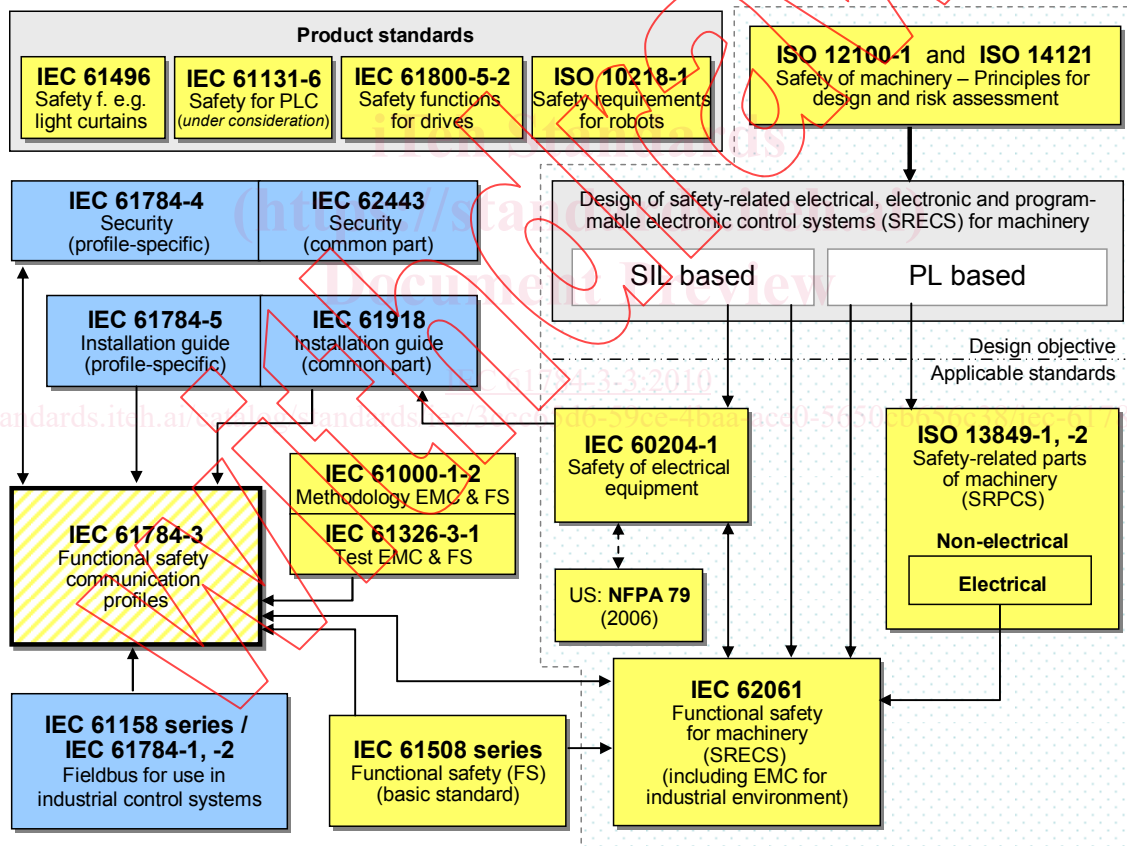
0 Introduction

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.

