

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

PRICE CODE
CODE PRIX

XH

ICS 25.040; 35.100.05

ISBN 978-2-8322-0888-5

**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.....	11
INTRODUCTION.....	13
1 Scope.....	16
2 Normative references	16
3 Terms, definitions, symbols, abbreviated terms and conventions	17
3.1 Terms and definitions	17
3.1.1 Common terms and definitions	17
3.1.2 CPF 2: Additional terms and definitions	21
3.2 Symbols and abbreviated terms.....	22
3.2.1 Common symbols and abbreviated terms	22
3.2.2 CPF 2: Additional symbols and abbreviated terms	22
3.3 Conventions	23
4 Overview of FSCP 2/1 (CIP Safety™).....	23
4.1 General.....	23
4.2 FSCP 2/1	23
5 General	24
5.1 External documents providing specifications for the profile.....	24
5.2 Safety functional requirements.....	25
5.3 Safety measures	25
5.4 Safety communication layer structure.....	26
5.5 Relationships with FAL (and DLL, PhL)	26
5.5.1 General	26
5.5.2 Data types.....	26
6 Safety communication layer services.....	27
6.1 Introduction.....	27
6.2 Connection object	27
6.2.1 General	27
6.2.2 Class attribute extensions	27
6.2.3 Service extensions	28
6.2.4 Explicit message response format for SafetyOpen and SafetyClose	28
6.3 Connection Manager object.....	29
6.3.1 General	29
6.3.2 ForwardOpen for safety	29
6.3.3 Safety network segment	31
6.3.4 Originator rules for calculating the connection parameter CRC	33
6.3.5 SafetyOpen processing flowcharts.....	33
6.3.6 Checks required by Multipoint producers with existing connections	36
6.3.7 Electronic key usage for safety.....	36
6.3.8 RPI vs. API in safety connections	36
6.3.9 Application path construction for safety	36
6.3.10 Safety Validator connection types.....	38
6.3.11 Application reply data in a successful SafetyOpen response.....	39
6.3.12 Unsuccessful SafetyOpen response	40
6.3.13 ForwardClose for safety.....	43
6.4 Identity object.....	43
6.4.1 General	43

6.4.2	Changes to common services	43
6.5	Link objects	44
6.5.1	DeviceNet object changes	44
6.5.2	TCP/IP Interface object changes	44
6.6	Safety Supervisor object.....	45
6.6.1	General	45
6.6.2	Safety Supervisor class attributes.....	45
6.6.3	Subclasses	46
6.6.4	Safety Supervisor instance attributes.....	46
6.6.5	Semantics	49
6.6.6	Subclasses	55
6.6.7	Safety Supervisor common services	55
6.6.8	Safety Supervisor behavior.....	66
6.7	Safety Validator object	73
6.7.1	General	73
6.7.2	Class attributes	73
6.7.3	Instance attributes	74
6.7.4	Class services	80
6.7.5	Instance services.....	80
6.7.6	Object behavior	81
6.8	Connection Configuration Object.....	84
6.8.1	General	84
6.8.2	Class attribute extensions	84
6.8.3	Instance attributes, additions and extensions.	84
6.8.4	Instance attribute semantics extensions or restrictions for safety.....	86
6.8.5	Special Safety Related Parameters – (Attribute 13)	91
6.8.6	Object-specific services.....	95
6.8.7	Common service extensions for safety.....	95
6.8.8	Object behavior	97
7	Safety communication layer protocol	98
7.1	Safety PDU format	98
7.1.1	Safety PDU encoding	98
7.1.2	Safety CRC	108
7.2	Communication protocol behavior.....	109
7.2.1	Sequence of safety checks	109
7.2.2	Connection termination.....	109
7.2.3	Cross checking error	109
7.3	Time stamp operation.....	110
7.4	Protocol sequence diagrams	111
7.4.1	General	111
7.4.2	Normal safety transmission.....	111
7.4.3	Lost, corrupted and delayed message transmission.....	112
7.4.4	Lost, corrupted or delayed message transmission with production repeated.....	115
7.4.5	Point-to-point ping	117
7.4.6	Multipoint ping on CP 2/3 Safety.....	118
7.4.7	Multipoint ping on CP 2/2 safety networks	119
7.4.8	Multipoint ping – retry with success	120
7.4.9	Multipoint ping – retry with timeout	121

7.5	Safety protocol definition	122
7.5.1	General	122
7.5.2	High level view of a safety device	122
7.5.3	Safety Validator object	123
7.5.4	Relationship between SafetyValidatorServer and SafetyValidatorClient	123
7.5.5	SafetyValidatorClient function definition	124
7.5.6	SafetyValidatorServer function definition	132
7.6	Safety message and protocol data specifications	142
7.6.1	Mode octet	142
7.6.2	Time Stamp Section	143
7.6.3	Time Coordination Message	143
7.6.4	Time correction message	144
7.6.5	Safety data production	144
7.6.6	Producer dynamic variables	151
7.6.7	Producer per consumer dynamic variables	153
7.6.8	Consumer data variables	155
7.6.9	Consumer input static variables	157
7.6.10	Consumer dynamic variables	157
8	Safety communication layer management	159
8.1	Overview	159
8.2	Definition of the measures used during connection establishment	160
8.3	Originator-Target relationship validation	163
8.4	Detection of mis-routed connection requests	164
8.5	SafetyOpen processing	164
8.6	Ownership management	165
8.7	Bridging different physical layers	166
8.8	Safety connection establishment	167
8.8.1	Overview	167
8.8.2	Basic facts for connection establishment	167
8.8.3	Configuring safety connections	168
8.8.4	Network time expectation multiplier	169
8.8.5	Establishing connections	171
8.8.6	Recommendations for consumer number allocation	173
8.8.7	Recommendations for connection establishment	174
8.8.8	Ownership establishment	174
8.8.9	Ownership use cases	175
8.8.10	PID/CID usage and establishment	178
8.8.11	Proper PID/CID usage in multipoint and point-to-point connections	178
8.8.12	Network supported services	180
8.8.13	FSCP 2/1 Safety device type	181
8.9	Safety configuration process	185
8.9.1	Introduction to safety configuration	185
8.9.2	Configuration goals	185
8.9.3	Configuration overview	186
8.9.4	User configuration guidelines	187
8.9.5	Configuration process SIL3 justification	188
8.9.6	Device functions for tool configuration	189
8.9.7	Password security	189

8.9.8	SNCT interface services	189
8.9.9	Configuration lock.....	189
8.9.10	Effect of configuration lock on device behavior	190
8.9.11	Configuration ownership	191
8.9.12	Configuration mode	191
8.9.13	Measures used to ensure integrity of configuration process	191
8.9.14	Download process	193
8.9.15	Verification process	196
8.9.16	Verification process	199
8.9.17	Configuration error analysis.....	200
8.10	Electronic Data Sheets extensions for safety	203
8.10.1	General rules for EDS based safety devices	203
8.10.2	EDS extensions for safety	204
9	System requirements.....	208
9.1	Indicators and switches	208
9.1.1	General indicator requirements.....	208
9.1.2	LED indications for setting the device UNID.....	208
9.1.3	Module Status LED.....	209
9.1.4	Indicator warning	209
9.1.5	Network Status LED.....	209
9.1.6	MACID determination.....	211
9.1.7	Reset switch.....	212
9.2	Installation guidelines.....	213
9.3	Safety function response time	213
9.3.1	Overview.....	213
9.3.2	Network time expectation	213
9.3.3	Equations for calculating network reaction times	214
9.4	Duration of demands	216
9.5	Constraints for calculation of system characteristics	216
9.5.1	Number of nodes	216
9.5.2	Network PFH	216
9.5.3	Bit Error Rate (BER)	218
9.6	Maintenance.....	219
9.7	Safety manual	219
10	Certification.....	219
Annex A (informative) Additional information for functional safety communication profiles of CPF 2.....		220
A.1 Hash function example code.....		220
Bibliography.....		232
Table 1 – Communications errors and detection measures matrix.....		25
Table 2 – New class attributes		27
Table 3 – Service extensions		28
Table 4 – SafetyOpen and SafetyClose response format		28
Table 5 – Safety network segment identifier.....		31
Table 6 – Safety network segment definition		31
Table 7 – Safety network segment router format		33

