

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

EESTI STANDARDI EESSÕNA

NATIONAL FOREWORD

See Eesti standard EVS-EN 61784-3-2:2017 sisaldab Euroopa standardi EN 61784-3-2:2017 ingliskeelset teksti.	This Estonian standard EVS-EN 61784-3-2:2017 consists of the English text of the European standard EN 61784-3-2:2017.
Standard on jõustunud sellekohase teate avaldamisega EVS Teatajas.	This standard has been endorsed with a notification published in the official bulletin of the Estonian Centre for Standardisation.
Euroopa standardimisorganisatsioonid on teinud Euroopa standardi rahvuslikele liikmetele kättesaadavaks 10.11.2017.	Date of Availability of the European standard is 10.11.2017.
Standard on kättesaadav Eesti Standardikeskusest.	The standard is available from the Estonian Centre for Standardisation.

Tagasisidet standardi sisu kohta on võimalik edastada, kasutades EVS-i veebilehel asuvat tagasiside vormi või saates e-kirja meiliaadressile standardiosakond@evs.ee.

ICS 25.040.40, 35.100.05

Standardite reprodutseerimise ja levitamise õigus kuulub Eesti Standardikeskusele

Andmete paljundamine, taastekitamine, kopeerimine, salvestamine elektroonsesse süsteemi või edastamine ükskõik millises vormis või millisel teel ilma Eesti Standardikeskuse kirjaliku loata on keelatud.

Kui Teil on küsimusi standardite autorikaitse kohta, võtke palun ühendust Eesti Standardikeskusega:
Koduleht www.evs.ee; telefon 605 5050; e-post info@evs.ee

The right to reproduce and distribute standards belongs to the Estonian Centre for Standardisation

No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying, without a written permission from the Estonian Centre for Standardisation.

If you have any questions about copyright, please contact Estonian Centre for Standardisation:

Homepage www.evs.ee; phone +372 605 5050; e-mail info@evs.ee

English Version

**Industrial communication networks - Profiles - Part 3-2:
Functional safety fieldbuses - Additional specifications for CPF 2
(IEC 61784-3-2:2016)**

Réseaux de communication industriels - Profils - Partie 3-2:
Bus de terrain de sécurité fonctionnelle - Spécifications
supplémentaires pour CPF 2
(IEC 61784-3-2:2016)

Industrielle Kommunikationsnetze - Profile - Teil 3-2:
Funktional sichere Übertragung bei Feldbussen -
Zusätzliche Festlegungen für die
Kommunikationsprofilfamilie 2
(IEC 61784-3-2:2016)

This European Standard was approved by CENELEC on 2016-08-17. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.



European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

European foreword

The text of document 65C/851/FDIS, future edition 3 of IEC 61784-3-2, prepared by SC 65C "Industrial networks", of IEC/TC 65 "Industrial-process measurement, control and automation" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN 61784-3-2:2017.

The following dates are fixed:

- latest date by which the document has to be (dop) 2018-05-10
implemented at national level by
publication of an identical national
standard or by endorsement
- latest date by which the national (dow) 2020-11-10
standards conflicting with the
document have to be withdrawn

This document supersedes EN 61784-3-2:2010.

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

Endorsement notice

The text of the International Standard IEC 61784-3-2:2016 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following notes have to be added for the standards indicated:

IEC 61000-6-7	NOTE	Harmonized as EN 61000-6-7.
IEC 61131-6	NOTE	Harmonized as EN 61131-6.
IEC 61158 (all parts)	NOTE	Harmonized as EN 61158 (all parts).
IEC 61496 (all parts)	NOTE	Harmonized as EN 61496 (all parts).
IEC 61508-1:2010	NOTE	Harmonized as EN 61508-1:2010 (not modified).
IEC 61508-4:2010	NOTE	Harmonized as EN 61508-4:2010 (not modified).
IEC 61508-5:2010	NOTE	Harmonized as EN 61508-5:2010 (not modified).
IEC 61511 (all parts)	NOTE	Harmonized as EN 61511 (all parts).
IEC 61784-5 (all parts)	NOTE	Harmonized as EN 61784-5 (all parts).
IEC 61800-5-2	NOTE	Harmonized as EN 61800-5-2.
IEC 62061	NOTE	Harmonized as EN 62061.
IEC 62443 (all parts)	NOTE	Harmonized as prEN 62443 (all parts)
IEC/TR 62685	NOTE	Harmonized as CLC/TR 62685.
ISO 10218-1	NOTE	Harmonized as EN ISO 10218-1.
ISO 12100	NOTE	Harmonized as EN ISO 12100.
ISO 13849 (all parts)	NOTE	Harmonized as EN ISO 13849 (all parts).
IEC 62026-3	NOTE	Harmonized as EN 62026-3.

Annex ZA (normative)

Normative references to international publications with their corresponding European publications

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.

NOTE 1 Where an International Publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

NOTE 2 Up-to-date information on the latest versions of the European Standards listed in this annex is available here: www.cenelec.eu.

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
IEC 61131-2	-	Industrial-process measurement and control – Programmable controllers – Part 2: Equipment requirements and tests	EN 61131-2	-
IEC 61131-3	-	Programmable controllers - Part 3: Programming languages	EN 61131-3	-
IEC 61158-2	-	Industrial communication networks - Fieldbus specifications - Part 2: Physical layer specification and service definition	EN 61158-2	-
IEC 61158-3-2	-	Industrial communication networks - Fieldbus specifications - Part 3-2: Data-link layer service definition - Type 2 elements	EN 61158-3-2	-
IEC 61158-3-19	-	Industrial communication networks - Fieldbus specifications - Part 3-19: Data-link layer service definition - Type 19 elements	EN 61158-3-19	-
IEC 61158-4-2	-	Industrial communication networks - Fieldbus specifications - Part 4-2: Data-link layer protocol specification - Type 2 elements	EN 61158-4-2	-
IEC 61158-4-19	-	Industrial communication networks - Fieldbus specifications - Part 4-19: Data-link layer protocol specification - Type 19 elements	EN 61158-4-19	-
IEC 61158-5-2	-	Industrial communication networks - Fieldbus specifications - Part 5-2: Application layer service definition - Type 2 elements	EN 61158-5-2	-
IEC 61158-5-19	-	Industrial communication networks - Fieldbus specifications - Part 5-19: Application layer service definition - Type 19 elements	EN 61158-5-19	-
IEC 61158-6-2	-	Industrial communication networks - Fieldbus specifications - Part 6-2: Application layer protocol specification - Type 2 elements	EN 61158-6-2	-
IEC 61158-6-19	-	Industrial communication networks - Fieldbus specifications - Part 6-19: Application layer protocol specification - Type 19 elements	EN 61158-6-19	-

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	EN 61326-3-1	-
IEC 61326-3-2	-	Electrical equipment for measurement, control and laboratory use ζ EMC requirements ζ Part 3-2: Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety) ζ Industrial applications with specified electromagnetic environment	-	-
IEC 61508	series	Functional safety of electrical/electronic/programmable electronic safety-related systems	EN 61508	series
IEC 61784-1	-	Industrial communication networks - Profiles - Part 1: Fieldbus profiles	EN 61784-1	-
IEC 61784-2	-	Industrial communication networks - Profiles - Part 2: Additional fieldbus profiles for real-time networks based on ISO/IEC 8802-3	EN 61784-2	-
IEC 61784-3	-	Industrial communication networks - Profiles - Part 3: Functional safety fieldbuses - General rules and profile definitions	EN 61784-3	-
IEC 61784-5-2	-	Industrial communication networks - Profiles - Part 5-2: Installation of fieldbuses - Installation profiles for CPF 2	EN 61784-5-2	-
IEC 61918 (mod)	-	Industrial communication networks - Installation of communication networks in industrial premises	EN 61918	-
ISO 13849-1	2006	Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design	EN ISO 13849-1	2008
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	-	-

