



IEC 61784-3-3

Edition 1.0 2007-12

INTERNATIONAL STANDARD

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

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

PRICE CODE **XE**

ICS 35.100.20 25.040.40

ISBN 2-8318-9400-X

CONTENTS

FOREWORD.....	8
INTRODUCTION.....	10
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	19
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	23
3.3 Conventions	24
4 Overview of FSCP 3/1 (PROFIsafe™)	25
5 General	27
5.1 External documents providing specifications for the profile	27
5.2 Safety functional requirements	27
5.3 Safety measures	28
5.4 Safety communication layer structure	29
5.4.1 Principle of FSCP 3/1 safety communication	29
5.4.2 CPF 3 communication structures	30
5.5 Relationships with FAL (and DLL, PhL)	33
5.5.1 Device model.....	33
5.5.2 Application and communication relationships.....	33
5.5.3 Message format.....	35
5.5.4 Data types.....	35
6 Safety communication layer services	36
6.1 F-Host services	36
6.2 F-Device services.....	39
6.3 Diagnosis	40
6.3.1 Safety alarm generation.....	40
6.3.2 F-Device safety layer diagnosis including the iPar-Server.....	40
7 Safety communication layer protocol	41
7.1 Safety PDU format	41
7.1.1 Safety PDU structure.....	41
7.1.2 Safety I/O data	42
7.1.3 Status and Control Byte.....	42
7.1.4 (Virtual) Consecutive Number.....	44
7.1.5 CRC2 Signature	45
7.1.6 Appended standard I/O data	46
7.2 FSCP 3/1 behavior	46
7.2.1 General	46
7.2.2 F-Host state diagram	47
7.2.3 F-Device state diagram.....	50
7.2.4 Sequence diagrams.....	54
7.2.5 Timing diagram for a counter reset	60
7.2.6 Monitoring of safety times.....	60

7.3	Reaction in the event of a malfunction.....	63
7.3.1	Repetition.....	63
7.3.2	Loss.....	63
7.3.3	Insertion.....	63
7.3.4	Incorrect sequence.....	63
7.3.5	Corruption of safety data.....	63
7.3.6	Delay.....	64
7.3.7	Masquerade.....	64
7.3.8	Memory failures within switches.....	65
7.3.9	Network boundaries and router.....	66
7.4	F-Startup and change coordination.....	66
7.4.1	Standard startup procedure.....	66
7.4.2	iParameter assignment deblocking.....	66
8	Safety communication layer management.....	67
8.1	F-Parameter.....	67
8.1.1	Summary.....	67
8.1.2	F_Source/Destination_Address (codename).....	67
8.1.3	F_WD_Time (F-Watchdog time).....	68
8.1.4	F_Prm_Flag1 (Parameters for the safety layer management).....	68
8.1.5	F_Prm_Flag2 (Parameters for the safety layer management).....	69
8.1.6	F_iPar_CRC (value of iPar_CRC across F-Parameters).....	70
8.1.7	F_Par_CRC (CRC1 across F-Parameters).....	71
8.1.8	Structure of the F-Parameter record data object.....	71
8.1.9	F-Data fraction.....	71
8.2	iParameter and iPar_CRC.....	72
8.3	Safety parameterization.....	73
8.3.1	Objectives.....	73
8.3.2	GSD and GSDML safety extensions.....	73
8.3.3	Securing safety parameters and GSD data.....	74
8.4	Safety configuration.....	76
8.4.1	Securing the safety I/O data description (CRC7).....	76
8.4.2	Dataltem data type section examples.....	77
8.5	Data type information usage.....	79
8.5.1	F-Channel driver.....	79
8.5.2	Rules for standard F-Channel drivers.....	80
8.5.3	Recommendations for F-Channel drivers.....	80
8.6	Safety parameter assignment mechanisms.....	81
8.6.1	F-Parameter assignment.....	81
8.6.2	General iParameter assignment.....	82
8.6.3	System integration requirements for iParameterization tools.....	83
8.6.4	iPar-Server.....	84
9	System requirements.....	92
9.1	Indicators and switches.....	92
9.2	Installation guidelines.....	93
9.3	Safety function response time.....	93
9.3.1	Model.....	93
9.3.2	Calculation and optimization.....	95
9.3.3	Adjustment of watchdog times for FSCP 3/1.....	96
9.3.4	Engineering tool support.....	97

