

Industrial communication networks — Profiles —

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

ICS 25.040.40; 35.100.05

National foreword

This British Standard is the UK implementation of EN 61784-3-2:2008. It is identical to IEC 61784-3-2:2007.

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.

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 29 August 2008

© BSI 2008

ISBN 978 0 580 61649 5

Amendments/corrigenda issued since publication

Date	Comments

**Industrial communication networks -
Profiles -
Part 3-2: Functional safety fieldbuses -
Additional specifications for CPF 2
(IEC 61784-3-2:2007)**

Réseaux de communication industriels -
Profils -
Partie 3-2: Bus de terrain
de sécurité fonctionnelle -
Spécification supplémentaire pour CPF 2
(CEI 61784-3-2:2007)

Industrielle Kommunikationsnetze -
Profile -
Teil 3-2: Funktional sichere Übertragung
bei Feldbussen -
Zusätzliche Festlegungen
für die Kommunikationsprofilfamilie 2
(IEC 61784-3-2:2007)

This European Standard was approved by CENELEC on 2008-05-01. 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 Central Secretariat 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 Central Secretariat has the same status as the official versions.

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

CENELEC

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

Central Secretariat: rue de Stassart 35, B - 1050 Brussels

Foreword

The text of document 65C/470/FDIS, future edition 1 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 was approved by CENELEC as EN 61784-3-2 on 2008-05-01.

The following dates were fixed:

- latest date by which the EN has to be implemented
at national level by publication of an identical
national standard or by endorsement (dop) 2009-02-01
- latest date by which the national standards conflicting
with the EN have to be withdrawn (dow) 2011-05-01

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

US 6,631,476 [RA]	Safety network for industrial controller providing redundant connections on single media
US 6,701,198 [RA]	Safety network for industrial controller allowing initialization on standard networks
US 6,721,900 [RA]	Safety network for industrial controller having reduced bandwidth requirements
US 6,891,850 [RA]	Network independent safety protocol for industrial controller
US 6,915,444 [RA]	Network independent safety protocol for industrial controller using data manipulation techniques

The IEC and CENELEC take no position concerning the evidence, validity and scope of these patent rights.

The holders of these patent rights have assured the IEC that they are willing to negotiate licences under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statements of the holders of these patent rights are registered with IEC.

Information may be obtained from:

[RA] Rockwell Automation, Inc.
1201 S. Second Street
Milwaukee, WI 53204
USA
Attention: Intellectual Property Dept.

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

Annex ZA has been added by CENELEC.

Endorsement notice

The text of the International Standard IEC 61784-3-2:2007 was approved by CENELEC as a European Standard without any modification.

CONTENTS

INTRODUCTION.....	12
1 Scope.....	15
2 Normative references	15
3 Terms, definitions, symbols, abbreviated terms and conventions	16
3.1 Terms and definitions	16
3.1.1 Common terms and definitions	16
3.1.2 CPF 2: Additional terms and definitions	20
3.2 Symbols and abbreviated terms.....	21
3.2.1 Common symbols and abbreviated terms	21
3.2.2 CPF 2: Additional symbols and abbreviated terms	21
3.3 Conventions	22
4 Overview of FSCP 2/1 (CIP Safety™).....	22
4.1 General.....	22
4.2 FSCP 2/1	22
5 General	23
5.1 External documents providing specifications for the profile.....	23
5.2 Safety functional requirements	24
5.3 Safety measures	24
5.4 Safety communication layer structure	25
5.5 Relationships with FAL (and DLL, PhL)	25
5.5.1 General	25
5.5.2 Data types	25
6 Safety communication layer services	26
6.1 Introduction	26
6.2 Connection object	26
6.2.1 General	26
6.2.2 Class attribute extensions	26
6.2.3 Service extensions	27
6.2.4 Explicit message response format for SafetyOpen and SafetyClose	27
6.3 Connection Manager object.....	28
6.3.1 General	28
6.3.2 ForwardOpen for safety	28
6.3.3 Safety network segment	30
6.3.4 Originator rules for calculating the connection parameter CRC	32
6.3.5 SafetyOpen processing flowcharts	32
6.3.6 Checks required by Multipoint producers with existing connections	35
6.3.7 Electronic key usage for safety	35
6.3.8 RPI vs. API in safety connections	35
6.3.9 Application path construction for safety	35
6.3.10 Safety Validator connection types.....	37
6.3.11 Application reply data in a successful SafetyOpen response.....	38
6.3.12 Unsuccessful SafetyOpen response	39
6.3.13 ForwardClose for safety.....	42
6.4 Identity object.....	42
6.4.1 General	42

6.4.2	Changes to common services	42
6.5	Link objects	43
6.5.1	DeviceNet object changes	43
6.5.2	TCP/IP Interface object changes	43
6.6	Safety Supervisor object	44
6.6.1	General	44
6.6.2	Safety Supervisor class attributes	44
6.6.3	Subclasses	45
6.6.4	Safety Supervisor instance attributes	45
6.6.5	Semantics	48
6.6.6	Subclasses	54
6.6.7	Safety Supervisor common services	54
6.6.8	Safety Supervisor behavior	65
6.7	Safety Validator object	72
6.7.1	General	72
6.7.2	Class attributes	72
6.7.3	Instance attributes	73
6.7.4	Class services	79
6.7.5	Instance services	79
6.7.6	Object behavior	80
6.8	Connection Configuration Object	83
6.8.1	General	83
6.8.2	Class attribute extensions	83
6.8.3	Instance attributes, additions and extensions.	83
6.8.4	Instance attribute semantics extensions or restrictions for safety	85
6.8.5	Special Safety Related Parameters – (Attribute 13)	90
6.8.6	Object-specific services	94
6.8.7	Common service extensions for safety	94
6.8.8	Object behavior	96
7	Safety communication layer protocol	97
7.1	Safety PDU format	97
7.1.1	Safety PDU encoding	97
7.1.2	Safety CRC	107
7.2	Communication protocol behavior	108
7.2.1	Sequence of safety checks	108
7.2.2	Connection termination	108
7.2.3	Cross checking error	109
7.3	Time stamp operation	109
7.4	Protocol sequence diagrams	110
7.4.1	General	110
7.4.2	Normal safety transmission	110
7.4.3	Lost, corrupted and delayed message transmission	111
7.4.4	Lost, corrupted or delayed message transmission with production repeated	114
7.4.5	Point-to-point ping	116
7.4.6	Multipoint ping on CP 2/3 Safety	117
7.4.7	Multipoint ping on CP 2/2 safety networks	118
7.4.8	Multipoint ping – retry with success	119
7.4.9	Multipoint ping – retry with timeout	119

7.5	Safety protocol definition	121
7.5.1	General	121
7.5.2	High level view of a safety device	121
7.5.3	Safety Validator object	122
7.5.4	Relationship between SafetyValidatorServer and SafetyValidatorClient	122
7.5.5	SafetyValidatorClient function definition	123
7.5.6	SafetyValidatorServer function definition	131
7.6	Safety message and protocol data specifications	141
7.6.1	Mode octet	141
7.6.2	Time Stamp Section	142
7.6.3	Time Coordination Message	142
7.6.4	Time correction message	143
7.6.5	Safety data production	143
7.6.6	Producer dynamic variables	150
7.6.7	Producer per consumer dynamic variables	152
7.6.8	Consumer data variables	154
7.6.9	Consumer input static variables	156
7.6.10	Consumer dynamic variables	156
8	Safety communication layer management	158
8.1	Overview	158
8.2	Definition of the measures used during connection establishment	159
8.3	Originator-Target relationship validation	162
8.4	Detection of mis-routed connection requests	163
8.5	SafetyOpen processing	163
8.6	Ownership management	164
8.7	Bridging different physical layers	165
8.8	Safety connection establishment	166
8.8.1	Overview	166
8.8.2	Basic facts for connection establishment	166
8.8.3	Configuring safety connections	167
8.8.4	Network time expectation multiplier	168
8.8.5	Establishing connections	170
8.8.6	Recommendations for consumer number allocation	172
8.8.7	Recommendations for connection establishment	173
8.8.8	Ownership establishment	173
8.8.9	Ownership use cases	174
8.8.10	PID/CID usage and establishment	177
8.8.11	Proper PID/CID usage in multipoint and point-to-point connections	177
8.8.12	Network supported services	179
8.8.13	FSCP 2/1 Safety device type	180
8.9	Safety configuration process	184
8.9.1	Introduction to safety configuration	184
8.9.2	Configuration goals	184
8.9.3	Configuration overview	186
8.9.4	User configuration guidelines	186
8.9.5	Configuration process SIL3 justification	187
8.9.6	Device functions for tool configuration	188
8.9.7	Password security	188

