



IEC 61784-3-2

Edition 1.0 2007-12

INTERNATIONAL STANDARD

**Industrial communication networks – Profiles –
Part 3-2: Functional safety fieldbuses – Additional specifications for CPF 2**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

PRICE CODE **XK**

ICS 35.100.05 25.040.40

ISBN 2-8318-9399-2

CONTENTS

FOREWORD.....	11
INTRODUCTION.....	13
1 Scope.....	17
2 Normative references	17
3 Terms, definitions, symbols, abbreviated terms and conventions	18
3.1 Terms and definitions	18
3.1.1 Common terms and definitions	18
3.1.2 CPF 2: Additional terms and definitions	22
3.2 Symbols and abbreviated terms.....	23
3.2.1 Common symbols and abbreviated terms	23
3.2.2 CPF 2: Additional symbols and abbreviated terms	23
3.3 Conventions	24
4 Overview of FSCP 2/1 (CIP Safety™).....	24
4.1 General.....	24
4.2 FSCP 2/1	24
5 General	25
5.1 External documents providing specifications for the profile.....	25
5.2 Safety functional requirements	26
5.3 Safety measures	26
5.4 Safety communication layer structure	27
5.5 Relationships with FAL (and DLL, PhL)	27
5.5.1 General	27
5.5.2 Data types.....	27
6 Safety communication layer services	28
6.1 Introduction	28
6.2 Connection object	28
6.2.1 General	28
6.2.2 Class attribute extensions	28
6.2.3 Service extensions	29
6.2.4 Explicit message response format for SafetyOpen and SafetyClose	29
6.3 Connection Manager object.....	30
6.3.1 General	30
6.3.2 ForwardOpen for safety	30
6.3.3 Safety network segment	32
6.3.4 Originator rules for calculating the connection parameter CRC	34
6.3.5 SafetyOpen processing flowcharts.....	34
6.3.6 Checks required by Multipoint producers with existing connections	37
6.3.7 Electronic key usage for safety	37
6.3.8 RPI vs. API in safety connections	37
6.3.9 Application path construction for safety	37
6.3.10 Safety Validator connection types.....	39
6.3.11 Application reply data in a successful SafetyOpen response.....	40
6.3.12 Unsuccessful SafetyOpen response	41
6.3.13 ForwardClose for safety.....	44
6.4 Identity object.....	44
6.4.1 General	44

6.4.2	Changes to common services	44
6.5	Link objects	45
6.5.1	DeviceNet object changes	45
6.5.2	TCP/IP Interface object changes	45
6.6	Safety Supervisor object.....	46
6.6.1	General	46
6.6.2	Safety Supervisor class attributes.....	46
6.6.3	Subclasses	47
6.6.4	Safety Supervisor instance attributes.....	47
6.6.5	Semantics	50
6.6.6	Subclasses.....	56
6.6.7	Safety Supervisor common services	56
6.6.8	Safety Supervisor behavior.....	67
6.7	Safety Validator object	74
6.7.1	General	74
6.7.2	Class attributes	74
6.7.3	Instance attributes	75
6.7.4	Class services	81
6.7.5	Instance services.....	81
6.7.6	Object behavior	82
6.8	Connection Configuration Object	85
6.8.1	General	85
6.8.2	Class attribute extensions	85
6.8.3	Instance attributes, additions and extensions.	85
6.8.4	Instance attribute semantics extensions or restrictions for safety.....	87
6.8.5	Special Safety Related Parameters – (Attribute 13)	92
6.8.6	Object-specific services.....	96
6.8.7	Common service extensions for safety.....	96
6.8.8	Object behavior	98
7	Safety communication layer protocol	99
7.1	Safety PDU format	99
7.1.1	Safety PDU encoding	99
7.1.2	Safety CRC	109
7.2	Communication protocol behavior.....	110
7.2.1	Sequence of safety checks	110
7.2.2	Connection termination.....	110
7.2.3	Cross checking error	111
7.3	Time stamp operation.....	111
7.4	Protocol sequence diagrams	112
7.4.1	General	112
7.4.2	Normal safety transmission.....	112
7.4.3	Lost, corrupted and delayed message transmission.....	113
7.4.4	Lost, corrupted or delayed message transmission with production repeated.....	116
7.4.5	Point-to-point ping	118
7.4.6	Multipoint ping on CP 2/3 Safety.....	119
7.4.7	Multipoint ping on CP 2/2 safety networks	120
7.4.8	Multipoint ping – retry with success	121
7.4.9	Multipoint ping – retry with timeout	122