9.3.5	Retries (repetition of messages)	97
9.4	Duration of demands	98
9.5	Constraints for the calculation of system characteristics	99
9.5.1	Probabilistic considerations	99
9.5.2	Safety related constraints	101
9.5.3	Non safety related constraints (availability).....	102
9.6	Maintenance.....	102
9.6.1	F-Module commissioning / replacement.....	102
9.6.2	Identification and maintenance functions	102
9.7	Safety manual	103
9.8	Wireless transmission channels.....	103
9.8.1	Black Channel approach.....	103
9.8.2	Availability.....	104
9.8.3	Security measures.....	104
9.8.4	Stationary and mobile applications	106
9.9	Conformance classes	106
10	Certification.....	107
10.1	Safety policy	107
10.2	Obligations.....	108
Annex A (informative) Additional information for functional safety communication profiles of CPF 3		109
A.1	Hash function calculation.....	109
A.2	Response time measurements.....	111
Bibliography.....		115
Table 1	– Deployed measures to master or slave	28
Table 2	– Data types used for FSCP s/w	35
Table 3	– Safety layer diagnosis messages	40
Table 4	– F-Host states and transitions.....	48
Table 5	– F-Device states and transitions	52
Table 6	– SIL monitor times	63
Table 7	– Remedies for switch failures.....	65
Table 8	– Safety network boundaries	66
Table 9	– I/O data structure items (Version 2).....	76
Table 10	– Sample F-Channel drivers	80
Table 11	– Requirements for iParameterization.....	83
Table 12	– Specifier for the iPar-Server Request	87
Table 13	– Structure of the Read_RES_PDU ("read record").....	88
Table 14	– Structure of the Write_REQ_PDU ("write record").....	89
Table 15	– Structure of the Pull_RES_PDU ("Pull").....	89
Table 16	– Structure of the Push_REQ_PDU ("Push")	89
Table 17	– iPar-Server states and transitions.....	91
Table 18	– iPar-Server management measures.....	92
Table 19	– Information to be included in the safety manual.....	103
Table 20	– Security measures for WLAN (IEEE 802.11i).....	105

Table 21 – Security measures for Bluetooth (IEEE 802.15.1)	106
Table 22 – F-Host conformance class requirements	107
Table A.1 – The table "Crctab24" for 24 bit CRC signature calculations	110
Table A.2 – The table "Crctab32" for 32 bit CRC signature calculations	111
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	25
Figure 4 – Structure of an FSCP 3/1 safety PDU	26
Figure 5 – Safe communication modes	27
Figure 6 – Standard CPF 3 transmission system	29
Figure 7 – Safety layer architecture	30
Figure 8 – Basic communication layers	30
Figure 9 – Multiport switch bus structure	31
Figure 10 – Linear bus structure	31
Figure 11 – Crossing network borders with routers	32
Figure 12 – Complete safety transmission paths	32
Figure 13 – Device model	33
Figure 14 – Application relationships of a modular device	34
Figure 15 – Application and communication relationships (AR/CR)	34
Figure 16 – Message format	35
Figure 17 – FSCP 3/1 communication structure	37
Figure 18 – F user interface of F-Host driver instances	37
Figure 19 – F-Device driver interfaces	39
Figure 20 – Safety PDU for CPF 3	42
Figure 21 – Status Byte	42
Figure 22 – Control Byte	43
Figure 23 – The Toggle Bit function	44
Figure 24 – F-Device consecutive Number	44
Figure 25 – CRC2 generation (F-Host output)	45
Figure 26 – Details of the CRC2 calculation (reverse order)	46
Figure 27 – Safety layer communication relationship	46
Figure 28 – F-Host state diagram	47
Figure 29 – F-Device state diagram	51
Figure 30 – Interaction F-Host / F-Device during start-up	54
Figure 31 – Interaction F-Host / F-Device during F-Host power off → on	55
Figure 32 – Interaction F-Host / F-Device with delayed power on	56
Figure 33 – Interaction F-Host / F-Device during power off → on	57
Figure 34 – Interaction F-Host / F-Device while host recognizes CRC error	58
Figure 35 – Interaction F-Host / F-Device while device recognizes CRC error	59
Figure 36 – Impact of the counter reset signal	60
Figure 37 – Monitoring the message transit time F-Host ↔ F-Output	61

