



BSI Standards Publication

Industrial communication networks — Profiles

Part 3-2: Functional safety fieldbuses — Additional specifications for CPF 2 (IEC 61784-3-2:2016)

National foreword

This British Standard is the UK implementation of EN 61784-3-2:2017. It is identical to IEC 61784-3-2:2016. It supersedes BS EN 61784-3-2:2010, which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee AMT/7, Industrial communications: process measurement and control, including fieldbus.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2017
Published by BSI Standards Limited 2017

ISBN 978 0 580 85167 4

ICS 25.040.40; 35.100.05

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 December 2017.

Amendments/corrigenda issued since publication

Date	Text affected
------	---------------

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.....	194

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.

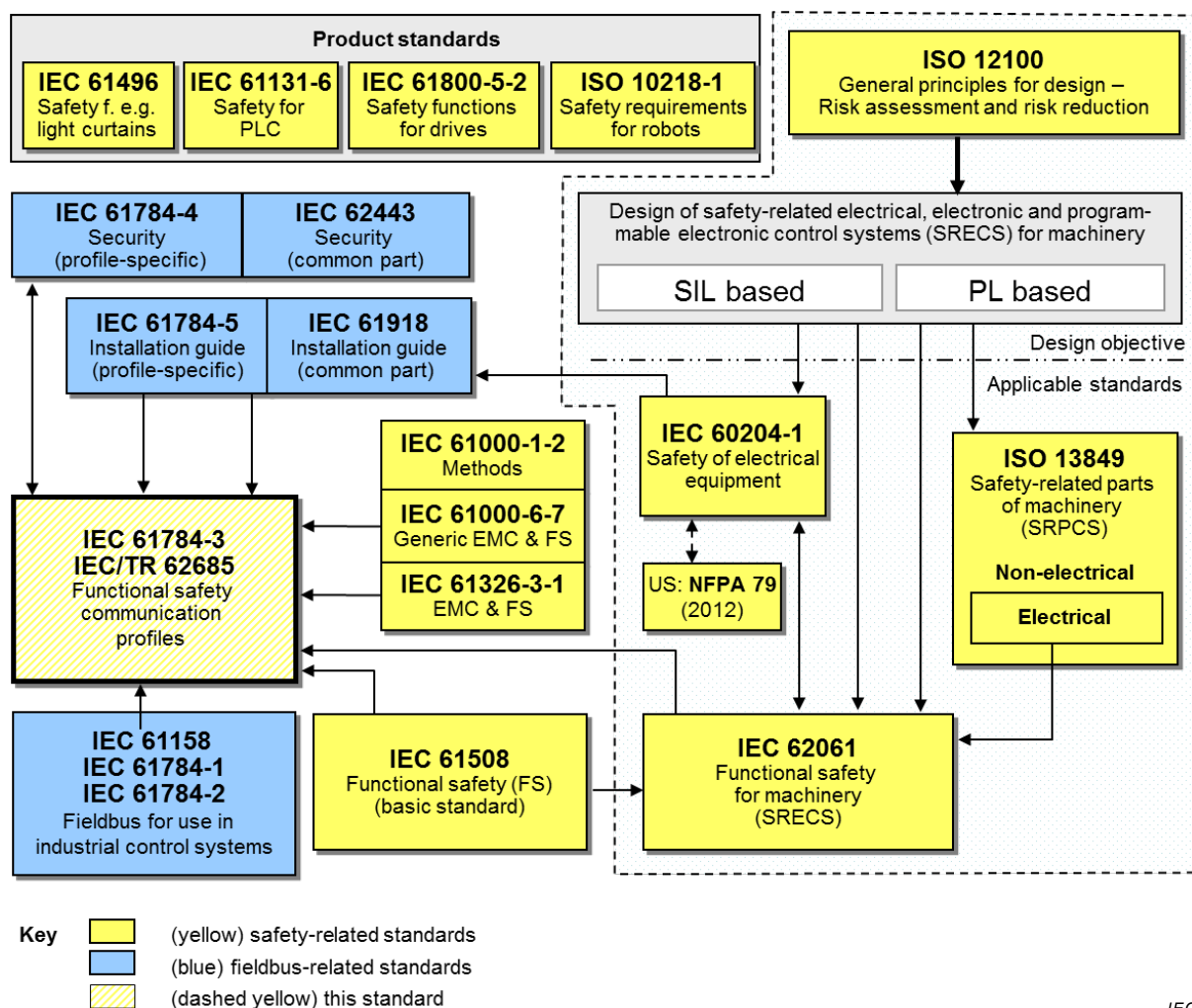
0 Introduction

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.

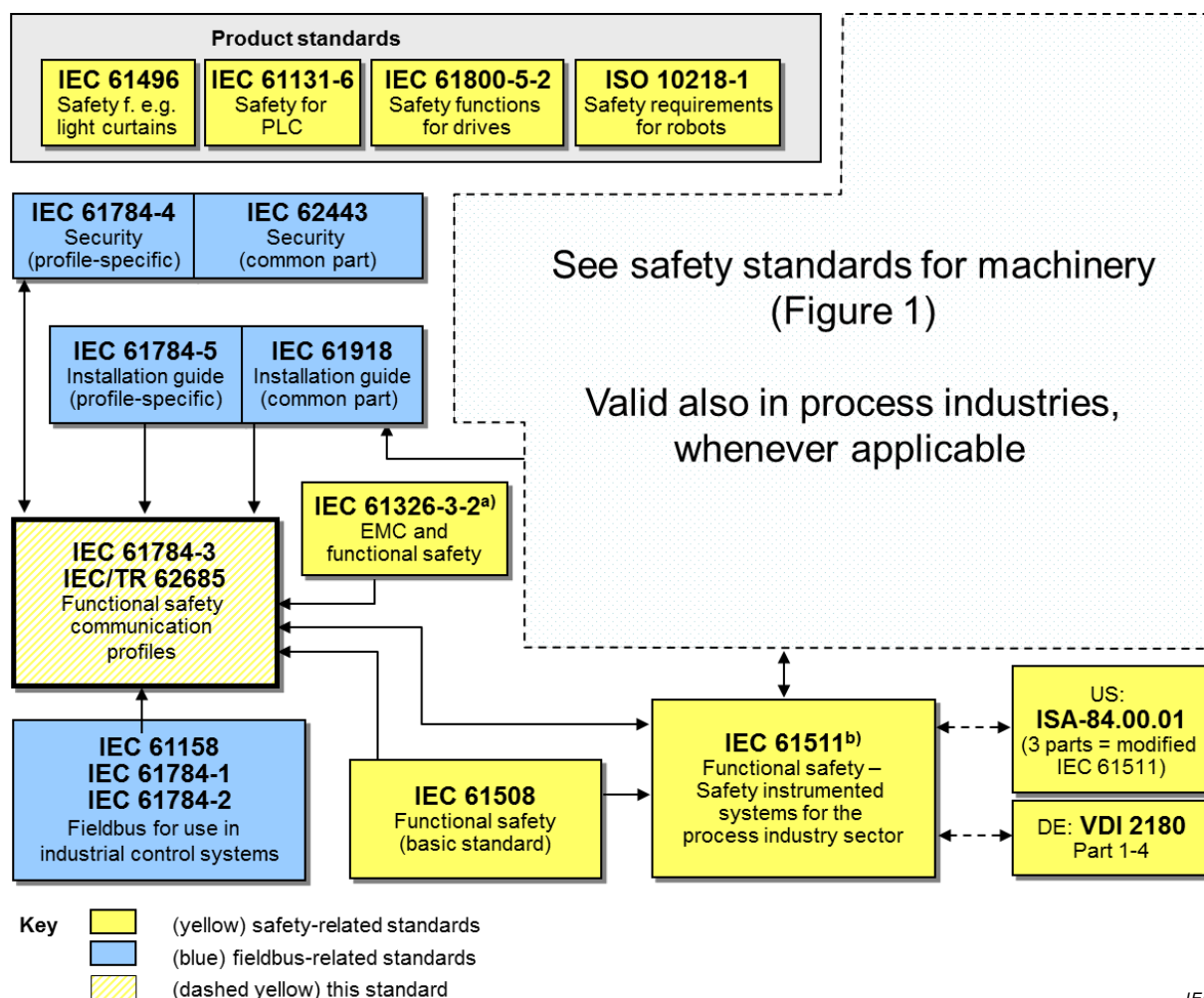
Figure 1 shows the relationships between this standard and relevant safety and fieldbus standards in a machinery environment.



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.



^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”.

IEC 61158-4-2, *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 8802-3*

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

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

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

ISO 13849-1:2006, *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*

³ To be published.

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 following terms and definitions apply.

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:—.

3.1.1.1

availability

probability for an automated system that for a given period of time there are no unsatisfactory system conditions such as loss of production

3.1.1.2

bit error probability

P_e

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

3.1.1.3

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.