8.9.8	SNCT interface services	188
8.9.9	Configuration lock.....	188
8.9.10	Effect of configuration lock on device behavior	189
8.9.11	Configuration ownership	190
8.9.12	Configuration mode	190
8.9.13	Measures used to ensure integrity of configuration process	190
8.9.14	Download process	192
8.9.15	Verification process	195
8.9.16	Verification process	198
8.9.17	Configuration error analysis.....	199
8.10	Electronic Data Sheets extensions for safety	202
8.10.1	General rules for EDS based safety devices	202
8.10.2	EDS extensions for safety	203
9	System requirements.....	207
9.1	Indicators and switches	207
9.1.1	General indicator requirements.....	207
9.1.2	LED indications for setting the device UNID.....	207
9.1.3	Module Status LED.....	208
9.1.4	Indicator warning	208
9.1.5	Network Status LED	208
9.1.6	MACID determination	210
9.1.7	Reset switch.....	211
9.2	Installation guidelines.....	212
9.3	Safety function response time	212
9.3.1	Overview	212
9.3.2	Network time expectation	212
9.3.3	Equations for calculating network reaction times	213
9.4	Duration of demands	215
9.5	Constraints for calculation of system characteristics.....	215
9.5.1	Number of nodes	215
9.5.2	Network PFH	215
9.5.3	Bit Error Rate (BER)	217
9.6	Maintenance.....	218
9.7	Safety manual	218
10	Certification.....	218
Annex A (informative)	Additional information for functional safety communication profiles of CPF 2	219
A.1	Hash function example code.....	219
Annex ZA (normative)	Normative references to international publications with their corresponding European publications	233
Bibliography.....		231
Table 1 – Communications errors and detection measures matrix.....		24
Table 2 – New class attributes		26
Table 3 – Service extensions		27
Table 4 – SafetyOpen and SafetyClose response format		27
Table 5 – Safety network segment identifier.....		30
Table 6 – Safety network segment definition.....		30
Table 7 – Safety network segment router format		32

Table 8 – Multipoint producer parameter evaluation rules	35
Table 9 – ForwardOpen setting options for safety connections.....	37
Table 10 – Network connection parameters for safety connections	38
Table 11 – CP 2/3 Safety target application reply (size: 10 octets).....	39
Table 12 – SafetyOpen target application reply (size: 16 octets).....	39
Table 13 – New and extended error codes for safety	40
Table 14 – SafetyOpen error event guidance table.....	41
Table 15 – Identity object common service changes	42
Table 16 – New DeviceNet object instance attribute	43
Table 17 – New TCP/IP Interface object Instance Attribute	43
Table 18 – Safety Supervisor class attributes	44
Table 19 – Safety Supervisor instance attributes	45
Table 20 – Device status attribute state values	49
Table 21 – Exception status attribute format	49
Table 22 – Common exception detail attribute values	50
Table 23 – Exception detail format summary.....	51
Table 24 – Summary of device behavior for various CFUNID values	53
Table 25 – Safety Supervisor common services	55
Table 26 – Safety Supervisor object specific services	55
Table 27 – Configure_Request message structure	57
Table 28 – Validate_Configuration message structure.....	57
Table 29 – Validate_Configuration success message structure	57
Table 30 – Validate_Configuration error code	58
Table 31 – Validate_Configuration extended codes.....	58
Table 32 – Set_Password message structure.....	60
Table 33 – Reset_Password message structure.....	60
Table 34 – Configuration_Lock/Unlock message structure	61
Table 35 – Mode_Change message structure	61
Table 36 – Safety_Reset message structure	62
Table 37 – Safety Supervisor safety reset types	62
Table 38 – Attribute bit map parameter	62
Table 39 – Reset processing rules for rest types.....	63
Table 40 – Propose_TUNID service	63
Table 41 – Apply_TUNID service	64
Table 42 – Safety Supervisor events.....	66
Table 43 – State event matrix for Safety Supervisor.....	67
Table 44 – Configuration owner control vs. device state.....	70
Table 45 – State mapping of Safety Supervisor to Identity object.....	71
Table 46 – Safety Supervisor object event mapping.....	71
Table 47 – Identity object event mapping.....	72
Table 48 – Safety Validator class attributes	73
Table 49 – Safety Validator instance attributes	73
Table 50 – Safety Validator state assignments.....	76

Table 51 – Safety Validator type, bit field assignments	76
Table 52 – Multipoint producer SafetyOpen parameter evaluation rules	78
Table 53 – Safety Validator class services	79
Table 54 – Safety Validator instance services	79
Table 55 – Safety Validator Get_Attributes_All service data	80
Table 56 – Safety Validator state event matrix	82
Table 57 – State mapping between Safety Supervisor and Safety Validator objects	83
Table 58 – Connection configuration object class attribute extensions	83
Table 59 – Connection Configuration Object instance attribute additions/extensions	84
Table 60 – Connection flag bit definitions	86
Table 61 – O-to-T connection parameters	87
Table 62 – T-to-O connection parameters	88
Table 63 – Data map formats	89
Table 64 – Data map format 0	90
Table 65 – Data map format 1	90
Table 66 – Target device's SCCRC values	92
Table 67 – Target device's SCTS values	93
Table 68 – Time correction connection parameters for multipoint connection	93
Table 69 – Connection Configuration Object-specific services	94
Table 70 – Get_Attributes_All Response service data (added attributes)	95
Table 71 – Set_Attributes_All Request service data (added attributes)	95
Table 72 – State Mapping between Safety Supervisor and the CCO objects	96
Table 73 – Connection sections and PDU formats	98
Table 74 – Mode octet variables	99
Table 75 – Time Stamp variables	101
Table 76 – Time Coordination message variables	102
Table 77 – Time Correction Message variables	104
Table 78 – CRC polynomials used	107
Table 79 – Connection sections and message formats	108
Table 80 – Data reception - Link triggered	133
Table 81 – Time_Correction reception - Link triggered	134
Table 82 – Data reception - Application triggered	134
Table 83 – Time_Correction reception - Application triggered	134
Table 84 – Consuming application – Safety data monitoring	135
Table 85 – Producer connection status determination	144
Table 86 – Consuming safety connection status	154
Table 87 – Connection establishment errors and measures to detect errors	159
Table 88 – SNN Date/Time allocations	160
Table 89 – SNN legal range of time values	160
Table 90 – Safety connection parameters	168
Table 91 – SafetyOpen summary	170
Table 92 – Originator/Target service mapping	181
Table 93 – Unsupported originator/target service types	184

Table 94 – Configuration goals	185
Table 95 – Configuration owner control vs. device state.....	190
Table 96 – Errors and detection measures	199
Table 97 – Parameter class keywords.....	204
Table 98 – New Connection Manager section keywords for safety	204
Table 99 – Connection Manager field usage for safety.....	205
Table 100 – Connection parameter field settings for safety	206
Table 101 – LED indications for setting UNID	207
Table 102 – Module Status LED.....	208
Table 103 – Network status LED states	209
Table 104 – Connection reaction time type – producing/consuming applications	213
Figure 1 – Relationships of IEC 61784-3 with other standards (machinery)	12
Figure 2 – Relationships of IEC 61784-3 with other standards (process).....	13
Figure 3 – Relationship of Safety Validators	23
Figure 4 – Communication layers.....	25
Figure 5 – ForwardOpen with safety network segment	29
Figure 6 – Safety network target format	31
Figure 7 – Target Processing SafetyOpen with no configuration data (Form 2 SafetyOpen)	33
Figure 8 – Target Processing for SafetyOpen with configuration data (Form 1 SafetyOpen)	34
Figure 9 – Applying device configuration.....	58
Figure 10 – Configure and Validate processing flowcharts	59
Figure 11 – UNID handling during “Waiting for TUNID”	65
Figure 12 – Safety Supervisor state diagram.....	66
Figure 13 – Configuration, testing and locked relationships.....	70
Figure 14 – Safety connection types	77
Figure 15 – Safety Validator state transition diagram	81
Figure 16 – Connection Configuration Object state diagram.....	96
Figure 17 – Connection Configuration Object data flow.....	97
Figure 18 – Format of the mode octet	98
Figure 19 – 1 or 2 octet data section.....	99
Figure 20 – 3 to 250 octet data section format	100
Figure 21 – Time Stamp section format.....	101
Figure 22 – Time Coordination message encoding.....	102
Figure 23 – Time Correction message encoding	103
Figure 24 – 1 or 2 octet point-to-point PDU encoding.....	105
Figure 25 – 1 or 2 Octet multipoint PDU encoding.....	105
Figure 26 – 1 or 2 Octet, multipoint, Format 2 safety connection format.....	106
Figure 27 – 3 to 250 Octet Point-to-point PDU encoding	106
Figure 28 – 3 to 248 Octet Multipoint PDU encoding	106
Figure 29 – 3 to 248 Octet, Multipoint, safety connection format	107