7.5	Safety protocol definition	123
7.5.1	General	123
7.5.2	High level view of a safety device	123
7.5.3	Safety Validator object	124
7.5.4	Relationship between SafetyValidatorServer and SafetyValidatorClient	124
7.5.5	SafetyValidatorClient function definition	125
7.5.6	SafetyValidatorServer function definition	133
7.6	Safety message and protocol data specifications	143
7.6.1	Mode octet	143
7.6.2	Time Stamp Section	144
7.6.3	Time Coordination Message	144
7.6.4	Time correction message	145
7.6.5	Safety data production	145
7.6.6	Producer dynamic variables	152
7.6.7	Producer per consumer dynamic variables	154
7.6.8	Consumer data variables	156
7.6.9	Consumer input static variables	158
7.6.10	Consumer dynamic variables	158
8	Safety communication layer management	160
8.1	Overview	160
8.2	Definition of the measures used during connection establishment	161
8.3	Originator-Target relationship validation	164
8.4	Detection of mis-routed connection requests	165
8.5	SafetyOpen processing	165
8.6	Ownership management	166
8.7	Bridging different physical layers	167
8.8	Safety connection establishment	168
8.8.1	Overview	168
8.8.2	Basic facts for connection establishment	168
8.8.3	Configuring safety connections	169
8.8.4	Network time expectation multiplier	170
8.8.5	Establishing connections	172
8.8.6	Recommendations for consumer number allocation	174
8.8.7	Recommendations for connection establishment	175
8.8.8	Ownership establishment	175
8.8.9	Ownership use cases	176
8.8.10	PID/CID usage and establishment	179
8.8.11	Proper PID/CID usage in multipoint and point-to-point connections	179
8.8.12	Network supported services	181
8.8.13	FSCP 2/1 Safety device type	182
8.9	Safety configuration process	186
8.9.1	Introduction to safety configuration	186
8.9.2	Configuration goals	186
8.9.3	Configuration overview	187
8.9.4	User configuration guidelines	188
8.9.5	Configuration process SIL3 justification	189
8.9.6	Device functions for tool configuration	190
8.9.7	Password security	190

8.9.8	SNCT interface services	190
8.9.9	Configuration lock.....	190
8.9.10	Effect of configuration lock on device behavior	191
8.9.11	Configuration ownership	192
8.9.12	Configuration mode	192
8.9.13	Measures used to ensure integrity of configuration process	192
8.9.14	Download process	194
8.9.15	Verification process	197
8.9.16	Verification process	200
8.9.17	Configuration error analysis.....	201
8.10	Electronic Data Sheets extensions for safety.....	204
8.10.1	General rules for EDS based safety devices	204
8.10.2	EDS extensions for safety	205
9	System requirements.....	209
9.1	Indicators and switches	209
9.1.1	General indicator requirements.....	209
9.1.2	LED indications for setting the device UNID.....	209
9.1.3	Module Status LED.....	210
9.1.4	Indicator warning	210
9.1.5	Network Status LED	210
9.1.6	MACID determination	212
9.1.7	Reset switch.....	213
9.2	Installation guidelines.....	214
9.3	Safety function response time	214
9.3.1	Overview	214
9.3.2	Network time expectation	214
9.3.3	Equations for calculating network reaction times	215
9.4	Duration of demands	217
9.5	Constraints for calculation of system characteristics.....	217
9.5.1	Number of nodes	217
9.5.2	Network PFH.....	217
9.5.3	Bit Error Rate (BER).....	219
9.6	Maintenance.....	220
9.7	Safety manual	220
10	Certification.....	220
Annex A (informative) Additional information for functional safety communication profiles of CPF 2		221
A.1	Hash function example code.....	221
Bibliography.....		233
Table 1 – Communications errors and detection measures matrix.....		26
Table 2 – New class attributes		28
Table 3 – Service extensions		29
Table 4 – SafetyOpen and SafetyClose response format		29
Table 5 – Safety network segment identifier.....		32
Table 6 – Safety network segment definition.....		32
Table 7 – Safety network segment router format.....		34

