BS EN IEC 61784-3-2:2021

BSI Standards Publication

Industrial communication networks — Profiles

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

Documents
Document Sharing Hub

Full document details: BS EN IEC 61784-3-2:2021

National foreword

This British Standard is the UK implementation of EN IEC 61784-3-2:2021. It is identical to IEC 61784-3-2:2021. It supersedes BS EN 61784-3-2:2017, which will be withdrawn on 23 June 2024.

The UK participation in its preparation was entrusted to Technical Committee GEL/65, Measurement and control.

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

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

© The British Standards Institution 2021
Published by BSI Standards Limited 2021

ISBN 978 0 580 52358 8

ICS 25.040.40; 35.100.05

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

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 June 2021.

Amendments/corrigenda issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: BS EN IEC 61784-3-2:2021

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN IEC 61784-3-2

June 2021

ICS 25.040.40; 35.100.05

Supersedes EN 61784-3-2:2017 and all of its amendments and corrigenda (if any)

English Version

Industrial communication networks - Profiles - Part 3-2: Functional safety fieldbuses - Additional specifications for CPF 2 (IEC 61784-3-2:2021)

Réseaux de communication industriels - Profils - Partie 3-2: Bus de terrain de sécurité fonctionnelle - Spécifications supplémentaires pour CPF 2 (IEC 61784-3-2:2021)

Industrielle Kommunikationsnetze - Profile - Teil 3-2: Funktional sichere Übertragung bei Feldbussen - Zusätzliche Festlegungen für die Kommunikationsprofilfamilie 2 (IEC 61784-3-2:2021)

This European Standard was approved by CENELEC on 2021-06-23. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

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

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

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

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

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

© 2021 CENELEC All rights of exploitation in any form and by any means reserved worldwide for CENELEC Members.

Ref. No. EN IEC 61784-3-2:2021 E

AVA Documents Document Sharing Hub

Full document details: BS EN IEC 61784-3-2:2021

European foreword

The text of document 65C/1083/FDIS, future edition 4 of IEC 61784-3-2, prepared by SC 65C "Industrial networks" of IEC/TC 65 "Industrial-process measurement, control and automation" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN IEC 61784-3-2:2021.

The following dates are fixed:

- latest date by which the document has to be implemented at national level by publication of an identical national standard or by endorsement (dop) 2022-03-23
- latest date by which the national standards conflicting with the document have to be withdrawn (dow) 2024-06-23

This document supersedes EN 61784-3-2:2017 and all of its amendments and corrigenda (if any).

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

Endorsement notice

The text of the International Standard IEC 61784-3-2:2021 was approved by CENELEC as a European Standard without any modification.

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

IEC 61000-1-2	NOTE	Harmonized as EN 61000-1-2
IEC 61000-6-7	NOTE	Harmonized as EN 61000-6-7
IEC 61010-2-201	NOTE	Harmonized as EN IEC 61010-2-201
IEC 61131-6	NOTE	Harmonized as EN 61131-6
IEC 61158 (series)	NOTE	Harmonized as EN 61158 (series)
IEC 61158-5 (series)	NOTE	Harmonized as EN 61158-5 (series)
IEC 61496 (series)	NOTE	Harmonized as EN IEC 61496 (series)
IEC 61508-1:2010	NOTE	Harmonized as EN 61508-1:2010 (not modified)
IEC 61508-4:2010	NOTE	Harmonized as EN 61508-4:2010 (not modified)
IEC 61508-5:2010	NOTE	Harmonized as EN 61508-5:2010 (not modified)
IEC 61511 (series)	NOTE	Harmonized as EN 61511 (series)
IEC 61784-3 (series)	NOTE	Harmonized as EN 61784-3 (series)
IEC 61784-5 (series)	NOTE	Harmonized as EN IEC 61784-5 (series)
IEC 61800-5-2	NOTE	Harmonized as EN 61800-5-2
IEC 62061	NOTE	Harmonized as EN 62061
IEC 62443 (series)	NOTE	Harmonized as EN IEC 62443 (series)
ISO 10218-1	NOTE	Harmonized as EN ISO 10218-1
ISO 13849 (series)	NOTE	Harmonized as EN ISO 13849 (series)

Documents
Document Sharing Hub

Full document details: BS EN IEC 61784-3-2:2021

Annex ZA
(normative)

Normative references to international publications with their corresponding European publications

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

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

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

Publication	Year	Title	EN/HD	Year
IEC 61131-2	-	Industrial-process measurement and control - Programmable controllers - Part 2: Equipment requirements and tests	-	-
IEC 61131-3	-	Programmable controllers - Part 3: Programming languages	EN 61131-3	-
IEC 61158-2	2014	Industrial communication networks - Fieldbus specifications - Part 2: Physical layer specification and service definition	EN 61158-2	2014
IEC 61158-3-2	-	Industrial communication networks - Fieldbus specifications - Part 3-2: Data-lonk layer service definition - Type 2 elements	EN 61158-3-2	-
IEC 61158-3-19	-	Industrial communication networks - Fieldbus specifications - Part 3-19: Data-link layer service definition - Type 19 elements	EN IEC 61158-3-19	-
IEC 61158-4-2	2019	Industrial communication networks - Fieldbus specifications - Part 4-2: Data-link layer protocol specification - Type 2 elements	EN IEC 61158-4-2	2019
IEC 61158-4-19	-	Industrial communication networks - Fieldbus specifications - Part 4 -19: Data-link layer protocol specification - Type 19 elements	EN IEC 61158-4-19	-
IEC 61158-5-2	-	Industrial communication networks - Fieldbus specifications - Part 5-2: Application layer service definition - Type 2 elements	EN IEC 61158-5-2	-
IEC 61158-5-19	-	Industrial communication networks - Fieldbus specifications - Part 5-19: Application layer service definition - Type 19 elements	EN IEC 61158-5-19	-

Documents
Document Sharing Hub
Full document details: BS EN IEC 61784-3-2:2021

Publication	Year	Title	EN/HD	Year
IEC 61158-6-2	-	Industrial communication networks - Fieldbus specifications - Part 6-2: Application layer protocol specification - Type 2 elements	EN IEC 61158-6-2	-
IEC 61158-6-19	-	Industrial communication networks - Fieldbus specifications - Part 6-19: Application layer protocol specification - Type 19 elements	EN IEC 61158-6-19	-
IEC 61326-3-1	-	Electrical equipment for measurement, control and laboratory use - EMC requirements - Part 3-1: Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety) – General industrial applications	EN 61326-3-1	-
IEC 61326-3-2	-	Electrical equipment for measurement, control and laboratory use - EMC requirements - Part 3-2: Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety) - Industrial applications with specified electromagnetic environment	EN IEC 61326-3-2	-
IEC 61508	series	Functional safety of electrical/electronic/programmable electronic safety-related systems	EN 61508	series
IEC 61784-1	-	Industrial communication networks - Profiles Part 1: Fieldbus profiles	EN IEC 61784-1	-
IEC 61784-2	-	Industrial communication networks - Profiles - Part 2: Additional fieldbus profiles for real-time networks based on ISO/IEC/IEEE 8802-3	EN IEC 61784-2	-
IEC 61784-3	2021	Industrial communication networks - Profiles - Part 3: Functional safety fieldbuses - General rules and profile definitions	EN IEC 61784-3	2021
IEC 61784-5-2	-	Industrial communication networks - Profiles - Part 5-2: Installation of fieldbuses - Installation profiles for CPF 2	EN IEC 61784-5-2	-
IEC 61918	-	Industrial communication networks - Installation of communication networks in industrial premises	EN IEC 61918	-
IEC 62026-3	-	Low-voltage switchgear and controlgear - Controller-device interfaces (CDIs) - Part 3: DeviceNet	-	-
ISO 13849-1	2015	Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design	EN ISO 13849-1	2015

