

# 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 © 2021 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  
[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 corrigendum or an amendment might have been published.

#### IEC publications search - [webstore.iec.ch/advsearchform](http://webstore.iec.ch/advsearchform)

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 It also gives information on projects, replaced and withdrawn publications.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 once a month by email.

#### 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: [sales@iec.ch](mailto:sales@iec.ch).

#### IEC online collection - [oc.iec.ch](http://oc.iec.ch)

Discover our powerful search engine and read freely all the publications previews. With a subscription you will always have access to up to date content tailored to your needs.

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

The world's leading online dictionary on electrotechnology, containing more than 22 000 terminological entries in English and French, with equivalent terms in 18 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

### 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.

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

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 une fois par mois par email.

#### 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: [sales@iec.ch](mailto:sales@iec.ch).

#### IEC online collection - [oc.iec.ch](http://oc.iec.ch)

Découvrez notre puissant moteur de recherche et consultez gratuitement tous les aperçus des publications. Avec un abonnement, vous aurez toujours accès à un contenu à jour adapté à vos besoins.

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

Le premier dictionnaire d'électrotechnologie en ligne au monde, avec plus de 22 000 articles terminologiques en anglais et en français, ainsi que les termes équivalents dans 16 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

# INTERNATIONAL STANDARD

## NORME INTERNATIONALE



---

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

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

INTERNATIONAL  
ELECTROTECHNICAL  
COMMISSION

COMMISSION  
ELECTROTECHNIQUE  
INTERNATIONALE

---

ICS 25.040.40; 35.100.05

ISBN 978-2-8322-9747-6

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

## CONTENTS

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

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

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

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

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

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

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

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

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

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

Copyright © IEC 2021. A preview generated by EVS

## INTERNATIONAL ELECTROTECHNICAL COMMISSION

**INDUSTRIAL COMMUNICATION NETWORKS –  
PROFILES –****Part 3-2: Functional safety fieldbuses –  
Additional specifications for CPF 2**

## FOREWORD

- 1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as “IEC Publication(s)”). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
- 2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
- 3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
- 4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
- 5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
- 6) All users should ensure that they have the latest edition of this publication.
- 7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
- 8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
- 9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