Table 8 – Multipoint producer parameter evaluation rules	37
Table 9 – ForwardOpen setting options for safety connections.....	39
Table 10 – Network connection parameters for safety connections	40
Table 11 – CP 2/3 Safety target application reply (size: 10 octets).....	41
Table 12 – SafetyOpen target application reply (size: 16 octets).....	41
Table 13 – New and extended error codes for safety	42
Table 14 – SafetyOpen error event guidance table.....	43
Table 15 – Identity object common service changes	44
Table 16 – New DeviceNet object instance attribute	45
Table 17 – New TCP/IP Interface object Instance Attribute	45
Table 18 – Safety Supervisor class attributes	46
Table 19 – Safety Supervisor instance attributes	47
Table 20 – Device status attribute state values	51
Table 21 – Exception status attribute format	51
Table 22 – Common exception detail attribute values	52
Table 23 – Exception detail format summary.....	53
Table 24 – Summary of device behavior for various CFUNID values	55
Table 25 – Safety Supervisor common services	57
Table 26 – Safety Supervisor object specific services	57
Table 27 – Configure_Request message structure	59
Table 28 – Validate_Configuration message structure.....	59
Table 29 – Validate_Configuration success message structure	59
Table 30 – Validate_Configuration error code	60
Table 31 – Validate_Configuration extended codes.....	60
Table 32 – Set_Password message structure.....	62
Table 33 – Reset_Password message structure.....	62
Table 34 – Configuration_Lock/Unlock message structure	63
Table 35 – Mode_Change message structure	63
Table 36 – Safety_Reset message structure	64
Table 37 – Safety Supervisor safety reset types	64
Table 38 – Attribute bit map parameter	64
Table 39 – Reset processing rules for rest types.....	65
Table 40 – Propose_TUNID service	65
Table 41 – Apply_TUNID service	66
Table 42 – Safety Supervisor events.....	68
Table 43 – State event matrix for Safety Supervisor.....	69
Table 44 – Configuration owner control vs. device state.....	72
Table 45 – State mapping of Safety Supervisor to Identity object.....	73
Table 46 – Safety Supervisor object event mapping.....	73
Table 47 – Identity object event mapping.....	74
Table 48 – Safety Validator class attributes	75
Table 49 – Safety Validator instance attributes	75
Table 50 – Safety Validator state assignments.....	78

Table 51 – Safety Validator type, bit field assignments	78
Table 52 – Multipoint producer SafetyOpen parameter evaluation rules	80
Table 53 – Safety Validator class services	81
Table 54 – Safety Validator instance services	81
Table 55 – Safety Validator Get_Attributes_All service data	82
Table 56 – Safety Validator state event matrix	84
Table 57 – State mapping between Safety Supervisor and Safety Validator objects	85
Table 58 – Connection configuration object class attribute extensions	85
Table 59 – Connection Configuration Object instance attribute additions/extensions	86
Table 60 – Connection flag bit definitions	88
Table 61 – O-to-T connection parameters	89
Table 62 – T-to-O connection parameters	90
Table 63 – Data map formats	91
Table 64 – Data map format 0	92
Table 65 – Data map format 1	92
Table 66 – Target device's SCCRC values	94
Table 67 – Target device's SCTS values	95
Table 68 – Time correction connection parameters for multipoint connection	95
Table 69 – Connection Configuration Object-specific services	96
Table 70 – Get_Attributes_All Response service data (added attributes)	97
Table 71 – Set_Attributes_All Request service data (added attributes)	97
Table 72 – State Mapping between Safety Supervisor and the CCO objects	98
Table 73 – Connection sections and PDU formats	100
Table 74 – Mode octet variables	101
Table 75 – Time Stamp variables	103
Table 76 – Time Coordination message variables	104
Table 77 – Time Correction Message variables	106
Table 78 – CRC polynomials used	109
Table 79 – Connection sections and message formats	110
Table 80 – Data reception - Link triggered	135
Table 81 – Time_Correction reception - Link triggered	136
Table 82 – Data reception - Application triggered	136
Table 83 – Time_Correction reception - Application triggered	136
Table 84 – Consuming application – Safety data monitoring	137
Table 85 – Producer connection status determination	146
Table 86 – Consuming safety connection status	156
Table 87 – Connection establishment errors and measures to detect errors	161
Table 88 – SNN Date/Time allocations	162
Table 89 – SNN legal range of time values	162
Table 90 – Safety connection parameters	170
Table 91 – SafetyOpen summary	172
Table 92 – Originator/Target service mapping	183
Table 93 – Unsupported originator/target service types	183

