IEC 61784-3-2

Edition 4.0 2021-05

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

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

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



IEC 61784-3-2:2021-05(en-fr)

THIS PUBLICATION IS COPYRIGHT PROTECTED
Copyright © 2021 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'IEC ou du Comité national de l'IEC du pays du demandeur. Si vous avez des questions sur le copyright de l'IEC ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de l'IEC de votre pays de résidence.

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

About the IEC
The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications
The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigendum or an amendment might have been published.

IEC publications search - webstore.iec.ch/advsearchform
The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee, …). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

IEC Customer Service Centre - webstore.iec.ch/csc
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

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

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

A propos de l'IEC
La Commission Electrotechnique Internationale (IEC) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications IEC
Le contenu technique des publications IEC est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Recherche de publications IEC - webstore.iec.ch/advsearchform
La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études, …). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

IEC Just Published - webstore.iec.ch/justpublished
Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et une fois par mois par email.

Service Clients - webstore.iec.ch/csc
Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: sales@iec.ch.

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

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

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

IEC 61784-3-2

Edition 4.0 2021-05

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

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

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

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

ICS 25.040.40; 35.100.05

ISBN 978-2-8322-9747-6

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

® Registered trademark of the International Electrotechnical Commission
Marque déposée de la Commission Electrotechnique Internationale

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

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

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

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

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

IECNORM.COM : Click to view the full PDF of 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

IECNORM.COM : Click to view the full PDF of 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

IECNORM.COM : Click to view the full PDF of 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

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

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

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

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

IECNORM.COM : Click to view the full PDF of 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

IECNORM.COM : Click to view the full PDF of 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

IECNORM.COM : Click to view the full PDF of 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.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

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

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

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

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

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

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

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

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

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

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available at www.iec.ch/members_experts/refdocs. 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.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

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

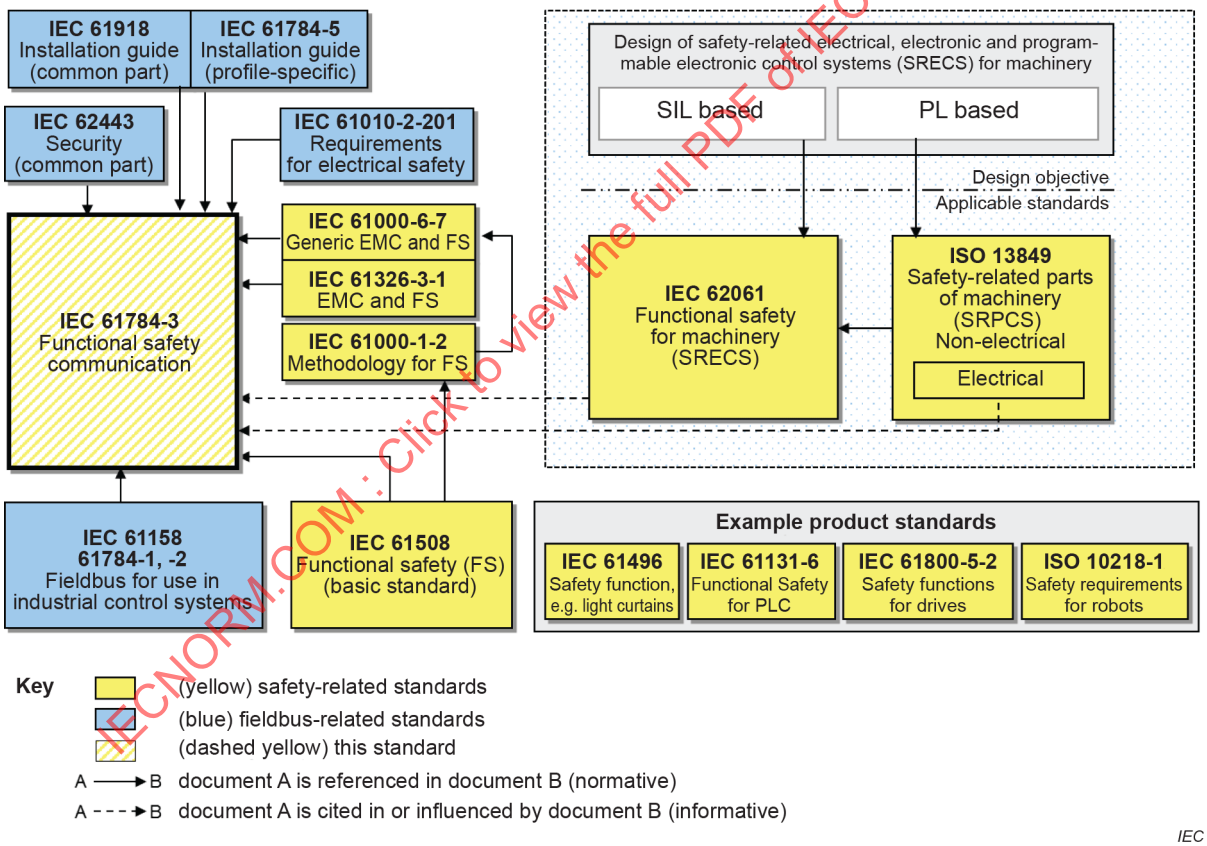
0 Introduction

0.1 General

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

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

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

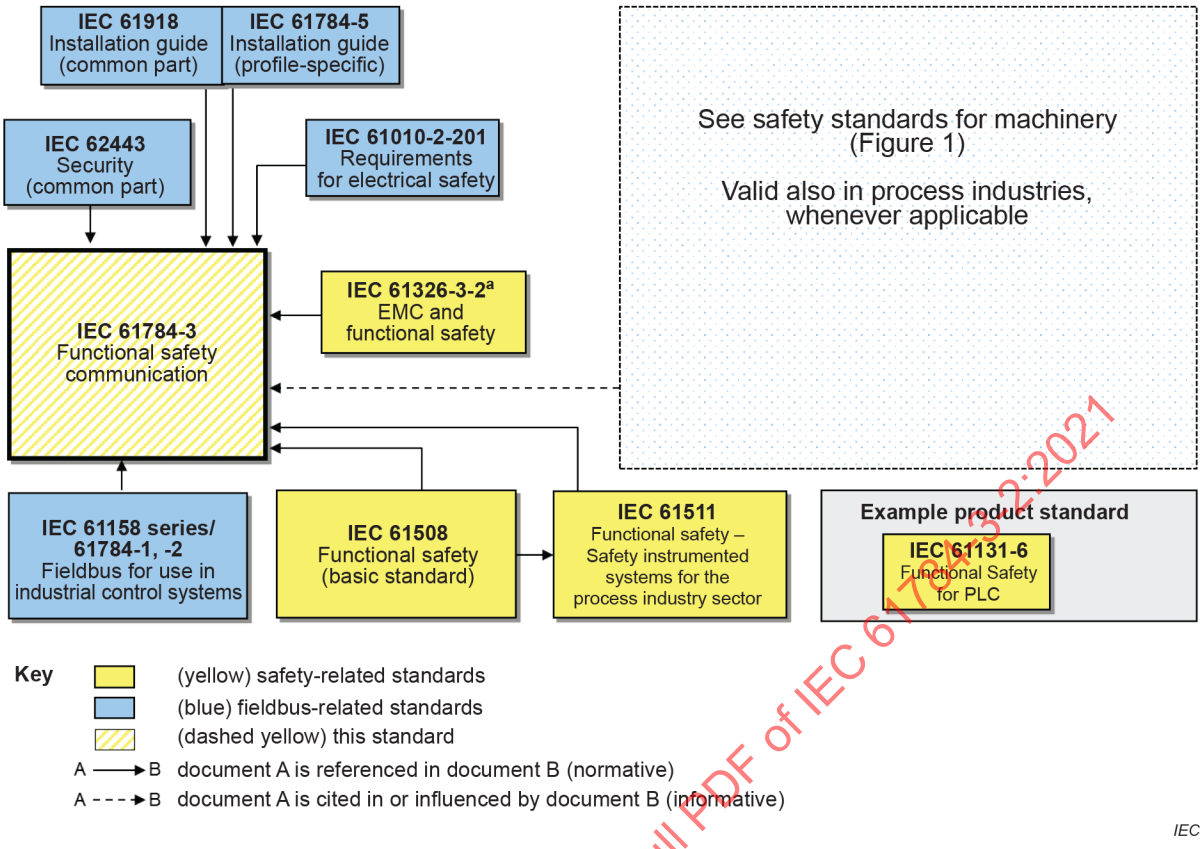


NOTE IEC 62061 specifies the relationship between PL (Category) and SIL.

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.

IECNORM.COM : Click to view the full PDF of 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.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

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.

IECNORM.COM : Click to view the full PDF of 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*

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

IECNORM.COM : Click to view the full PDF of 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

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

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]

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

2 Figures in square brackets refer to the bibliography.

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]

IECNORM.COM : Click to view the full PDF of 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]

IECNORM.COM : Click to view the full PDF of 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

IECNORM.COM : Click to view the full PDF of 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]

IECNORM.COM : Click to view the full PDF of 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]

IECNORM.COM : Click to view the full PDF of 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.

IECNORM.COM : Click to view the full PDF of 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.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

---

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).

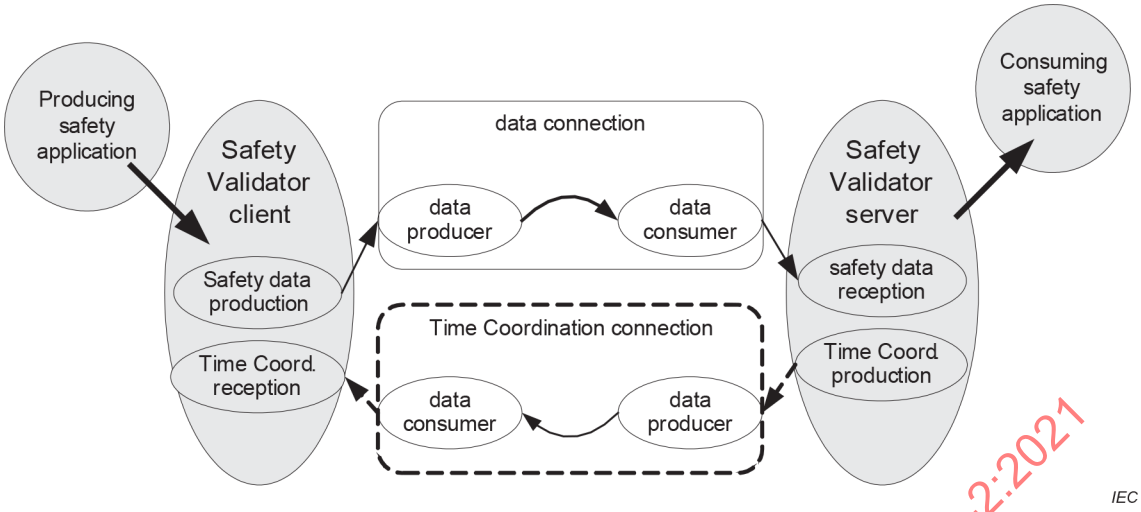


Figure 3 – Relationship of Safety Validators

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.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

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.

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.

IECNORM.COM : Click to view the full PDF of 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.

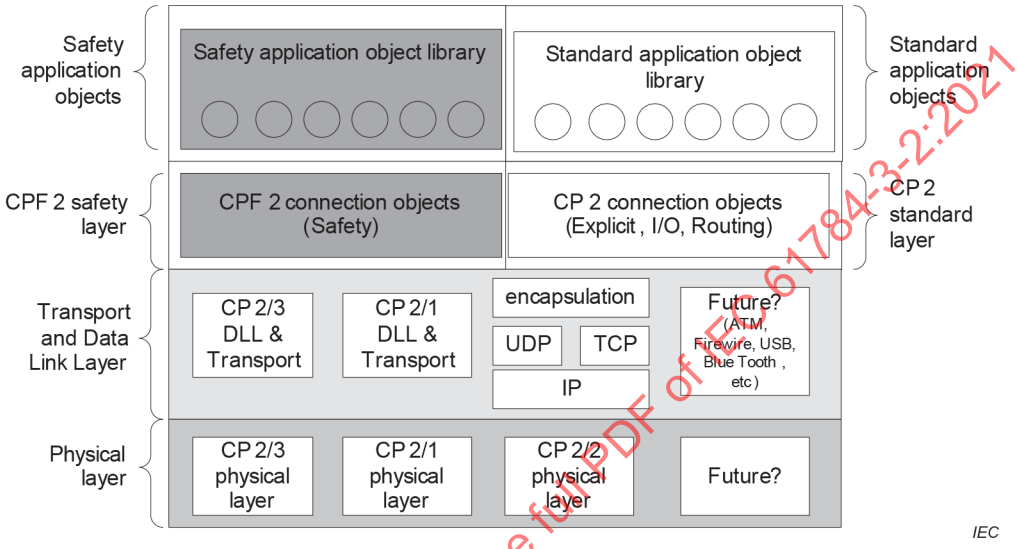


Figure 4 – Communication layers

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.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

---

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.

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 success count	UINT	Count of successful SafetyOpen requests issued from this node to another target
				SafetyOpen request failure count	UINT	Count of unsuccessful SafetyOpen requests issued from this node to another target
				SafetyClose request success count	UINT	Count of successful SafetyClose requests issued from this node to another target
				SafetyClose request failure count[b]	UINT	Count of unsuccessful SafetyClose requests issued from this node to another target
				SafetyOpen indication success count	UINT	Count of successful SafetyOpen requests issued from an external originator to this node
				SafetyOpen indication failure count[b]	UINT	Count of unsuccessful SafetyOpen requests issued from an external originator to this node
				SafetyClose indication success count	UINT	Count of successful SafetyClose requests issued from an external originator to this node
				SafetyClose indication failure count[b]	UINT	Count of unsuccessful SafetyClose requests issued from an external originator to this node

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

[b] Included in class attribute 8.

IECNORM.COM : Click to view the full PDF of 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.

IECNORM.COM : Click to view the full PDF of 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

IECNORM.COM : Click to view the full PDF of 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

IECNORM.COM : Click to view the full PDF of 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.

IECNORM.COM : Click to view the full PDF of 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

IECNORM.COM : Click to view the full PDF of 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)

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

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.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

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.

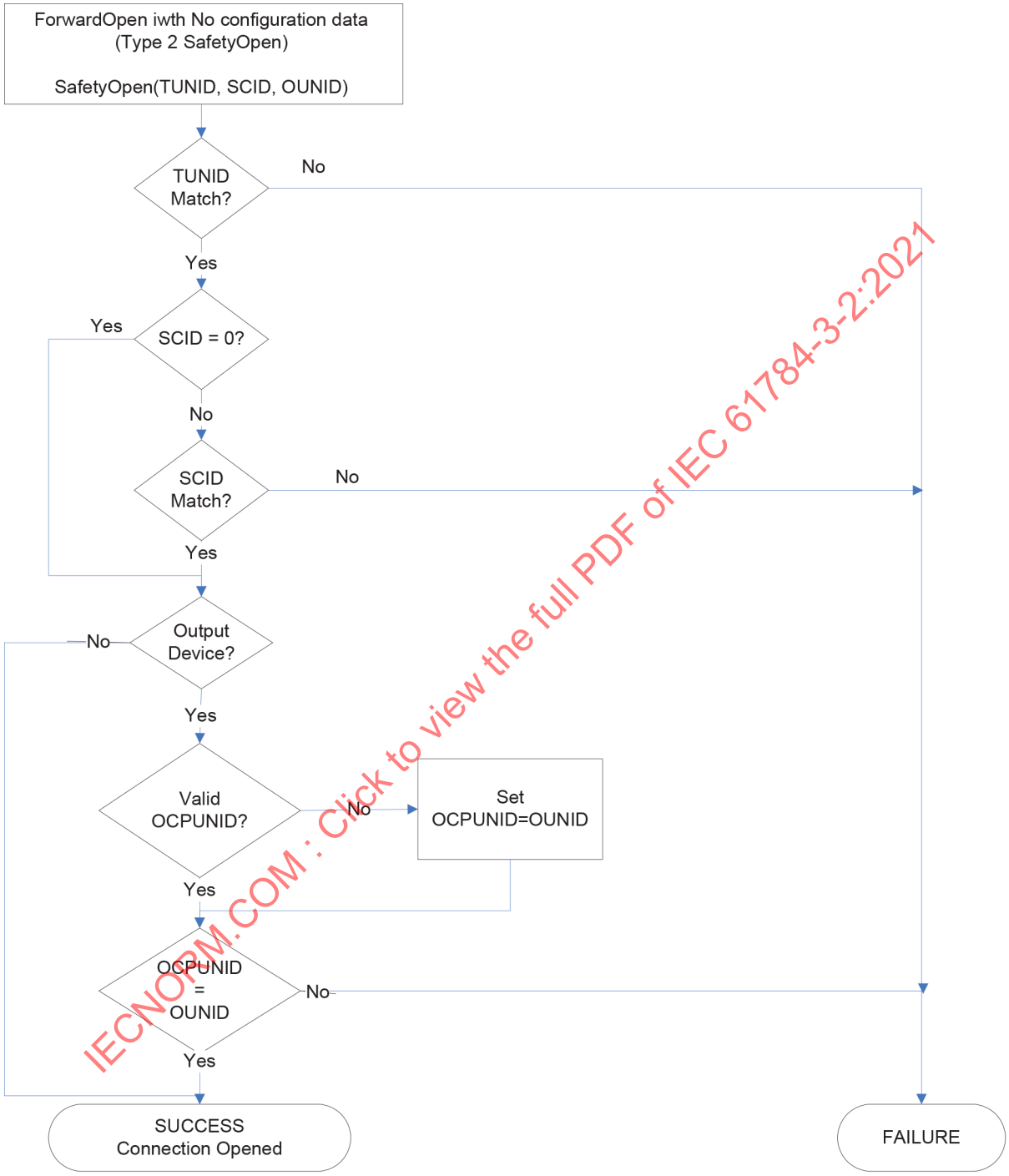
6.3.5 SafetyOpen processing flowcharts

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;

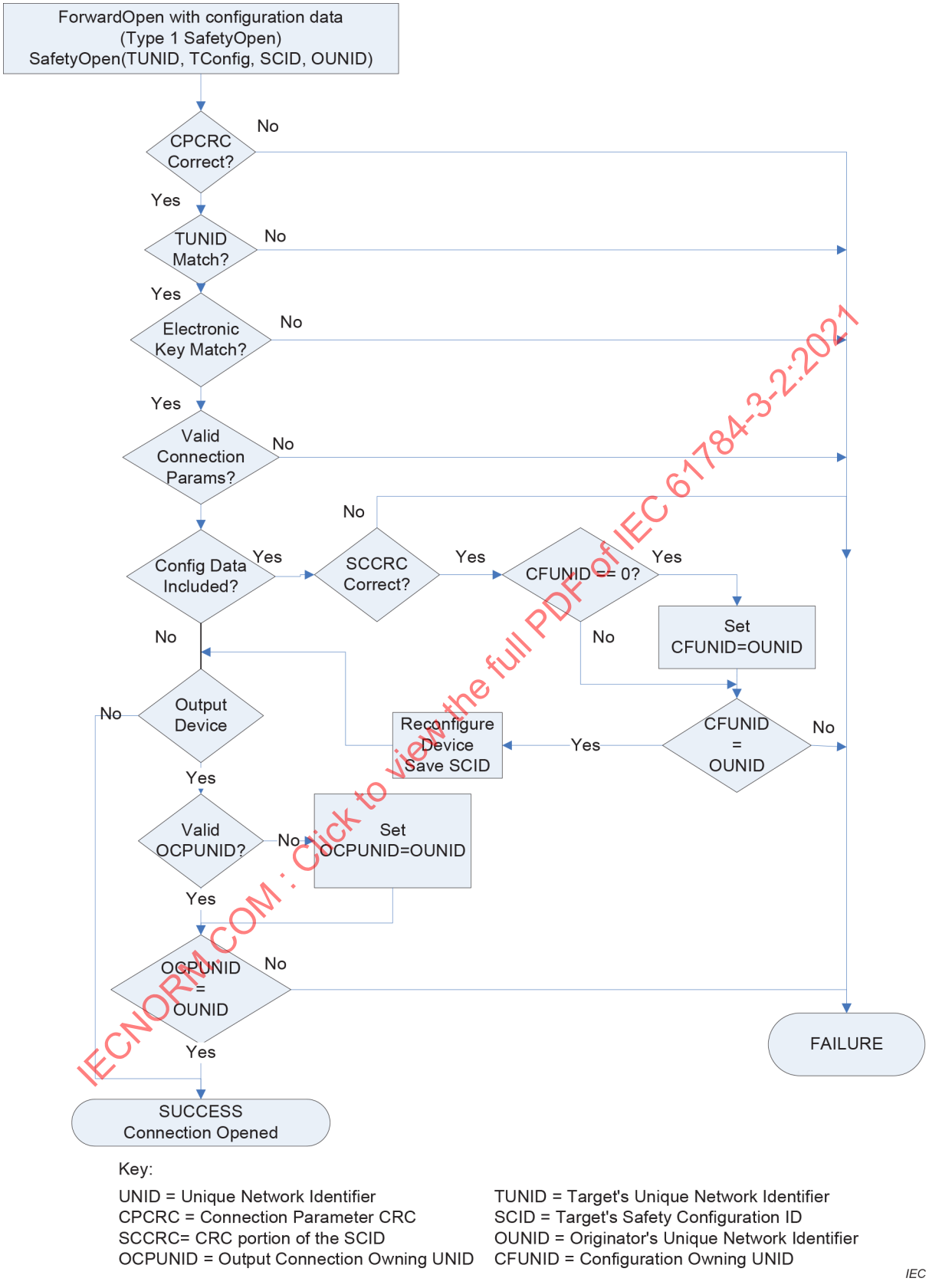
b) The target checks that the electronic key segment matches (see 6.3.7);

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



IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

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



IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

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

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

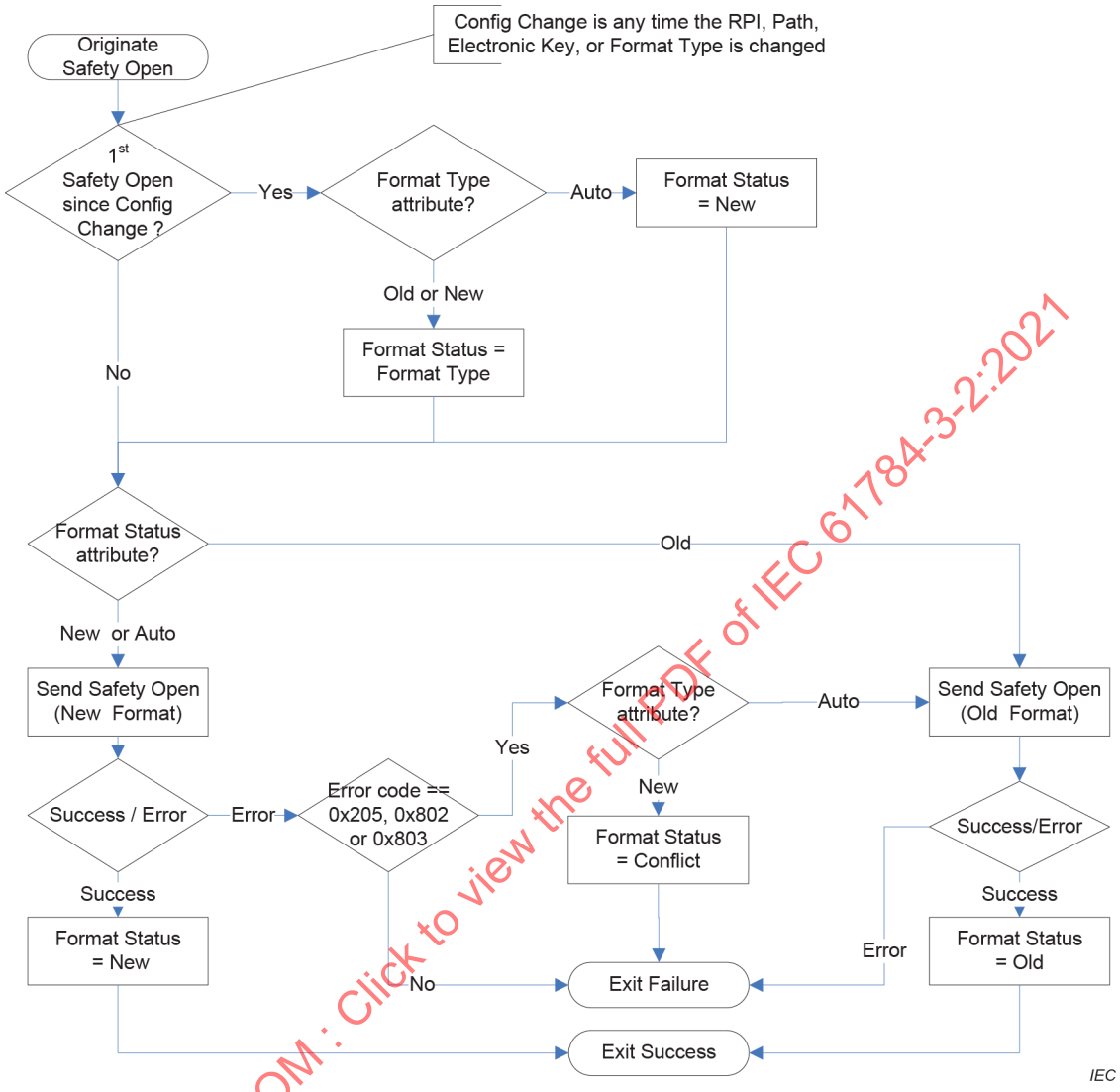


Figure 9 – Originator logic to determine which format to use

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

6.3.6 Checks required by Multipoint producers with existing connections

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

Table 9 – Multipoint producer parameter evaluation rules

Safety parameter	Producer evaluation rule if connection exists	Error response[a] (if appropriate)	
		General	Extended
Ping_Interval EPI Multiplier	Shall match existing P.I.E.M.	01_{hex}	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.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

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;

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

- [A, E, G] compressed format for output connections.

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

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

6.3.9.3 ANSI extended symbol segment application paths

Character strings are frequently used to provide access to user-defined process variables on devices that support them.

When a device supports production of the data of a safety process variable on a safety input connection, a single application path comprised of an ANSI Extended Symbol segment (see IEC 61158-6-2) shall be used to encode the string name of the safety process variable.

The following rules apply to ANSI Extended Symbol Segment application path construction.

- No configuration data may be sent since no configuration path may be specified.
- No input assembly definition is required since the data format for the process variable is user defined.
- The O-to-T connection is the Time Coordination connection.
- The T-to-O connection contains the safety process variable data. The EDS path format for the single application path is "SYMBOL_ANSI" (see IEC 61158-6-2 for more information) for Type 2a, 2b SafetyOpen connections.

6.3.10 Safety Validator connection types

The Safety Validator function, depending on the safety connection type provided in the SafetyOpen, will always require between 2-3 connection resources. The SafetyOpen contains the connection information to allow a target to set up these connections appropriately. This Subclause 6.3.10 will show how the connection types are determined by how the SafetyOpen shall be filled out.

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

The Safety Validator function can determine which connection resources will be required by looking at the parameter in the SafetyOpen. The various SafetyOpen parameters as well as the key parameters that the safety function will need to determine the types of connections are defined in Table 10 for connections with object instances and/or connection point application paths and in Table 11 for connections with an ANSI Extended Symbol Segment application path.

Connection object instances could be unavailable due to target identifier capacity or limitations;It is possible that unallocated connection identifiers are not available. Or the device could be lacking sufficient processing throughput to handle the additional connection; etc. Safety Connection objects require resources similar to standard I/O connections.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Table 10 – ForwardOpen setting options for safety connections with object-based application paths

O-to-T connection type	T-to-O connection type	Transport type/ trigger	App path 1	App path 2[a]	App path 3[a]	Max consumer number	Safety Validator connection type	Key decision factors	Target role
Point-to-point	Point-to-point	Applica-tion, Class 0, Client	Vendor defined Null Path [b]	Vendor defined Null Path	Safety Input App. object	1	Point-to-point Producer (Input)	2-point-to-point + Client	Producing connec-tion: Safety data Consumer connec-tion: Coordina-tion
Point-to-point	Point-to-point	Applica-tion, Class 0, Server	Vendor defined Null Path	Safety Output App. object	Vendor defined Null Path	1	Point-to-point Consumer (Output)	2- point-to-point + Server	Consu-ming connec-tion: Safety data Producing connec-tion: Coordina-tion
Point-to-point	Multipoint	Applica-tion, Class 0, Client	Vendor defined Null Path	Vendor defined Null Path	Safety Input App. object	2-15	Multipoint Producer CP 2/3	2 – Multipoint + 1 point-to-point + Client	Producing connec-tion: Safety data Producing connec-tion: Correction Consu-ming connec-tion: coordina-tion
Point-to-point	Multipoint	Applica-tion, Class 0, Client	Vendor defined Null Path	Vendor defined Null Path	Safety input app. object	2-15	Multipoint Producer CP 2/2	1 – Multipoint + 1 point-to-point + Client	Producing connec-tion: Safety data + correction Consu-ming connec-tion: Coordina-tion

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

O-to-T connection type	T-to-O connection type	Transport type/ trigger	App path 1	App path 2[a]	App path 3[a]	Max consumer number	Safety Validator connection type	Key decision factors	Target role
Multipoint	Point-to-point	Applica-tion, Class 0, Server	Vendor defined Null Path	Safety output app. object	Vendor defined Null Path	2-15	Multipoint Consumer CP 2/3	2 – Multipoint + 1 point-to-point + Server	Consu-ming connec-tion: Safety data Consuming connec-tion: Correction Producing connec-tion: coordina-tion
Multipoint	Point-to-point	Applica-tion, Class 0, Server	Vendor defined Null Path	Safety output app. object	Vendor defined Null Path	2-15	Multipoint Consumer CP 2/2	1 – Multipoint + 1 point-to-point + Server	Consu-ming conne-ction: Safety Data + correction Producing connec-tion: coordina-tion

[a] Input and Output with respect to the network.

[b] Devices configurable via EDS shall define an application Null Path in the EDS file.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Table 11 – ForwardOpen setting options for safety connections with ANSI Extended symbol segment application path

O-to-T connection type	T-to-O connection type	Transport type/ trigger	App path	Max consumer number	Safety Validator connection type	Key decision factors	Target role
Point-to-point	Point-to-point	Application, Class 0, Client	ANSI Extended Symbol Segment	1	Point-to-point Producer (Input)	2-point-to-point + Client	Producing connection: Safety data Consumer connection: Coordination
Point-to-point	Multipoint	Application, Class 0, Client	ANSI Extended Symbol Segment	2-15	Multipoint Producer CP 2/3	2 – Multipoint + 1 point-to-point + Client	Producing connection: Safety data Producing connection: Correction Consuming connection: coordination
Point-to-point	Multipoint	Application, Class 0, Client	Safety input app. object	2-15	Multipoint Producer CP 2/2	1 – Multipoint + 1 point-to-point + Client	Producing connection: Safety data + correction Consuming connection: Coordination

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Table 12 defines which network connection parameters to use for all three connections associated with each safety connection type.

Table 12 – Network connection parameters for safety connections

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

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

6.3.11 Application reply data in a successful SafetyOpen response

The format for a SafetyOpen response for Success is the same as the Forward_Open_Reply as defined in IEC 61158-6-2. The data return is defined in Table 13.

The target of a SafetyOpen shall return the data defined in Table 13 through Table 16 in the Application Reply field of the SafetyOpen response. The consumer number and PID reply data is only of significance when the originator is the consumer.

Table 13 – SafetyOpen target application reply (size: 10 octets)

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

When the Target of a connection is using the Extended Format on CP 2/2 or CP 16/3 links, it shall use the 14 octet EF SafetyOpen Target Application reply defined in Table 14.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Table 14 – EF CP 2/2 or CP 16/3 SafetyOpen target application reply (size: 14 octets)

Parameter Name	Data Type	Description
Consumer_Number	UINT	
PID/CID	STRUCT of:	Target Identifier used to generate a PID or CID seed value
Target Vendor Id	UINT	Target's Vendor Id
Target Device Serial Number	UDINT	Target's Device Serial Number
Target Connection Serial Number	UINT	Connection Serial Number Target assigned to the connection. The Safety Validator instance Id shall be used
Initial Time Stamp[a]	UINT	Used by Consumer to initialize Last_Time_Stamp_for_Rollover
Initial Rollover Value[a]	UINT	Used by Consumer to initialize TS_Rollover_Count

[a] Point-to-point producers echo back the values received in the SafetyOpen. Multipoint producers as well as point-to-point consumers respond with their internal values (e.g. Clock_Count_RC_Offset).

Table 15 – BF CP 2/3 SafetyOpen target application reply (size: 18 octets)

Parameter name	Data type	Description
Consumer_Number[a]	UINT	
PID/CID	STRUCT of:	Target Identifier used to generate a PID or CID seed value
Target Vendor Id	UINT	Target's Vendor Id
Target Device Serial Number	UDINT	Target's Device Serial Number
Target Connection Serial Number	UINT	Connection Serial Number Target assigned to the connection. The Safety Validator instance Id shall be used
Time_Correction_Connection_ID[a]	UDINT	Connection ID selected by the Target for the Time Correction connection. If chosen by the originator, then the value is echoed back
Time_Correction_API	UDINT	Returns same value received in the Request packet

[a] When a CP 2/3 Safety target receives a SafetyOpen that is not multipoint (thus no Time Correction connection is established) the Time_Correction_Connection_ID parameter shall be set to $FFFF_{hex}$. If the target is not a multipoint producer, the consumer number is set to $FFFF_{hex}$.

When the Target of a connection is using the Extended Format on CP 2/3, it shall use the 22 octet EF SafetyOpen Target Application reply defined in Table 16.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Table 16 – EF CP 2/3 SafetyOpen target application reply (size: 22 octets)

Parameter Name	Data Type	Description
Consumer_Number[a]	UINT	
PID/CID	STRUCT of:	Target Identifier used to generate a PID or CID seed value
Target Vendor Id	UINT	Target's Vendor Id
Target Device Serial Number	UDINT	Target's Device Serial Number
Target Connection Serial Number	UINT	Connection Serial Number Target assigned to the connection. The Safety Validator instance Id shall be used
Time_Correction_Connection_ID[a]	UDINT	Connection ID selected by the Target for the Time Correction connection. If chosen by the originator, then the value is echoed back
Time_Correction_API	UDINT	Returns same value received in the Request packet
Initial Time Stamp[b]	UINT	Used by Consumer to initialize Last_Time_Stamp_for_Rollover
Initial Rollover Value[b]	UINT	Used by Consumer to initialize TS_Rollover_Count

[a] When a CP 2/3 Safety target receives a SafetyOpen that is not multipoint (thus no Time Correction connection is established) the Time_Correction_Connection_ID parameter shall be set to $FFFF_{hex}$. If the target is not a multipoint producer, the consumer number is set to $FFFF_{hex}$.

[b] Point-to-point producers echo back the values received in the SafetyOpen. Multipoint producers as well as point-to-point consumers respond with their internal values (e.g. Clock_Count_RC_Offset).

6.3.12 Unsuccessful SafetyOpen response

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

Table 17 defines new extended error codes for safety and shows the extended definition of existing error codes.