3.1.1.4

bridge

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

3.1.1.5

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]

3.1.1.6

communication channel

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

3.1.1.7

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

3.1.1.8

connection

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

3.1.1.9

Cyclic Redundancy Check

CRC

<value> redundant data derived from, and stored or transmitted together with, a block of data in order to detect data corruption

<method> procedure used to calculate the redundant data

Note 1 to entry: Terms “CRC code” and “CRC signature”, and labels such as CRC1, CRC2, may also be used in this standard to refer to the redundant data.

Note 2 to entry: See also [32], [33]⁴.

3.1.1.10

defined communication system

defined channel

fixed number or fixed maximum number of participants linked by a *fieldbus* based *communication system* with well-known and fixed properties, such as installation conditions, electromagnetic immunity, industrial (*active*) *network elements*, and where the *risk* of unauthorized access is reduced to a tolerated level according to the lifecycle model of IEC 62443, using for example zones and conduits

3.1.1.11

error

discrepancy between a computed, observed or measured value or condition and the true, specified or theoretically correct value or condition

Note 1 to entry: Errors may be due to design mistakes within hardware/software and/or corrupted information due to electromagnetic interference and/or other effects.

Note 2 to entry: Errors do not necessarily result in a *failure* or a *fault*.

[SOURCE: IEC 61508-4:2010, 3.6.11, modified – notes added]

3.1.1.12

failure

termination of the ability of a functional unit to perform a required function or operation of a functional unit in any way other than as required

Note 1 to entry: Failure may be due to an *error* (for example, problem with hardware/software design or message disruption)

[SOURCE: IEC 61508-4:2010, 3.6.4, modified – notes and figures replaced]

3.1.1.13

fault

abnormal condition that may cause a reduction in, or loss of, the capability of a functional unit to perform a required function

Note 1 to entry: IEC 60050-191:1990, 191.05.01 defines “fault” as a state characterized by the inability to perform a required function, excluding the inability during preventive maintenance or other planned actions, or due to lack of external resources.

[SOURCE: IEC 61508-4:2010, 3.6.1, modified – figure reference deleted]

3.1.1.14

fieldbus

communication system based on serial data transfer and used in industrial automation or process control applications

⁴ Figures in square brackets refer to the bibliography.

3.1.1.15**DLPDU**

DEPRECATED: frame

Data Link Protocol Data Unit

3.1.1.16**hash function**

(mathematical) function that maps values from a (possibly very) large set of values into a (usually) smaller range of values

Note 1 to entry: Hash functions can be used to detect data corruption.

Note 2 to entry: Common hash functions include parity, checksum or CRC.

[SOURCE: IEC TR 62210:2003, 4.1.12, modified – addition of “usually” and notes]

3.1.1.17**hazard**

state or set of conditions of a system that, together with other related conditions will inevitably lead to harm to persons, property or environment

3.1.1.18**master**

active communication entity able to initiate and schedule communication activities by other stations which may be masters or slaves

3.1.1.19**message**

ordered series of octets intended to convey information

[SOURCE: ISO/IEC 2382-16:1996, 16.02.01, modified – character replaced by octet]

3.1.1.20**nuisance trip**

spurious trip with no harmful effect

Note 1 to entry: Internal abnormal errors can be caused in *communication systems* such as wireless transmission, for example by too many retries in the presence of interferences.

3.1.1.21**performance level**

PL

discrete level used to specify the ability of safety-related parts of control systems to perform a *safety function* under foreseeable conditions

[SOURCE: ISO 13849-1:2006, 3.1.23]

3.1.1.22**redundancy**

existence of more than one means for performing a required function or for representing information

[SOURCE: IEC 61508-4:2010, 3.4.6, modified – example and notes deleted]

3.1.1.23**reliability**

probability that an automated system can perform a required function under given conditions for a given time interval (t1,t2)

Note 1 to entry: It is generally assumed that the automated system is in a state to perform this required function at the beginning of the time interval.

Note 2 to entry: The term "reliability" is also used to denote the reliability performance quantified by this probability.

Note 3 to entry: Within the MTBF or MTTF period of time, the probability that an automated system will perform a required function under given conditions is decreasing.

Note 4 to entry: Reliability differs from *availability*.

[SOURCE: IEC TR 62059-11:2002, 3.17, modified – use of "automated system" instead of "item" and addition of two notes]

3.1.1.24

residual error rate

statistical rate at which the SCL *safety measures* fail to detect *errors*

3.1.1.25

risk

combination of the probability of occurrence of harm and the severity of that harm

Note 1 to entry: For more discussion on this concept see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6, and ISO/IEC Guide 51:2014, definition 3.9, modified – different note]

3.1.1.26

safety communication channel

communication channel starting at the top of the SCL of the source and ending at the top of the SCL of the sink

Note 1 to entry: It can be modelled as two SCLs connected by a *black channel* or a *defined communication system*, or a *defined channel*.

3.1.1.27

safety communication layer

SCL

communication layer above the FAL that includes all necessary additional measures to ensure safe transmission of data in accordance with the requirements of IEC 61508

3.1.1.28

safety connection

connection that utilizes the safety protocol for communications transactions

3.1.1.29

safety data

data transmitted across a safety network using a safety protocol

Note 1 to entry: The *Safety Communication Layer* does not ensure safety of the data itself, only that the data is transmitted safely.

3.1.1.30

safety device

device designed in accordance with IEC 61508 and which implements the functional safety communication profile

3.1.1.31

safety function

function to be implemented by an E/E/PE *safety-related system* or other *risk* reduction measures, that is intended to achieve or maintain a safe state for the EUC, in respect of a specific hazardous event

[SOURCE: IEC 61508-4:2010, 3.5.1, modified – references and example deleted]

3.1.1.32

safety function response time

worst case elapsed time following an actuation of a safety sensor connected to a *fieldbus*, until the corresponding safe state of its safety actuator(s) is achieved in the presence of *errors* or *failures* in the *safety function*

Note 1 to entry: This concept is introduced in IEC 61784-3:—, 5.2.4 and addressed by the functional safety communication profiles defined in this part.

3.1.1.33

safety integrity level

SIL

discrete level (one out of a possible four), corresponding to a range of safety integrity values, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest

Note 1 to entry: The target *failure* measures (see IEC 61508-4:2010, 3.5.17) for the four safety integrity levels are specified in Tables 2 and 3 of IEC 61508-1:2010.

Note 2 to entry: Safety integrity levels are used for specifying the safety integrity requirements of the *safety functions* to be allocated to the E/E/PE *safety-related systems*.

Note 3 to entry: A safety integrity level (SIL) is not a property of a system, subsystem, element or component. The correct interpretation of the phrase “SIL_{*n*} *safety-related system*” (where *n* is 1, 2, 3 or 4) is that the system is potentially capable of supporting *safety functions* with a safety integrity level up to *n*.

[SOURCE: IEC 61508-4:2010, 3.5.8]

3.1.1.34

safety measure

measure to control possible communication *errors* that is designed and implemented in compliance with the requirements of IEC 61508

Note 1 to entry: In practice, several safety measures are combined to achieve the required *safety integrity level*.

Note 2 to entry: Communication *errors* and related safety measures are detailed in IEC 61784-3:—, 5.3 and 5.4.

3.1.1.35

safety PDU

SPDU

PDU transferred through the *safety communication channel*

Note 1 to entry: The SPDU may include more than one copy of the *safety data* using differing coding structures and *hash functions* together with explicit parts of additional protections such as a key, a sequence count, or a *time stamp* mechanism.

Note 2 to entry: Redundant SCLs may provide two different versions of the SPDU for insertion into separate fields of the *fieldbus frame*.

3.1.1.36

safety-related application

programs designed in accordance with IEC 61508 to meet the SIL requirements of the application

3.1.1.37

safety-related system

system performing *safety functions* according to IEC 61508

3.1.1.38

slave

passive communication entity able to receive *messages* and send them in response to another communication entity which may be a *master* or a slave

3.1.1.39

spurious trip

trip caused by the safety system without a process demand

3.1.1.40

time stamp

time information included in a *message*

3.1.2 CPF 2: Additional terms and definitions

3.1.2.1

base format

format used for connection RPIs of less than 100 ms or for applications where dropped connections can be tolerated

3.1.2.2

extended format

format used for connection RPIs of more than 100 ms or for applications where there is a need to avoid dropped connections

3.1.2.3

ping

request for the consumer to acknowledge the reception of a message

3.1.2.4

ping response

response to a ping

3.1.2.5

signature

method of uniquely identifying a set of data

Note 1 to entry: This could be by revision, checksum or some other method that is agreed upon by the originating and target devices.