Table 94 – Configuration goals	187
Table 95 – Configuration owner control vs. device state.....	192
Table 96 – Errors and detection measures	201
Table 97 – Parameter class keywords.....	206
Table 98 – New Connection Manager section keywords for safety	206
Table 99 – Connection Manager field usage for safety	207
Table 100 – Connection parameter field settings for safety	208
Table 101 – LED indications for setting UNID	209
Table 102 – Module Status LED.....	210
Table 103 – Network status LED states	211
Table 104 – Connection reaction time type – producing/consuming applications	215
Figure 1 – Relationships of IEC 61784-3 with other standards (machinery)	13
Figure 2 – Relationships of IEC 61784-3 with other standards (process).....	14
Figure 3 – Relationship of Safety Validators	25
Figure 4 – Communication layers.....	27
Figure 5 – ForwardOpen with safety network segment	31
Figure 6 – Safety network target format	33
Figure 7 – Target Processing SafetyOpen with no configuration data (Form 2 SafetyOpen)	35
Figure 8 – Target Processing for SafetyOpen with configuration data (Form 1 SafetyOpen)	36
Figure 9 – Applying device configuration.....	60
Figure 10 – Configure and Validate processing flowcharts	61
Figure 11 – UNID handling during “Waiting for TUNID”	67
Figure 12 – Safety Supervisor state diagram.....	68
Figure 13 – Configuration, testing and locked relationships.....	72
Figure 14 – Safety connection types	79
Figure 15 – Safety Validator state transition diagram	83
Figure 16 – Connection Configuration Object state diagram.....	98
Figure 17 – Connection Configuration Object data flow.....	99
Figure 18 – Format of the mode octet	100
Figure 19 – 1 or 2 octet data section.....	101
Figure 20 – 3 to 250 octet data section format	102
Figure 21 – Time Stamp section format.....	103
Figure 22 – Time Coordination message encoding.....	104
Figure 23 – Time Correction message encoding	105
Figure 24 – 1 or 2 octet point-to-point PDU encoding.....	107
Figure 25 – 1 or 2 Octet multipoint PDU encoding.....	107
Figure 26 – 1 or 2 Octet, multipoint, Format 2 safety connection format.....	108
Figure 27 – 3 to 250 Octet Point-to-point PDU encoding	108
Figure 28 – 3 to 248 Octet Multipoint PDU encoding	108
Figure 29 – 3 to 248 Octet, Multipoint, safety connection format	109

