

INTERNATIONAL STANDARD

NORME INTERNATIONALE



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

**Réseaux de communication industriels – Profils –
Partie 3-2: Bus de terrain de sécurité fonctionnelle – Spécifications
supplémentaires pour CPF 2**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 25.040.40; 35.100.05

ISBN 978-2-8322-9747-6

Warning! Make sure that you obtained this publication from an authorized distributor. Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.
--

CONTENTS

FOREWORD	12
0 Introduction	14
0.1 General.....	14
0.2 Patent declaration	15
1 Scope	17
2 Normative references	17
3 Terms, definitions, symbols, abbreviated terms and conventions	19
3.1 Terms and definitions.....	19
3.1.1 Common terms and definitions.....	19
3.1.2 CPF 2: Additional terms and definitions	24
3.2 Symbols and abbreviated terms	25
3.2.1 Common symbols and abbreviated terms.....	25
3.2.2 CPF 2: Additional symbols and abbreviated terms	26
3.3 Conventions.....	27
4 Overview of FSCP 2/1 (CIP Safety™)	27
4.1 General.....	27
4.2 FSCP 2/1	27
5 General	28
5.1 External documents providing specifications for the profile	28
5.2 Safety functional requirements	29
5.3 Safety measures	29
5.4 Safety communication layer structure.....	30
5.5 Relationships with FAL (and DLL, PhL)	30
5.5.1 General	30
5.5.2 Data types	30
6 Safety communication layer services	31
6.1 General.....	31
6.2 Connection object	31
6.2.1 General	31
6.2.2 Class attribute extensions.....	31
6.2.3 Service extensions	32
6.2.4 Explicit message response format for SafetyOpen and SafetyClose.....	32
6.3 Connection Manager object.....	33
6.3.1 General	33
6.3.2 ForwardOpen for safety	33
6.3.3 Safety network segment	35
6.3.4 Originator rules for calculating the connection parameter CRC	38
6.3.5 SafetyOpen processing flowcharts	38
6.3.6 Checks required by Multipoint producers with existing connections.....	41
6.3.7 Electronic key usage for safety	42
6.3.8 RPI vs. API in safety connections	42
6.3.9 Application path construction rules for safety connections	42
6.3.10 Safety Validator connection types	44
6.3.11 Application reply data in a successful SafetyOpen response.....	48
6.3.12 Unsuccessful SafetyOpen response.....	50
6.3.13 ForwardClose for safety.....	52

6.4	Identity object	52
6.4.1	General	52
6.4.2	Changes to common services	53
6.4.3	Extensions for CP 16/3 devices	53
6.5	Link objects	53
6.5.1	DeviceNet object changes	53
6.5.2	TCP/IP Interface object changes.....	54
6.5.3	SERCOS III Link object.....	54
6.6	Safety Supervisor object	56
6.6.1	General	56
6.6.2	Safety Supervisor class attributes.....	56
6.6.3	Subclasses	57
6.6.4	Safety Supervisor instance attributes.....	57
6.6.5	Semantics.....	61
6.6.6	Subclasses	67
6.6.7	Safety Supervisor common services	68
6.6.8	Safety Supervisor behavior	80
6.7	Safety Validator object	87
6.7.1	General	87
6.7.2	Class attributes	87
6.7.3	Instance attributes	88
6.7.4	Class services	94
6.7.5	Instance services.....	94
6.7.6	Object behavior	95
6.8	Connection Configuration Object.....	98
6.8.1	General	98
6.8.2	Class attribute extensions.....	98
6.8.3	Instance attributes, additions and extensions.....	98
6.8.4	Instance attribute semantics extensions or restrictions for safety	101
6.8.5	Special Safety Related Parameters – (Attribute 13)	106
6.8.6	Object-specific services	112
6.8.7	Common service extensions for safety	112
6.8.8	Object behavior	114
7	Safety communication layer protocol	115
7.1	Safety PDU format	115
7.1.1	Safety PDU encoding.....	115
7.1.2	Safety CRC	127
7.2	Communication protocol behavior	128
7.2.1	Sequence of safety checks	128
7.2.2	Connection termination	128
7.2.3	Cross checking error.....	129
7.3	Time stamp operation	129
7.4	Rollover counts in the EF	130
7.5	Protocol sequence diagrams	130
7.5.1	General	130
7.5.2	Normal safety transmission.....	130
7.5.3	Lost, corrupted and delayed message transmission	132
7.5.4	Lost, corrupted or delayed message transmission with production repeated	134

7.5.5	Point-to-point ping	136
7.5.6	Multipoint ping on CP 2/3 Safety	137
7.5.7	Multipoint ping on CP 2/2 safety networks	139
7.5.8	Multipoint ping – retry with success	139
7.5.9	Multipoint ping – retry with timeout	140
7.6	Safety protocol definition	141
7.6.1	General	141
7.6.2	High level view of a safety device	141
7.6.3	Safety Validator object.....	142
7.6.4	Relationship between SafetyValidatorServer and SafetyValidatorClient	142
7.6.5	Extended Format time stamp rollover handling	143
7.6.6	SafetyValidatorClient function definition.....	149
7.6.7	SafetyValidatorServer function definition	157
7.7	Safety message and protocol data specifications	170
7.7.1	Mode octet	170
7.7.2	Time Stamp Section	171
7.7.3	Time Coordination Message	171
7.7.4	Time correction message.....	172
7.7.5	Safety data production.....	172
7.7.6	Producer dynamic variables.....	180
7.7.7	Producer per consumer dynamic variables.....	182
7.7.8	Consumer data variables	183
7.7.9	Consumer input static variables	185
7.7.10	Consumer dynamic variables	186
8	Safety communication layer management.....	188
8.1	Overview.....	188
8.2	Definition of the measures used during connection establishment	188
8.3	Originator-Target relationship validation.....	192
8.4	Detection of mis-routed connection requests.....	193
8.5	SafetyOpen processing	193
8.6	Ownership management	193
8.7	Bridging different physical layers	194
8.8	Safety connection establishment.....	196
8.8.1	Overview	196
8.8.2	Basic facts for connection establishment	196
8.8.3	Configuring safety connections	197
8.8.4	Network time expectation multiplier	198
8.8.5	Establishing connections	200
8.8.6	Recommendations for consumer number allocation	203
8.8.7	Recommendations for connection establishment.....	203
8.8.8	Ownership establishment.....	204
8.8.9	Ownership use cases.....	204
8.8.10	PID/CID usage and establishment	207
8.8.11	Proper PID/CID usage in multipoint and point-to-point connections.....	208
8.8.12	Network supported services.....	210
8.8.13	FSCP 2/1 safety device type.....	211
8.9	Safety configuration process	215
8.9.1	Introduction to safety configuration	215
8.9.2	Configuration goals.....	215

8.9.3	Configuration overview	216
8.9.4	User configuration guidelines.....	217
8.9.5	Configuration process justification	218
8.9.6	Device functions for tool configuration	219
8.9.7	Password security	219
8.9.8	SNCT interface services	219
8.9.9	Configuration lock.....	220
8.9.10	Effect of configuration lock on device behavior	220
8.9.11	Configuration ownership	222
8.9.12	Configuration mode	222
8.9.13	Measures used to ensure integrity of configuration process	222
8.9.14	Download process	224
8.9.15	Verification process	227
8.9.16	Configuration error analysis	230
8.10	Electronic Data Sheets extensions for safety	234
8.10.1	General rules for EDS based safety devices	234
8.10.2	EDS extensions for safety.....	235
8.11	Requirements for CP 2/2.....	240
8.11.1	EPI rules for safety messages that travel over CP 2/2	240
8.11.2	Default safety I/O service	240
8.11.3	Duplicate IP detection.....	241
8.11.4	Priority for safety connections.....	241
8.12	Requirements for CP 2/3.....	241
8.12.1	Allocation of CP 2/3 identifiers.....	241
8.12.2	Additional requirements	244
8.13	CP 16/3 requirements	244
8.13.1	General architecture for CPF 2 on CP 16/3.....	244
8.13.2	Baseline FSCP 2/1 on CP 16/3 device	244
8.13.3	Supported objects and services in CP 16/3 devices	245
8.13.4	Transport layer requirements	246
8.13.5	FSCP 2/1 and the CP 16/3 device model	248
8.13.6	UNID assignment on CP 16/3	249
9	System requirements	252
9.1	Indicators and switches.....	252
9.1.1	General indicator requirements.....	252
9.1.2	LED indications for setting the device UNID.....	252
9.1.3	Module Status LED	252
9.1.4	Indicator warning	253
9.1.5	Network Status LED	253
9.1.6	Switches.....	254
9.2	Installation guidelines	256
9.3	Safety function response time	257
9.3.1	Overview	257
9.3.2	Network time expectation.....	257
9.3.3	Equations for calculating network reaction times.....	258
9.4	Duration of demands.....	260
9.5	Constraints for calculation of system characteristics	260
9.5.1	Number of nodes	260
9.5.2	Network PFH of Extended Format.....	260