Table 17 – New and extended error codes for safety

General status	Extended status	Explanation
01_{hex}	0105_{hex}	Ownership conflict or OUNID mismatch. The configuration is already owned by another originator
01_{hex}	0106_{hex}	Ownership conflict or OUNID mismatch. The output connection was already owned by another originator
01_{hex}	0205_{hex}	Parameter Error in Unconnected Send service or Parameter Error in SafetyOpen or SafetyClose
01_{hex}	0801_{hex}	Incompatible Multipoint RPI. An existing connection has been established at a different RPI
01_{hex}	0802_{hex}	Invalid Safety Connection size
01_{hex}	0803_{hex}	Invalid Safety Connection format
01_{hex}	0804_{hex}	Invalid Time Correction Connection Parameters
01_{hex}	0805_{hex}	Invalid Ping Interval EPI Multiplier
01_{hex}	0806_{hex}	Time Coordination Msg Min Multiplier
01_{hex}	0807_{hex}	Network Time Expectation Multiplier

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

General status	Extended status	Explanation
01_{hex}	0808_{hex}	Timeout Multiplier
01_{hex}	0809_{hex}	Invalid Max Consumer Number
01_{hex}	$080A_{hex}$	Invalid CPCRC
01_{hex}	$080B_{hex}$	Time Correction Connection Id invalid
01_{hex}	$080C_{hex}$	SCID Mismatch. The SCID was non-zero and did not match the value in the target
01_{hex}	$080D_{hex}$	TUNID not set. Device is out-of-box and TUNID has not been set, so connections are not allowed
01_{hex}	$080E_{hex}$	TUNID Mismatch. The TUNID provided does not match. The message was likely routed to this node in error
01_{hex}	$080F_{hex}$	Configuration operation not allowed
01_{hex}	0815_{hex}	Incompatible Multipoint Ping Interval EPI Multiplier. An existing connection has been established with a different Ping Interval EPI Multiplier.
01_{hex}	0816_{hex}	Incompatible Multipoint Max Consumer Number. An existing connection has been established with a different Max Consumer Number.
01_{hex}	0817_{hex}	Incompatible Multipoint Safety Network Segment Type. An existing connection has been established with a different Safety Network Segment Type.

[a] Reserved extended status code ranges for FSCP 2/1 are defined as 0801_{hex} through $080F_{hex}$ and 0815_{hex} through 0834_{hex} (see CPF 2).

Event/Error Matrix Table 18 provides guidance for which error codes to use for possible errors detected in processing a SafetyOpen. This is not intended to be an exhaustive list.

Table 18 – SafetyOpen error event guidance table

Event	Error type	General status	Extended status
The target device received a SafetyOpen request in states of Safety Supervisor object other than Idle and Executing	Configuration operation not allowed	01_{hex}	$080F_{hex}$
	Device not configured	01_{hex}	110_{hex}
Safety Connection Type (name) Invalid	Safety parameter error – Invalid Connection Type	01_{hex}	315_{hex}
Safety Connection Size Invalid	Safety parameter error – Invalid Safety Connection Size	01_{hex}	0802_{hex}
Safety Connection Format Invalid	Safety parameter error – Invalid Safety Connection Format	01_{hex}	0803_{hex}
Time Correction Connection Parameters Invalid	Safety parameter error – Invalid Time Correction Connection Parameters	01_{hex}	0804_{hex}
Ping Interval EPI Multiplier was out of the range	Safety parameter error – Invalid Ping Interval EPI Multiplier	01_{hex}	0805_{hex}
Time Coordination Message Min Multiplier was out of the range	Safety parameter error – Time Coordination Msg Min Multiplier	01_{hex}	0806_{hex}
Time Expectation Multiplier was out of the range	Safety parameter error – Time Expectation Multiplier	01_{hex}	0807_{hex}
Timeout Multiplier was out of the range	Safety parameter error – Timeout Multiplier	01_{hex}	0808_{hex}

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Event	Error type	General status	Extended status
Max Consumer Number not within the limits in Multipoint Producer	Safety parameter error – Invalid Max Consumer Number	01_{hex}	0809_{hex}
CPCRC value in SafetyOpen and calculated CPCRC value	Safety parameter error – Invalid CPCRC	01_{hex}	$080A_{hex}$
Time Correction Connection Id Invalid	Safety parameter error – Time Correction Connection Id invalid	01_{hex}	$080B_{hex}$
RPI requested is incompatible with previously established multipoint connections	Incompatible multipoint RPI	01_{hex}	801_{hex}
O-to-T RPI, T-to-O RPI, or Time Correction RPI is not supported	RPI not supported	01_{hex}	0111_{hex}
All Safety Validator Instances are being used	Connection Manager or connection object cannot support any more connections	01_{hex}	0113_{hex}

6.3.13 ForwardClose for safety

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

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

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

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

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

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

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

6.4 Identity object

6.4.1 General

Class Code: 01_{hex}

This Subclause 6.4 describes changes to the Identity object to support safety.

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

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

6.4.2 Changes to common services

Table 19 defines the services of the Identity object that require updates.

Table 19 – Identity object common service changes

Service code	Need in implementation		Service name	Description of service
	Class	Instance		
05_{hex}	n/a	Optional[a]	Reset	Optionally invokes the Type 0 Reset Service for the device

[a] Conditional – Safety devices are only allowed to optionally support the Type 0 Identity Reset service when there are no established Safety or Standard I/O connections. If I/O connections are established, the device shall reply with "Device State" error. This service, when executed shall affect the entire device. When a device supports Reset Type 0, all other Identity Reset Types shall not be supported and shall reply to any requests with an "Invalid Parameter (0x20)" error.

6.4.3 Extensions for CP 16/3 devices

Extensions of the Identity object for CP 16/3 devices are specified in Table 20.

Some of the attributes of the object extensions for CP 16/3 refer CP 16/3 IDNs (Identification Numbers) using the CP 16/3 nomenclature, e.g. S-0-1300. These CP 16/3 IDNs are specified in full detail in IEC 61158-4-19.

Table 20 – Identity object extensions for CP 16/3 devices

Attrib ID	Need in implem.	Access rule	Name	Data type	Description of attribute	Semantics of value
1	Required	Get	Vendor ID	See IEC 61158-5-2		
2	Required	Get	Device Type	See IEC 61158-5-2		
3	Required	Get	Product Code	See IEC 61158-5-2		
4	Required	Get	Revision	See IEC 61158-5-2		
5	Required	Get	Status	See IEC 61158-5-2		
6	Required	Get	Serial Number	See IEC 61158-5-2		
7	Required	Get	Product Name	See IEC 61158-5-2		First 32 characters of CP 16/3 S-0-1300.x.4
8-18	Optional	See IEC 61158-5-2				

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

6.5 Link objects

6.5.1 DeviceNet object changes

6.5.1.1 Additional attribute for safety

Class Code: 03_{hex}

This Subclause 6.5.1 defines the changes and additions required of the DeviceNet object to support safety. An attribute shall be added to allow the Safety Network Number (SNN) to be read. The definition for this attribute is defined in Table 21.

Table 21 – New DeviceNet object instance attribute

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

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

6.5.1.2 Quick Connect restriction for safety

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

6.5.2 TCP/IP Interface object changes

Class Code: $F5_{hex}$

This Subclause 6.5.2 defines the changes and additions required of the TCP/IP Interface object to support safety. An attribute shall be added to allow the Safety Network Number (SNN) to be read. The definition for this attribute is defined in Table 22.

Table 22 – New TCP/IP Interface object instance attribute

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

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

6.5.3 SERCOS III Link object

6.5.3.1 General

Class Code: $4C_{hex}$

This Subclause 6.5.3 provides information on the SERCOS III link object. The SERCOS III Link object shall be present in all products that support FSCP 2/1 on CP 16/3. If multiple CP 16/3 links exist in a device, multiple instances of the SERCOS III Link Object shall be used. Attribute 1 allows the Safety Network Number (SNN) to be read.

6.5.3.2 Class attributes

SERCOS III Link object class attributes are defined in Table 23.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Table 23 – SERCOS III Link object class attributes

Attrib ID	Need in implem.	Access rule	Name	Data type	Description of attribute	Semantics of value
1	This attribute is optional and is described in IEC 61158-5-2					
2	Conditional[a]	Get	Max Instance	UINT	Maximum instance number of an object currently created in this class level of the device	The largest instance number of a created object at this class hierarchy level.
3 thru 7	This attribute is optional and is described in IEC 61158-5-2					

[a] If the device has multiple CP 16/3 interface links, then this attribute is required to be supported

6.5.3.3 Instance Attributes

SERCOS III Link object instance attributes are defined in Table 24.

Table 24 – SERCOS III Link object instance attributes

Attrib ID	Need in implem.	Access rule	Name	Data type	Description of attribute	Semantics of value
1	Required	Get	Safety Network Number	6 OCTETS	System-wide unique number for the subnet this device resides on	Attribute shall contain the SNN portion of the TUNID in the Safety Supervisor. See 8.2 for further definition of this attribute
2	Optional	Get	Communication Cycle Time	UDINT	CP 16/3 S-0-1002	
3	Optional	Get	Interface Status	WORD	CP 16/3 S-0-1014	
4	Optional	Get	Error Counter MST-P/S	UINT	CP 16/3 S-0-1028	
5	Optional	Get	Error counter Port1 and Port2	Struct of:	CP 16/3 S-0-1035	
			Error counter Port1	UINT		
			Error counter Port2	UINT		
6	Optional	Get	SERCOS ® Address	UINT	CP 16/3 S-0-1040	

6.5.3.4 Common services

The definition for the SERCOS III Link Object common services is defined in Table 25.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Table 25 – SERCOS III Link Object Common Services

Service code	Need in implementation		Service name	Description of service
	Class	Instance		
$0E_{hex}$	Conditional[a]	Required	Get_Attribute_Single	Used top read an object attribute
[a] Conditional – Required if any class attributes are supported.				

6.6 Safety Supervisor object

6.6.1 General

Class Code: 39_{hex}

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

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

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

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

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

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

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

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

6.6.2 Safety Supervisor class attributes

The Class attributes used by the Safety Supervisor are defined in Table 26.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Table 26 – Safety Supervisor class attributes

Attribute ID	Need in implementation	Access rule	Name	Date type	Description of attribute
1 – 96	These class attributes are described in IEC 61158-6-2				
97-98	Reserved by FSCP 2/1 for future use				
99	Conditional[a]	Get	Subclass	UINT	Identifies a subset of additional class attributes, services, and behaviors

[a] If the value of Subclass is 00 which identifies "no subclass", then this attribute should be in implementation, otherwise, this attribute shall be in the implementation.

6.6.3 Subclasses

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

6.6.4 Safety Supervisor instance attributes

The instance attributes for the Safet Supervisor are defined in Table 27.

Table 27 – Safety Supervisor instance attributes

Attr ID	Need in implementation	Access rule	NV	Name	Date type	Description of attribute
1	Optional	Get	NV	Number of Attributes	USINT	Number of Attributes supported by the object instance
2	Optional	Get	NV	Attribute List	ARRAY of USINT	List of attributes supported by the object instance
3	Reserved					
4	Reserved					
5	Optional	Get	NV	Manufacturer Name	Short String	ASCII Text, Max. 20 characters, see 6.6.5.1
6	Optional	Get	NV	Manufacturer Model Number	Short String	ASCII Text, Max. 20 characters, Manufacturer specified
7	Optional	Get	NV	Software Revision Level	Short String	ASCII Text, Max. 6 characters, see 6.6.5.2
8	Optional	Get	NV	Hardware Revision Level	Short String	ASCII Text, Max. 6 characters, see 6.6.5.3
9	Optional	Get	NV	Manufacturer Serial Number	Short String	ASCII Text, Max. 30 characters, manufacturer specified, see 6.6.5.4
10	Optional	Get	NV	Device Configuration	Short String	ASCII Text, Max. 50 Characters, manufacturer specified. Optional additional information about the device configuration
11	Required	Get	V	Device Status	USINT	See 6.6.5.5
12	Required	Get	V	Exception Status	SWORD	See 6.6.5.6

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Attr ID	Need in implementation	Access rule	NV	Name	Date type	Description of attribute
13	Conditional based on Exception Status Bit 7	Get	V	Exception Detail Alarm	STRUCT of:	A Structure of 3 structures containing a bit-mapped representation of the alarm detail
				Common Exception Detail	STRUCT of:	
				Size	USINT	Number of Common Exception Detail Octets
	Conditional based on Size [f]			Detail	ARRAY of:	See 6.6.5.7
				Detail	SWORD	See 6.6.5.7
				Device Exception Detail	STRUCT of:	
				Size	USINT	Number of Device Exception Detail Octets
	Conditional based on Size [f]			Detail	ARRAY of:	Manufacturer specified
				Detail n	SWORD	Manufacturer specified
				Manufacturer Exception Detail	STRUCT of:	
				Size	USINT	Number of Manufacturer Excpetoin Detail Octets
				Detail	ARRAY of:	Manufacturer specified
				Detail n	SWORD	Manufacturer specified
14	Conditional Based on Exception Status Bit 7	Get	V	Exception Detail Warning	STRUCT of:	A Structure of 3 structures containing a bit-mapped representation of the warning detail
				Common Exception Detail	STRUCT of:	
				Size	USINT	Number of Common Detail octets
	Conditional based on Size [f]			Detail	ARRAY of:	See 6.6.5.8
				Detail n	SWORD	See 6.6.5.8
				Device Exception Detail	STRUCT of:	
				Size	USINT	Number of Device Detail octets
	Conditional based on Size [f]			Detail	ARRAY of:	Manufacturer specified
				Detail n	SWORD	Manufacturer specified
				Manufacturer Exception Detail	STRUCT of:	
				Size	USINT	Number of Manufacturer Detail octets
				Detail	ARRAY of:	Manufacturer specified
				Detail n	SWORD	Manufacturer specified

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Attr ID	Need in implementation	Access rule	NV	Name	Date type	Description of attribute
15	Conditional [e]	Set	NV	Alarm Enable	BOOL	See 6.6.5.12
16	Conditional [e]	Set	NV	Warning Enable	BOOL	See 6.6.5.12
17	Optional	Set	V/NV [a]	Time	DATE_AND_TIME	The value of the Device's internal real-time clock
18	Conditional [g]	Get	NV	Clock Power Cycle Behavior	USINT	Describes the behavior of the device's internal real-time clock (the "Time" attribute) during a power cycle: 0 = [default] clock always resets during power cycle 1 = clock value is stored in nonvolatile memory at power down 2 = clock is battery-backed and runs without device power 3-255 = reserved
19	Optional	Get	NV	Last Maintenance Date	DATE	The date on which the device was last serviced
20	Optional	Get	NV	Next Scheduled Maintenance Date	DATE	The date on which it is recommended that the device next be serviced
21	Optional	Get	NV	Scheduled Maintenance Expiration Timer	INT	See 6.6.5.14
22	Conditional [h]	Set	NV	Scheduled Maintenance Expiration Warning Enable	BOOL	See 6.6.5.15
23	Optional	Get	NV	Run Hours	UDINT	An indication of the number of hours that the device has had power applied
24	Conditional [c]	Set [i]	NV	Configuration Lock	BOOL	Marks the device configuration contained within as Verified and locked, or alternatively as unverified, unlocked, and changeable
25	Conditional [c]	Get	NV	Configuration UNID	10 octets	CFUNID – Identifies the owner of a Device Configuration: All FF_{hex} = Tool-only configuration. 0 = un-owned, accept any owner
26	Required	Get	NV	Safety Configuration Identifier	10 octets	The SCID is comprised of the Safety Configuration CRC + Safety Configuration Time Stamp. This is the signature for the Configuration
27	Conditional [j]	Get	NV	Target UNID	10 octets	The current UNID of the device

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Attr ID	Need in implementation	Access rule	NV	Name	Date type	Description of attribute
28	Conditional[d]	Get	NV	Output Connection Point Owners		
				Number of Array Entries	UINT	Number of OCPUNID STRUCT entries
				Output Owners	ARRAY of STRUCT	
				OCPUNID	10 octets	The owner UNID for the output resource. 0 = un-owned, accept any owner (default)
				ePath Size	USINT	Path size, number of octets
				Application Resource	Packed ePath	The path to owned resource (i.e. 20 04 24 01 – Assembly class, instance 1)
29	Conditional [k]	Get	V	Proposed TUNID	10 octets	The UNID value that an originator is attempting to set in the device
30	Conditional [j]	Get	NV	Target UNID List	STRUCT of	
				Number of Target UNIDs	USINT	Number of Target UNID list entries
				Target UNIDs	ARRAY of STRUCT	List of (Port Number, Target UNID) pairs
				Port Number	UINT	See IEC 61158-4-2:2019, 7.11.4.3
				Target UNID	10 OCTETS	Target UNID associated with a specific CIP Port Number
31	Conditional [k]	Get	V	Proposed UNID List	STRUCT of	
				Number of Proposed TUNIDs	USINT	Number of Proposed Target UNID list entries
				Proposed TUNIDs	ARRAY of STRUCT	List of (Port Number, Proposed Target UNID) pairs
				Port Number	UINT	See IEC 61158-4-2:2019, 7.11.4.3
				Proposed TUNID	10 OCTETS	Proposed Target UNID associated with a specific CIP Port Number
97-98	Reserved by FSCP 2/1 for Future Use					
99	Conditional [b]	Get	NV	Subclass	UINT	Identifies a subset of additional instance attributes, services, and behaviors

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

[a] The nonvolatile behavior of the Time attribute is conditional: Attribute 17 is NV if Attribute 18 = 1, otherwise it is V.

[b] If the value of Subclass is 00 which identifies "no subclass", then this attribute should be in implementation, otherwise, this attribute shall be in implementation.

[c] Safety devices which support the SNCT interface (i.e. not configured by the SafetyOpen or some vendor specific means) shall support this attribute.

[d] Conditional – the Output Connection Owner attribute shall be supported for all safety output assemblies.

[e] Conditional – Required for FSCP 2/1 devices, but optional for FSCP 2/1 on CP 16/3 devices.

[f] "Conditional based on Size" means that the exception detail is present when the size is greater than zero.

[g] Required if Time (Attribute 17) is supported.

[h] Required if Scheduled Maintenance Expiration Time (Attribute 21) is supported.

[i] Set only by "Configuration Lock/Unlock" service.

[j] Single safety port devices shall support Attribute 27 (Target UNID). Multiple safety port devices shall only support Attribute 40 (Target UNID List).

[k] Single safety port devices that support the SNCT shall support Attribute 29 (Proposed TUNID) unless they are configured by vendor specific means. Multiple safety port devices that support the SNCT shall only support Attribute 31 (Proposed TUNID List) unless they are configured by vendor specific means.

6.6.5 Semantics

6.6.5.1 Manufacturer name

The Manufacturer Name attribute identifies the manufacturer of the device.

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

6.6.5.2 Software revision level

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

6.6.5.3 Hardware revision level

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

6.6.5.4 Manufacturer's serial number

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

6.6.5.5 Device status

This attribute represents the current state of the device. Its value changes as the state of the device changes. The Device status attribute state values are defined in Table 28.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Table 28 – Device status attribute state values

Attribute value	State
0	Undefined
1	Self-Testing
2	Idle
3	Self-Test exception
4	Executing
5	Abort
6	Critical Fault
7	Configuring
8	Waiting for TUNID
9-50	Reserved by FSCP 2/1
51	Waiting for TUNID with Torque Permitted [a]
52	Executing with Torque Permitted[a]
53-99	Device specific
100-255	Vendor specific

[a] Only allowed and defined in an appropriate device profile specification.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

6.6.5.6 Exception status

A single octet attribute whose value indicates that the status of the alarms and warnings for the device. This indication may be provided in one of two methods: Basic or Expanded.

For the Basic Method, bit seven of the Exception Status attribute is set to zero; all exceptions are reported exclusively through communication of this Exception Status attribute. The format of bits zero to six in this mode is device specific; the format may be further specified in an appropriate device profile specification; if it is not specified, then the format of bits zero to six is equivalent to that specified for the expanded method.

For the Expanded Method, bit seven of Exception Status attribute is set to one; exceptions are reported through the communication of this Exception Status attribute, formatted as specified in Table 29. In addition, the Exception Detail attributes are supported. The Exception Status bits are determined by a logical "OR" of the related Exception Detail bits, as indicated.

Table 29 – Exception status attribute format

Bit	Exception status bit map, Bit 7 Set to 0 Function	Exception status bit map, Bit 7 set to 1 Function
0	Device Specific definition (see Device Profile)	ALARM/Device-common[a]
1		ALARM/Device-specific
2		ALARM/Manufacturer-specific
3		Reserved – set to 0
4		WARNING/device-common[a]
5		WARNING/device-specific
6		WARNING/manufacturer-specific
7	0 = Basic Method	1 = Expanded Method

[a] The alarm or warning is not specific to the device type or device type manufacturer.

6.6.5.7 Exception detail alarm and exception detail warning

The formats of these two attributes are identical. Therefore, they are described together here.

Attributes that relate the detailed status of the alarms or warnings are associated with the device. Each attribute is a structure containing three members; these three members respectively relate the detailed status of exceptions that are common (i.e., not device-specific), device-specific but not manufacturer-specific, and manufacturer-specific. The common detail is defined in 6.6.5.8 and 6.6.5.9. The device-specific detail is defined in the appropriate Device Profile. The manufacturer- specific detail is defined by the manufacturer. A SIZE value of zero indicates that no detail is defined for the associated exception detail structure.

Each of the three structure members is defined as a structure containing an ordered list (i.e., array) of OCTETS of length SIZE, and an unsigned integer whose value is SIZE. Each of the octets in each array has a specific mapping. This mapping is formatted as 8 bits representing 8 independent conditions, whereas a value of 1 indicates that the condition is set (or present), and a value of 0 indicates that the condition is cleared (or not present). If a device does not support an exception detail, the corresponding bit is never set. The bitmaps for alarms and warnings in the corresponding attributes are structured in parallel so that a condition may have either alarm or warning set depending on severity. If a condition inherently cannot be both alarm and warning, then the parallel bit position corresponding to the other state shall remain "0".

The existence of an exception detail variable structure is dependent on the value of the Exception Status Attribute; the existence of an exception detail variable structure is only required if bit seven of the Exception Status attribute is set to 1 (indicating Expanded method reporting) and the bit (among bits zero to six) of the Exception Status attribute corresponding to the particular exception type is also set to 1.

6.6.5.8 Common exception detail

This structure relates exception conditions (i.e., alarms or warnings) which are common to all devices. The Detail element of the structure is an ordered list (i.e., array) of octets of length SIZE which is the value of the structure element Size. For each octet in the Detail field, all bits which are not identified are reserved for future standardization.

The first octet in this attribute is CommonExceptionDetail[0]. Additional exception details, if provided, are named CommonExceptionDetail[1], CommonExceptionDetail[SIZE]. The specific exception associated with each of the bitmaps is given in Table 30. The SIZE for this revision is two (2). The criteria details for each exception condition are outside the scope of this document.

6.6.5.9 Common exception detail attribute values

Table 30 – Common exception detail attribute values

Common Exception Detail [0] [a]	Common Exception Detail [1] [a]
Internal diagnostic exception	power supply over current
Microprocessor exception	reserved power supply
EPROM exception	power supply output voltage
EEPROM exception	power supply input voltage
RAM exception	scheduled maintenance due
Reserved	notify manufacturer
Internal real-time exception	reset exception
Reserved	Reserved

[a] If a device does not support an exception detail, the corresponding bit is never set.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

6.6.5.10 Device exception detail

This structure, similar in form to Common Exception Detail, relates exception conditions which are specific to individual devices on the network and are defined in their respective device profiles. The Detail element of the structure is an ordered list (i.e., array) of octets of length SIZE which is the value of the structure element size. For a detailed description of this attribute, consult the appropriate specific device profile.

6.6.5.11 Manufacturer exception detail

This structure (see Table 31), similar in form to Common Exception Detail, relates exception conditions which are specific to the manufacturers of individual devices on the network and are defined by them in their product documentation. The Detail element of the structure is an ordered list (i.e., array) of octets of length SIZE which is the value of the structure element Size. For a detailed description of this attribute, consult the appropriate specific device manufacturer documentation.

Table 31 – Exception detail format summary

Detail component	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Common exception detail size	0	0	0	0	0	0	0	0
Common exception detail 0	Res.	Real-time fault	Res.	Data memory	Non-volatile memory	Code memory	Micro-processor	Diagnostic
Common exception detail 1	Res.	Reset exception	Notify vendor	Scheduled maint. due	PS input voltage	PS output voltage	Res.	PS over current
Device exception detail size	TBD[a]	TBD[a]	TBD[a]	TBD[a]	TBD[a]	TBD[a]	TBD[a]	TBD[a]
Device exception detail 0	--	--	--	--	--	--	--	--
Device exception detail n	--	--	--	--	--	--	--	--
Manufacturer exception detail size	TBD[a]	TBD[a]	TBD[a]	TBD[a]	TBD[a]	TBD[a]	TBD[a]	TBD[a]
Manufacturer detail 0	--	--	--	--	--	--	--	--
Manufacturer detail n	--	--	--	--	--	--	--	--

[a] Consult the appropriate specific device manufacturer documentation for complete defintion.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

6.6.5.12 Alarm enable and warning enable

These Boolean attributes are used to enable (1) or disable (0) the Safety Supervisor object's process of setting Exception bits. When disabled, corresponding bits are never set; and, if they were set, disabling clears them. Also, alarm and warning states are not retained; when enabled, bits shall be set only if the corresponding condition is true.

The default state for these Enable attributes is enabled (1).

6.6.5.13 Time

This optional attribute represents the value of the time and date as maintained by the device's real-time clock with a resolution of one millisecond.

The default value for the Time attribute is zero (0), corresponding to 00:00:00, 1970-01-01.

6.6.5.14 Scheduled maintenance expiration timer

This attribute, with a resolution of one hour, is used to cause a warning which indicates that a device calibration is due. A Safety Supervisor timer decrements this attribute once per hour while power is applied. When the attribute is no longer positive and the Scheduled Maintenance Expiration Warning Enable attribute is set to enabled, a Scheduled Maintenance Expiration Warning condition is generated. This causes the Scheduled Maintenance Due Warning bit to be set.

The Scheduled Maintenance Expiration Timer attribute, when implemented, shall not wrap; when the attribute reaches its most negative value, it no longer decrements. The Scheduled Maintenance Expiration Timer, when implemented, shall continue to decrement irrespective of the state of the Scheduled Maintenance Expiration Warning Enable attribute. The Scheduled Maintenance Expiration Timer, when implemented, shall be maintained in nonvolatile memory.

6.6.5.15 Scheduled maintenance expiration warning enable

This Boolean attribute is used to enable (1) or disable (0) the Safety Supervisor object's process of setting the Scheduled Maintenance Due Exception bit. When disabled, the corresponding bit is never set; and, if it was set, disabling clears it. When enabled, the bit shall be set only if the corresponding condition is true.

The default state for this Enable attribute is enabled (1).

6.6.5.16 Configuration lock

The Configuration Lock attribute, when implemented with the SNCT interface, shall be used to mark the device configuration as verified and to lock down the configuration; 0 = Unlocked (unverified and changeable), 1 = Locked (verified and not changeable).

The default value for the Configuration Lock attribute is 0 = unlocked. Its primary use is for safety devices that are configured by the SNCT (i.e. not configured by the SafetyOpen). After the tool has configured the device and the user has validated the configuration, the software sets this flag to lock out any further changes. It is an option that this flag be protected by password which requires user verification before the configuration can be unlocked and changed.

While a device has the Configuration Lock attribute set, it shall reject Configure_Requests, Type 1 and 2 Safety Reset, and any valid Type 1 SafetyOpen.

6.6.5.17 Configuration UNID (CFUNID)

The Configuration UNID attribute shall be implemented as part of the SNCT interface. The Configuration UNID identifies the owner of the configuration in this safety device. The Configuration UNID attribute can be set by a number of means. The Configuration UNID attribute shall have the following special meanings assigned:

- All octets set to 00_{hex} = No owner, accept any,
- All octets set to FF_{hex} = Software Tool is the assigned owner.

The default for the Configuration UNID shall be all octets set to 00_{hex}.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

When the Configuration UNID attribute is set to "No owner, accept any", FSCP 2/1 safety devices shall capture the first configuration source (Type 1 and/or Configure_Request) as the owner (see Table 32).

The CFUNID value is used in conjunction with the OUNID value provided in either the Configure_Request or a Type 1 SafetyOpen. See Table 32 for the definition of how devices respond to the various services based on what the CFUNID is set to at the time the service is received. SNCT shall always use all FF_{hex} for the OUNID.

EXAMPLE If the CFUNID is set to all FF_{hex}, then the OUNID of the Configure_Request shall equal this value to process the command.

Table 32 – Summary of device behavior for various CFUNID values

Service	Value of CFUNID		
	FF_{hex}	00_{hex}	OUNID
Configure_Request (FF_{hex}) from SNCT	Accept	Accept Set CFUNID = FF_{hex}	Fail
Configure_Request (OUNID)	Fail	Accept Set CFUNID = OUNID	Accept only if CFUNID = OUNID Fail otherwise
Type 1 SafetyOpen	Fail	Accept Set CFUNID = OUNID	Accept only if CFUNID = OUNID Fail otherwise

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

6.6.5.18 Safety Configuration Identifier (SCID)

The Safety Configuration Identifier attribute is the signature on the safety configuration. This attribute is a concatenation of the Safety Configuration CRC (SCCRC) + Safety Configuration Time Stamp (SCTS). These values are obtained from either the SafetyOpen or from the Safety Configuration Software during configuration validation.

The default for SCID attribute in the Safety Supervisor shall be 0.

When a device enters Configuring mode, the SCID attribute shall be set to 0 and maintained at this value (through power cycles) until a successful Validate has been executed.

```
typedef struct _S_SCID
{
DWORD           dwCRC;   //calculated by device
DWORD           dwTime;  // set by software
WORD            wDate;
} S_SCID;
```

6.6.5.19 Target UNID (TUNID)

The Target UNID is an NV attribute that reflects the UNID saved with the configuration.

If a single safety port device, the Target UNID attribute in the Safety Supervisor shall always reflect either the default or the current Target UNID saved through the UNID setting process. If a multiple safety port device, the Target List UNID attribute (Attribute 30) in the Safety Supervisor shall always reflect either the default or the current Target UNIDs saved through the UNID list setting process.

The UNID(s) of a device shall be stored to NV as part of the UNID(s) setting operation.

The UNID(s) of a device shall be stored to the DeviceNet object, TCP/IP Interface object, or SERCOS III object's SNN attribute as part of the UNID(s) setting operation.

A device in Manufacturers default state shall have an invalid Target UNID(s) value in its NV (for example ten octets of FF_{hex}) for each of its safety ports.

The UNID(s) of a device shall be read from NV during power up and loaded into an attribute of the Safety Supervisor object and Safety_Network_Number attribute of the DeviceNet object, TCP/IP Interface object, or SERCOS III object.

If the UNID represents a valid Number (not equal to out-of-box), this number shall be compared to the NodeID. In case of a match the device continues its startup procedure. In case of a mismatch the Device transits to Abort.

When a device faults from a Switch-NV setting mismatch, it shall allow either a reset to out-of-box, or a Recover request issued to the Safety Supervisor to clear the Abort. In both cases, the device shall move to the "Waiting for TUNID" state.

The reading of the UNID attribute in the Safety Supervisor shall be done with safety integrity.

The applying of configuration data and UNID to NV shall be done with safety integrity.

6.6.5.20 Proposed TUNID

The default value for the Proposed TUNID attribute shall be all FF_{hex}.

While a device is going through the "Propose_TUNID/Apply_TUNID" process, this attribute reflects the value being proposed. Once the apply operation is complete, this attribute shall be set back to the out-of-box default of all FF_{hex}.

6.6.5.21 Output Connection Owner (OCPUNID)

This attribute is only used for safety connection to outputs. Safety connections to outputs define an owner to prevent errant connections from hijacking an output resource in a validated safety system. This owner Id identifies which originator safety device has been given ownership rights to this safety output connection. This parameter is obtained from the Safety Segment Parameters in the SafetyOpen. The OCPUNID value could be the same as Attribute 25 of the Safety Supervisor (CFUNID) when the device is also configured as part of the SafetyOpen. Since device may have more than one output resource and may allow for separate owners of each, this attribute is arranged as a structure to allow for each resource to be separately maintained. The resource is identified by a Logical Segment address.

The default for all OCPUNIDs shall be 0 (accept any owner) with the ePath for each pointing to the respective resource.

6.6.5.22 Target UNID List

See 6.6.5.19 for the definition of the Target UNID members of this attribute.

6.6.5.23 Proposed TUNID List

See 6.6.5.20 for the definition of the Proposed TUNID members of this attribute.

6.6.6 Subclasses

Each instance level subclass defines a unique meaning for an overlapping range of instance attribute IDs and/or instance service IDs. The range for subclass definitions begins at ID 96_{hex}

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

and numbers downward for attributes, and ID 63_{hex} and numbers downward for services. The subclass for a given instance is identified by the value of its Subclass instance attribute. There are no subclasses currently defined for the instances.

6.6.7 Safety Supervisor common services

6.6.7.1 Common services overview

The common services supported by the Safety Supervisor are defined in Table 33. The Safety Supervisor object specific services are defined in Table 34.

Table 33 – Safety Supervisor common services

Service code	Need in implementation		Service name	Description of service
	Class	Instance		
$0E_{hex}$	Conditional	Required	Get_Attribute_Single	Returns the contents of the specified attribute
010_{hex}	n/a	Required	Set_Attribute_Single	Modifies an attribute value
$0D_{hex}$	n/a	Conditional [a]	Apply	Applies a pending configuration to NV memory, and moves the device to the Idle state
15_{hex}	n/a	Optional	Restore	Restores last applied configuration in devices that support it

[a] Safety devices which support the SNCT interface (i.e. not configured by the SafetyOpen or some vendor specific means) shall support this service.

Any Safety Supervisor instance service may be requested internally by the device as specified by the manufacturer.

Table 34 – Safety Supervisor object specific services

Service code	Need in implementation		Service name	Description of service
	Class	Instance		
$4B_{hex}$			Reserved	
$4C_{hex}$	n/a	Optional	Recover	Moves the device out of the Abort State
$4E_{hex}$	n/a	Optional	Perform_Diagnostics	Causes the device to perform a set of diagnostic routines if appropriate
$4F_{hex}$	n/a	Conditional[a]	Configure_Request	Moves the device to the Configuring State if appropriate. This service requires a password be provided to be executed
50_{hex}	n/a	Conditional[a]	Validate_Configuration	Causes the device to perform a validation check of the pending configuration. This service requires the software to provide the SCID (CRC + Time Stamp)
51_{hex}	n/a	Conditional[a]	Set_Password	Used to set a password attribute in the Supervisor object
52_{hex}	n/a	Conditional[a]	Configuration_Lock/ Unlock	This service acts upon the Configuration Lock attribute in the Safety Supervisor. This service requires a password be provided to be executed

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Service code	Need in implementation		Service name	Description of service
	Class	Instance		
53_{hex}	n/a	Conditional[c]	Mode Change	Shall be in implementation for Logic devices which support "executing" independent of I/O connections. A password is required to execute mode changes in safety devices
54_{hex}	n/a	Type 0 Conditional [e], Type 1 and 2 Conditional[a]	Safety Reset	Resets the device in a manner similar to the Identity object, except that a password is required to execute
55_{hex}	n/a	Conditional[b]	Reset Password	Used to reset the password in a device. Data contents of this message is vendor specific
56_{hex}	n/a	Conditional [d]	Propose_TUNID	Used to initiate the setting of the TUNID in an out-of-box device
57_{hex}	n/a	Conditional [d]	Apply_TUNID	Used to complete the TUNID setting operation.
58_{hex}	n/a	Conditional [f]	Propose_TUNID_List	Used to initiate setting the TUNID list in an out-of-box device.
59_{hex}	n/a	Conditional [f]	Apply_TUNID_List	Used to complete setting the TUNID list operation.

[a] Shall be in implementation for FSCP 2/1 safety devices which support the SNCT interface.

[b] Conditional on supporting the password service as part of the SNCT interface.

[c] Shall be in implementation for FSCP 2/1 safety devices which support the SNCT interface and are Logic devices which support "executing" independent of I/O connections. A password is required to execute mode changes in safety devices.

[d] Shall be in implementation only for single port FSCP 2/1 safety devices which support the SNCT interface but highly recommended for devices which are configurable by Type 1 SafetyOpen. Optional for devices which use vendor-specific configuration. Multiple safety port devices shall not implement the Propose_TUNID and Apply_TUNID services.

[e] Conditional – Required for FSCP 2/1 devices, but optional for FSCP 2/1 on CP 16/3 devices and safety devices which use vendor-specific configuration.

[f] Conditional – Multiple safety port devices that support the SNCT interface shall support the Propose_TUNID_List and Apply_TUNID_List services. Single safety port devices shall not support Propose_TUNID_List and Apply_TUNID_List services. Multiple safety port devices with vendor-specific configuration may support the Propose_TUNID_List and Apply_TUNID_List services.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Any Safety Supervisor instance service may be requested internally by the device as specified by the manufacturer. Generally, these requests will be generated as the result of an event such as the activation of a button or external contact closure.