Table 8 – Multipoint producer parameter evaluation rules	36
Table 9 – ForwardOpen setting options for safety connections.....	38
Table 10 – Network connection parameters for safety connections	39
Table 11 – CP 2/3 Safety target application reply (size: 10 octets).....	40
Table 12 – SafetyOpen target application reply (size: 16 octets)	40
Table 13 – New and extended error codes for safety	41
Table 14 – SafetyOpen error event guidance table.....	42
Table 15 – Identity object common service changes	43
Table 16 – New DeviceNet object instance attribute	44
Table 17 – New TCP/IP Interface object Instance Attribute	44
Table 18 – Safety Supervisor class attributes	45
Table 19 – Safety Supervisor instance attributes	46
Table 20 – Device status attribute state values	50
Table 21 – Exception status attribute format	50
Table 22 – Common exception detail attribute values	51
Table 23 – Exception detail format summary.....	52
Table 24 – Summary of device behavior for various CFUNID values	54
Table 25 – Safety Supervisor common services	56
Table 26 – Safety Supervisor object specific services	56
Table 27 – Configure_Request message structure	58
Table 28 – Validate_Configuration message structure.....	58
Table 29 – Validate_Configuration success message structure	58
Table 30 – Validate_Configuration error code	59
Table 31 – Validate_Configuration extended codes	59
Table 32 – Set_Password message structure.....	61
Table 33 – Reset_Password message structure	61
Table 34 – Configuration_Lock/Unlock message structure	62
Table 35 – Mode_Change message structure	62
Table 36 – Safety_Reset message structure	63
Table 37 – Safety Supervisor safety reset types	63
Table 38 – Attribute bit map parameter	63
Table 39 – Reset processing rules for rest types.....	64
Table 40 – Propose_TUNID service	64
Table 41 – Apply_TUNID service	65
Table 42 – Safety Supervisor events.....	67
Table 43 – State event matrix for Safety Supervisor.....	68
Table 44 – Configuration owner control vs. device state.....	71
Table 45 – State mapping of Safety Supervisor to Identity object	72
Table 46 – Safety Supervisor object event mapping	72
Table 47 – Identity object event mapping	73
Table 48 – Safety Validator class attributes	74
Table 49 – Safety Validator instance attributes	74
Table 50 – Safety Validator state assignments.....	77

Table 51 – Safety Validator type, bit field assignments	77
Table 52 – Multipoint producer SafetyOpen parameter evaluation rules	79
Table 53 – Safety Validator class services	80
Table 54 – Safety Validator instance services	80
Table 55 – Safety Validator Get_Attributes_All service data	81
Table 56 – Safety Validator state event matrix	83
Table 57 – State mapping between Safety Supervisor and Safety Validator objects	84
Table 58 – Connection configuration object class attribute extensions	84
Table 59 – Connection Configuration Object instance attribute additions/extensions	85
Table 60 – Connection flag bit definitions	87
Table 61 – O-to-T connection parameters	88
Table 62 – T-to-O connection parameters	89
Table 63 – Data map formats	90
Table 64 – Data map format 0	91
Table 65 – Data map format 1	91
Table 66 – Target device's SCCRC values	93
Table 67 – Target device's SCTS values	94
Table 68 – Time correction connection parameters for multipoint connection	94
Table 69 – Connection Configuration Object-specific services	95
Table 70 – Get_Attributes_All Response service data (added attributes)	96
Table 71 – Set_Attributes_All Request service data (added attributes)	96
Table 72 – State Mapping between Safety Supervisor and the CCO objects	97
Table 73 – Connection sections and PDU formats	99
Table 74 – Mode octet variables	100
Table 75 – Time Stamp variables	102
Table 76 – Time Coordination message variables	103
Table 77 – Time Correction Message variables	105
Table 78 – CRC polynomials used	108
Table 79 – Connection sections and message formats	109
Table 80 – Data reception - Link triggered	134
Table 81 – Time_Correction reception - Link triggered	135
Table 82 – Data reception - Application triggered	135
Table 83 – Time_Correction reception - Application triggered	135
Table 84 – Consuming application – Safety data monitoring	136
Table 85 – Producer connection status determination	145
Table 86 – Consuming safety connection status	155
Table 87 – Connection establishment errors and measures to detect errors	160
Table 88 – SNN Date/Time allocations	161
Table 89 – SNN legal range of time values	161
Table 90 – Safety connection parameters	169
Table 91 – SafetyOpen summary	171
Table 92 – Originator/Target service mapping	182
Table 93 – Unsupported originator/target service types	182

Table 94 – Configuration goals	186
Table 95 – Configuration owner control vs. device state.....	191
Table 96 – Errors and detection measures	200
Table 97 – Parameter class keywords.....	205
Table 98 – New Connection Manager section keywords for safety	205
Table 99 – Connection Manager field usage for safety	206
Table 100 – Connection parameter field settings for safety	207
Table 101 – LED indications for setting UNID	208
Table 102 – Module Status LED.....	209
Table 103 – Network status LED states	210
Table 104 – Connection reaction time type – producing/consuming applications.....	214
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	24
Figure 4 – Communication layers.....	26
Figure 5 – ForwardOpen with safety network segment.....	30
Figure 6 – Safety network target format.....	32
Figure 7 – Target Processing SafetyOpen with no configuration data (Form 2 SafetyOpen)	34
Figure 8 – Target Processing for SafetyOpen with configuration data (Form 1 SafetyOpen)	35
Figure 9 – Applying device configuration.....	59
Figure 10 – Configure and Validate processing flowcharts	60
Figure 11 – UNID handling during “Waiting for TUNID”	66
Figure 12 – Safety Supervisor state diagram.....	67
Figure 13 – Configuration, testing and locked relationships.....	71
Figure 14 – Safety connection types	78
Figure 15 – Safety Validator state transition diagram	82
Figure 16 – Connection Configuration Object state diagram.....	97
Figure 17 – Connection Configuration Object data flow.....	98
Figure 18 – Format of the mode octet	99
Figure 19 – 1 or 2 octet data section.....	100
Figure 20 – 3 to 250 octet data section format	101
Figure 21 – Time Stamp section format.....	102
Figure 22 – Time Coordination message encoding.....	103
Figure 23 – Time Correction message encoding	104
Figure 24 – 1 or 2 octet point-to-point PDU encoding.....	106
Figure 25 – 1 or 2 Octet multipoint PDU encoding.....	106
Figure 26 – 1 or 2 Octet, multipoint, Format 2 safety connection format	107
Figure 27 – 3 to 250 Octet Point-to-point PDU encoding	107
Figure 28 – 3 to 248 Octet Multipoint PDU encoding	107
Figure 29 – 3 to 248 Octet, Multipoint, safety connection format	108

Figure 30 – Time stamp sequence	110
Figure 31 – Sequence diagram of a normal producer/consumer safety sequence.....	111
Figure 32 – Sequence diagram of a normal producer/consumer safety sequence (production repeated)	112
Figure 33 – Sequence diagram of a corrupted producer to consumer message	113
Figure 34 – Sequence diagram of a lost producer to consumer message	114
Figure 35 – Sequence diagram of a delayed message	115
Figure 36 – Sequence diagram of a corrupted producer to consumer message with production repeated	116
Figure 37 – Sequence diagram of a connection terminated due to delays	117
Figure 38 – Sequence diagram of a failure of safety CRC check	117
Figure 39 – Sequence diagram of a point-to-point ping - normal response	118
Figure 40 – Sequence diagram of a successful multipoint ping, CP 2/3 safety	119
Figure 41 – Sequence diagram of a successful multipoint ping, CP 2/2 safety	120
Figure 42 – Sequence diagram of a multipoint ping retry	121
Figure 43 – Sequence diagram of a multipoint ping timeout	121
Figure 44 – Safety device reference model entity relation diagram	122
Figure 45 – Two devices interchanging safety data via a SafetyValidatorClient and a SafetyValidatorServer	123
Figure 46 – Safety production data flow	124
Figure 47 – Consumer safety data monitoring	133
Figure 48 – SafetyValidatorServer - application triggered	133
Figure 49 – Target ownership	164
Figure 50 – SafetyOpen forms	165
Figure 51 – Connection ownership state chart	165
Figure 52 – SafetyOpen UNID mapping	166
Figure 53 – Common CPF 2 application layer	166
Figure 54 – End-to-End routing example	167
Figure 55 – Sources for safety related connection parameters	170
Figure 56 – Parameter mapping between originator and target	170
Figure 57 – CP 2/3 Safety connection establishment in targets for Form 2a SafetyOpen	172
Figure 58 – General sequence to detect configuration is required	173
Figure 59 – PID/CID exchanges for two originator scenarios	178
Figure 60 – Seed generation for multipoint connections	179
Figure 61 – PID/CID runtime handling	180
Figure 62 – Connection categories and supported services	183
Figure 63 – Recommended connection types	184
Figure 64 – Logic-to-logic supported services	184
Figure 65 – Recommended connection types for logic to logic	185
Figure 66 – Configuration data transfers	186
Figure 67 – Protection measures in safety devices	188
Figure 68 – Configuration, testing and locked relationships	190
Figure 69 – Originator's configuration data	192
Figure 70 – SNCT to device download process	194

Figure 71 – SNCT Downloads to originators that perform Form 1 configuration	195
Figure 72 – Protection from locking and ownership	197
Figure 73 – Example of read back and comparison of original and printout	198
Figure 74 – Diverse display without full data read back	199
Figure 75 – Verification process including all alternatives	199
Figure 76 – Safety device MACID processing logic	212
Figure 77 – Safety function response time	213
Figure 78 – Safety function response time components	215
Figure 79 – Network protocol reliability block diagram (RBD)	216
Figure 80 – Network PFH summary	218

Withdrawn

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 Property 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.