Figure 30 – Time stamp sequence	111
Figure 31 – Sequence diagram of a normal producer/consumer safety sequence.....	112
Figure 32 – Sequence diagram of a normal producer/consumer safety sequence (production repeated)	113
Figure 33 – Sequence diagram of a corrupted producer to consumer message	114
Figure 34 – Sequence diagram of a lost producer to consumer message	115
Figure 35 – Sequence diagram of a delayed message	116
Figure 36 – Sequence diagram of a corrupted producer to consumer message with production repeated	117
Figure 37 – Sequence diagram of a connection terminated due to delays	118
Figure 38 – Sequence diagram of a failure of safety CRC check	118
Figure 39 – Sequence diagram of a point-to-point ping - normal response	119
Figure 40 – Sequence diagram of a successful multipoint ping, CP 2/3 safety	120
Figure 41 – Sequence diagram of a successful multipoint ping, CP 2/2 safety	121
Figure 42 – Sequence diagram of a multipoint ping retry.....	122
Figure 43 – Sequence diagram of a multipoint ping timeout	122
Figure 44 – Safety device reference model entity relation diagram.....	123
Figure 45 – Two devices interchanging safety data via a SafetyValidatorClient and a SafetyValidatorServer	124
Figure 46 – Safety production data flow	125
Figure 47 – Consumer safety data monitoring	134
Figure 48 – SafetyValidatorServer - application triggered	134
Figure 49 – Target ownership	165
Figure 50 – SafetyOpen forms	166
Figure 51 – Connection ownership state chart	166
Figure 52 – SafetyOpen UNID mapping	167
Figure 53 – Common CPF 2 application layer	167
Figure 54 – End-to-End routing example	168
Figure 55 – Sources for safety related connection parameters	171
Figure 56 – Parameter mapping between originator and target	171
Figure 57 – CP 2/3 Safety connection establishment in targets for Form 2a SafetyOpen.....	173
Figure 58 – General sequence to detect configuration is required	174
Figure 59 – PID/CID exchanges for two originator scenarios.....	179
Figure 60 – Seed generation for multipoint connections	180
Figure 61 – PID/CID runtime handling.....	181
Figure 62 – Connection categories and supported services.....	184
Figure 63 – Recommended connection types.....	185
Figure 64 – Logic-to-logic supported services	185
Figure 65 – Recommended connection types for logic to logic	186
Figure 66 – Configuration data transfers	187
Figure 67 – Protection measures in safety devices	189
Figure 68 – Configuration, testing and locked relationships.....	191
Figure 69 – Originator's configuration data	193
Figure 70 – SNCT to device download process	195

Figure 71 – SNCT Downloads to originators that perform Form 1 configuration..... 196

Figure 72 – Protection from locking and ownership 198

Figure 73 – Example of read back and comparison of original and printout 199

Figure 74 – Diverse display without full data read back..... 200

Figure 75 – Verification process including all alternatives 200

Figure 76 – Safety device MACID processing logic 213

Figure 77 – Safety function response time 214

Figure 78 – Safety function response time components 216

Figure 79 – Network protocol reliability block diagram (RBD) 217

Figure 80 – Network PFH summary..... 219

INTERNATIONAL ELECTROTECHNICAL COMMISSION

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES

**Part 3-2: Functional safety fieldbuses – Additional specifications
for CPF 2**

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 2 as follows, where the [xx] notation indicates the holder of the patent right:

US 6,631,476	[RA]	Safety network for industrial controller providing redundant connections on single media
US 6,701,198	[RA]	Safety network for industrial controller allowing initialization on standard networks
US 6,721,900	[RA]	Safety network for industrial controller having reduced bandwidth requirements
US 6,891,850	[RA]	Network independent safety protocol for industrial controller
US 6,915,444	[RA]	Network independent safety protocol for industrial controller using data manipulation techniques

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:

[RA] Rockwell Automation, Inc.
1201 S. Second Street
Milwaukee, WI 53204
USA
Attention: Intellectual Propert Dept.

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 61784-3-2 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://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.

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.