Figure 38 – Monitoring the message transit time F-Input ↔ F-Host	61
Figure 39 – F-Parameter data and CRC	64
Figure 40 – iParameter assignment deblocking by the F-Host	67
Figure 41 – F_Prm_Flag1	68
Figure 42 – F_Check_SeqNr	68
Figure 43 – F_Check_iPar	69
Figure 44 – F_SIL	69
Figure 45 – F_CRC_Length	69
Figure 46 – F_Prm_Flag2	70
Figure 47 – F_Block_ID	70
Figure 48 – F_Par_Version	70
Figure 49 – F-Parameter	71
Figure 50 – iParameter block	72
Figure 51 – F-Parameter extension within the GSDML specification	74
Figure 52 – CRC1 including iPar_CRC	75
Figure 53 – Algorithm to build CRC0	75
Figure 54 – Dataltem section for F_IN_OUT_1	77
Figure 55 – Dataltem section for F_IN_OUT_2	78
Figure 56 – Dataltem section for F_IN_OUT_5	78
Figure 57 – Dataltem section for F_IN_OUT_6	79
Figure 58 – F-Channel driver as "glue" between F-Device and user program	79
Figure 59 – Layout example of an F-Channel driver	80
Figure 60 – F-Parameter assignment for simple F-Devices and F-Slaves	81
Figure 61 – F and iParameter assignment for complex F-Devices	82
Figure 62 – System integration of CP-J-Tools	84
Figure 63 – iPar-Server mechanism (commissioning)	84
Figure 64 – iPar-Server mechanism (for example F-Device replacement)	85
Figure 65 – iPar-Server request coding ("status model")	86
Figure 66 – Coding of S... Type	87
Figure 67 – iPar-Server request coding ("alarm model")	88
Figure 68 – iPar-Server state diagram	90
Figure 69 – Example safety function with a critical response time path	93
Figure 70 – Simplified typical response time model	94
Figure 71 – Frequency distributions of typical response times of the model	94
Figure 72 – Context of delay times and watchdog times	95
Figure 73 – Timing sections forming the FSCP 3/1 F_WD_Time	96
Figure 74 – Frequency distribution of response times with message retries	97
Figure 75 – Retries with CP 3/1	98
Figure 76 – Retries with CP 3/RTE	98
Figure 77 – Residual error probabilities for the 24-bit polynomial	99
Figure 78 – Properness of the 32-bit polynomial for 52 octets	100
Figure 79 – Properness of the 32-bit polynomial for 132 octets	100
Figure 80 – Monitoring of corrupted messages	101

Figure 81 – Security for WLAN networks..... 104

Figure 82 – Security for Bluetooth networks..... 105

Figure A.83 – Typical "C" procedure of a cyclic redundancy check..... 109

Figure A.84 – Comparison of the response time model and a real application 112

Figure A.85 – Frequency distribution of measured response times..... 113

Figure A.86 – F-Host with standard and safety-related application programs 114

Currently in preview, click buy full version

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 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.

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:

EP 0672270-A2	[SI]	Verfahren zur Datenübertragung in einem Rechnersystem
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

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 A&D AS FA TC 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.

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.

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

FDIS	Report on voting
65C/470/FDIS	65C/481/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.

The committee has decided that the contents of this publication will remain unchanged until the maintenance result date indicated on the IEC web site under "<http://www.pre.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.

The list of all parts of the IEC 61784-3 series, under the general title *Industrial communication networks – Profiles – Functional safety fieldbuses*, can be found on the IEC website.

INTRODUCTION

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.