Documents
Document Sharing Hub

Full document details: BS EN IEC 61784-3-2:2021

Publication	Year	Title	EN/HD	Year
ISO 15745-2	2003	Industrial automation systems and integration -- Open systems application integration framework -- Part 2: Reference description for ISO 11898-based control systems	-	-
ISO 15745-3	2003	Industrial automation systems and integration - Open systems application integration framework -- Part 3: Reference description for IEC 61158 based control systems	-	-
ISO 15745-4	2003	Industrial automation systems and integration - Open systems application integration framework - Part 4: Reference description for Ethernet-based control systems	-	-

Documents
Document Sharing Hub
Full document details: BS EN IEC 61784-3-2:2021

This page deliberately left blank

Documents
Document Sharing Hub

Full document details: BS EN IEC 61784-3-2:2021

CONTENTS

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

AVA Documents
Document Sharing Hub

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

AVA Documents
Document Sharing Hub

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

Documents
Document Sharing Hub
Full document details: BS EN IEC 61784-3-2:2021

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

Documents
Document Sharing Hub
Full document details: BS EN IEC 61784-3-2:2021

9.5.3 Bit Error Rate (BER) 261
9.6 Maintenance 262
9.7 Safety manual 262
10 Assessment 262
Annex A (informative) Additional information for functional safety communication profiles of CPF 2 263
A.1 Hash function example code 263
A.2 Void 277
Annex B (informative) Information for assessment of the functional safety communication profiles of CPF 2 278
Bibliography 279

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

AVA Documents
Document Sharing Hub
Full document details: BS EN IEC 61784-3-2:2021

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

AVA Documents
Document Sharing Hub

Figure 73 – Connection categories and supported services 213
Figure 74 – Recommended connection types 214
Figure 75 – Logic-to-logic supported services 214
Figure 76 – Recommended connection types for logic to logic 215
Figure 77 – Configuration data transfers 216
Figure 78 – Protection measures in safety devices 218
Figure 79 – Configuration, testing and locked relationships 221
Figure 80 – Originator's configuration data 223
Figure 81 – SNCT to device download process 225
Figure 82 – SNCT Downloads to originators that perform Type 1 configuration 226
Figure 83 – Protection from locking and ownership 228
Figure 84 – Verification process including all alternatives 230
Figure 85 – Baseline FSCP 2/1 on CP 16/3 device 245
Figure 86 – FSCP 2/1 Adaptation Layer and SMP interaction 247
Figure 87 – FSCP 2/1 Adaptation 248
Figure 88 – CP 16/3 device model 249
Figure 89 – Adding a standard module to a modular device 251
Figure 90 – Safety device NodeID processing logic 256
Figure 91 – Safety function response time 257
Figure 92 – Safety function response time components 259
Figure 93 – Network protocol reliability block diagram (RBD) 260

Table 1 – Communications errors and detection measures matrix 29
Table 2 – New class attributes 31
Table 3 – Service extensions 32
Table 4 – SafetyOpen and SafetyClose response format 32
Table 5 – Safety network segment identifier 35
Table 6 – Safety network segment definition 35
Table 7 – Safety network segment router format 37
Table 8 – Safety Network Segment Extended Format 37
Table 9 – Multipoint producer parameter evaluation rules 42
Table 10 – ForwardOpen setting options for safety connections with object-based application paths 45
Table 11 – ForwardOpen setting options for safety connections with ANSI Extended symbol segment application path 47
Table 12 – Network connection parameters for safety connections 48
Table 13 – SafetyOpen target application reply (size: 10 octets) 48
Table 14 – EF CP 2/2 or CP 16/3 SafetyOpen target application reply (size: 14 octets) 49
Table 15 – BF CP 2/3 SafetyOpen target application reply (size: 18 octets) 49
Table 16 – EF CP 2/3 SafetyOpen target application reply (size: 22 octets) 50
Table 17 – New and extended error codes for safety 50
Table 18 – SafetyOpen error event guidance table 51
Table 19 – Identity object common service changes 53
Table 20 – Identity object extensions for CP 16/3 devices 53