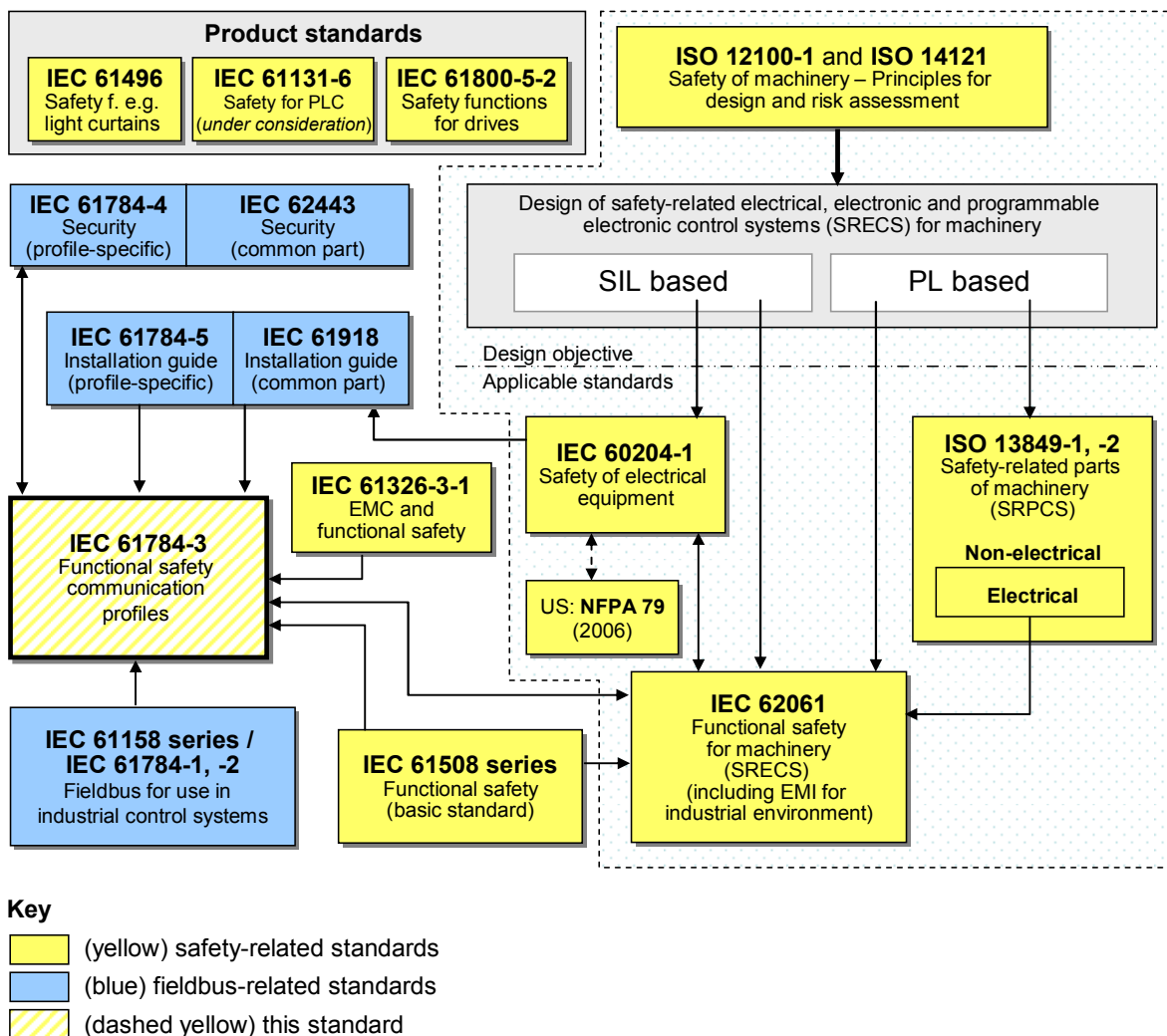
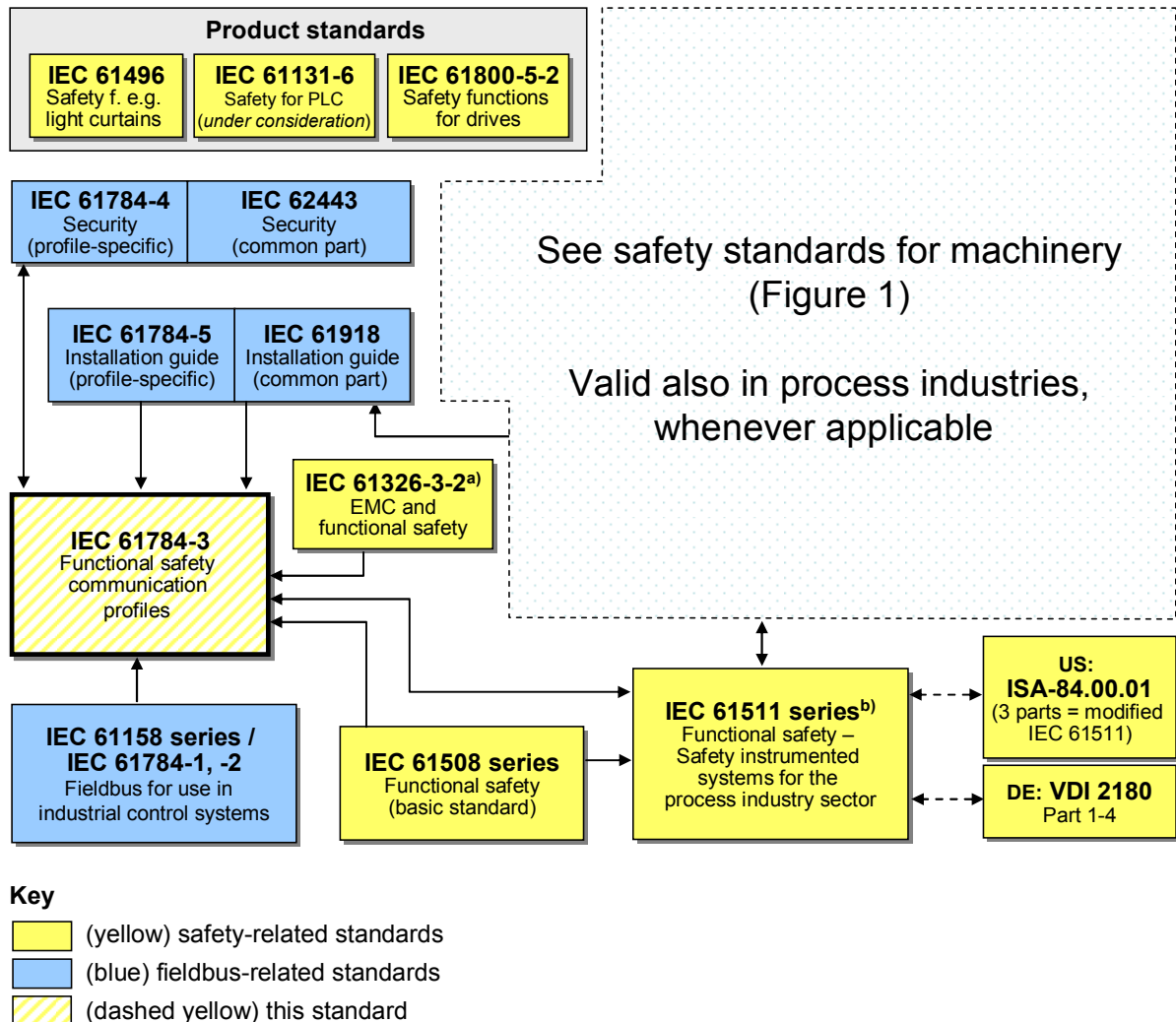