This bilingual version (2013-07) corresponds to the monolingual English version, published in 2007-12.

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.

The French version of this standard has not been voted upon.

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.

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.

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.

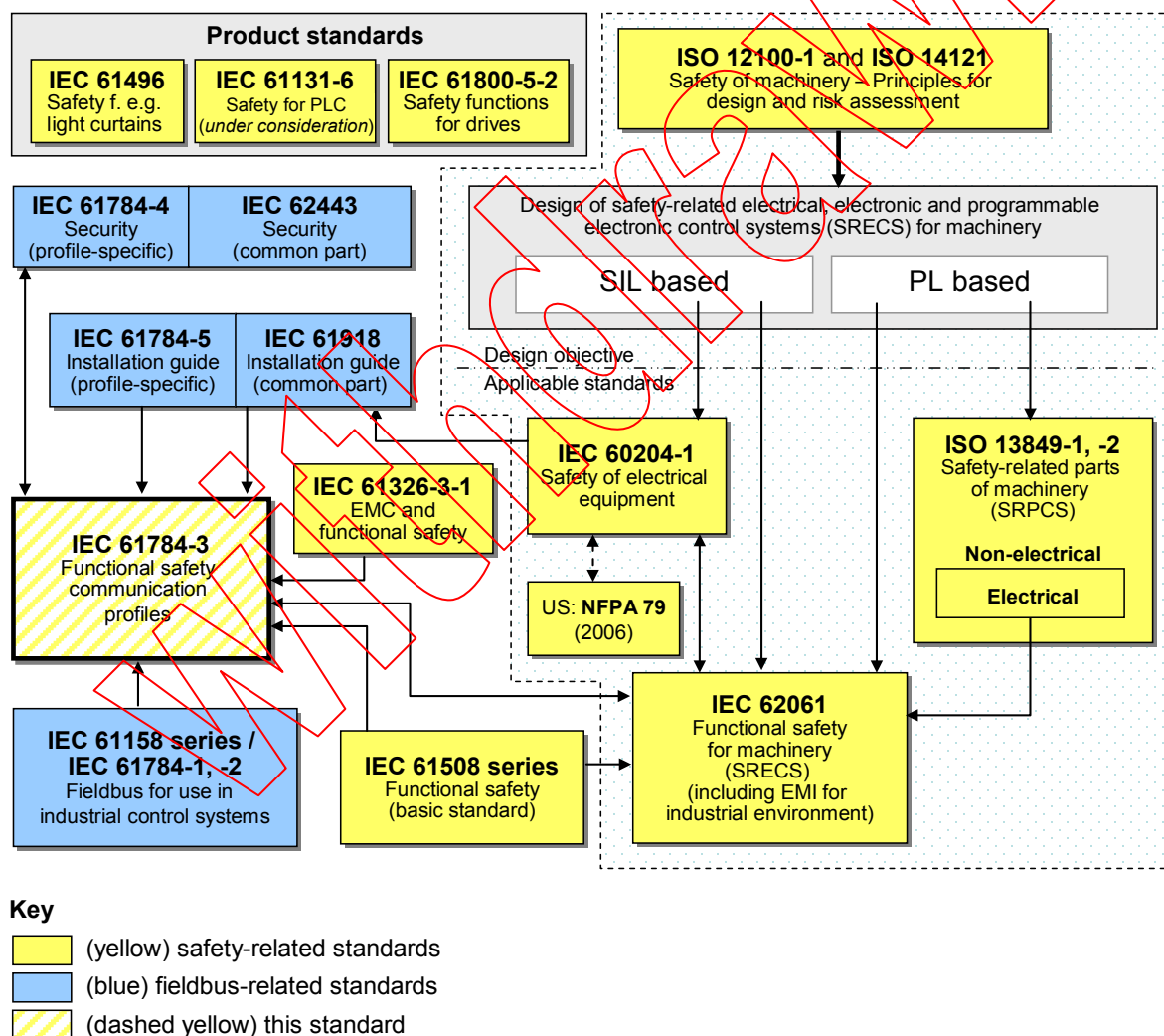
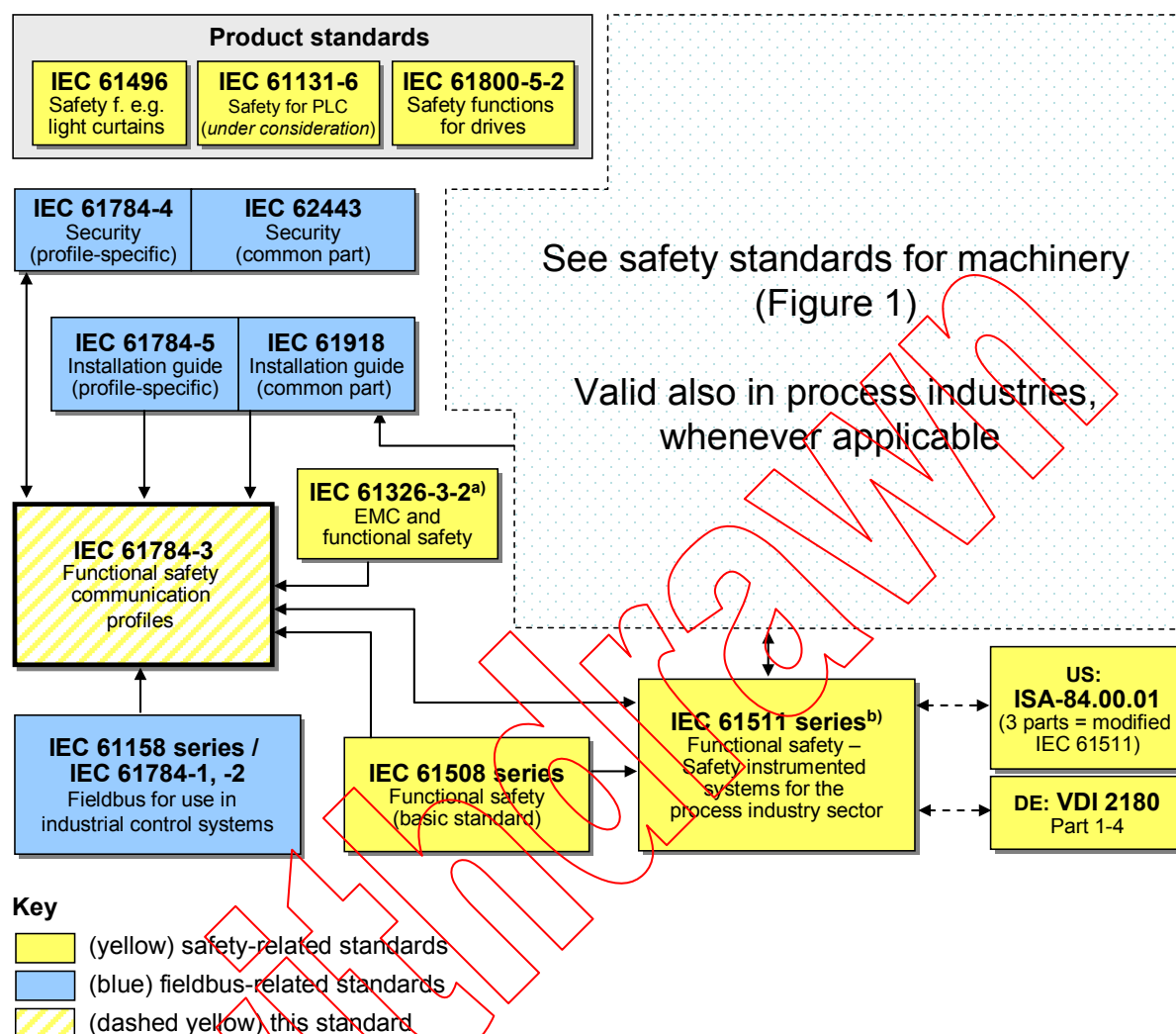


Figure 1 – Relationships of IEC 61784-3 with other standards (machinery)

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.

Withdrawn

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.

