

# 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**



**THIS PUBLICATION IS COPYRIGHT PROTECTED**  
**Copyright © 2016 IEC, Geneva, Switzerland**

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'IEC ou du Comité national de l'IEC du pays du demandeur. Si vous avez des questions sur le copyright de l'IEC ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de l'IEC de votre pays de résidence.

IEC Central Office  
3, rue de Varembe  
CH-1211 Geneva 20  
Switzerland

Tel.: +41 22 919 02 11  
Fax: +41 22 919 03 00  
[info@iec.ch](mailto:info@iec.ch)  
[www.iec.ch](http://www.iec.ch)

#### About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

#### About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

#### IEC Catalogue - [webstore.iec.ch/catalogue](http://webstore.iec.ch/catalogue)

The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

#### IEC publications search - [www.iec.ch/searchpub](http://www.iec.ch/searchpub)

The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee,...). It also gives information on projects, replaced and withdrawn publications.

#### IEC Just Published - [webstore.iec.ch/justpublished](http://webstore.iec.ch/justpublished)

Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and also once a month by email.

#### Electropedia - [www.electropedia.org](http://www.electropedia.org)

The world's leading online dictionary of electronic and electrical terms containing 20 000 terms and definitions in English and French, with equivalent terms in 15 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

#### IEC Glossary - [std.iec.ch/glossary](http://std.iec.ch/glossary)

65 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

#### IEC Customer Service Centre - [webstore.iec.ch/csc](http://webstore.iec.ch/csc)

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: [csc@iec.ch](mailto:csc@iec.ch).

#### A propos de l'IEC

La Commission Electrotechnique Internationale (IEC) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

#### A propos des publications IEC

Le contenu technique des publications IEC est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

#### Catalogue IEC - [webstore.iec.ch/catalogue](http://webstore.iec.ch/catalogue)

Application autonome pour consulter tous les renseignements bibliographiques sur les Normes internationales, Spécifications techniques, Rapports techniques et autres documents de l'IEC. Disponible pour PC, Mac OS, tablettes Android et iPad.

#### Recherche de publications IEC - [www.iec.ch/searchpub](http://www.iec.ch/searchpub)

La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études,...). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

#### IEC Just Published - [webstore.iec.ch/justpublished](http://webstore.iec.ch/justpublished)

Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et aussi une fois par mois par email.

#### Electropedia - [www.electropedia.org](http://www.electropedia.org)

Le premier dictionnaire en ligne de termes électroniques et électriques. Il contient 20 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans 15 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

#### Glossaire IEC - [std.iec.ch/glossary](http://std.iec.ch/glossary)

65 000 entrées terminologiques électrotechniques, en anglais et en français, extraites des articles Termes et Définitions des publications IEC parues depuis 2002. Plus certaines entrées antérieures extraites des publications des CE 37, 77, 86 et CISPR de l'IEC.

#### Service Clients - [webstore.iec.ch/csc](http://webstore.iec.ch/csc)

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: [csc@iec.ch](mailto:csc@iec.ch).

# 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 978-2-8322-3480-8

**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 .....	16
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.....	24
3.2.1 Common symbols and abbreviated terms.....	24
3.2.2 CPF 2: Additional symbols and abbreviated terms.....	25
3.3 Conventions.....	26
4 Overview of FSCP 2/1 (CIP Safety™).....	26
4.1 General.....	26
4.2 FSCP 2/1 .....	26
5 General.....	27
5.1 External documents providing specifications for the profile.....	27
5.2 Safety functional requirements .....	28
5.3 Safety measures .....	28
5.4 Safety communication layer structure .....	29
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.....	30
6.1 Introduction.....	30
6.2 Connection objects .....	31
6.2.1 General .....	31
6.2.2 Class attribute extensions .....	31
6.2.3 Service extensions.....	31
6.2.4 Explicit message response format for SafetyOpen and SafetyClose .....	32
6.3 Connection Manager object.....	32
6.3.1 General .....	32
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 for safety .....	42
6.3.10 Safety Validator connection types.....	43
6.3.11 Application reply data in a successful SafetyOpen response .....	46
6.3.12 Unsuccessful SafetyOpen response .....	48
6.3.13 ForwardClose for safety .....	50