Figure 30 – Time stamp sequence	109
Figure 31 – Sequence diagram of a normal producer/consumer safety sequence.....	110
Figure 32 – Sequence diagram of a normal producer/consumer safety sequence (production repeated)	111
Figure 33 – Sequence diagram of a corrupted producer to consumer message	112
Figure 34 – Sequence diagram of a lost producer to consumer message	113
Figure 35 – Sequence diagram of a delayed message	114
Figure 36 – Sequence diagram of a corrupted producer to consumer message with production repeated	115
Figure 37 – Sequence diagram of a connection terminated due to delays	116
Figure 38 – Sequence diagram of a failure of safety CRC check	116
Figure 39 – Sequence diagram of a point-to-point ping - normal response	117
Figure 40 – Sequence diagram of a successful multipoint ping, CP 2/3 safety	118
Figure 41 – Sequence diagram of a successful multipoint ping, CP 2/2 safety	119
Figure 42 – Sequence diagram of a multipoint ping retry.....	120
Figure 43 – Sequence diagram of a multipoint ping timeout	120
Figure 44 – Safety device reference model entity relation diagram.....	121
Figure 45 – Two devices interchanging safety data via a SafetyValidatorClient and a SafetyValidatorServer	122
Figure 46 – Safety production data flow	123
Figure 47 – Consumer safety data monitoring	132
Figure 48 – SafetyValidatorServer - application triggered	132
Figure 49 – Target ownership	163
Figure 50 – SafetyOpen forms	164
Figure 51 – Connection ownership state chart	164
Figure 52 – SafetyOpen UNID mapping	165
Figure 53 – Common CPF 2 application layer	165
Figure 54 – End-to-End routing example	166
Figure 55 – Sources for safety related connection parameters	169
Figure 56 – Parameter mapping between originator and target	169
Figure 57 – CP 2/3 Safety connection establishment in targets for Form 2a SafetyOpen.....	171
Figure 58 – General sequence to detect configuration is required	172
Figure 59 – PID/CID exchanges for two originator scenarios.....	177
Figure 60 – Seed generation for multipoint connections	178
Figure 61 – PID/CID runtime handling.....	179
Figure 62 – Connection categories and supported services.....	182
Figure 63 – Recommended connection types.....	183
Figure 64 – Logic-to-logic supported services	183
Figure 65 – Recommended connection types for logic to logic	184
Figure 66 – Configuration data transfers	185
Figure 67 – Protection measures in safety devices	187
Figure 68 – Configuration, testing and locked relationships.....	189
Figure 69 – Originator's configuration data	191
Figure 70 – SNCT to device download process	191

Figure 71 – SNCT Downloads to originators that perform Form 1 configuration.....	194
Figure 72 – Protection from locking and ownership	196
Figure 73 – Example of read back and comparison of original and printout	197
Figure 74 – Diverse display without full data read back.....	198
Figure 75 – Verification process including all alternatives	198
Figure 76 – Safety device MACID processing logic	211
Figure 77 – Safety function response time	212
Figure 78 – Safety function response time components	214
Figure 79 – Network protocol reliability block diagram (RBD)	215
Figure 80 – Network PFH summary.....	217

INTRODUCTION

The IEC 61158 fieldbus standard together with its companion standards IEC 61784-1 and IEC 61784-2 defines a set of communication protocols that enable distributed control of automation applications. Fieldbus technology is now considered well accepted and well proven. Thus many fieldbus enhancements are emerging, addressing not yet standardized areas such as real time, safety-related and security-related applications.

This standard explains the relevant principles for functional safety communications with reference to IEC 61508 series and specifies several safety communication layers (profiles and corresponding protocols) based on the communication profiles and protocol layers of IEC 61784-1, IEC 61784-2 and the IEC 61158 series. It does not cover electrical safety and intrinsic safety aspects.

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

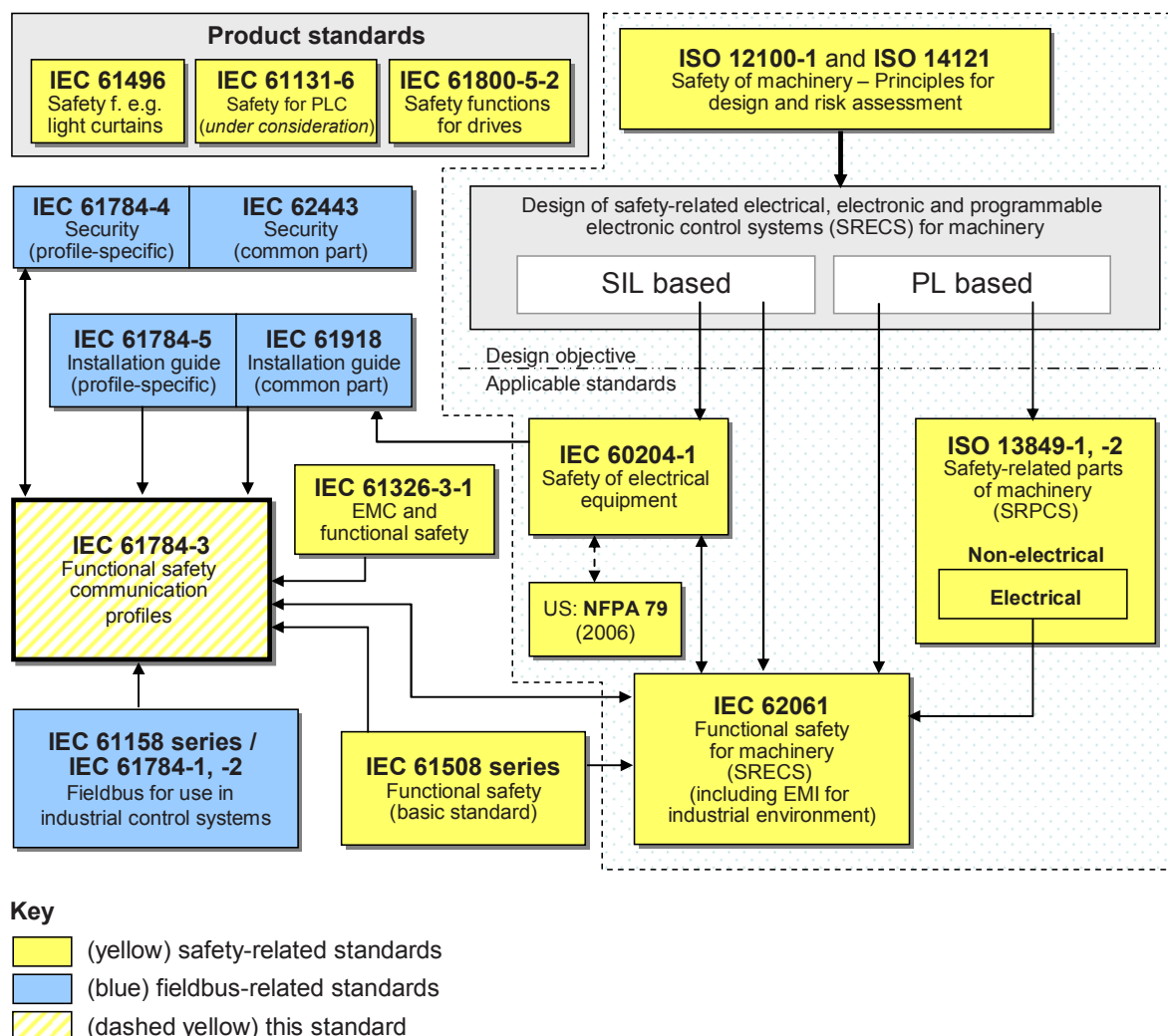
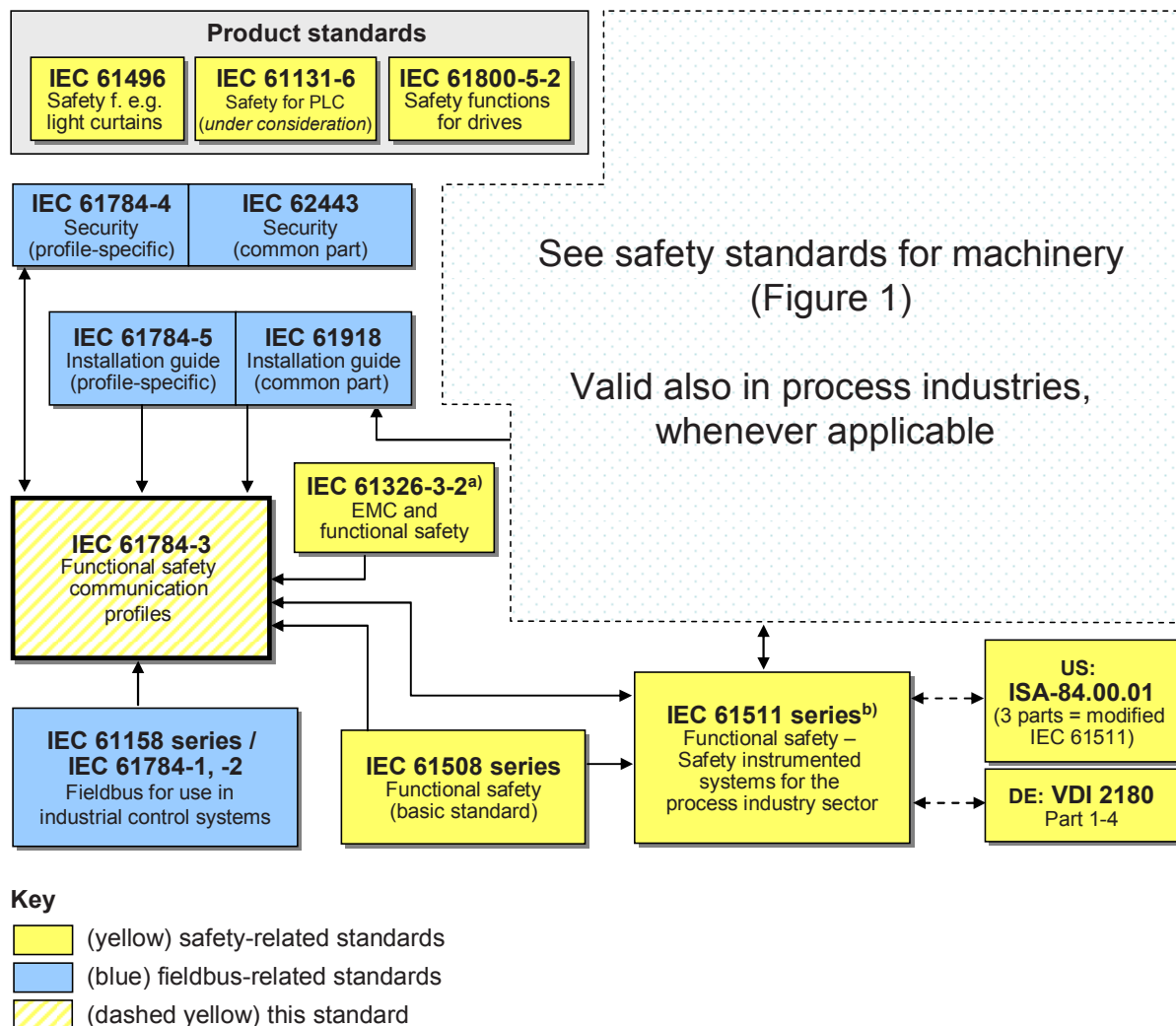