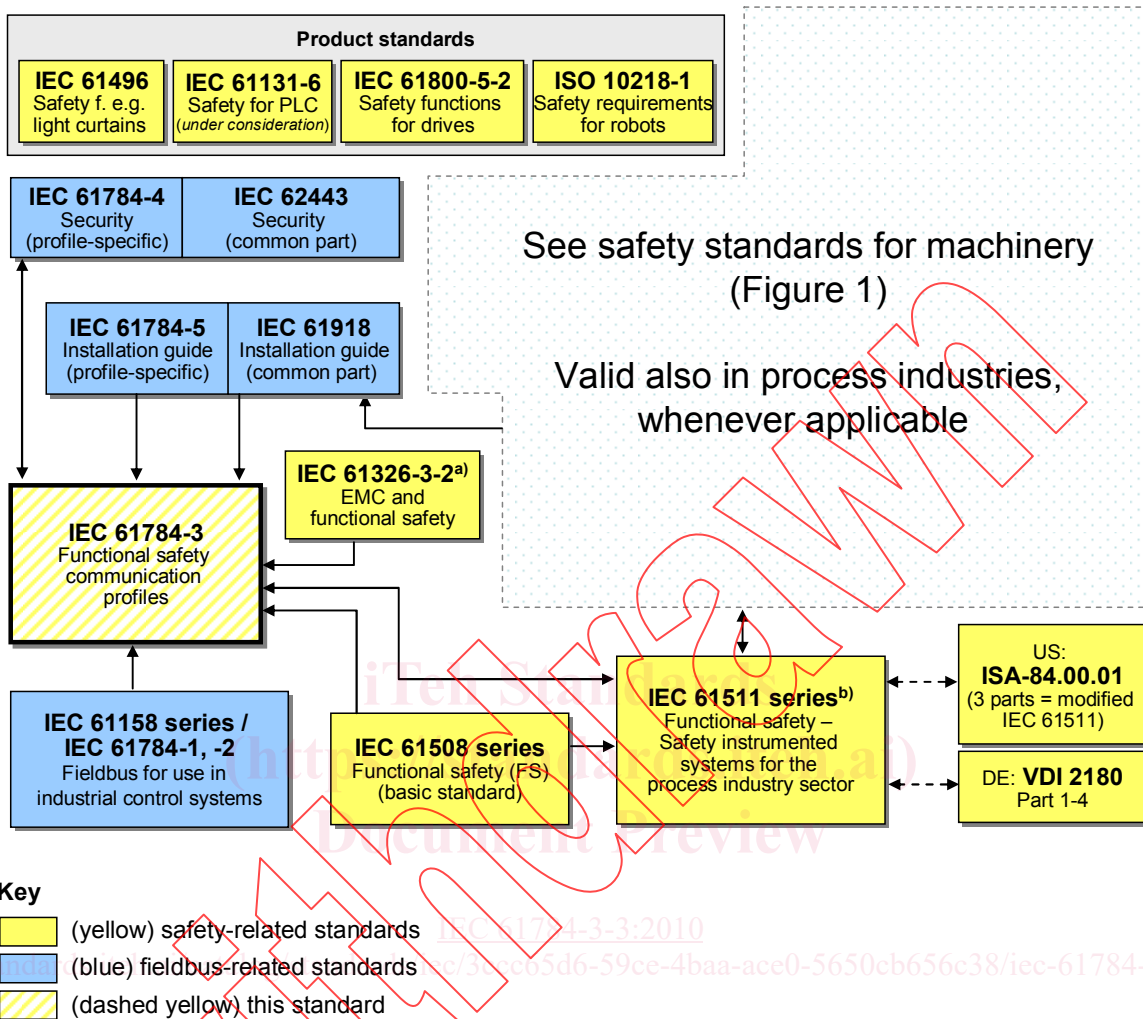


Key
 (yellow) safety-related standards
 (blue) fieldbus-related standards
 (dashed yellow) this standard

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

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

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



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

^b EN ratified.

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

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

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

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

This standard describes:

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

0.2 Patent declaration

The International Electrotechnical Commission (IEC) draws attention to the fact that it is claimed that compliance with this document may involve the use of patents concerning the functional safety communication profiles for family 3 as follows, where the [xx] notation indicates the holder of the patent right:

EP1267270-A2	[SI]	Method for data transfer
WO00/045562-A1	[SI]	Method and device for determining the reliability of data carriers
WO99/049373-A1	[SI]	Shortened data message of an automation system
EP1686732	[SI]	Method and system for transmitting protocol data units
EP1802019	[SI]	Identification of errors in data transmission
EP1921525-A1	[SI]	Method for operation of a safety-related system

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.

Information may be obtained from:

[SI] Siemens AG
 I IA AS FA TC
 76187 Karlsruhe
 GERMANY

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights other than those identified above. IEC shall not be held responsible for identifying any or all such patent rights.