SOMMAIRE

AVANT-PROPOS	243
INTRODUCTION	245
1 Domaine d'application	249
2 Références normatives	249
3 Termes, définitions, symboles, abréviations et conventions	251
3.1 Termes et définitions	251
3.1.1 Termes et définitions communs	251
3.1.2 CPF 2: Termes et définitions supplémentaires	255
3.2 Symboles et abréviations	255
3.2.1 Symboles et abréviations communs	255
3.2.2 CPF 2: Symboles et abréviations supplémentaires	255
3.3 Conventions	256
4 Présentation générale du FSCP 2/1 (CIP Safety™)	257
4.1 Généralités	257
4.2 FSCP 2/1	257
5 Généralités	258
5.1 Documents externes de spécifications applicables au profil	258
5.2 Exigences fonctionnelles de sécurité	259
5.3 Mesures de sécurité	259
5.4 Structure de la couche de communication de sécurité	260
5.5 Relations avec la FAL (et DLL, PhL)	261
5.5.1 Généralités	261
5.5.2 Types de données	261
6 Services de la couche de communication de sécurité	261
6.1 Introduction	261
6.2 Objet de connexion	261
6.2.1 Généralités	261
6.2.2 Extensions des attributs des classes	261
6.2.3 Extensions de services	262
6.2.4 Format de réponse de messages explicites pour SafetyOpen et SafetyClose	263
6.3 Objet Gestionnaire de connexion	263
6.3.1 Généralités	263
6.3.2 ForwardOpen pour la sécurité	264
6.3.3 Segment de réseau de sécurité	266
6.3.4 Règles du point d'origine pour le calcul du CRC de paramètre de connexion	268
6.3.5 Organigrammes de traitement de SafetyOpen	268
6.3.6 Contrôles requis par les producteurs multipoint avec les connexions existantes	272
6.3.7 Utilisation de la clé électronique de sécurité	273
6.3.8 RPI en fonction de API dans les connexions de sécurité	273
6.3.9 Élaboration du chemin d'application de sécurité	273
6.3.10 Types de connexion de l'objet de validation de sécurité	275
6.3.11 Données de réponse d'application dans une réponse SafetyOpen satisfaisante	277

6.3.12	Réponse SafetyOpen non satisfaisante	277
6.3.13	Service ForwardClose de sécurité	280
6.4	Objet Identité	280
6.4.1	Généralités.....	280
6.4.2	Modifications apportées aux services communs.....	280
6.5	Objets de liaison	281
6.5.1	Modifications apportées à l'objet DeviceNet.....	281
6.5.2	Modifications apportées à l'objet Interface TCP/IP	281
6.6	Objet Programme de contrôle de sécurité.....	282
6.6.1	Généralités.....	282
6.6.2	Attributs de classe de programme de contrôle de sécurité	282
6.6.3	Sous-classes	283
6.6.4	Attributs instance de programme de contrôle de sécurité.....	283
6.6.5	Sémantique	286
6.6.6	Sous-classes	293
6.6.7	Services communs du programme de contrôle de sécurité.....	294
6.6.8	Comportement du Programme de contrôle de sécurité.....	307
6.7	Objet de validation de sécurité	316
6.7.1	Généralités.....	316
6.7.2	Attributs de classe	316
6.7.3	Attributs instance.....	317
6.7.4	Services de classes.....	323
6.7.5	Services instance	323
6.7.6	Comportement d'objet	324
6.8	Objet de configuration de connexion.....	328
6.8.1	Généralités.....	328
6.8.2	Extensions d'attributs de classe.....	328
6.8.3	Attributs, ajouts et extensions instance.....	328
6.8.4	Extensions ou restrictions de sémantique des attributs instance pour des raisons de sécurité.....	331
6.8.5	Paramètres spéciaux relatifs à la sécurité – (Attribut 13)	336
6.8.6	Services spécifiques à l'objet.....	340
6.8.7	Extensions des services communs pour la sécurité	341
6.8.8	Comportement d'objet	342
7	Protocole de couche de communication de sécurité.....	344
7.1	Format PDU de sécurité	344
7.1.1	Codage PDU de sécurité	344
7.1.2	CRC de sécurité	355
7.2	Comportement du protocole de communication	356
7.2.1	Séquence des contrôles de sécurité	356
7.2.2	Terminaison de connexion.....	356
7.2.3	Erreur de contre vérification	357
7.3	Opération de datation.....	357
7.4	Diagrammes séquentiels de protocoles	358
7.4.1	Généralités.....	358
7.4.2	Transmission de sécurité normale	358
7.4.3	Transmission de messages perdus, corrompus et retardés.....	360
7.4.4	Transmission de messages perdus, corrompus ou retardés avec production répétée	363

7.4.5	Demande Ping point à point.....	366
7.4.6	Demande Ping multipoint avec sécurité CP 2/3.....	367
7.4.7	Demande Ping multipoint sur les réseaux de sécurité CP 2/2	369
7.4.8	Demande Ping multipoint – Retransmission aboutie	371
7.4.9	Demande Ping multipoint – Retransmission avec temporisation.....	371
7.5	Définition du protocole de sécurité	372
7.5.1	Généralités.....	372
7.5.2	Vue de haut niveau d'un dispositif de sécurité	373
7.5.3	Objet de validation de sécurité	374
7.5.4	Relations entre SafetyValidatorServer et SafetyValidatorClient.....	374
7.5.5	Définition de la fonction SafetyValidatorClient	376
7.5.6	Définition de la fonction SafetyValidatorServer	384
7.6	Spécifications des messages de sécurité et des données de protocole.....	395
7.6.1	Octet de mode.....	395
7.6.2	Section de datation.....	396
7.6.3	Message de coordination temporelle	396
7.6.4	Message de correction de temps	396
7.6.5	Production des données de sécurité.....	397
7.6.6	Variables dynamiques du producteur.....	404
7.6.7	Variables dynamiques de producteur par consommateur	407
7.6.8	Variables de données du consommateur.....	408
7.6.9	Variables statiques d'entrée du consommateur.....	410
7.6.10	Variables dynamiques du consommateur.....	411
8	Gestion de la couche de communication de sécurité.....	413
8.1	Présentation générale.....	413
8.2	Définition des mesures utilisées lors de l'établissement d'une connexion	413
8.3	Validation de la relation point d'origine-cible	417
8.4	Détection des demandes de connexion mal acheminées	418
8.5	Traitement de SafetyOpen.....	418
8.6	Gestion de propriété.....	418
8.7	Pontage de différentes couches physiques.....	420
8.8	Établissement de connexion de sécurité.....	421
8.8.1	Présentation générale	421
8.8.2	Faits de base pour l'établissement d'une connexion	422
8.8.3	Configuration des connexions de sécurité.....	422
8.8.4	Multiplicateur de délai de réseau	423
8.8.5	Établissement de connexions	425
8.8.6	Recommandations pour l'attribution d'un nombre de consommateurs	428
8.8.7	Recommandations pour l'établissement d'une connexion	429
8.8.8	Établissement de propriété	430
8.8.9	Cas d'utilisation de la propriété	430
8.8.10	Utilisation et établissement de la relation PID/CID	433
8.8.11	Utilisation PID/CID correcte dans les connexions multipoint et point à point.....	434
8.8.12	Services pris en charge par le réseau.....	438
8.8.13	Type de dispositif de sécurité FSCP 2/1	438
8.9	Processus de configuration de sécurité	443
8.9.1	Introduction à la configuration de sécurité	443
8.9.2	Objectifs de configuration	443

8.9.3	Présentation générale de la configuration	444
8.9.4	Lignes directrices pour la configuration de l'utilisateur	445
8.9.5	Justification de niveau SIL3 du processus de configuration	446
8.9.6	Fonctions de dispositifs pour configuration par outil	447
8.9.7	Sécurité par mot de passe	447
8.9.8	Services d'interface SNCT	447
8.9.9	Verrouillage de configuration	448
8.9.10	Influence du verrouillage de configuration sur le comportement des dispositifs	448
8.9.11	Propriété de configuration	450
8.9.12	Mode de configuration	450
8.9.13	Mesures d'assurance de l'intégrité du processus de configuration	450
8.9.14	Processus de téléchargement aval	453
8.9.15	Processus de vérification	457
8.9.16	Processus de vérification	460
8.9.17	Analyse des erreurs de configuration	462
8.10	Extensions de fiches techniques électroniques à des fins de sécurité	466
8.10.1	Règles générales applicables aux dispositifs de sécurité EDS	466
8.10.2	Extensions EDS à des fins de sécurité	467
9	Exigences système	471
9.1	Voyants et commutateurs	471
9.1.1	Exigences générales concernant les voyants	471
9.1.2	Indications DEL pour le paramétrage de l'UNID des dispositifs	471
9.1.3	DEL Etat du module	472
9.1.4	Avertissement lié aux voyants	472
9.1.5	DEL Etat de réseau	472
9.1.6	Détermination du MACID	474
9.1.7	Commutateur de réinitialisation	476
9.2	Lignes directrices d'installation	476
9.3	Temps de réponse de la fonction de sécurité	476
9.3.1	Présentation générale	476
9.3.2	Délai du réseau	478
9.3.3	Equations de calcul des temps de réaction du réseau	478
9.4	Durée des demandes	481
9.5	Contraintes liées au calcul des caractéristiques du système	481
9.5.1	Nombre de nœuds	481
9.5.2	PFH de réseau	481
9.5.3	Taux d'erreurs sur les bits (BER)	483
9.6	Maintenance	484
9.7	Manuel de sécurité	484
10	Certification	484
Annexe A (informative) Informations supplémentaires pour les profils de communication de sécurité fonctionnelle de la CPF 2		485
A.1 Exemple de code de fonction de hachage		485
Bibliographie		497