3.2 Symbols and abbreviated terms

3.2.1 Common symbols and abbreviated terms

CP	Communication Profile	[IEC 61784-1]
CPF	Communication Profile Family	[IEC 61784-1]
CRC	Cyclic Redundancy Check	
DLL	Data Link Layer	[ISO/IEC 7498-1]
DLPDU	Data Link Protocol Data Unit	
EMC	Electromagnetic Compatibility	
EUC	Equipment Under Control	[IEC 61508-4:2010]
E/E/PE	Electrical/Electronic/Programmable Electronic	[IEC 61508-4:2010]
FAL	Fieldbus Application Layer	[IEC 61158-5]
FS	Functional Safety	
FSCP	Functional Safety Communication Profile	
MTBF	Mean Time Between Failures	

MTTF	Mean Time To Failure	
PDU	Protocol Data Unit	[ISO/IEC 7498-1]
PFD	Probability of dangerous Failure on Demand	[IEC 61508-4:2010]
PFH	Average frequency of dangerous failure [h^{-1}] per hour	[IEC 61508-4:2010]
PhL	Physical Layer	[ISO/IEC 7498-1]
PL	Performance Level	[ISO 13849-1]
PLC	Programmable Logic Controller	
SCL	Safety Communication Layer	
SIL	Safety Integrity Level	[IEC 61508-4:2010]

3.2.2 CPF 2: Additional symbols and abbreviated terms

AIRS	Already In Requested Mode/State
BER	Bit Error Rate
BF	Base Format
CCO	Connection Configuration Object
CFUNID	Configuration UNID
CNP	Connection Point
CID	Consumer ID
CIP™ ⁵	Common Industrial Protocol (application framework shared among CPF 2 communication profiles)
CPCRC	Connection Parameter CRC
CTM	Connection Timeout Multiplier
EDS	Electronic Data Sheet
EF	Extended Format
EPI	Expected Packet Interval
LED	Light Emitting Diode
MACID	Device physical address (CP 2/3)
MOD	Module
NodeID	For CP 2/3 safety devices, this is the MACID of the device on the network. For CP 2/2 safety devices, this is the IP address of the device on the network. For CP 16/3 safety devices, this is the SDID of the device on the network.
NV	Non-Volatile
NVS	Non-Volatile Storage
OCPUNID	Output Connection Owner UNID
OSC	Object State Conflict
O-to-T	Originator to Target
OUNID	Originator UNID
PID	Producer Identifier
PS	Power Supply
Res.	Reserved
RPI	Requested Packet Interval
SCCRC	Safety Configuration Data CRC
SCID	Safety Configuration Identified
SCTS	Safety Configuration Time Stamp
SNCT	Safety Network Configuration Tool

⁵ For trade name declaration, see Clause 4.

SNN	Safety Network Number	
T-to-O	Target to Originator	
TBD	To Be Defined	
TNS	TUNID Not Set	
TUNID	Target UNID	
UML	Universal Modeling Language	[ISO/IEC 19501]
UNID	Unique Network Identifier	

3.3 Conventions

The conventions used for the descriptions of objects, services and protocols are described in IEC 61158-3-2, IEC 61158-4-2, IEC 61158-5-2, and IEC 61158-6-2.

As appropriate this part uses flow charts, UML Sequence Diagrams and “C” pseudo-code to describe concepts.

4 Overview of FSCP 2/1 (CIP Safety™)

4.1 General

Communication Profile Family 2 (commonly known as CIP™⁶) defines communication profiles based on IEC 61158-2 Type 2, IEC 61158-3-2, IEC 61158-4-2, IEC 61158-5-2, and IEC 61158-6-2.

Communication Profile Family 16 (commonly known as SERCOS®⁷) defines a communication profile CP 16/3 based on IEC 61158-3-19, IEC 61158-4-19, IEC 61158-5-19, and IEC 61158-6-19.

The basic profiles CP 2/1, CP 2/2, CP 2/3 and CP 16/3 are defined in IEC 61784-1 and IEC 61784-2. The CPF 2 functional safety communication profile FSCP 2/1 (CIP Safety™⁶) is based on the CPF 2 basic profiles in IEC 61784-1 and IEC 61784-2, the CP 16/3 basic profile in IEC 61784-2, and the safety communication layer specifications defined in this part.

4.2 FSCP 2/1

FSCP 2/1 is based on the producer/consumer model of CPF 2. The pairing of producers and consumers is an important part of the relationship that provides the high integrity needed for safety-related applications.

The FSCP 2/1 safety communication layer is specified using a Safety Validator object. This object is responsible for managing the FSCP 2/1 safety connections and serves as the interface between the safety-related application objects and the link layer connections, as shown in Figure 3. The Safety Validator ensures the integrity of the safety data transfers.

⁶ CIP™ (Common Industrial Protocol) and CIP Safety™ are trade names of the non-profit organization ODVA, Inc. This information is given for the convenience of users of this International Standard and does not constitute an endorsement by IEC of the trade name holder or any of its products. Compliance to this part does not require use of the trade names CIP™ or CIP Safety™. Use of the trade names CIP™ or CIP Safety™ requires permission of ODVA and compliance with conditions for their use (such as testing and validation).

⁷ SERCOS® is a trade name of SERCOS International e.V. This information is given for the convenience of users of this International Standard and does not constitute an endorsement by IEC of the trademark holder or any of its products. Compliance does not require use of the trade name SERCOS®. Use of the trade name SERCOS® requires permission of the trade name holder and compliance with conditions for its use (such as testing and validation).

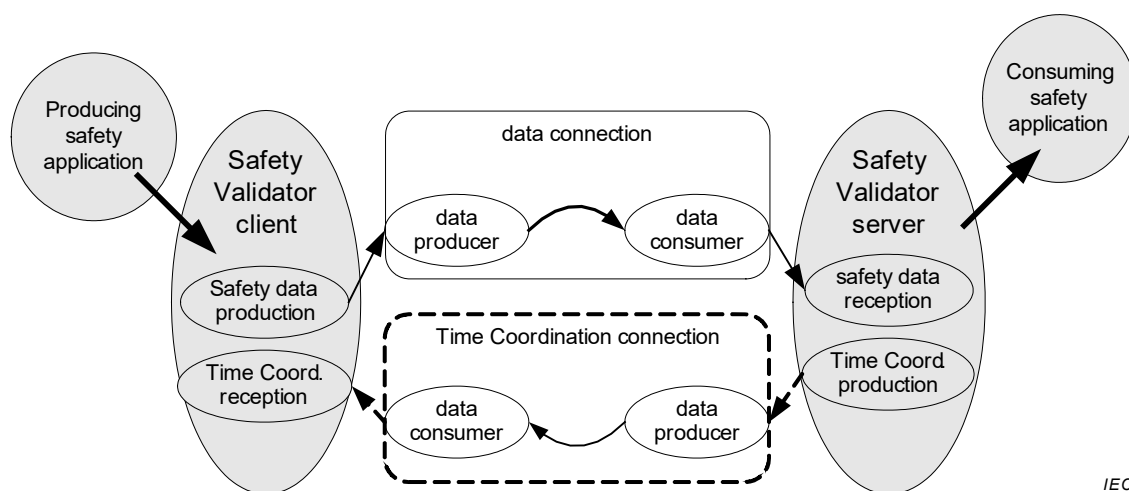


Figure 3 – Relationship of Safety Validators

The integrity of the safety data transfers is ensured as follows:

- the producing safety-related application uses an instance of a client Safety Validator to produce safety data and ensure time coordination;
- the client uses a link data producer to transmit the data and a link consumer to receive time coordination messages;
- the consuming safety-related application uses a server Safety Validator to receive and check data;
- the server uses a link consumer to receive data and a link producer to transmit time coordination messages.

FSCP 2/1 utilizes the black channel concept. The link producers and consumers have no knowledge of the safety packet and implement no safety function. The responsibility for high-integrity transfer and checking of safety data lies within the Safety Validators.

FSCP 2/1 uses the following measures to ensure the integrity of safety messaging:

- time stamp;
- connection authentication;
- data integrity assurance;
- redundancy with cross checking;
- different data integrity assurance systems.

Messages are produced with a timestamp that allows the consumer to verify the age of data being sent. Identification is encoded into each safety-related message to ensure that the correct consumer is using the message. All safety-related messages use a unique CRC. Safety-related data is sent redundantly. Diverse measures for producing safety-related messages are used to ensure that standard CPF 2 messages are not interpreted as safety messages.

5 General

5.1 External documents providing specifications for the profile

The following document is especially useful in understanding the design of FSCP 2/1 protocols:

- GS-ET-26 [30]

5.2 Safety functional requirements

The following requirements shall apply to the development of devices that implement the FSCP 2/1 protocol. The same requirements were used in the development of FSCP 2/1.