9.5.3	Bit Error Rate (BER)	261
9.6	Maintenance	262
9.7	Safety manual	262
10	Assessment	262
Annex A (informative) Additional information for functional safety communication profiles of CPF 2		263
A.1	Hash function example code	263
A.2	Void	277
Annex B (informative) Information for assessment of the functional safety communication profiles of CPF 2		278
Bibliography		279
Figure 1	– Relationships of IEC 61784-3 with other standards (machinery)	14
Figure 2	– Relationships of IEC 61784-3 with other standards (process)	15
Figure 3	– Relationship of Safety Validators	28
Figure 4	– Communication layers	30
Figure 5	– ForwardOpen with safety network segment	34
Figure 6	– Safety network target format	36
Figure 7	– Target Processing SafetyOpen with no configuration data (Type 2 SafetyOpen)	39
Figure 8	– Target Processing for SafetyOpen with configuration data (Type 1 SafetyOpen)	40
Figure 9	– Originator logic to determine which format to use	41
Figure 10	– Applying device configuration	72
Figure 11	– Configure and Validate processing flowcharts	73
Figure 12	– UNID handling during "Waiting for TUNID"	79
Figure 13	– Safety Supervisor state diagram	81
Figure 14	– Configuration, testing and locked relationships	85
Figure 15	– Safety connection types	92
Figure 16	– Safety Validator state transition diagram	96
Figure 17	– Logic for Auto-detecting format type	111
Figure 18	– Connection Configuration Object state diagram	114
Figure 19	– Connection Configuration Object data flow	115
Figure 20	– Format of the mode octet	117
Figure 21	– 1 or 2 octet data section, Base Format	117
Figure 22	– 1 or 2 octet data section, Extended Format	118
Figure 23	– 3 to 250 octet data section format, Base Format	118
Figure 24	– 3 to 250 octet data section format, Extended Format	119
Figure 25	– Time Stamp section format, Base Format	120
Figure 26	– BF Time Coordination message encoding	121
Figure 27	– EF Time Coordination message encoding	121
Figure 28	– BF Time Correction message encoding	122
Figure 29	– EF Time Correction message encoding	122
Figure 30	– 1 or 2 octet point-to-point PDU encoding	124
Figure 31	– 1 or 2 Octet multipoint PDU encoding	124

Figure 32 – 1 or 2 Octet, multipoint, Format 2 safety connection format	125
Figure 33 – 3 to 250 Octet Point-to-point PDU encoding	125
Figure 34 – 3 to 248 Octet Multipoint PDU encoding	126
Figure 35 – 3 to 248 Octet, Multipoint, safety connection format	126
Figure 36 – CRC Calculation order for Extended Format messages	127
Figure 37 – Time stamp sequence	129
Figure 38 – Sequence diagram of a normal producer/consumer safety sequence.....	130
Figure 39 – Sequence diagram of a normal producer/consumer safety sequence (production repeated)	131
Figure 40 – Sequence diagram of a corrupted producer to consumer message	132
Figure 41 – Sequence diagram of a lost producer to consumer message	133
Figure 42 – Sequence diagram of a delayed message	134
Figure 43 – Sequence diagram of a corrupted producer to consumer message with production repeated	135
Figure 44 – Sequence diagram of a connection terminated due to delays	135
Figure 45 – Sequence diagram of a failure of safety CRC check	136
Figure 46 – Sequence diagram of a point-to-point ping – normal response	136
Figure 47 – Sequence diagram of a successful multipoint ping, CP 2/3 safety.....	138
Figure 48 – Sequence diagram of a successful multipoint ping, CP 2/2 safety.....	139
Figure 49 – Sequence diagram of a multipoint ping retry.....	140
Figure 50 – Sequence diagram of a multipoint ping timeout	140
Figure 51 – Possible safety architectures for FSCP 2/1.....	141
Figure 52 – Safety device reference model entity relation diagram.....	142
Figure 53 – Two devices interchanging safety data via a SafetyValidatorClient and a SafetyValidatorServer	143
Figure 54 – Point-to-point, originating consumer. target producer	144
Figure 55 – Point-to-point, originator producer, target consumer.....	146
Figure 56 – Multi-point, originator consumer, target producer	147
Figure 57 – Safety production data flow	149
Figure 58 – Consumer safety data monitoring.....	158
Figure 59 – SafetyValidatorServer – application triggered.....	159
Figure 60 – Target ownership	192
Figure 61 – SafetyOpen forms	193
Figure 62 – Connection ownership state chart.....	194
Figure 63 – SafetyOpen UNID mapping	194
Figure 64 – Common CPF 2 application layer	195
Figure 65 – End-to-End routing example	195
Figure 66 – Sources for safety related connection parameters	199
Figure 67 – Parameter mapping between originator and target	200
Figure 68 – CP 2/3 Safety connection establishment in targets for Type 2a SafetyOpen	202
Figure 69 – General sequence to detect configuration is required	202
Figure 70 – PID/CID exchanges for two originator scenarios.....	208
Figure 71 – Seed generation for multipoint connections	209
Figure 72 – PID/CID runtime handling.....	210

Figure 73 – Connection categories and supported services.....	213
Figure 74 – Recommended connection types.....	214
Figure 75 – Logic-to-logic supported services.....	214
Figure 76 – Recommended connection types for logic to logic	215
Figure 77 – Configuration data transfers	216
Figure 78 – Protection measures in safety devices	218
Figure 79 – Configuration, testing and locked relationships.....	221
Figure 80 – Originator's configuration data.....	223
Figure 81 – SNCT to device download process	225
Figure 82 – SNCT Downloads to originators that perform Type 1 configuration	226
Figure 83 – Protection from locking and ownership	228
Figure 84 – Verification process including all alternatives	230
Figure 85 – Baseline FSCP 2/1 on CP 16/3 device.....	245
Figure 86 – FSCP 2/1 Adaptation Layer and SMP interaction.....	247
Figure 87 – FSCP 2/1 Adaptation.....	248
Figure 88 – CP 16/3 device model	249
Figure 89 – Adding a standard module to a modular device	251
Figure 90 – Safety device NodeID processing logic.....	256
Figure 91 – Safety function response time	257
Figure 92 – Safety function response time components	259
Figure 93 – Network protocol reliability block diagram (RBD)	260
Table 1 – Communications errors and detection measures matrix.....	29
Table 2 – New class attributes	31
Table 3 – Service extensions	32
Table 4 – SafetyOpen and SafetyClose response format.....	32
Table 5 – Safety network segment identifier.....	35
Table 6 – Safety network segment definition.....	35
Table 7 – Safety network segment router format	37
Table 8 – Safety Network Segment Extended Format	37
Table 9 – Multipoint producer parameter evaluation rules	42
Table 10 – ForwardOpen setting options for safety connections with object-based application paths.....	45
Table 11 – ForwardOpen setting options for safety connections with ANSI Extended symbol segment application path	47
Table 12 – Network connection parameters for safety connections	48
Table 13 – SafetyOpen target application reply (size: 10 octets)	48
Table 14 – EF CP 2/2 or CP 16/3 SafetyOpen target application reply (size: 14 octets)	49
Table 15 – BF CP 2/3 SafetyOpen target application reply (size: 18 octets)	49
Table 16 – EF CP 2/3 SafetyOpen target application reply (size: 22 octets)	50
Table 17 – New and extended error codes for safety.....	50
Table 18 – SafetyOpen error event guidance table.....	51
Table 19 – Identity object common service changes	53
Table 20 – Identity object extensions for CP 16/3 devices.....	53

Table 21 – New DeviceNet object instance attribute.....	54
Table 22 – New TCP/IP Interface object instance attribute.....	54
Table 23 – SERCOS III Link object class attributes.....	55
Table 24 – SERCOS III Link object instance attributes.....	55
Table 25 – SERCOS III Link Object Common Services	56
Table 26 – Safety Supervisor class attributes	57
Table 27 – Safety Supervisor instance attributes	57
Table 28 – Device status attribute state values	62
Table 29 – Exception status attribute format	62
Table 30 – Common exception detail attribute values	63
Table 31 – Exception detail format summary.....	64
Table 32 – Summary of device behavior for various CFUNID values	66
Table 33 – Safety Supervisor common services	68
Table 34 – Safety Supervisor object specific services	68
Table 35 – Configure_Request message structure	70
Table 36 – Validate_Configuration message structure.....	71
Table 37 – Validate_Configuration success message structure	71
Table 38 – Validate_Configuration error code	71
Table 39 – Validate_Configuration extended codes.....	71
Table 40 – Set_Password message structure.....	74
Table 41 – Reset_Password message structure.....	74
Table 42 – Configuration_Lock/Unlock message structure	75
Table 43 – Mode_Change message structure	75
Table 44 – Safety_Reset message structure	76
Table 45 – Safety Supervisor safety reset types	76
Table 46 – Attribute bit map parameter	76
Table 47 – Reset processing rules for reset types.....	77
Table 48 – Propose_TUNID service	77
Table 49 – Apply_TUNID service	78
Table 50 – Propose_TUNID_List service.....	80
Table 51 – Apply_TUNID_List service.....	80
Table 52 – Safety Supervisor events.....	81
Table 53 – State event matrix for Safety Supervisor.....	82
Table 54 – Configuration owner control vs. device state.....	85
Table 55 – State mapping of Safety Supervisor to Identity object.....	86
Table 56 – Safety Supervisor object event mapping.....	86
Table 57 – Identity object event mapping.....	87
Table 58 – Safety Validator class attributes	88
Table 59 – Safety Validator instance attributes	88
Table 60 – Safety Validator state assignments.....	91
Table 61 – Safety Validator type, bit field assignments	91
Table 62 – Multipoint producer SafetyOpen parameter evaluation rules	93
Table 63 – Safety Validator class services.....	94

Table 64 – Safety Validator instance services	95
Table 65 – Safety Validator Get_Attributes_All service data	95
Table 66 – Safety Validator state event matrix	97
Table 67 – State mapping between Safety Supervisor and Safety Validator objects	98
Table 68 – Connection configuration object class attribute extensions	98
Table 69 – Connection Configuration Object instance attribute additions/extensions	99
Table 70 – Connection flag bit definitions	101
Table 71 – O-to-T connection parameters	103
Table 72 – T-to-O connection parameters	104
Table 73 – Data map formats	105
Table 74 – Data map format 0	106
Table 75 – Data map format 1	106
Table 76 – Target device's SCCRC values	108
Table 77 – Target device's SCTS values	109
Table 78 – Time correction connection parameters for multipoint connection	109
Table 79 – Format Type attribute meaning	110
Table 80 – Format Status attribute meaning	111
Table 81 – Connection Configuration Object-specific services	112
Table 82 – Get_Attributes_All Response service data (added attributes)	112
Table 83 – Get_Attributes_All Response service data (added parameters)	113
Table 84 – Set_Attributes_All Request service data (added attributes)	113
Table 85 – Set_Attributes_All Response service data (added parameters)	114
Table 86 – State Mapping between Safety Supervisor and the CCO objects	114
Table 87 – Connection sections and PDU formats	116
Table 88 – Connection sections and message format	116
Table 89 – Mode octet variables	117
Table 90 – Time Stamp variables	120
Table 91 – Time Coordination message variables	121
Table 92 – Time Correction Message variables	123
Table 93 – CRC polynomials used	127
Table 94 – CRC usage for connection and configuration	128
Table 95 – Data reception – Link triggered	160
Table 96 – Time_Correction reception – Link triggered	160
Table 97 – Data reception – Application triggered	160
Table 98 – Time_Correction reception – Application triggered	161
Table 99 – Consuming application – Safety data monitoring	161
Table 100 – Producer connection status determination	173
Table 101 – Consuming safety connection status	184
Table 102 – Connection establishment errors and measures to detect errors	188
Table 103 – SNN Date/Time allocations	189
Table 104 – SNN legal range of time values	189
Table 105 – Safety connection parameters	198
Table 106 – SafetyOpen summary	201