6.4	Identity object .....	50
6.4.1	General .....	50
6.4.2	Changes to common services .....	50
6.4.3	Extensions for CP 16/3 devices .....	51
6.5	Link objects .....	51
6.5.1	DeviceNet object changes .....	51
6.5.2	TCP/IP Interface object changes .....	52
6.5.3	SERCOS III Link object .....	52
6.6	Safety Supervisor object .....	53
6.6.1	General .....	53
6.6.2	Safety Supervisor class attributes .....	54
6.6.3	Subclasses .....	54
6.6.4	Safety Supervisor instance attributes .....	54
6.6.5	Semantics .....	58
6.6.6	Subclasses .....	64
6.6.7	Safety Supervisor common services .....	64
6.6.8	Safety Supervisor behavior .....	75
6.7	Safety Validator object .....	82
6.7.1	General .....	82
6.7.2	Class attributes .....	82
6.7.3	Instance attributes .....	83
6.7.4	Class services .....	88
6.7.5	Instance services .....	89
6.7.6	Object behavior .....	89
6.8	Connection Configuration Object .....	92
6.8.1	General .....	92
6.8.2	Class attribute extensions .....	92
6.8.3	Instance attributes, additions and extensions .....	92
6.8.4	Instance attribute semantics extensions or restrictions for safety .....	95
6.8.5	Special Safety Related Parameters – (Attribute 13) .....	99
6.8.6	Object-specific services .....	105
6.8.7	Common service extensions for safety .....	105
6.8.8	Object behavior .....	107
7	Safety communication layer protocol .....	108
7.1	Safety PDU format .....	108
7.1.1	Safety PDU encoding .....	108
7.1.2	Safety CRC .....	120
7.2	Communication protocol behavior .....	121
7.2.1	Sequence of safety checks .....	121
7.2.2	Connection termination .....	121
7.2.3	Cross checking error .....	121
7.3	Time stamp operation .....	122
7.4	Rollover counts in the EF .....	123
7.5	Protocol sequence diagrams .....	123
7.5.1	General .....	123
7.5.2	Normal safety transmission .....	123
7.5.3	Lost, corrupted and delayed message transmission .....	124
7.5.4	Lost, corrupted or delayed message transmission with production repeated .....	127

7.5.5	Point-to-point ping.....	129
7.5.6	Multipoint ping on CP 2/3 Safety.....	130
7.5.7	Multipoint ping on CP 2/2 safety networks .....	131
7.5.8	Multipoint ping – retry with success .....	132
7.5.9	Multipoint ping – retry with timeout .....	133
7.6	Safety protocol definition .....	134
7.6.1	General .....	134
7.6.2	High level view of a safety device .....	134
7.6.3	Safety Validator object .....	134
7.6.4	Relationship between SafetyValidatorServer and SafetyValidatorClient .....	135
7.6.5	Extended Format time stamp rollover handling.....	135
7.6.6	SafetyValidatorClient function definition.....	140
7.6.7	SafetyValidatorServer function definition .....	148
7.7	Safety message and protocol data specifications .....	161
7.7.1	Mode octet.....	161
7.7.2	Time Stamp Section .....	162
7.7.3	Time Coordination Message .....	162
7.7.4	Time correction message .....	163
7.7.5	Safety data production .....	163
7.7.6	Producer dynamic variables .....	171
7.7.7	Producer per consumer dynamic variables.....	173
7.7.8	Consumer data variables.....	174
7.7.9	Consumer input static variables.....	176
7.7.10	Consumer dynamic variables.....	177
8	Safety communication layer management.....	179
8.1	Overview .....	179
8.2	Definition of the measures used during connection establishment .....	179
8.3	Originator-Target relationship validation .....	183
8.4	Detection of mis-routed connection requests.....	183
8.5	SafetyOpen processing .....	184
8.6	Ownership management.....	184
8.7	Bridging different physical layers .....	185
8.8	Safety connection establishment .....	187
8.8.1	Overview .....	187
8.8.2	Basic facts for connection establishment .....	187
8.8.3	Configuring safety connections.....	187
8.8.4	Network time expectation multiplier .....	189
8.8.5	Establishing connections .....	190
8.8.6	Recommendations for consumer number allocation.....	193
8.8.7	Recommendations for connection establishment.....	194
8.8.8	Ownership establishment .....	194
8.8.9	Ownership use cases .....	195
8.8.10	PID/CID usage and establishment .....	198
8.8.11	Proper PID/CID usage in multipoint and point-to-point connections .....	198
8.8.12	Network supported services .....	200
8.8.13	FSCP 2/1 safety device type .....	201
8.9	Safety configuration process .....	205
8.9.1	Introduction to safety configuration .....	205
8.9.2	Configuration goals .....	205