6.6.7.2 Recover service

The Recover service is used to transition the device application objects, out of the recoverable fault state, to the idle state. This service request may be originated internally, from application objects.

6.6.7.3 Perform_Diagnostics service

The Perform_Diagnotics service is used to instruct the Safety Supervisor object to perform a diagnostic test. A diagnostic test is either of type common or device-dependent. Common diagnostic tests could include: RAM, EPROM, non-volatile memory, and communications. The structure of common type diagnostic tests is implementation-specific. Details of device-dependent diagnostics are outside the scope of this document.

6.6.7.4 Configure_Request service

The Configure_Request service is used to transition the device application objects from the Abort, Execute or Idle state to the Configuring state.

When a Configure_Request is received, if the Configuration_Lock attribute is set, an "Object State Conflict (0Chex)" error shall be returned. The request contains three parameters; the password parameter contained in the Safety Supervisor, the Target device UNID, and the Originator UNID. These values are matched up against the Password, TUNID, and CFUNID in the device. The OUNID is needed to allow the device to determine if the source is a software tool or an ACR capable originator.

When the Configure Request command is accepted, the device shall only accept configuration messages to safety relevant objects over "this connection only". Any attempts to write to safety-relevant objects over other connections shall be rejected.

If a configuration connection fails for any reason, another Configure_Request shall be received (establishing a new connection source) before configuration changes can be made (even after a power-cycle).

The structure of the Configure_Request is defined in Table 35.

Table 35 – Configure_Request message structure

Name	Data type	Description
Service Code	USINT	$4F_{hex}$
Password	ARRAY of 16 OCTETS	
TUNID	ARRAY of 10 OCTETS	Target Device UNID. Used to detect misrouted requests
OUNID	ARRAY of 10 OCTETS	Originator Device UNID. If the originator is a software tool, this parameter shall be set to all FF_{hex}. If the originator is a device with ACR, this parameter shall be the device's OUNID

If a TUNID, OUNID mismatch error occurs when processing a Safety Supervisor Configure Request, an Invalid Parameter (20_{hex}) error code shall be returned.

If a password mismatch occurs when processing a Safety Supervisor Configure Request, a Privilege Violation ($0F_{hex}$) error code shall be returned.

6.6.7.5 Validate_Configuration service

This service causes the device to validate a pending configuration by executing a CRC calculation over this data and comparing it to the CRC provided in the message. If the CRC does not yield the same result, an error response as defined below is returned. Otherwise, a "success" response is returned. See Figure 10 and Figure 11 for the processing details for this service. This command can only be received over the connection that put the device into the configuration mode. The device NV saves the final SCID in Attribute 26 of the Safety Supervisor.

The structure of the Validate_Configuration message is defined in Table 36.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Table 36 – Validate_Configuration message structure

Name	Data type	Description
Service Code	USINT	50_{hex}
SCID	STRUCT of:	Safety Configuration ID
SCCRC	4 OCTETS	Proposed Safety Configuration CRC as calculated by the software. This is validated by the device
SCTS	6 OCTETS	Safety Configuration Time Stamp. This value marks the date and time of the configuration, which is used as a change detection mechanism

The structure of the Success Validate Reply is defined in Table 37.

Table 37 – Validate_Configuration success message structure

Name	Data type	Description
Service Code	USINT	50_{hex}
SCID	STRUCT of:	Safety Configuration ID
SCCRC	4 OCTETS	Safety Configuration CRC as calculated by the device
SCTS	6 OCTETS	Safety Configuration Time Stamp. This value is an echo of what was sent in the Validate request

If the Safety Supervisor Validate_Configuration command does not succeed, the error response shall send a class defined "Validation Error" ($D0_{hex}$). The following error code defined in Table 38 is defined as a Validation Error in the Safety Supervisor, additional error codes are defined in Table 39.

Table 38 – Validate_Configuration error code

General error code	Additional error code	Error name	Description
$D0_{hex}$	see Table 39	Validation Error	This error is a class specific error for the Safety Supervisor and is returned in response to a Validate_Configuration error

Table 39 – Validate_Configuration extended codes

Additional error codes	Reason code	Description
1	CRC mismatch	This is the default non-specific additional code, when no other additional information is available and the configuration CRC does not match the sent value
2	Invalid Configuration Parameter	This code can be used to indicate a parameter error if a device does specific validation of configuration data. NOTE This could happen even if the CRC's matched.
3	TUNID Not Set	This code can be used to indicate that the device is in the Waiting for TUNID state and needs to have its TUNID set

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

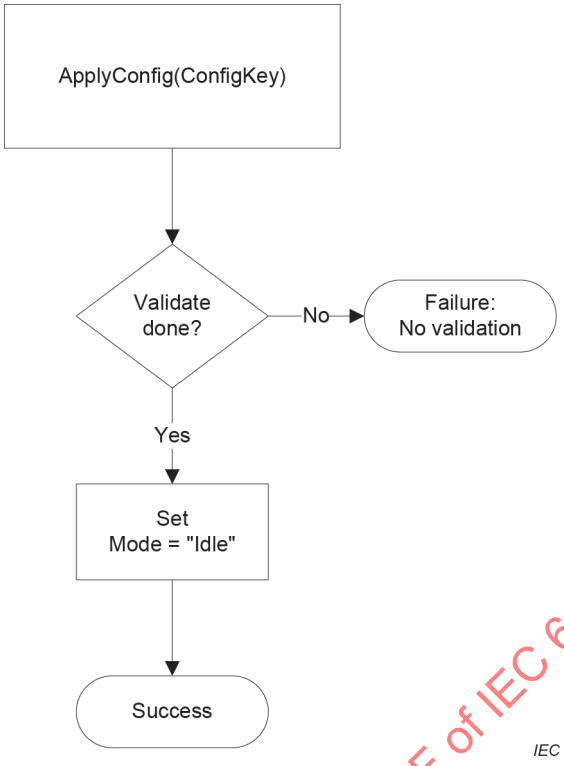
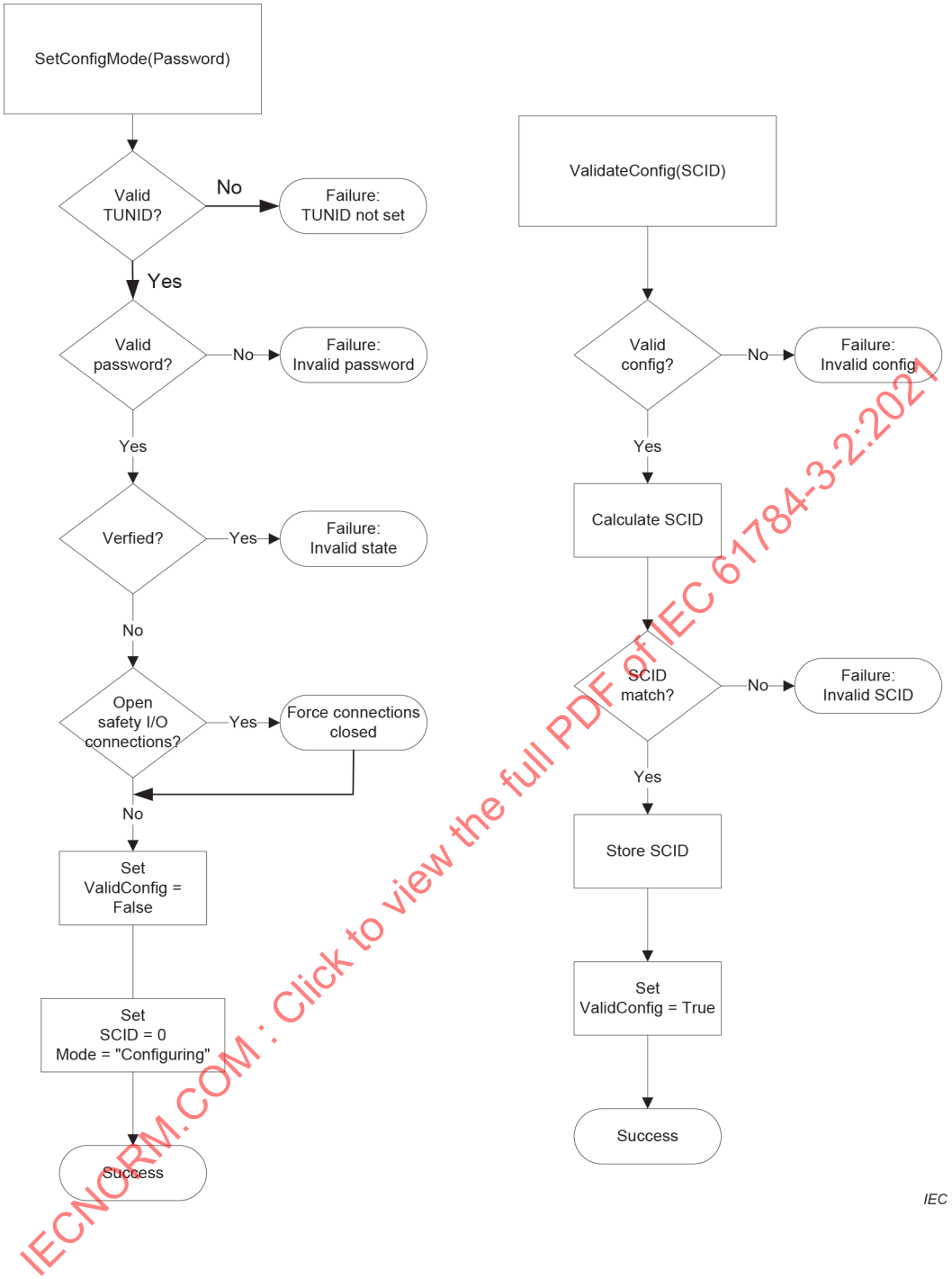


Figure 10 – Applying device configuration

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021



IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Figure 11 – Configure and Validate processing flowcharts

6.6.7.6 Set_Password service

The Set_Password service causes the device to set a Password in the Supervisor. This service takes 2 parameters. The first one is a password parameter representing the existing password, and the second is a parameter representing the new parameter. When setting a password for the first time, the Current Password parameter is set to the Out-of-box default (zero).

The structure of the Set_Password is defined in Table 40.

Table 40 – Set_Password message structure

Name	Data type	Description
Service Code	USINT	51_{hex}
Current Password	16 OCTETS	
New Password	16 OCTETS	

If a password mismatch occurs on the current password when processing a Safety Supervisor Set Password command, a Privilege Violation ($0F_{hex}$) error code shall be returned.

A password which is smaller than the password parameter shall be right-aligned in little endian order to the least significant octet of the 16 octet password parameter. The unused upper octets of the password parameter shall be zero-filled.

6.6.7.7 Reset_Password service

The Reset_Password service is provided to allow passwords in a device to be reset. The exact contents and usage has been made vendor specific to protect password integrity. This service requires 1 parameter plus a vendor specific data field. The required parameter is a data size field to identify the size of the vendor specific data field. The content of vendor data is assumed to be unique to the device and the means by which this service is used shall be provided by each vendor.

The structure of the Reset_Password is defined in Table 41.

Table 41 – Reset_Password message structure

Name	Data type	Description
Service Code	USINT	55_{hex}
Data Size	USINT	Number of vendor specific data octets
Vendor data	Data Size	Vendor data which contains data needed to cause the password to be reset

If a Data Size error occurs in the Safety Supervisor Reset_Password command, either error code 15_{hex} (too much data) or 13_{hex} (not enough data) shall be returned.

If a Vendor data mismatch occurs when processing a Safety Supervisor Reset_Password command, a Privilege Violation ($0F_{hex}$) error code shall be returned.

6.6.7.8 Configuration_Lock/Unlock service

The Configuration_Lock/Unlock service causes the device to modify the Configuration_Lock attribute in the Safety Supervisor. This service requires a value parameter (0 = unlocked, 1 = locked), and the password parameter. The password parameter is compared to the stored password and will only be executed if the password matches. If there is a password mismatch, a "Password Mismatch" error is returned.

The structure of the Configuration_Lock/Unlock is defined in Table 42.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Table 42 – Configuration_Lock/Unlock message structure

Name	Data type	Description
Service Code	USINT	52_{hex}
Value	BOOL	0 = unlocked, 1 = locked
Password	16 OCTETS	
TUNID	10 OCTETS	Target Device UNID. Used to detect misrouted requests

If a TUNID mismatch occurs in the Safety Supervisor Configuration_Lock/Unlock command, the Invalid Parameter (020_{hex}) error code shall be returned.

If a password mismatch occurs when processing a Safety Supervisor Configuration_Lock/Unlock command, a Privilege Violation ($0F_{hex}$) error code shall be returned.

6.6.7.9 Mode Change service

The Mode Change service is used by devices which need to move between Idle and Executing states regardless of its connection status. This command requires proper authorization to execute, so the password is required to execute.

The structure of the Mode Change is defined in Table 43.

Table 43 – Mode_Change message structure

Name	Data type	Description
Service Code	USINT	53_{hex}
Value	BOOL	0 = Idle, 1 = Executing
Password	16 OCTETS	

If a password mismatch occurs in the Safety Supervisor Mode Change command, an Privilege Violation ($0F_{hex}$) error code shall be returned.

6.6.7.10 Safety_Reset service

The Safety_Reset service is used to reset the device. The Safety_Reset service replaces the standard reset service defined so that it can be qualified by the password.

When a Type 1 or Type 2 Safety Reset is received, if the Configuration_Lock attribute is set, a "Object state conflict ($0C_{hex}$)" error shall be returned.

The structure of the Safety_Reset is defined in Table 44.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Table 44 – Safety_Reset message structure

Name	Data type	Description
Service Code	USINT	54_{hex}
Reset type	USINT	see Table 45
Password	16 OCTETS	
TUNID	10 OCTETS	Target Device UNID. Used to detect misrouted requests
Attribute_Bit_Map	USINT	Bit mapped parameter which indicates which attributes shall be preserved through the reset. This parameter is only included when the Reset Type is 2. See Table 46

If a TUNID mismatch occurs when sending the Safety Supervisor Safety Reset command, the Invalid Parameter (20_{hex}) error code shall be returned.

If a password mismatch occurs when processing a Safety Supervisor Safety Reset command, a Privilege Violation ($0F_{hex}$) error code shall be returned.

Table 45 – Safety Supervisor safety reset types

Value:	Type of reset
0	Emulate as closely as possible cycling power on the device
1	Return as closely as possible to the default configuration, and then emulate cycling power as closely as possible
2	Return as closely as possible to the out-of-box configuration except to preserve the parameters indicated by the Attribute Bit Map, and then emulate cycling power as closely as possible

Table 46 – Attribute bit map parameter

Bit	Attribute bit map assignments
0	When set, preserve Soft-set MACID
1	When set, preserve Soft-set Baud Rate
2	When set, preserve the TUNID
3	When set, preserve the Password
4	When set, preserve the CFUNID
5	When set, preserve the OCPUNID
6	Reserved, always 0
7	Use Extended Map (To be defined later)

Table 47 shows how a safety device shall process the various reset types based on the Lock/Unlock condition and safety connection status.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Table 47 – Reset processing rules for reset types

Reset Type	Possible Conditions when Reset is received			
	Safety Connection open / Locked	Safety Connection open / Unlocked	No Safety Connections / Locked	No Safety Connections / Unlocked
Type 0	Mode/State Error Response	Mode/State Error Response	Process and Respond	Process and Respond
Type 1	Mode/State Error Response	Mode/State Error Response	Mode/State Error Response	Process and Respond
Type 2	Mode/State Error Response	Mode/State Error Response	Mode/State Error Response	Process and Respond

6.6.7.11 Propose_TUNID service

The Propose_TUNID service establishes a proposed TUNID setting within the device. The value isn't stored in NV memory or in the TUNID attribute until the apply service is received.

The Propose_TUNID service shall only be accepted when the target device is in the Waiting_for_TUNID state.

Once the TUNID is successfully set, it can transition to Configuring.

The NodeID of the TUNID shall be matched up against the MACID of the DeviceNet object or IP attribute of the TCP/IP object or the SDID of the SERCOS III Link Object.

The value in the NodeID attribute will be either what was read on the switches or what was set by a tool. In either case, the MACID/IP portion of the Proposed_TUNID shall match this.

The structure of the Propose_TUNID service is defined in Table 48.

Table 48 – Propose_TUNID service

Name	Data type	Description
Service Code	USINT	56hex
TUNID	10 OCTETS	Proposed Target Device UNID value

If an originator wants to cancel a propose/apply operation, sending a propose service with a TUNID of all FF_{hex} shall cancel the operation.

The following pseudo code defines the berhavior of the Propose_TUNID service:

```
TUNIDProposedHandler()
{
IF (Device_State=Waiting_for_TUNID)
   THEN IF (Propose_TUNID[TUNID] != all FFhex)
         THEN IF (Propose_TUNID[TUNID_MACID] == NodeID)
              THEN
    TUNIDProposedAttr = Propose_TUNID[TUNID]
                   NET LED Flash sequence is started
                   Return Success Reply
              ELSE

   Error Code “Invalid Parameter” is returned
   ELSE // cancel propose_apply operation, returns att. to all FFhex
```

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

```
        Stop NET LED Flash Sequence
       TUNIDProposedAttr = Propose_TUNID[TUNID]
        Return Success Reply
ELSE
       Error Code “Object State Conflict” is returned
}
```

6.6.7.12 Apply_TUNID service

The structure of the Apply_TUNID service is defined in Table 49 and a processing flow chart is defined in Figure 12.

Table 49 – Apply_TUNID service

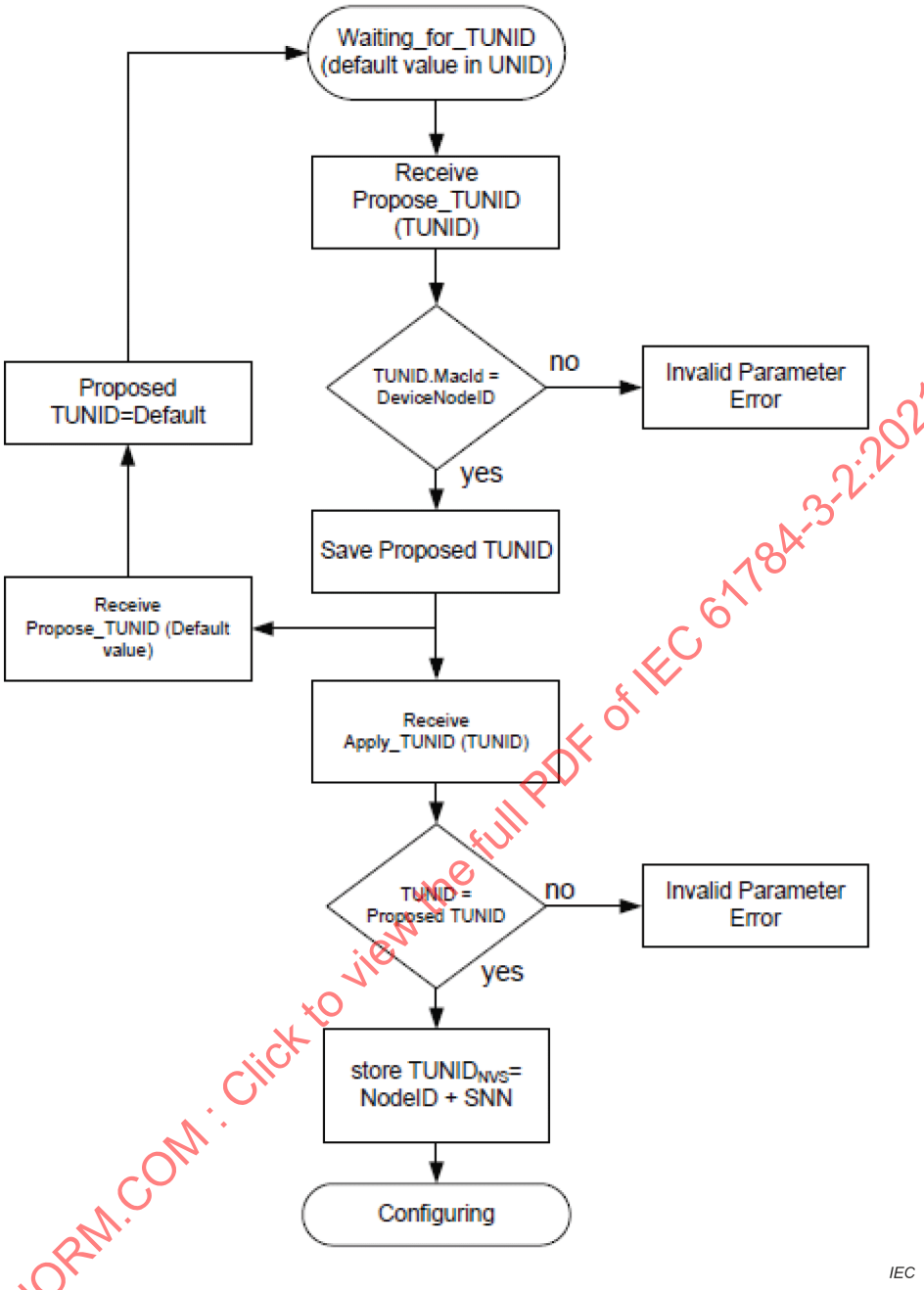
Name	Data type	Description
Service Code	USINT	57_{hex}
TUNID	10 OCTETS	Proposed Target Device UNID value

The Apply_TUNID service shall validate the TUNID against the proposed value, stops the LED flashing, saves the TUNID to nonvolatile storage, updates the TUNID attribute in the Supervisor, and sets the proposed_TUNID attribute to all FF_{hex}. The Supervisor shall then transition to Configuring.

The following pseudo code defines the berhavior of the Apply_TUNID service:

```
Apply_TUNIDHandler()
{
IF (Device_State=Waiting_for_TUNID)
   THEN IF {(Apply_TUNID[TUNID] != all FFhex)
                  AND (TUNIDProposedAttr == Apply_TUNID[TUNID])
         THEN
             Stop Flash Sequence
             Target_UNID = TUNIDProposedVar[TUNID]
//NV Memory operation
// Set SNN attribute in DeviceNet, SERCOS III Link object or TCP/IP
object, NV Memory operation
             Safety_Network_Number = TUNIDProposedVar[SNN]
             TUNIDProposedVar[TUNID] = TUNID_OUT_OF_BOX_DEFAULT
             Return Success Reply
             Device_State = CONFIGURING
         ELSE
             Error Code “Invalid Parameter” is returned
   ELSE
      Error Code “Object State Conflict” is returned
}
```

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021



IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Figure 12 – UNID handling during "Waiting for TUNID"

6.6.7.13 Propose_TUNID_List service

The Propose_TUNID_List service establishes the TUNID setting for each port within a device. Apply Subclause 6.6.7.11 to each Proposed TUNID in the list. The structure of the Propose_TUNID service is defined in Table 50.

Table 50 – Propose_TUNID_List service

Name	Data type	Description
Service Code	USINT	57_{hex}
Number of Proposed TUNIDs	USINT	Number of Proposed Target UNID list entries
Proposed TUNIDs	ARRAY of STRUCT	List of (Port Number, Proposed TUNID) pairs
Port Number	UINT	See IEC 61158-4-2:2019, 7.11.4.3
Proposed TUNID	10 OCTETS	Proposed TUNID associated with its a specific CIP Port Number

6.6.7.14 Apply_TUNID_List service

The Apply_TUNID_List service commits the Proposed TUNID setting for each port within a device. Apply Subclause 6.6.7.12 to each Proposed TUNID in the list. The structure of the Apply_TUNID service is defined in Table 51.

Table 51 – Apply_TUNID_List service

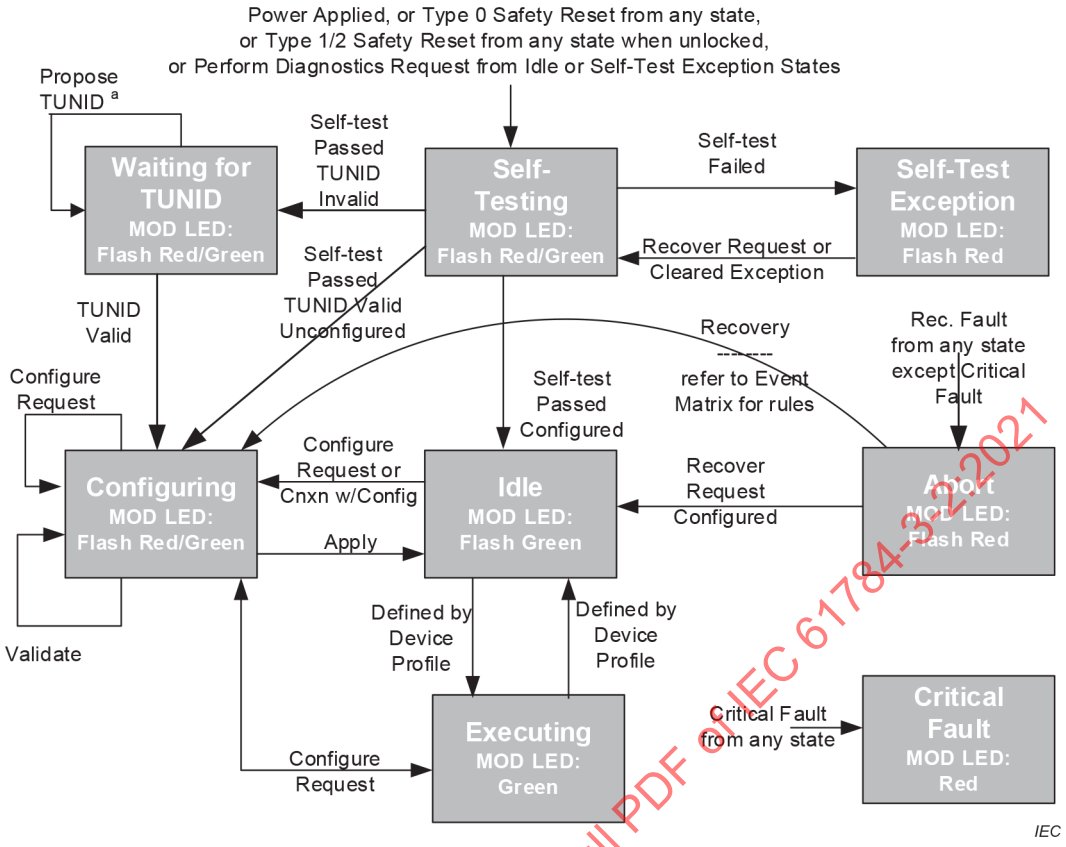
Name	Data type	Description
Service Code	USINT	57_{hex}
TUNID	10 OCTETS	Proposed Target Device UNID value

6.6.8 Safety Supervisor behavior

6.6.8.1 Safety Supervisor object states

Figure 13 shows the state diagram defining the behavior of the Safety Supervisor object, further information on the Safety Supervisor events are given in Table 52. Module Status LED behavior is governed by the Safety Supervisor states as shown in the diagram. Device Type specific state extensions are allowed and explicitly defined in the safety device profiles. Device specific modifications to the Module Status LED behavior are also allowed and explicitly defined in the safety device profiles. Waiting for TUNID state and associated LED behavior is vendor-specific for devices which do not support the Propose/Apply TUNID services.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021



[a] After Propose_TUNID service request, NET LED flashes Red/Green using Fast 250 ms / 250 ms pattern until successful Apply_TUNID.

Figure 13 – Safety Supervisor state diagram

Table 52 – Safety Supervisor events

State	Description
Executing	Device is executing, (for example, is fully configured, has no errors, and has met vendor defined criteria). This state, and the transitions into or out of it, shall be further specified in an appropriate device profile specification
Self-Testing	Object instance exists and has been initialized; all attributes have appropriate initial values (as indicated herein and in applicable device profile specification). Exception Status bits have been reset. Device is performing device-specific and device type specific test to determine if it is qualified to execute its application process
Self-Test Exception	Object has detected an exception condition during self-testing. The details of the exception are stored in the appropriate attribute values of the Safety Supervisor object
Idle	Object and device have been initialized, successfully completed self-testing, and has a valid configuration. Further, the device is not executing the operational components of its device specific functions. Configuring and Idle are persistent states that are preserved through power cycles
Abort	Object instance is in a Abort state; this state can only be entered due to internally generated events. The conditions required for exit from a recoverable fault is defined in the Event Matrix
Waiting for TUNID	Device exits Self-testing and finds the NV saved TUNID is at the out-of-box default value. It remains in this state until the TUNID setting sequence (i.e. propose/apply in SNCT interface) is successfully completed. Only then can the device be configured
Configuring	Object and device have been initialized, successfully completed self-testing, but does NOT have a valid configuration. Configuring and Idle are sticky states that are preserved through power cycles
Critical Fault	The object (and device) is in a fault state from which there is no recovery. Processing of particular object services could be impossible in this state. Possible additional conditions required for exit from a critical fault are outside the scope of this document

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

The Safety Supervisor Status attribute value indicates the overall state of the device. It is updated on appropriate state transitions within the Safety Supervisor object. Attribute values 1 to 8 represent valid states. A value of zero indicates that the Safety Supervisor state is unknown; conditions under which a zero value may occur are outside the scope of this document.

6.6.8.2 Safety Supervisor state event matrix

Table 53 defines the states and events for the Safety Supervisor.

Table 53 – State event matrix for Safety Supervisor

Event	State							
	Waiting for TUNID	**Configuring (Safety State)**	**Idle (Safety State)**	**Self-Test (Safety State)**	**Self-Test Exception (Safety State)**	**Executing**	**Abort (Safety State)**	**Critical Fault (Safety State)**
Power Applied			--	Default Entry Point performs its Self-test application process	--	--	--	Transition to SELF TEST
Self-Test Passed			Not Applicable	Transition to Last Saved State if not out-of-box Else, Wait for TUNID	Not Applicable	Not Applicable	Not Applicable	Not Applicable
Self-Test Failed			Not Applicable	Set appropriate Exception Status Bits and Transition to SELF TEST EXCEPTION	Not Applicable	Not Applicable	Not Applicable	Not Applicable
Propose TUNID	Validate Settings and Flash Net LED Red/Green using fast 250 ms/ 250 ms pattern	Error OSC[b]	Error OSC[b]	Error OSC[b]	Error OSC[b]	Error OSC[b]	Error OSC[b]	Error OSC[b]
Apply TUNID	Save TUNID to NV memory, Transition to Config-uring	Error OSC[b]	Error OSC[b]	Error OSC[b]	Error OSC[b]	Error OSC[b]	Error OSC[b]	Error OSC[b]
Exception Condition Cleared			Not Applicable	Not Applicable	Set appropriate Exception Status Bits and Transition to SELF TESTING	Not Applicable	Not Applicable	Not Applicable

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Event	State							
	Waiting for TUNID	**Configuring (Safety State)**	**Idle (Safety State)**	**Self-Test (Safety State)**	**Self-Test Exception (Safety State)**	**Executing**	**Abort (Safety State)**	**Critical Fault (Safety State)**
Critical Fault	Transition to CRITICAL FAULT	Transition to CRITICAL FAULT	Transition to CRITICAL FAULT	Transition to CRITICAL FAULT	Transition to CRITICAL FAULT	Transition to CRITICAL FAULT	Transition to CRITICAL FAULT	Ignore Event
Configure Request	Error TNS[c]	Stay in state Validate and accept	If not Locked, Transition to Configuring	Error OSC[b]	Error OSC[b]	If not Locked, Drop Connections Apply Safety State Go to Configu-ring	If Configured: Transition to IDLE --- Unconfig-ured: Transition to Configuring --- If Switch/TUNID mismatch Error OSC[b]	Error OSC[b]
Validate Configuration	Error OSC[b]	Stay in state – Store Result	Error OSC[b]	Error OSC[b]	Error OSC[b]	Error OSC[b]	Error OSC[b]	Error OSC[b]
Apply Request	Error OSC[b]	Transition to Idle if Valid	Error OSC[b]	Error OSC[b]	Error OSC[b]	Error OSC[b]	Error OSC[b]	Error OSC[b]
Type 1 SafetyOpen	Error TNS[c]	Apply configuration Transition to Executing if Config. Valid	Transition to Configuring, Proceed to IDLE/EXECUTING dependent on Profile	Error OSC[b]	Error OSC[b]	Drop Connec-tions, Transition to Configuring, Proceed to IDLE EXECUTING dependent on Profile	Error OSC[c]	Error OSC[b]
Type 0 Safety Reset	Transition to SELF TEST	Transition to SELF TEST	Transition to SELF TEST	Transition to SELF TEST	Transition to SELF TEST	Transition to SELF TEST (SRS15)	Transition to SELF TEST	Transition to SELF TEST if possible
Type 1 / 2 Safety Reset	If not Locked, Process type Transition to SELF TEST	If not Locked, Process type Transition to SELF TEST	If not Locked, Process type Transition to SELF TEST	If not Locked, Process type Transition to SELF TEST	If not Locked, Process type Transition to SELF TEST	If not Locked, Process type Transition to SELF TEST (SRS15)	If not Locked, Process type Transition to SELF TEST	If not Locked, Process type Transition to SELF TEST
Internal Abort Request	Transition to Abort	Transition to Abort	Transition to Abort	Error OSC[b]	Error OSC[b]	Transition to Abort	Error AIRS[a]	Error OSC[b]

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Event	State							
	Waiting for TUNID	**Configuring (Safety State)**	**Idle (Safety State)**	**Self-Test (Safety State)**	**Self-Test Exception (Safety State)**	**Executing**	**Abort (Safety State)**	**Critical Fault (Safety State)**
Recover Request	Error OSC[b]	Error OSC[b]	Error OSC[b]	Restart SELF TESTING	Transition to SELF TESTING	Error OSC[b]	If Configu-red: Transition to IDLE --- Unconfig-ured: Transition to Configu-ring --- If Switch/TUNID mismatch Error OSC[b]	Error OSC[b]
Perform Diagnostics Request	Error OSC[b]	Error OSC[b]	Transition to SELF TEST	Restart SELF TEST	Transition to SELF TEST	Error OSC[b]	Perform all device diagnostic tests	Error OSC[b]
Safety Connection Failed	Ignore Event	Ignore Event	Ignore Event	Ignore Event[d]	Ignore Event	Device Profile Defined	Ignore Event[d]	Ignore Event[d]
Safety I/O Connection established	Not Possible	Not Possible	Device Profile Defined	Ignore Event[d]	Not Possible	Device Profile Defined	Not Possible	Not Possible
Safety I/O Connection Deleted	Ignore Event[d]	Ignore Event[d]	Ignore Event[d]	Ignore Event[d]	Not Possible	Device Profile Defined	Ignore Event[d]	Error OSC[b]
Mode Change	Error OSC[b]	Error OSC[b]	Device Profile Defined	Error OSC[b]	Error OSC[b]	Device Profile Defined	Error OSC[b]	Error OSC[b]
Restore	Error OSC[b]	Restore Previous Configuration	Error OSC[b]	Error OSC[b]	Error OSC[b]	Ignore Event[d]	Error OSC[b]	Error OSC[b]
Lock/ Unlock	Error OSC[b]	Error OSC[b]	if valid, Execute and reply	Error OSC[b]	Error OSC[b]	if valid, Execute and reply	if valid, Execute and reply	if valid, Execute and reply, if possible
LED Definitions for States								
Module Status LED	Flashing Red/Green	Flashing Red/Green	Flashing Green	Flashing Red/Green	Flashing Red	Solid Green	Flashing Red	Solid Red

[a] Error AIRS = Error Response "Already in Requested Mode/State" (Code $0B_{hex}$).

[b] Error OSC = Error Response "Object State Conflict" (Code $0C_{hex}$) when possible.

[c] Error TNS= Error Response "TUNID not Set", 01_{hex} extended code or $80D_{hex}$ object specific extended code.

[d] Ignore Event:: defined as "event has no effect on the state", no response necessary.

Any Safety Supervisor instance service may be requested internally by the device as specified by the manufacturer. Generally, these requests will be generated as the result of an event such as a diagnostic failure.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

6.6.8.3 Effect of locking on device behavior

Figure 14 defines the effect that the "locked" condition has on the ability of a device to be configured; devices which are locked will reject all attempts to change any configuration data that affects the SCID.