Table 107 – Originator/Target service mapping	212
Table 108 – Unsupported originator/target service types	212
Table 109 – Configuration goals	216
Table 110 – Configuration owner control vs. device state	221
Table 111 – Errors and detection measures	231
Table 112 – Object Class section keywords	235
Table 113 – Safety Classx entry format	236
Table 114 – Parameter class keywords	236
Table 115 – New Connection Manager section keywords for safety	237
Table 116 – Connection Manager field usage for safety	238
Table 117 – Connection parameter field settings for safety	240
Table 118 – CP 2/3 ID assignment rules	241
Table 119 – LED indications for setting UNID	252
Table 120 – Module Status LED	253
Table 121 – Network status LED states	253
Table 122 – Connection reaction time type – producing/consuming applications	258

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 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.
- 9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

IEC 61784-3-2 has been prepared by subcommittee 65C: Industrial networks, of IEC technical committee 65: Industrial-process measurement, control and automation. It is an International Standard.

This fourth edition cancels and replaces the third edition published in 2016. This edition constitutes a technical revision.

This edition includes the following significant technical changes with respect to the previous edition:

- addition of two new Safety Supervisor object states in 6.6.5.5;
- addition of Net LED behaviour requirement for the proposing TUNID process in 6.6.8, 9.1.2 and 9.1.5;
- addition of application path support for process variables in 6.3.9 and 6.3.10;
- addition of multi-port device support in 6.6.4, 6.6.5, 6.6.7 and miscellaneous places;

- correction of network reaction time equations in 9.3.3;
- addition of SIL support up to SIL 3 in 7.6, 8.7, 8.9, 9.5 and miscellaneous places;
- clean up of configuration procedure guidelines in 8.9.14 and 8.9.15;
- switch change detection in 9.1.6;
- deprecation of base format in 3.1.2, 7.1.1.1 and 6.3.3.2;
- fixing Max_Fault_Number value to 2 in 6.3.3.4, 6.8.3 and 8.8.3;
- updated network PFH calculation in 9.5.2;
- miscellaneous minor corrections made since the last publication.

The text of this International Standard is based on the following documents:

FDIS	Report on voting
65C/1083/FDIS	65C/1087/RVD

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

The language used for the development of this International Standard is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/standardsdev/publications.

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 document will remain unchanged until the stability date indicated on the IEC website under "<http://webstore.iec.ch>" in the data related to the specific document. At this date, the document 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.

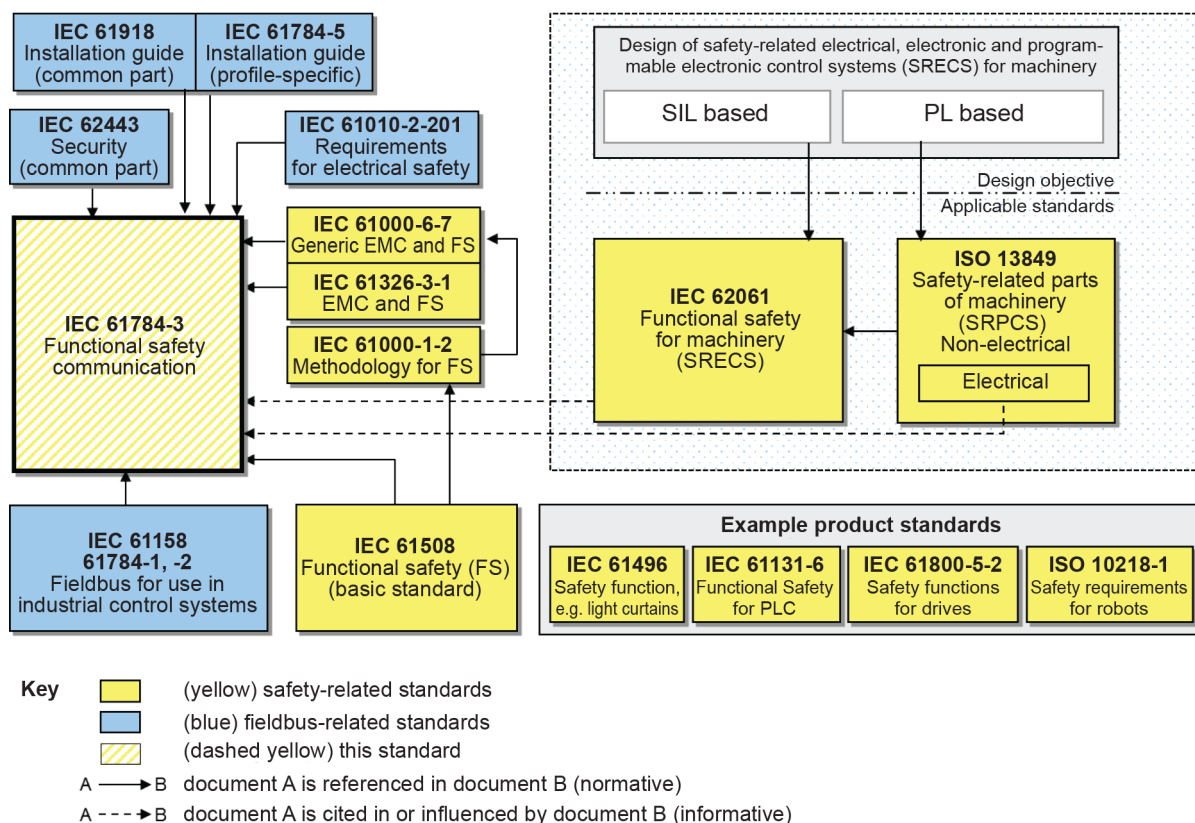
0 Introduction

0.1 General

The IEC 61158 (all parts) 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, fieldbus enhancements continue to emerge, addressing applications for areas such as real time and safety-related applications.

IEC 61784-3 (all parts) explains the relevant principles for functional safety communications with reference to IEC 61508 (all parts) 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 IEC 61158 (all parts). It does not cover electrical safety and intrinsic safety aspects. It also does not cover security aspects, nor does it provide any requirements for security.

Figure 1 shows the relationships between IEC 61784-3 (all parts) and relevant safety and fieldbus standards in a machinery environment.

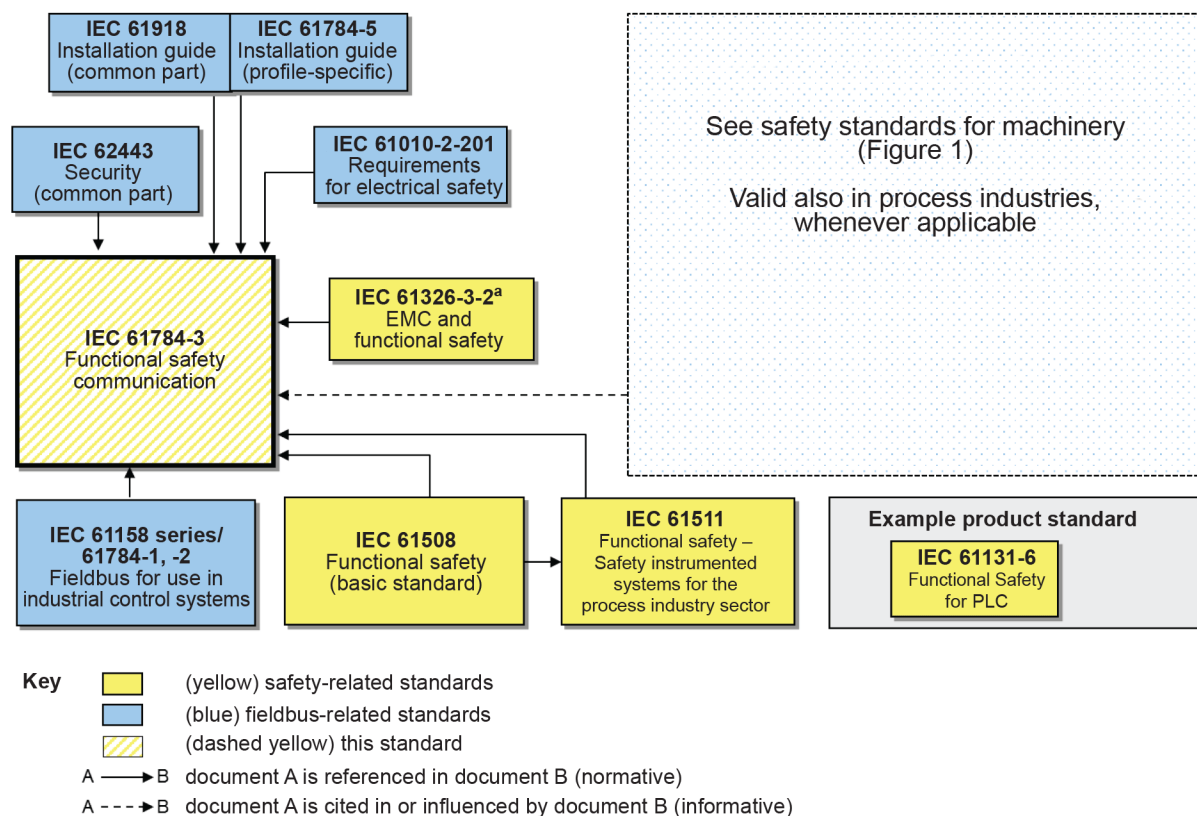


IEC

NOTE IEC 62061 specifies the relationship between PL (Category) and SIL.