8.9.3	Configuration overview .....	206
8.9.4	User configuration guidelines .....	207
8.9.5	Configuration process SIL3 justification .....	208
8.9.6	Device functions for tool configuration .....	209
8.9.7	Password security .....	209
8.9.8	SNCT interface services .....	209
8.9.9	Configuration lock .....	209
8.9.10	Effect of configuration lock on device behavior .....	210
8.9.11	Configuration ownership .....	211
8.9.12	Configuration mode .....	211
8.9.13	Measures used to ensure integrity of configuration process .....	211
8.9.14	Download process .....	213
8.9.15	Verification process .....	216
8.9.16	Verification process .....	218
8.9.17	Configuration error analysis .....	219
8.10	Electronic Data Sheets extensions for safety .....	223
8.10.1	General rules for EDS based safety devices .....	223
8.10.2	EDS extensions for safety .....	224
8.11	Requirements for CP 2/2 .....	229
8.11.1	EPI rules for safety messages that travel over CP 2/2 .....	229
8.11.2	Default safety I/O service .....	229
8.11.3	Duplicate IP detection .....	229
8.11.4	Priority for safety connections .....	229
8.12	Requirements for CP 2/3 .....	230
8.12.1	Allocation of CP 2/3 identifiers .....	230
8.12.2	Additional requirements .....	232
8.13	CP 16/3 requirements .....	232
8.13.1	General architecture for CP 2 on CP 16/3 .....	232
8.13.2	Baseline FSCP 2/1 on CP 16/3 device .....	233
8.13.3	Supported objects and services in CP 16/3 devices .....	234
8.13.4	Transport layer requirements .....	234
8.13.5	FSCP 2/1 and the CP 16/3 device model .....	237
8.13.6	UNID assignment on CP 16/3 .....	238
9	System requirements .....	241
9.1	Indicators and switches .....	241
9.1.1	General indicator requirements .....	241
9.1.2	LED indications for setting the device UNID .....	241
9.1.3	Module Status LED .....	241
9.1.4	Indicator warning .....	242
9.1.5	Network Status LED .....	242
9.1.6	Switches .....	243
9.2	Installation guidelines .....	245
9.3	Safety function response time .....	246
9.3.1	Overview .....	246
9.3.2	Network time expectation .....	246
9.3.3	Equations for calculating network reaction times .....	247
9.4	Duration of demands .....	249
9.5	Constraints for calculation of system characteristics .....	249
9.5.1	Number of nodes .....	249

9.5.2	Network PFH .....	249
9.5.3	Bit Error Rate (BER) .....	252
9.6	Maintenance .....	253
9.7	Safety manual .....	253
10	Assessment .....	253
Annex A (informative) Additional information for functional safety communication profiles of CPF 2 .....		254
A.1	Hash function example code .....	254
A.2	.....	268
Annex B (informative) Information for assessment of the functional safety communication profiles of CPF 2 .....		269
Bibliography .....		270
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 .....	27
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 (Form 2 SafetyOpen) .....	39
Figure 8	– Target Processing for SafetyOpen with configuration data (Form 1 SafetyOpen) .....	40
Figure 9	– Originator logic to determine which format to use .....	41
Figure 10	– Applying device configuration .....	68
Figure 11	– Configure and Validate processing flowcharts .....	69
Figure 12	– UNID handling during “Waiting for TUNID” .....	75
Figure 13	– Safety Supervisor state diagram .....	76
Figure 14	– Configuration, tuning and locked relationships .....	80
Figure 15	– Safety connection types .....	86
Figure 16	– Safety Validator state transition diagram .....	90
Figure 17	– Logic for auto-detecting format type .....	104
Figure 18	– Connection Configuration Object state diagram .....	107
Figure 19	– Connection Configuration Object data flow .....	108
Figure 20	– Format of the mode octet .....	109
Figure 21	– 1 or 2 octet data section, Base Format .....	110
Figure 22	– 1 or 2 octet data section, Extended Format .....	111
Figure 23	– 3 to 250 octet data section format, Base Format .....	111
Figure 24	– 3 to 250 octet data section format, Extended Format .....	112
Figure 25	– Time Stamp section format, Base Format .....	113
Figure 26	– BF Time Coordination message encoding .....	114
Figure 27	– EF Time Coordination message encoding .....	114
Figure 28	– BF Time Correction message encoding .....	115
Figure 29	– EF Time Correction message encoding .....	115