Tableau 1 – Erreurs de communication et matrice de mesures de détection..... 259

Tableau 2 – Nouveaux attributs de classe..... 261

Tableau 3 – Extensions de services	263
Tableau 4 – Format de réponse SafetyOpen et SafetyClose	263
Tableau 5 – Identifiant de segment de réseau de sécurité.....	266
Tableau 6 – Définition du segment de réseau de sécurité	266
Tableau 7 – Format de routage de segment de réseau de sécurité	268
Tableau 8 – Règles d'évaluation des paramètres de production multipoint.....	273
Tableau 9 – Options de paramétrage du service ForwardOpen pour les connexions de sécurité.....	275
Tableau 10 – Paramètres de connexion de réseau pour les connexions de sécurité.....	276
Tableau 11 – Réponse d'application de cible de sécurité CP 2/3 (taille: 10 octets)	277
Tableau 12 – Réponse d'application de cible SafetyOpen (taille: 16 octets)	277
Tableau 13 – Nouveaux codes d'erreurs étendus de sécurité.....	278
Tableau 14 – Tableau de recommandations concernant les événements d'erreur SafetyOpen.....	279
Tableau 15 – Modifications apportées aux services communs de l'objet Identité	280
Tableau 16 – Nouvel attribut instance de l'objet DeviceNet.....	281
Tableau 17 – Nouvel attribut instance de l'objet Interface TCP/IP	281
Tableau 18 – Attributs de classe de programme de contrôle de sécurité	283
Tableau 19 – Attributs instance de programme de contrôle de sécurité.....	283
Tableau 20 – Valeurs d'indication de l'attribut Etat du dispositif	287
Tableau 21 – Format de l'attribut Etat d'exception	288
Tableau 22 – Valeurs communes de l'attribut Détail d'exception	289
Tableau 23 – Synthèse du format de détail d'exception.....	290
Tableau 24 – Synthèse du comportement des dispositifs pour diverses valeurs CFUNID	292
Tableau 25 – Services communs du programme de contrôle de sécurité.....	294
Tableau 26 – Services spécifiques de l'objet Programme de contrôle de sécurité	294
Tableau 27 – Structure de message Configure_Request.....	296
Tableau 28 – Structure de message Validate_Configuration	297
Tableau 29 – Structure de message de réussite Validate_Configuration	297
Tableau 30 – Code d'erreur Validate_Configuration	297
Tableau 31 – Codes étendus Validate_Configuration	298
Tableau 32 – Structure de message Set_Password	300
Tableau 33 – Structure de message Reset_Password.....	301
Tableau 34 – Structure de message Configuration_Lock/Unlock	301
Tableau 35 – Structure de message Mode_Change	302
Tableau 36 – Structure de message Safety_Reset.....	302
Tableau 37 – Types de réinitialisation de sécurité du Programme de contrôle de sécurité.....	302
Tableau 38 – Paramètre d'attribut Mode point.....	303
Tableau 39 – Règles de traitement applicables aux types de réinitialisation.....	303
Tableau 40 – Service Propose_TUNID	304
Tableau 41 – Service Apply_TUNID	304
Tableau 42 – Événements liés au Programme de contrôle de sécurité	308

Tableau 43 – Matrice d'événements d'état du Programme de contrôle de sécurité	309
Tableau 44 – Contrôle du propriétaire de configuration par rapport à l'état du dispositif.....	314
Tableau 45 – Mise en correspondance des états du Programme de contrôle de sécurité et de l'objet Identité	314
Tableau 46 – Mise en correspondance des événements de l'objet Programme de contrôle de sécurité	315
Tableau 47 – Mise en correspondance des événements d'objet Identité	316
Tableau 48 – Attributs de classe de l'Objet de validation de sécurité	316
Tableau 49 – Attributs instance de l'Objet de validation de sécurité	317
Tableau 50 – Attributions d'états de l'Objet de validation de sécurité	319
Tableau 51 – Type d'Objet de validation de sécurité, attributions de champs de bits.....	319
Tableau 52 – Règles d'évaluation du paramètre SafetyOpen des producteurs multipoint.....	321
Tableau 53 – Services de classes de l'Objet de validation de sécurité.....	323
Tableau 54 – Services instance de l'Objet de validation de sécurité.....	323
Tableau 55 – Données du service Get_Attributes_All de l'Objet de Validation de sécurité.....	324
Tableau 56 – Matrice d'événements d'état de l'Objet de validation de sécurité	327
Tableau 57 – Mise en correspondance des états des objets Programme de contrôle de sécurité et Validation de sécurité	327
Tableau 58 – Extensions d'attributs de classe d'objet de configuration de connexion.....	328
Tableau 59 – Ajouts/extensions d'attributs instance d'Objet de configuration de connexion	329
Tableau 60 – Définitions des bits de drapeaux de connexion	331
Tableau 61 – Paramètres de connexion O-à-T	333
Tableau 62 – Paramètres de connexion T-à-O	334
Tableau 63 – Formats de mise en correspondance des données	335
Tableau 64 – Format 0 de mise en correspondance des données	336
Tableau 65 – Format 1 de mise en correspondance des données	336
Tableau 66 – Valeurs SCCRC du dispositif cible	339
Tableau 67 – Valeurs SCTS du dispositif cible.....	339
Tableau 68 – Paramètres de connexion de correction de temps pour une connexion multipoint.....	339
Tableau 69 – Services spécifiques à l'objet Configuration de connexion	340
Tableau 70 – Données du service de réponse Get_Attributes_All (attributs ajoutés)	341
Tableau 71 – Données du service de Demande Set_Attributes_All (attributs ajoutés)	342
Tableau 72 – Mise en correspondance des états des objets Programme de contrôle de sécurité et CCO	343
Tableau 73 – Sections de connexion et formats PDU	345
Tableau 74 – Variables de l'octet Mode	346
Tableau 75 – Variables de datation.....	348
Tableau 76 – Variables du message de coordination temporelle	349
Tableau 77 – Variables du message de correction de temps.....	350
Tableau 78 – Polynômes de CRC utilisés	355
Tableau 79 – Sections de connexion et formats de messages.....	356
Tableau 80 – Réception des données – Déclenchée par la liaison	387

Tableau 81 – Réception Time_Correction – Déclenchée par la liaison	387
Tableau 82 – Réception des données – Déclenchée par l'application.....	388
Tableau 83 – Réception de Time_Correction – Déclenchée par l'application	388
Tableau 84 – Application de consommation – Contrôle des données de sécurité	388
Tableau 85 – Détermination de l'état de la connexion du producteur.....	397
Tableau 86 – État de la connexion de sécurité de consommation.....	409
Tableau 87 – Erreurs d'établissement de connexion et mesures de détection des erreurs.....	413
Tableau 88 – Attributions de Date/Heure SNN	414
Tableau 89 – Plage légale SNN des valeurs temporelles	414
Tableau 90 – Paramètres de connexion de sécurité	423
Tableau 91 – Récapitulatif SafetyOpen	426
Tableau 92 – Mise en correspondance des services point d'origine/cible	439
Tableau 93 – Types de service point d'origine/cible non pris en charge	439
Tableau 94 – Objectifs de configuration	443
Tableau 95 – Contrôle du propriétaire de configuration par rapport à l'état du dispositif.....	450
Tableau 96 – Erreurs et mesures de détection	462
Tableau 97 – Mot clés de classes de paramètres.....	467
Tableau 98 – Nouveaux mots clés de la section Gestionnaire de connexion à des fins de sécurité.....	468
Tableau 99 – Utilisation du champ Gestionnaire de connexion à des fins de sécurité.....	469
Tableau 100 – Paramétrages du champ de paramètres de connexion à des fins de sécurité.....	470
Tableau 101 – Indications DEL pour le paramétrage de l'UNID	471
Tableau 102 – DEL Etat du module.....	472
Tableau 103 – Etats de la DEL Etat du réseau.....	473
Tableau 104 – Type de temps de réaction de connexion – applications de production/consommation	479
Figure 1 – Relations entre la CEI 61784-3 et d'autres normes (machines).....	246
Figure 2 – Relations entre la CEI 61784-3 et d'autres normes (transformation)	248
Figure 3 – Relation des objets de validation de sécurité.....	258
Figure 4 – Couches de communication	260
Figure 5 – ForwardOpen avec segment de réseau de sécurité	266
Figure 6 – Format cible de réseau de sécurité	267
Figure 7 – Service SafetyOpen de traitement de cible sans données de configuration (SafetyOpen de forme 2).....	270
Figure 8 – Service SafetyOpen de traitement de cible avec données de configuration (SafetyOpen de forme 1).....	272
Figure 9 – Application de configuration de dispositif	298
Figure 10 – Organigrammes de traitement de Configuration et Validation	300
Figure 11 – Traitement UNID pendant l'état "Waiting for TUNID".....	307
Figure 12 – Diagramme d'états du Programme de contrôle de sécurité	308
Figure 13 – Relations entre configuration, essais et verrouillage.....	313