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

Figure 2 shows the relationships between IEC 61784-3 (all parts) and relevant safety and fieldbus standards in a process environment.



IEC

^a For specified electromagnetic environments; otherwise IEC 61326-3-1 or IEC 61000-6-7.

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 (all parts) 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 IEC 61784-3 (all parts) 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 (FSCP) within this system – implementation of a functional safety communication profile in a standard device is not sufficient to qualify it as a safety device.

IEC 61784-3 (all parts) describes:

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

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

The holder of these patent rights has assured IEC that s/he is willing to negotiate licences under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statement of the holder of these patent rights is registered with IEC. Information may be obtained from the patent database available at <http://patents.iec.ch>.

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

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES –

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

1 Scope

This part of IEC 61784-3 (all parts) 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. This safety communication layer is intended for implementation in safety devices only.

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 document 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 (all parts)¹ for functional safety. These mechanisms may be used in various industrial applications such as process control, manufacturing automation and machinery.

This document 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 document in a standard device is not sufficient to qualify it as a safety device.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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, *Industrial-process measurement and control – Programmable controllers – Part 2: Equipment requirements and tests*

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

IEC 61158-2:2014, *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 – Type 2 elements*

IEC 61158-3-19, *Industrial communication networks – Fieldbus specifications – Part 3-19: Data-link layer service definition – Type 19 elements*

¹ In the following pages of this document, "IEC 61508" will be used for "IEC 61508 (all parts)".

IEC 61158-4-2:2019, *Industrial communication networks – Fieldbus specifications – Part 4-2: Data-link layer protocol specification – Type 2 elements*

IEC 61158-4-19, *Industrial communication networks – Fieldbus specifications – Part 4-19: Data-link layer protocol specification – Type 19 elements*

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

IEC 61158-5-19, *Industrial communication networks – Fieldbus specifications – Part 5-19: Application layer service definition – Type 19 elements*

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

IEC 61158-6-19, *Industrial communication networks – Fieldbus specifications – Part 6-19: Application layer protocol specification – Type 19 elements*

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*

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 electromagnetic environment*

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/IEEE 8802-3*

IEC 61784-3:2021, *Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions*

IEC 61784-5-2, *Industrial communication networks – Profiles – Part 5-2: 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 13849-1:2015, *Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design*

ISO 15745-2:2003, *Industrial automation systems and integration – Open systems application integration framework – Part 2: Reference description for ISO 11898-based control systems*

ISO 15745-3:2003, *Industrial automation systems and integration – Open systems application integration framework – Part 3: Reference description for IEC 61158-based control systems*

ISO 15745-4:2003, *Industrial automation systems and integration – Open systems application integration framework – Part 4: Reference description for Ethernet-based control systems*

SOMMAIRE

AVANT-PROPOS	292
0 Introduction	294
0.1 Généralités	294
0.2 Déclaration de brevets	296
1 Domaine d'application	297
2 Références normatives	297
3 Termes, définitions, symboles, abréviations et conventions	299
3.1 Termes et définitions	299
3.1.1 Termes et définitions communs	299
3.1.2 CPF 2: Termes et définitions supplémentaires	305
3.2 Symboles et abréviations	306
3.2.1 Symboles et abréviations communs	306
3.2.2 CPF 2: Symboles et abréviations supplémentaires.....	307
3.3 Conventions.....	308
4 Présentation générale du FSCP 2/1 (CIP Safety™)	308
4.1 Généralités	308
4.2 FSCP 2/1	308
5 Généralités.....	310
5.1 Documents externes de spécifications applicables au profil	310
5.2 Exigences fonctionnelles de sécurité	310
5.3 Mesures de sécurité.....	310
5.4 Structure de la couche de communication de sécurité	311
5.5 Relations avec la FAL (et DLL, PhL)	312
5.5.1 Généralités	312
5.5.2 Types de données	312
6 Services de la couche de communication de sécurité	312
6.1 Généralités	312
6.2 Objet Connexion	313
6.2.1 Généralités.....	313
6.2.2 Extensions des attributs de classe.....	313
6.2.3 Extensions de services	314
6.2.4 Format de réponse de messages explicites pour SafetyOpen et SafetyClose	314
6.3 Objet Gestionnaire de connexion	315
6.3.1 Généralités.....	315
6.3.2 ForwardOpen pour la sécurité.....	315
6.3.3 Segment de réseau de sécurité	317
6.3.4 Règles du point d'origine pour le calcul du CRC de paramètre de connexion.....	321
6.3.5 Organigrammes de traitement de SafetyOpen.....	322
6.3.6 Contrôles exigés par les producteurs multipoints avec les connexions existantes.....	325
6.3.7 Utilisation de la clé électronique de sécurité	326
6.3.8 RPI en fonction d'API dans les connexions de sécurité	326
6.3.9 Règles d'élaboration du chemin d'application pour les connexions de sécurité	327

6.3.10	Types de connexions de l'objet de validation de sécurité	329
6.3.11	Données de réponse d'application dans une réponse SafetyOpen satisfaisante	333
6.3.12	Réponse SafetyOpen non satisfaisante	335
6.3.13	Service ForwardClose de sécurité	337
6.4	Objet Identité	338
6.4.1	Généralités	338
6.4.2	Modifications apportées aux services communs	338
6.4.3	Extensions pour les appareils CP 16/3	338
6.5	Objets de liaison	339
6.5.1	Modifications apportées à l'objet DeviceNet	339
6.5.2	Modifications apportées à l'objet Interface TCP/IP	340
6.5.3	Objet Liaison SERCOS III	340
6.6	Objet Programme de contrôle de sécurité	341
6.6.1	Généralités	341
6.6.2	Attributs de classe du programme de contrôle de sécurité	342
6.6.3	Sous-classes	343
6.6.4	Attributs instance du Programme de contrôle de sécurité	343
6.6.5	Sémantique	347
6.6.6	Sous-classes	355
6.6.7	Services communs du programme de contrôle de sécurité	355
6.6.8	Comportement du Programme de contrôle de sécurité	369
6.7	Objet de validation de sécurité	377
6.7.1	Généralités	377
6.7.2	Attributs de classe	378
6.7.3	Attributs instance	378
6.7.4	Services de classes	385
6.7.5	Services instance	386
6.7.6	Comportement d'objet	386
6.8	Connection Configuration Object (Objet de configuration de connexion)	389
6.8.1	Généralités	389
6.8.2	Extensions des attributs de classe	389
6.8.3	Attributs instance, ajouts et extensions	389
6.8.4	Extensions ou restrictions de sémantique des attributs instance pour des raisons de sécurité	392
6.8.5	Paramètres spéciaux relatifs à la sécurité – (attribut 13)	398
6.8.6	Services spécifiques à l'objet	403
6.8.7	Extensions des services communs pour la sécurité	404
6.8.8	Comportement d'objet	405
7	Protocole de couche de communication de sécurité	407
7.1	Format PDU de sécurité	407
7.1.1	Codage PDU de sécurité	407
7.1.2	CRC de sécurité	419
7.2	Comportement du protocole de communication	420
7.2.1	Séquence des contrôles de sécurité	420
7.2.2	Fin de connexion	421
7.2.3	Erreur de contre-vérification	421
7.3	Opération de datation	421
7.4	Comptages de remplacement dans l'EF	423

7.5	Diagrammes séquentiels de protocoles	423
7.5.1	Généralités	423
7.5.2	Transmission de sécurité normale	423
7.5.3	Transmission de messages perdus, corrompus et retardés	425
7.5.4	Transmission de messages perdus, corrompus ou retardés avec production répétée.....	427
7.5.5	Demande Ping point à point.....	429
7.5.6	Demande Ping multipoint avec sécurité CP 2/3.....	430
7.5.7	Demande Ping multipoint sur les réseaux de sécurité CP 2/2.....	432
7.5.8	Demande Ping multipoint – Retransmission aboutie.....	432
7.5.9	Demande Ping multipoint – Retransmission avec temporisation	433
7.6	Définition du protocole de sécurité	434
7.6.1	Généralités	434
7.6.2	Vue de haut niveau d'un appareil de sécurité.....	434
7.6.3	Objet de validation de sécurité.....	435
7.6.4	Relation entre SafetyValidatorServer et SafetyValidatorClient	436
7.6.5	Gestion du remplacement de la datation de format étendu.....	437
7.6.6	Définition de la fonction SafetyValidatorClient	443
7.6.7	Définition de la fonction SafetyValidatorServer	452
7.7	Spécifications des messages de sécurité et des données de protocole	465
7.7.1	Octet Mode.....	465
7.7.2	Section de datation.....	466
7.7.3	Message de coordination temporelle.....	466
7.7.4	Message de correction de temps	466
7.7.5	Production des données de sécurité	467
7.7.6	Variables dynamiques du producteur	475
7.7.7	Variables dynamiques de producteur par consommateur	477
7.7.8	Variables de données du consommateur	479
7.7.9	Variables statiques d'entrée du consommateur	481
7.7.10	Variables dynamiques du consommateur	482
8	Gestion de la couche de communication de sécurité.....	484
8.1	Présentation générale	484
8.2	Définition des mesures utilisées lors de l'établissement d'une connexion	484
8.3	Validation de la relation point d'origine cible	488
8.4	Détection des demandes de connexion mal acheminées.....	489
8.5	Traitement de SafetyOpen	489
8.6	Gestion de propriété	489
8.7	Pontage de différentes couches physiques	490
8.8	Etablissement de connexion de sécurité	492
8.8.1	Présentation générale.....	492
8.8.2	Faits de base pour l'établissement d'une connexion.....	492
8.8.3	Configuration des connexions de sécurité.....	493
8.8.4	Multiplicateur de délai du réseau	494
8.8.5	Etablissement de connexions	496
8.8.6	Recommandations pour l'attribution d'un numéro de consommateur	499
8.8.7	Recommandations pour l'établissement d'une connexion.....	499
8.8.8	Etablissement de propriété	500
8.8.9	Cas d'utilisation de la propriété.....	500
8.8.10	Utilisation et établissement de la relation PID/CID	504