- The FSCP 2/1 protocol is designed to support Safety Integrity Level 3 (SIL3) (see IEC 61508), and PLe/category 4 (see ISO 13849-1).
- The safety state for discrete data is the unenergized state (0). For analog values the unenergized state shall be defined by the safety-related application.
- The basic requirements for the development of the FSCP 2/1 protocol are in IEC 61784-3.
- FSCP 2/1 protocol is implemented using a black channel approach; there is no safety related dependency on the standard CPF 2 communication profiles.
- Implementations of FSCP 2/1 shall comply with IEC 61508.
- Environmental conditions shall be according to IEC 61131-2 for the basic levels and IEC 61326-3-1, IEC 61326-3-2 for the safety margin tests, unless there are specific product standards.
- Safety communication and standard communication shall be independent. However, standard devices and safety devices shall be able to use the same communication channel.
- Unless specified in this part, the CPF 2 requirements shall be unchanged for safety.

5.3 Safety measures

Table 1 contains the measures used to detect communication errors and the coverage provided by each measure as used.

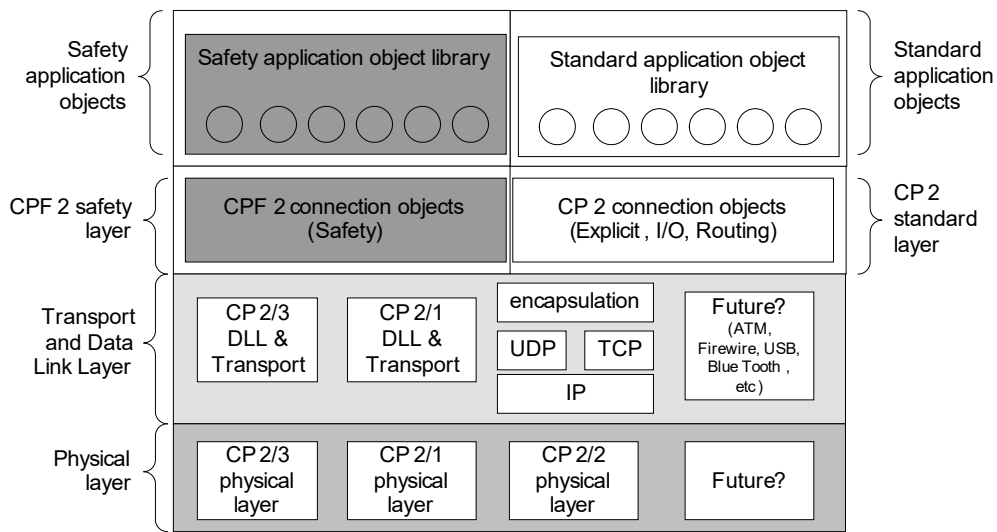
Table 1 – Communications errors and detection measures matrix

Communication errors	Safety measures							
	Sequence number	Time stamp	Time expectation	Connection authentication	Feedback message	Data integrity assurance	Redundancy with cross checking	Different data integrity assurance systems
Corruption						X	X	
Unintended repetition		X				X ^a	(X) ^e	
Incorrect sequence		X				X ^a	(X) ^e	
Loss			X ^c			X ^a	(X) ^e	
Unacceptable delay		(X) ^e	X					
Insertion		X ^d		X		X ^a	(X) ^e	
Masquerade		X ^d		X		X ^b	X ^f	X
Addressing				X		X ^b		
^a The safety related CRC provides additional protection for communication errors in messages. ^b Encoding the unique identifier into the safety related CRC prevent masquerade and addressing errors. ^c A message not received within the time expectation will be detected. ^d Masquerade or inserted messages will not have the expected time stamp. ^e Not claimed for FSCP 2/1. ^f Masquerade will likely not have redundant data and will fail the cross-check.								

5.4 Safety communication layer structure

The safety protocol is layered on top of the standard network protocol (the standard protocol stack is a black channel). Figure 4 shows how the safety communication layer is related to the existing CPF 2 layers.

The safety layers accept safety data from the safety-related application circuit. The safety layers then formulate a safety message, transmit the safety message, receive and decode the safety message. Once the safety message is decoded and verified, the data is presented to the receiving safety-related application circuit.



IEC

Figure 4 – Communication layers

5.5 Relationships with FAL (and DLL, PhL)

5.5.1 General

This safety communication layer shall only be used in conjunction with CPF 2 communication profiles (CP 2/3 (DeviceNet™⁸), CP 2/2 (EtherNet/IP™⁹), and CP 16/3 (SERCOS III™¹⁰)). There are no requirements of CPF 2 communications profiles other than those defined in this part.

5.5.2 Data types

Profiles defined in this part support all the CPF 2 data types as defined in IEC 61158-5-2.

6 Safety communication layer services

6.1 Introduction

This Clause 6 defines the extensions to existing CPF 2 objects and new objects for Safety. Safety connections use Class 0 connections for I/O messages. Standard Explicit message connections are used for the establishment of Safety I/O connections.

⁸ DeviceNet™ is a trade name of the non-profit organization ODVA, Inc. This information is given for the convenience of users of this International Standard and does not constitute an endorsement by IEC of the trade name holder or any of its products. Compliance to this part does not require use of the trade name DeviceNet™. Use of the trade name DeviceNet™ requires permission of ODVA.

⁹ EtherNet/IP™ is a trade name of ODVA, Inc. This information is given for the convenience of users of this International Standard and does not constitute an endorsement by IEC of the trade name holder or any of its products. Compliance to this part does not require use of the trade name EtherNet/IP™. Use of the trade name EtherNet/IP™ requires permission of ODVA.

¹⁰ SERCOS® and SERCOS® interface are trade names of SERCOS International e.V. This information is given for the convenience of users of this International Standard and does not constitute an endorsement by IEC of the trademark holder or any of its products. Compliance to this profile does not require use of the trade name SERCOS®. Use of the trade name SERCOS® requires permission of the trade name holder.

6.2 Connection object

6.2.1 General

Several safety specific class attributes and services are defined to support safety. CP 2/3 Safety nodes which reside on FSCP 2/1 shall implement the SafetyOpen and SafetyClose services of the Connection object.

6.2.2 Class attribute extensions

Table 2 defines the class attributes used by safety devices.

Table 2 – New class attributes

Attrib ID	Need in implementation	Access rule	N V	Name	Date type	Description of attribute
8	Optional	Get	V	Connection request error count	UINT	Diagnostic Counter that is a running count of SafetyOpen or SafetyClose faults ^a
9	Optional	Get	V	Safety connection counters	STRUCT of:	Status counters
				SafetyOpen request success count	UINT	Count of successful SafetyOpen requests issued from this node to another target
				SafetyOpen request failure count	UINT	Count of unsuccessful SafetyOpen requests issued from this node to another target
				SafetyClose request success count	UINT	Count of successful SafetyClose requests issued from this node to another target
				SafetyClose request failure count ^b	UINT	Count of unsuccessful SafetyClose requests issued from this node to another target
				SafetyOpen indication success count	UINT	Count of successful SafetyOpen requests issued from an external originator to this node
				SafetyOpen indication failure count ^b	UINT	Count of unsuccessful SafetyOpen requests issued from an external originator to this node
				SafetyClose indication success count	UINT	Count of successful SafetyClose requests issued from an external originator to this node
				SafetyClose indication failure count ^b	UINT	Count of unsuccessful SafetyClose requests issued from an external originator to this node

^a Attribute 8 is the sum of the 4 failure counters in attribute 9. Having this single attribute represent connection errors can be used in monitoring software to efficiently monitor errors without polling the additional attribute 9 structures. Once attribute 8 is non-zero then the monitoring software can examine attribute 9 for more details.

^b Included in class attribute 8.

6.2.3 Service extensions

Table 3 defines services for use by CP 2/3 safety devices on FSCP 2/1. These services shall be supported by a target device on FSCP 2/1. The SafetyOpen and SafetyClose services, used in lieu of the ForwardOpen and ForwardClose services of the Connection Manager object, inherit the identical behavior from those Connection Manager services.

Table 3 – Service extensions

Service code	Need in implementation		Service name	Description of service
	Class	Instance		
4D _{hex}	Optional	N/A	Reset Counters	This service resets class attributes 8 and 9 to zero
4E _{hex}	Required	N/A	SafetyClose	Used to close a Safety I/O connection. See the ForwardClose service of the Connection Manager object 6.3.13
54 _{hex}	Required	N/A	SafetyOpen ^a	Used to establish a safety I/O connection. See the ForwardOpen service of the Connection Manager object 6.3.2
^a The SafetyOpen service data shall contain a Safety Network Segment in the Connection_Path field.				

6.2.4 Explicit message response format for SafetyOpen and SafetyClose

The SafetyOpen and SafetyClose service responses have a common response format. This format contains status information for both success and failure. If the service response is a success, response data specific to each service is returned. If the service response is an error, a successful FSCP 2/1 status indicated by the general error code FF_{hex} is returned, along with a variable amount of extended error information.