Figure 1 – Relationships of IEC 61784-3 with other standards (machinery)

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



^a For specified electromagnetic environments; otherwise IEC 61326-3-1.

^b EN ratified.

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

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

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

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

This standard describes

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

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES

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

1 Scope

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

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

This part¹ defines mechanisms for the transmission of safety-relevant messages among participants within a distributed network using fieldbus technology in accordance with the requirements of IEC 61508 series for functional safety. These mechanisms may be used in various industrial applications such as process control, manufacturing automation and machinery.

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

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

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 61131-2, *Programmable controllers – Part 2: Equipment requirements and tests*

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

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

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

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

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

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

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

IEC 61326-3-1, *Electrical equipment for measurement, control and laboratory use – EMC requirements – Part 3-1: Immunity requirements for safety-related systems and for equipment intended to perform safety related functions (functional safety) – General industrial applications*²

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

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

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

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

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

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

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

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

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

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

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

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.

3.1.1 Common terms and definitions

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

NOTE Availability depends on MTBF (mean time between failure) and MDT (mean down time):
$$\text{Availability} = \text{MTBF} / (\text{MTBF} + \text{MDT}).$$

² To be published.

3.1.1.2

black channel

communication channel without available evidence of design or validation according to IEC 61508 series

3.1.1.3

bridge

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

3.1.1.4

communication channel

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

3.1.1.5

communication system

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

3.1.1.6

connection

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

3.1.1.7

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 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 See also [28], [29]³.

3.1.1.8

error

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

NOTE 1 An error can be caused by a faulty item, e.g. a computing error made by faulty computer equipment.

[IEV 191-05-24], [IEC 61508-4:1998], [IEC 61158]

NOTE 2 Errors may be due to design mistakes within hardware/software and/or corrupted information due to electromagnetic interference and/or other effects.

NOTE 3 Errors do not necessarily result in a *failure* or a *fault*.

3.1.1.9

failure

termination of the ability of a functional unit to perform a required function

NOTE 1 The definition in IEC 191-04-01 is the same, with additional notes.

[IEC 61508-4:1998], [ISO/IEC 2382-14.01.11]

NOTE 2 Failure may be due to an *error* (for example, problem with hardware/software design or message disruption)

³ Figures in square brackets refer to the bibliography.

3.1.1.10**fault**

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

NOTE IEC 191-05-01 defines “fault” as a state characterized by the inability to perform a required function, excluding the inability during preventative maintenance or other planned actions, or due to lack of external resources.

[IEC 61508-4:1998], [ISO/IEC 2382-14.01.10]

3.1.1.11**fieldbus**

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

3.1.1.12**frame**

denigrated synonym for DLPDU

3.1.1.13**hash function**

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

NOTE 1 Hash functions can be used to detect data corruption.

NOTE 2 Common hash functions include parity, checksum or CRC.

[IEC 62210, modified]

3.1.1.14**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

3.1.1.15**master**

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

3.1.1.16**message**

ordered series of octets intended to convey information

[ISO/IEC 2382-16.02.01, modified]

3.1.1.17**nuisance trip**

spurious trip with no harmful effect

NOTE Internal abnormal errors can be caused in communication systems such as wireless transmission, for example by too many retries in the presence of interferences.

3.1.1.18**redundancy**

existence of means, in addition to the means which would be sufficient for a functional unit to perform a required function or for data to represent information

EXAMPLE Duplicated functional components and the addition of parity bits are both instances of redundancy.

NOTE 1 Redundancy is used primarily to improve reliability or availability.

NOTE 2 The definition in IEC 191-15-01 is less complete.

[IEC 61508-4:1998], [ISO/IEC 2382-14.01.12]

3.1.1.19

reliability

probability that an automated system can perform a required function under given conditions for a given time interval (t_1, t_2)

NOTE 1 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 The term "reliability" is also used to denote the reliability performance quantified by this probability.

NOTE 3 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 Reliability differs from availability.

[IEC 62059-11, modified]

3.1.1.20

risk

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

[IEC 61508-4:1998]

3.1.1.21

safety communication layer (SCL)

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

3.1.1.22

safety connection

connection that utilizes the safety protocol for communications transactions

3.1.1.23

safety data

data transmitted across a safety network using a safety protocol

NOTE The Safety Communication Layer does not ensure safety of the data itself, only that the data is transmitted safely.

3.1.1.24

safety device

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

3.1.1.25

safety function

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

[IEC 61508-4:1998]

3.1.1.26

safety function response time

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

NOTE This concept is introduced in IEC 61784-3, 5.2.4 and addressed by the functional safety communication profiles defined in this part.

3.1.1.27**safety integrity level (SIL)**

discrete level (one out of a possible four) for specifying the safety integrity requirements of the *safety functions* to be allocated to the E/E/PE safety-related systems, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest

NOTE The target failure measures for the four safety integrity levels are specified in Tables 2 and 3 of IEC 61508-1.

[IEC 61508-4:1998]

3.1.1.28**safety measure**

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

NOTE 1 In practice, several safety measures are combined to achieve the required safety integrity level.

NOTE 2 Communication *errors* and related safety measures are detailed in IEC 61784-3, 5.3 and 5.4.

3.1.1.29**safety-related application**

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

3.1.1.30**safety-related system**

system performing *safety functions* according to IEC 61508

3.1.1.31**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

3.1.1.32**spurious trip**

trip caused by the safety system without a process demand

3.1.1.33**time stamp**

time information included in a *message*

3.1.2 CPF 2: Additional terms and definitions**3.1.2.1****ping**

request for the consumer to acknowledge the reception of a message

3.1.2.2**ping response**

response to a ping

3.1.2.3**signature**

method of uniquely identifying a set of data

NOTE 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	
EMI	Electro-Magnetic Interference	
EUC	Equipment Under Control	[IEC 61508-4:1998]
FAL	Fieldbus Application Layer	[IEC 61158-5]
FSCP	Functional Safety Communication Profile	
E/E/PE	Electrical/Electronic/Programmable Electronic	[IEC 61508-4:1998]
PDU	Protocol Data Unit	[ISO/IEC 7498-1]
PFD	Average Probability of Failure on Demand	[IEC 61508-6:1998]
PFH	Probability of Failure per Hour	[IEC 61508-6:1998]
PhL	Physical Layer	[ISO/IEC 7498-1]
PLC	Programmable Logic Controller	
SCL	Safety Communication Layer	
SIL	Safety Integrity Level	[IEC 61508-4:1998]

3.2.2 CPF 2: Additional symbols and abbreviated terms

AIRS	Already In Requested Mode/State
BER	Bit Error Rate
CCO	Connection Configuration Object
CFUNID	Configuration UNID
CNP	Connection Point
CID	Consumer ID
CIP™	Common Industrial Protocol (application framework shared among CPF 2 communication profiles)
CPCRC	Connection Parameter CRC
CTM	Connection Timeout Multiplier
EDS	Electronic Data Sheet
EPI	Expected Packet Interval
LED	Light Emitting Diode
MACID	Device physical address on network
MOD	Module
NV	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
SNN	Safety Network Number
T-to-O	Target to Originator
TBD	To Be Defined
TNS	TUNID Not Set
TUNID	Target UNID
UNID	Unique Network Identifier
UML	Universal Modeling Language

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™⁴) 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.