Figure 14 – Types de connexion de sécurité	321
Figure 15 – Diagramme de transition d'état de l'Objet de validation de sécurité	326
Figure 16 – Diagramme d'états de l'objet Configuration de connexion.....	343
Figure 17 – Flux de données de l'objet Configuration de connexion	344
Figure 18 – Format de l'octet Mode.....	345
Figure 19 – Section de données à 1 ou 2 octets.....	346
Figure 20 – Format de section de données de 3 à 250 octets	347
Figure 21 – Format de section de datation	347
Figure 22 – Codage du message de coordination temporelle	348
Figure 23 – Codage du message de correction de temps	350
Figure 24 – Codage PDU point à point à 1 ou 2 octets	351
Figure 25 – Codage PDU multipoint à 1 ou 2 octets	352
Figure 26 – Format de connexion de sécurité de format 2 multipoint à 1 ou 2 octets.....	353
Figure 27 – Codage PDU point à point de 3 à 250 octets	353
Figure 28 – Codage PDU multipoint de 3 à 248 octets	354
Figure 29 – Format de connexion de sécurité multipoint de 3 à 248 octets.....	355
Figure 30 – Séquence de datation	357
Figure 31 – Diagramme d'une séquence de sécurité producteur/consommateur normale	359
Figure 32 – Diagramme d'une séquence de sécurité producteur/consommateur normale (production répétée).....	360
Figure 33 – Diagramme séquentiel d'un message producteur vers consommateur corrompu	361
Figure 34 – Diagramme séquentiel d'un message producteur vers consommateur perdu	362
Figure 35 – Diagramme séquentiel d'un message retardé	363
Figure 36 – Diagramme séquentiel d'un message producteur vers consommateur corrompu avec production répétée	364
Figure 37 – Diagramme séquentiel d'une terminaison de connexion occasionnée par des retards	365
Figure 38 – Diagramme séquentiel d'un contrôle CRC de sécurité non satisfait	366
Figure 39 – Diagramme séquentiel d'une demande Ping point à point – réponse normale	367
Figure 40 – Diagramme séquentiel d'une demande Ping multipoint satisfaisante, sécurité CP 2/3	369
Figure 41 – Diagramme séquentiel d'une demande Ping multipoint satisfaisante, sécurité CP 2/2	370
Figure 42 – Diagramme séquentiel d'une retransmission de demande Ping multipoint	371
Figure 43 – Diagramme séquentiel d'une temporisation de demande Ping multipoint	372
Figure 44 – Diagramme de relations des entités de modèle de référence d'un dispositif de sécurité.....	374
Figure 45 – Deux dispositifs échangeant des données de sécurité via un SafetyValidatorClient et un SafetyValidatorServer.....	375
Figure 46 – Flux de données de production de sécurité	376
Figure 47 – Contrôle des données de sécurité de consommation	385
Figure 48 – SafetyValidatorServer – déclenché par l'application	386

Figure 49 – Propriété cible.....	417
Figure 50 – Formes SafetyOpen	418
Figure 51 – Diagramme d'états de la propriété de connexion	419
Figure 52 – Mise en correspondance de l'UNID de service SafetyOpen	420
Figure 53 – Couche application CPF 2 commune	420
Figure 54 – Exemple d'acheminement de bout en bout	421
Figure 55 – Sources des paramètres de connexion relative à la sécurité	424
Figure 56 – Mise en correspondance des paramètres entre le point d'origine et la cible.....	425
Figure 57 – Établissement d'une connexion de sécurité CP 2/3 dans les cibles pour un service SafetyOpen de forme 2a	427
Figure 58 – Séquence générale de détection de la nécessité d'une configuration	428
Figure 59 – Echanges PID/CID pour deux scénarios de point d'origine	434
Figure 60 – Génération des valeurs de marquage pour les connexions multipoint	436
Figure 61 – Traitement d'exécution PID/CID	438
Figure 62 – Catégories de connexion et services pris en charge	440
Figure 63 – Types de connexion recommandés	441
Figure 64 – Services pris en charge logique à logique	442
Figure 65 – Types de connexion recommandés pour les services logique à logique.....	443
Figure 66 – Transferts de données de configuration	444
Figure 67 – Mesures de protection des dispositifs de sécurité.....	446
Figure 68 – Relations entre configuration, essais et verrouillage.....	449
Figure 69 – Données de configuration du point d'origine.....	451
Figure 70 – Processus de téléchargement aval du SNCT au dispositif	455
Figure 71 – Téléchargements aval du SNCT vers les points d'origine qui réalisent la configuration de forme 1	456
Figure 72 – Protection contre le verrouillage et propriété	458
Figure 73 – Exemple de relecture et de comparaison du point d'origine et de l'exemplaire	459
Figure 74 – Affichage divers sans relecture complète des données.....	460
Figure 75 – Processus de vérification comprenant toutes les méthodes alternatives	462
Figure 76 – Logique de traitement du MACID des dispositifs de sécurité	476
Figure 77 – Temps de réponse de la fonction de sécurité	477
Figure 78 – Composantes du temps de réponse de la fonction de sécurité	480
Figure 79 –Schéma de principe de fiabilité de protocole de réseau (RBD)	481
Figure 80 – Synthèse de la PFH de réseau	483

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 (CEI) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de la CEI). La CEI 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, la CEI – 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 la CEI"). 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 la CEI, participent également aux travaux. La CEI 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 la CEI concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de la CEI intéressés sont représentés dans chaque comité d'études.
- 3) Les Publications de la CEI se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de la CEI. Tous les efforts raisonnables sont entrepris afin que la CEI s'assure de l'exactitude du contenu technique de ses publications; la CEI 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 la CEI s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de la CEI dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de la CEI et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
- 5) La CEI 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 la CEI. La CEI 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 la CEI, 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 la CEI, 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 la CEI ou de toute autre Publication de la CEI, 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 la CEI peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. La CEI ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et de ne pas avoir signalé leur existence.

La commission électrotechnique internationale (CEI) attire l'attention sur le fait qu'il est déclaré que la conformité avec le présent document peut impliquer l'utilisation de brevets concernant les profils de communication de sécurité fonctionnelle pour la famille 2, où la notation [xx] désigne le détenteur des droits de propriété.

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

contrôler using data manipulation techniques

La CEI ne prend pas position eu égard à la preuve, la validité et la portée de ces droits de propriété.

Les détenteurs de ces droits de propriété ont donné l'assurance à la CEI qu'ils consentent à négocier des licences avec des demandeurs du monde entier, en des termes et à des conditions raisonnables et non discriminatoires. A ce propos, la déclaration des détenteurs de ces droits de propriété est enregistrée à la CEI.

Des informations peuvent être obtenues auprès de:

[RA] Rockwell Automation, Inc.
1201 S. Second Street
Milwaukee, WI 53204
USA
Contact: Département de la propriété intellectuelle.

L'attention est attirée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété autres que ceux mentionnés ci-dessus. La CEI ne saurait être tenue pour responsable de ne pas avoir dûment signalé tout ou partie de ces droits de propriété.

La Norme internationale CEI 61784-3-2 a été établie par le sous-comité 65C: Réseaux de communication industriels, du comité d'études 65 de la CEI: Mesure, commande et automation dans les processus industriels.

La présente version bilingue (2013-06) correspond à la version anglaise monolingue publiée en 2007-12.

Le texte anglais de cette norme est issu des documents 65C/470/FDIS et 65C/481/RVD.