The response format for the SafetyOpen and SafetyClose object Specific services are defined in Table 4:

Table 4 – SafetyOpen and SafetyClose response format

Parameter name	Data type	Description of response parameter
Reserved	USINT	Reserved
General status	USINT	One of the general status codes listed in IEC 61158-6-2 (status codes)
Size of additional status	USINT	Number of 16 bit words in Additional status array
Additional status	ARRAY of UINT	Additional status
Response data	ARRAY of OCTET	Response data from request or additional error data if general status indicated an error

The Response Data and General/Additional Statuses for the SafetyOpen and SafetyClose services shall match the Response Data and General/Additional Statuses for the ForwardOpen and ForwardClose services of the Connection Manager object, respectively.

6.3 Connection Manager object

6.3.1 General

CP 2/2 and CP 16/3 safety devices shall use a ForwardOpen with a Safety Network Segment to establish safety connections. This segment uniquely identifies the ForwardOpen service as a safety ForwardOpen. Throughout this subclause 6.3, the term “SafetyOpen” shall refer to both the ForwardOpen service of the Connection Manager object (when containing a Safety Network Segment) and the SafetyOpen service of the Connection object.

6.3.2 ForwardOpen for safety

6.3.2.1 ForwardOpen for safety contents

The contents of the ForwardOpen service of the Connection Manager object, including the safety network segment, are outlined in Figure 5 below. The proper settings for the various parameters in the ForwardOpen are given in Figure 5.

Parameter Name		Data Type / Size	Target Destination and Semantics
Priority/Time_tick		OCTET	Connection manager servicing request
Time-out_ticks		USINT	Connection manager servicing request
O-to-T Network Connection ID		UDINT	Consuming connection instance:: CIP consumed connection ID
T-to-O Network Connection ID		UDINT	Producing connection instance:: CIP producing connection ID
Connection Serial Number		UINT	Value: Unique (to originator) 16-bit number. Destination: Connection manager servicing request
Originator Vendor ID		UINT	Connection manager servicing request
Originator Serial Number		UDINT	Connection manager servicing request
Connection Timeout Multiplier		USINT	Producing and consuming connection instance: Timeout Multiplier
Reserved		3 OCTETS	
O-to-T RPI		UDINT	Consuming connection instance: EPR
O-to-T Network Connection Parameters	Redundant Owner	WORD	Value: 0 (Safety Connections do not support redundancy); Destination: Connection Manager
	Connection Type		Value: Point-to-point; Destination: Connection Manager
	Priority		Value: High Priority; Destination: Connection Manager
	Fixed/Variable		Value: Fixed; Destination: Connection Manager
	Connection Size (in octets)		Value: Size of safety PDU including the Mode Octet, Actual, Complement, and Time stamp sections Destination: Consuming connection instance: Consumed connection size attribute
T-to-O RPI		UDINT	Producing connection instance: EPR
T to O Network Connection Parameters	Redundant Owner	WORD	Value: 0 (Safety connections do not support redundancy); Destination: Connection Manager
	Connection Type		Value: Point-to-point; Destination: Connection Manager
	Priority		Value: High Priority; Destination: Connection Manager
	Fixed/Variable		Value: Fixed; Destination: Connection Manager
	Connection Size (in octets)		Value: Size of safety PDU including the Mode Octet, Actual, Complement, and Time stamp sections. Destination: Producing Connection Instance: Produced connection size
Transport Type/Trigger		SWORD	Value: Safety single or multipoint. Destination: Validator instance. Trigger always set to Application. Client/Server: depending on direction

Parameter Name			Data Type / Size	Target Destination and Semantics	
Connection_Path_Size			USINT	Number of 16 bit words in the Connection_Path field – destination is Connection Manager servicing request. NOTE Value included in CRC calculation does not include the words used for Network/Port segments.	
Connection_Path (Padded EPATH)	Path			Variable	Consumed by intermediate bridge connection manager(s). Each Router Format-safety Network Segment immediately follows the (CPF 2 – to-CPF 2) bridge for which it is intended
	Logical Segment: Electronic Key	Vendor ID	UINT	Value: Electronic Key of required target. Servicing Connection Manager or Connection object	
		Prod Type	UINT		
		Prod Code	UINT		
		Compatible/ Major Rev	SWORD		
		Minor Rev	USINT		
	Application Path 1	Logical Segment: Class	Variable; 1 word typically	Refer to IEC 61158-6-2 for rules on setting/parsing these paths	
		Logical Segment: Instance	Variable; 1 word typically		
	Application Path 2	Logical Segment: Connection Point	Variable; 1 word typically	Refer to IEC 61158-6-2 for rules on setting/parsing these paths	
	Application Path 3	Logical Segment: Connection Point	Variable; 1 word typically	Refer to IEC 61158-6-2 for rules on setting/parsing these paths	
	Config Data		Data Segment: Simple Data	Variable	Configuration data to apply to the Safety-related application object identified by Config Path
	Network Segment: Safety	Safety Segment Name		50 _{hex}	Safety Network Segment
		Segment Size		USINT	Target format size = 54 octets
		Segment Format		USINT	Target format = 0
Network Safety Data		ARRAY of OCTET	Safety Network Segment data		

Key

	= Connection/Safety Validator fields covered by Connection Parameters CRC
	= Configuration Data Segment covered by SCCV

Figure 5 – ForwardOpen with safety network segment

6.3.2.2 ForwardOpen for safety for Extended Format

Safety Originators that support the Extended Format may connect to Targets with RPI's of 100 ms or less with either the Extended Format (EF) or the Base Format (BF).

Safety Originators that connect with a CP 2/2 target, a CP 16/3 target, or a CP 2/3 target with a CP 2/2 hop or CP 16/3 hop within the path and have an RPI of greater than 100 ms shall use the Extended Format.

A variety of methods may be used to assure this. EDS files and configuration software can pre-configure the choice, or the originator can use a dynamic algorithm to make the determinations.

The mechanism used by the originator to indicate to a target that the Extended Format is being requested will be with a new Safety Network Segment Format as defined in 6.3.3.

6.3.3 Safety network segment

6.3.3.1 Common format

The Safety Connection Parameters Segment Type has been added to the CPF 2 Network Segment definition as segment type 10_{hex} (resulting in a segment value of 50_{hex}). The updated Network Segment definition is defined in Table 5.

Table 5 – Safety network segment identifier

Network segment type	Network segment name
50 _{hex}	Safety segment

The format of the Safety Network Segment is defined in Table 6. This segment type is in the range of Network Segment types, which contains a data size field. The Safety Segment Format parameter, the first parameter in the data area, indicates which data follows.

Table 6 – Safety network segment definition

Octet offset	Field name	Data type	description
0	Segment Type	SWORD	Indicates Safety Network Segment (50 _{hex})
1	Network Segment data length	SWORD	Length of segment data to follow (in words)
2	Safety Network Segment format	USINT	Indicates type of Safety Network Segment 0 = Target format 1 = Router format 2 = EF format 3 – 255 = Reserved
3 – n	Safety Network Segment data	ARRAY of OCTET	Safety Network Segment data, defined by segment format

6.3.3.2 Safety network segment: target format (00_{hex})

The target format is directed at the target of the connection. The value of the Network Segment Data Length parameter shall be 27 (1b_{hex}) which corresponds to 27 WORDS. Figure 6 defines the safety network target format.

Field name	Data type	Description
Reserved	SWORD	Pad
Configuration CRC (SCCRC)	UDINT	CRC-S4 of target Config Data Segment. A value of 0 is an indicator that SCID check can be skipped
Configuration Time Stamp (SCTS)	DATE_AND_TIME	Time and Date stamp of the configuration. A value of 0 is an indicator that SCID check can be skipped. 6 octet value (Date: 2 octets, Time: 4 octets)
Time Correction EPI	UDINT	Not used: 0 When used: Time Correction Connection Instance:: EPI
Time Correction Network Connection Parameters	WORD	Network Connection Parameters for the Time Correction connection. This field uses the same definition as the Network Connection Parameter within the Connection Manager object. When not used: 0 (Null). When used: Fixed, High Priority, Multipoint
Target_UNID (TUNID)	STRUCT of: 10 OCTETS	UNID of the target device. This value is a 10 octet value consisting of the Safety Network Id (6 octets) and the Node Address (4 octet address)
Originator UNID (OUNID)	STRUCT of: 10 OCTETS	UNID of the Originator device. This value is a 10 octet value consisting of the Safety Network Id (6 octets) and the Node Address (4 octet address)
Ping_Interval_EPI_Multiplier	UINT	Number that defines the Ping_Count_Interval for the connection. Valid range of values is given in 7.7.5.10
Time_Coord_Msg_Min_Multiplier	UINT	For Producing Connection Instance. Valid range is 0 to 7 813
Network_Time_Expectation_Multiplier	UINT	For Consuming Connection Instance. Valid range is 1 to 45 313
Timeout_Multiplier	USINT	Used by producer and consumer to timeout connections. Valid range 1 to 4
Max_Consumer_Number	USINT	Value: 1 (Point-to-point), 2-15(Multipoint)
Connection Parameters CRC (CPCRC)	UDINT	CRC-S4 of target connection parameters in this request
Time Correction Connection ID	UDINT	Not Used: FFFFFFFF _{hex} When used: Time Correction Connection Instance:: Connection ID

Key

 = Safety Segment fields covered by Connection Parameters CRC

Figure 6 – Safety network target format**6.3.3.3 Safety network segment: router format (01_{hex})**

The router format is directed at an intermediate router along the connection path when that router needs to know this is a Safety ForwardOpen. Currently, only CP 2/3 routers need this network segment directed to them. The Network Segment is applied to the subnet from which the connection request originated. Router Format Safety Network Segments only appear in the Path portion of the Connection_Path of a Safety ForwardOpen. The total segment length is 6 words. The safety network segment router format is defined in Table 7.