AVA Documents
Document Sharing Hub

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

AVA Documents
Document Sharing Hub

Full document details: BS EN IEC 61784-3-2:2021

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

AVA Documents
Document Sharing Hub

Full document details: BS EN IEC 61784-3-2:2021

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

Documents
Document Sharing Hub

Full document details: BS EN IEC 61784-3-2:2021

INTERNATIONAL ELECTROTECHNICAL COMMISSION

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES –

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

FOREWORD

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

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

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

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

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

AVA Documents Document Sharing Hub

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

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

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

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

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

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

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

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

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

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

Documents
Document Sharing Hub

Full document details: BS EN IEC 61784-3-2:2021

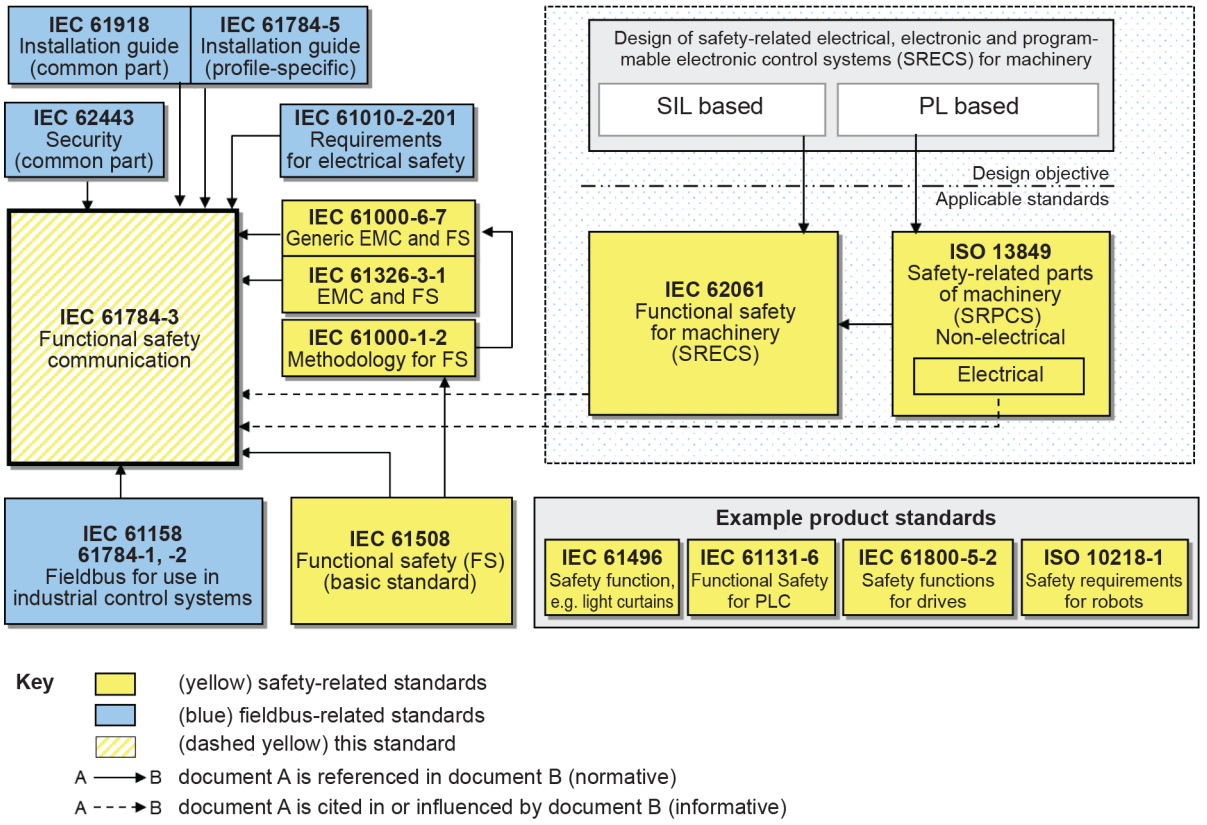
0 Introduction

0.1 General

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

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

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

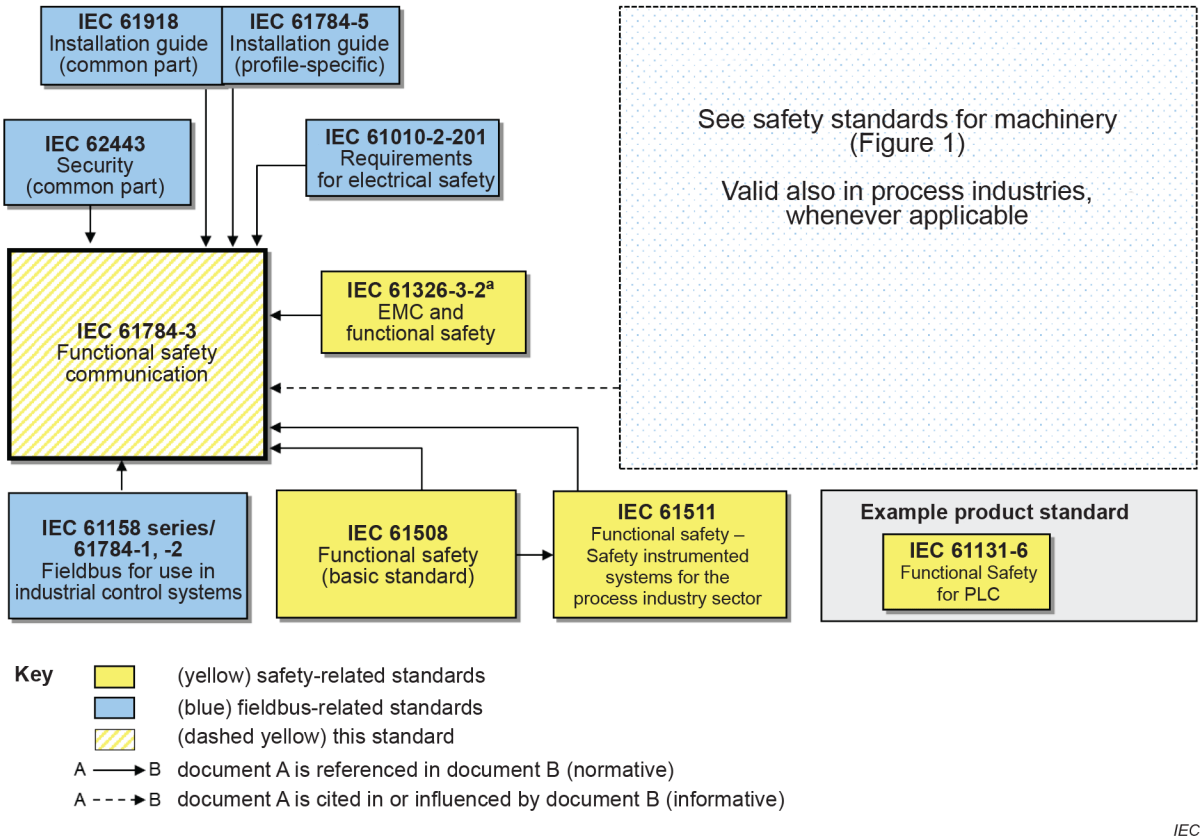


NOTE IEC 62061 specifies the relationship between PL (Category) and SIL.

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

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

Documents
Document Sharing Hub
Full document details: BS EN IEC 61784-3-2:2021



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

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

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

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

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

IEC 61784-3 (all parts) describes:

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

0.2 Patent declaration

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

AVA Documents
Document Sharing Hub

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

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

Documents
Document Sharing Hub

Full document details: BS EN IEC 61784-3-2:2021

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES –

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

1 Scope

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

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

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

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

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

2 Normative references

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

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

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

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

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

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

[1] In the following pages of this document, "IEC 61508" will be used for "IEC 61508 (all parts)".

Documents
Document Sharing Hub

Full document details: BS EN IEC 61784-3-2:2021

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Documents
Document Sharing Hub

Full document details: BS EN IEC 61784-3-2:2021

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

3 Terms, definitions, symbols, abbreviated terms and conventions

3.1 Terms and definitions

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

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

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

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

3.1.1 Common terms and definitions

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

3.1.1.1
bit error probability
Pe
probability for a given bit to be received with the incorrect value

3.1.1.2
black channel
defined communication system containing one or more elements without evidence of design or validation according to IEC 61508

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

3.1.1.3
bridge
abstract device that connects multiple network segments along the data link layer

3.1.1.4
closed communication system
fixed number or fixed maximum number of participants linked by a *communication system* with well-known and fixed properties, and where the *risk* of unauthorized access is considered negligible

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

3.1.1.5
communication channel
logical *connection* between two end-points within a *communication system*

3.1.1.6
communication system
arrangement of hardware, software and propagation media to allow the transfer of *messages* (ISO/IEC 7498-1 application layer) from one application to another

3.1.1.7
connection
logical binding between two application objects within the same or different devices

AVA Documents Document Sharing Hub

3.1.1.8
Cyclic Redundancy Check
CRC
<value> redundant data derived from, and stored or transmitted together with, a block of data in order to detect data corruption

<method> procedure used to calculate the redundant data

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

Note 2 to entry: See also [26], [27] [2].

3.1.1.9
defined communication system
defined channel
fixed number or fixed maximum number of participants linked by a *fieldbus* based *communication system* with well-known and fixed properties, such as installation conditions, electromagnetic immunity, industrial *(active) network elements*, and where the *risk* of unauthorized access is reduced to a tolerated level according to the lifecycle model of IEC 62443 (all parts), using for example zones and conduits

3.1.1.10
device
physical entity connected to the fieldbus composed of communication element and possibly other functional elements

[SOURCE: IEC 61158-2:2014, 3.1.13, modified – Note to entry and some details have been deleted.]

3.1.1.11
DLPDU
DEPRECATED: frame
Data Link Protocol Data Unit

3.1.1.12
error
discrepancy between a computed, observed or measured value or condition and the true, specified or theoretically correct value or condition

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

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

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

3.1.1.13
failure
termination of the ability of a functional unit to perform a required function or operation of a functional unit in any way other than as required

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

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

[2] Figures in square brackets refer to the bibliography.

Documents
Document Sharing Hub
Full document details: BS EN IEC 61784-3-2:2021

3.1.1.14
fault
abnormal condition that may cause a reduction in, or loss of, the capability of a functional unit to perform a required function

Note 1 to entry: IEC 60050-191:1990, 191-05-01 defines "fault" as a state characterized by the inability to perform a required function, excluding the inability during preventive maintenance or other planned actions, or due to lack of external resources.