8.8.11	Utilisation PID/CID correcte dans les connexions multipoints et point à point	505
8.8.12	Services pris en charge par le réseau	507
8.8.13	Type d'appareil de sécurité FSCP 2/1	507
8.9	Processus de configuration de sécurité	511
8.9.1	Introduction à la configuration de sécurité	511
8.9.2	Objectifs de configuration	511
8.9.3	Présentation générale de la configuration	512
8.9.4	Lignes directrices pour la configuration par l'utilisateur	513
8.9.5	Justification du processus de configuration	514
8.9.6	Fonctions d'appareils pour configuration par outil	515
8.9.7	Sécurité par mot de passe	515
8.9.8	Services d'interface SNCT	516
8.9.9	Verrouillage de configuration	516
8.9.10	Influence du verrouillage de configuration sur le comportement des appareils	516
8.9.11	Propriété de configuration	518
8.9.12	Mode de configuration	518
8.9.13	Mesures d'assurance de l'intégrité du processus de configuration	518
8.9.14	Processus de téléchargement aval	520
8.9.15	Processus de vérification	523
8.9.16	Analyse des erreurs de configuration	526
8.10	Extensions de fiches techniques électroniques à des fins de sécurité	531
8.10.1	Règles générales applicables aux appareils de sécurité EDS	531
8.10.2	Extensions EDS à des fins de sécurité	531
8.11	Exigences pour le CP 2/2	537
8.11.1	Règles EPI applicables aux messages de sécurité acheminés par le CP 2/2	537
8.11.2	Service E/S de sécurité par défaut	538
8.11.3	Duplication de détection IP	538
8.11.4	Priorité pour les connexions de sécurité	538
8.12	Exigences pour le CP 2/3	538
8.12.1	Attribution des identifiants CP 2/3	538
8.12.2	Exigences supplémentaires	541
8.13	Exigences pour le CP 16/3	541
8.13.1	Architecture générale de la CPF 2 sur le CP 16/3	541
8.13.2	FSCP 2/1 de référence des appareils CP 16/3	542
8.13.3	Objets et services pris en charge dans les appareils CP 16/3	543
8.13.4	Exigences relatives aux couches de transport	544
8.13.5	FSCP 2/1 et modèle d'appareil CP 16/3	546
8.13.6	Attribution d'un UNID sur le CP 16/3	547
9	Exigences système	550
9.1	Indicateurs et commutateurs	550
9.1.1	Exigences générales concernant les indicateurs	550
9.1.2	Indications LED pour le paramétrage de l'UNID des appareils	550
9.1.3	LED d'état du module	551
9.1.4	Avertissement lié aux indicateurs	551
9.1.5	LED d'état du réseau	551
9.1.6	Commutateurs	553

9.2	Lignes directrices relatives à l'installation	555
9.3	Temps de réponse de la fonction de sécurité	555
9.3.1	Présentation générale	555
9.3.2	Délai du réseau	556
9.3.3	Equations de calcul des temps de réaction du réseau	556
9.4	Durée des demandes (ou sollicitations)	559
9.5	Contraintes liées au calcul des caractéristiques du système	559
9.5.1	Nombre de nœuds	559
9.5.2	PFH de réseau du format étendu	559
9.5.3	Taux d'erreurs sur les bits (BER)	560
9.6	Maintenance	561
9.7	Manuel de sécurité	561
10	Evaluation	561
Annexe A (informative) Informations supplémentaires pour les profils de communication de sécurité fonctionnelle de la CPF 2		562
A.1	Exemple de code de fonction de hachage	562
A.2	Vide	576
Annexe B (informative) Information pour l'évaluation des profils de communication de sécurité fonctionnelle de la CPF 2		577
Bibliographie		578
Figure 1 – Relations entre l'IEC 61784-3 et d'autres normes (machines)		294
Figure 2 – Relations entre l'IEC 61784-3 et d'autres normes (transformation)		295
Figure 3 – Relation des Objets de validation de sécurité		309
Figure 4 – Couches de communication		312
Figure 5 – ForwardOpen avec segment de réseau de sécurité		316
Figure 6 – Format cible de réseau de sécurité		319
Figure 7 – Service SafetyOpen de traitement de cible sans données de configuration (SafetyOpen de type 2)		323
Figure 8 – Service SafetyOpen de traitement de cible avec données de configuration (SafetyOpen de type 1)		324
Figure 9 – Logique du point d'origine permettant de déterminer le format à utiliser		325
Figure 10 – Application de configuration d'appareil		360
Figure 11 – Organigrammes de traitement de Configuration et Validation		361
Figure 12 – Traitement d'UNID pendant l'état "Attente du TUNID"		368
Figure 13 – Diagramme d'états du Programme de contrôle de sécurité		370
Figure 14 – Relations entre configuration, essais et verrouillage		375
Figure 15 – Types de connexions de sécurité		383
Figure 16 – Diagramme de transitions d'état de l'Objet de validation de sécurité		387
Figure 17 – Logique pour le type de format Autodétection		402
Figure 18 – Diagramme d'états de l'objet Configuration de connexion		406
Figure 19 – Flux de données de l'objet Configuration de connexion		406
Figure 20 – Format de l'octet Mode		409
Figure 21 – Section de données à 1 ou 2 octets, format de base		410
Figure 22 – Section de données à 1 ou 2 octets, format étendu		410
Figure 23 – Format de section de données de 3 à 250 octets, format de base		411

Figure 24 – Format de section de données de 3 à 250 octets, format étendu	411
Figure 25 – Format de section de datation, format de base	412
Figure 26 – Codage du message de coordination temporelle BF	413
Figure 27 – Codage du message de coordination temporelle EF	413
Figure 28 – Codage du message de correction de temps BF	415
Figure 29 – Codage du message de correction de temps EF	415
Figure 30 – Codage PDU point à point à 1 ou 2 octets	416
Figure 31 – Codage PDU multipoint à 1 ou 2 octets	417
Figure 32 – Format de connexion de sécurité de format 2 multipoint à 1 ou 2 octets	417
Figure 33 – Codage PDU point à point de 3 à 250 octets	418
Figure 34 – Codage PDU multipoint de 3 à 248 octets	418
Figure 35 – Format de connexion de sécurité multipoint de 3 à 248 octets	419
Figure 36 – Ordre de calcul du CRC pour les messages de format étendu	419
Figure 37 – Séquence de datation	422
Figure 38 – Diagramme d'une séquence de sécurité producteur/consommateur normale	423
Figure 39 – Diagramme d'une séquence de sécurité producteur/consommateur normale (production répétée)	424
Figure 40 – Diagramme séquentiel d'un message producteur vers consommateur corrompu	425
Figure 41 – Diagramme séquentiel d'un message producteur vers consommateur perdu	426
Figure 42 – Diagramme séquentiel d'un message retardé	427
Figure 43 – Diagramme séquentiel d'un message producteur vers consommateur corrompu avec production répétée	427
Figure 44 – Diagramme séquentiel d'une fin de connexion occasionnée par des retards	428
Figure 45 – Diagramme séquentiel d'un contrôle CRC de sécurité non satisfaisant	429
Figure 46 – Diagramme séquentiel d'une demande Ping point à point – réponse normale	429
Figure 47 – Diagramme séquentiel d'une demande Ping multipoint satisfaisante, sécurité CP 2/3	431
Figure 48 – Diagramme séquentiel d'une demande Ping multipoint satisfaisante, sécurité CP 2/2	432
Figure 49 – Diagramme séquentiel d'une retransmission de demande Ping multipoint	433
Figure 50 – Diagramme séquentiel d'une temporisation de demande Ping multipoint	433
Figure 51 – Architectures de sécurité possibles pour le FSCP 2/1	434
Figure 52 – Diagramme de relations des entités de modèle de référence d'un appareil de sécurité	435
Figure 53 – Deux appareils qui échangent des données de sécurité par l'intermédiaire des fonctions SafetyValidatorClient et SafetyValidatorServer	436
Figure 54 – Consommateur d'origine et producteur cible point à point	438
Figure 55 – Producteur d'origine et consommateur cible point à point	440
Figure 56 – Consommateur d'origine et producteur cible multipoint	441
Figure 57 – Flux de données de production de sécurité	443
Figure 58 – Contrôle des données de sécurité de consommation	453
Figure 59 – SafetyValidatorServer – déclenchée par l'application	453