Table 7 – Safety network segment router format

Field name	Data type	Description
Reserved	SWORD	Reserved, value = 0
Time Correction Connection ID	UDINT	Not Used: FFFFFFFF _{hex} When used: Time Correction connection instance:: Connection ID
Time Correction EPI	UDINT	Not used: 0 When used: Time Correction connection instance:: EPI
Time Correction Network Connection Parameters	WORD	Network Connection Parameters for the Time Correction connection. This field uses the same definition as the Network Connection Parameter within the Connection Manager object. Not used: 0 (Null). When used: Fixed, High Priority, Multipoint

6.3.3.4 Safety network segment: Extended Format (0x02)

The Extended Format is directed at the target of the connection and shown in Table 8.

All EF safety connections shall be established using the Extended Format safety network segment in a Forward Open (CP 2/2 or CP 16/3) or a SafetyOpen (CP 2/3).

Table 8 – Safety Network Segment Extended Format

Field Name	Data Type	Description
Reserved	octet	Pad
Configuration CRC (SCCRC)	UDINT	CRC-S32 of target Config Data Segment. A value of 0 is an indicator that SCID check can be skipped
Configuration TimeStamp (SCTS)	DATE_AND_TIME	Time and Date stamp of the configuration. A value of 0 is an indicator that SCID check can be skipped. 6 octet value (Date: 2 octets, Time: 4 octets)
Time Correction EPI	UDINT	Not used: 0 When used: Time Correction Connection Instance:: EPI
Time Correction Network Connection Parameters	WORD	Network Connection Parameters for the Time Correction connection. This field uses the same definition as the Network Connection Parameter within the Connection Manager object. When not used: 0 (Null). When used: Fixed, High Priority, Multipoint
Target_UNID (TUNID)	STRUCT of: UINT 10: octets	UNID of the target device. This value is a 10 octet value consisting of the Safety Network Id (6 octets) and the Node Address (4 octet address)
Originator UNID (OUNID)	STRUCT of: UINT 10: octets	UNID of the Originator device. This value is a 10 octet value consisting of the Safety Network Id (6 octets) and the Node Address (4 octet address)
Ping_Interval_EPI_Multiplier	UINT	Number that defines the Ping_Count_Interval for the connection. Valid range of values is given in 7.7.5.10
Time_Coord_Msg_Min_Multiplier	UINT	For Producing Connection Instance. Valid range is 0 to 7 813
Network_Time_Expectation_Multiplier	UINT	For Consuming Connection Instance. Valid range is 1 to 45 313

Field Name	Data Type	Description
Timeout_Multiplier	USINT	Used by producer and consumer to timeout connections. Valid range of 1 to 255 for HiAvailabilityFormat
Max_Consumer_Number	USINT	Value: 1 (Point to point), 2-15(Multipoint)
Max_Fault_Number	UINT	Used by both producers and consumers to determine how many erroneous packets can be dropped before a connection shall be closed. Valid range is 0 to 255 ^b Default = 5. A value of 0 indicates connections shall be closed on any detected error
Connection Parameters CRC (CPCRC)	UDINT	CRC-S32 of target connection parameters in this request
Time Correction Connection ID ^a	UDINT	Not Used: 0xFFFFFFFF When used: Time Correction Connection Instance:: Connection ID
Initial Time Stamp ^a	UINT	Used by Consumer to initialize Last_Time_Stamp_for_Rollover. Consuming Originator sets to 0xFFFF
Initial Rollover Value ^a	UINT	Used by Consumer to initialize TS_Rollover_Count. Consuming Originator sets to 0xFFFF
^a These fields are NOT included in the CPCRC.		
^b See 8.8.3 for originator configuration rules and restrictions		

6.3.4 Originator rules for calculating the connection parameter CRC

The Connection Parameter CRC (CPCRC) is only calculated when a connection is initially configured or when that connection configuration is changed. This value remains static in the originator otherwise.

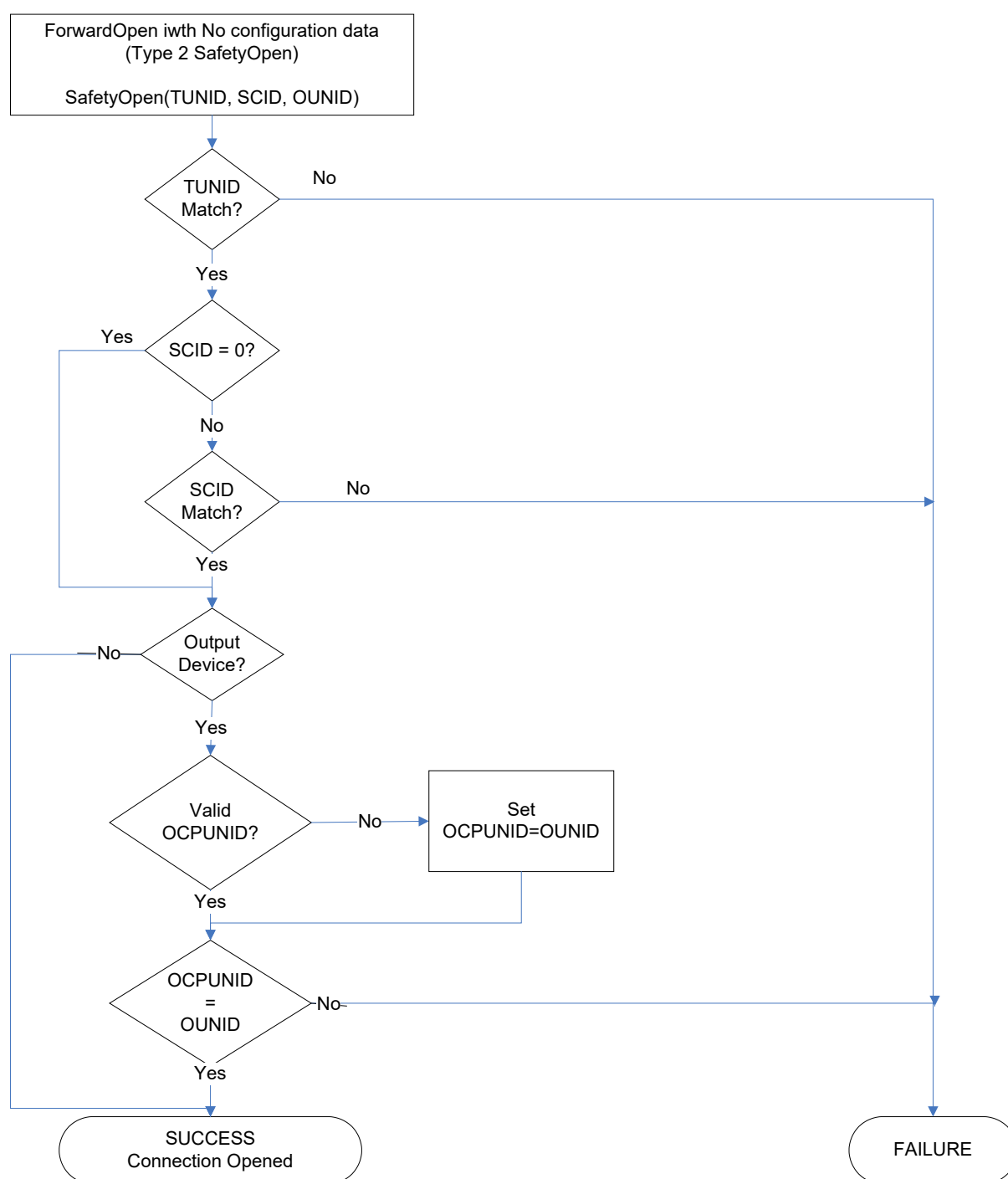
The connection path size in the SafetyOpen changes value depending on whether an originator is sending configuration data or not. Since this field is included in the CPCRC calculation, originators need to calculate and maintain two values when they support the SafetyOpen configuration function. One value is used when configuring a device while opening the connection and the other value is used when just opening the connection (no configuration data is included).