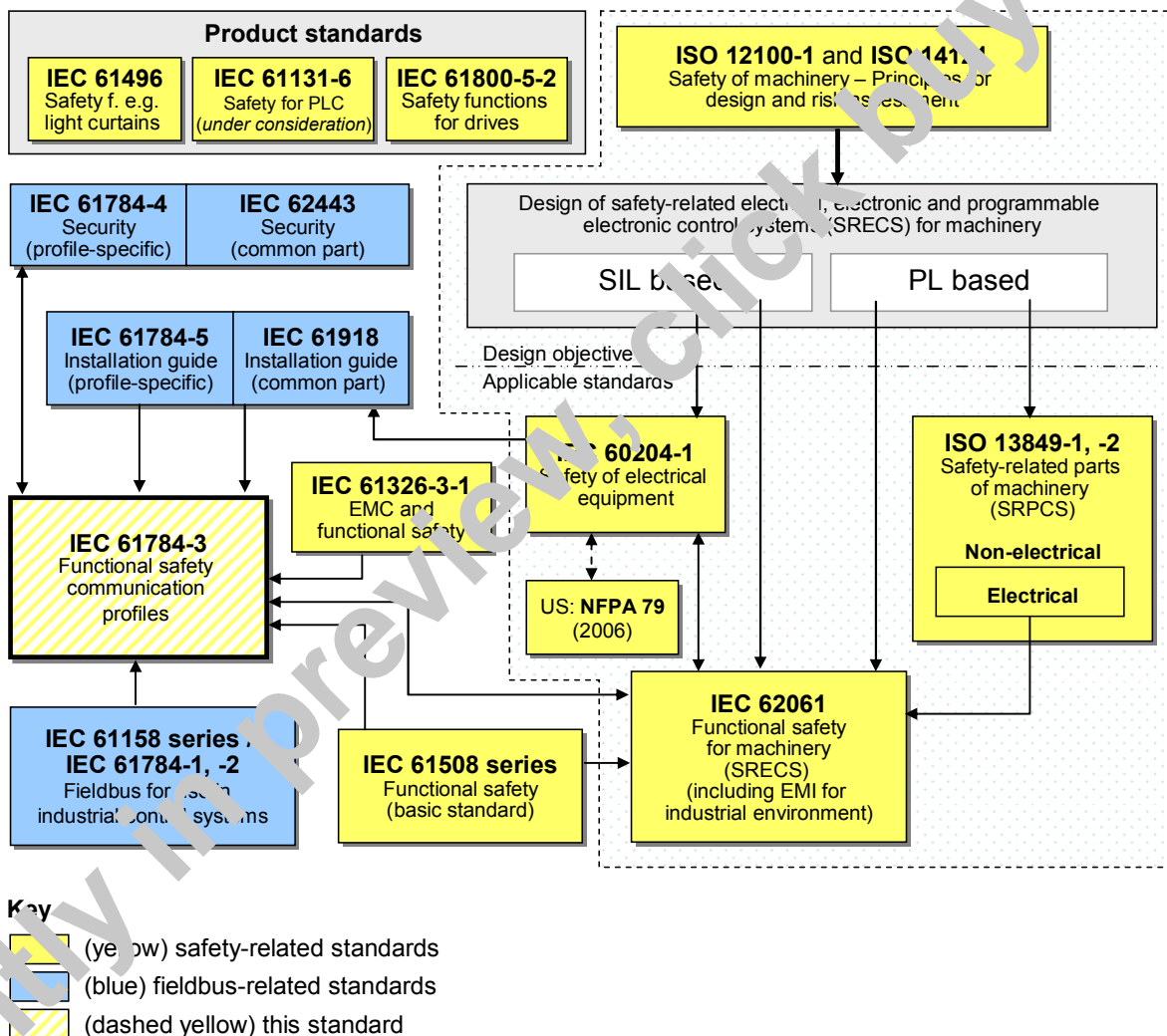
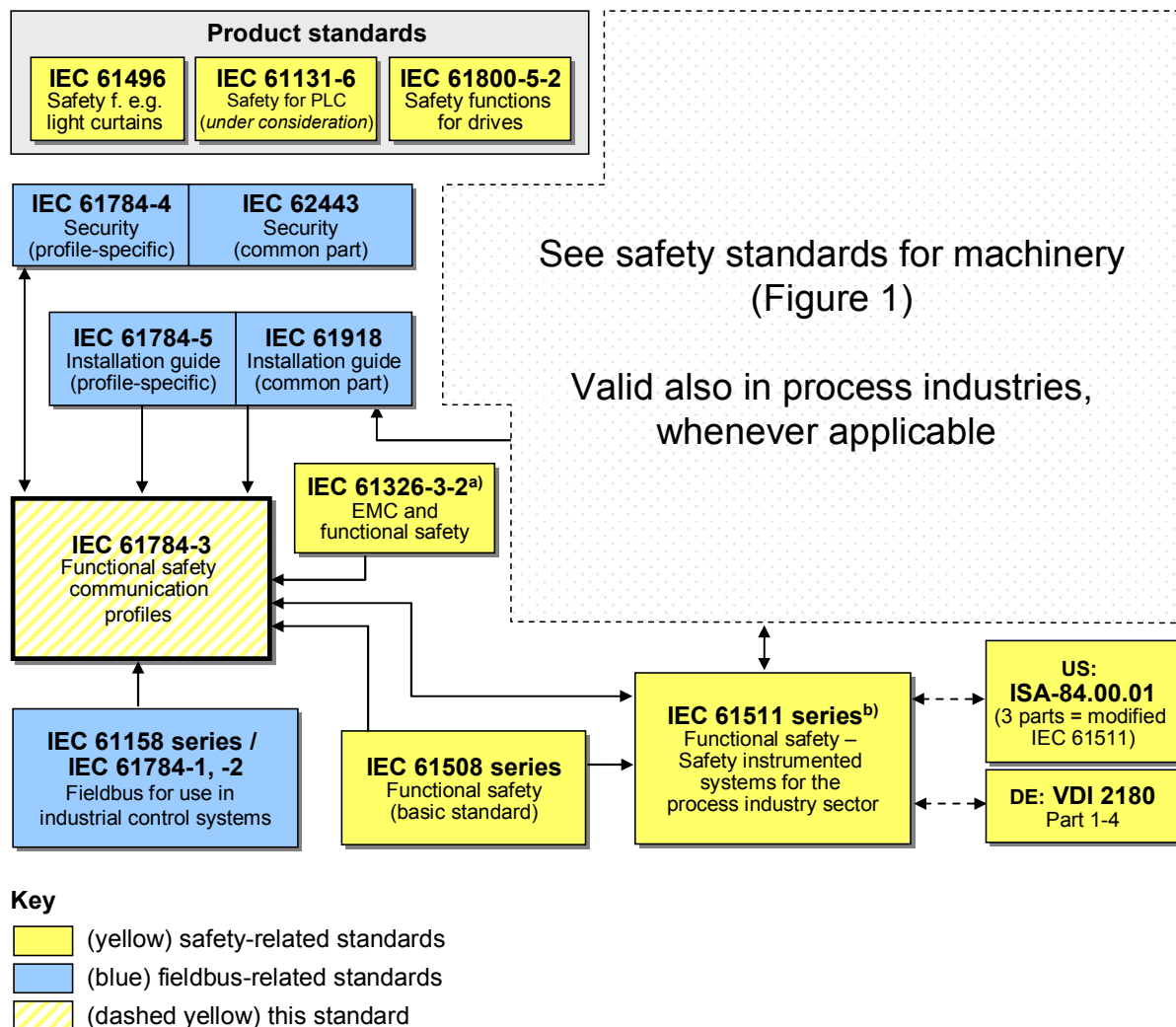