Figure 30 – 1 or 2 octet point-to-point PDU encoding.....	117
Figure 31 – 1 or 2 Octet multipoint PDU encoding .....	117
Figure 32 – 1 or 2 Octet, multipoint, Format 2 safety connection format .....	118
Figure 33 – 3 to 250 Octet Point-to-point PDU encoding .....	118
Figure 34 – 3 to 248 Octet Multipoint PDU encoding .....	119
Figure 35 – 3 to 248 Octet, Multipoint, safety connection format .....	119
Figure 36 – CRC Calculation order for Extended Format messages .....	120
Figure 37 – Time stamp sequence.....	122
Figure 38 – Sequence diagram of a normal producer/consumer safety sequence .....	123
Figure 39 – Sequence diagram of a normal producer/consumer safety sequence (production repeated).....	124
Figure 40 – Sequence diagram of a corrupted producer to consumer message.....	125
Figure 41 – Sequence diagram of a lost producer to consumer message.....	126
Figure 42 – Sequence diagram of a delayed message .....	127
Figure 43 – Sequence diagram of a corrupted producer to consumer message with production repeated.....	128
Figure 44 – Sequence diagram of a connection terminated due to delays .....	129
Figure 45 – Sequence diagram of a failure of safety CRC check .....	129
Figure 46 – Sequence diagram of a point-to-point ping – normal response .....	130
Figure 47 – Sequence diagram of a successful multipoint ping, CP 2/3 safety .....	131
Figure 48 – Sequence diagram of a successful multipoint ping, CP 2/2 safety .....	132
Figure 49 – Sequence diagram of a multipoint ping retry .....	133
Figure 50 – Sequence diagram of a multipoint ping timeout .....	133
Figure 51 – Safety device reference model entity relation diagram .....	134
Figure 52 – Two devices interchanging safety data via a SafetyValidatorClient and a SafetyValidatorServer .....	135
Figure 53 – Point-to-point, originator consumer, target producer.....	137
Figure 54 – Point-to-point, originator producer, target consumer .....	138
Figure 55 – Multi-point, originator consumer, target producer.....	139
Figure 56 – Safety production data flow.....	140
Figure 57 – Consumer safety data monitoring.....	149
Figure 58 – SafetyValidatorServer – application triggered.....	150
Figure 59 – Target ownership.....	183
Figure 60 – SafetyOpen forms.....	184
Figure 61 – Connection ownership state chart .....	185
Figure 62 – SafetyOpen UNID mapping .....	185
Figure 63 – Common CPF 2 application layer .....	186
Figure 64 – End-to-End routing example .....	186
Figure 65 – Sources for safety related connection parameters .....	189
Figure 66 – Parameter mapping between originator and target.....	190
Figure 67 – CP 2/3 Safety connection establishment in targets for Form 2a SafetyOpen.....	192
Figure 68 – General sequence to detect configuration is required .....	193
Figure 69 – PID/CID exchanges for two originator scenarios .....	198
Figure 70 – Seed generation for multipoint connections .....	199