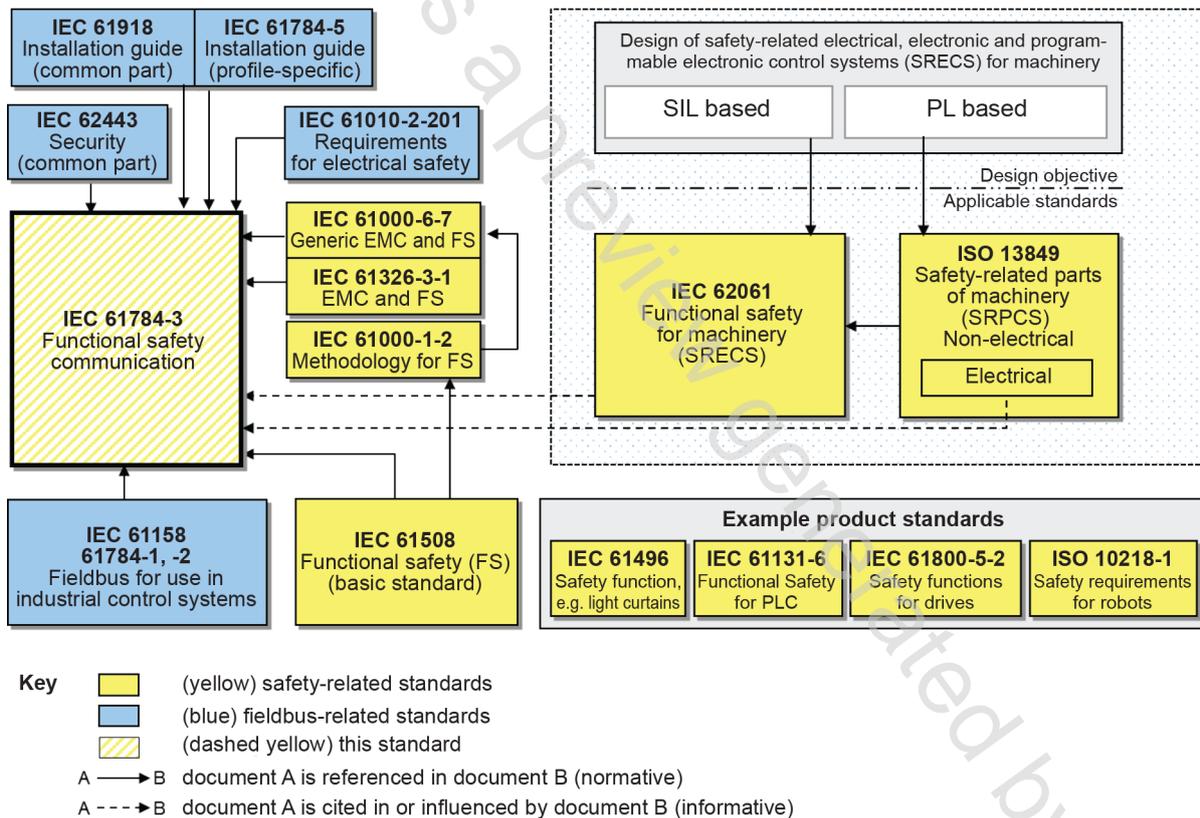
## 0 Introduction

### 0.1 General

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

IEC 61784-3 (all parts) explains the relevant principles for functional safety communications with reference to IEC 61508 (all parts) and specifies several safety communication layers (profiles and corresponding protocols) based on the communication profiles and protocol layers of IEC 61784-1, IEC 61784-2 and IEC 61158 (all parts). It does not cover electrical safety and intrinsic safety aspects. It also does not cover security aspects, nor does it provide any requirements for security.

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

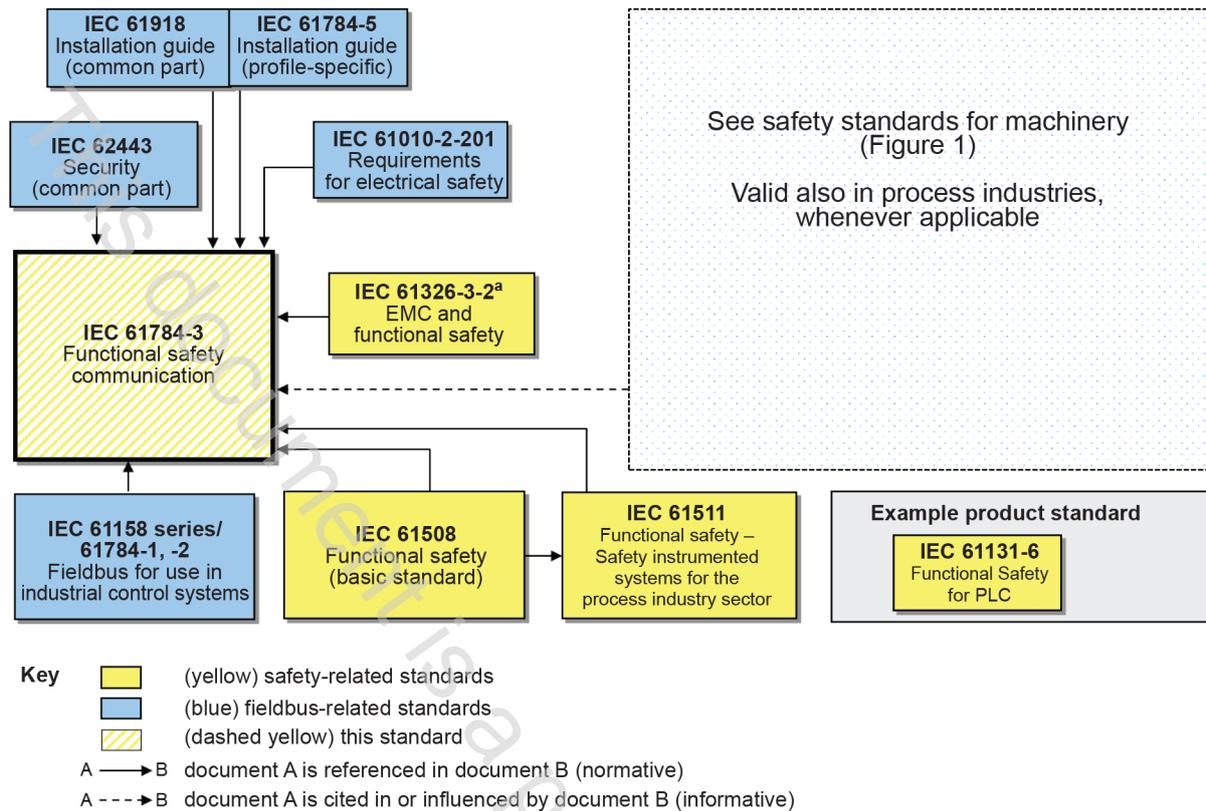


IEC

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

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

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



IEC

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

**Figure 2 – Relationships of IEC 61784-3 with other standards (process)**

Safety communication layers which are implemented as parts of safety-related systems according to IEC 61508 (all parts) provide the necessary confidence in the transportation of messages (information) between two or more participants on a fieldbus in a safety-related system, or sufficient confidence of safe behaviour in the event of fieldbus errors or failures.