Le rapport de vote 65C/481/RVD donne toute information sur le vote ayant abouti à l'approbation de cette norme.

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

Cette publication a été rédigée selon les Directives ISO/CEI, Partie 2.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de stabilité indiquée sur le site web de la CEI sous "<http://webstore.iec.ch>" dans les données relatives à la publication recherchée. A cette date, la publication sera

- reconduite,
- supprimée,
- remplacée par une édition révisée, ou
- amendée.

La liste de toutes les parties de la série CEI 61784-3, présentées sous le titre général *Réseaux de communication industriels – Profils – Bus de terrain de sécurité fonctionnelle*, peut être consultée sur le site Web de la CEI.

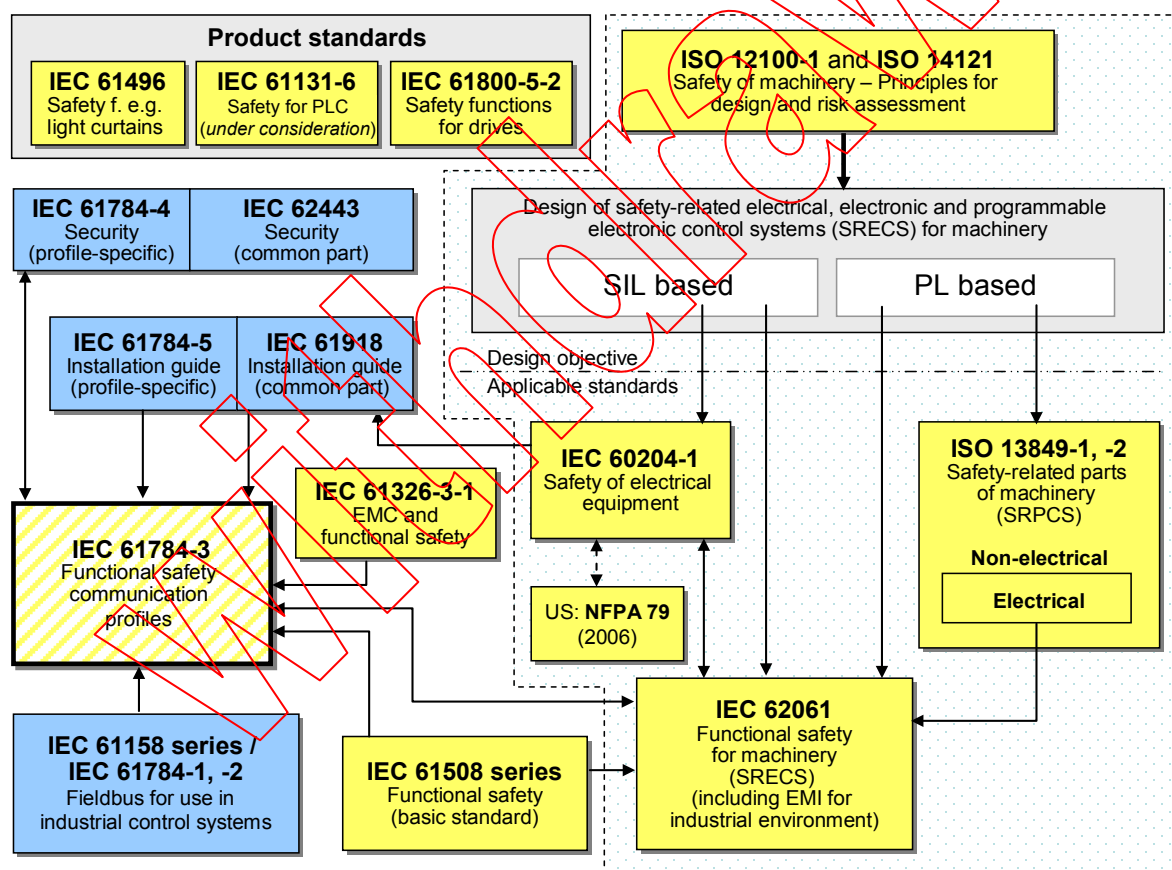
IMPORTANT – Le logo "colour inside" qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante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

INTRODUCTION

La CEI 61158 relative aux bus de terrain, ainsi que ses normes associées CEI 61784-1 et CEI 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. Ainsi de nombreuses améliorations des bus de terrain se développent pour traiter de domaines non encore normalisés tels que les applications en temps réel relatives à la sécurité et à la sûreté.

La présente norme définit les principes pertinents applicables aux communications en termes de sécurité fonctionnelle en référence à la série CEI 61508, et spécifie plusieurs couches de communication de sécurité (profils et protocoles correspondants) basées sur les profils de communication et les couches de protocoles de la CEI 61784-1, de la CEI 61784-2 et de la série CEI 61158. Elle ne couvre pas les aspects relatifs à la sécurité électrique et à la sécurité intrinsèque.

La Figure 1 illustre les relations entre la présente norme et les normes pertinentes relatives à la sécurité et au bus de terrain dans un environnement machines.