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

3.1.1.15
fieldbus
communication system based on serial data transfer and used in industrial automation or process control applications

3.1.1.16
functional safety communication profile
FSCP
technology specification for the implementation of an SCL

3.1.1.17
hash function
(mathematical) function that maps values from a (possibly very) large set of values into a (usually) smaller range of values

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

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

3.1.1.18
hazard
potential source of harm

Note 1 to entry: The term includes danger to persons arising within a short time scale (for example, fire and explosion) and also those that have a long-term effect on a person's health (for example, release of a toxic substance).

[SOURCE: IEC 61508-4:2010, 3.1.2 and ISO/IEC Guide 51:2014, definition 3.2]

3.1.1.19
master
communication entity able to initiate and schedule communication activities by other stations which may be masters or slaves

3.1.1.20
message
<information theory and communication theory> ordered sequence of characters (usually octets) intended to convey information

[SOURCE: ISO/IEC 2382:2015, 2123205, modified – insertion of "(usually octets)", deletion of notes and source]

3.1.1.21
performance level
PL
discrete level used to specify the ability of safety-related parts of control systems to perform a *safety function* under foreseeable conditions

[SOURCE: ISO 13849-1:2015, 3.1.23]

Documents
Document Sharing Hub

Full document details: BS EN IEC 61784-3-2:2021

3.1.1.22
redundancy
existence of more than one means for performing a required function or for representing information

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

3.1.1.23
residual error rate
statistical rate at which the SCL *safety measures* fail to detect *errors*

3.1.1.24
risk
combination of the probability of occurrence of harm and the severity of that harm

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

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

3.1.1.25
safety communication channel
communication channel starting at the top of the SCL of the source and ending at the top of the SCL of the sink

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

3.1.1.26
safety communication layer
SCL
communication layer above the FAL that includes all necessary additional measures to ensure safe transmission of data in accordance with the requirements of IEC 61508

3.1.1.27
safety connection
connection that utilizes the safety protocol for communications transactions

3.1.1.28
safety data
data transmitted across a safety network using a safety protocol

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

3.1.1.29
safety device
device designed in accordance with IEC 61508 and which implements the functional safety communication profile

3.1.1.30
safety function
function to be implemented by an E/E/PE *safety-related system* or other *risk* reduction measures, that is intended to achieve or maintain a safe state for the EUC, in respect of a specific hazardous event

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

Documents
Document Sharing Hub

Full document details: BS EN IEC 61784-3-2:2021

3.1.1.31
safety function response time
worst case elapsed time following an actuation of a safety sensor connected to a *fieldbus*, until the corresponding safe state of its safety actuator(s) is achieved in the presence of *errors* or *failures* in the *safety function*

Note 1 to entry: This concept is introduced in IEC 61784-3:2021, 5.2.4 and addressed by the functional safety communication profiles defined in this document.

3.1.1.32
safety integrity level
SIL
discrete level (one out of a possible four), corresponding to a range of safety integrity values, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest

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

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

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

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

3.1.1.33
safety measure
measure to control possible communication *errors* that is designed and implemented in compliance with the requirements of IEC 61508

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

Note 2 to entry: Communication *errors* and related safety measures are detailed in IEC 61784-3:2021, 5.3 and 5.4.

3.1.1.34
safety PDU
SPDU
PDU transferred through the *safety communication channel*

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

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

3.1.1.35
safety-related application
programs designed in accordance with IEC 61508 to meet the SIL requirements of the application

3.1.1.36
safety-related system
system performing *safety functions* according to IEC 61508

3.1.1.37
slave
communication entity able to receive *messages* and send them in response to another communication entity which may be a *master* or a slave, but not to initiate communication activities

Documents
Document Sharing Hub
Full document details: BS EN IEC 61784-3-2:2021

3.1.1.38
spurious trip
trip caused by the safety system without a process demand

3.1.1.39
time stamp
time information included in a *message*

3.1.2 CPF 2: Additional terms and definitions

3.1.2.1
base format
format used for connection RPIs of less than 100 ms or for applications where dropped connections can be tolerated

3.1.2.2
deprecate
action to withdraw official support for or discourage the use of (something, such as a software product) in favor of a newer or better alternative

3.1.2.3
extended format
format used for connection RPIs of more than 100 ms or for applications where there is a need to avoid dropped connections

3.1.2.4
ping
request for the consumer to acknowledge the reception of a message

3.1.2.5
ping response
response to a ping

3.1.2.6
originator
node that requests the creation of a connection

3.1.2.7
signature
method of uniquely identifying a set of data

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

3.1.2.8
single safety port device
originator, target, or mixed originator/target device that performs safety communications on one and only one CIP port

3.1.2.9
systematic capability
measure (expressed on a scale of SC 1 to SC 4) of the confidence that the systematic safety integrity of an element meets the requirements of the specified SIL, in respect of the specified element safety function, when the element is applied in accordance with the instructions specified in the compliant item safety manual for the element

[SOURCE: IEC 61508-4:2010, 3.5.9, modified – notes deleted]

Documents
Document Sharing Hub

Full document details: BS EN IEC 61784-3-2:2021

3.1.2.10
systematic safety integrity
part of the safety integrity of a safety-related system relating to systematic failures in a dangerous mode of failure

[SOURCE: IEC 61508-4:2010, 3.5.6, modified – note deleted]

3.1.2.11
target
node that receives a connection creation request

3.2 Symbols and abbreviated terms

3.2.1 Common symbols and abbreviated terms

CP	Communication Profile	[IEC 61784-1]
CPF	Communication Profile Family	[IEC 61784-1]
CRC	Cyclic Redundancy Check	
DLL	Data Link Layer	[ISO/IEC 7498-1]
DLPDU	Data Link Protocol Data Unit	
EMC	Electromagnetic Compatibility	
EUC	Equipment Under Control	[IEC 61508-4:2010]
E/E/PE	Electrical/Electronic/Programmable Electronic	[IEC 61508-4:2010]
FAL	Fieldbus Application Layer	[IEC 61158-5 (all parts)]
FS	Functional Safety	
FSCP	Functional Safety Communication Profile	
MTBF	Mean Time Between Failures	
MTTF	Mean Time To Failure	
PDU	Protocol Data Unit	[ISO/IEC 7498-1]
PFD	Probability of dangerous Failure on Demand	[IEC 61508-4:2010]
PFH	Average frequency of dangerous failure [h^{-1}] per hour	[IEC 61508-4:2010]
PhL	Physical Layer	[ISO/IEC 7498-1]
PL	Performance Level	[ISO 13849-1]
PLC	Programmable Logic Controller	
SCL	Safety Communication Layer	
SIL	Safety Integrity Level	[IEC 61508-4:2010]