Figure 71 – PID/CID runtime handling .....	200
Figure 72 – Connection categories and supported services.....	203
Figure 73 – Recommended connection types.....	204
Figure 74 – Logic-to-logic supported services.....	204
Figure 75 – Recommended connection types for logic to logic .....	205
Figure 76 – Configuration data transfers.....	206
Figure 77 – Protection measures in safety devices .....	208
Figure 78 – Configuration, testing and locked relationships.....	210
Figure 79 – Originator's configuration data .....	212
Figure 80 – SNCT to device download process.....	214
Figure 81 – SNCT Downloads to originators that perform Form 1 configuration .....	215
Figure 82 – Protection from locking and ownership .....	217
Figure 83 – Example of read back and comparison of original and printout.....	217
Figure 84 – Diverse display without full data read back.....	218
Figure 85 – Verification process including all alternatives .....	219
Figure 86 – Baseline FSCP 2/1 on CP 16/3 device .....	233
Figure 87 – FSCP 2/1 Adaptation Layer and SMP interaction.....	236
Figure 88 – FSCP 2/1 Adaptation .....	237
Figure 89 – CP 16/3 device model.....	238
Figure 90 – Adding a standard module to a modular device .....	240
Figure 91 – Safety device NodeID processing logic.....	245
Figure 92 – Safety function response time.....	246
Figure 93 – Safety function response time components .....	248
Figure 94 – Network protocol reliability Block Diagram (RBD) .....	249
Figure 95 – Network PFH summary .....	251
Figure 96 – Extended Format PFH summary .....	252
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 .....	44
Table 11 – Network connection parameters for safety connections.....	46
Table 12 – CP 2/3 Safety target application reply (size: 10 octets).....	46
Table 13 – EF CP 2/3 Safety target application reply (size: 14 octets).....	47
Table 14 – SafetyOpen target application reply (size: 18 octets) .....	47
Table 15 – EF SafetyOpen target application reply (size: 22 octets).....	48
Table 16 – New and extended error codes for safety .....	48

Table 17 – SafetyOpen error event guidance table .....	49
Table 18 – Identity object common service changes .....	51
Table 19 – Identity object extensions for CP 16/3 devices.....	51
Table 20 – New DeviceNet object instance attribute .....	51
Table 21 – New TCP/IP Interface object instance attribute .....	52
Table 22 – SERCOS III Link object class attributes.....	52
Table 23 – SERCOS III Link object instance attributes.....	53
Table 24 – SERCOS III Link Object Common Services .....	53
Table 25 – Safety Supervisor class attributes .....	54
Table 26 – Safety Supervisor instance attributes .....	55
Table 27 – Device status attribute state values.....	59
Table 28 – Exception status attribute format.....	59
Table 29 – Common exception detail attribute values .....	60
Table 30 – Exception detail format summary .....	61
Table 31 – Summary of device behavior for various CFUNID values .....	63
Table 32 – Safety Supervisor common services.....	65
Table 33 – Safety Supervisor object specific services .....	65
Table 34 – Configure_Request message structure.....	67
Table 35 – Validate_Configuration message structure.....	67
Table 36 – Validate_Configuration success message structure .....	67
Table 37 – Validate_Configuration error code.....	68
Table 38 – Validate_Configuration extended codes.....	68
Table 39 – Set_Password message structure .....	70
Table 40 – Reset_Password message structure.....	70
Table 41 – Configuration_Lock/Unlock message structure .....	71
Table 42 – Mode_Change message structure .....	71
Table 43 – Safety_Reset message structure.....	72
Table 44 – Safety Supervisor safety reset types .....	72
Table 45 – Attribute bit map parameter.....	72
Table 46 – Reset processing rules for reset types.....	73
Table 47 – Propose_TUNID service.....	73
Table 48 – Apply_TUNID service.....	74
Table 49 – Safety Supervisor events .....	76
Table 50 – State event matrix for Safety Supervisor .....	77
Table 51 – Configuration owner control vs. device state.....	80
Table 52 – State mapping of Safety Supervisor to Identity object .....	81
Table 53 – Safety Supervisor object event mapping.....	81
Table 54 – Identity object event mapping.....	82
Table 55 – Safety Validator class attributes .....	83
Table 56 – Safety Validator instance attributes .....	83
Table 57 – Safety Validator state assignments .....	85
Table 58 – Safety Validator type, bit field assignments .....	86
Table 59 – Multipoint producer SafetyOpen parameter evaluation rules.....	87