The basic profiles CP 2/1, CP 2/2, and CP 2/3 are defined in IEC 61784-1 and IEC 61784-2. The CPF 2 functional safety communication profile FSCP 2/1 (CIP Safety™⁴) is based on the CPF 2 basic profiles in IEC 61784-1 and 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.

⁴ CIP™ (Common Industrial Protocol) and CIP Safety™ are trade names of the non-profit organization Open DeviceNet Vendor Association, Inc (ODVA). 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.

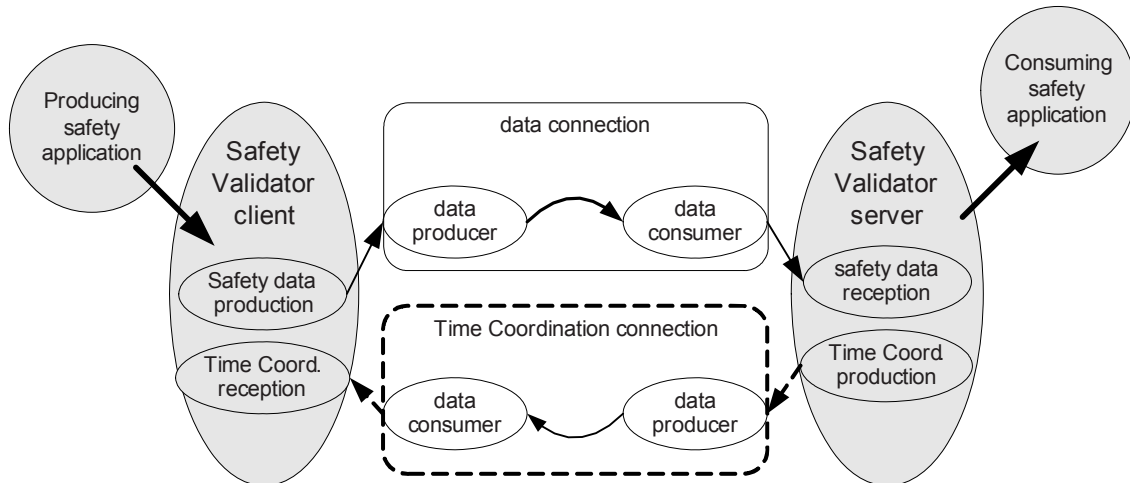


Figure 3 – Relationship of Safety Validators

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 documents are especially useful in understanding the design of FSCP 2/1 protocols:

- GS-ET-26 [27]

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 category 4 (refer to EN 954-1).
- 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 series.
- Environmental conditions shall be according to IEC 61131-2 for the basic levels and IEC 61326-3 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.

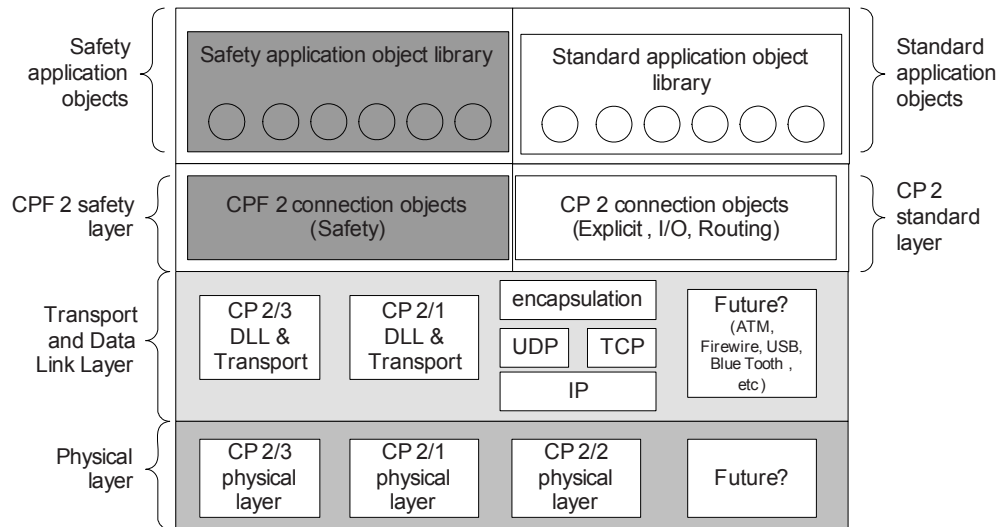


Figure 4 – Communication layers

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™ 5), CP 2/2 (EtherNet/IP™ 6)). 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 for Type 2.

⁵ DeviceNet™ is a trade name of the non-profit organization Open DeviceNet Vendor Association, Inc (ODVA). 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.

⁶ EtherNet/IP™ is a trade name of ControlNet International, Ltd. (CI) and Open DeviceNet Vendor Association, Inc (ODVA). 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 either CI or ODVA.

6 Safety communication layer services

6.1 Introduction

This subclause 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.

6.2 Connection object

6.2.1 General

Several safety specific class attributes and services are defined to support safety. 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 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

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, 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

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

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

Parameter Name			Data Type / Size	Target Destination and Semantics	
	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	
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

6.3.3 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 below.

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 – 255 = Reserved
3 thru 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 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 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 7.6.5.10
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 0 to 42 969
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

6.3.4 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.