Documents
Document Sharing Hub
Full document details: BS EN IEC 61784-3-2:2021

3.2.2 CPF 2: Additional symbols and abbreviated terms

AIRS	Already In Requested Mode/State	
BER	Bit Error Rate	
BF	Base Format	
CCO	Connection Configuration Object	
CFUNID	Configuration UNID	
CNP	Connection Point	
CID	Consumer ID	
CIP™[3]	Common Industrial Protocol (application framework shared among CPF 2 communication profiles)	
CPCRC	Connection Parameter CRC	
CTM	Connection Timeout Multiplier	
EDS	Electronic Data Sheet	
EF	Extended Format	
EPI	Expected Packet Interval	
LED	Light Emitting Diode	
MACID	Device physical address (CP 2/3)	
MOD	Module	
NodeID	For CP 2/3 safety devices, this is the MACID of the device on the network. For CP 2/2 safety devices, this is the IP address of the device on the network. For CP 16/3 safety devices, this is the SDID of the device on the network.	
NV	Non-Volatile	
NVS	Non-Volatile Storage	
OCPUNID	Output Connection Owner UNID	
OSC	Object State Conflict	
O-to-T	Originator to Target	
OUNID	Originator UNID	
PID	Producer Identifier	
PS	Power Supply	
Res.	Reserved	
RPI	Requested Packet Interval	
SCCRC	Safety Configuration Data CRC	
SCID	Safety Configuration Identified	
SCTS	Safety Configuration Time Stamp	
SNCT	Safety Network Configuration Tool	
SNN	Safety Network Number	
T-to-O	Target to Originator	
TBD	To Be Defined	
TNS	TUNID Not Set	
TUNID	Target UNID	
UML	Universal Modeling Language	[ISO/IEC 19501]

[3] For trade name declaration, see Clause 4.

Documents
Document Sharing Hub

Full document details: BS EN IEC 61784-3-2:2021

UNID Unique Network Identifier

3.3 Conventions

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

As appropriate this document 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.

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

The basic profiles CP 2/1, CP 2/2, CP 2/3 and CP 16/3 are defined in IEC 61784-1 and IEC 61784-2. The CPF 2 functional safety communication profile FSCP 2/1 (CIP Safety™[4]) is based on the CPF 2 basic profiles in IEC 61784-1 and IEC 61784-2, the CP 16/3 basic profile in IEC 61784-2, and the safety communication layer specifications defined in this document.

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 ODVA, Inc. This information is given for the convenience of users of this document and does not constitute an endorsement by IEC of the trade name holder or any of its products. Compliance to this document does not require use of the trade names CIP™ or CIP Safety™. Use of the trade names CIP™ or CIP Safety™ requires permission of ODVA and compliance with conditions for their use (such as testing and validation).

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

AVA Documents
Document Sharing Hub

Full document details: BS EN IEC 61784-3-2:2021

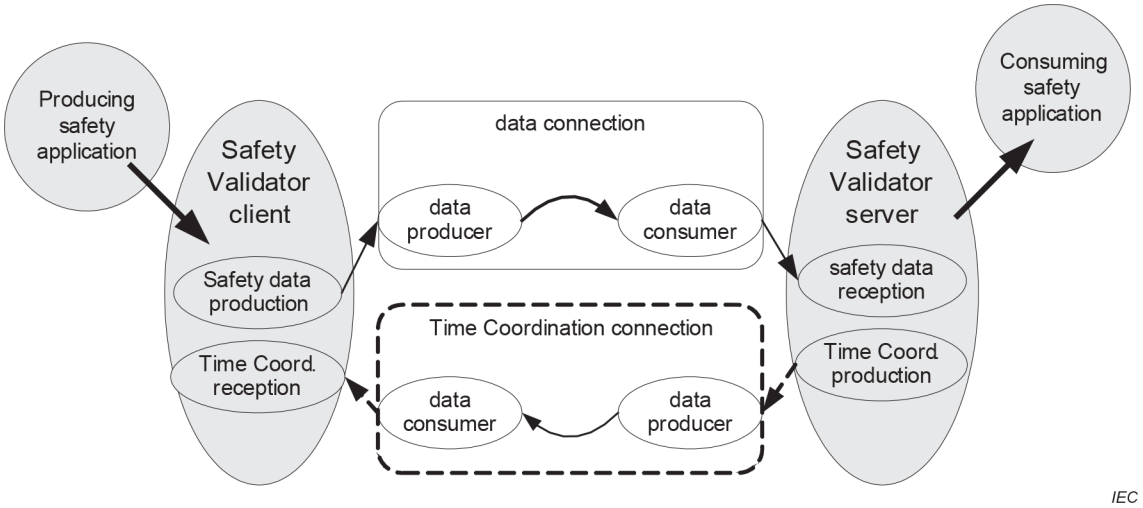


Figure 3 – Relationship of Safety Validators

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

Documents [30] and [31] provide additional specifications which are relevant when implementing the SCL defined in this document.

Documents
Document Sharing Hub
Full document details: BS EN IEC 61784-3-2:2021

5.2 Safety functional requirements

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

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

5.3 Safety measures

Table 1 contains the measures used to the 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.

Documents
Document Sharing Hub
Full document details: BS EN IEC 61784-3-2:2021

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.

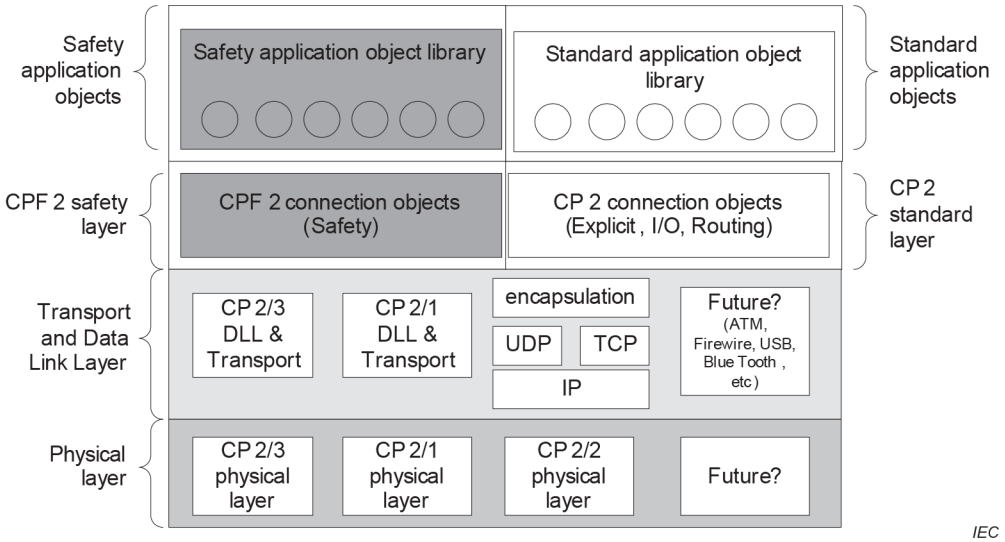


Figure 4 – Communication layers

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™[6]), CP 2/2 (EtherNet/IP™[7]), and CP 16/3 (SERCOS III™[8])). There are no requirements of CPF 2 communications profiles other than those defined in this document.

5.5.2 Data types

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

---

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

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

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

AVA Documents Document Sharing Hub

6 Safety communication layer services

6.1 General

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

6.2 Connection object

6.2.1 General

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

6.2.2 Class attribute extensions

Table 2 defines the class attributes used by safety devices.

Table 2 – New class attributes

Attrib ID	Need in implementation	Access rule	N V	Name	Date type	Description of attribute
8	Optional	Get	V	Connection request error count	UINT	Diagnostic Counter that is a running count of SafetyOpen or SafetyClose faults[a]
9	Optional	Get	V	Safety connection counters	STRUCT of:	Status counters
				SafetyOpen request suc-cess 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.