Figure 60 – Propriété cible.....	488
Figure 61 – Formes de SafetyOpen	489
Figure 62 – Diagramme d'états de la propriété de connexion	490
Figure 63 – Mapping de l'UNID de service SafetyOpen	490
Figure 64 – Couche application CPF 2 commune	491
Figure 65 – Exemple d'acheminement de bout en bout	491
Figure 66 – Sources des paramètres de connexion relative à la sécurité	495
Figure 67 – Mapping des paramètres entre le point d'origine et la cible	496
Figure 68 – Etablissement d'une connexion de sécurité CP 2/3 dans les cibles pour un service SafetyOpen de type 2a	498
Figure 69 – Séquence générale de détection de l'exigence d'une configuration	498
Figure 70 – Echanges PID/CID pour deux scénarios de point d'origine	504
Figure 71 – Génération des valeurs de départ pour les connexions multipoints	505
Figure 72 – Traitement d'exécution PID/CID	506
Figure 73 – Catégories de connexions et services pris en charge	509
Figure 74 – Types de connexions recommandés.....	510
Figure 75 – Services logique à logique pris en charge	510
Figure 76 – Types de connexions recommandés pour les services logique à logique	511
Figure 77 – Transferts de données de configuration.....	512
Figure 78 – Mesures de protection des appareils de sécurité	514
Figure 79 – Relations entre configuration, essais et verrouillage.....	517
Figure 80 – Données de configuration du point d'origine	519
Figure 81 – Processus de téléchargement aval du SNCT à l'appareil.....	521
Figure 82 – Téléchargements aval du SNCT vers les points d'origine qui réalisent la configuration de type 1	522
Figure 83 – Protection contre le verrouillage et propriété	524
Figure 84 – Processus de vérification comprenant toutes les méthodes alternatives	526
Figure 85 – FSCP 2/1 de référence des appareils CP 16/3	543
Figure 86 – Interaction entre couches d'adaptation FSCP 2/1 et SMP.....	545
Figure 87 – Couche d'adaptation FSCP 2/1	546
Figure 88 – Modèle d'appareil CP 16/3	547
Figure 89 – Ajout d'un module normalisé à un appareil modulaire	549
Figure 90 – Logique de traitement du NodeID des appareils de sécurité	554
Figure 91 – Temps de réponse de la fonction de sécurité	555
Figure 92 – Composantes du temps de réponse de la fonction de sécurité	558
Figure 93 – Schéma de principe de fiabilité (RBD) de protocole de réseau	559
Tableau 1 – Erreurs de communication et matrice de mesures de détection.....	311
Tableau 2 – Nouveaux attributs de classe.....	313
Tableau 3 – Extensions de services	314
Tableau 4 – Format de réponse SafetyOpen et SafetyClose	314
Tableau 5 – Identifiant de segment de réseau de sécurité.....	317
Tableau 6 – Définition du segment de réseau de sécurité	317
Tableau 7 – Format de routage de segment de réseau de sécurité	320

Tableau 8 – Format étendu de segment de réseau de sécurité	320
Tableau 9 – Règles d'évaluation des paramètres de production multipoint	326
Tableau 10 – Options de paramétrage du service ForwardOpen pour les connexions de sécurité qui comportent des chemins d'application qui reposent sur des objets	330
Tableau 11 – Options de paramétrage du service ForwardOpen pour les connexions de sécurité qui comportent un chemin d'application de segment de symbole étendu ANSI	332
Tableau 12 – Paramètres de connexion de réseau pour les connexions de sécurité	333
Tableau 13 – Réponse d'application de cible SafetyOpen (taille: 10 octets)	333
Tableau 14 – Réponse d'application de cible SafetyOpen EF CP 2/2 ou CP 16/3 (taille: 14 octets)	334
Tableau 15 – Réponse d'application de cible SafetyOpen BF CP 2/3 (taille: 18 octets)	334
Tableau 16 – Réponse d'application de cible SafetyOpen EF CP 2/3 (taille: 22 octets)	335
Tableau 17 – Nouveaux codes d'erreurs étendus de sécurité	335
Tableau 18 – Tableau de recommandations concernant les événements d'erreur SafetyOpen	336
Tableau 19 – Modifications apportées aux services communs de l'objet Identité	338
Tableau 20 – Extensions de l'objet Identité pour les appareils CP 16/3	339
Tableau 21 – Nouvel attribut instance de l'objet DeviceNet	339
Tableau 22 – Nouvel attribut instance de l'objet Interface TCP/IP	340
Tableau 23 – Attributs de classe de l'objet Liaison SERCOS III	340
Tableau 24 – Attributs instance de l'objet Liaison SERCOS III	341
Tableau 25 – Services communs de l'objet Liaison SERCOS III	341
Tableau 26 – Attributs de classe du Programme de contrôle de sécurité	342
Tableau 27 – Attributs instance du Programme de contrôle de sécurité	343
Tableau 28 – Valeurs d'indication de l'attribut Etat de l'appareil	348
Tableau 29 – Format de l'attribut Etat d'exception	349
Tableau 30 – Valeurs de l'attribut Détail d'exception commun	350
Tableau 31 – Synthèse du format de détail d'exception	351
Tableau 32 – Synthèse du comportement des appareils pour différentes valeurs CFUNID	353
Tableau 33 – Services communs du Programme de contrôle de sécurité	355
Tableau 34 – Services spécifiques de l'objet Programme de contrôle de sécurité	356
Tableau 35 – Structure de message Configure_Request	358
Tableau 36 – Structure de message Validate_Configuration	358
Tableau 37 – Structure de message de réussite Validate_Configuration	359
Tableau 38 – Code d'erreur de Validate_Configuration	359
Tableau 39 – Codes étendus de Validate_Configuration	359
Tableau 40 – Structure de message Set_Password	362
Tableau 41 – Structure de message Reset_Password	362
Tableau 42 – Structure de message Configuration_Lock/Unlock	363
Tableau 43 – Structure de message Mode_Change	363
Tableau 44 – Structure de message Safety_Reset	364
Tableau 45 – Types de réinitialisations de sécurité du Programme de contrôle de sécurité	364
Tableau 46 – Paramètre d'attribut Mode point	365

Tableau 47 – Règles de traitement applicables aux types de réinitialisations	365
Tableau 48 – Service Propose_TUNID	366
Tableau 49 – Service Apply_TUNID	366
Tableau 50 – Service Propose_TUNID_List	369
Tableau 51 – Service Apply_TUNID_List.....	369
Tableau 52 – Événements liés au Programme de contrôle de sécurité	370
Tableau 53 – Matrice d'événements d'état du Programme de contrôle de sécurité	371
Tableau 54 – Contrôle de la propriété de configuration en fonction de l'état de l'appareil	375
Tableau 55 – Mapping des états du Programme de contrôle de sécurité vers l'objet Identité	376
Tableau 56 – Mapping des événements de l'objet Programme de contrôle de sécurité.....	376
Tableau 57 – Mapping des événements de l'objet Identité	377
Tableau 58 – Attributs de classe de l'Objet de validation de sécurité	378
Tableau 59 – Attributs instance de l'Objet de validation de sécurité	378
Tableau 60 – Attributions d'états de l'Objet de validation de sécurité	382
Tableau 61 – Type d'Objet de validation de sécurité, attributions de champs de bits.....	382
Tableau 62 – Règles d'évaluation du paramètre SafetyOpen des producteurs multipoints	384
Tableau 63 – Services de classes de l'Objet de validation de sécurité	385
Tableau 64 – Services instance de l'Objet de validation de sécurité.....	386
Tableau 65 – Données du service Get_Attributes_All de l'Objet de validation de sécurité.....	386
Tableau 66 – Matrice d'événements d'état de l'Objet de validation de sécurité.....	388
Tableau 67 – Mapping des états entre le Programme de contrôle de sécurité et l'Objet de validation de sécurité	389
Tableau 68 – Extensions des attributs de classe de l'objet Configuration de connexion	389
Tableau 69 – Ajouts/extensions d'attributs instance de l'objet Configuration de connexion	390
Tableau 70 – Définition des bits de drapeaux de connexion	393
Tableau 71 – Paramètres de connexion O-to-T	394
Tableau 72 – Paramètres de connexion T-to-O	395
Tableau 73 – Formats de mapping des données	396
Tableau 74 – Format 0 de mapping des données	397
Tableau 75 – Format 1 de mapping des données	397
Tableau 76 – Valeurs SCCRC de l'appareil cible.....	400
Tableau 77 – Valeurs SCTS de l'appareil cible.....	400
Tableau 78 – Paramètres de connexion de correction de temps pour une connexion multipoint.....	401
Tableau 79 – Signification de l'attribut Type de format	402
Tableau 80 – Signification de l'attribut Etat du format	403
Tableau 81 – Services spécifiques à l'objet Configuration de connexion	403
Tableau 82 – Données du service de réponse Get_Attributes_All (attributs ajoutés)	404
Tableau 83 – Données du service de réponse Get_Attributes_All (paramètres ajoutés)	404
Tableau 84 – Données du service de demande Set_Attributes_All (attributs ajoutés).....	405

Tableau 85 – Données du service de réponse Set_Attributes_All (paramètres ajoutés).....	405
Tableau 86 – Mapping des états entre le Programme de contrôle de sécurité et les objets CCO	406
Tableau 87 – Sections de connexion et formats PDU	408
Tableau 88 – Sections de connexion et format de message	408
Tableau 89 – Variables de l'octet Mode	409
Tableau 90 – Variables de datation	412
Tableau 91 – Variables du message de coordination temporelle	413
Tableau 92 – Variables du message de correction de temps	415
Tableau 93 – Polynômes de CRC utilisés.....	420
Tableau 94 – Utilisation des CRC pour la connexion et la configuration	420
Tableau 95 – Réception des données – Déclenchée par la liaison	454
Tableau 96 – Réception de Time_Correction – Déclenchée par la liaison.....	455
Tableau 97 – Réception des données – Déclenchée par l'application.....	455
Tableau 98 – Réception de Time_Correction – Déclenchée par l'application	455
Tableau 99 – Application de consommation – Contrôle des données de sécurité	456
Tableau 100 – Détermination de l'état de la connexion du producteur	467
Tableau 101 – Etat de la connexion de sécurité de consommation.....	479
Tableau 102 – Erreurs d'établissement de connexion et mesures de détection des erreurs.....	484
Tableau 103 – Attributions de Date/Heure SNN	485
Tableau 104 – Plage légale de SNN des valeurs temporelles.....	485
Tableau 105 – Paramètres de connexion de sécurité	494
Tableau 106 – Récapitulatif SafetyOpen	497
Tableau 107 – Mapping des services point d'origine/cible	508
Tableau 108 – Types de services point d'origine/cible non pris en charge.....	508
Tableau 109 – Objectifs de configuration	512
Tableau 110 – Contrôle de la propriété de configuration en fonction de l'état de l'appareil.....	517
Tableau 111 – Erreurs et mesures de détection	527
Tableau 112 – Mots clés des sections de classe d'objet.....	532
Tableau 113 – Format d'entrée Classex de sécurité.....	533
Tableau 114 – Mots clés de classes de paramètres	533
Tableau 115 – Nouveaux mots clés de la section Gestionnaire de connexion à des fins de sécurité.....	534
Tableau 116 – Utilisation du champ Gestionnaire de connexion à des fins de sécurité.....	535
Tableau 117 – Paramétrages du champ Paramètres de connexion à des fins de sécurité.....	537
Tableau 118 – Règles d'attribution d'ID CP 2/3	539
Tableau 119 – Indications LED pour le paramétrage de l'UNID	550
Tableau 120 – LED d'état du module	551
Tableau 121 – Etats de la LED d'état du réseau.....	552
Tableau 122 – Type de temps de réaction de connexion – applications de production/consommation	557

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

RÉSEAUX DE COMMUNICATION INDUSTRIELS – PROFILS –

Partie 3-2: Bus de terrain de sécurité fonctionnelle – Spécifications supplémentaires pour CPF 2

AVANT-PROPOS

- 1) La Commission Electrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
- 2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
- 3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
- 4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
- 5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
- 6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
- 7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.
- 8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
- 9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets.