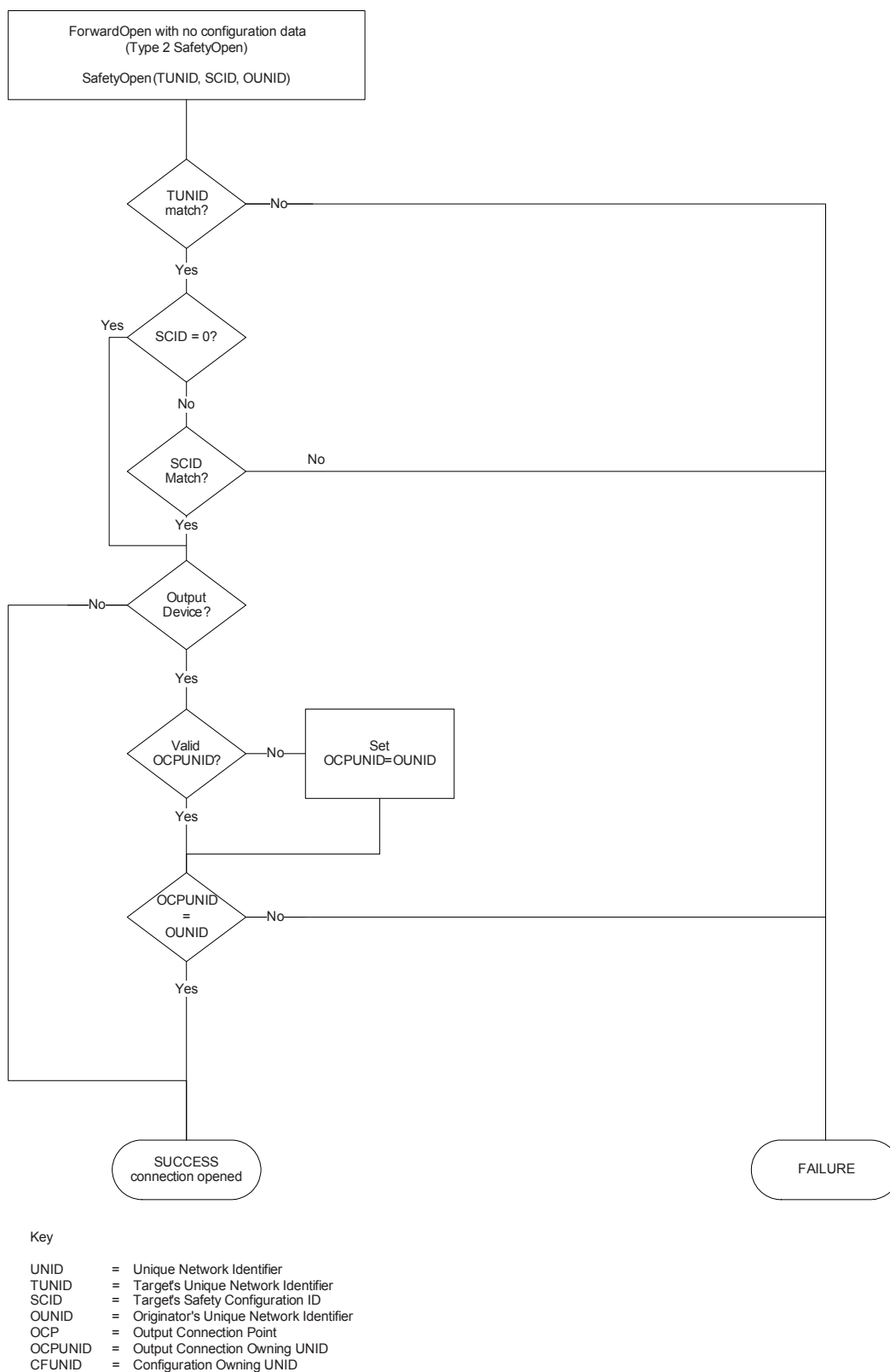
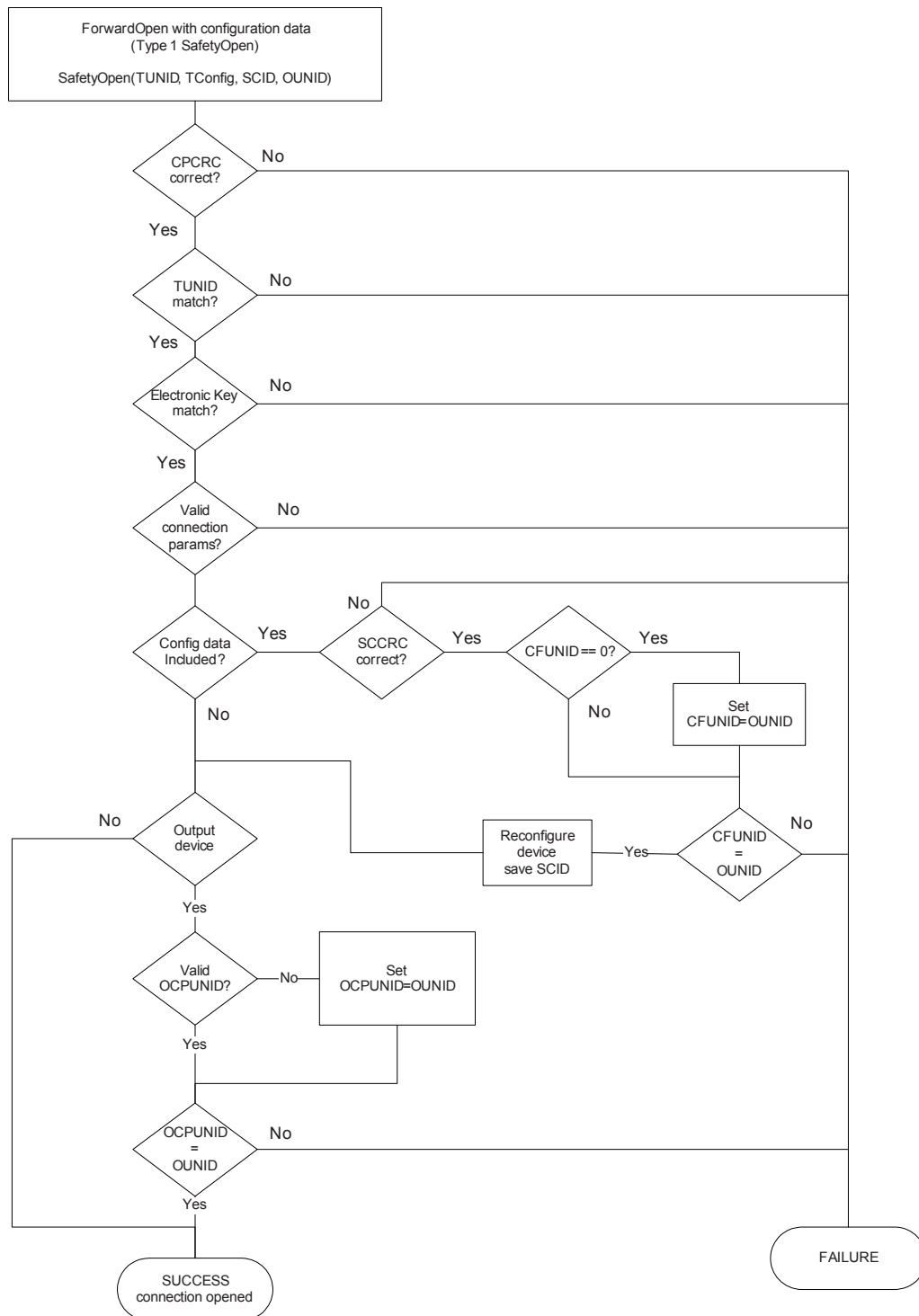


**Figure 7 – Target Processing SafetyOpen with no configuration data
(Form 2 SafetyOpen)**



Key

UNID	=	Unique Network Identifier
TUNID	=	Target's Unique Network Identifier
CPCRC	=	Connection Parameter CRC
SCID	=	Target's Safety Configuration ID
SCCRC	=	CRC portion of the SCID
OUNID	=	Originator's Unique Network Identifier
OCPUNID	=	Output Connection Owning UNID
CFUNID	=	Configuration Owning UNID

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

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 8 defines the multipoint producer parameter evaluation rules.

Table 8 – 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}
^a At the option of the device developer, another connection could also be opened rather than return an error response.			

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 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 +/- 128 µs.

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: (CP stands for Connection Point).

[Class] [Class #] [Instance] [Instance #] [CNP] [Consumer CP] [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 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 9. 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 9 – 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
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:

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

Table 10 – Network connection parameters for safety connections

Target type	Network connection parameter	Proper parameter value	Description
Point-to-point producer	O-to-T	4406 _{hex}	Point-to-point high priority, fixed
	T-to-O	4408 _{hex}	Point-to-point high priority, fixed
	Time Correction	0000 _{hex}	Not used
Point-to-point producer	O-to-T	4408 _{hex}	Point-to-point high priority, fixed
	T-to-O	4406 _{hex}	Point-to-point high priority, fixed
	Time Correction	0000 _{hex}	Not used
Multipoint producer	O-to-T	4406 _{hex}	Point-to-point high priority, fixed
	T-to-O	240E _{hex}	Multipoint high priority, fixed
	Time Correction	2406 _{hex}	Multipoint high priority, fixed

Successful SafetyOpen responses shall return the connection identifiers used, as well as the Consumer_Number assigned to the originator (always FFFF_{hex} for point-to-point connections).

6.3.11 Application reply data in a successful SafetyOpen response

The format for a SafetyOpen response for Success is the same as the Forward_Open_Reply as defined in IEC 61158-6-2. The data return is defined in Table 11.

The target of a SafetyOpen shall return the data defined in Table 12 in the Application Reply field of the SafetyOpen response. The consumer number and PID reply data is only of significance when the originator is the consumer.

Table 11 – CP 2/3 Safety target application reply (size: 10 octets)

Parameter name	Data type	Description
Consumer_Number	UINT	
PID/CID	STRUCT of:	Target Identifier used to generate a PID or CID seed value
Target Vendor Id	UINT	Target's Vendor Id
Target Device Serial Number	UDINT	Target's Device Serial Number
Target Connection Serial Number	UINT	Connection Serial Number Target assigned to the connection. The Safety Validator instance Id shall be used

Table 12 – SafetyOpen target application reply (size: 16 octets)

Parameter name ^a	Data type	Description
Consumer_Number	UINT	
PID/CID	STRUCT of:	Target Identifier used to generate a PID or CID seed value
Target Vendor Id	UINT	Target's Vendor Id
Target Device Serial Number	UDINT	Target's Device Serial Number
Target Connection Serial Number	UINT	Connection Serial Number Target assigned to the connection. The Safety Validator instance Id shall be used
Time_Correction_Connection_ID	UDINT	Connection ID selected by the Target for the Time Correction connection. If chosen by the originator, then the value is echoed back
Time_Correction_API	UDINT	Returns same value received in the Request packet
^a These fields are always present in the Application Reply field. When a CP 2/3 Safety target receives a SafetyOpen that is not multipoint (thus no Time Correction connection is established) the Time_Correction_Connection_ID parameter shall be set to FFFF _{hex} . If the target is not a multipoint producer, the consumer number is set to FFFF _{hex} .		

6.3.12 Unsuccessful SafetyOpen response

The SafetyOpen has some special error cases that do not map to the existing set of error codes, and extends the definition of existing error codes.

Table 13 defines new extended error codes for safety and shows the extended definition of existing error codes.