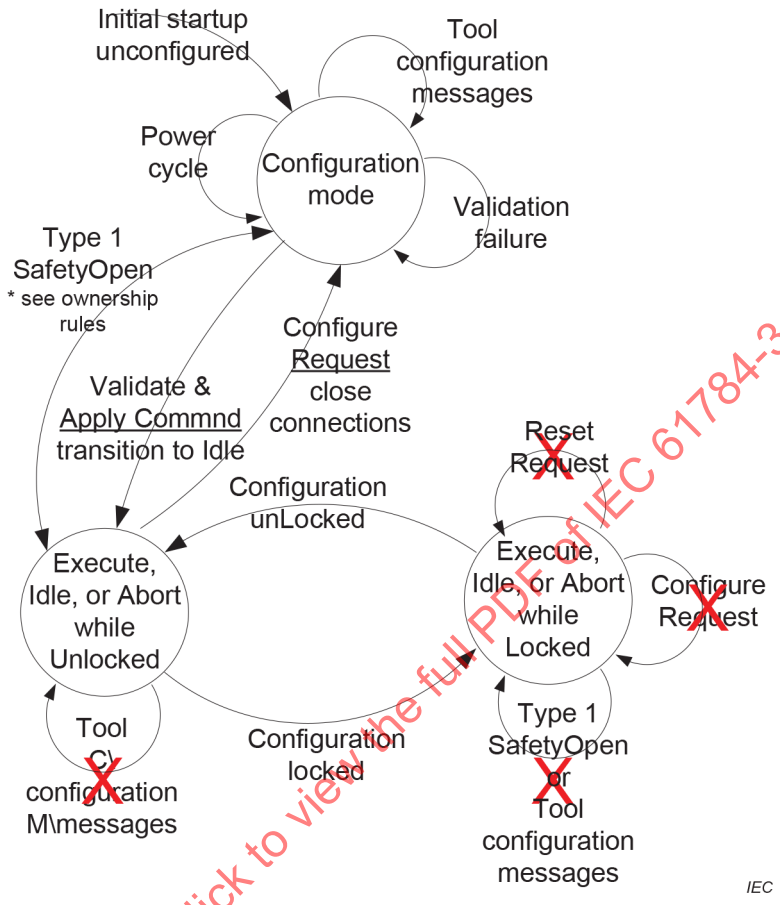


Figure 14 – Configuration, testing and locked relationships

Table 54 defines the effect that ownership has on a device's ability to be configured. It shows that owned devices can only be Type 1 configured by the originator that has the owner UNID. A locked device can never be configured regardless of its ownership.

Table 54 – Configuration owner control vs. device state

Ownership rules	Configure mode	Execute/Idle Mode Unlocked	Execute/Idle Mode Locked
Config Owned (Config. OUNID = Owner UNID)	Type 1 accepted by owner only	Type 1 accepted by owner only	All Type 1 rejected
Config Un-owned (Config. OUNID = 0)	Type 1 accepted from anyone	Type 1 accepted from anyone	All Type 1 rejected
SW Tool Owned (Config. OUNID = all FF_{hex})	No Type 1 accepted	No Type 1 accepted	All Type 1 rejected

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

6.6.8.4 State mapping of Safety Supervisor object to Identity object

Table 55 defines the mapping of Safety Supervisor states to states defined for the Identity object. This state mapping defines the interface between these three objects. The identity object state attribute (if supported) shall follow this table.

Table 55 – State mapping of Safety Supervisor to Identity object

Safety Supervisor	Identity
Self-Testing	Device Self-Testing
Self-Test Exception	Major Unrecoverable
Idle	Standby
Configuring	Standby
Waiting for TUNID	Standby
Executing	Operational
Abort	Major Recoverable
Critical Fault	Major Unrecoverable

6.6.8.5 Safety Supervisor object event to Identity object event mapping

Table 56 describes the mapping of defined Safety Supervisor events to equivalent events defined for the Identity object. This event mapping defines the interface between these objects. This mapping is provided for reference purposes.

Table 56 – Safety Supervisor object event mapping

Safety Supervisor state events map to ->	Equivalent Identity event
Power Applied	Power Applied
Self-Test Failed	Failed Tests
Self-Test Passed	Passed Tests
Propose TUNID	No equivalent event
Apply TUNID	No equivalent event
Exception Condition Cleared	Fault Corrected
Critical Fault	Major Unrecoverable Fault
Configure Request	Deactivated
Validate Configuration	No equivalent event
Apply Configuration	Activated
Type 1 SafetyOpen	No equivalent event
Safety Reset	Reset
Abort (Internal)	Major Recoverable Fault
Recover Request	Fault Corrected
Perform Diagnostic Request	No equivalent event
Safety Connection Failed	Deactivated
Safety Connection Established	Activated
Safety Connection Deleted	No equivalent event
Mode Change	No equivalent event
Restore	No equivalent event
Lock/Unlock	No equivalent event

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

6.6.8.6 Identity object event to Safety Supervisor event mapping

Table 57 describes the mapping of defined Identity objects event conditions to equivalent events defined for the Safety Supervisor object. This event mapping defines the equivalent events between these objects. This mapping is provided for reference purposes only; the Safety Supervisor object is the controlling object in safety devices and only events defined by the supervisor shall be implemented in safety devices.

Table 57 – Identity object event mapping

Identity events map to ->	Safety Supervisor events
Power applied	Power applied
Failed tests	Self-Test failed
Passed tests	Self-Test passed
Deactivated	Configure request
Activated	Apply configuration
Major recoverable fault	Abort (internal)
Major unrecoverable fault	Critical fault
Minor fault	No effect
Fault corrected	Exception condition cleared
Reset	Service not supported error

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

6.7 Safety Validator object

6.7.1 General

Class Code: $3A_{hex}$

The Safety Validator object is designed for use in safety devices on all FSCP 2/1 networks. The Safety Validator contains the information necessary to coordinate and maintain reliable safety connections between client and server safety-related applications. The primary role of the Safety Validator function is to act as a safety transport manager of multiple low-level CPF 2 connections that together form a complete safety connection.

The device containing the Safety Validator object can create several instances of the Safety Validator object for each safety-related application connection point (for example application data assembly) supported by the device.

The Safety Validator object supports two basic safety transport types: Point-to-point and Multipoint. Each safety transport type has a defined set of low-level CPF 2 connections that shall be allocated along with the Safety Validator object when a safety connection is instantiated by a SafetyOpen.

6.7.2 Class attributes

The class attributes for the safety supervisor are defined in Table 58.

Table 58 – Safety Validator class attributes

Attr ID	Need in implem.	Access rule	Name	Data type	Description of attribute	Semantics of value
1 – 7	Optional	Get			See IEC 61158-5-2 and IEC 61158-6-2 for a description of the optional, reserved class attributes	
8	Required	Get	Safety Connection Fault Count	UINT	Diagnostic Counter that is a running count of Safety Connection Faults	

Safety Connection Fault Count: this Safety Connection Fault Count attribute in the Safety Validator shall be a running count (with auto-rollover) of how many times any safety connection was faulted for any reason.

6.7.3 Instance attributes

6.7.3.1 Instance attributes overview

Most attribute values are derived, hard coded, or obtained from the dynamic connection establishment process. The only settable attribute value is the Max Data Age diagnostic. A complete list of the instance attributes is defined in Table 59.

Table 59 – Safety Validator instance attributes

Attr ID	Need in Implementation	Access rule	NV	Name	Data type	Description of attribute	Semantics of value
1	Required	Get		Safety Validator State	USINT	State of the safety connection	
2	Required	Get		Safety Validator Type	USINT	Safety Validator type used in this instance	See 6.7.3.3
3	Optional	Get		Ping Interval EPI Multiplier	UINT	Number that defines the Ping_Count_Interval for a particular connection	16 to 1 000
4	Optional	Get		Time Coord Msg Min Multiplier	STRUCT of:		
				Time Coord Msg Min Multiplier array size	USINT	Size of array equals Max Consumer number for multipoint producers and 1 for point-to-point and multipoint consumer	
				Time Coord Msg Min Multiplier	Array of: UINT	Minimum number of 128 µs increments it could take for a Time Coordination Message to traverse from the consumer to the producer	0 – 7 813

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Attr ID	Need in Implementation	Acces s rule	NV	Name	Data type	Description of attribute	Semantics of value
5	Optional	Get		Network Time Expectation Multiplier	STRUCT of:		
				Network Time Expectation Multiplier array size	USINT	Size of array equals Max Consumer number for multipoint producers and 1 for point-to-point and multipoint consumer	
				Network Time Expectation Multiplier	Array of: UINT	Maximum number of 128 µs increments that a consumer shall allow the age of the safety data to reach	0 – 45 313
6	Optional	Get		Timeout Multiplier	STRUCT of:		
				Timeout Multiplier array size	USINT	Size of array equals Max Consumer number for multipoint producers and 1 for point-to-point and multipoint consumer	
				Timeout Multiplier	Array of: USINT	Determines the number of messages that may be lost before declaring a connection error	Base Format: 1-4 Extended Format: 1-255
7	Optional	Get		Max Consumer Number	USINT	Maximum number of consumers allowed for the connection	1 (Point-to-point) 2-15 (Multipoint)
8	Optional[a]	Get		Data Connection Instance	UINT	Connection Instance ID of the Safety Data Connection	
9	Optional[a]	Get		Coordination Connection Instance	STRUCT of:	Connection Instance IDs of the Safety Coordination Connection	1-max number of connections in the device
				Coordination Connection Instance array size	USINT	Size of array equals Max Consumer number for multipoint producers and 1 for point-to-point and multipoint consumer	
				Coordination Connection Instance	ARRAY of: UINT		
10	Optional[a]	Get		Correction Connection Instance	UINT	Connection Instance ID of the Time Correction Connection	0 (when not used) 1-max number of connections in the device

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Attr ID	Need in Implementation	Acces s rule	NV	Name	Data type	Description of attribute	Semantics of value
11	Optional[a]	Get		CCO Binding	UINT	Instance Id of a CCO which holds the connection Establishment settings for this connection. Only used by safety connection originators	0 (when not used or no binding present)
12	Required	Set		Max Data Age	UINT	Diagnostic which holds the largest Data Age detected in 128 µs increments. Attribute only used for Safety Consumers	The Set shall only be supported by the consumer. The only valid value for the Set is zero. See 6.7.3.13.
13	Required	Get		Application Data Path	Packed EPATH	Points to the application data attached to this safety connection	
14	Optional	Get	V	Error Code	UINT	Reason for error within this instance	0 if no error, else implementation specific error code
15	Conditional[b]	Get	V	Producer/ Consumer Fault Counters	STRUCT of:		
				Producer/ Consumer Counter Array Size	USINT	Size of array equals Max Consumer number for multipoint producers and 1 and 1 for point to point and multipoint consumer	
				Producer/ Consumer Fault Counter	ARRAY of: USINT	Number of faults detected this hout	See 6.7.3.14

[a] It is optional that these parameters be made publicly visible. However, all Validator instances shall have internal parameters which represent these variables.

[b] If the device support the Extended Format then this attribute is required.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

6.7.3.2 Safety Validator state

This attribute defines the current state of the Safety Validator object instance. Transitions in this state attribute reflect the current state of the object; the definitions are defined in Table 60. This attribute can be used to determine the condition of established safety connections.

Table 60 – Safety Validator state assignments

Value	State name	Description
0	Unallocated	In this state the Safety Validator object has either not been allocated to a connection or has been closed
1	Initializing	In this state the Safety Validator object is in the process of exchanging time coordination information across the connection. The "safety" connection is not yet fully established
2	Established	In this state the Safety Validator instance is fully established and producing/consuming safety data on behalf of the safety-related application
3	Connection_Failed	This state is entered when all connections associated with this Validator have failed for any reason. In producers, all multipoint consumer connections shall have failed. As long as any consumer is still operating, the producer would remain in the Established state
4-255	Reserved	

6.7.3.3 Safety Validator type

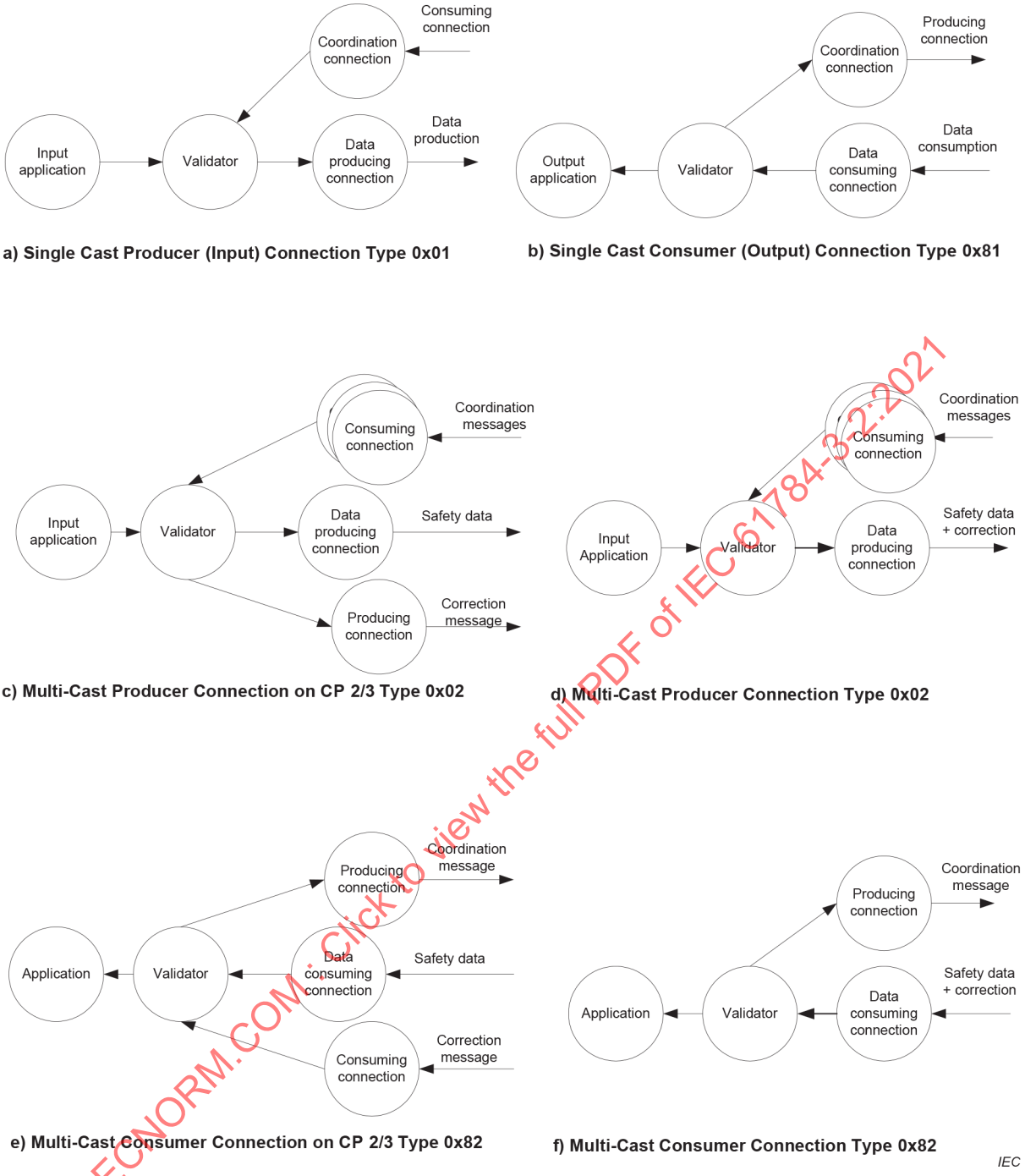
This attribute defines the type of Safety Validator transport that is being used, the definition is defined in Table 61. Targets shall derive this value from the Safety Connection parameters in the SafetyOpen.

Table 61 – Safety Validator type, bit field assignments

Bit 7	Bits 0 – 6
Producer(client) = 0/ Consumer(server) = 1	Safety Connection Type: 0 = unallocated 1 = Point-to-point 2 = Multipoint 3-127 = Reserved

The transports for each Safety Validator Type are depicted in Figure 15. This attribute can be used to query a device to determine the type of connection that has been established.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021



IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Figure 15 – Safety connection types

6.7.3.4 Ping interval EPI multiplier

This attribute is used as part of the Safety Validator function. This parameter is obtained from the Safety Segment Parameters in the SafetyOpen. The rules Multipoint producers shall follow for evaluating this parameter from multiple consumers are defined in Table 62.

6.7.3.5 Time Coord Msg min multiplier

This attribute is used as part of the Safety Validator function. This parameter is obtained from the Safety Segment Parameters in the SafetyOpen. The rules Multipoint producers shall follow for evaluating this parameter from multiple consumers are defined in Table 62.

Table 62 – Multipoint producer SafetyOpen parameter evaluation rules

Safety parameter	Producer evaluation rule	Error response (if appropriate)
Ping Interval EPI Multiplier	Shall match existing P.I.E.M. (first consumer sets it)	Invalid parameter
Time_Coord Msg Min Multiplier	Accept any (all can be different)	NA
Network Time Expectation Multiplier	Accept any (all can be different)	NA
Timeout Multiplier	Accept any (all can be different)	NA
Max Consumer Number	Shall match existing Max_Consumer_Number (first consumer sets it)	Invalid parameter

6.7.3.6 Network time expectation multiplier

This attribute defines the connection reaction time associated with this connection. This parameter is obtained from the Safety Segment Parameters in the SafetyOpen. The rules Multipoint producers shall follow for evaluating this parameter from multiple consumers are defined in Table 62.

6.7.3.7 Timeout multiplier

This attribute defines the tolerance the Safety Validator will have for lost messages before faulting a connection and taking a safety action. This parameter is obtained from the Safety Segment Parameters in the SafetyOpen. The rules Multipoint producers shall follow for evaluating this parameter from multiple consumers is defined in Table 62.

6.7.3.8 Max consumer number

This attribute defines the maximum number of consumers that are allowed to connect to a multipoint producer (Type 82). Both Multipoint Consumers and Producers have to know this value to function properly. This parameter is obtained from the Safety Segment Parameters in the SafetyOpen. The rules Multipoint producers shall follow for evaluating this parameter from multiple consumers is defined in Table 62.

6.7.3.9 Data connection instance

This attribute identifies the instance of the connection object responsible for the Safety Data connection. This attribute is assigned as part of the connection establishment process.

6.7.3.10 Coordination connection instance

This attribute identifies the instance of the connection object responsible for the Time Coordination connection. This attribute is assigned as part of the connection establishment process.

6.7.3.11 Correction connection instance

This attribute identifies the instance of the connection object responsible for the Time Correction connection if used. This attribute is assigned as part of the connection establishment process.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

6.7.3.12 CCO binding

This attribute identifies the Connection Configuration instance that was used to set up this safety connection. This binding is required to notify the CCO function when the connection is closed so that it can attempt to re-establish the connection. This attribute is only used in connection originators. This attribute may either be assigned as part of the connection establishment process or hard coded at design time.

6.7.3.13 Max data age

The data age of received packet data is defined as the difference between the consumer's 128 µs clock and received Time Stamp at the time the packet is received. The Max Data Age attribute is the maximum value this age has reached while the connection is/was established. The value can be used by diagnostic tools to fine tune the Network Time Expectation Multiplier.

The Max Data Age attribute shall always reflect the largest value the connection's data age reaches without exceeding the expectation multiplier.

If a safety connection is ever faulted and closed, the Max Data Age attribute shall be re-initialized to 0 when the connection is re-established.

6.7.3.14 Producer/Consumer Fault Counter

For connections which are using the Extended Format, this attribute reflects the internal Producer or Consumer Fault Counters.

When the connection is a EF Consuming connection, the Producer/Consumer Fault Counter attribute shall reflect the Consumer_Fault_Counters. When the connection is a EF Producing connection, the attribute shall reflect the Producer_Fault_Counter.

The attribute is used in the assessment tests which verify proper operation of the EF fault detection behavior.

6.7.4 Class services

The class services supported by the Safety Validator are defined in Table 63.

Table 63 – Safety Validator class services

Service code	Need in implementation	Name	Description of service
$0E_{hex}$	Required	Get_Attribute_Single	Used to read a Safety Validator object Class attribute value
$4B_{hex}$	Optional	Reset all error counters	Used to reset class attribute 8 in all instances

6.7.5 Instance services

6.7.5.1 Instance services overview

The instance services supported by the Safety Validator are defined in Table 64.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Table 64 – Safety Validator instance services

Service code	Need in implementation	Name	Description of service
01_{hex}	Optional	Get_Attribute_All	Returns the values of all instance attributes
$0E_{hex}$	Required	Get_Attribute_Single	Used to read a Safety Validator object attribute value
10_{hex}	Required	Set_Attribute_Single	Used to reset the Max Data Age Attribute
$4B_{hex}$	Optional	Reset error code	Used to reset instance attribute 14

6.7.5.2 Get_Attributes_All Response

The response data for the Get_Attributes_All service is defined in Table 65.

Table 65 – Safety Validator Get_Attributes_All service data

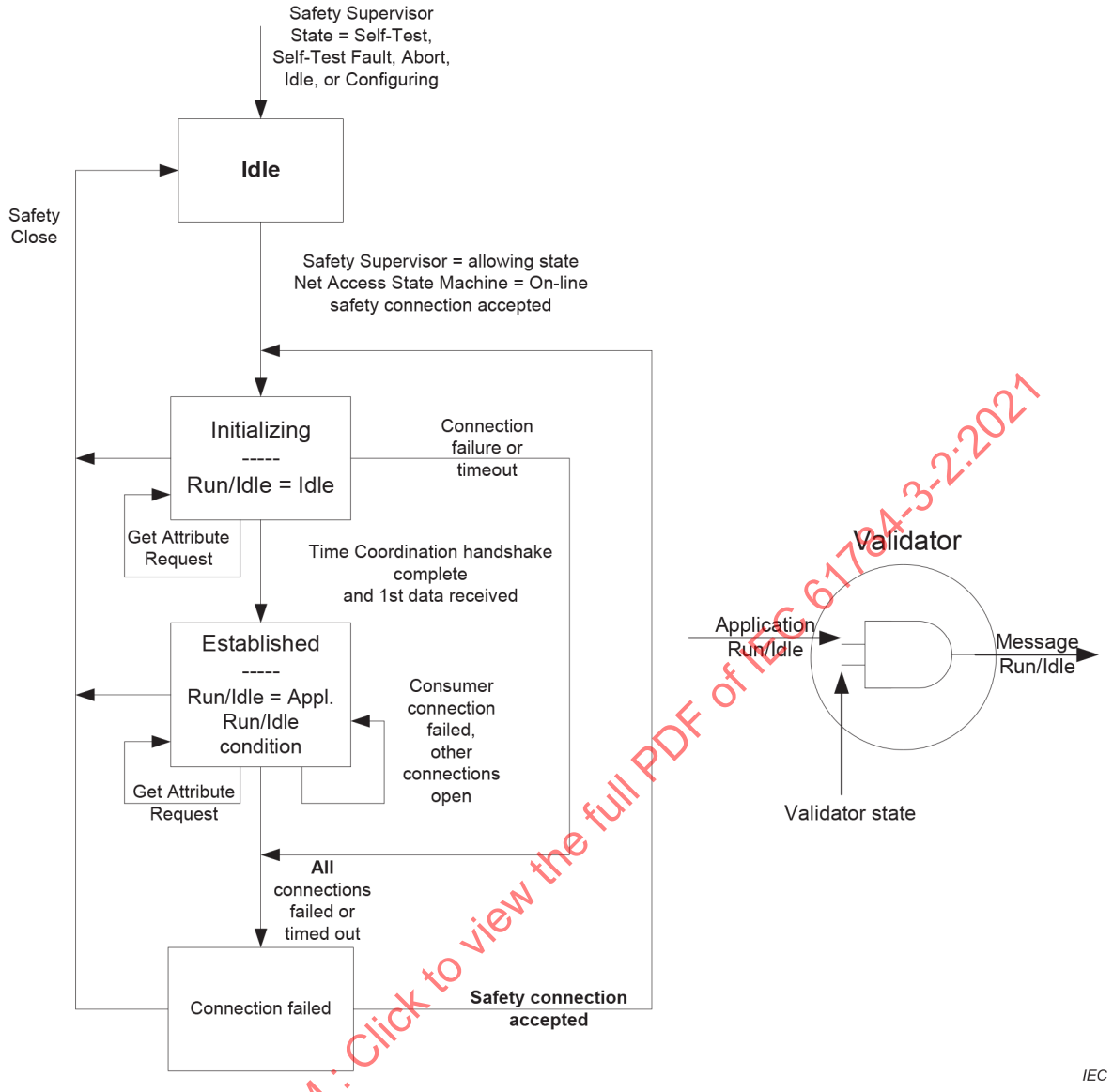
Attribute ID	Octet number	Name	Data type
1	0	Safety Validator State	USINT
2	1	Safety Validator Type	USINT
3	2,3	Ping Interval EPI Multiplier	UINT
4	variable	Time Coord Msg Min Multiplier	STRUCT
5	variable	Network Time Expectation	STRUCT
6	variable	Timeout Multiplier	STRUCT
7	variable	Max Consumer Number	USINT
8	variable	Data connection Instance	UINT = 0 if not supported
9	variable	Coordination Connection Instance	UINT = 0 if not supported
10	variable	Correction Connection Instance	STRUCT
11	variable	CCO Binding	UINT = 0 if not supported
12	variable	Max Data Age	UINT
13	variable	Application Path	Packed EPATH
14		Error Code	UINT

6.7.6 Object behavior

6.7.6.1 State transition diagram

The behavior of the Safety Validator object is illustrated in Figure 16 and Table 66.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021



IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Figure 16 – Safety Validator state transition diagram

6.7.6.2 IDLE

The Idle state is initial state entered after Power-up/Self-test. This state is the normal state when no connections are open or failed.

6.7.6.3 Initializing

For multipoint producers, this state exists for each consumer connection handled by the producer. For point-to-point producers and all consumers, this state relates to the entire Safety Validator connection.

6.7.6.4 Established

For multipoint producers, this state exists for each consumer connection handled by the producer. For point-to-point producers and all consumers, this state relates to the entire Safety Validator connection.

6.7.6.5 Connection_Failed

This state is entered when all connections associated with the Safety Validator have failed. It can remain in this state until either a SafetyClose is received, or the connection is re-established from a matching originator (i.e. OUNID and Application Path match a connection resource).

6.7.6.6 State event matrix

Table 66 is the state event matrix that defines the Safety Validator behavior. Table 67 maps the Safety Validator states to the Safety Supervisor states.

Table 66 – Safety Validator state event matrix

Event	State			
	Idle	Initializing	Executing	Connection failed
Power applied and Self-Test complete	Initial state	--	--	
Safety Supervisor = allowing state, Net Access State Machine = On-line, New safety connection requested	Validate Request and transition to Initializing	If multipoint producer, Initialize safety connection	If Multipoint producer, Initialize safety connection	Match OUNID and Application Path, If match, Transition to Initializing
Time coordination handshake complete	--	Transition to Executing	If multipoint producer, New Consumer On-line	--
Consumer fails in Multipoint producer while other consumers still on-line	--	Flash NET status LED Red	Flash NET status LED Red	--
All connections failed	--	Transition to Connection Failed	Transition to Connection Failed	Flash NET status LED Red
Matching consumer connection request (i.e. OUNID and Application path match a failed consumer connection)	--	Transition Consumer to Initializing	Transition Consumer to Initializing	Transition to Initializing
SafetyClose received	Success Reply, stay in Idle	Success Reply, Transition to Idle	Success Reply, Transition to Idle	Success Reply, Transition to Idle

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Table 67 – State mapping between Safety Supervisor and Safety Validator objects

Safety Supervisor	Safety Validator
Self-Testing	Idle
Self-Test Exception	Idle
Waiting for TUNID	Idle
Idle	Idle[a], Initializing Executing, or Connection_Failed
Configuring	Idle
Executing	Idle[a], Initializing or Executing, or Connection_Failed
Abort	Idle
Critical Fault	Idle

[a] A Safety Validator shall only accept connections when the Safety Supervisor is in the state that can accept connections which is device dependent (i.e. Executing only, or Execute/Idle). A Safety Validator instance could be Idle while another Safety Validator is still active.

6.8 Connection Configuration Object

6.8.1 General

This Subclause 6.8 defines the extensions to the Connection Configuration Object, Class $F3_{hex}$ for FSCP 2/1. See IEC 61158-4-2 for the complete definition.

Class Code: F3hex

6.8.2 Class attribute extensions

The class attributes for use by FSCP 2/1 devices are defined in Table 68.

Table 68 – Connection configuration object class attribute extensions

Attribute ID	Need in implem.	Access rule	Name	Data type	Description of attribute
9	Conditional[a]	Set	Edit Signature	UDINT	Created and used by configuration software to detect modifications to the instance attribute values

[a] This attribute is only required in devices not using the Safety SNCT interface.

6.8.3 Instance attributes, additions and extensions.

Table 69 defines the instance attributes and changes for use by FSCP 2/1 devices.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Table 69 – Connection Configuration Object instance attribute additions/extensions

Attr ID	Need in implem.	Access rule	NV	Name	Data type	Description of attribute	Semantics of value
9	Required	Set	NV	Data Map	STRUCT of:		
				format_number	UINT	This number determines the map format used	2-99 Reserved 100 – 199 Vendor Specific All other values are Reserved
				Data_Map data_size	UINT	Size, in octets, of Map information	
				Data_Map_data	Array of octet	Data Map format data based on Format number	
10	Optional	Set	NV	Config #2 Data2	STRUCT of:		
				config_data_size	UINT	Length of config_data in octets	
				config_data	Array of octet	Config # 2 data	
11	Optional	Set	NV	Proxy Device ID	STRUCT of:		
				vendor_id	UINT	Vendor ID	
				product_type	UINT	Device Type	
				product_ code	UINT	Product Code	
				major_rev	USINT	Major revision	
				minor_rev	USINT	Minor revision	
12	Conditional[a]	Set	NV	Connection Disable	BOOL		0 – connection is enabled. 1 – connection is disabled. When an Open service is received this value shall be set to 0. When a Close or Stop service is received this value shall be set to 1

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Attr ID	Need in implem.	Access rule	NV	Name	Data type	Description of attribute	Semantics of value
13	Conditional[a]	Set	NV	Safety Parameters	STRUCT of:		
				reserved	USINT	Reserved	Shall be zero
				reserved	USINT	Reserved	Shall be zero
				Configuration CRC	UDINT	CRC-S4 over the target device configuration data in Attribute 7 and 10	This value calculated by the configuration software on the data in Attr. 7 and10 after the configuration is applied
				Configuration Signature	DATE AND TIME		
				Time Correction EPI	UDINT		
				Time Correction Connection Parameters	WORD		
				Target UNID	10 octets		UNID of target device
				Reserved space for Originator UNID	10 octets	All zeros	Allows FW to easily stuff OUNID into safety segment
				Ping Int EPI Mult	UINT		
				Time Coord Msg Min Mult	UINT		
				Net Time Exp Mult	UINT		
				Timeout Multiplier	USINT		
				Max Consumer Number	USINT		
14	Conditional[a]	Get	NV	Connection Parameter CRC	UDINT	CRC-S4 over the connection parameters used in a SafetyOpen	This value is calculated by this device only once when the configuration is applied. It shall be readable by configuration software
15	Conditional[a]	Set	NV	Configuration Instance	UINT	Which object has configuration for this node	= 0 when no object assigned
16	Conditional[a]	Set	NV	Id Allocation	BOOL	When cleared, the originator will allocate the network Ids for its produced connections	0: allocate the Id for produced connections (default) 1; ask target for produced Ids
17	Conditional[a]	Get		Target Connection Serial Number	UINT	The instance # of the Target's Safety Validator. Target Connection Serial Number returned during connection establishment. Read by diagnostic tools	0 when connection is not established

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Attr ID	Need in implem.	Access rule	NV	Name	Data type	Description of attribute	Semantics of value
20	Conditional[b]	Set	NV	Format Type	USINT	Defines which format to use in connecting to a target	0 = Auto (default) 1 = "Base" 2 = "Extended"
21	Conditional[b]	Get	NV	Format Status	USINT	Indicates which format is currently in use when the Format Type is Auto (or if no agreement on a format could be obtained)	0 = Auto 1 = "Base" 2 = "Extended" 0xFF = "conflict detected"
22	Conditional[b]	Set	NV	Max Fault Number	UINT	Number of erroneous packets within one hour after which a connection is closed. Used by both producers and consumers.	Default = 5 A value of 0 indicates connections shall be closed on any detected error

[a] This attribute is required for a device which supports safety connections; otherwise this attribute is optional.

[b] This attribute is required for a device which supports the Extended Format; otherwise this attribute is optional.

6.8.4 Instance attribute semantics extensions or restrictions for safety

6.8.4.1 Connection flags – (Attribute 2)

Connection Flags are defined in Table 70.

Table 70 – Connection flag bit definitions

Bits	Definition for safety devices
Bit 0:	Connection Direction Always 0 = Originator of connection
Bit 1-3:	O-to-T Real time transfer format Always 101 = Safety Format
Bit 4-6:	T-to-O Real time transfer format Always 101 = Safety Format
Bit 7-15:	Not used. Always 0
Value:	$005A_{hex}$ = Originator $005B_{hex}$ = Target

6.8.4.2 CS Data Index Number – (Attribute 4)

CS Data Index is not used, shall be FFFF $FFFF_{hex}$.

6.8.4.3 Connection Timeout Multiplier – (part of Attribute 5)

Connection Timeout Multiplier for safety is used by the producer and consumer to timeout any of the 3 standard connections. It is used by the consumer of the connection to determine if the connection needs to timeout.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

The timeout value for the connection is defined as:

Connection RPI × (CTM + 1) × 4

Range: 0 to 7

where

0 = (0x4);

1 = (0x8);

2 = (0x12);

3 = (0x16);

4 = (0x20);

5 = (0x24);

6 = (0x28);

7 = (0x32).

Value: Always 1 (x8)

6.8.4.4 Transport Class and Trigger – (part of Attribute 5)

The value of the Transport Class and Trigger for safety is 20_{hex} for an Input Connection or $A0_{hex}$ for an Output Connection.

6.8.4.5 O-to-T RPI – (part of Attribute 5)

If direction is 0 (Client / T-to-O), then this is the Time Coordination RPI and the T-to-O RPI is the Data Production RPI.

If direction is 1 (Server / O-to-T), then this is the Data Production RPI and the T-to-O RPI is the Time Coordination RPI.

The Time Coordination RPI is defined as:

Range: 100 µs to 100 000 000 µs

Ping Interval EPI Multiplier × Data Production RPI

Data Production RPI

Range: 100 µs to 1 000 000 µs

6.8.4.6 O-to-T connection parameters – (part of Attribute 5)

O-toT connection parameters are defined in Table 71.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Table 71 – O-to-T connection parameters

Bits	Parameter	Value
0-8	Connection size (in octets)	If the direction is 1 (Server / O-to-T), it is the size of the Safety Message: If Data Size is 1-2 octets: Application Data Size + 6 If Data Size is 3-250 octets: (Application Data Size × 2) + 8 If the direction is 0 (Client / T-to-O), it is the size of the Time Coordination Message (6 octets) Range: 7-510
9	Fixed/Variable	Always 0 (Fixed)
10-11	Priority	Always 01 (High)
12	Reserved	Always 0
13-14	Connection Type	Always 10 (Point-to-point)
15	Redundant Owner	Always 0 (safety doesn't support redundancy)

6.8.4.7 T-to-O RPI – (part of Attribute 5)

If direction is 0 (Client / T-to-O), then this is the Data Production RPI and the O-to-T RPI is the Time Coordination RPI.

If direction is1 (Server / O-to-T), then this is the Time Coordination RPI and the O-to-T RPI is the Data Production RPI.

Value: see O-to-T RPI.