L'IEC 61784-3-2 a été établie par le sous-comité 65C: Réseaux industriels, du comité d'études 65 de l'IEC: Mesure, commande et automation dans les processus industriels. Il s'agit d'une Norme internationale.

Cette quatrième édition annule et remplace la troisième édition parue en 2016. Cette édition constitue une révision technique.

Cette édition inclut les modifications techniques majeures suivantes par rapport à l'édition précédente:

- ajout de deux nouveaux états de l'objet Programme de contrôle de sécurité en 6.6.5.5;

- ajout de l'exigence relative au comportement des LED réseau pour le processus de proposition de TUNID en 6.6.8, 9.1.2 et 9.1.5;
- ajout de la prise en charge du chemin d'application pour les variables de processus en 6.3.9 et 6.3.10;
- ajout de la prise en charge des appareils multiports en 6.6.4, 6.6.5, 6.6.7 et en différents endroits;
- correction des équations de temps de réaction du réseau en 9.3.3;
- ajout de la prise en charge SIL jusqu'au niveau SIL3 en 7.6, 8.7, 8.9, 9.5 et en différents endroits;
- reprise des lignes directrices relatives à la procédure de configuration en 8.9.14 et 8.9.15;
- détection des modifications de commutateur en 9.1.6;
- utilisation déconseillée du format de base en 3.1.2, 7.1.1.1 et 6.3.3.2;
- définition de la valeur Max_Fault_Number sur 2 en 6.3.3.4, 6.8.3 et 8.8.3;
- mise à jour du calcul de la PFH de réseau en 9.5.2;
- apport de diverses corrections mineures depuis la dernière publication.

Le texte de cette Norme internationale est issu des documents suivants:

FDIS	Rapport de vote
65C/1083/FDIS	65C/1087/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à son approbation.

La version française de cette norme n'a pas été soumise au vote.

La langue employée pour l'élaboration de cette Norme internationale est l'anglais.

Le présent document a été rédigé selon les Directives ISO/IEC, Partie 2, il a été développé selon les Directives ISO/IEC, Partie 1 et les Directives ISO/IEC, Supplément IEC, disponibles sous www.iec.ch/members_experts/refdocs. Les principaux types de documents développés par l'IEC sont décrits plus en détail sous www.iec.ch/standardsdev/publications.

Une liste de toutes les parties de la série IEC 61784-3, publiées sous le titre général *Réseaux de communication industriels – Profils – Bus de terrain de sécurité fonctionnelle*, peut être consultée sur le site web de l'IEC.

Le comité a décidé que le contenu du présent document ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous "webstore.iec.ch" dans les données relatives au document recherché. A cette date, le document sera

- reconduit,
- supprimé,
- remplacé par une édition révisée, ou
- amendé.

IMPORTANT – Le logo "colour inside" qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

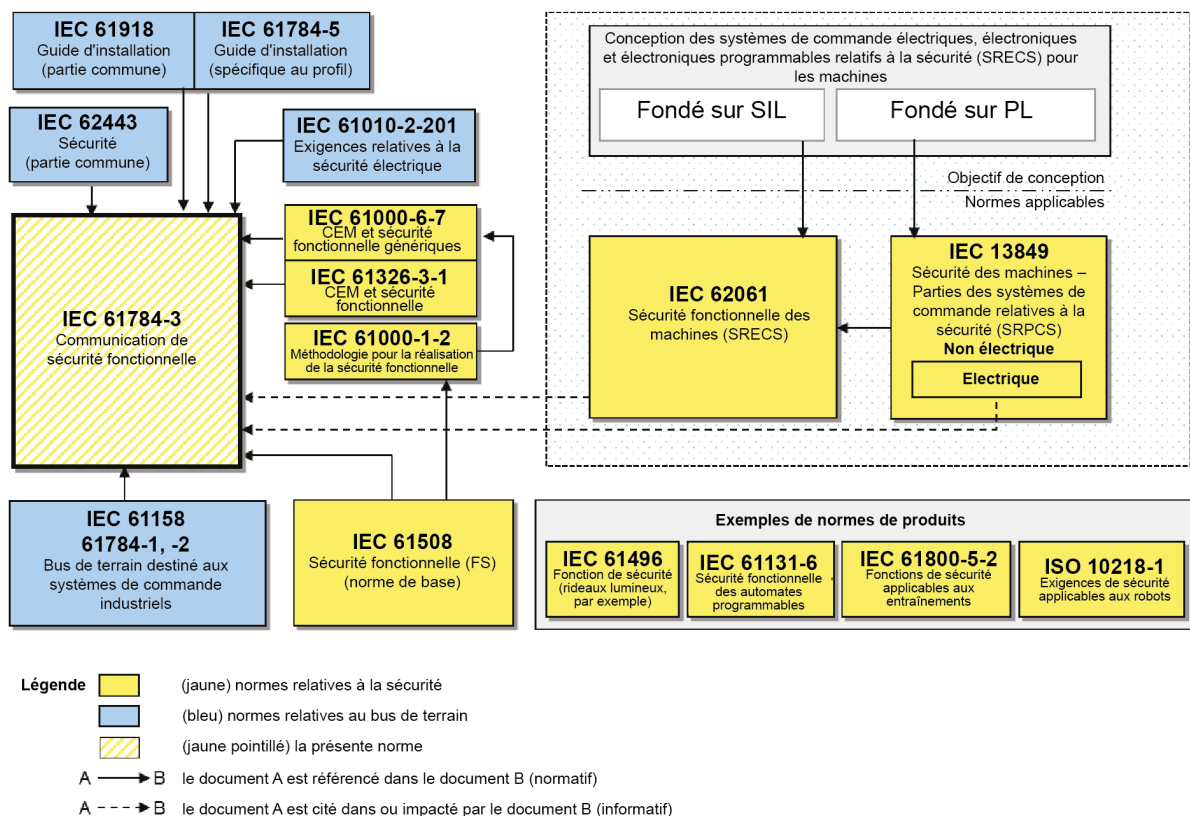
0 Introduction

0.1 Généralités

L'IEC 61158 (toutes les parties), relative aux bus de terrain, ainsi que ses normes associées IEC 61784-1 et IEC 61784-2, définissent un ensemble de protocoles de communication qui assurent la commande répartie d'applications automatisées. La technologie de bus de terrain est désormais reconnue et bien éprouvée. Les améliorations des bus de terrain se poursuivent; elles couvrent des applications pour des domaines comme les applications en temps réel relatives à la sécurité.

La série IEC 61784-3 (toutes les parties) explique les principes pertinents pour les communications de sécurité fonctionnelle en référence à l'IEC 61508 (toutes les parties) et spécifie plusieurs couches de communication de sécurité (profils et protocoles correspondants) qui reposent sur les profils de communication et les couches de protocole de l'IEC 61784-1, l'IEC 61784-2 et l'IEC 61158 (toutes les parties). Elle ne couvre pas les aspects relatifs à la sécurité électrique et à la sécurité intrinsèque. Elle ne couvre pas non plus les aspects relatifs à la sûreté et ne prévoit aucune exigence en matière de sûreté.

La Figure 1 représente les relations entre l'IEC 61784-3 (toutes les parties) et les normes pertinentes relatives à la sécurité et aux bus de terrain dans un environnement de machines.

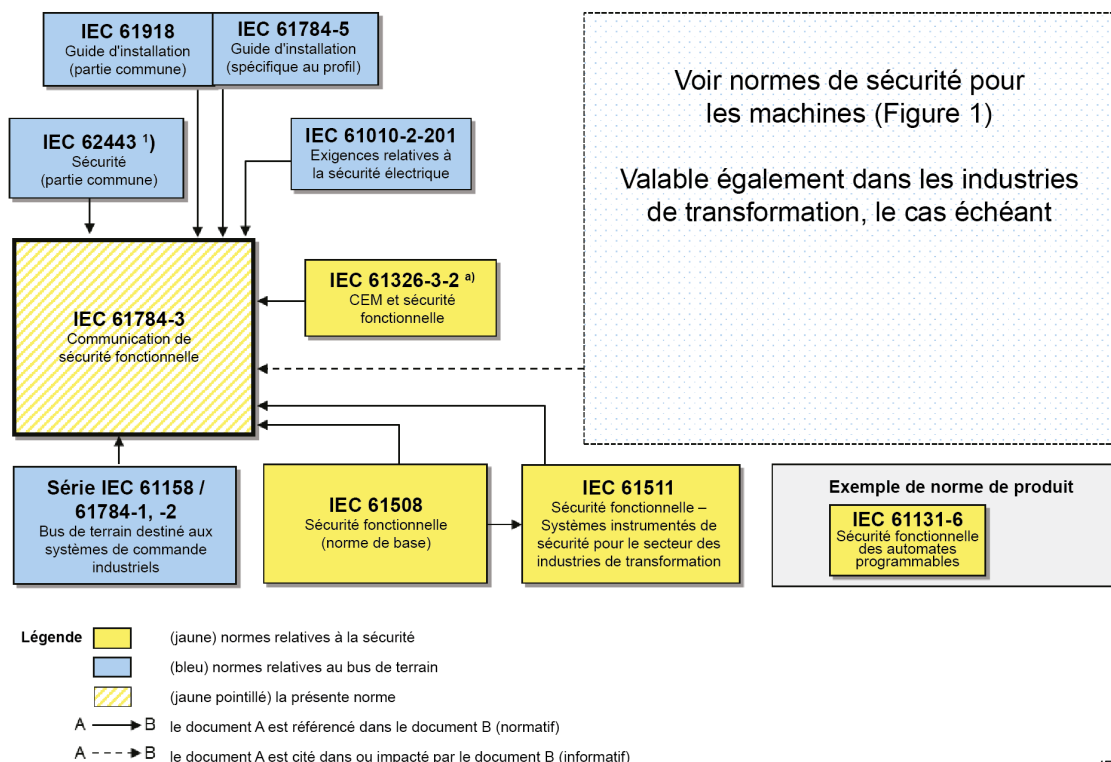


IEC

NOTE L'IEC 62061 spécifie la relation entre PL (Catégorie) et SIL.