Figure 1 – Relationships of IEC 61784-3 with other standards (machinery)

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 3-2: Functional safety fieldbuses – Additional specifications for CPF 2

1 Scope

This part of the IEC 61784-3 series specifies a safety communication layer (services and protocol) based on CPF 2 of IEC 61784-1, IEC 61784-2 and IEC 61158 Type 2. 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 series 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 61131-3, *Programmable controllers – Part 3: Programming languages*

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

IEC 61158-3-2, *Industrial communication networks – Fieldbus specifications – Part 3-2: Data-link layer service definition*

IEC 61158-4-2, *Industrial communication networks – Fieldbus specifications – Part 4-2: Data-link layer protocol specification*

IEC 61158-5-2, *Industrial communication networks – Fieldbus specifications – Part 5-2: Application layer service definition*

IEC 61158-6-2, *Industrial communication networks – Fieldbus specifications – Part 6-2: Application layer protocol specification*

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

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 applications*²

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 environment*²

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

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 61784-5-2, *Industrial communication networks – Profiles – Part 5: Installation of fieldbuses – Installation profiles for CPF 2*

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

IEC 62026-3, *Low-voltage switchgear and controlgear – Controller-device interfaces (CDIs) – Part 3: DeviceNet*

ISO 15745-2, *Industrial automation systems and integration – Open systems application integration framework – Part 2: Reference description for ISO 11898-based control systems*

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*

² To be published.