6.8.4.8 T-to-O Connection parameters – (part of Attribute 5)

The T-to-O connection parameters are defined in Table 72.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Table 72 – T-to-O connection parameters

Bits	Parameter	Value
0-8	Connection size (in octets)	If the direction is 0 (Client / T-to-O), it is the size of the Safety Message. For Point-to-point, see O-to-T Connection Parameters. For Multipoint with a Data Size of 1-2 octets: Application Data Size + 12 For Multipoint with a Data Size of 3-248 octets: (Application Data Size × 2) + 14 Multipoint calculations shall include the Time Correction Section. This is required for all multipoint connections to ensure the proper calculation of the CPCRC in the SafetyOpen. The value is fixed up by the Target Device. If the direction is 1 (Server / O-to-T), it is the size of the Time Coordination Message (6 octets). Range: 7-508
9	Fixed/Variable	Always 0 (Fixed)
10-11	Priority	Always 01 (High)
12	Reserved	Always 0
13-14	Connection Type	01 (Multipoint) 10 (Point-to-point) Default: 10 (Point-to-point)
15	Redundant Owner	Always 0 (safety doesn't support redundancy)

6.8.4.9 Connection Path (Attribute 6)

6.8.4.9.1 Connection Path size

The Connection Path Size is the number of 16-bit words stored in Connection Path. This path shall be adjusted to remove the size of the bridge path elements when the CPCRC is calculated (i.e. the size used in the calculation shall be the value the target will see after the bridge(s) have stripped away their segments and appropriately adjusted this size).

6.8.4.9.2 Connection Path

The connection paths associated with the connection in the following order: (1) Bridge Path, (2) Configuration Path, (3) Consumption Path, and (4) Production Path.

The bridge path (1) shall be separated by the originator from the application path 2, 3, and 4 at the time the SafetyOpen is built and when the CPCRC is calculated.

6.8.4.9.3 Bridge Path

Valid path constructed for the route between the originator and target.

6.8.4.9.4 Configuration Path

Valid path if configuration data is present in Attributes 7 or 8, or Null path otherwise. The path in all cases comes from the Target Applet (i.e. EDS File).

6.8.4.9.5 Target Consumption Path

Valid path if direction 1 (Server / O-to-T) or Null Path otherwise. The path in all cases comes from the Target Applet (i.e. EDS File).

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

6.8.4.9.6 Target Production Path

Valid path if direction is 0 (Client / T-to-O) or Null Path otherwise. The path in all cases comes from the Target Applet (i.e. EDS File).

6.8.4.10 Config # 1 Data Size (part of Attribute 7)

Usage is optional for Safety, zero if not used.

6.8.4.11 Config # 1 Data (part of Attribute 7)

Usage is optional for Safety and shall be concatenated with the contents of Config#2 data.

6.8.4.12 Config # 2 Data Size (part of Attribute 10)

Number of octets stored in Config #2 Data (below).

Range: 1 to < Max Allowable Configuration Size>

6.8.4.13 Config # 2 Data (part of Attribute 10)

Used to store the target device's configuration data.

6.8.4.14 Data Map (Attribute 9)

6.8.4.14.1 Map format allocation

Table 73 defines a set of map formats that are currently defined in the standard range. The vendor specific range is still available to be used for special map formats.

Table 73 – Data map formats

Format number	Format name	Data Map data Size (in octets)	Data Map data	Comment
0	Open scanner format.	4 octets	See Table 74	Simple format which maps data in word granularity to input and output image tables
1	Octet-Index Scanner format	4 octets	See Table 75	Simple format which maps data in octet granularity to input and output image tables
2-99	Reserved			
100-199	Vendor specific			
200 – 65 535	Reserved			

6.8.4.14.2 Format 0 usage for safety scanners

Data map format 0 contains the Map Data structure using the format described in Map Format Type, defined in Table 74.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Table 74 – Data map format 0

Name	Data type	Description	Value
Originator to Target data image offset	UINT	The offset, in 16 bit units, in the originator to target image table	If the direction is 0 (Client / T-to-O): Always 0. If the direction is 1 (Server / O-to-T): Word offset into the Safety Output Data Table
Target to Originator data image offset	UINT	The offset, in 16 bit units, in the target to originator image table	If the direction is 0 (Client / T-to-O): Word offset into the Safety Input Data Table. If the direction is 1 (Server / O-to-T): Always 0

6.8.4.14.3 Format 1 usage for safety scanners

Data map format 1 contains the Map Data structure using the format described in Map Format Type, defined in Table 75.

Table 75 – Data map format 1

Name	Data type	Description	Value
Originator to Target data image offset	UINT	The offset, in 8 bit units, in the originator to target image table	If the direction is 0 (Client / T-to-O): Always 0. If the direction is 1 (Server / O-to-T): octet offset into the Safety Output Data Table
Target to Originator data image offset	UINT	The offset, in 8 bit units, in the target to originator image table	If the direction is 0 (Client / T-to-O): octet offset into the Safety Input Data Table. If the direction is 1 (Server / O-to-T): Always 0

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

6.8.4.15 Proxy Device ID

Proxy Device ID is never used.

6.8.4.16 Connection Disable (Attribute 12)

When the Connection Disable attribute in the CCO object is TRUE, the connection shall remain disabled through power cycles. When the Connection Disable attribute in the CCO object is FALSE, the connection shall remain enabled through power cycles.

6.8.5 Special Safety Related Parameters – (Attribute 13)

6.8.5.1 Ping Interval EPI Multiplier

This attribute is used as part of the safety Validator function. This parameter is part of the Safety Segment Parameters in the SafetyOpen. Ping_Interval_EPI_Multiplier is the number that defines the Ping_Count_Interval for the safety connection.

Devices implementing the safety extensions to the CCO object shall perform a range check on the Ping Interval EPI Multiplier during a Validate_Configuration request.

Ping Interval EPI Multiplier usage is defined as follows:

Range: [Max_Consumer_Number × Timeout_Multiplier.PI +15] to 1 000.

Default:

If the direction is 0 (Client / T-to-O): 100

If the direction is 1 (Server / O-to-T): 19

6.8.5.2 Time Coord Msg Min Multiplier

This attribute is used as part of the Safety Validator function. This parameter is obtained from the safety segment parameters in the SafetyOpen. Time_Coord_Msg_Min_Multiplier is the minimum number of 128 µs increments it could take for a Time Coordination Message to traverse from the consumer to the producer. The default is 0.

Devices implementing the safety extensions to the CCO object shall perform a range check on the Time_Coord_Msg_Min_Mulitiplier during a Validate_Configuration request.

Time Coord Msg Min Multiplier usage is defined as follows:

Range: 0 to 7 813, which equates to 0 s to 1 s.

Default: 2 for non-bridge; 3 or more when bridging is added.

6.8.5.3 Network Time Expectation Multiplier

This attribute is used as part of the Safety Validator function. This parameter is part of the safety segment parameters in the SafetyOpen. Network_Time_Expectation_Multiplier is the maximum number of 128 µs increments that a consumer shall allow the age of the safety data to reach.

Device implementing the safety extensions to the CCO object shall perform a range check on the Network_Time_Expectation_Multiplier during a Validate_Configuration request.

Network Time Expectation Multiplier usage is defined as follows:

Range 0 to 45 313, which equates to 0 s to 5,8 s.

Equation See details in 8.8.4.

6.8.5.4 Timeout Multiplier

This attribute is used as part of the Safety Validator function. This parameter is part of the safety segment parameters in the SafetyOpen.

Device implementing the safety extensions to the CCO object shall perform a range check on the Timeout_Multiplier during a Validate_Configuration request.

Timeout Multiplier usage is defined as follows:

Range Base Format	1 to 4
Range Extended Format	1 to 255
Default	2

6.8.5.5 Max Consumer Number

This attribute defines the maximum number of consumers that are allowed to connect to a multipoint producer (Type 2). Both Multipoint Consumers and Producers needs to know this value to function properly. This attribute is used as part of the safety Validator function. This parameter is part of the Safety Segment Parameters in the SafetyOpen.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Device implementing the safety extensions to the CCO object shall perform a range check on the Max Consumer Number during a Validate_Configuration request.

Max Consumer Number usage is defined as follows:

Range: 1 to 15
Default: 15
Value: Comes from the Target Applet (i.e. EDS File)

6.8.5.6 Target Connection UNID

This attribute is the UNID of the target safety device for this connection. This parameter is part of the Safety Segment Parameters in the SafetyOpen and is checked by the target device to confirm the request didn't get misrouted. The only way to confirm this value is correct is through user testing of the connection.

Target UNID format on CP 2/3 is defined as follows:

OCTET 0-5: Safety Network Number
OCTET 6: CP 2/3 MACID
OCTET 7-9: Always 0 for CP 2/3

6.8.5.7 Safety Configuration CRC (SCCRC)

The SCCRC serves as a signature for the device configuration and can be used to confirm the integrity of the configuration over time. The configuration software shall calculate the SCCRC over the configuration data in the exact order it appears in the SafetyOpen message. This same calculation is done by target devices and compared to this value.

The SCCRC shall be calculated over the configuration data by the device whenever a device configuration is validated (i.e. Validate_Configuration Request to the safety supervisor or type 1 safety connection).

The SCCRC shall be saved to NV storage along with the other NV attributes whenever a configuration is applied (i.e. apply request to the safety supervisor).

The user shall be instructed in the safety manual to test safety connection configurations after they are applied in an originator to confirm the target connection is operating as intended.

The target device's SCCRC usage is shown in Table 76.

Table 76 – Target device's SCCRC values

Safety connection type	SCCRC value
Type 1	SCCRC identifying configuration data in Config #2 Data
Type 2a	SCCRC identifying the expected target device configuration
Type 2b	0

6.8.5.8 Safety Configuration Signature (Time Stamp)

The target device's SCTS values are shown in Table 77.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Table 77 – Target device's SCTS values

Safety connection type	SCTS value
Type 1	SCTS identifying configuration data in Config #1 Data
Type 2a	SCTS identifying the expected target device configuration
Type 2b	0

6.8.5.9 Time Correction EPI

This parameter defines the EPI for the Time Correction Message used in a multipoint connection.

The Value for a multipoint connection is:

Ping Interval EPI Multiplier × Data Production RPI;

Otherwise 0.

6.8.5.10 Time Correction Connection Parameters

Defines the Connection Parameters used in the Time Correction Message used in a multipoint connection.

The value is 0000_{hex} for a non Multipoint connections or 2406_{hex} for a Multipoint connection, defined as showin Table 78.

Table 78 – Time correction connection parameters for multipoint connection

Bits	Parameter	Value
0-8	Connection size (in octets)	Size of the Time Correction Message which is 6 octets
9	Fixed/Variable	Always 0 (Fixed)
10-11	Priority	Always 01 (High)
12	Reserved	Always 0
13-14	Connection Type	01 (Multipoint)
15	Redundant Owner	Always 0 (safety doesn't support redundancy)

6.8.5.11 Connection Parameter CRC (CPCRC) – (Attribute 14)

The Connection Parameter CRC attribute shall be calculated by this originator device whenever the originator's configuration is validated (i.e. Validate_Configuration request to the safety supervisor).

The CPCRC shall be saved to NV storage along with the other NV attributes whenever a configuration is applied (i.e. apply request to the safety supervisor).

The user should be required to test this connection after it is applied to confirm the connection configuration. From that point on, the CPCRC serves as a signature for that connection configuration and can be used to confirm the integrity of the configuration over time. The calculation itself is done over the connection parameters in SafetyOpen in the exact order they appear in the message. This same calculation is done by target devices and compared to this value, so the exact order shall be followed.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

6.8.5.12 Configuration Instance – (Attribute 15)

This attribute provides the linkage to the instance of the object assigned to this connection. The attribute may be used when the target's configuration data cannot be sent via the SafetyOpen. A value of 0 (default) for this attribute indicates that no object is assigned.

6.8.5.13 Id Allocation

This Boolean attribute is used to give the user some flexibility in how originators allocate Ids on connection establishment. This is particularly important for FSCP 2/1 on CP 2/3. The default behavior is for the originator to provide Ids for the connections in which it is the producer. If the user sets this attribute, the originator will instead ask the Target to provide an Id for these produced connections. A user may want to do this when the originator has a large number of connections and does not have enough to do the application. This attribute only applies to non-multipoint productions (multipoint productions shall always be allocated by the producer). This function is considered an advanced function and great care should be taken when presenting this feature to a user. The user shall be advised it should only used in limited application scenarios where connection repeatability can be guaranteed.

6.8.5.14 Format Type

Table 79 defines the meaning of the Format Type attribute.

Table 79 – Format Type attribute meaning

Format Type Value Name	Meaning
Auto	The Originator will determine which format to use at first connection establishment
Base	The Originator will use the existing format at the next connection establishment
Extended	The Originator will use the Extended Format at the next connection establishment

If the Format Type attribute is not set it will default to Auto the originator will determine which format to use. If the Format Type attribute is optionally configured to "Base", the originator will only use the "Base" format. If the Format Type attribute is optionally configured to "Extended", the originator will only use the "Extended" format.

If the Format Type is Base or Extended and a Target responds with a "Invalid Safety Connection Format" Error (0x01, 0x803) or "Invalid Safety Connection Size" Error (0x01, 0x802), the Format Status attribute shall be set to 0xFF (Conflict Detected).

The Format Type attribute can not be changed while the connection is active. If the format is set to Auto, the following logic shown in Figure 17 shall be used:

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

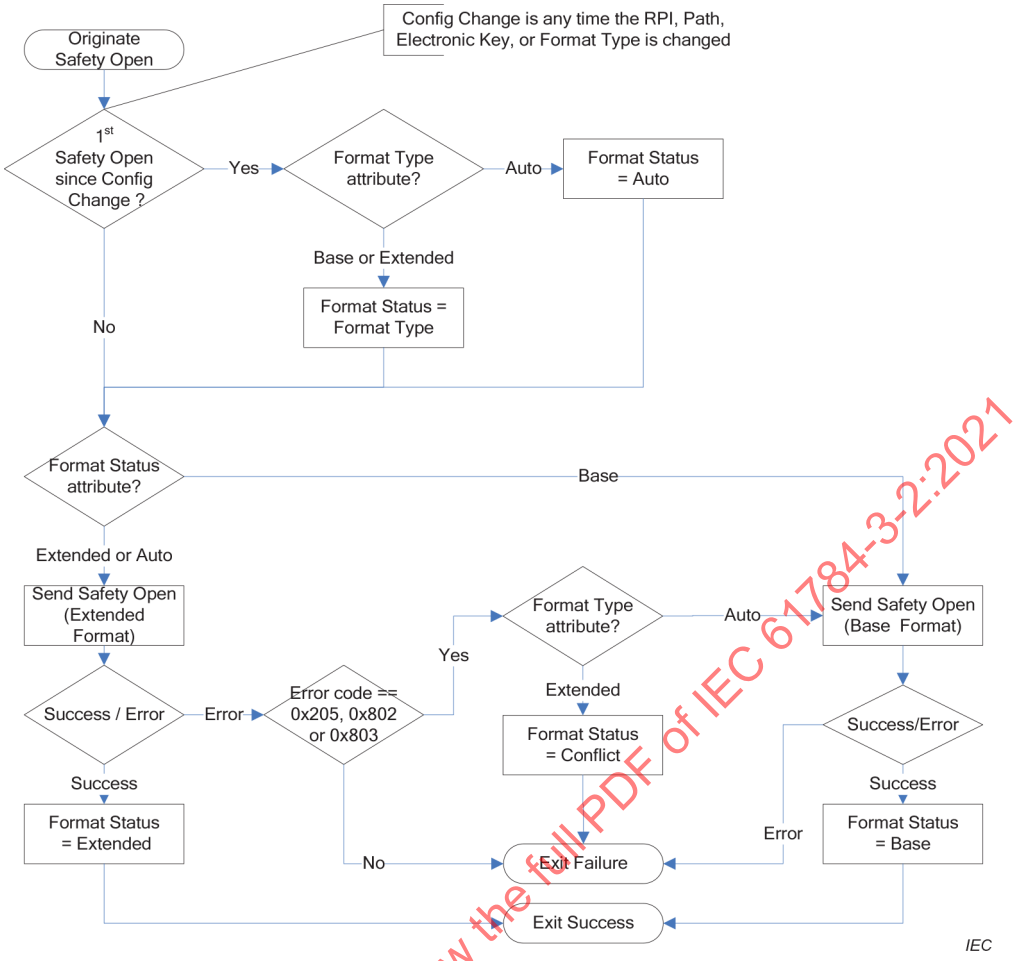


Figure 17 – Logic for Auto-detecting format type

6.8.5.15 Format Status

Table 80 defines the meaning of the Format Status attribute.

Table 80 – Format Status attribute meaning

Format Status Value Name	Meaning Originator	Meaning Target
Auto	The Originator has not yet determined which format to use	NA
"Base"	If Format Type is Auto The Originator has determined target requires old format If Format type is 'Base, The originator will only connect with old format If Format type is 'Extended This condition should never occur	The target is using the "Base" format
"Extended"	If Format Type is Auto The Originator has determined target will accept new format If Format type is 'Base, The condition should never occur If Format type is 'Extended The originator will only connect with the new format	The target is using the "Extended"
"Conflict Detected"	If Format type is Base or Extended and Segment type errors are received, there is setting conflict between Target and Originator. This status flags this condition	The target is receiving SafetyOpen requests for a format it doesn't support

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

6.8.6 Object-specific services

The Connection Configuration Object provides the following Object Specific Services, defined in Table 81.

Table 81 – Connection Configuration Object-specific services

Service	Need in implementation		Service name	Description of service
	Class	Instance		
$4B_{hex}$	Conditional[a]	N/A	Kick-Timer	Kicks Edit Watchdog Timer
$4C_{hex}$	Optional	Conditional[b]	Open	Opens connections
$4D_{hex}$	Optional	Conditional[b]	Close	Closes connections
$4E_{hex}$	Optional	Conditional[b]	Stop	Stops connections
$4F_{hex}$	Conditional[a]	N/A	Change Start	Manages session editing
50_{hex}	Required	N/A	Get Status	Get status for multiple connections
51_{hex}	Conditional[a]	N/A	Change Complete	Completes session editing
52_{hex}	Conditional[a]	N/A	Audit Changes	Audits pending changes

[a] Safety devices shall not implement these services since the software configuration tool will coordinate configuration through the Safety Supervisor.

[b] Safety devices shall support the Open, Close and Stop services. These services shall only be accepted when the device is unlocked. If the device is locked, it shall respond with a "Device state conflict" error.

6.8.7 Common service extensions for safety

6.8.7.1 Get Attribute All (Service Code 01_{hex})

The added attributes to the end of the Get_Attribute_All response are defined in Table 82 and Table 83. All other parameters of this service are as defined in the standard CCO object in IEC 61158-5-2 and IEC 61158-6-2.

Table 82 – Get_Attributes_All Response service data (added attributes)

Name	Data type	Description
Safety Parameters	STRUCT of:	
	USINT	Pad, set to zero
	USINT	Pad, set to zero
	UDINT	Configuration CRC (SCCRC)
	DATE AND TIME	Configuration Time Stamp (SCTS)
	UDINT	Time Correction EPI
	WORD	Time Correction Connection Parameters
	10:octets	Target UNID
	10:octets	Pad, set to zero
	UINT	Ping Int EPI Mult
	UINT	Time Coord Msg Min Mult
	UINT	Net Time Exp Mult
	USINT	Timeout Multiplier
	USINT	Max Consumer Number

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Name	Data type	Description
Connection Parameter CRC	UDINT	CRC-32 over the connection parameters used in a SafetyOpen
Configuration Instance	UINT	
ID Allocation Flag	BOOL	
Target Connection Serial Number	UINT	Safety Validator Instance returned from Target during connection establishment

Table 83 – Get_Attributes_All Response service data (added parameters)

Name	Data type	Description
Length	USINT	Length of additional safety paramters = 4
Format Type	USINT	
Format Status	USINT	
Max Fault Number	UINT	

6.8.7.2 Set_Attribute_All (Service Code 02_{hex})

The added attributes to the end of the Set_Attribute_All response shall be extended as defined in Table 84 and Table 85. All other parameters of this service are as defined in the standard CCO object in IEC 61158-5-2 and IEC 61158-6-2.

Table 84 – Set_Attributes_All Request service data (added attributes)

Name	Data type	Description
Safety parameters	STRUCT of:	
	USINT	Pad, set to zero
	USINT	Pad, set to zero
	UDINT	Configuration CRC (SCCRC) (value set = 0, device does this calc)
	DATE AND TIME	Configuration Time Stamp (SCTS) (if applicable, else = 0)
	UDINT	Time Correction EPI
	WORD	Time Correction Connection parameters
	10octets	Target UNID
	10octets	Pad, set to zero
	UINT	Ping Int EPI Mult
	UINT	Time Coord Msg Min Mult
	UINT	Net Time Exp Mult
	USINT	Timeout Multiplier
	USINT	Max Consumer Number
Configuration instance	UINT	
ID Allocation flag	BOOL	

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Table 85 – Set_Attributes_All Response service data (added parameters)

Name	Data type	Description
Length	USINT	Length of additional safety paramters = 3
Format Type	USINT	
Max Fault Number	UINT	

6.8.7.3 Restore (Service Code 15_{hex})

Safety devices shall not implement the Restore service at either class or instance level since the configuration tool will coordinate configuration through the Safety Supervisor.

6.8.8 Object behavior

The Connection Configuration object behavior for safety devices shall be controlled by the Safety Supervisor and follow the behavior defined in Table 86, Figure 18, and Figure 19.

Table 86 – State Mapping between Safety Supervisor and the CCO objects

Safety Supervisor	Connection Configuration
Self-Testing	Edits not allowed
Self-Test exception	Edits not allowed
Idle	Edits not allowed
Configuring	Edits allowed
Executing	Edits not allowed
Abort	Edits not allowed
Critical fault	Edits not allowed

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

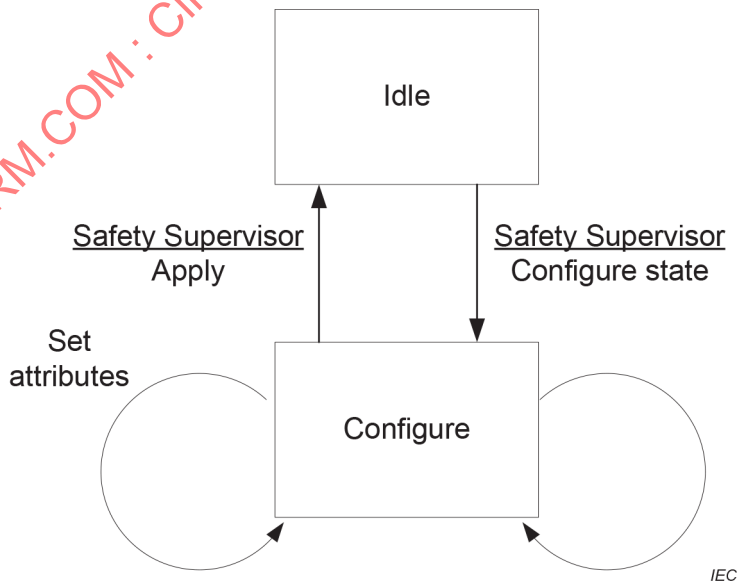


Figure 18 – Connection Configuration Object state diagram

The Data flow for the Connection Configuration object while in the Configure State is defined in Figure 19.

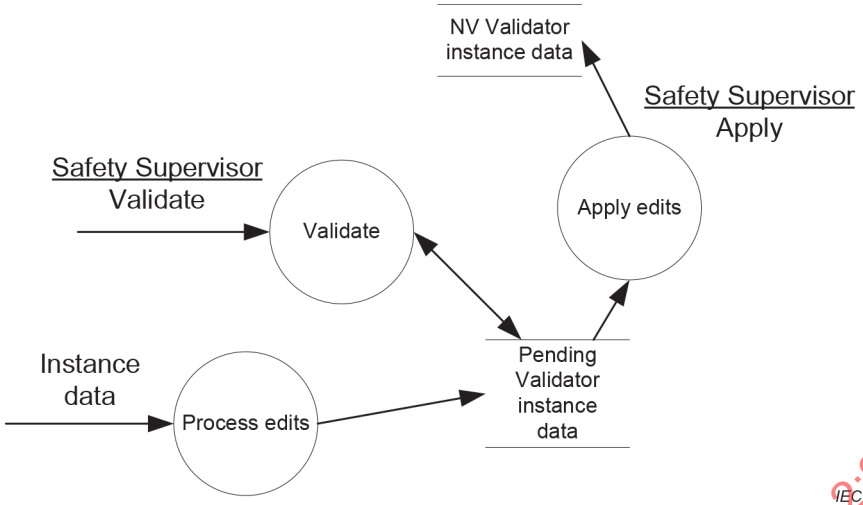


Figure 19 – Connection Configuration Object data flow

7 Safety communication layer protocol

7.1 Safety PDU format

7.1.1 Safety PDU encoding

7.1.1.1 General encoding rules

The Safety Protocol defines nine section encoding formats that are used in different combinations for safety messaging. The nine types of section encoding formats are:

- BF 1 or 2 octet data section (see 7.1.1.4),
- EF 1 or 2 octet data section (see 7.1.1.4),
- BF 3 to 250 octet data section (see 7.1.1.6),
- EF 3 to 250 octet data section (see 7.1.1.6),
- BF Time stamp section (see 7.1.1.8),
- BF Time coordination section (see 7.1.1.9),
- EF Time coordination section (see 7.1.1.9),
- BF Time correction section (see 7.1.1.9).
- EF Time correction section (see 7.1.1.9).

These section encodings are used to construct six safety message types of connection formats. In all six message types, both the Base Format and the Extended Format can be used. The six types of connection formats are:

- 1 or 2 octet point-to-point (see 7.1.1.13),
- 1 or 2 octet Multipoint Format 1 (see 7.1.1.14),
- 1 or 2 octet Multipoint Format 2 (see 7.1.1.15),
- 3 to 248 octet Multipoint Format 1 (see 7.1.1.16),
- 3 to 248 octet Multipoint Format 1 (see 7.1.1.17),
- 3 to 248 octet Multipoint Format 2 (see 7.1.1.18).

Table 87 defines which sections are used within the various message types for the six different connection format types:

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Table 87 – Connection sections and PDU formats

Safety Connection format			Message types					
			Data message[b]				Time Coordination message[b]	Time Correction message
Data size	Safety Connection type	Network hop type	1 or 2 octet data section	3 to 250 octet data section	Time Stamp section[a]	Time Correction section	Time Coordination section	Time Correction section
1 or 2 octets	Point-to-point	All	X		X[a]		X	
	Multipoint	CP 2/3	X		X[a]		X	X
		CP 2/2	X		X[a]	X	X	
3 to 248 octets	Point-to-point	All		X	X[a]		X	
	Multipoint	CP 2/3		X	X[a]		X	X
		CP 2/2		X	X[a]	X	X	

[a] Base Format has independent section for Time Stamp; it is part of the data section in the Extended Format.

[b] Message can use either Base or Extended Format.

Originators and targets shall follow selection criteria shown in Table 88 for the usage of the Base and Extended Formats.

The Base Format is deprecated from FSCP 2/1. FSCP 2/1 requires that only the extended format be used.

Table 88 – Connection sections and message format

Type	Base Format	Extended Format
Originator	Deprecated[a]	Required
Target	Deprecated[a]	Required

[a] Optional for backward compatibility support.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

7.1.1.2 Mode octet

The Mode octet is described outside of the section definitions because various parts are included in the various section CRCs. The layout of the Mode octet is defined in Figure 20. In the Base Format, bits 0 to 4 of the mode octet are part of the time stamp section, while bits 5 to 7 are part of the data sections. In the short packet Extended Format, bits 5 to 7 are part of the data CRC. In the large packet Extended Format, bits 0 to 4 of the mode octet are part of the complement data CRC, while bits 5 to 7 are part of the true data CRC. The variables used in the mode octet, brief descriptions and references to complete descriptions are given in Table 89.

Mode Octet							
7	6	5	4	3	2	1	0
Run_Idle	TBD_2_Bit	TBD_Bit	N_Run_Idle	TBD_2_Bit_Copy	N_TBD_Bit	Ping_Count	
N_Run_Idle[a]	N_TBD_2_Bit[a]	N_TBD_Bit[a]					

[a] The values are not sent in the data packet, there are derived by the consumer.

Figure 20 – Format of the mode octet

Table 89 – Mode octet variables

Name	Description	Reference
Run_Idle	Run_Idle shall be used to indicated the usability of the data as determined by the Producer Safety-related application	7.7.1.1
N_Run_Idle	Complement of the Run_Idle	7.7.1.2
TBD_2_Bit	Reserved for future use	7.7.1.3
TBD_2_Bit Copy	Copy of the TBD_2_Bit	7.7.1.4
TBD_Bit	Reserved for future use The TBD_Bit Shall be set to 0 by the Safety Validator	7.7.1.6
N_TBD_Bit	Complement of the TBD_Bit	7.7.1.7
Ping_Count	The ping count is used for determining when a consumer shall send a time coordination message	7.7.1.5

7.1.1.3 Mode octet CRC processing for Base Format

The Mode octet processing within the BF CRCs shall be done as follows:

- CRC Type Mode Octet logic prior to inclusion within the CRC;
- Actual Data CRC Mode Octet AND $E0_{hex}$;
- Complement Data CRC (Mode Octet XOR FF_{hex}) AND $E0_{hex}$;
- Time Stamp Section CRC Mode Octet AND $1F_{hex}$.

7.1.1.4 1 or 2 octet data section, Base Format

The 1 or 2 octet data section shall consist of the actual data octet or octets, the mode octet, the actual CRC, and the complement CRC. The layout of the 1 or 2 octet data section is defined in Figure 21.

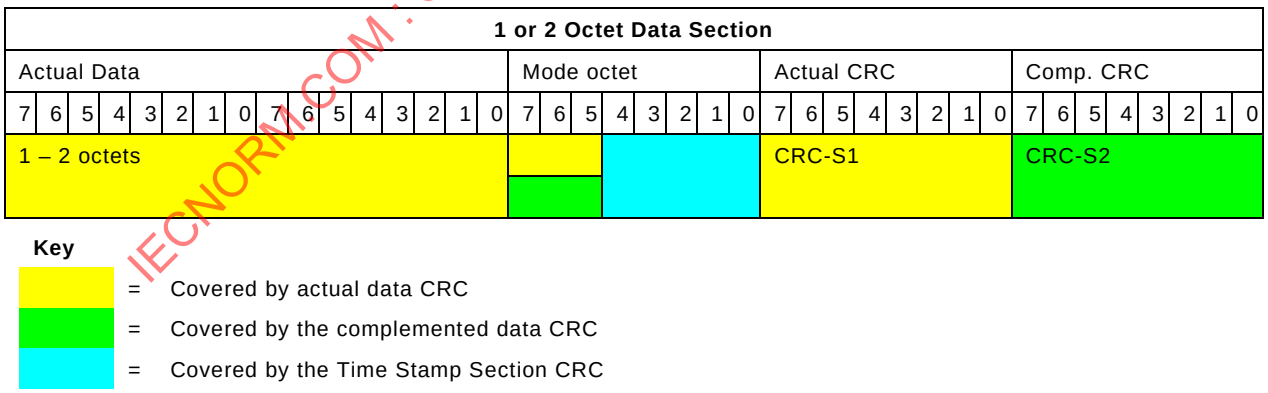


Figure 21 – 1 or 2 octet data section, Base Format

The BF 1 or 2 Octet Actual Data CRC calculation shall include:

- Producer Identifier (PID) (by CRC-S1);
- The (Mode Octet) AND ($E0_{hex}$) (by CRC-S1);
- Actual Data octet(s) (by CRC-S1).

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

The BF 1 or 2 Octet Complement Data CRC calculation shall include:

- Producer Identifier (PID) (by CRC-S1);
- The (Mode Octet XOR FF_{hex}) AND ($E0_{hex}$) (by CRC-S2);
- Complemented Data octets XOR FF_{hex} (by CRC-S2).

NOTE The PID uses CRC-S1 for both the actual and the complement CRC calculation.

7.1.1.5 1 or 2 octet data section, Extended Format

The 1 or 2 octet data section for the Extended Format shall consist of the actual data octet or octets, the mode octet, the time stamp, and CRC-S5 calculated over the entire packet. The format of the 1 or 2 octect data section, Extended Format is shown in Figure 22.

1 – 2 Octet Data Section, Extended Format					
Actual Data	Mode Octet[a]	CRC S5		Time Stamp	CRC S5
2 octets	1 octet	2 octets		2 octets	1 octet
1 – 2 Octets		CRC-S5_0	CRC-S5_1	Time Stamp	CRC-S5_2

[a] Bits 0-4 are not included in the CRC calculation.

Key

= Covered by CRC S5

Figure 22 – 1 or 2 octet data section, Extended Format

The EF 1 or 2 octect data section CRC calculation shall use CRC-S5 and include:

- Producer Identifier (PID);
- 16-bit Rollover count;
- Mode Octet AND ($E0_{hex}$);
- Actual Data octet(s);
- Time Stamp.

7.1.1.6 3 to 250 octet data section, Base Format

The 3 to 250 octet data section shall consist of the actual data octets, the mode octet, the actual CRC, the complement data octets, and the complement CRC. The layout of the 3 or 250 Octet Data section is defined in Figure 23.

3 – 250 octet Data Section				
Actual Data	Mode octet	Actual CRC	Complemented Data	Comp. CRC
3 – 250 octets		CRC-S3	3-250 octets	CRC-S3

Key

= Covered by actual data CRC

= Covered by the complemented data CRC

= Covered by the Time Stamp Section CRC

Figure 23 – 3 to 250 octet data section format, Base Format

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

The BF 3-to-250 octet actual data CRC calculation shall include:

- Producer Identifier (PID) (by CRC-S3);
- The (Mode Octet) AND ($E0_{hex}$) (by CRC-S3);
- Actual Data octet(s) (by CRC-S3).

The BF 3-to-250 octet complement data CRC calculation shall include:

- Producer Identifier (PID) (by CRC-S3);
- The (Mode Octet XOR FF_{hex}) AND ($E0_{hex}$) (by CRC-S3);
- Complemented Data octets XOR FF_{hex} (by CRC-S3).

7.1.1.7 3 to 250 octet data section, Extended Format

The EF 3 to 250 Octet Data section shall consist of the actual data octets, the mode octet, CRC-S3, the complement data octets, the time stamp and CRC-S5. The EF 3 to 250 octet data section is shown in Figure 24.

3-250 Octet Extended Format							
Actual Data	Mode Octet		Actual Data CRC	Complement Data	Complement Data CRC	Time Stamp	Compl. Data CRC
3-250 octets	1 octet		2 octets	3 – 250 octets	2 octets	2 octets	1 octet
3 – 250 Octets			CRC-S3	Complement 3-250 Octets	CRC-S5_0 CRC-S5-_1	Time Stamp	CRC-S5_2

Figure 24 – 3 to 250 octet data section format, Extended Format

The EF 3-to250 Octet Actual Data CRC calculation shall include:

- Producer Identifier (PID) *(by CRC-S3)*;
- Rollover Count *(by CRC-S3)*;
- The (Mode Octet) **AND** (0xE0) *(by CRC-S3)*;
- Actual Data octet(s) *(by CRC-S3)*.

The EF 3-to250 Octet Complement Data CRC calculation shall include:

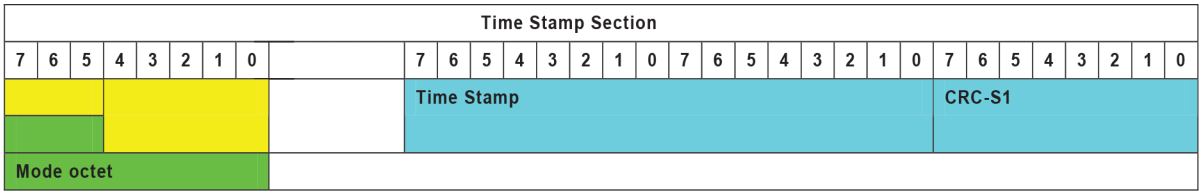
- Producer Identifier (PID) *(by CRC-S5)*;
- Rollover Count *(by CRC-S5)*;
- Mode Octet **AND** 0x1F *(by CRC-S5)*;
- Actual Data octets **XOR** 0xFF *(by CRC-S5)*;
- Time Stamp *(by CRC-S5)*.