Figure 1 – Relations entre l'IEC 61784-3 et d'autres normes (machines)

La Figure 2 représente les relations entre l'IEC 61784-3 (toutes les parties) et les normes pertinentes relatives à la sécurité et aux bus de terrain dans un environnement de processus.



^a Pour les environnements électromagnétiques spécifiés; sinon, l'IEC 61326-3-1 ou l'IEC 61000-6-7 s'applique.

Figure 2 – Relations entre l'IEC 61784-3 et d'autres normes (transformation)

Les couches de communication de sécurité mises en œuvre dans le cadre de systèmes relatifs à la sécurité conformément à l'IEC 61508 (toutes les parties) assurent la confiance nécessaire à accorder à la transmission de messages (informations) entre plusieurs participants sur un bus de terrain dans un système relatif à la sécurité ou une fiabilité suffisante dans le comportement de sécurité en cas d'erreurs ou de défaillances du bus de terrain.

Les couches de communication de sécurité spécifiées dans l'IEC 61784-3 (toutes les parties) permettent de s'assurer qu'un bus de terrain peut être utilisé dans des applications qui nécessitent une sécurité fonctionnelle jusqu'au niveau d'intégrité de sécurité (SIL) spécifié par son profil de communication de sécurité fonctionnelle correspondant.

La revendication du SIL qui en résulte pour un système dépend de la mise en œuvre du profil de communication de sécurité fonctionnelle (FSCP) retenu au sein du système (la mise en œuvre du profil de communication de sécurité fonctionnelle dans un appareil normal ne suffit pas à le qualifier d'appareil de sécurité).

L'IEC 61784-3 (toutes les parties) décrit:

- les principes de base de la mise en œuvre des exigences de l'IEC 61508 (toutes les parties) pour les communications de données relatives à la sécurité, y compris les anomalies de transmission potentielles, les mesures correctives et des considérations relatives à l'intégrité des données;
- les profils de communication de sécurité fonctionnelle pour plusieurs familles de profils de communication dans l'IEC 61784-1 et l'IEC 61784-2, y compris les extensions de la couche de sécurité aux sections relatives au service et aux protocoles de communication de l'IEC 61158 (toutes les parties).

0.2 Déclaration de brevets

La Commission Electrotechnique Internationale (IEC) attire l'attention sur le fait qu'il est déclaré que la conformité avec les dispositions du présent document peut impliquer l'utilisation de brevets intéressant les profils de communication de sécurité fonctionnelle pour la famille 2. L'IEC ne prend pas position quant à la preuve, à la validité et à la portée de ces droits de propriété.

Le détenteur de ces droits de propriété a donné l'assurance à l'IEC qu'il consent à négocier des licences avec des demandeurs du monde entier à des termes et conditions raisonnables et non discriminatoires. A ce propos, la déclaration du détenteur des droits de propriété est enregistrée à l'IEC. Des informations peuvent être obtenues dans la base de données des droits de propriété, disponible à l'adresse suivante: <http://patents.iec.ch>.

L'attention est d'autre part attirée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété autres que ceux qui ont été enregistrés dans la base de données des droits de propriété. L'IEC ne saurait être tenue pour responsable de l'identification de ces droits de propriété en tout ou partie.

RÉSEAUX DE COMMUNICATION INDUSTRIELS – PROFILS –

Partie 3-2: Bus de terrain de sécurité fonctionnelle – Spécifications supplémentaires pour CPF 2

1 Domaine d'application

La présente partie de l'IEC 61784-3 (toutes les parties) spécifie une couche de communication de sécurité (services et protocole) qui repose sur la CPF 2 de l'IEC 61784-1, l'IEC 61784-2 et l'IEC 61158, Type 2. Elle identifie les principes applicables aux communications de sécurité fonctionnelle définies dans l'IEC 61784-3, qui correspondent à cette couche de communication de sécurité. Cette couche de communication de sécurité est destinée à être mise en œuvre uniquement sur les appareils de sécurité.

NOTE 1 Elle ne couvre pas les aspects relatifs à la sécurité électrique et à la sécurité intrinsèque. La sécurité électrique concerne les dangers tels que les chocs électriques. La sécurité intrinsèque concerne les dangers associés aux atmosphères explosibles.

Le présent document définit les mécanismes de transmission des messages relatifs à la sécurité entre les participants d'un réseau réparti, en utilisant la technologie de bus de terrain conformément aux exigences de la série IEC 61508 (toutes les parties)¹ concernant la sécurité fonctionnelle. Ces mécanismes peuvent être utilisés dans différentes applications industrielles, par exemple la commande de processus, l'usinage automatique et les machines.

Le présent document fournit des lignes directrices aux développeurs, ainsi qu'aux évaluateurs d'appareils et de systèmes conformes.

NOTE 2 La revendication du SIL qui en résulte pour un système dépend de la mise en œuvre du profil de communication de sécurité fonctionnelle retenu au sein du système (la mise en œuvre d'un profil de communication de sécurité fonctionnelle conforme au présent document dans un appareil normal ne suffit pas à le qualifier d'appareil de sécurité).

2 Références normatives

Les documents suivants sont cités dans le texte de sorte qu'ils constituent, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

IEC 61131-2, *Mesurage et contrôle des processus industriels – Automates programmables – Partie 2: Exigences et essais des équipements*

IEC 61131-3, *Automates programmes – Partie 3: Langages de programmation*

IEC 61158-2:2014, *Réseaux de communications industriels – Spécifications des bus de terrain – Partie 2: Spécification et définition des services de la couche physique*

IEC 61158-3-2, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 3-2: Définition des services de la couche liaison de données – Eléments de type 2*

¹ Dans les pages suivantes du présent document, "IEC 61508" remplace "IEC 61508 (toutes les parties)".

IEC 61158-3-19, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 3-19: Définition des services de la couche liaison de données – Eléments de type 19*

IEC 61158-4-2:2019, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 4-2: Spécification du protocole de la couche de liaison de données – Eléments de Type 2*

IEC 61158-4-19, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 4-19: Spécification du protocole de la couche de liaison de données – Eléments de type 19*

IEC 61158-5-2, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 5-2: Définition des services de la couche application – Eléments de type 2*

IEC 61158-5-19, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 5-19: Définition des services de la couche application – Eléments de type 19*

IEC 61158-6-2, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 6-2: Spécification de protocole de couche application – Eléments de type 2*

IEC 61158-6-19, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 6-19: Spécification de protocole de la couche application – Eléments de type 19*

IEC 61326-3-1, *Matériel électrique de mesure, de commande et de laboratoire – Exigences relatives à la CEM – Partie 3-1: Exigences d'immunité pour les systèmes relatifs à la sécurité et pour les matériels destinés à réaliser des fonctions relatives à la sécurité (sécurité fonctionnelle) – Applications industrielles générales*

IEC 61326-3-2, *Matériel électrique de mesure, de commande et de laboratoire – Exigences relatives à la CEM – Partie 3-2: Exigences d'immunité pour les systèmes relatifs à la sécurité et pour les matériels destinés à réaliser des fonctions relatives à la sécurité (sécurité fonctionnelle) – Applications industrielles dont l'environnement électromagnétique est spécifié*

IEC 61508 (toutes les parties), *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité*

IEC 61784-1, *Réseaux de communication industriels – Profils – Partie 1: Profils de bus de terrain*

IEC 61784-2, *Réseaux de communication industriels – Profils – Partie 2: Profils de bus de terrain supplémentaires pour les réseaux en temps réel fondés sur l'ISO/IEC/IEEE 8802-3*

IEC 61784-3:2021, *Réseaux de communication industriels – Profils – Partie 3: Bus de terrain de sécurité fonctionnelle – Règles générales et définitions de profils*

IEC 61784-5-2, *Réseaux de communication industriels – Profils – Partie 5-2: Installation des bus de terrain – Profils d'installation pour CPF 2*

IEC 61918, *Réseaux de communication industriels – Installation de réseaux de communication dans des locaux industriels*

IEC 62026-3, *Appareillage à basse tension – Interfaces appareil de commande-appareil (CDI) – Partie 3: DeviceNet*

ISO 13849-1:2015, *Sécurité des machines – Parties des systèmes de commande relatives à la sécurité – Partie 1: Principes généraux de conception*

ISO 15745-2:2003, *Industrial automation systems and integration – Open systems application integration framework – Part 2: Reference description for ISO 11898-based control systems* (disponible en anglais seulement)

ISO 15745-3:2003, *Industrial automation systems and integration – Open systems application integration framework – Part 3: Reference description for IEC 61158-based control systems* (disponible en anglais seulement)

ISO 15745-4:2003, *Industrial automation systems and integration – Open systems application integration framework – Part 4: Reference description for Ethernet-based control systems* (disponible en anglais seulement)