Also, the path size shall be “pre-adjusted” to remove the path entries that get stripped off by routers as the Safety ForwardOpen traverses each sub-net. The requirement is that the originator is responsible for calculating the CPCRC value based on what the SafetyOpen or ForwardOpen will be when the target receives it so that the target can perform a simple calculation in all cases.

6.3.5 SafetyOpen processing flowcharts

The following flowcharts outline the required behavior of a target upon receipt of a SafetyOpen:

- Verify the Connection Parameter CRC. As depicted in Figure 6, the connection parameter CRC covers the SafetyOpen fields that will be used by the target. Routers along the path shall not modify these fields;
- The target checks that the electronic key segment matches (see 6.3.7);
- Depending on the type of safety connection, the logic is defined in Figure 7 or Figure 8 shall be followed.



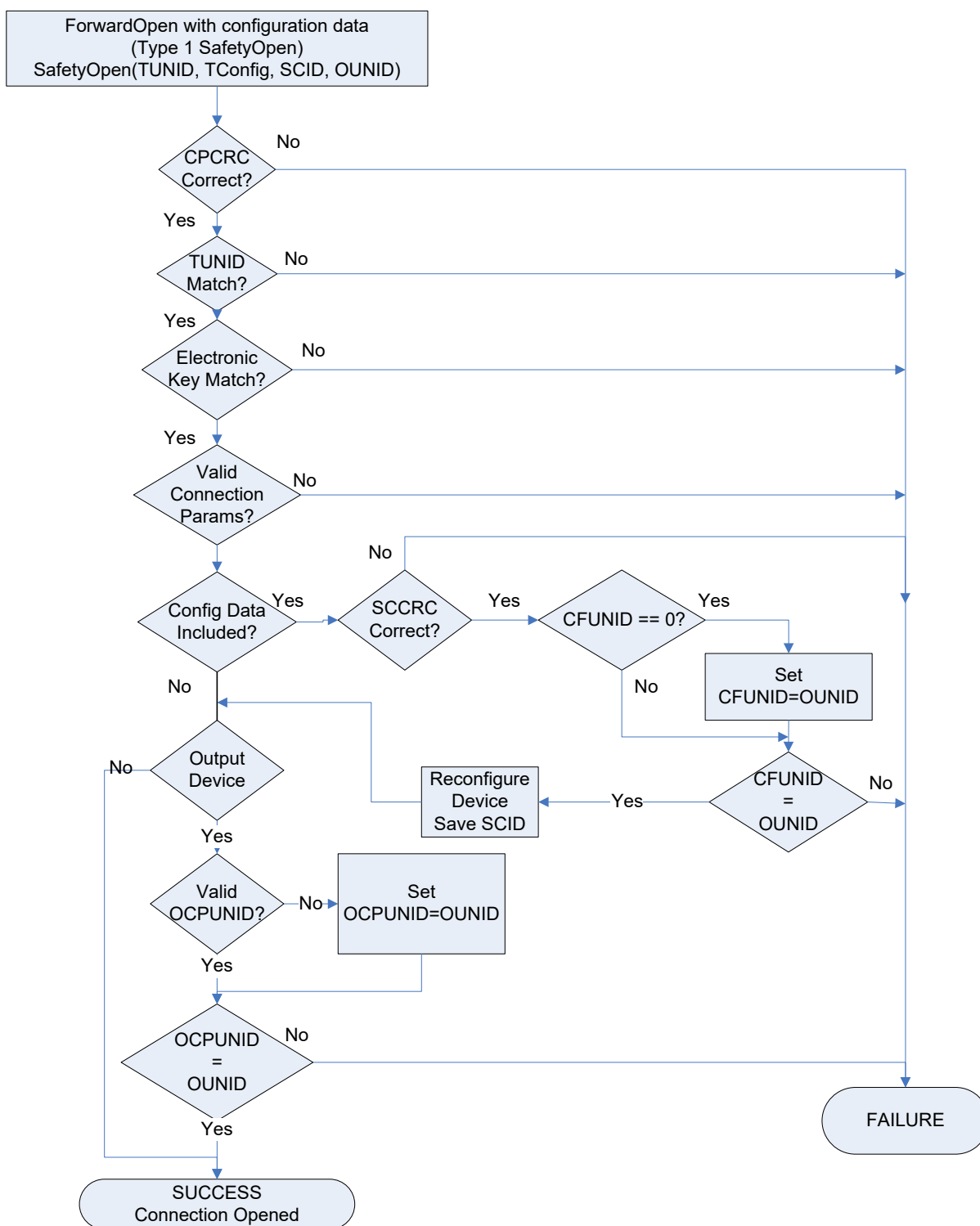
Key:

UNID = Unique Network Identifier
 SCID = Target's Safety Configuration ID
 OCP = Output Connection Point
 CFUNID = Configuration Owning UNID

TUNID = Target's Unique Network Identifier
 OUNID = Originator's Unique Network Identifier
 OCPUNID = Output Connection Owning UNID

IEC

**Figure 7 – Target Processing SafetyOpen with no configuration data
(Form 2 SafetyOpen)**



Key:

UNID = Unique Network Identifier

CPCRC = Connection Parameter CRC

SCCRC= CRC portion of the SCID

OCPUNID = Output Connection Owning UNID

TUNID = Target's Unique Network Identifier

SCID = Target's Safety Configuration ID

OUNID = Originator's Unique Network Identifier

CFUNID = Configuration Owning UNID

IEC

**Figure 8 – Target Processing for SafetyOpen with configuration data
(Form 1 SafetyOpen)**

Safety Originators that do not support any other means to determine which format to connect with can implement the logic shown in Figure 9 to dynamically determine the format.

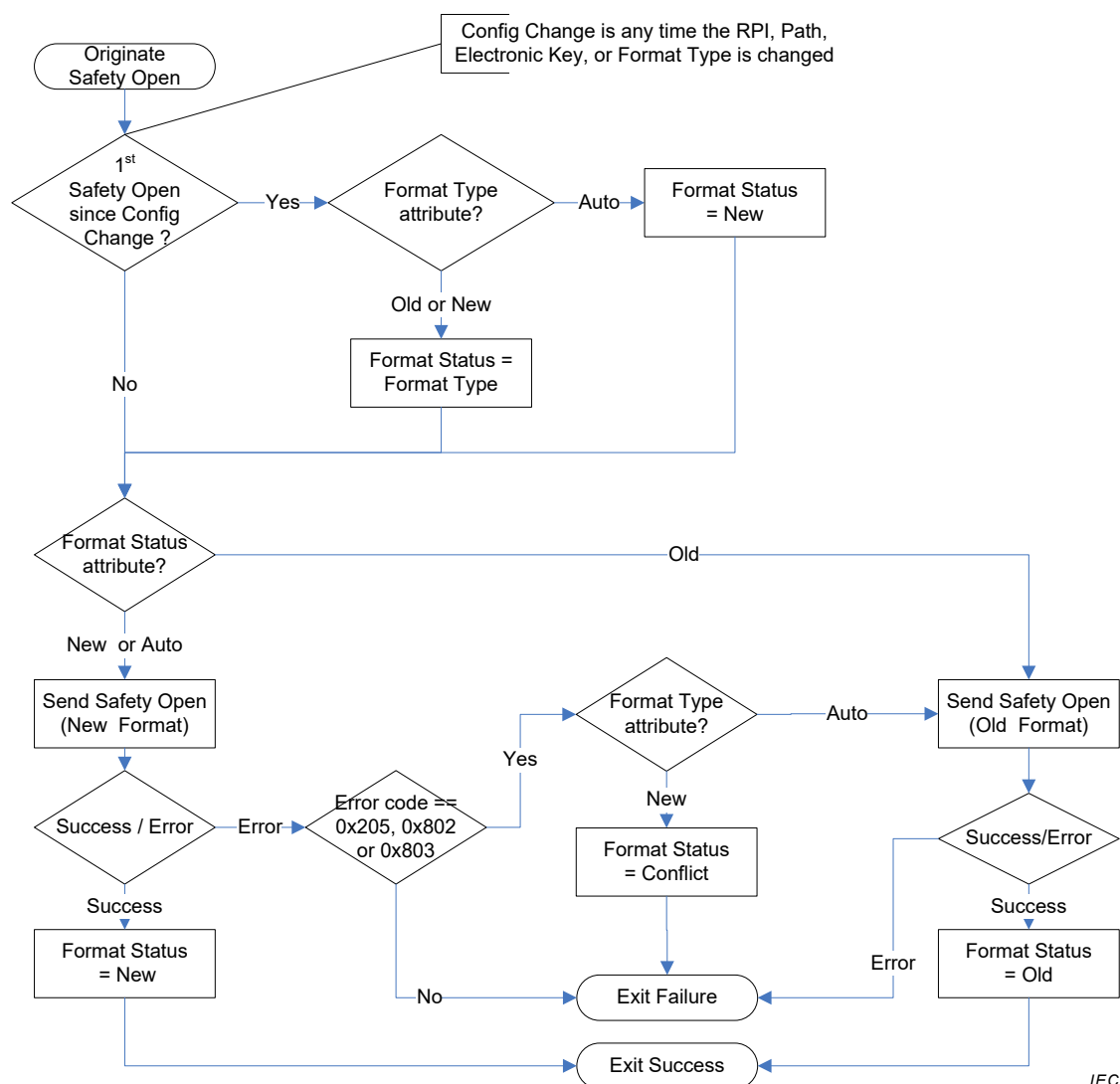


Figure 9 – Originator logic to determine which format to use

6.3.6 Checks required by Multipoint producers with existing connections

There is a distinct possibility that the safety parameters used in a ForwardOpen or SafetyOpen from various consuming originators will not always be the same. A consistent set of rules shall be used for how a Multipoint producing target evaluates these parameters when they conflict with other already established consuming connections. Table 9 defines the multipoint producer parameter evaluation rules.