Documents
Document Sharing Hub

Full document details: BS EN IEC 61784-3-2:2021

6.2.3 Service extensions

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

Table 3 – Service extensions

Service code	Need in implementation		Service name	Description of service
	Class	Instance		
$4D_{hex}$	Optional	N/A	Reset Counters	This service resets class attributes 8 and 9 to zero
$4E_{hex}$	Required	N/A	SafetyClose	Used to close a Safety I/O connection. See the ForwardClose service of the Connection Manager object 6.3.13
54_{hex}	Required	N/A	SafetyOpen[a]	Used to establish a safety I/O connection. See the ForwardOpen service of the Connection Manager object 6.3.2

[a] The SafetyOpen service data shall contain a Safety Network Segment in the Connection_Path field.

6.2.4 Explicit message response format for SafetyOpen and SafetyClose

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

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

Table 4 – SafetyOpen and SafetyClose response format

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

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

Documents
Document Sharing Hub
Full document details: BS EN IEC 61784-3-2:2021

6.3 Connection Manager object

6.3.1 General

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

6.3.2 ForwardOpen for safety

6.3.2.1 ForwardOpen for safety contents

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

Parameter Name		Data Type / Size	Target Destination and Semantics
Priority/Time_tick		OCTET	Connection manager servicing request
Time-out_ticks		USINT	Connection manager servicing request
O-to-T Network Connection ID		UDINT	Consuming connection instance:: CIP consumed connection ID
T-to-O Network Connection ID		UDINT	Producing connection instance:: CIP producing connection ID
Connection Serial Number		UINT	Value: Unique (to originator) 16-bit number. Destination: Connection manager servicing request
Originator Vendor ID		UINT	Connection manager servicing request
Originator Serial Number		UDINT	Connection manager servicing request
Connection Timeout Multiplier		USINT	Producing and consuming connection instance: Timeout Multiplier
Reserved		3 OCTETS	
O-to-T RPI		UDINT	Consuming connection instance: EPR
O-to-T Network Connection Parameters	Redundant Owner	WORD	Value: 0 (Safety Connections do not support redundancy); Destination: Connection Manager
	Connection Type		Value: Point-to-point; Destination: Connection Manager
	Priority		Value: 1 (High '01') or 2 (Schedule '10'); 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: 1 (High '01') or 2 (Schedule '10'); Destination: Connection Manager
	Fixed/Variable		Value: Fixed; Destination: Connection Manager

Documents
Document Sharing Hub
Full document details: BS EN IEC 61784-3-2:2021

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 Each router removes the Routing Segments contained in the Connection_Path that apply to it before forwarding the request to the next hop/target. The Target Network Segments area is reserved for gray/black channel target network segments. Therefore the Connection_Path_Size value included in the Connection Parameter CRC calculation does not include the words used for the Routing Segments and Target Network Segments present in the originator's Connection_Path field.
Connection_Path (Padded EPATH)				
	Port Segment Group(s)		Variable	Consumed by intermediate router Connection Manager(s). See IEC 61158-6-2. NOTE Each Router Format Safety Network Segment immediately follows the Port segment of the (CPF 2–to–CP 2/3) 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	
	Target Network Segments		Variable	See IEC 61158-6-2 for more infomration. Note that the Target Safety Segment is placed after the Application Path(s) and any (optional) Config Data. This position is reserved for black channel target network segments.
	Application Path(s)		See 6.3.9 for safety connection application path construction rules.	
	Config Data	Data Segment: Simple Data	Variable	Configuration data to apply to the Safety-related application object identified by Config Path
	Target Safety Segment		50_{hex}	Safety Network Segment for target, see 6.3.3.

Key

= Connection/Safety Validator fields covered by Connection Parameters CRC

= Configuration Data Segment coved by SCCV

Figure 5 – ForwardOpen with safety network segment

Documents
Document Sharing Hub

Full document details: BS EN IEC 61784-3-2:2021

6.3.2.2 ForwardOpen for safety for Extended Format

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

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

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

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

6.3.3 Safety network segment

6.3.3.1 Common format

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

Table 5 – Safety network segment identifier

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

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

Table 6 – Safety network segment definition

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

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

Devices are no longer required to implement the Base Format. Devices which no longer support the format shall respond to Safety Connection requests using the Target Format with Safety Parameter Error – Invalid Safety Connection Format, 01_{hex}, 0803_{hex}. Originators may continue to support this Target Format for backward compatibility to existing devices.

Documents
Document Sharing Hub
Full document details: BS EN IEC 61784-3-2:2021

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

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

Key

= Safety Segment fields covered by Connection Parameters CRC

Figure 6 – Safety network target format

Documents
Document Sharing Hub
Full document details: BS EN IEC 61784-3-2:2021

6.3.3.3 Safety network segment: router format (01_{hex})

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

Table 7 – Safety network segment router format

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

6.3.3.4 Safety network segment: Extended Format (0x02)

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

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

Table 8 – Safety Network Segment Extended Format

Field Name	Data Type	Description
Reserved	octet	Pad
Configuration CRC (SCCRC)	UDINT	CRC-S32 of target Config Data Segment. A value of 0 is an indicator that SCID check can be skipped
Configuration TimeStamp (SCTS)	DATE_AND_TIME	Time and Date stamp of the configuration. A value of 0 is an indicator that SCID check can be skipped. 6 octet value (Date: 2 octets, Time: 4 octets)
Time Correction EPI	UDINT	Not used: 0 When used: Time Correction Connection Instance:: EPI
Time Correction Network Connection Parameters	WORD	Network Connection Parameters for the Time Correction connection. This field uses the same definition as the Network Connection Parameter within the Connection Manager object. When not used: 0 (Null). When used: Fixed, High Priority, Multipoint
Target_UNID (TUNID)	STRUCT of: UINT 10: octets	UNID of the target device. This value is a 10 octet value consisting of the Safety Network Id (6 octets) and the Node Address (4 octet address)

Documents
Document Sharing Hub

Field Name	Data Type	Description
Originator UNID (OUNID)	STRUCT of: UINT 10: octets	UNID of the Originator device. This value is a 10 octet value consisting of the Safety Network Id (6 octets) and the Node Address (4 octet address)
Ping_Interval_EPI_Multiplier	UINT	Number that defines the Ping_Count_Interval for the connection. Valid range of values is given in 7.7.5.10
Time_Coord_Msg_Min_Multiplier	UINT	For Producing Connection Instance. Valid range is 0 to 7 813
Network_Time_Expectation_Multiplier	UINT	For Consuming Connection Instance. Valid range is 1 to 45 313
Timeout_Multiplier	USINT	Used by producer and consumer to timeout connections. Valid range of 1 to 255 for Extended Format
Max_Consumer_Number	USINT	Value: 1 (Point to point), 2-15(Multipoint)
Max_Fault_Number	UINT	Number of erroneous packets within one hour after which a connection is closed. Used by both producers and consumers. Value = 2
Connection Parameters CRC (CPCRC)	UDINT	CRC-S32 of target connection parameters in this request
Time Correction Connection ID[a]	UDINT	Not Used: 0xFFFFFFFF When used: Time Correction Connection Instance:: Connection ID
Initial Time Stamp[a]	UINT	Used by Consumer to initialize Last_Time_Stamp_for_Rollover. Consuming Originator sets to 0xFFFF
Initial Rollover Value[a]	UINT	Used by Consumer to initialize TS_Rollover_Count. Consuming Originator sets to 0xFFFF

[a] These fields are NOT included in the CPCRC.