7.1.1.8 Time Stamp section, Base Format

The Time Stamp section is composed of the mode octet, the Time_Stamp, and the time stamp CRC. The layout of the Time Stamp section is defined in Figure 25.

Descriptions of the Time Stamp section variables is defined in Table 90.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021



IEC

Key

= Covered by actual data CRC

= Covered by the complemented data CRC

= Covered by the Time Stamp Section CRC

Figure 25 – Time Stamp section format, Base Format

Table 90 – Time Stamp variables

Name	Description	Reference
Data_Time_Stamp	Point-to-point -- Data_Time_Stamp is the time the data was sampled for production relative to the consumers clock. Multipoint -- Data_Time_Stamp is the time the data was sampled for production relative to the producers clock	7.7.2

The BF Time Stamp CRC calculation shall include:

- Producer Identifier octet (PID) (by CRC-S1);
- The (Mode Octet) AND ($1F_{hex}$) (by CRC-S1);
- Time Stamp octet(s) (by CRC-S1).

7.1.1.9 Time Coordination section

The Time Coordination section shall be sent from the consumer to the producer in response to a change in the ping count.

The Time Coordination section is used as the Time Coordination Message for all point-to-point and multipoint time coordination requests. There are two formats: the Base Format (BF) and Extended Format (EF).

The encoding for the BF time coordination section is defined in Figure 26 and the EF time coordination section is defined in Figure 27. The variables used in the time coordination section, brief descriptions and references to complete descriptions are given in Table 91.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

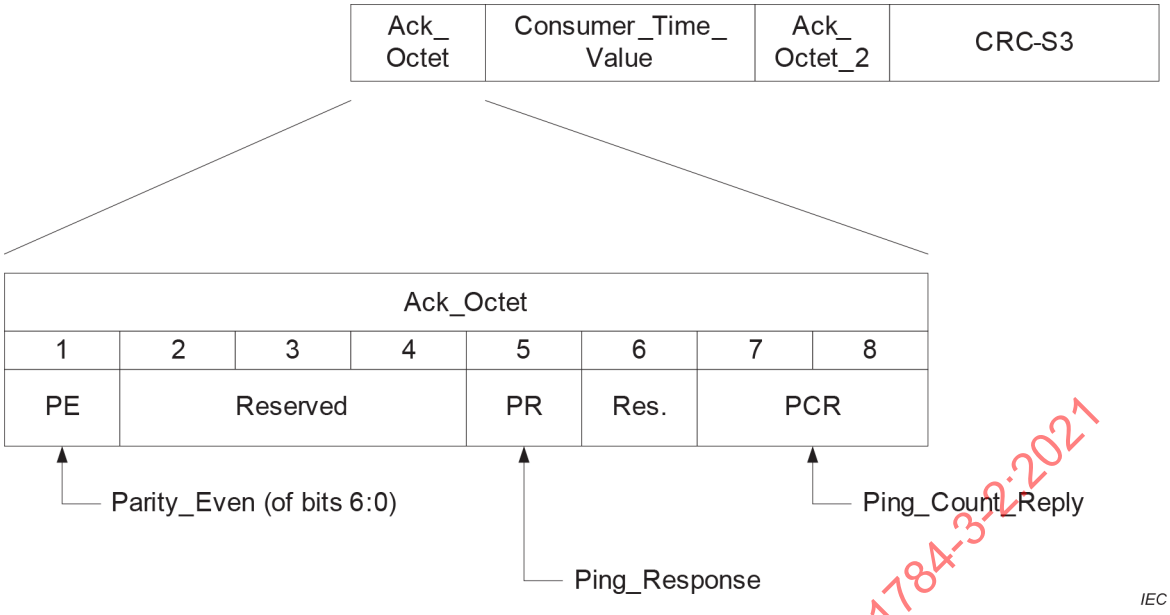


Figure 26 – BF Time Coordination message encoding

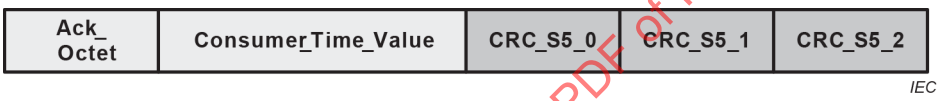


Figure 27 – EF Time Coordination message encoding

Table 91 – Time Coordination message variables

Name	Description	Reference
Consumer_Time_Value	Consumer_Time_Value in the Time Coordination message shall (as closely as possible) mark the time at which the consumer sends a ping response message	7.7.3.2
Ack_Octet	Consisting of:	
Parity_Even	The Parity_Even bit in the Time Coordination message shall be even parity of bits 0 to 6 of the message	
Ping_Response_Bit	The Ping_Response_Bit in the Time Coordination message shall indicates that a ping response is being sent	7.7.3.1
Ping_Count_Reply	Ping_Count_Reply in the Time Coordination message shall indicates which ping request the consumer is responding to	7.7.3.3
Reserved	Reserved, set to zero	
CRC-S3	CRC covering the data within the BF time coordination message	
CRC-S5	CRC covering the data within the EF time coordination message	

The following rule shall be used for the calculation of the parity bit in the Time Coordination message:

Bit 7 of the Ack_Octet form even parity on the Ack_Octet.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

The following rule shall be used for setting of the bits in Ack_Octet_2 of the Time Coordination message:

Ack_Octet_2 = ((Ack_Octet XOR FF_{hex}) AND 55_{hex}) OR (Ack_Octet AND AA_{hex}).

When a connection is established with the Extended Format, the EF Time Coordination format shall be used; otherwise the BF Time Coordination format shall be used.

7.1.1.10 Time Coordination CRC calculation

The Time Coordination CRC calculation shall include:

- Consumer Identifier (CID) (by CRC-S3 or CRC-S5);
- Ack Octet (by CRC-S3 CRC-S5);
- Consumer_Time_Value (by CRC-S3 CRC-S5).

Ack_Octet_2 in the Time Coordination message shall not be included in the Safety CRC.

7.1.1.11 Time Correction section

The Time Correction message shall be sent from a multipoint producer to each multipoint consumer, once every ping interval. The time correction message, which contains consumer specific information, is sent by the producer to the consumer at a slower rate then the produced data The Time Correction message sends consumer specific information to the consumer at a slower rate then the produced data. The encoding for the BF time correction message is defined in Figure 28 and the EF time correction section is defined in Figure 29. The variables used in the time correction section are defined in Table 92.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

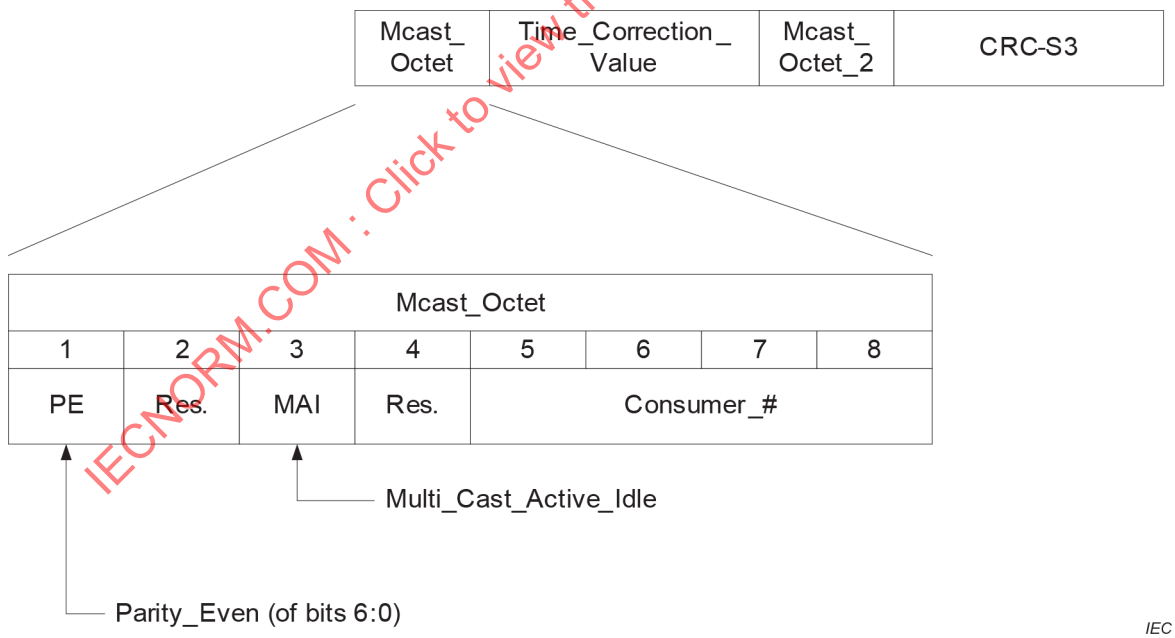


Figure 28 – BF Time Correction message encoding



Figure 29 – EF Time Correction message encoding

Table 92 – Time Correction Message variables

Name	Description	Reference
Consumer_Time_Correction_Value	Consumer_Time_Correction_Value in the Time Correction message shall be used to correct the data time stamp and make the time relative to the multipoint consumers clock	7.7.4.2
MCast_Octet	Consisting of:	
Parity_Even	Parity_Even in the Time Correction message shall be the even parity of bits 0 to 6 of the Message	
Multi_Cast_Active_Idle	Multi_Cast_Active_Idle in the Time Correction message shall indicate Idle if transmitted before this consumer has responded with a valid time coordination message	7.7.4.3
Consumer_#	The Consumer_# in the Time Correction message shall indicates the number of the consumer that this message is directed to	7.7.4.1
Reserved	Reserved, set to zero	7.7.4.4
CRC-S3	CRC covering the data within the BF time correction message	
CRC-S5	CRC covering the data within the EF time correction message	

The following rule shall be used for the calculation of the parity bit in the Time Correction message:

Bit 7 of the MCast _Octet form even parity on the MCast _Octet.

The following rule shall be used for setting of the bits in Mcast_Octet_2 in the Time Correction message:

MCast_Octet_2 = ((MCast_Octet XOR FF_{hex}) AND 55_{hex}) OR (MCast_Octet AND AA_{hex}).

When a connection is established with the Extended Format, the EF Time Correction format shall be used; otherwise the BF Time Correction format shall be used.

7.1.1.12 Time Correction CRC calculation

The Time Correction CRC calculation shall include:

- Producer Identifier (PID) (by CRC-S3);
- Mcast_Octet (by CRC-S3);
- Time_Correction_Value (by CRC-S3).

MCast_Octet_2 of the Time Correction message shall not be included in the Safety CRC.

7.1.1.13 1 or 2 Octet, point-to-point, safety connection format

Figure 30 defines the section organization for 1 or 2 octet point-to-point safety connection format.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

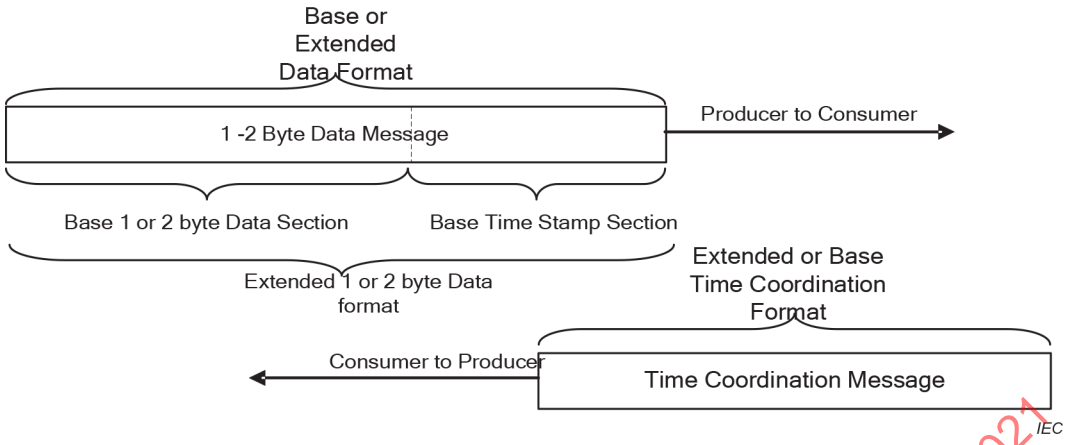


Figure 30 – 1 or 2 octet point-to-point PDU encoding

7.1.1.14 1 or 2 Octet, multipoint, Format 1 connection format

Figure 31 defines the section organization for the 1 or 2 octet Format 1, multipoint connection format.

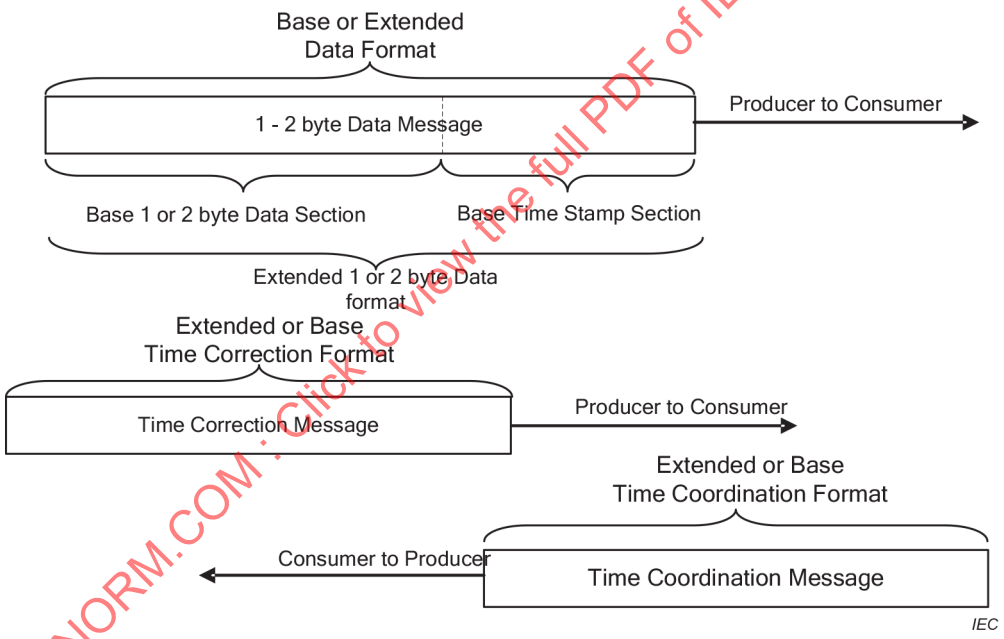


Figure 31 – 1 or 2 Octet multipoint PDU encoding

7.1.1.15 1 or 2 Octet, multipoint, Format 2, safety connection format

Figure 32 defines the section organization for 1 or 2 octet multipoint format 2 safety connection format.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

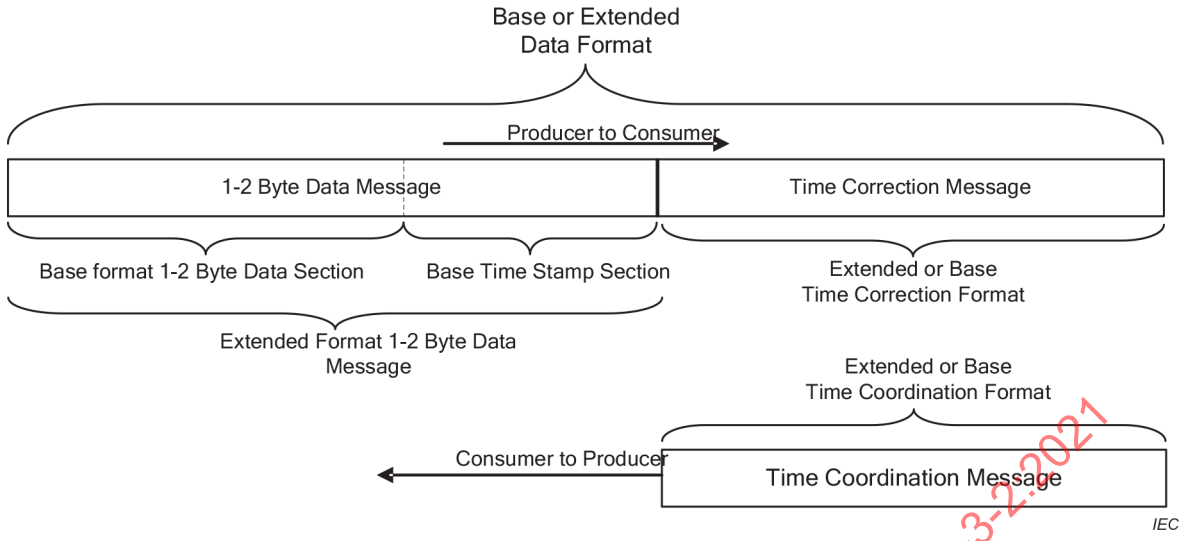
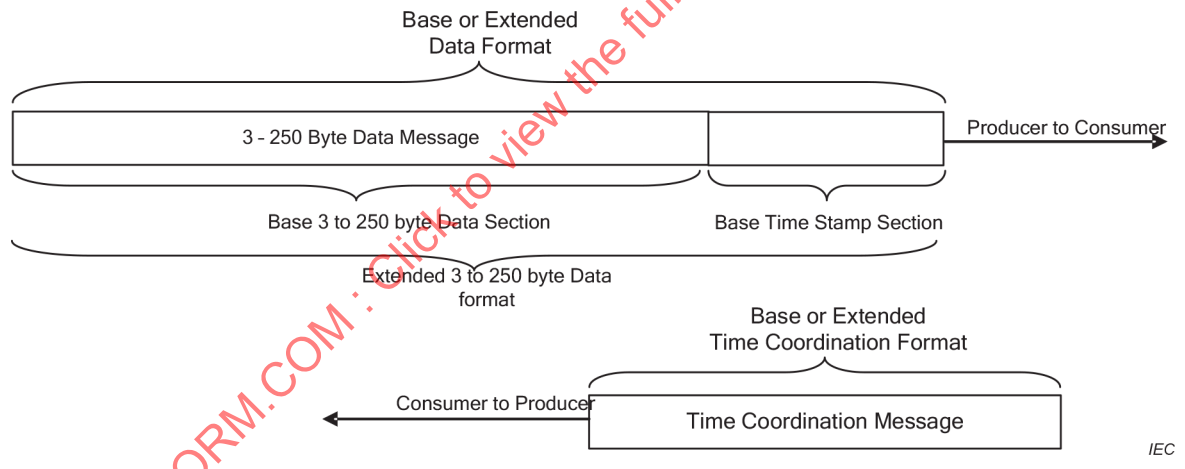


Figure 32 – 1 or 2 Octet, multipoint, Format 2 safety connection format

7.1.1.16 3 to 250 octet, point-to-point, safety connection format

Figure 33 defines the section organization for 3 to 250 octet point-to-point safety connection format.



IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Figure 33 – 3 to 250 Octet Point-to-point PDU encoding

7.1.1.17 3 to 248 Octet, multipoint, Format 1 Safety PDU format

Figure 34 defines the section organization for 3 to 248 octet multipoint safety connection format.

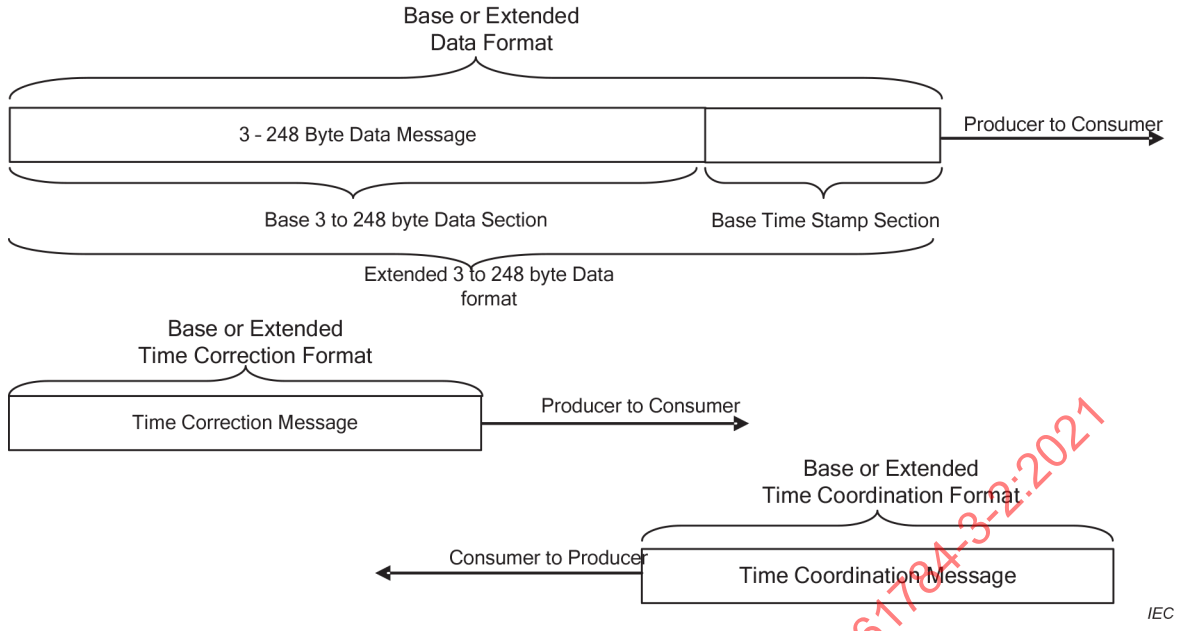
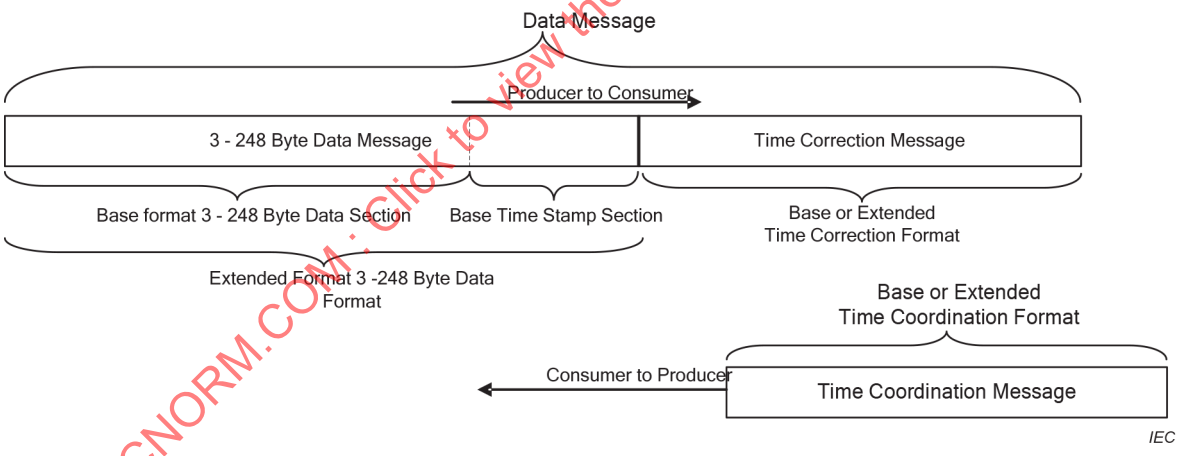


Figure 34 – 3 to 248 Octet Multipoint PDU encoding

7.1.1.18 3 to 248 Octet, multipoint, Format 2, safety PDU format

Figure 35 defines the section organization for 3 to 248 octet multipoint safety connection format.



IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Figure 35 – 3 to 248 Octet, Multipoint, safety connection format

7.1.1.19 Calculation order for Extended Format CRC calculations

Figure 36 shows where the rollover count fits into the CRC calculations for the Extended Format messages.

NOTE The CRC seed is still based on the PID/CID as in the Base Format; the Rollover count is treated as an additional data parameter.

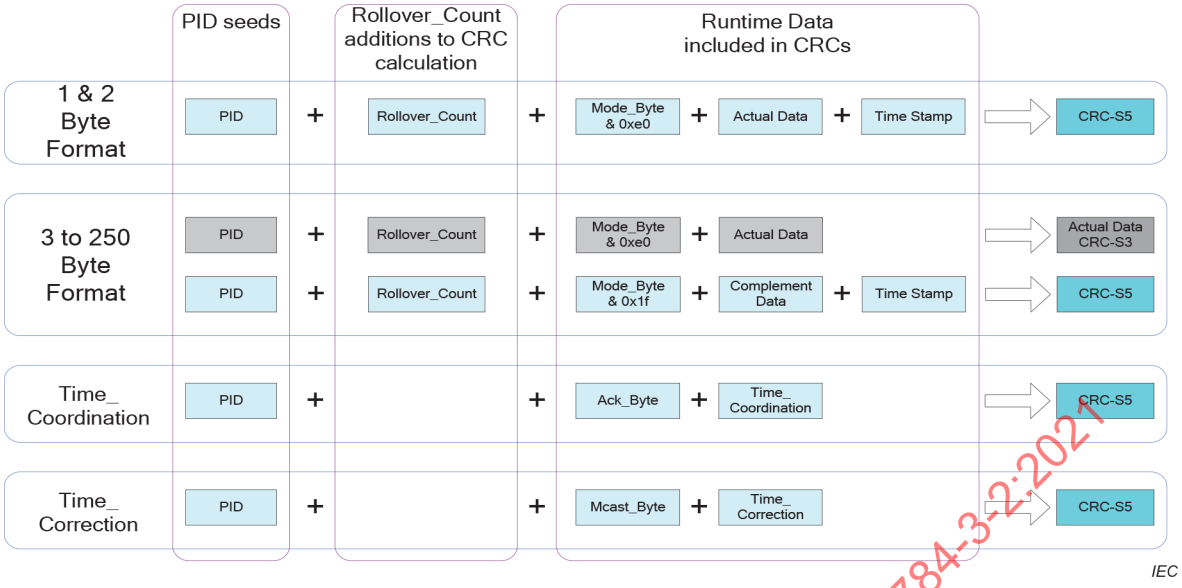


Figure 36 – CRC Calculation order for Extended Format messages

7.1.2 Safety CRC

7.1.2.1 Safety CRC overview

There are five safety CRCs used in the various sections in FSCP 2/1.

- An 8-bit CRC (CRC-S1 or CRC-S2) is used for the BF data sections containing up to two octets of safety data and the time stamp sections.
- A 16-bit CRC (CRC-S3) is used for BF and EF data sections for 3 to 250 octets of data and for the BF time correction and time coordination messages.
- A 24-bit CRC (CRC-S5) is used for the EF data format up to two octets of safety data and for the EF complement data sections for 3 to 250 octets of data. The 24-bit CRC is also used for the time correction and time coordination messages in EF.
- A 32-bit CRC (CRC-S4) is used for connection establishment, configuration, and the Safety extension to the EDS file definition.

Calculations of these CRCs are described in Annex A.

7.1.2.2 CRC polynomials

Table 93 defines the polynomials used in FSCP 2/1.

Table 93 – CRC polynomials used

Name	Hex value of polynomial
CRC-S1	37_{hex}
CRC-S2	$3B_{hex}$
CRC-S3	$080F_{hex}$
CRC-S4	$EDB88320_{hex}$
CRC-S5	$5D6DCB_{hex}$

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

7.1.2.3 CRC usage specifications

The I/O messaging CRC usage is defined in 7.1 using CRC-S1, CRC-S2, and CRC-S3, but there are a number of other CRCs defined in FSCP 2/1 for connection establishment, configuration, and the Safety extension to the EDS file definition. Table 94 defines which algorithm is used and the starting seed value for each use.

Table 94 – CRC usage for connection and configuration

CRC name	Algorithm used	Starting seed value	Description
SCCRC	CRC-S4 (see Clause A.1)	$FFFFFFFF_{hex}$	Safety Configuration CRC
CPCRC	CRC-S4 (see Clause A.1)	$FFFFFFFF_{hex}$	Connection Parameter CRC
Password CRC	CRC-S4 (see Clause A.1)	$FDFDFDFD_{hex}$	Used to encrypt passwords before transmission
EDS File CRC	CRC-S4 (see Clause A.1)	$FDFDFDFD_{hex}$	Used to provide integrity over EDS files used by safety devices

7.2 Communication protocol behavior

7.2.1 Sequence of safety checks

The following Sequence of checks shall be used to check messages.

a) Ping count check;
b) Evaluate Time stamp section CRC;
c) Evaluated Time Stamps;
d) Evaluate Actual Data CRC;
e) Evaluate Complement Data CRC;
f) Perform Cross-Check.

7.2.2 Connection termination

When a producer detects an error that requires connection termination (i.e. ping response outside of Producer Ping Interval) it shall terminate the connection, and notify the application of the action.

All consumers shall monitor the periodic transmission of data and go to a safety state if the periodic transmissions cease. If the consumer detects an error, it shall go to a safety state and terminate the consuming connection associated with that error.

When the Safety Layer detects an error requiring connection termination the termination shall be implemented using the following sequence.

a) The safety layer detects an error requiring termination.
b) The safety layer notifies the application program by setting the connection status to indicate a safety communications fault.
c) The safety-related application shall transition data and I/O (for example set outputs to the safety state) associated with the connection to a safety state.
d) The safety layer shall notify the underlying communications system of an error and request the termination of the connection by setting its status to indicate a safety communications error.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

e) The safety layer shall not transition from its safety state until the fault is cleared and a connection restart sequence is initiated.

7.2.3 Cross checking error

When crosschecked safety data are found to be different, the data is treated as faulty. The BF consumer shall terminate the connection (see 7.2.2) and the EF consumer will increment the Consumer_Fault_Count and drop the packet if the count is less than the Max_Fault_Number, or terminate the connection if is equal to or greater than the Max_Fault_Number.

7.3 Time stamp operation

The time stamp allows for the calculation of the timeliness of receipt of data in the consumer. Figure 37 shows the time stamp sequence of operations for a simple point-to-point producer consumer pair.

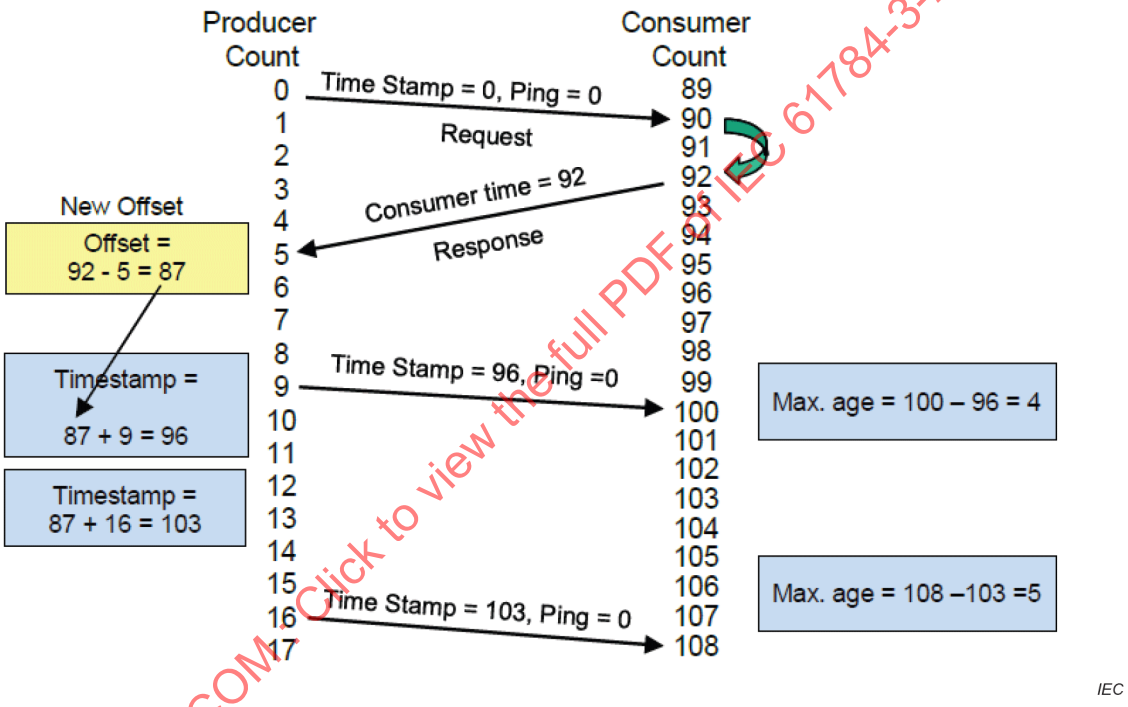


Figure 37 – Time stamp sequence

Upon connection establishment, the producer shall request an initial ping response.

When the consumer sees a change in the ping count, the consumer shall prepare a Time Coordination response message that contains the consumer's value of its clock count.

The producer shall use the clock count in the Time Coordination response to calculate an offset that will be applied to future productions.

At each scheduled production, the producer shall use the value of its own clock count and the offset to calculate the time stamp and sends it to the consumer along with the data.

The consumer shall use the value received from the producer to calculate the age of the data by subtracting the producer's time stamp from its current clock count. If the calculated delta is less than the maximum delta specified by the user, the data is ok and the data is used by the application within the device. If the delta is greater than the user specified value, the data is deemed to be to old too use and the connection is terminated.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Once each Ping Interval, the producer shall request another ping response from the consumer. This will cause a recalculation of producer offset and prevent the slow aging of data due to time errors.

A time correction factor is added to account for the maximum skew and drift of clocks in an asynchronous system. This message is used to adjust the offset in the producer.

7.4 Rollover counts in the EF

A rollover count is employed in conjunction with the transmitted Time Stamp to extend the effective operating range of the Time Stamp to 32 bits. The Rollover count is not transmitted with the time stamp however. The initial values for the rollover count are set at connection establishment and maintained independently by both producer and consumer. The rollover count value is included in the data CRC calculation so both ends shall agree on the current value at all times for packets to be received successfully.

7.5 Protocol sequence diagrams

7.5.1 General

The protocol sequence diagrams show the relationship between producers and consumers with respect to time and events. Time flows from the top of each figure to the bottom. Normal messages that are received at the producer or consumer are shown in normal text boxes. Anomalous messages are shown in bolded text boxes. Messages that were expected but not received are shown as unboxed text.

7.5.2 Normal safety transmission

Normal communication between a safety producer and consumer requires a sequence of periodic messages. When the consumer receives a valid message, the transaction is complete as defined in Figure 38.

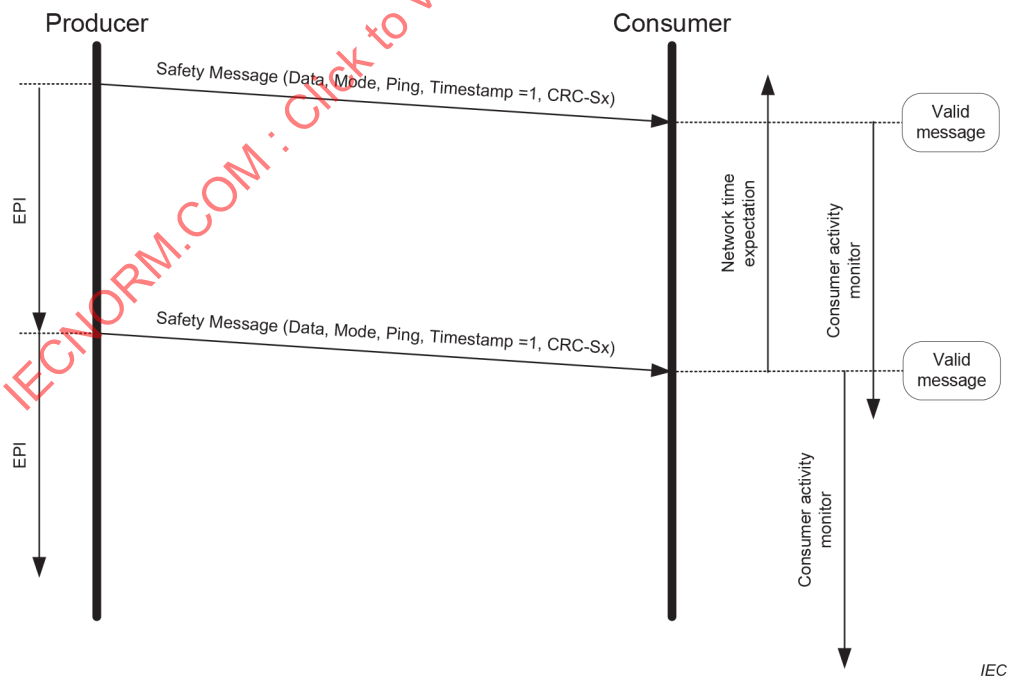


Figure 38 – Sequence diagram of a normal producer/consumer safety sequence

The safety producer produces data at a fixed rate called the Expected Packet Interval (EPI).