Key

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

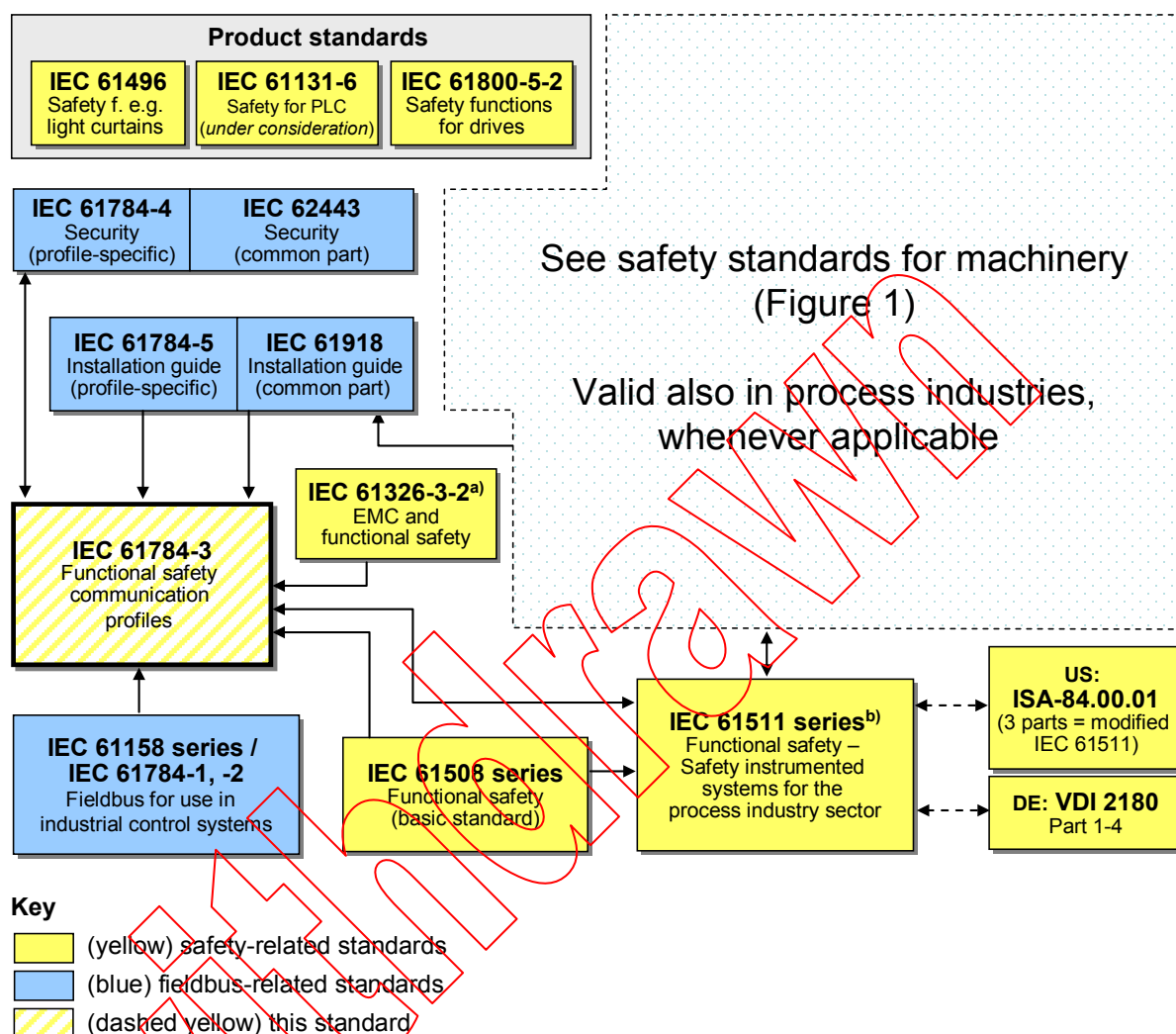
Légende

Anglais	Français
Product standards	Normes de produits

Anglais	Français
Safety function, e.g. light curtains	Fonction de sécurité, par exemple barrières photo électriques
Safety for PLC (under consideration)	Sécurité relative aux automates programmables (à l'étude)
Safety functions for drives	Fonctions de sécurité applicables aux entraînements
Safety requirements for robots	Exigences de sécurité applicables aux robots
Safety of machinery – Principles for design and risk assessment	Sécurité des machines – Principes généraux de conception et d'appréciation du risque
Security (profile-specific)	Sûreté (spécifique au profil)
Security (common part)	Sûreté (partie commune)
Design of safety-related electrical, electronic and programmable electronic control systems (SRECS) for machinery	Conception des systèmes de commande électriques, électroniques et électroniques programmables relatifs à la sécurité pour les machines
SIL based	Basé sur SIL
PL based	Basé sur PL
Installation guide (profile-specific)	Guide d'installation (spécifique au profil)
Installation guide (common part)	Guide d'installation (partie commune)
Design objective	Objectif de conception
Applicable standards	Normes applicables
Safety of electrical equipment	Sécurité des équipements électriques
Safety-related parts of machinery (SRPCS)	Parties des systèmes de commande relatives à la sécurité
Non-electrical	Non électrique
Electrical	Électrique
EMC and functional safety	Compatibilité électromagnétique et sécurité fonctionnelle
Functional safety communication profiles	Profils de communication de sécurité fonctionnelle
IEC 61158 series / IEC 61784-1,-2 Fieldbus for use in industrial control systems	Série CEI 61158 / CEI 61784-1,-2 Bus de terrain pour utilisation dans des systèmes de commande industriels
IEC 61508 series, Functional safety (basic standard)	Série CEI 61508 Sécurité fonctionnelle (norme de base)
Functional safety for machinery (SRECS) (including EMI for industrial environment)	Sécurité fonctionnelle des systèmes de commande électriques, électroniques et électroniques programmables (y compris les perturbations électromagnétiques dans l'environnement industriel)
Key	Légende
(yellow) safety-related standards	(jaune) normes relatives à la sécurité
(blue) fieldbus-related standards	(bleu) normes relatives au bus de terrain
(dashed) yellow) this standard	(jaunestrié) la présente norme

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

La Figure 2 illustre les relations entre la présente norme et les normes pertinentes relatives à la sécurité et au bus de terrain dans un environnement de transformation.



Légende

Anglais	Français
Product standards	Normes de produits
Safety f. e.g. light curtains	Fonction de sécurité, par exemple barrières photo électriques
Safety for PLC (under consideration)	Sécurité relative aux automates programmables (à l'étude)
Safety functions for drives	Fonctions de sécurité applicables aux entraînements
Safety requirements for robots	Exigences de sécurité applicables aux robots
Security (profile-specific)	Sûreté (spécifique au profil)
Security (common part)	Sûreté (partie commune)
Installation guide (profile-specific)	Guide d'installation (spécifique au profil)
Installation guide (common part)	Guide d'installation (partie commune)
See safety standards for machinery (Figure 1)	Voir normes de sécurité pour les machines (Figure 1)
Valid also in process industries, whenever applicable	Valable également dans les industries de transformation, le cas échéant
Functional safety communication profiles	Profils de communication de sécurité fonctionnelle

Anglais	Français
IEC 61326-3-2 ^{a)} EMC and functional safety	CEI 61326-3-2 ^{a)} CEM et sécurité fonctionnelle
IEC 61158 series/ IEC 61784-1,-2, Fieldbus for use in industrial control systems	Série CEI 61158/ CEI 61784-1,-2 Bus de terrain pour utilisation dans des systèmes de commande industriels
IEC 61508 series, Functional safety (basic standard)	Série CEI 61508 Sécurité fonctionnelle (norme de base)
IEC 61511 series ^{b)} Functional safety–safety instrumented systems for the process industry sector	Série CEI 61511 ^{b)} Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur des industries de transformation
US: ISA-84.00.01 (3 parts = modified IEC 61511)	US: ISA-84.00.01 (3 parties = CEI 61511 modifiée)
DE: VDI 2180 Part 1 –4	DE: VDI 2180 Parties 1 à 4
Key	Légende
(yellow) safety-related standards	(jaune) normes relatives à la sécurité
(blue) fieldbus-related standards	(bleu) normes relatives au bus de terrain
(dashed) yellow) this standard	(jaune strié) la présente norme

^a Pour des environnements électromagnétiques spécifiés, sinon CEI 61326-3-1.

^b EN ratifiée.

Figure 2 – Relations entre la CEI 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 la série CEI 61508, assurent la confiance nécessaire à accorder à la transmission de messages (information) entre deux participants ou plus 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 la présente norme permettent de garantir cette assurance en utilisant un bus de terrain dans des applications nécessitant 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 retenu au sein du système – la mise en œuvre du profil de communication de sécurité fonctionnelle dans un dispositif normal ne suffit pas à le qualifier de dispositif de sécurité.

La présente norme décrit:

- les principes de base de mise en œuvre des exigences de la série CEI 61508 pour les communications de données relatives à la sécurité, y compris les défauts de transmission potentiels, les mesures correctives et les considérations concernant l'intégrité des données;
- la description individuelle des profils de sécurité fonctionnelle pour plusieurs familles de profils de communication dans la CEI 61784-1 et la CEI 61784-2;
- les extensions de la couche de sécurité aux sections relatives au service et aux protocoles de communication de la série CEI 61158.

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 la série CEI 61784-3 spécifie une couche de communication relative à la sécurité (services et protocole) fondée sur la CPF 2 de la CEI 61784-1, la CEI 61784-2 et le Type 2 de la CEI 61158. Elle identifie les principes applicables aux communications de sécurité fonctionnelle définies dans la CEI 61784-3, et appropriées à cette couche de communication 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.

La présente partie¹ 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 CEI 61508 concernant la sécurité fonctionnelle. Ces mécanismes peuvent être utilisés dans diverses applications industrielles, telles que la commande de processus, l'usinage automatique et les machines.

La présente partie fournit des lignes directrices tant pour les développeurs que pour les évaluateurs de dispositifs et 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 du profil de communication de sécurité fonctionnelle, conforme à la présente partie, dans un dispositif normal ne suffit pas à le qualifier de dispositif de sécurité.

2 Références normatives

Les documents de référence suivants sont indispensables pour l'application 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, *Programmable controllers – Part 2: Equipment requirements and tests* (disponible uniquement en anglais)

IEC 61131-3, *Programmable controllers – Part 3: Programming languages* (disponible uniquement en anglais)

CEI 61158-2, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 2: Spécification de couche physique et définition des services*

IEC 61158-3-2, *Industrial communication networks – Fieldbus specifications – Part 3-2: Data-link layer service definition* (disponible uniquement en anglais)

IEC 61158-4-2, *Industrial communication networks – Fieldbus specifications – Part 4-2: Data-link layer protocol specification* (disponible uniquement en anglais)

¹ Dans les pages suivantes de la présente norme, "la présente partie" se substitue à "cette partie de la série CEI 61784-3".

IEC 61158-5-2, *Industrial communication networks – Fieldbus specifications – Part 5-2: Application layer service definition* (disponible uniquement en anglais)

IEC 61158-6-2, *Industrial communication networks – Fieldbus specifications – Part 6-2: Application layer protocol specification* (disponible uniquement en anglais)

CEI 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*²

CEI 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*²

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

CEI 61784-1, *Réseaux de communications industriels – Profils – Partie 1: Profils de bus de terrain*

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

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

IEC 61784-5-2, *Industrial communication networks – Profiles – Part 5: Installation of fieldbuses – Installation profiles for CPF 2* (disponible uniquement en anglais)

IEC 61918, *Industrial communication networks – Installation of communication networks in industrial premises* (disponible uniquement en anglais)

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

ISO 15745-2, *Systèmes d'automatisation industrielle et intégration – Cadres d'intégration d'application pour les systèmes ouverts – Partie 2: Description de référence pour les systèmes de contrôle fondés sur l'ISO 11898*

ISO 15745-3, *Systèmes d'automatisation industrielle et intégration – Cadres d'intégration d'application pour systèmes ouverts – Partie 3: Description de référence pour les systèmes de contrôle fondés sur la CEI 61158*

ISO 15745-4, *Systèmes d'automatisation industrielle et intégration – Cadres d'intégration d'application pour les systèmes ouverts – Partie 4: Description de référence pour les systèmes de contrôle fondés sur Ethernet*

² A publier.