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

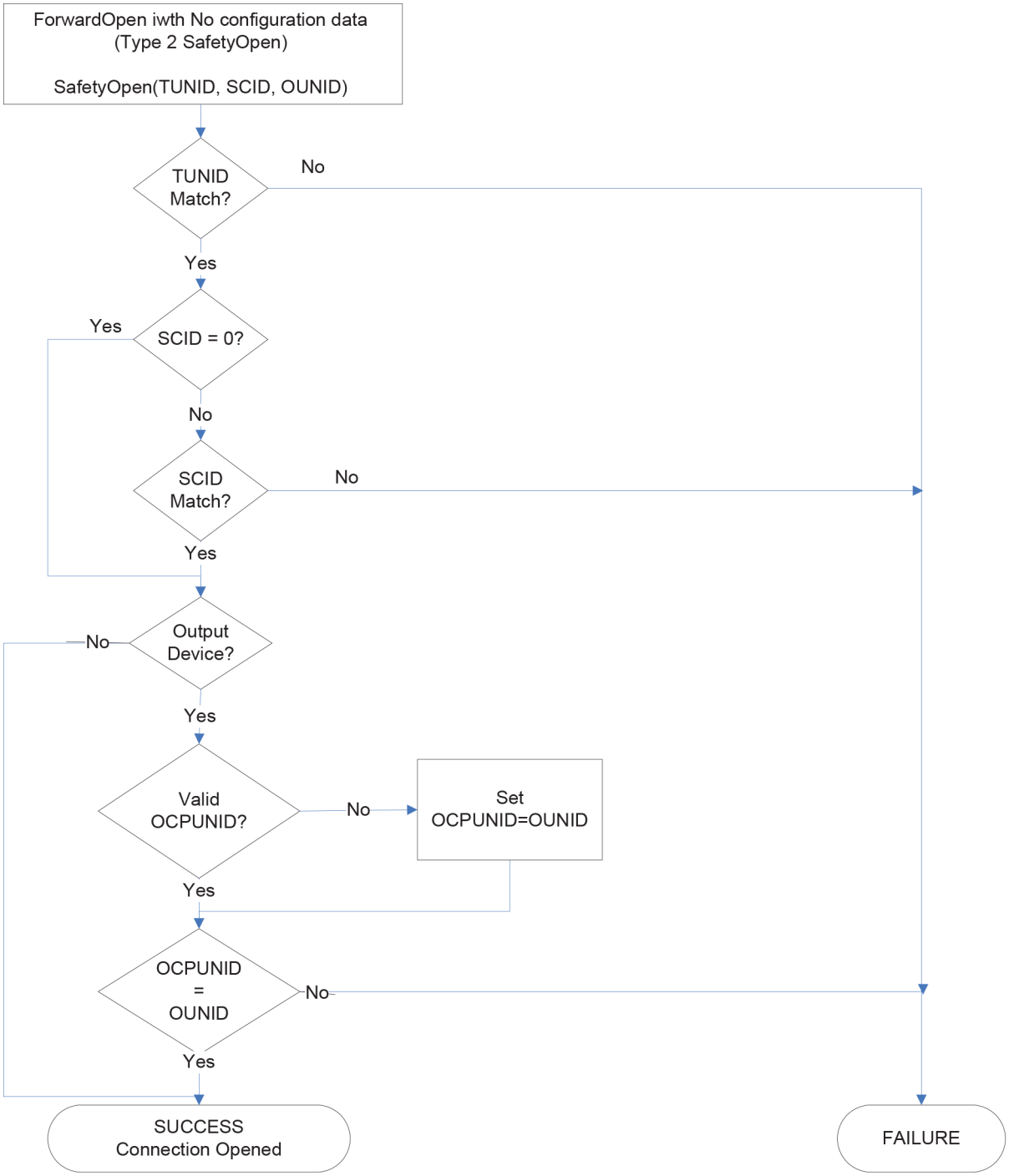
The following flowcharts outline the required behavior of a target upon receipt of a SafetyOpen:

a) 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;

AVA Documents Document Sharing Hub

b) The target checks that the electronic key segment matches (see 6.3.7);

c) Depending on the type of safety connection, the logic is defined in Figure 7 or Figure 8 shall be followed.



Key:

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

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

IEC

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

Documents
Document Sharing Hub
Full document details: BS EN IEC 61784-3-2:2021

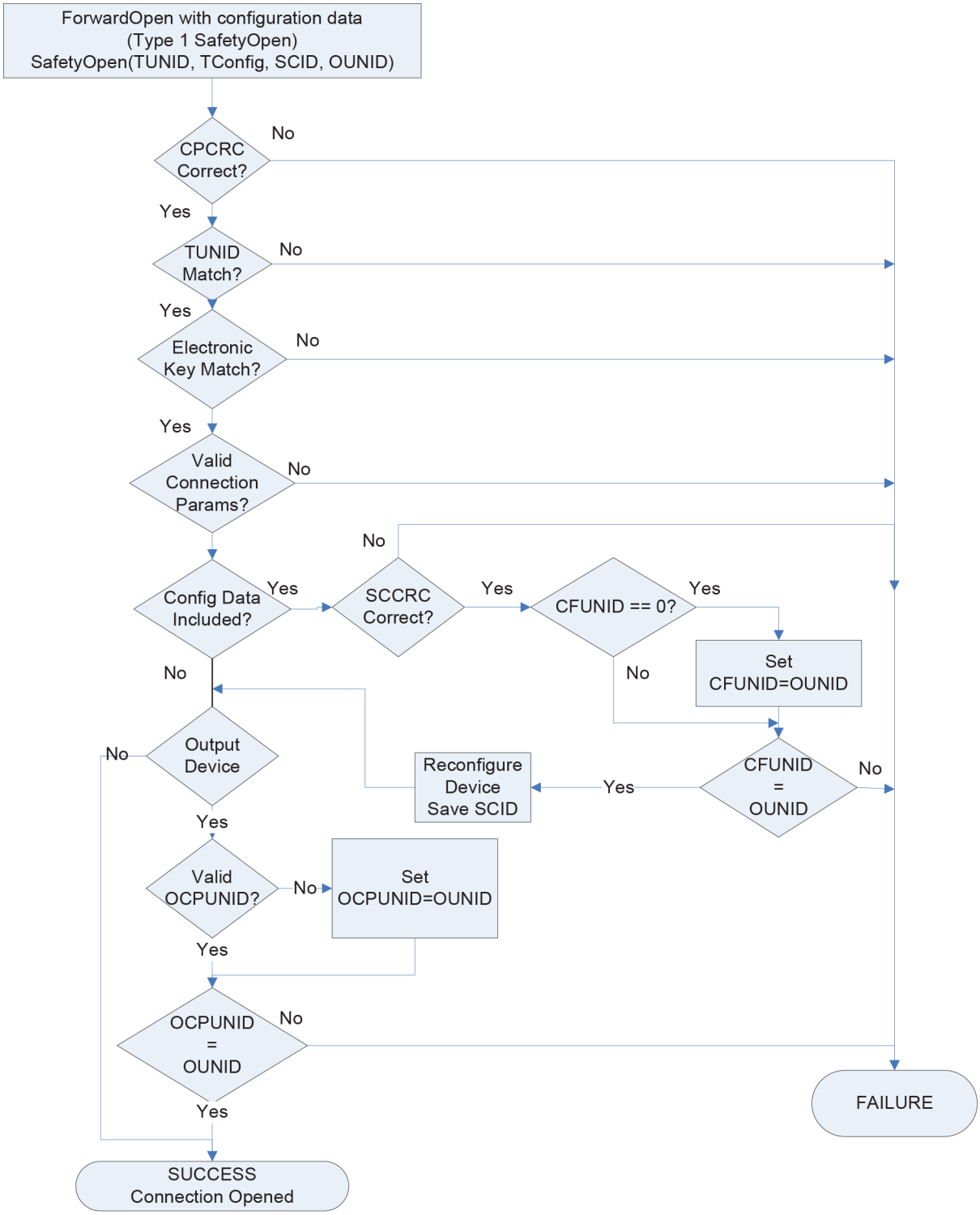


Figure 8 – Target Processing for SafetyOpen with configuration data (Type 1 SafetyOpen)