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Link-triggered consumers shall maintain an activity timer, which is reset after receiving a valid expected message.

If a valid message has not been received before the activity timer expires, the link-triggered consumer shall terminate the connection (see 7.2.2) and go to the defined safety state.

Consumers shall check the age of the data received by checking the time stamps received.

If the age of the data is greater than the network time expectation the consumer shall terminate the connection (see 7.2.2) and go to the defined safety state.

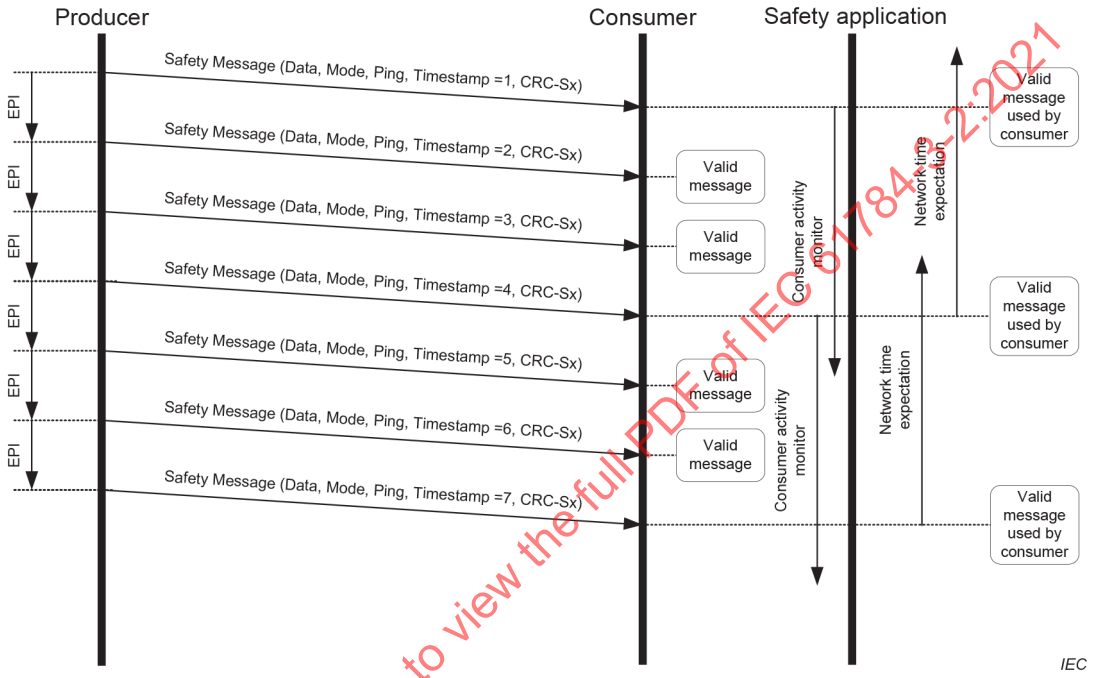


Figure 39 – Sequence diagram of a normal producer/consumer safety sequence (production repeated)

Safety communications shall be configurable with production repeated. In this case, the consumer does not use every packet that is sent to it.

When safety communication is sent with repeated production, application-triggered consumers shall use the last packet received to complete the transaction, as show in Figure 39.

The consumers using Base Format connections shall see the Timestamp increase for each successive period, or the connection shall be terminated (see 7.2.2).

Consumers using Extended Format connections shall see the Timestamp increase for each successive period. If the consumer receives a packet with an out-of-sequence Timestamp, it shall drop the packet unless the Consumer Fault Counter has reached the Max Fault Number; in which case the connection shall be terminated.

Messaging with production repeated offers the additional advantage of using the most current data.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

7.5.3 Lost, corrupted and delayed message transmission

Due to external disturbances it may be possible for the message to be corrupted as it is transmitted from the producer to the consumer, as defined in Figure 40. If a corrupted message is detected at the standard layer, it shall be discarded and not presented to the application. This will result in an expiration of the consumer activity monitor or the data age will exceed the network time expectation and the consumer terminates the connection (see 7.2.2) and goes to the defined safety state.

If the transmitted CRC-Sx and data are checked and any found to be in error, or the data cross-check is found to be in error, the consumer shall either drop the packet (Extended Format AND (Consumer_Fault_Count < Max_Fault_Number)), or terminate the connection and go to the defined safety state (Base Format OR Extended Format) AND (Consumer_Fault_Count ≥ Max_Fault_Number) (see 7.2.2).

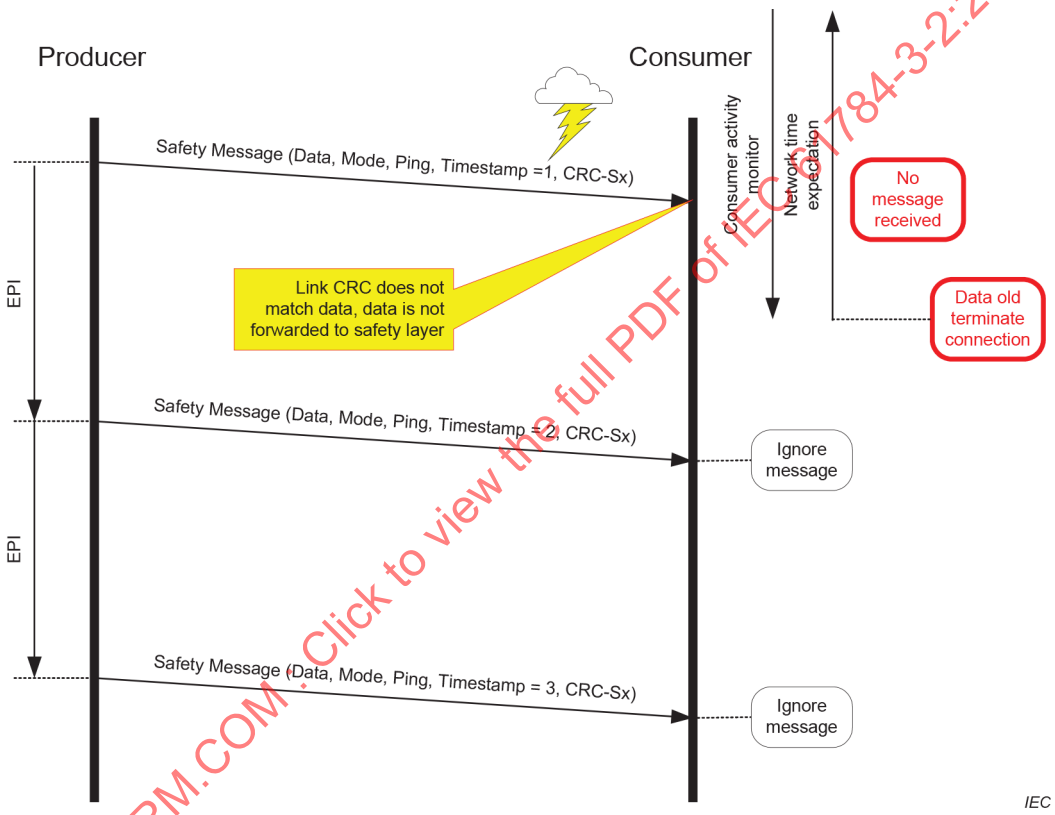


Figure 40 – Sequence diagram of a corrupted producer to consumer message

Due to external disturbances it may be possible for the message to be lost as it is transmitted from the producer to the consumer, as defined in Figure 41. This will result in an expiration of the consumer activity monitor or the data age will exceed the network time expectation and the consumer terminates the connection (see 7.2.2) and goes to the defined safety state.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

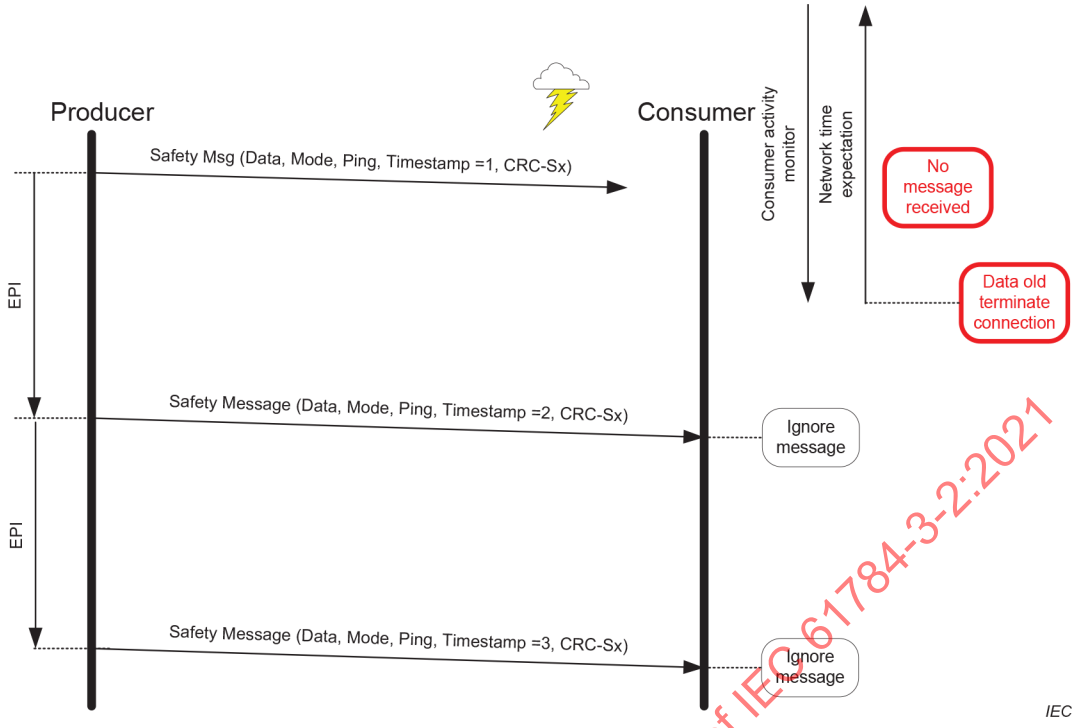


Figure 41 – Sequence diagram of a lost producer to consumer message

Messages may be delayed in transmission. If a message is delayed such that it is received

- beyond the consumer activity monitor (link-triggered application), or
- the data age exceeds the network time expectation,

Then all further messages are ignored, and the connection shall be terminated.

In both cases the consumer terminates the connection (see 7.2.2) and goes to the defined safety state. This behavior is defined in Figure 42.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

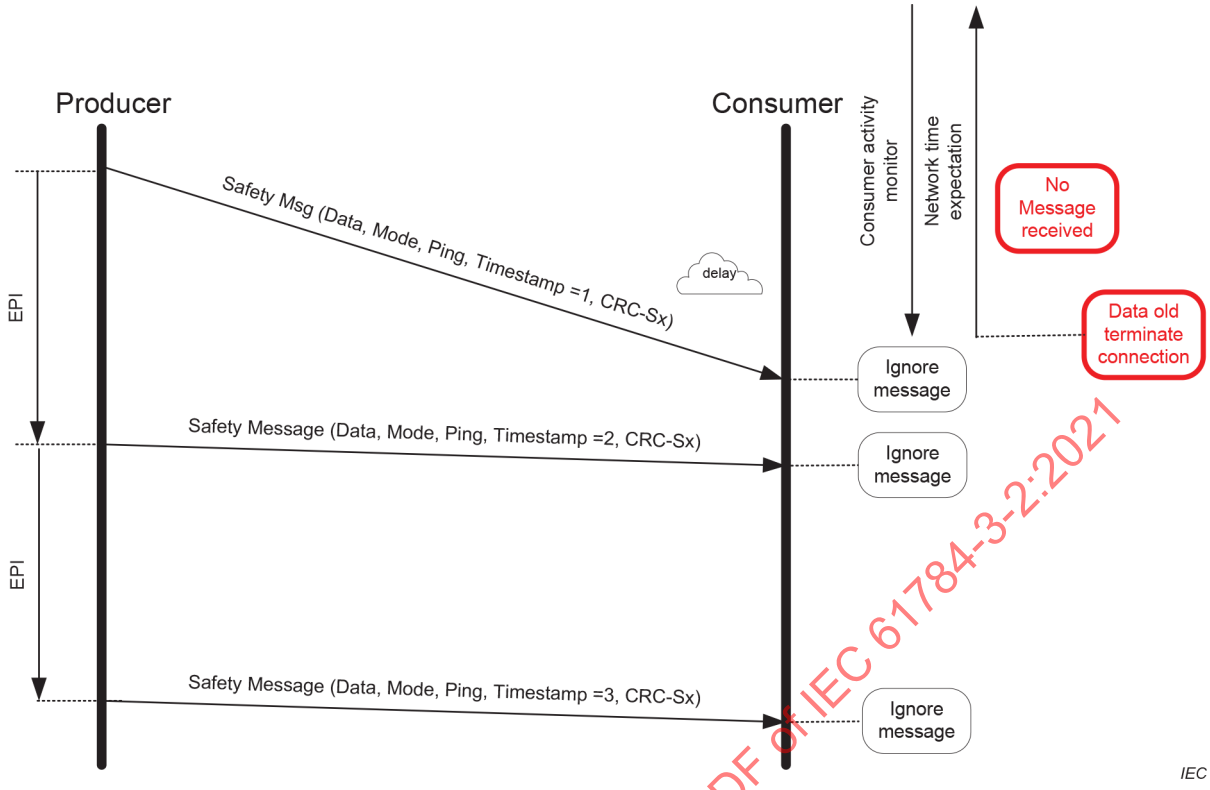


Figure 42 – Sequence diagram of a delayed message

7.5.4 Lost, corrupted or delayed message transmission with production repeated

Due to external disturbances it may be possible for the message to be corrupted as it is transmitted from the producer to the consumer, as defined in Figure 43. In order to, minimize spurious trips and increase the availability of the overall system, production may be repeated.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

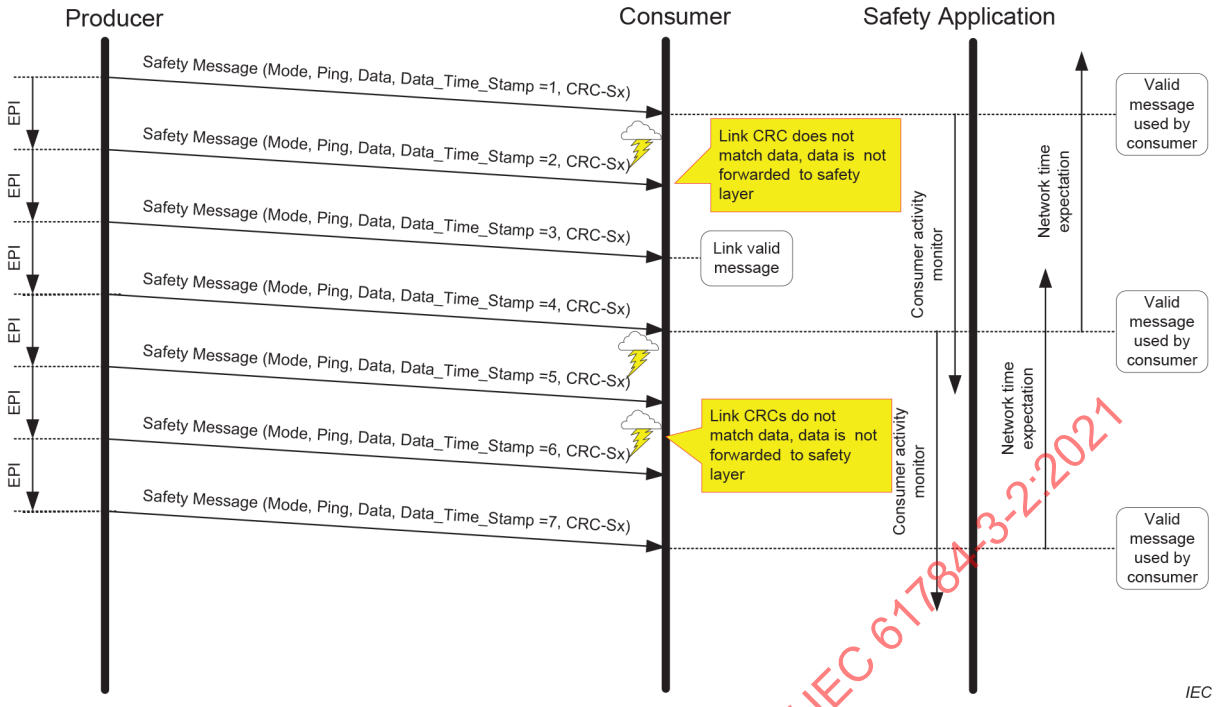


Figure 43 – Sequence diagram of a corrupted producer to consumer message with production repeated

If there are errors that are detected in the standard layers, the messages can be discarded, as long as a valid and expected message is received within the consumer activity monitor and the age of the data does not exceed the network time expectation.

Valid repeated messages shall be overwritten. The most recent valid message is used by the application.

Due to external disturbances, it may be possible for a series of messages to be delayed resulting in a lost connection. This sequence is defined in Figure 44. If no valid messages are received before the consumer periodic timer expires, the connection will be terminated (see 7.2.2).

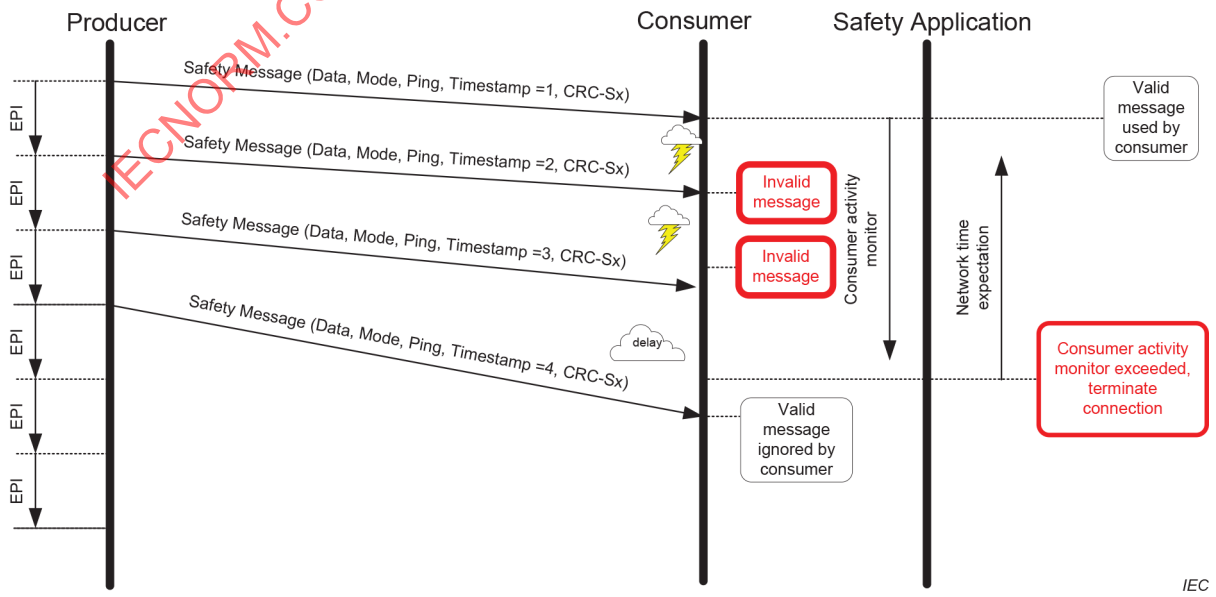


Figure 44 – Sequence diagram of a connection terminated due to delays

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

A valid link message that fails a Safety CRC check will cause the consumer to assume the underlying link is untrustworthy and depending on the format used and/or number of occurrences, could cause the connection to be terminated. This sequence is defined in Figure 45.

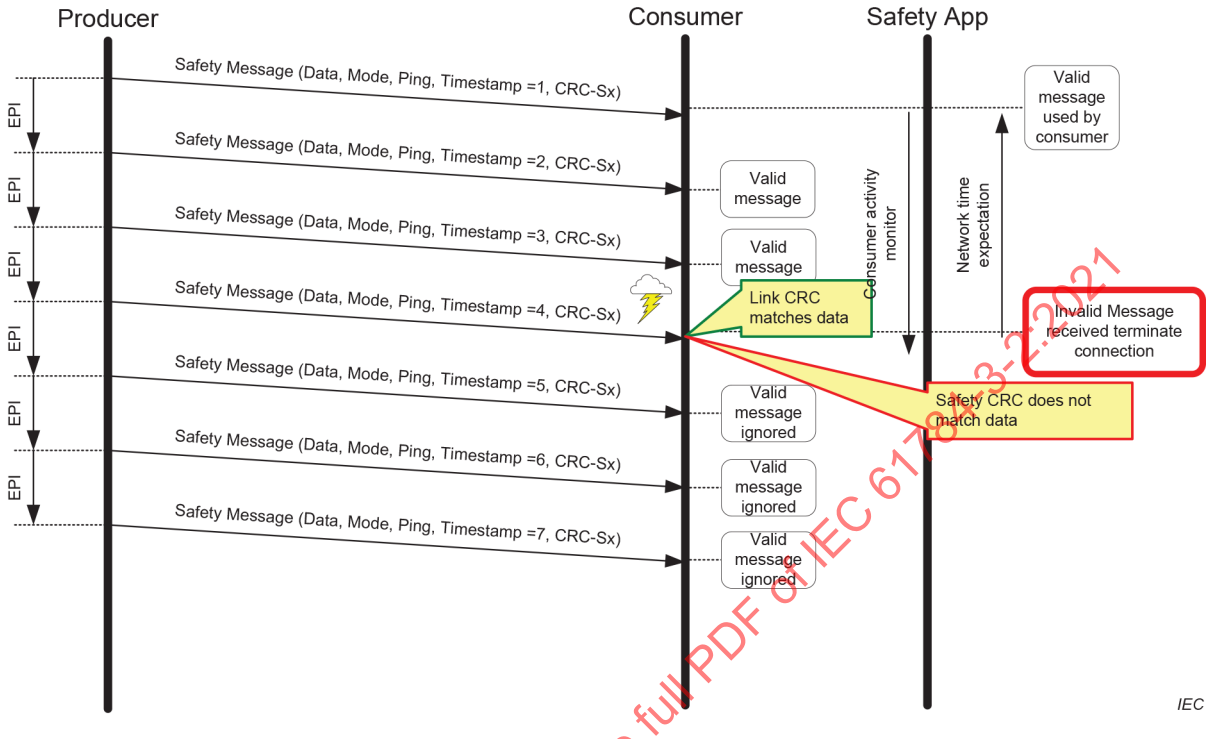


Figure 45 – Sequence diagram of a failure of safety CRC check

7.5.5 Point-to-point ping

In order to maintain consistent delay timing between producers and consumers a ping request and response message transaction sequence is used. The producer is fully described in 7.6.6 and the consumer is fully described in 7.6.7. This sequence of messages for a point-to-point ping is defined in Figure 46.

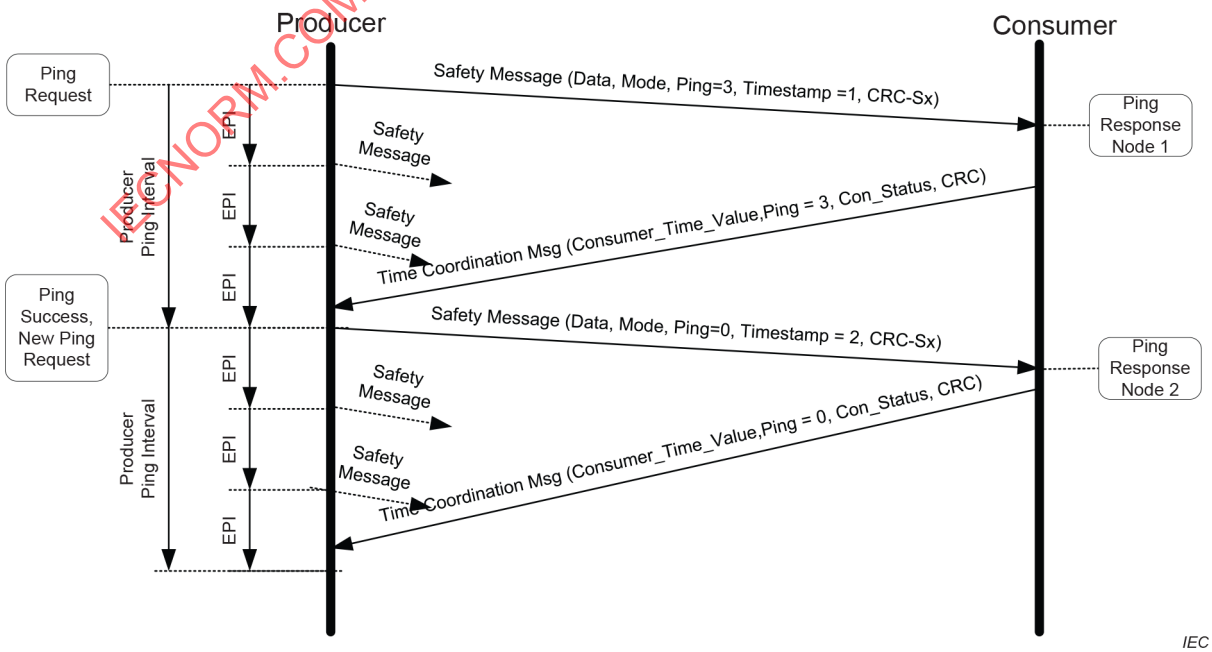


Figure 46 – Sequence diagram of a point-to-point ping – normal response

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

At each point-to-point producer ping interval, the ping count shall be incremented in the next available safety message header.

The point-to-point producer ping interval shall be a multiple of the EPI; ping requests shall be made at a rate based on the Ping_Interval_EPI_Mulitplier.

When a point-to-point consumer sees a change in the ping count the consumer generates a time coordination message.

The time coordination message (see 7.5.2) shall be received by the producer within a prescribed time frame. If the time coordination message is not received within that time frame the connection shall be terminated by the producer (see 7.2.2).

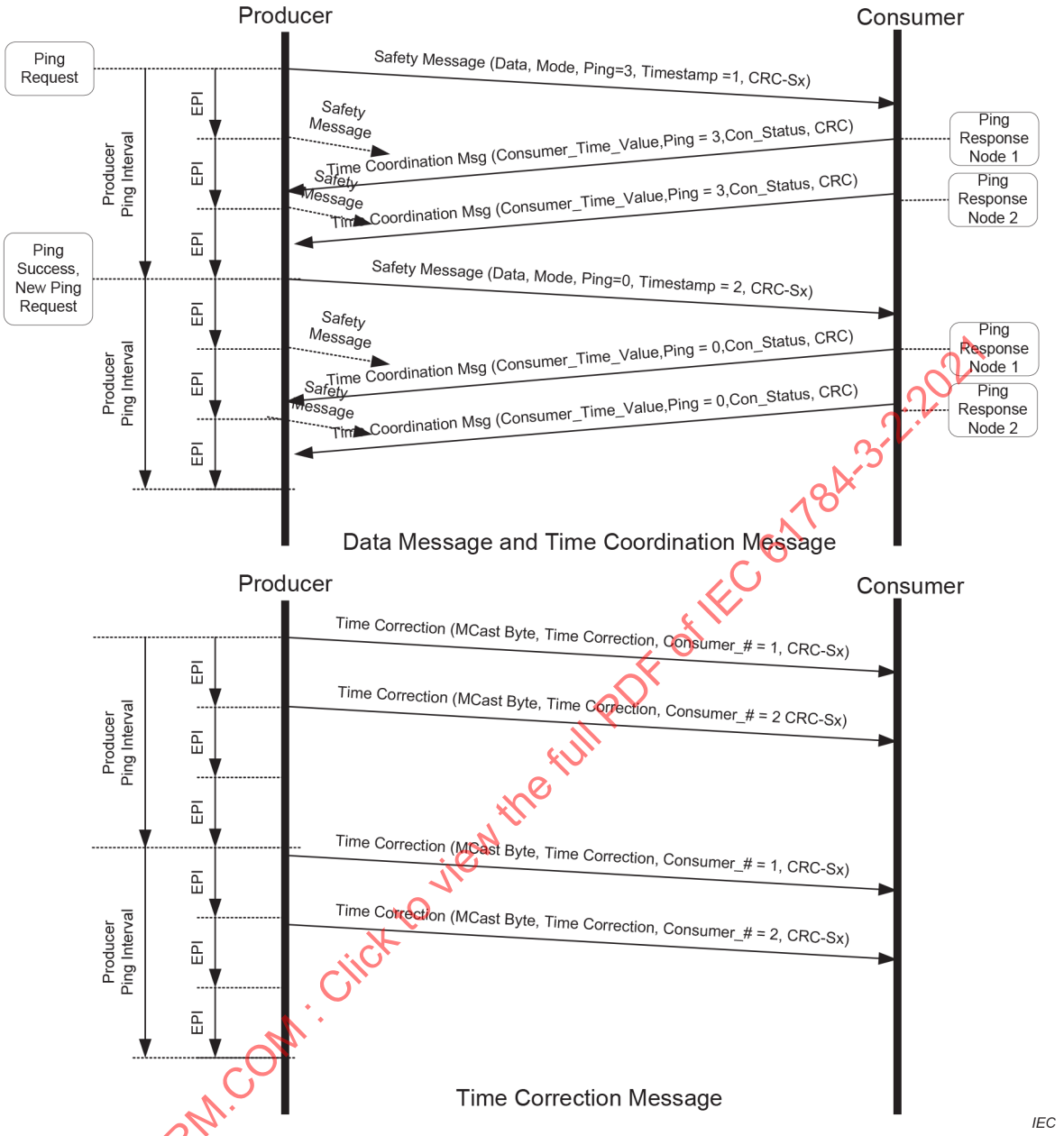
7.5.6 Multipoint ping on CP 2/3 Safety

In order to maintain consistent delay timing between producers and consumers a ping request and response message transaction sequence is used.

For CP 2/3 Safety Multipoint connections, a separate message shall be used to communicate time correction information form the produce to each multipoint consumer.

The producer is fully described in 7.6.6 and the consumer is fully described in 7.6.7. This sequence of messages for multipoint ping is defined in Figure 47. For clarity the time correction message is defined on a separate diagram.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021



IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Figure 47 – Sequence diagram of a successful multipoint ping, CP 2/3 safety

During each multipoint producer ping interval, a ping request will be sent from the multipoint producers to multipoint consumers requesting a response.

All multipoint consumers shall respond to a change in the ping request value, consumers other than consumer 1 shall wait Consumer_Number -1 times the EPI to reply.

All of the multipoint consumers shall respond within the ping interval of the request or the next one.

Time correction messages shall be sent to the multipoint consumers at a rate to ensure that each consumer gets a time correction message within a single producer ping interval.

7.5.7 Multipoint ping on CP 2/2 safety networks

In order to maintain delay timing between multipoint producers and its consumers, a ping request and response is used. For CP 2/2 Safety networks the time correction message shall be concatenated with the safety data message and sent as a single message. The producer is fully described in 7.6.6 and the consumer is fully described in 7.6.7. This sequence of messages for multipoint ping is defined in Figure 48.

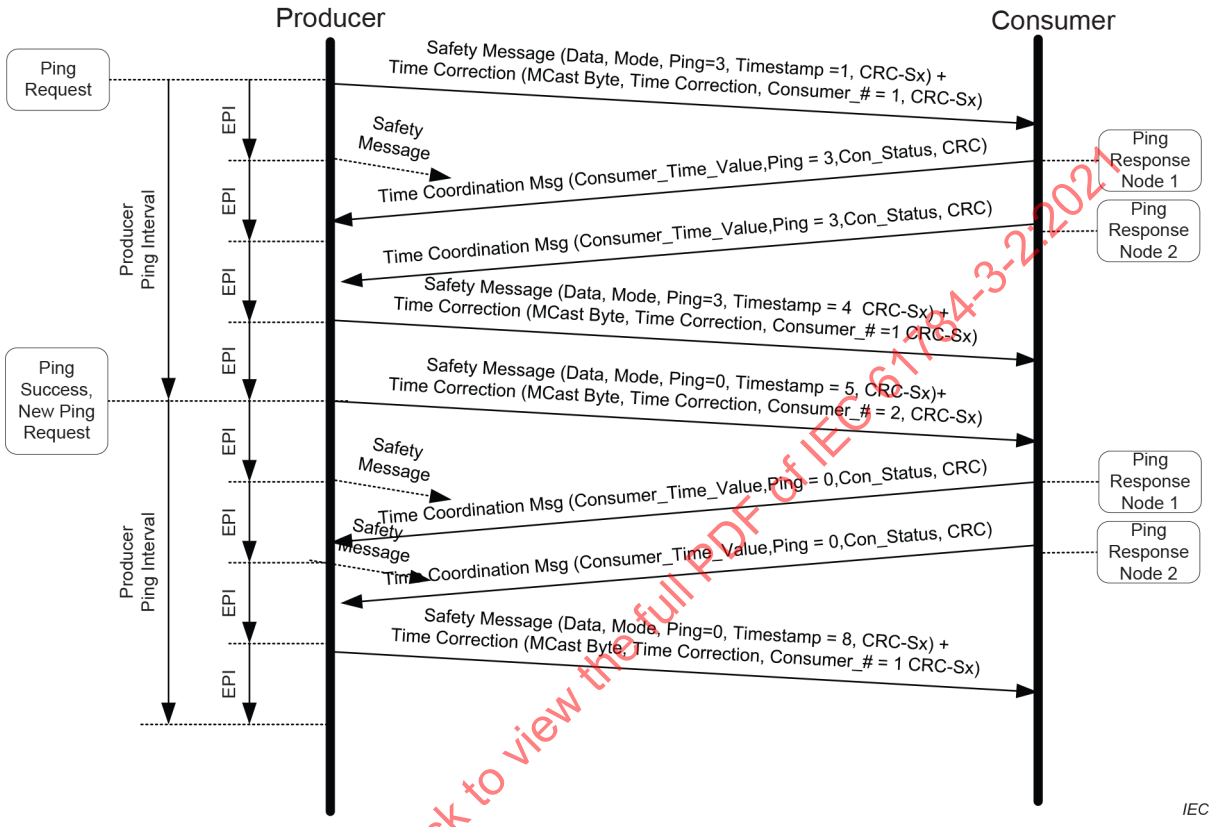


Figure 48 – Sequence diagram of a successful multipoint ping, CP 2/2 safety

During each producer ping interval, a ping request is sent from the multipoint producers to multipoint consumers requesting a response.

7.5.8 Multipoint ping – retry with success

This sequence of messages for a multipoint ping with retries is defined in Figure 49. The time correction connection is not defined for clarity.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

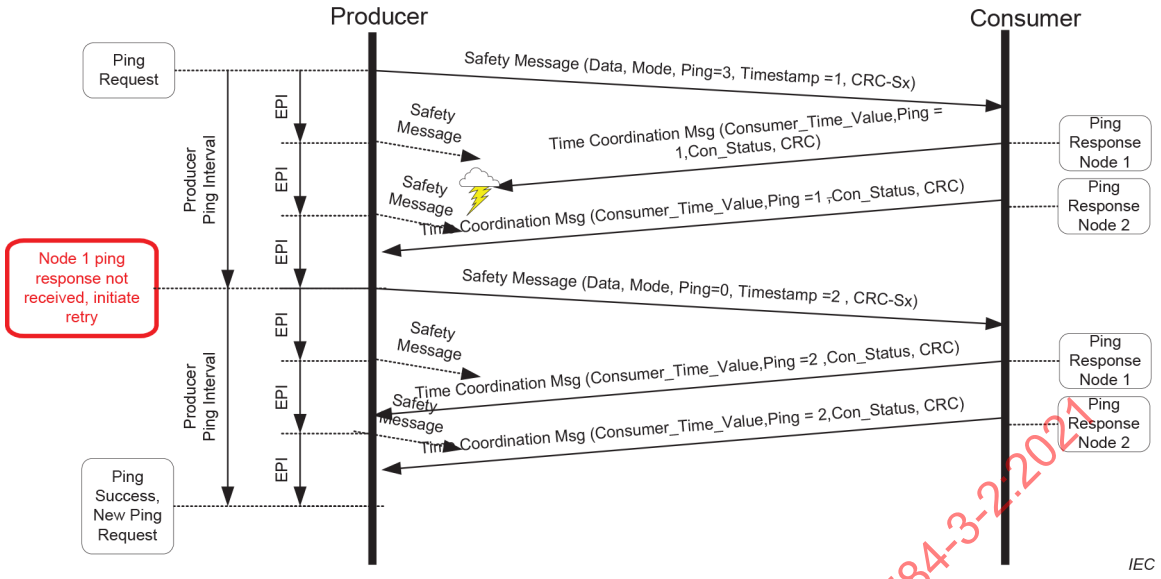


Figure 49 – Sequence diagram of a multipoint ping retry

If a multipoint time coordination message is lost or delayed past the (Timeout_Multiplier.PI + 2) ping intervals, an error shall be generated and the connection closed.