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 object	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 CPF 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, testing 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, originating 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

a preview generated by EVS

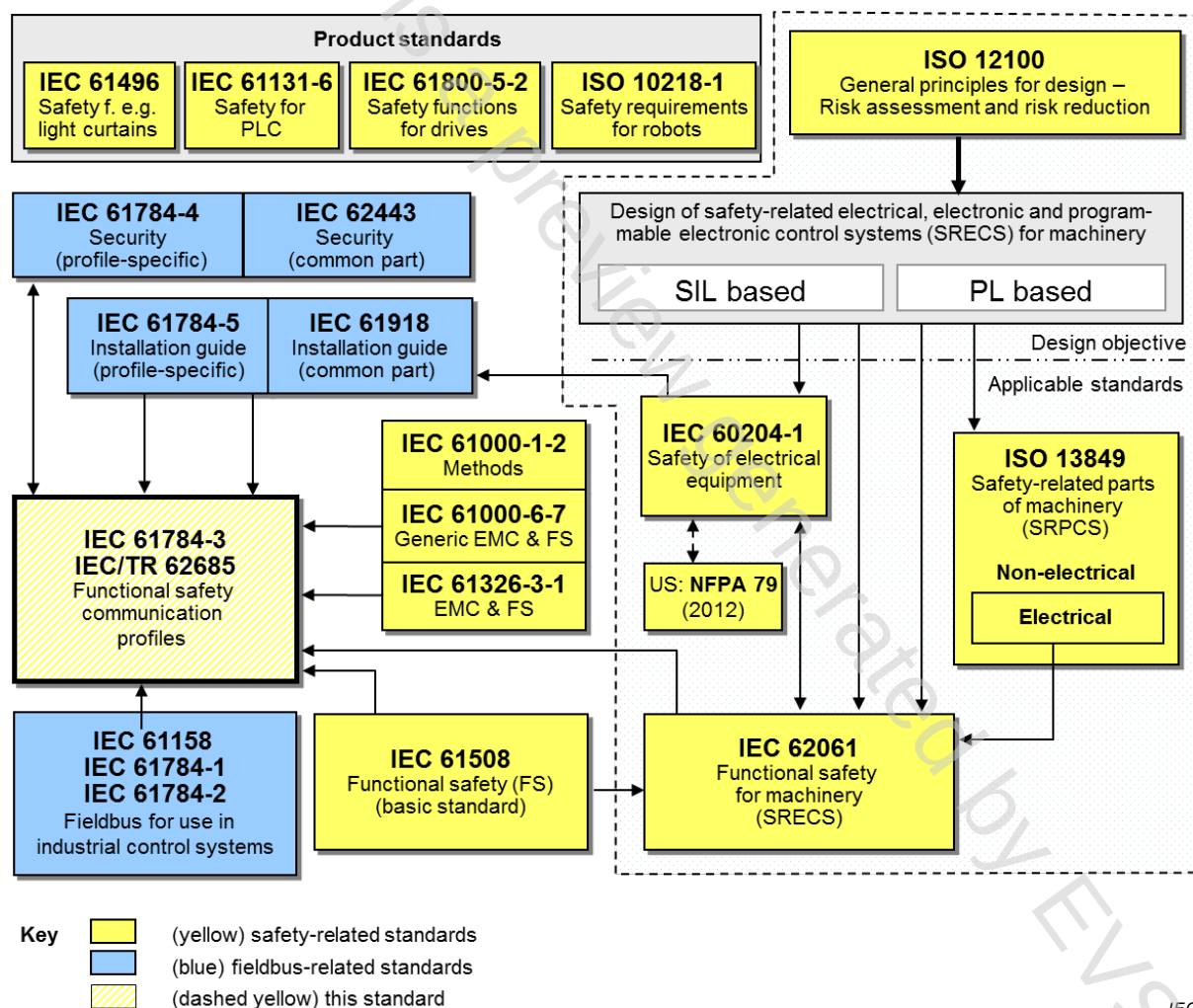
0 Introduction

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.