Table 9 – Multipoint producer parameter evaluation rules

Safety parameter	Producer evaluation rule if connection exists	Error response ^a (if appropriate)	
		General	Extended
Ping_Interval EPI Multiplier	Shall match existing P.I.E.M.	01 _{hex} 00 _{hex}	0801 _{hex} 0012 _{hex}
Time Coord Msg Min Multiplier	Accept any (all can be different)	N/A	
Network Time Expectation Multiplier	Accept any (all can be different)	N/A	
Timeout_Multiplier	Accept any (all can be different)	N/A	
Max_Consumer_Number	Shall match existing Max_Consumer_Number	00 _{hex} 01 _{hex}	0801 _{hex} 002A _{hex}
T-to-O RPI, O-to-T RPI, and Time Correction RPI	Shall match existing connection RPIs	01 _{hex}	0111 _{hex}
Network Segment Type	Shall match existing connection format ^b	0x01	0x803
Max_Fault_Number	Accept any (all can be different)	N/A	
^a At the option of the device developer, another connection could also be opened rather than return an error response.			
^b Subsequent connection requests on an existing multi-point connection shall all be the same format as the existing connection			

6.3.7 Electronic key usage for safety

Safety originators and targets shall meet the following requirements for use of the Electronic Key segment within a SafetyOpen.

The Electronic Key segment shall be present in all SafetyOpen or Safety ForwardOpen service requests.

The Electronic Key shall always be processed by Target devices with integrity (cannot be confirmed externally).

The compatibility bit and behavior in the Electronic Key shall be supported as defined by safety originators and targets. Wildcards (fields set to 0) for individual fields within the Electronic Key shall not be supported.

6.3.8 RPI vs. API in safety connections

Safety devices do not have the ability to negotiate the RPI value. Safety Targets either accept the requested RPI because it can be supported, or it rejects it completely. The tolerance around an acceptable RPI request shall be $\pm 128 \mu\text{s}$.

The T-to-O API, O-to-T API, and Time Correction API in a success response shall always be the same value received in the SafetyOpen.

6.3.9 Application path construction for safety

IEC 61158-6-2 defines a method to construct an application path in a SafetyOpen for 3 references: one for configuration, one for consumed data and one for produced data.

The possible path types are identified as follows:

A. - [Class] [Assembly] [Instance] [Configuration-instance]

- B. - [Class] [Assembly] [Instance] [Producer-instance]
- C. - [Class] [Assembly] [Instance] [Consumer-instance]
- D. - [Class] [Assembly] [Instance] [Device-defined NULL instance]
- E. - [CNP] [Consumer CNP]
- F. - [CNP] [Producer CNP]
- G. - [CNP] [Device-defined NULL CNP]

When all 3 paths referenced the same class, they are often formatted in a compressed format: (CNP stands for Connection Point).

[Class] [Class #] [Instance] [Instance #] [CNP] [Consumer CNP] [CNP] [Producer CNP]

Since all three paths shall reference the same class, a NULL instance value shall be reserved in that class (by the device developers) to use the compressed form for safety. The NULL value will be used for the portion of the path that references the Time Coordination connection and configuration connection (in non-configuring originators). If a common class reference is not practical, the long form shall be used.

The following rules apply to SafetyOpen path construction:

- all devices shall support the long form at a minimum;
- a Null path or Null connection point shall be used to represent the Time Coordination connection;
- a Null path or Null connection point shall be used for the configuration path when no configuration data can ever be sent on the connection;
- on any connections, which can accept a Form 1 SafetyOpen, Originators shall always send a valid configuration path even if no configuration data is present (i.e. Form 2a).

The “Null” path or connection point used shall be one of the module’s choosing. The method of making this selection in an EDS file will be via the Data Path field in the Connection Manager section. Devices configured by configuration applet also shall provide this path.

Safety device designers can choose the path format to specify in their EDS files from the following options. The possible three-path combinations for Form 1, 2a SafetyOpen on connections, which will accept configuration are:

- [A, D, B] for the input connection;
- [A, G, F] compressed format for input connections;
- [A, C, D] for the output connection;
- [A, E, G] compressed format for output connections.

The possible three-path combinations for Form 2a, 2b SafetyOpen on connections, which will not accept configuration data are:

- [D, D, B] for the input connection;
- [D, G, F] compressed format for input connections;
- [D, C, D] for the output connection;
- [D, E, G] compressed format for output connections.

6.3.10 Safety Validator connection types

The Safety Validator function, depending on the safety connection type provided in the SafetyOpen, will always require between 2-3 connection resources. The SafetyOpen contains the connection information to allow a target to set up these connections appropriately. This

subclause 6.3.10 will show how the connection types are determined by how the SafetyOpen shall be filled out.

One basic assumption is that connections for Time Coordination and Time Correction messages do not require a path entry since they have an implied path to the Safety Validator object coordinating the safety connection. The various connection scenarios are described in the Validator object in 6.7.

The Safety Validator function can determine which connection resources will be required by looking at the parameter in the SafetyOpen. The various SafetyOpen parameters as well as the key parameters that the safety function will need to determine the types of connections are defined in Table 10. Connection object instances may not be available due to target identifier capacity or limitations; there may be no unallocated connection identifiers. Or the device may not have the processing throughput to handle the additional connection; etc. Safety Connection objects requires resources similar to standard I/O connections.

Table 10 – ForwardOpen setting options for safety connections

O-to-T connection type	T-to-O connection type	Transport type/trigger	App path 1	App path 2 ^a	App path 3 ^a	Max consumer number	Safety Validator connection type	Key decision factors	Target role
Point-to-point	Point-to-point	Application, Class 0, Client	Vendor defined Null Path ^b	Vendor defined Null Path	Safety Input App. object	1	Point-to-point Producer (Input)	2-point-to-point + Client	Producing connection: Safety data Consumer connection: Coordination
Point-to-point	Point-to-point	Application, Class 0, Server	Vendor defined Null Path	Safety Output App. object	Vendor defined Null Path	1	Point-to-point Consumer (Output)	2- point-to-point + Server	Consuming connection: Safety data Producing connection: Coordination
Point-to-point	Multipoint	Application, Class 0, Client	Vendor defined Null Path	Vendor defined Null Path	Safety Input App. object	2-15	Multipoint Producer CP 2/3	2 – Multipoint + 1 point-to-point + Client	Producing connection: Safety data Producing connection: Correction Consuming connection: coordination

O-to-T connection type	T-to-O connection type	Transport type/trigger	App path 1	App path 2 ^a	App path 3 ^a	Max consumer number	Safety Validator connection type	Key decision factors	Target role
Point-to-point	Multipoint	Application, Class 0, Client	Vendor defined Null Path	Vendor defined Null Path	Safety input app. object	2-15	Multipoint Producer CP 2/2	1 – Multipoint + 1 point-to-point + Client	Producing connection: Safety data + correction Consuming connection: Coordination
Multipoint	Point-to-point	Application, Class 0, Server	Vendor defined Null Path	Safety output app. object	Vendor defined Null Path	2-15	Multipoint Consumer CP 2/3	2 – Multipoint + 1 point-to-point + Server	Consuming connection: Safety data Consuming connection: Correction Producing connection: coordination
Multipoint	Point-to-point	Application, Class 0, Server	Vendor defined Null Path	Safety output app. object	Vendor defined Null Path	2-15	Multipoint Consumer CP 2/2	1 – Multipoint + 1 point-to-point + Server	Consuming connection: Safety Data + correction Producing connection: coordination
^a Input and Output with respect to the network. ^b Devices configurable via EDS shall define an application Null Path in the EDS file.									

Table 11 defines which network connection parameters to use for all three connections associated with each safety connection type.