Documents
Document Sharing Hub
Full document details: BS EN IEC 61784-3-2:2021

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

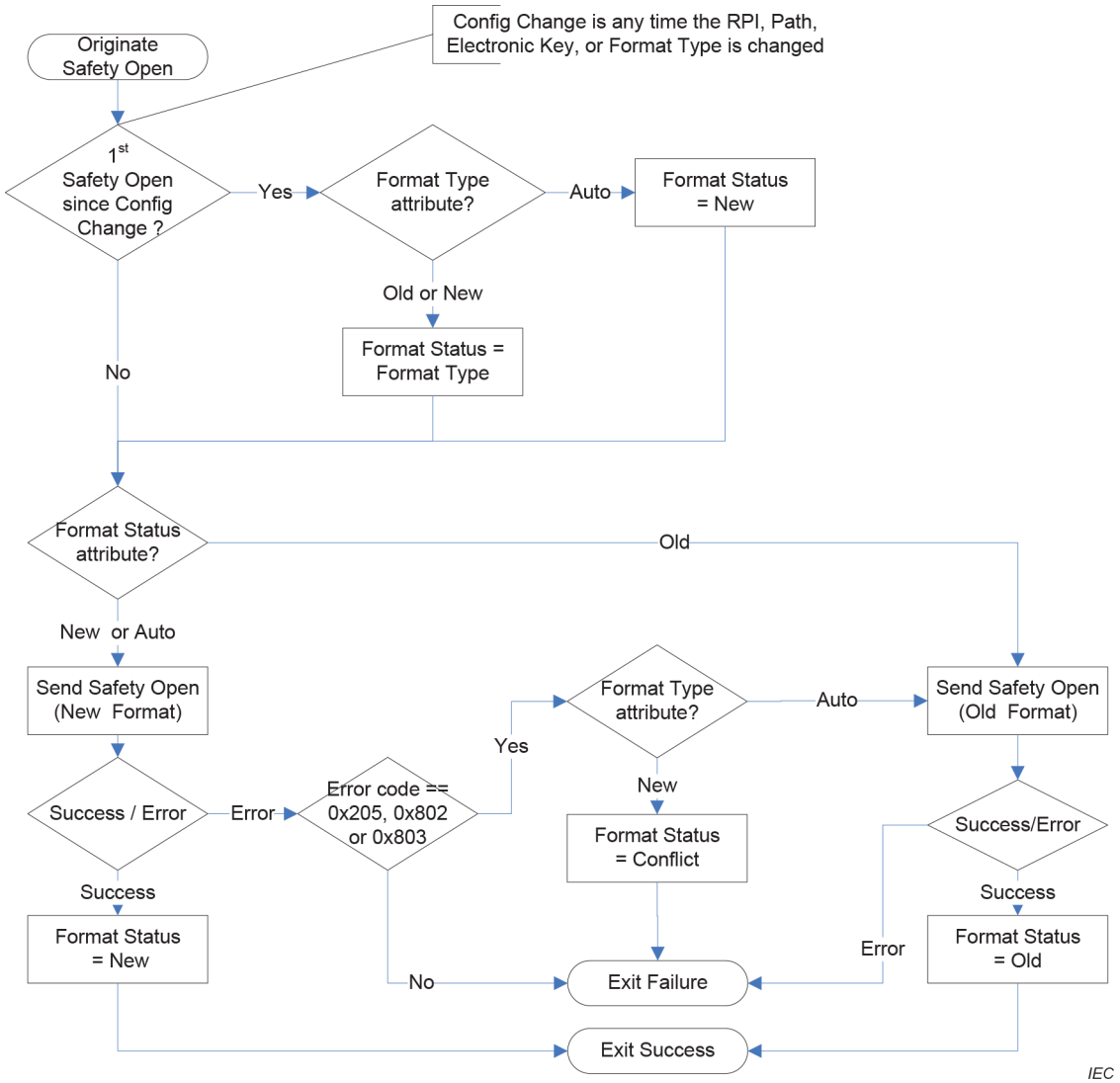


Figure 9 – Originator logic to determine which format to use

6.3.6 Checks required by Multipoint producers with existing connections

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

Documents
Document Sharing Hub
Full document details: BS EN IEC 61784-3-2:2021

Table 9 – Multipoint producer parameter evaluation rules

Safety parameter	Producer evaluation rule if connection exists	Error response[a] (if appropriate)	
		General	Extended
Ping_Interval EPI Multiplier	Shall match existing P.I.E.M.	01_{hex}	0815_{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	01_{hex}	0816_{hex}
T-to-O RPI, O-to-T RPI	Shall match existing connection RPIs	01_{hex}	0112_{hex}
Time Correction RPI	Shall match existing connection Time Correction RPI	01_{hex}	0801_{hex}
Safety Network Segment Type	Shall match existing connection format[b]	0x01	$0x817_{hex}$
Max_Fault_Number	Accept any (all can be different)	N/A	

[a] At the option of the device developer, another connection could also be opened rather than return an error response; this flexibility differs from the requirements specified for standard multipoint connections in CPF 2.

[b] Subsequent connection requests on an existing multi-point connection shall all be the same format as the existing connection.

6.3.7 Electronic key usage for safety

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

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

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

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

6.3.8 RPI vs. API in safety connections

Safety devices do not have the ability to negotiate the RPI value. Safety Targets either accept the requested RPI because it can be supported, or it rejects it completely. The tolerance around an acceptable RPI request shall be ± 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 rules for safety connections

6.3.9.1 General

The rules for the usage of the three possible target application paths contained in the Connection Path parameter of a ForwardOpen for a standard connection are based on the Network Connection Parameter Connection Type values and the presence of the Data Segment as defined in IEC 61158-6-2.

AVA Documents Document Sharing Hub

Since the Network Connection Parameter Connection Type values are never Null for safety connections, the application path construction rules specific to safety connections are provided in Subclauses 6.3.9.2 to 6.3.9.3.

6.3.9.2 Assembly object instance and/or Connection Point application paths

I/O targets typically use a combination of object instances and/or connection points to identify the application data available on any given target connection.

When Assembly object instances and/or connection points are used to identify a safety connection target, 3 references (one for configuration, one for consumed data and one for produced data) shall be provided.

The possible path types are identified as follows:

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

B. - [Class] [Assembly] [Instance] [Producer-instance]

C. - [Class] [Assembly] [Instance] [Consumer-instance]

D. - [Class] [Assembly] [Instance] [Device-defined NULL instance)]

E. - [CNP] [Consumer CNP]

F. - [CNP] [Producer CNP]

G. - [CNP] [Device-defined NULL CNP]

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

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

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

The following rules apply to SafetyOpen path construction:

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

Documents
Document Sharing Hub

Full document details: BS EN IEC 61784-3-2:2021