Safety communication layers specified in IEC 61784-3 (all parts) do this in such a way that a fieldbus can be used for applications requiring functional safety up to the Safety Integrity Level (SIL) specified by its corresponding functional safety communication profile.

The resulting SIL claim of a system depends on the implementation of the selected functional safety communication profile (FSCP) within this system – implementation of a functional safety communication profile in a standard device is not sufficient to qualify it as a safety device.

IEC 61784-3 (all parts) describes:

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

## 0.2 Patent declaration

The International Electrotechnical Commission (IEC) draws attention to the fact that it is claimed that compliance with this document may involve the use of patents concerning the functional safety communication profiles for family 2. IEC takes no position concerning the evidence, validity, and scope of these patent rights.

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

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

This document is a preview generated by EVS

## INDUSTRIAL COMMUNICATION NETWORKS – PROFILES –

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

#### 1 Scope

This part of IEC 61784-3 (all parts) specifies a safety communication layer (services and protocol) based on CPF 2 of IEC 61784-1, IEC 61784-2 and IEC 61158 Type 2. It identifies the principles for functional safety communications defined in IEC 61784-3 that are relevant for this safety communication layer. This safety communication layer is intended for implementation in safety devices only.

NOTE 1 It does not cover electrical safety and intrinsic safety aspects. Electrical safety relates to hazards such as electrical shock. Intrinsic safety relates to hazards associated with potentially explosive atmospheres.

This document defines mechanisms for the transmission of safety-relevant messages among participants within a distributed network using fieldbus technology in accordance with the requirements of IEC 61508 (all parts)<sup>1</sup> for functional safety. These mechanisms may be used in various industrial applications such as process control, manufacturing automation and machinery.

This document provides guidelines for both developers and assessors of compliant devices and systems.

NOTE 2 The resulting SIL claim of a system depends on the implementation of the selected functional safety communication profile within this system – implementation of a functional safety communication profile according to this document in a standard device is not sufficient to qualify it as a safety device.

#### 2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 61131-2, *Industrial-process measurement and control – Programmable controllers – Part 2: Equipment requirements and tests*

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

IEC 61158-2:2014, *Industrial communication networks – Fieldbus specifications – Part 2: Physical layer specification and service definition*

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

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

---

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

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

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

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

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

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

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

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

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

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

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

IEC 61784-2, *Industrial communication networks – Profiles – Part 2: Additional fieldbus profiles for real-time networks based on ISO/IEC/IEEE 8802-3*

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

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

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

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

ISO 13849-1:2015, *Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design*

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

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

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

### 3 Terms, definitions, symbols, abbreviated terms and conventions

#### 3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC 61784-3 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at <http://www.electropedia.org/>
- ISO Online browsing platform: available at <http://www.iso.org/obp>

NOTE Italics are used in the definitions to highlight terms which are themselves defined in 3.1.

##### 3.1.1 Common terms and definitions

NOTE These common terms and definitions are inherited from IEC 61784-3:2021.

###### 3.1.1.1

###### **bit error probability**

$P_e$

probability for a given bit to be received with the incorrect value

###### 3.1.1.2

###### **black channel**

*defined communication system* containing one or more elements without evidence of design or validation according to IEC 61508

Note 1 to entry: This definition expands the usual meaning of channel to include the system that contains the channel.

###### 3.1.1.3

###### **bridge**

abstract device that connects multiple network segments along the data link layer

###### 3.1.1.4

###### **closed communication system**

fixed number or fixed maximum number of participants linked by a *communication system* with well-known and fixed properties, and where the *risk* of unauthorized access is considered negligible

[SOURCE: IEC 62280:2014, 3.1.6, modified – transmission replaced by communication]

###### 3.1.1.5

###### **communication channel**

logical *connection* between two end-points within a *communication system*

###### 3.1.1.6

###### **communication system**

arrangement of hardware, software and propagation media to allow the transfer of *messages* (ISO/IEC 7498-1 application layer) from one application to another

###### 3.1.1.7

###### **connection**

logical binding between two application objects within the same or different devices