Table 60 – Safety Validator class services.....	88
Table 61 – Safety Validator instance services.....	89
Table 62 – Safety Validator Get_Attributes_All service data .....	89
Table 63 – Safety Validator state event matrix.....	91
Table 64 – State mapping between Safety Supervisor and Safety Validator objects.....	92
Table 65 – Connection configuration object class attribute extensions.....	92
Table 66 – Connection Configuration Object instance attribute additions/extensions.....	92
Table 67 – Connection flag bit definitions .....	95
Table 68 – O-to-T connection parameters.....	96
Table 69 – T-to-O connection parameters.....	97
Table 70 – Data map formats .....	98
Table 71 – Data map format 0 .....	99
Table 72 – Data map format 1 .....	99
Table 73 – Target device’s SCCRC values .....	101
Table 74 – Target device’s SCTS values .....	101
Table 75 – Time correction connection parameters for multipoint connection.....	102
Table 76 – Format Type attribute meaning .....	103
Table 77 – Format Status attribute meaning .....	104
Table 78 – Connection Configuration Object-specific services.....	105
Table 79 – Get_Attributes_All Response service data (added attributes ) .....	105
Table 80 – Get_Attributes_All Response service data (added parameters ) .....	106
Table 81 – Set_Attributes_All Request service data (added attributes).....	106
Table 82 – Set_Attributes_All Response service data (added parameters ) .....	106
Table 83 – State Mapping between Safety Supervisor and the CCO objects.....	107
Table 84 – Connection sections and PDU formats .....	109
Table 85 – Mode octet variables.....	110
Table 86 – Time Stamp variables .....	113
Table 87 – Time Coordination message variables .....	114
Table 88 – Time Correction Message variables .....	116
Table 89 – CRC polynomials used.....	120
Table 90 – Connection sections and message formats.....	121
Table 91 – Data reception – Link triggered .....	151
Table 92 – Time_Correction reception – Link triggered .....	151
Table 93 – Data reception – Application triggered.....	151
Table 94 – Time_Correction reception – Application triggered.....	152
Table 95 – Consuming application – Safety data monitoring.....	152
Table 96 – Producer connection status determination .....	164
Table 97 – Consuming safety connection status .....	175
Table 98 – Connection establishment errors and measures to detect errors .....	179
Table 99 – SNN Date/Time allocations .....	180
Table 100 – SNN legal range of time values .....	180
Table 101 – Safety connection parameters.....	188
Table 102 – SafetyOpen summary.....	191

Table 103 – Originator/Target service mapping..... 202

Table 104 – Unsupported originator/target service types..... 202

Table 105 – Configuration goals..... 206

Table 106 – Configuration owner control vs. device state..... 211

Table 107 – Errors and detection measures..... 220

Table 108 – Object Class section keywords..... 224

Table 109 – Safety Classx entry format ..... 225

Table 110 – Parameter class keywords ..... 225

Table 111 – New Connection Manager section keywords for safety..... 226

Table 112 – Connection Manager field usage for safety ..... 227

Table 113 – Connection parameter field settings for safety ..... 228

Table 114 – CP 2/3 ID assignment rules..... 230

Table 115 – LED indications for setting UNID ..... 241

Table 116 – Module Status LED ..... 242

Table 117 – Network status LED states ..... 242

Table 118 – Connection reaction time type – producing/consuming applications..... 247

# 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.

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 third edition cancels and replaces the second edition published in 2010. This edition constitutes a technical revision. The main changes with respect to the previous edition are listed below (and highlighted in yellow in this document).

- Added detailed requirements for use of FSCP 2/1 in conjunction with CP 16/3 (see 4.1, 6.4.3, 6.5.3, 8.2, 8.13, and miscellaneous references when referencing CPF 2 networks);
- Defined object class section keywords for safety to EDS file definition in 8.10.2.1;
- New sections on safety CRC overview in 7.1.2.1 and Rollover counts for EF format in 7.4;
- Corrections to PFH calculations in 9.5.2;

- Change from MACID to NodeID as general reference to network identifier;
- Miscellaneous minor corrections made since the last publication.

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

FDIS	Report on voting
65C/851/FDIS	65C/854/RVD

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

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

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

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC web site under "<http://webstore.iec.ch>" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

**IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.**

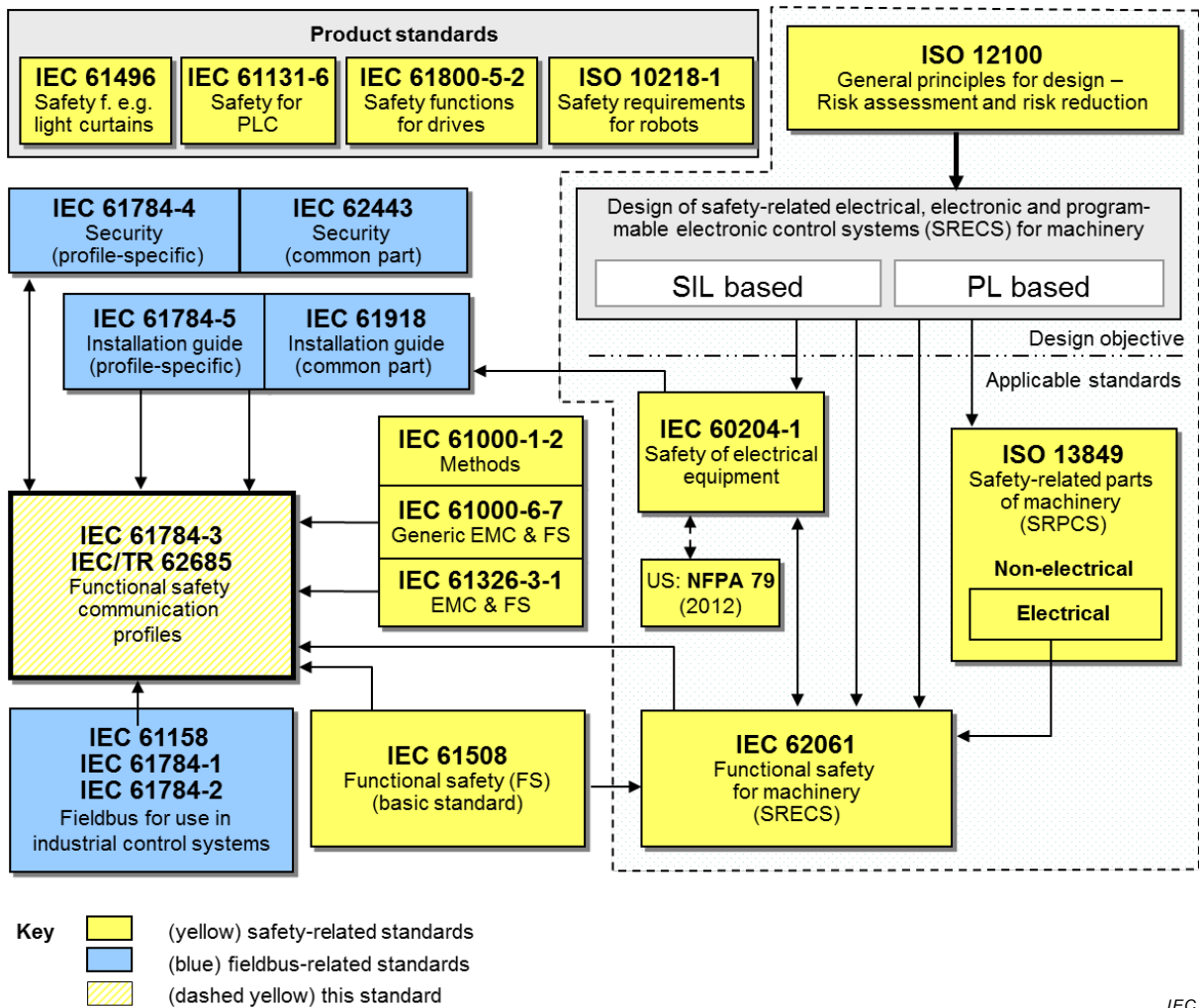
## 0 Introduction

### 0.1 General

The IEC 61158 fieldbus standard together with its companion standards IEC 61784-1 and IEC 61784-2 defines a set of communication protocols that enable distributed control of automation applications. Fieldbus technology is now considered well accepted and well proven. Thus fieldbus enhancements continue to emerge, addressing applications for 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.