Table 13 – New and extended error codes for safety

General status	Extended status	Explanation
01 _{hex}	0105 _{hex}	Ownership conflict or OUNID mismatch. The configuration is already owned by another originator
01 _{hex}	0106 _{hex}	Ownership conflict or OUNID mismatch. The output connection was already owned by another originator
01 _{hex}	0205 _{hex}	Parameter Error in Unconnected Send service or Parameter Error in SafetyOpen or SafetyClose
01 _{hex}	801 _{hex}	Incompatible Multipoint RPI. An existing connection has been established at a different RPI
01 _{hex}	802 _{hex}	Invalid Safety Connection size
01 _{hex}	803 _{hex}	Invalid Safety Connection format
01 _{hex}	804 _{hex}	Invalid Time Correction Connection Parameters
01 _{hex}	805 _{hex}	Invalid Ping Interval EPI Multiplier
01 _{hex}	806 _{hex}	Time Coordination Msg Min Multiplier
01 _{hex}	807 _{hex}	Network Time Expectation Multiplier
01 _{hex}	808 _{hex}	Timeout Multiplier
01 _{hex}	809 _{hex}	Invalid Max Consumer Number
01 _{hex}	80A _{hex}	Invalid CPCRC
01 _{hex}	80B _{hex}	Time Correction Connection Id invalid
01 _{hex}	80C _{hex}	SCID Mismatch. The SCID was non-zero and did not match the value in the target
01 _{hex}	80D _{hex}	TUNID not set. Device is out-of-box and TUNID has not been set, so connections are not allowed
01 _{hex}	80E _{hex}	TUNID Mismatch. The TUNID provided does not match. The message was likely routed to this node in error
01 _{hex}	80F _{hex}	Configuration operation not allowed

Event/Error Matrix Table 14 provides guidance for which error codes to use for possible errors detected in processing a SafetyOpen. This is not intended to be an exhaustive list.

Table 14 – SafetyOpen error event guidance table

Event	Error type	General status	Extended status
The target device received a SafetyOpen request in states of Safety Supervisor object other than Idle and Executing.	Configuration operation not allowed	01 _{hex}	080F _{hex}
	Device not configured	01 _{hex}	110 _{hex}
Safety Connection Type (name) Invalid	Safety parameter error – Invalid Connection Type	01 _{hex}	315 _{hex}
Safety Connection Size Invalid	Safety parameter error – Invalid Safety Connection Size	01 _{hex}	0802 _{hex}
Safety Connection Format Invalid	Safety parameter error – Invalid Safety Connection Format	01 _{hex}	0803 _{hex}
Time Correction Connection Parameters Invalid	Safety parameter error – Invalid Time Correction Connection Parameters	01 _{hex}	0804 _{hex}
Ping Interval EPI Multiplier was out of the range	Safety parameter error – Invalid Ping Interval EPI Multiplier	01 _{hex}	0805 _{hex}
Time Coordination Message Min Multiplier was out of the range	Safety parameter error – Time Coordination Msg Min Multiplier	01 _{hex}	0806 _{hex}
Time Expectation Multiplier was out of the range	Safety parameter error – Time Expectation Multiplier	01 _{hex}	0807 _{hex}
Timeout Multiplier was out of the range	Safety parameter error – Timeout Multiplier	01 _{hex}	0808 _{hex}
Max Consumer Number not within the limits in Multipoint Producer	Safety parameter error – Invalid Max Consumer Number	01 _{hex}	0809 _{hex}
CPCRC value in SafetyOpen and calculated CPCRC value.	Safety parameter error – Invalid CPCRC	01 _{hex}	080A _{hex}
Time Correction Connection Id Invalid	Safety parameter error – Time Correction Connection Id invalid	01 _{hex}	080B _{hex}
RPI requested is incompatible with previously established multipoint connections	Incompatible multipoint RPI	01 _{hex}	801 _{hex}
O-to-T RPI, T-to-O RPI, or Time Correction RPI is not supported	RPI not supported	01 _{hex}	0111 _{hex}
All Safety Validator Instances are being used.	Connection Manager or connection object cannot support any more connections.	01 _{hex}	0113 _{hex}

6.3.13 ForwardClose for safety

There are no additional behaviors defined for the ForwardClose service when used to close a Safety connection. In the following Safety Requirements, the term “SafetyClose” refers to both the ForwardClose of the Connection Manager object and the SafetyClose of the Connection object.

The SafetyClose Service shall be used to close connections with a Safety Targets (and in the case of a ForwardClose all other nodes in the connection path).

The SafetyClose request shall remove a connection from all the nodes participating in the original connection.

The SafetyClose request shall cause all resources in all nodes participating in the connection to be deallocated, including connection IDs, bandwidth, and internal memory buffers.

Targets receiving the SafetyClose service request shall close the connection who's Originator Vendor ID, Connection Serial Number, and Originator Serial Number parameters match. Additional information provided by this service (ie, Connection Path) shall be ignored by the target.

A SafetyClose Success reply shall be returned after the connection has been deleted at the target.

When a SafetyClose success reply is received, the originator and each intermediate node along the path, closes the connection and releases resources associated with that connection when the success response is received. But the originator shall also close the connection if no response is received within a vendor selected wait period.

6.4 Identity object

6.4.1 General

Class Code: 01hex

This subclause describes changes to the Identity object to support safety.

All CPF 2 safety devices shall replace the Identity object state behavior with the behavior defined in the Safety Supervisor object.

6.4.2 Changes to common services

Table 15 defines the services of the Identity object that require updates.

Table 15 – Identity object common service changes

Service code	Need in implementation		Service name	Description of service
	Class	Instance		
05 _{hex}	Optional	Conditional ^a	Reset	Invokes the Reset Service for the device
^a Conditional – The Identity object Reset service shall not be supported in safety devices (reply to any requests with “Service Not Supported” error). The service shall be replaced by the Reset service defined by the Safety Supervisor.				

6.5 Link objects

6.5.1 DeviceNet object changes

6.5.1.1 Additional attribute for safety

Class Code: 03hex

This subclause defines the changes and additions required of the DeviceNet object to support safety. An attribute shall be added to allow the Safety Network Number (SNN) to be read. The definition for this attribute is defined in Table 16.

Table 16 – New DeviceNet object instance attribute

Attrib ID	Need in implem.	Access rule	Name	Data type	Description of attribute	Semantics of value
11	Required	Get	Safety Network Number	6 OCTETS	System-wide unique number for the subnet this device resides on.	Attribute shall contain the SNN portion of the TUNID in the Safety Supervisor. See 8.2 for further definition of this attribute

Devices implementing FSCP 2/1 on CP 2/3 shall support attributes 11 of the DeviceNet object.

6.5.1.2 Quick Connect restriction for safety

All CP 2/3 safety devices shall not support the Quick Connect feature. The Quick Connect attribute shall not be supported and shall respond to any Get/Set attribute service with the error code “Attribute not supported”.

6.5.2 TCP/IP Interface object changes

Class Code: F5hex

This subclause defines the changes and additions required of the TCP/IP Interface object to support safety. An attribute shall be added to allow the Safety Network Number (SNN) to be read. The definition for this attribute is defined in Table 17.

Table 17 – New TCP/IP Interface object Instance Attribute

Attrib ID	Need in implem.	Access rule	Name	Data type	Description of attribute	Semantics of value
7	Required	Get	Safety Network Number	6 OCTETS	System-wide unique number for the subnet this device resides on.	Attribute shall contain the SNN portion of the TUNID in the Safety Supervisor. See 8.2 for further definition of this attribute

Devices implementing FSCP 2/1 on CP 2/2 Safety shall support attribute 7 of the TCP/IP Interface object.

6.6 Safety Supervisor object

6.6.1 General

Class Code: 39 hex

The Safety Supervisor is the core object of FSCP 2/1 Safety Devices. There are two fundamental Safety Supervisor implementations defined:

- Baseline Supervisor – defined as a supervisor implementation that supports all the “required” attributes and services defined by this object definition. The baseline Supervisor includes all state machine behavior excluding state event processing for services not required (see 6.6.8);
- SNCT Supervisor – defined as a supervisor implementation that supports all the Baseline functionality plus the attributes and services that are marked “conditional” on SNCT support.

All safety devices on a FSCP 2/1 safety network shall support the baseline Safety Supervisor definition.

Because many of the parameters in the safety supervisor object are deemed safety critical, the attributes of this object shall have a higher integrity than standard object data.

The state behavior of the Safety Supervisor object shall control the state of entire device. All objects in a safety device are required to be subservient to the states and commands of the Safety Supervisor to manage its functions and behaviors.

The Safety Supervisor object centralizes application object state definitions and related status information, exception status indications (alarms and warnings), and defines a behavior model which is assumed by objects identified as belonging to safety devices. That is, if a reset is requested of the Safety Supervisor object instance, it is performed by this object instance as well as all of its associated application objects.