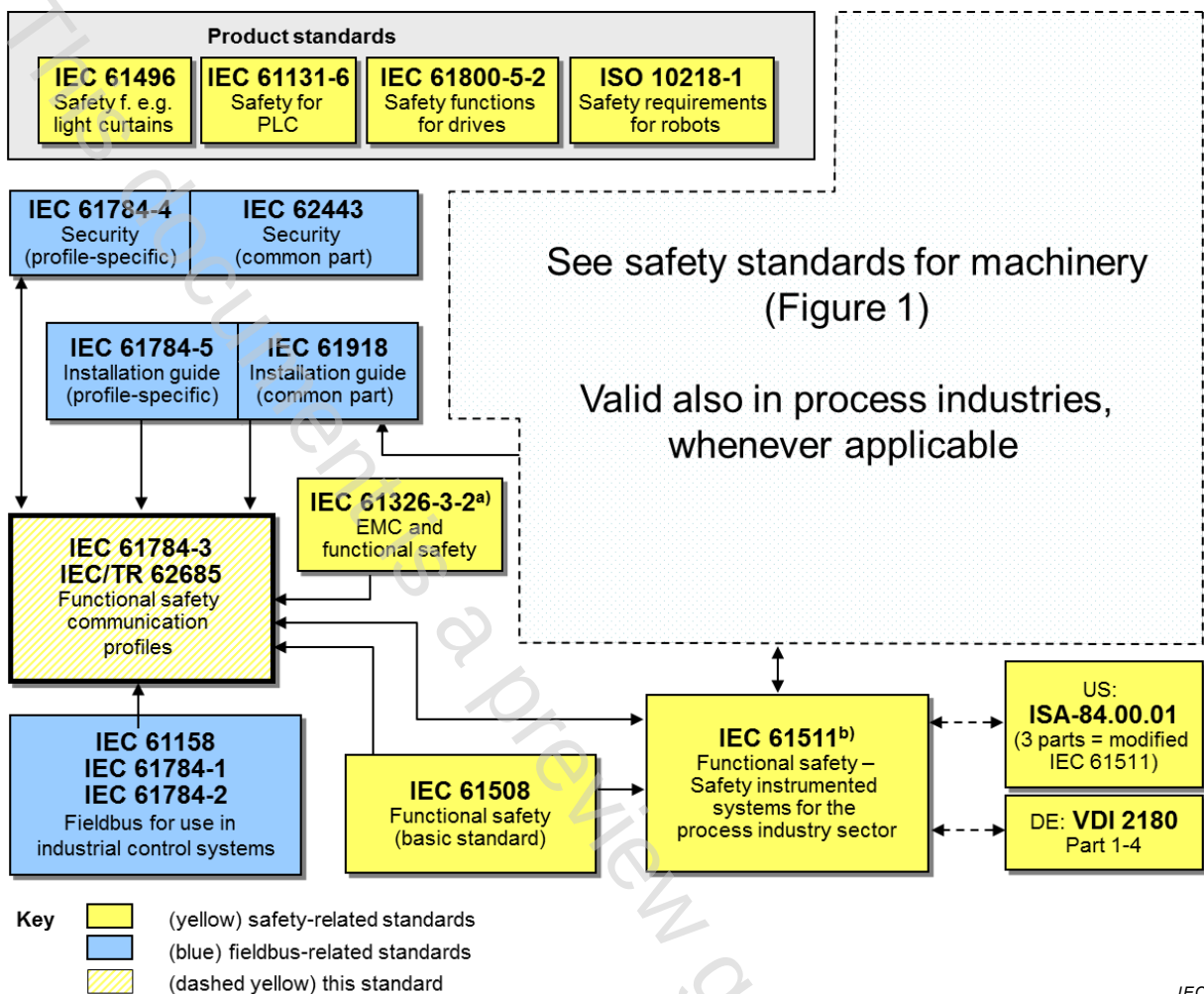
Figure 1 shows the relationships between this standard and relevant safety and fieldbus standards in a machinery environment.



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.



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

^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 (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) 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 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 series² 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*

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

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