Figure 1 – Relationships of IEC 61784-3 with other standards (machinery)

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.

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES

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

1 Scope

This part of the IEC 61784-3 series specifies a safety communication layer (services and protocol) based on CPF 3 of IEC 61784-1, IEC 61784-2 (CP 3/1, CP 3/2, CP 3/4, CP 3/5 and CP 3/6) and IEC 61158 Types 3 and 10. 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 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 61010-1, *Safety requirements for electrical equipment for measurement, control, and laboratory use – Part 1: General requirements*

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

IEC 61131-3, *Programmable controllers – Part 3: Programming languages*

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

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

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

IEC 61158-4-3, *Industrial communication networks – Fieldbus specifications – Part 4-3: Data-link layer protocol specification*

IEC 61158-5-3, *Industrial communication networks – Fieldbus specifications – Part 5-3: Application layer service definition*

¹ In the following pages of this standard, “this part” will be used for “this part of the IEC 61784-3 series”.

IEC 61158-5-10, *Industrial communication networks – Fieldbus specifications – Part 5-10: Application layer service definition*

IEC 61158-6-3, *Industrial communication networks – Fieldbus specifications – Part 4-3: Application layer protocol specification*

IEC 61158-6-10, *Industrial communication networks – Fieldbus specifications – Part 4-10: Application layer protocol specification*

IEC 61326-3-1, *Electrical equipment for measurement, control and laboratory use – EMC requirements – Part 3-1: Immunity requirements for safety-related systems and for equipment intended to perform safety related functions (functional safety) – General industrial applications²*

IEC 61326-3-2, *Electrical equipment for measurement, control and laboratory use – EMC requirements – Part 3-2: Immunity requirements for safety-related systems and for equipment intended to perform safety related functions (functional safety) – Industrial applications with specified EM environment²*

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

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

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

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 61784-5-3, *Industrial communication networks – Profiles – Part 5: Installation of fieldbuses – Installation profiles for CPF 3*

IEC 61918, *Industrial communication networks – Installation of communication networks in industrial premises*

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

IEC 62280-1:2002, *Railway applications – Communication, signalling and processing systems – Part 1: Safety-related communication in closed transmission systems*

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

IEC/TR 62390, *Common automation device – Profile guideline*

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

² To be published.

ISO 15745-3, *Industrial automation systems and integration – Open systems application integration framework – Part 3: Reference description for IEC 61158-based control systems*

ISO 15745-4, *Industrial automation systems and integration – Open systems application integration framework – Part 4: Reference description for Ethernet-based control systems – Amendment 1: PROFINET profiles*