The Identity object shall get its state information from the Safety Supervisor object. A reset request to the Identity object is not supported by FSCP 2/1 Safety devices (see 6.4 and shall be replaced by a reset request to the Safety Supervisor object which has additional qualifiers to execute the request. Further relationships are specified in 6.6.8.

Additionally, some instance attributes are reserved to allow for future extension to implement profiles defined for the semiconductor industry.

6.6.2 Safety Supervisor class attributes

The Class attributes used by the Safety Supervisor are defined in Table 18.

Table 18 – Safety Supervisor class attributes

Attribute ID	Need in implementation	Access rule	Name	Date type	Description of attribute
1 thru 96	These class attributes are described in IEC 61158-6-2				
97-98	Reserved by FSCP 2/1 for future use				
99	Conditional ^a	Get	Subclass	UINT	Identifies a subset of additional class attributes, services, and behaviors
^a If the value of Subclass is 00 which identifies “no subclass”, then this attribute should be in implementation, otherwise, this attribute shall be in the implementation.					

6.6.3 Subclasses

Each class level subclass defines a unique meaning for an overlapping range of class attribute IDs and/or class service IDs. The range for subclass definitions begins at ID 96 and numbers downward for attributes, and ID 63_{hex} and numbers downward for services. The subclass for a given class is identified by the value of its subclass class attribute. There are presently no subclasses defined for the class instance.

6.6.4 Safety Supervisor instance attributes

The instance attributes for the Safet Supervisor are defined in Table 19.

Table 19 – Safety Supervisor instance attributes

Attr ID	Need in implementation	Access rule	NV	Name	Date type	Description of attribute
1	Optional	Get	NV	Number of Attributes	USINT	Number of Attributes supported by the object instance
2	Optional	Get	NV	Attribute List	ARRAY of USINT	List of attributes supported by the object instance
3	Reserved					
4	Reserved					
5	Optional	Get	NV	Manufacturer Name	Short String	ASCII Text, Max. 20 characters, see 6.6.5.1
6	Optional	Get	NV	Manufacturer Model Number	Short String	ASCII Text, Max. 20 characters, Manufacturer specified
7	Optional	Get	NV	Software Revision Level	Short String	ASCII Text, Max. 6 characters, see 6.6.5.2
8	Optional	Get	NV	Hardware Revision Level	Short String	ASCII Text, Max. 6 characters, see 6.6.5.3
9	Optional	Get	NV	Manufacturer Serial Number	Short String	ASCII Text, Max. 30 characters, manufacturer specified, see 6.6.5.4
10	Optional	Get	NV	Device Configuration	Short String	ASCII Text, Max. 50 Characters, manufacturer specified. Optional additional information about the device configuration
11	Required	Get	V	Device Status	USINT	see 6.6.5.5
12	Required	Get	V	Exception Status	SWORD	see 6.6.5.6
13	Conditional based on Exception Status Bit 7	Get	V	Exception Detail Alarm	STRUCT of:	A Structure of 3 structures containing a bit-mapped representation of the alarm detail
				Common Exception Detail	STRUCT of:	
				Size	USINT	Number of Common Exception Detail Octets
				Detail	ARRAY of:	see 6.6.5.7
				Detail	SWORD	see 6.6.5.7
				Device Exception Detail	STRUCT of:	

Attr ID	Need in implementation	Access rule	NV	Name	Date type	Description of attribute
				Size	USINT	Number of Device Exception Detail Octets
				Detail	ARRAY of:	Manufacturer specified
				Detail n	SWORD	Manufacturer specified
				Manufacturer Exception Detail	STRUCT of:	
				Size	USINT	Number of Manufacturer Exception Detail Octets
				Detail	ARRAY of:	Manufacturer specified
				Detail n	SWORD	Manufacturer specified
14	Conditional Based on Exception Status Bit 7	Get	V	Exception Detail Warning	STRUCT of:	A Structure of 3 structures containing a bit-mapped representation of the warning detail
				Common Exception Detail	STRUCT of:	
				Size	USINT	Number of Common Detail Octets
				Detail	ARRAY of:	see 6.6.5.8
				Detail n	SWORD	see 6.6.5.8
				Device Exception Detail	STRUCT of:	
				Size	USINT	Number of Device Detail Octets
				Detail	ARRAY of:	Manufacturer specified
				Detail n	SWORD	Manufacturer specified
				Manufacturer Exception Detail	STRUCT of:	
				Size	USINT	Number of Manufacturer Detail Octets
				Detail	ARRAY of:	Manufacturer Specified
				Detail n	SWORD	Manufacturer Specified
15	Required	Set	NV	Alarm Enable	BOOL	see 6.6.5.12
16	Required	Set	NV	Warning Enable	BOOL	see 6.6.5.12
17	Optional	Set	a	Time	DATE_AND_TIME	The value of the Device's internal real-time clock.
18	Optional	Get	NV	Clock Power Cycle Behavior	USINT	Describes the behavior of the device's internal real-time clock (the "Time" attribute) during a power cycle 0 = [default] clock always resets during power cycle 1 = clock value is stored in

Attr ID	Need in implementation	Access rule	NV	Name	Date type	Description of attribute
						nonvolatile memory at power down 2 = clock is battery-backed and runs without device power. 3-255 = Reserved
19	Optional	Get	NV	Last Maintenance Date	DATE	The date on which the device was last serviced
20	Optional	Get	NV	Next Scheduled Maintenance Date	DATE	The date on which it is recommended that the device next be serviced
21	Optional	Get	NV	Scheduled Maintenance Expiration Timer	INT	see 6.6.5.13
22	Conditional – Required if Calibration Expiration is supported	Set	NV	Scheduled Maintenance Expiration Warning Enable	BOOL	see 6.6.5.14
23	Optional	Get	NV	Run Hours	UDINT	An indication of the number of hours that the device has had power applied.
24	Conditional ^c	Set only by "Configuration Lock/Unlock" Service Gettable	NV	Configuration Lock	BOOL	Marks the device configuration contained within as Verified and locked, or alternatively as unverified, unlocked, and changeable.
25	Conditional ^c	Get	NV	Configuration UNID	10 octets	CFUNID - Identifies the owner of a Device Configuration. All FF _{hex} = Tool-only configuration. 0 = un-owned, accept any owner
26	Required	Get	NV	Safety Configuration Identifier	10 octets	The SCID is comprised of the Safety Configuration CRC + Safety Configuration Time Stamp. This is the signature for the Configuration
27	Required	Get	NV	Target UNID	10 octets	The current UNID of the device.
28	Conditional ^d	Get	NV	Output Connection Point Owners		
				Number of Array Entries	UINT	Number of OCPUNID STRUCT entries
				Output Owners	ARRAY of STRUCT	

Attr ID	Need in implementation	Access rule	NV	Name	Date type	Description of attribute
				OCPUNID	10 octets	The owner UNID for the output resource 0 = un-owned, accept any owner (default)
				ePath Size	USINT	Path size, number of octets
				Application Resource	Packed ePath	The path to owned resource (i.e. 20 04 24 01 - Assembly class, instance 1)
29	Conditional ^c	Get		Proposed TUNID	10 octets	The UNID value that an originator is attempting to set in the device.
97-98	Reserved by FSCP 2/1 for Future Use					
99	Conditional ^b	Get	NV	Subclass	UINT	Identifies a subset of additional instance attributes, services, and behaviors
^a The nonvolatile behavior of the Time attribute is conditional on the value of the Clock Power Cycle Behavior attribute. ^b If the value of Subclass is 00 which identifies "no subclass", then this attribute should be in implementation, otherwise, this attribute shall be in implementation. ^c Safety Devices which support the SNCT interface (i.e. not configured by the SafetyOpen or some vendor specific means) shall support this attribute. ^d Conditional – the Output Connection Owner attribute shall be supported for all safety output assemblies.						

6.6.5 Semantics

6.6.5.1 Manufacturer name

The Manufacturer Name attribute, identifies the manufacturer of the device.

The Manufacturer Name attribute is not guaranteed, by specification, to be unique. Therefore, it is not a substitute for the corresponding attribute of the Identity object and should not be used for identification purposes.

6.6.5.2 Software revision level

This is an ASCII coded text string representing the revision of the software corresponding to the specific device identified by the Identity object.

6.6.5.3 Hardware revision level

This is an ASCII coded text string representing the revision of the hardware which is identified by the Identity object. The manufacturer of the device shall control this revision such that modifications to the device hardware may be tracked.

6.6.5.4 Manufacturer's serial number

This attribute is a string representation of the vendor's serial number of the device, formatted to fit most manufacturing tracking systems. It is not required that this attribute match the Identity object's serial number which is used to uniquely identify the device in the network environment.

6.6.5.5 Device status

This attribute represents the current state of the device. Its value changes as the state of the device changes. The Device status attribute state values are defined in Table 20.