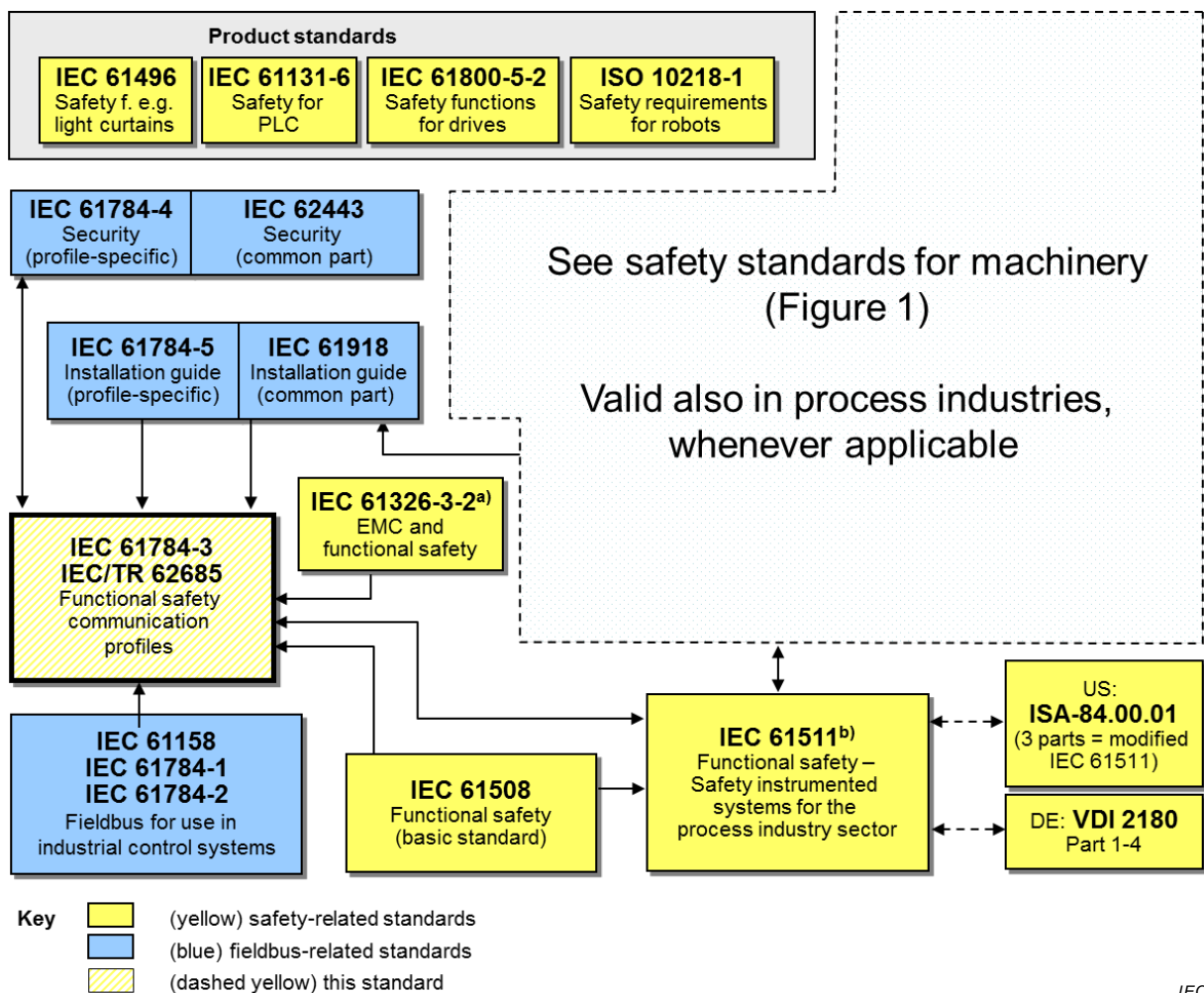
Figure 1 shows the relationships between this standard and relevant safety and fieldbus standards in a machinery environment.



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

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

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



<sup>a</sup> For specified electromagnetic environments; otherwise IEC 61326-3-1 or IEC 61000-6-7.

<sup>b</sup> 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 (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.

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;
- 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 the IEC 61158 series.

## 0.2 Patent declaration

The International Electrotechnical Commission (IEC) draws attention to the fact that it is claimed that compliance with this document may involve the use of patents concerning the functional safety communication profiles for family 2 as follows, where the [xx] notation indicates the holder of the patent rights:

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 holder of these patent rights has assured the IEC that he/she is willing to negotiate licences either free of charge or 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:

[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.

ISO ([www.iso.org/patents](http://www.iso.org/patents)) and IEC (<http://patents.iec.ch>) maintain on-line data bases of patents relevant to their standards. Users are encouraged to consult the data bases for the most up to date information concerning patents.

## 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. 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 part<sup>1</sup> 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<sup>2</sup> 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 documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. 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 – Type 2 elements*

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

---

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

<sup>2</sup> In the following pages of this standard, “IEC 61508” will be used for “IEC 61508 series”.