7.5.9 Multipoint ping – retry with timeout

The sequence of messages for a multipoint ping with retries and timeout is defined in Figure 50. The time correction connection is not defined for clarity.

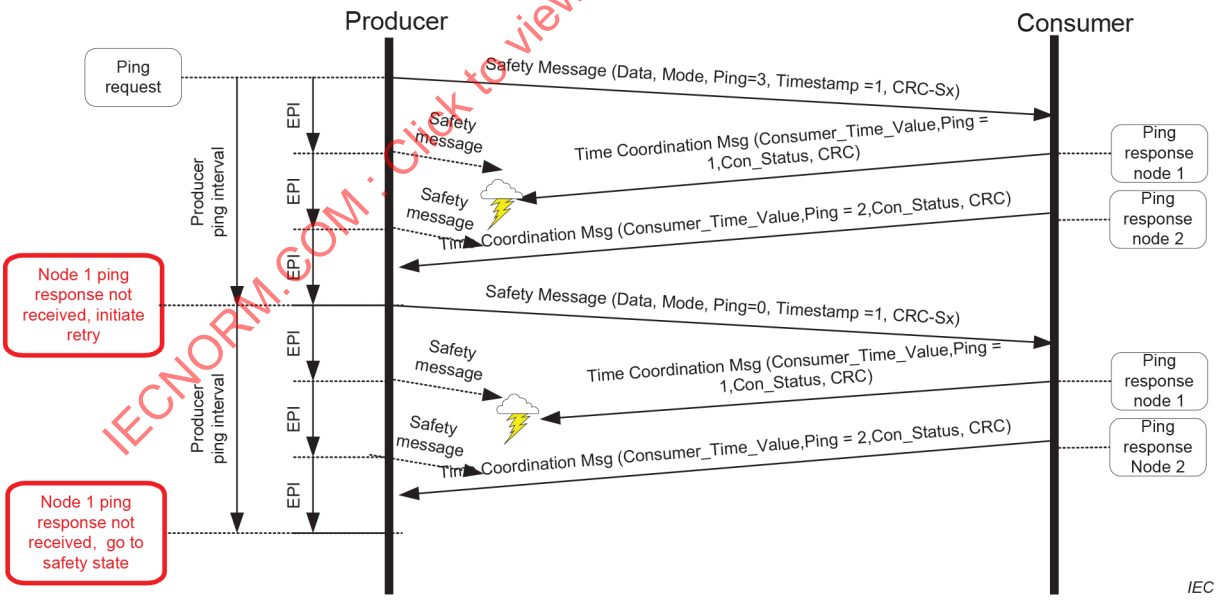


Figure 50 – Sequence diagram of a multipoint ping timeout

If the ping response continues to be delayed, the producer will indicate a fault in the producer status for the specific consumer and the consumer will go to the defined safety state. If the ping was delayed due to a fault in the consumer, the consumer will have already gone to a safety state.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

7.6 Safety protocol definition

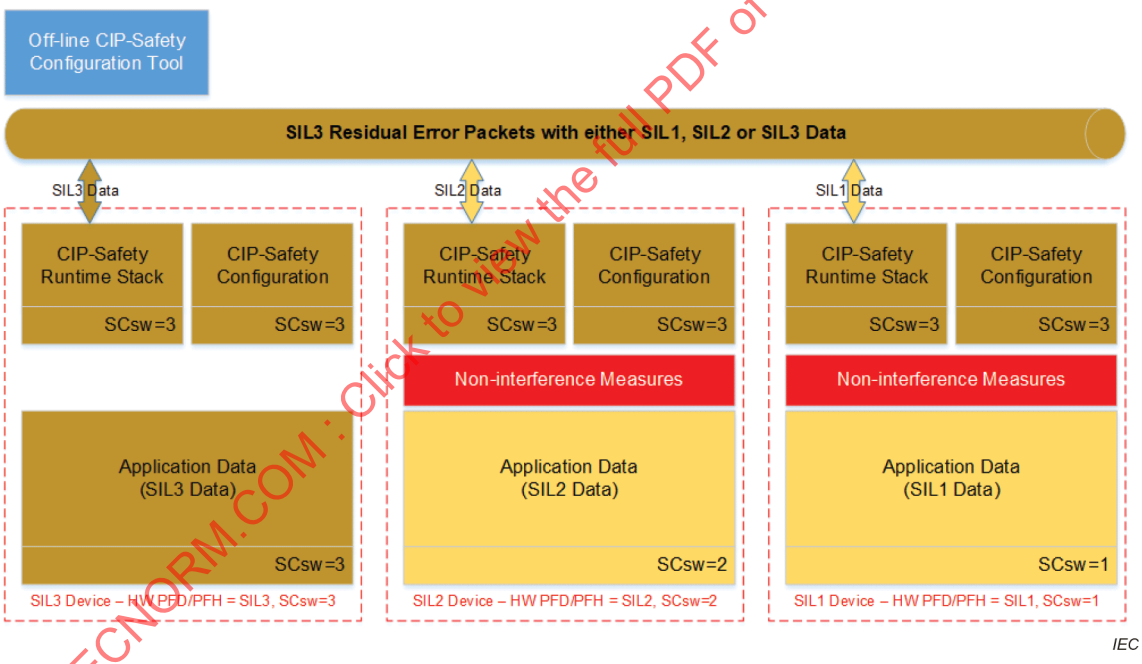
7.6.1 General

The safety layer is a layer of service residing between the standard CPF 2 transport layer and the safety-related application layer as defined in Figure 52. This safety layer need not be directly addressable in the CPF 2 framework; rather it is a behavior associated with a connection between applications exchanging safety data in a SIL 3 application. This behavior is implemented as the Safety Validator object as described in 6.7.

There may be multiple methods of accomplishing this desired behavior. The objects in this Subclause 7.6 are to be considered a reference model. Individual products and applications may choose to implement this behavior, as they deem necessary. However, this behavior needs to be expressed here to form a basis for product development.

7.6.2 High level view of a safety device

Figure 51 shows a number of possible safety architectures which could use FSCP 2/1. It shows that any SIL level from 1-3 is possible for using FSCP 2/1. However, it also shows that in all cases, the FSCP 2/1 runtime stack and FSCP 2/1 configuration are developed with an SC3 development process. The assessment of the systematic capability, SIL level requirements, and appropriate non-interference measures is carried out by the safety certification body.



IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Figure 51 – Possible safety architectures for FSCP 2/1

Figure 52 shows an example model of a SIL3 safety device containing one or more safety-related application objects. Each safety-related application objects functions with a pair of Safety Validator objects to exchange safety data between the CPF 2 transport layer and the safety I/O electronic circuitry. These electronics are designed to provide a level of error detection and fault isolation suitable for SIL 3 applications. Each of the two Safety Validator objects is associated with a network communication channel such as CP 2/3 or CP 2/2. This example model assumes a 1oo2 Safety Topology in which two independent CPUs participate in the safety protocol. However with different hardware architectures, FSCP 2/1 technology may be suitable for use in safety applications less than SIL3.

All implementations of FSCP 2/1 technology shall use a safety certifying agency to ensure that the design and implementation of the FSCP 2/1 protocol (safety-related communication software) provides a Systematic Capability of SC3 according to IEC 61508.

The FSCP 2/1 protocol shall be considered as part of a complete device, and the integration of the FSCP 2/1 protocol into the device shall be done to achieve/maintain SC3. For example, a Vendor cannot use a separately certified FSCP 2/1 stack (one that does provide SIL3 and SC3) in their product without regard to the need to provide SC3 for the integration of the safety communication software in the integrated product.

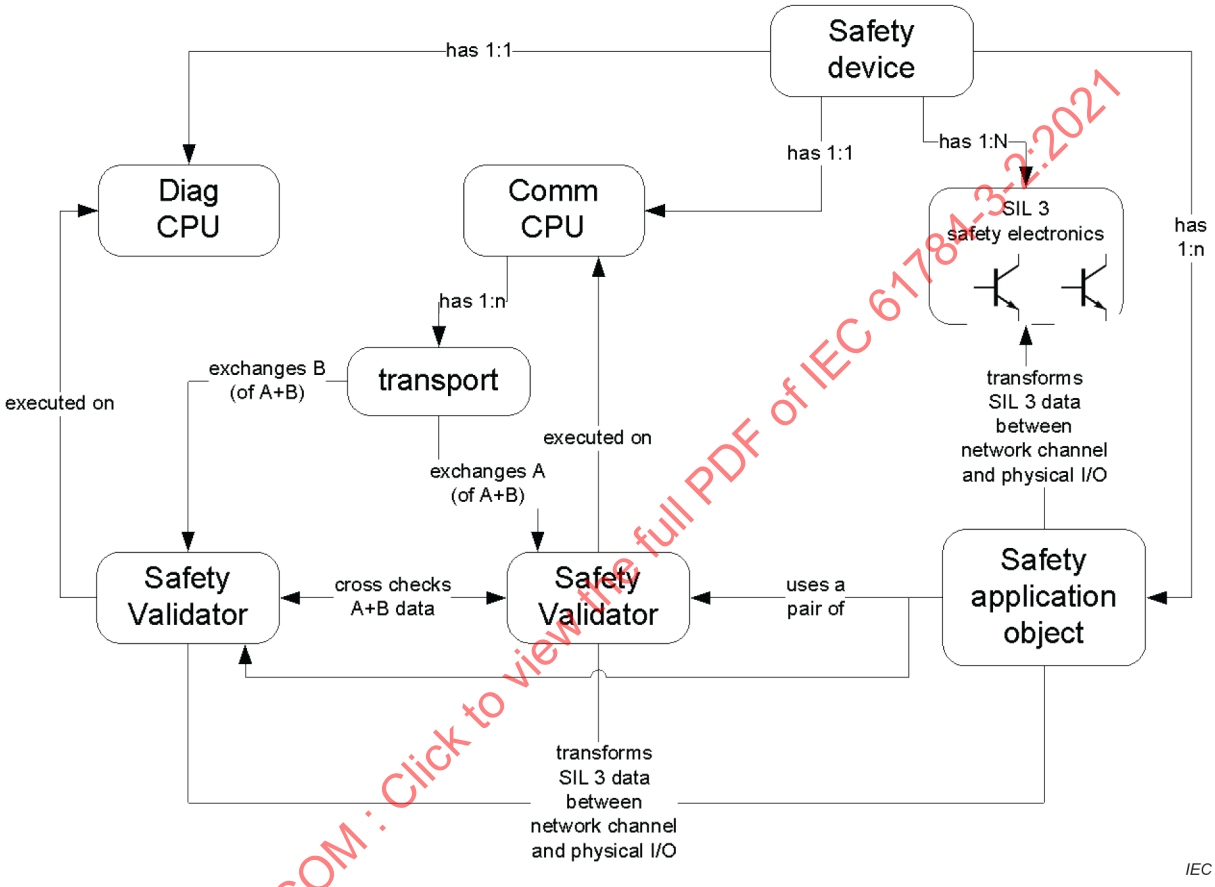


Figure 52 – Safety device reference model entity relation diagram

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

7.6.3 Safety Validator object

Subclause 6.7 defines a Safety Validator object from which both the SafetyValidatorServer and SafetyValidatorClient functions are implemented.

The general principles and common attributes of these two safety layer functions are defined in 7.6.4.

7.6.4 Relationship between SafetyValidatorServer and SafetyValidatorClient

Figure 53 shows a high level view of two devices interchanging data via a SafetyValidatorClient and a SafetyValidatorServer. A safety producing application uses a SafetyValidatorClient to send safety data to a safety consuming application that uses a SafetyValidatorServer.

NOTE Only one of the redundant paths interfaces to the CPF 2 transport layer. The A+B (actual and complement) data is encapsulated in a single transport frame and only one processor is involved in the reception and transmission of the data frames.

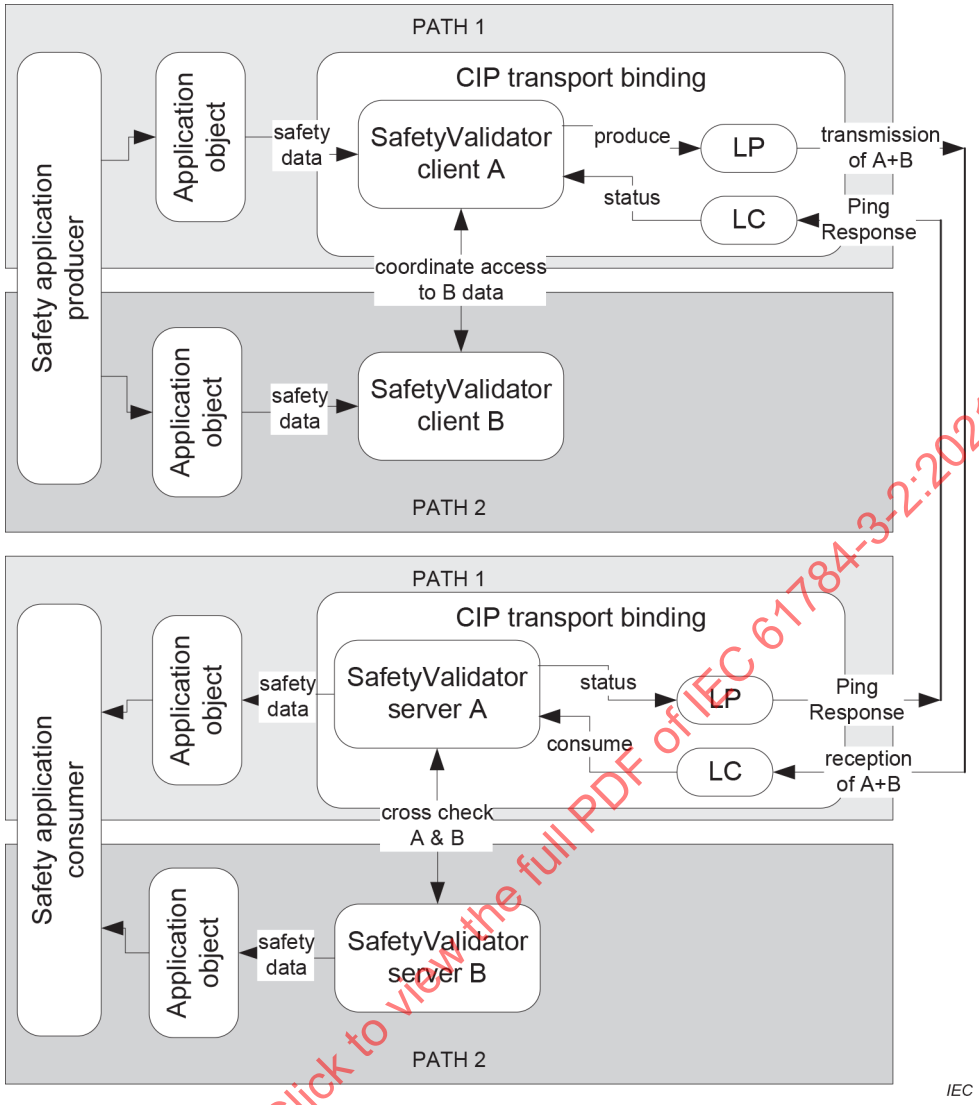


Figure 53 – Two devices interchanging safety data via a SafetyValidatorClient and a SafetyValidatorServer

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

7.6.5 Extended Format time stamp rollover handling

7.6.5.1 General

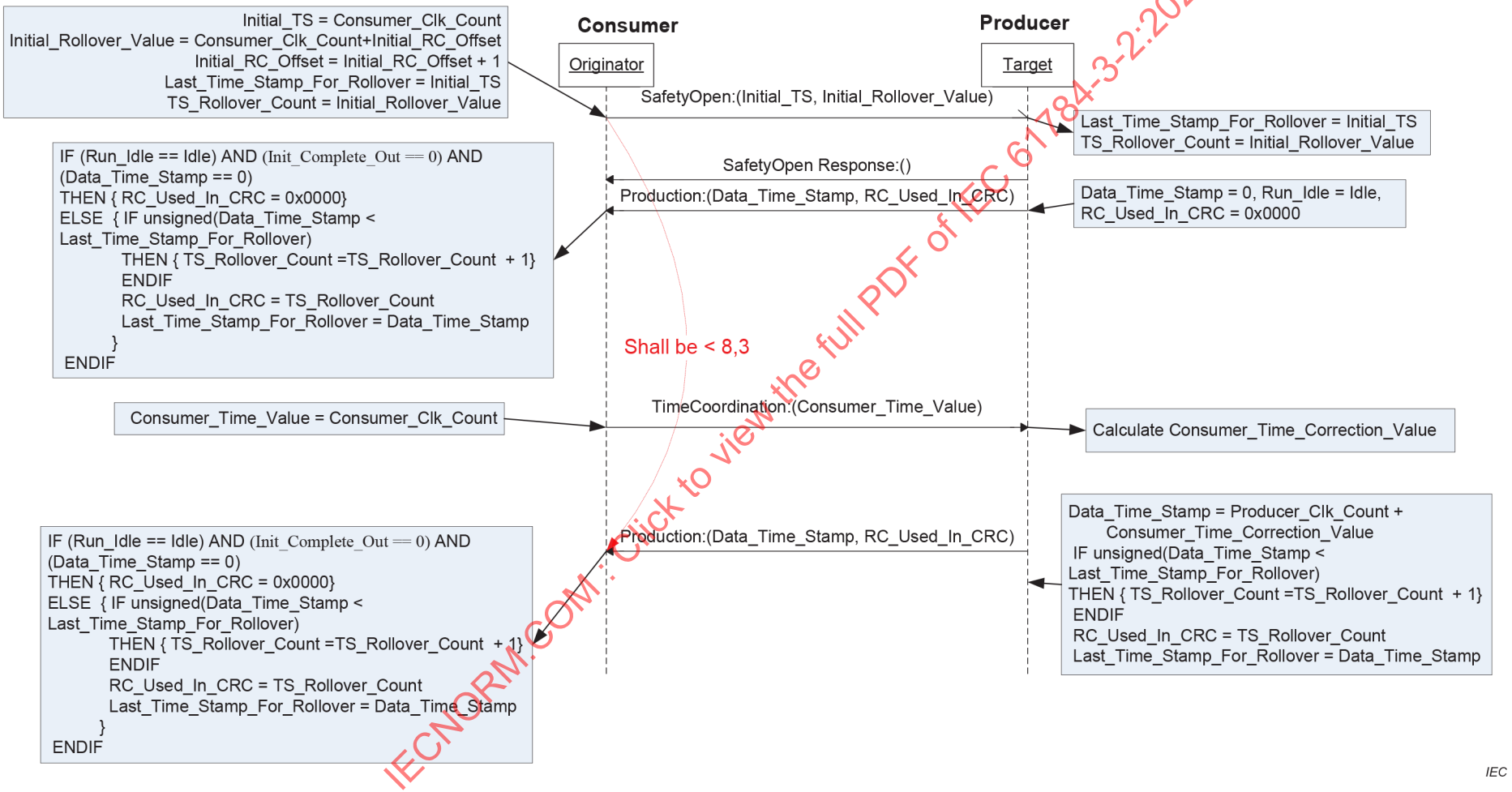
The Extended Format requires coordinated synchronization between producers and consumers on connection establishment along with maintenance operations to detect and handle Time Stamp rollover events. Subclauses 7.6.5.2 to 7.6.5.4 graphically show these operations for each unique case. The example code shows these operations in their proper place in the code as well.

7.6.5.2 Point-to-point, originator consumer, target producer

When point-to-point connections are originated by the consumer, the originator has to provide initialization values in the SafetyOpen. The target uses these values to initialize production parameters.

The rollover count used in the Extended Format point-to-point CRC shall be zero until the initial Time Coordination exchange has been completed.

The complete process is shown in Figure 54.



IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Figure 54 – Point-to-point, originating consumer. target producer

The time between the generation of the Safety Open and the Consumers processing of the first packet produced after the producers reception of the Time_Coordination message shall be less than 8,3 s.

7.6.5.3 Point-to-point, originator producer, target consumer

When Extended Format point to point connections are originated by the producer, the target consumer shall provide initialization values in the SafetyOpen Response. The originator producer uses these values to initialize production parameters.

The complete process is shown in Figure 55.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

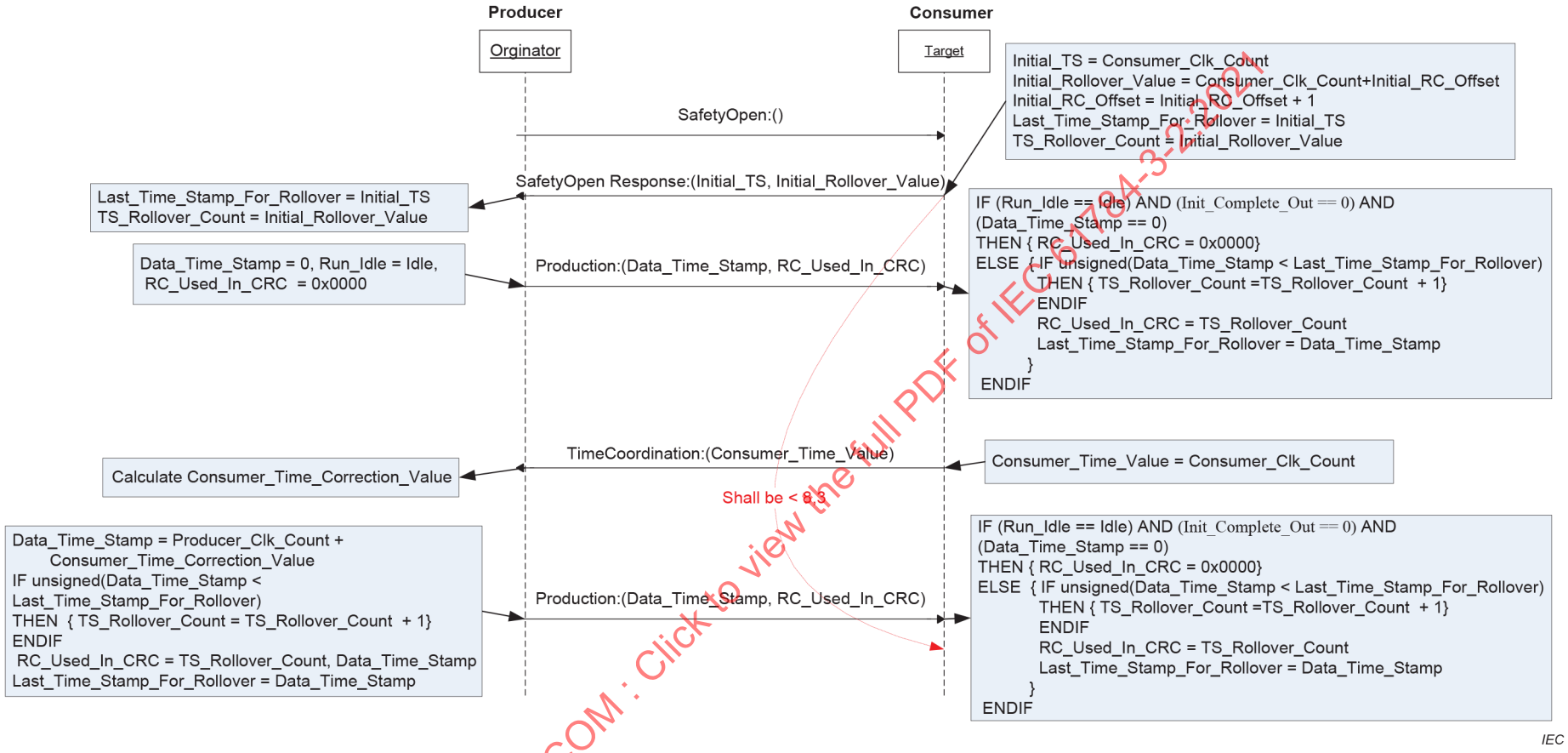


Figure 55 – Point-to-point, originator producer, target consumer

The time between the generation of the Safety Open Response and the Consumers processing of the first packet produced after the producers reception of the Time_Coordination message shall be less than 8,3 s.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

7.6.5.4 Multi-point, originator consumer, target producer

When Extended Format multi-point connections are originated by the consumer; the target producer shall provide initialization values in the SafetyOpen Response. The target consumer uses these values to initialize production parameters. The values the target producer sends in the SafetyOpen Response differs depending on whether this is the 1st consumer to request a connection or not.

The active seeding of the CRC with the rollover count in Extended Format Multi-point messages shall begin immediately on first production.

The complete process is shown in Figure 56.

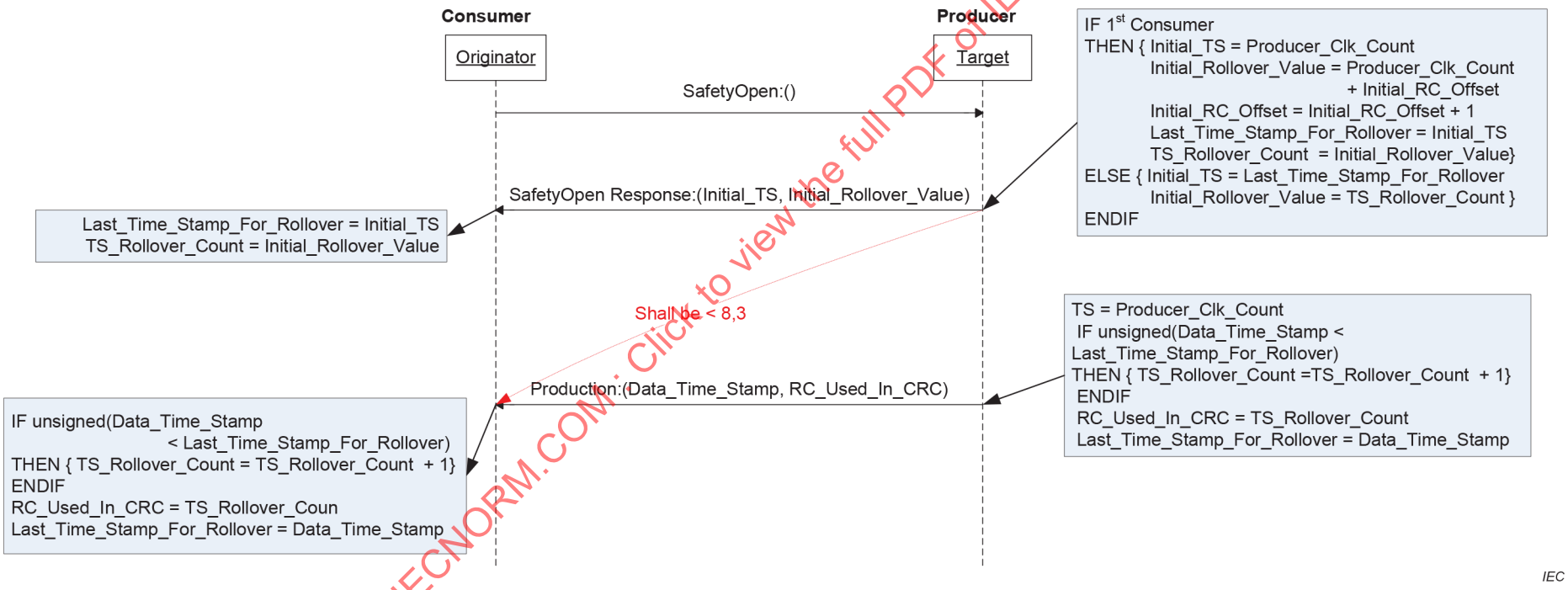


Figure 56 – Multi-point, originator consumer, target producer

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

The time between the generation of the Safety Open Response and the Consumers processing of the first packet shall be less than 8,3 s.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

7.6.6 SafetyValidatorClient function definition

7.6.6.1 General

The SafetyValidatorClient is the embodiment of the safety layer that augments a standard connection on CP 2/3 or CP 2/2 to transmit safety data. It coordinates the production of application data with a peer instance of the SafetyValidatorServer.

7.6.6.2 Safety production

This Subclause 7.6.6 describes the production of data and the interfaces between the application, the SafetyValidatorClient and the underlying link layer. The focus is on the SafetyValidatorClient run-time behavior and its interfaces. The application itself shall be of high integrity to meet the target SIL level and this can be accomplished in many ways and is ultimately a vendor design decision.

Figure 57 graphically shows the data flow between the SafetyValidatorClient and a producing safety-related application. Safety_Data_Out is produced at a periodic rate, referred to as the Expected Packet Interval (EPI). The SafetyValidatorClient shall sample, capture, and time stamp the data to be sent every EPI time period.

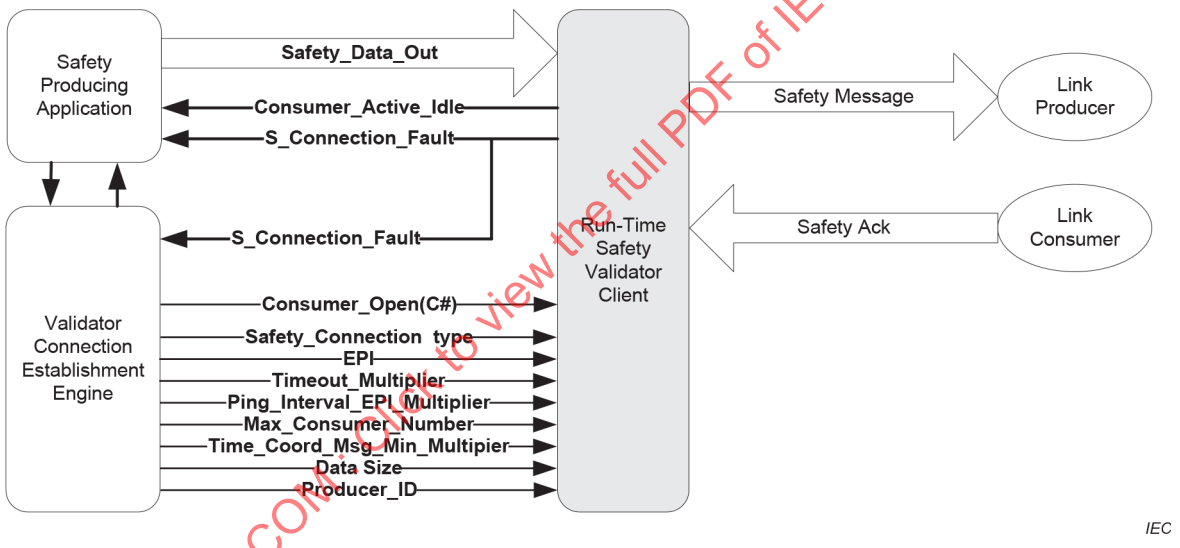


Figure 57 – Safety production data flow

7.6.6.3 Producing application interface

The producing application provides Safety_Data_Out to the SafetyValidatorClient. The SafetyValidatorClient shall build the Mode_Octet, Actual_Data, and Complement_Data, and Time stamp section.

The SafetyValidatorClient shall provide safety connection status back to the producing application for each consumer.

7.6.6.4 Safety data production logic

Subclauses 7.6.6.4 to 7.6.6.8 describe the logic that shall be followed by all safety data producers. The actual implementation of the logic may vary, but equivalent results shall be obtained. The logic in this document assumes an asynchronous producing application that makes the safety data available to the SafetyValidatorClient.

Definitions for the variables used in the safety data production logic can be found in 7.7.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

7.6.6.5 Example safety data production cold start logic

The production logic to initiate a cold start of a connection is:

```
////////////////////////////////////////////////////////////////
// Cold start after connection establishment processing
////////////////////////////////////////////////////////////////
// This Logic should be executed at the transition of the
//  producing connection from closed to open.
// For Point-to-point connections this logic may
//  be performed any time the connection is Opened or Re-Opened.
////////////////////////////////////////////////////////////////

Ping_Interval_EPI_Count = 0,
RR_Con_Num_Index_Pntr = Max_Consumer_Number,

// Initialize the ping count in the safety message to 0
Mode_Octet.Ping_Count = 0,

// Time_Drift_Per_Ping_Interval, the minimum value is 1
Time_Drift_Per_Ping_Interval =
Roundup(EPI × Ping_Interval_EPI_Multiplier / 320000),

FOR (Consumer_Num = 1 to Max_Consumer_Number),
{
      // Producer Dynamic Variables
      Consumer_Active_Idle[Consumer_Num-1] = Idle,
      S_Connection_Fault[Consumer_Num-1] = OK,
      Producer_Rcved_Time_Value[Consumer_Num-1] = 0x0000,
      Consumer_Time_Correction_Value[Consumer_Num-1] = 0x0000,
      Ping_Int_Since_Last_Time_Coord_Msg_Count[Consumer_Num-1] =
0x0000,
      Consumer_Time_Value[Consumer_Num-1] = 0x0000

      // Producer Derived Variables

      // Time_Drift_Constant, the minimum value is 1.
(Time_Drift_Constant is not
      // saved but is used in the calculation of the
      // Connection_Correction_Constant below.)
      Time_Drift_Constant =
                  Roundup((Timeout_Multiplier[Consumer_Num-1] +1)×EPI ×
                        Ping_Interval_EPI_Multiplier / 320000),

      // Connection_Correction_Constant
      Connection_Correction_Constant[Consumer_Num-1] =
Time_Drift_Constant + 1 – Time_Coord_Msg_Min_Multiplier [Consumer_Num-
1],

      // Time_Coord_Response_EPI_Limit
      Time_Coord_Response_EPI_Limit[Consumer_Num-1]= Roundup((5000000 +
                  (Time_Coord_Msg_Min_Multiplier[Consumer_Num-1]×128) +
                  (EPI × ( Consumer_Num – 1))) / EPI),

      // Time_Coord_Response_EPI_Limit has a maximum value of 1000
      IF (Time_Coord_Response_EPI_Limit[Consumer_Num-1] > 1000),
      THEN
      {
            Time_Coord_Response_EPI_Limit[Consumer_Num-1] = 1000,
      }
      ENDIF
}
```

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

```
ENDFOR

////////////////////////////////////////////////////////////////
// end, Cold start after connection establishment processing
////////////////////////////////////////////////////////////////
```

7.6.6.6 Example safety data production multipoint consumer re-start logic

The logic allows individual multipoint consumers to be stopped and restarted while the multipoint production continues to other consumers.

This Subclause 7.6.6.6 defines the logic needed to restart an individual consumer, but it does not represent an efficient implementation of how to detect that the individual connection has been restarted.

```
////////////////////////////////////////////////////////////////
// Re-initialization of Multipoint production to individual consumers
////////////////////////////////////////////////////////////////
// This Logic should be executed after a multipoint consumer performs
//  a successful open to a multipoint producer while the production
//  is in process to re-initialize production to that consumer number
////////////////////////////////////////////////////////////////
FOR (Consumer_Num = 1 to Max_Consumer_Number),
{
IF (Consumer_Open(Consumer_Num-1)transitions from Closed to Open)
  THEN
  {
      // Producer Dynamic Variables
       Consumer_Active_Idle[Consumer_Num-1] = Idle,
       S_Connection_Fault[Consumer_Num-1] = OK,
       Producer_Rcved_Time_Value[Consumer_Num-1] = 0x0000,
       Consumer_Time_Correction_Value[Consumer_Num-1] = 0x0000,
       Ping_Int_Since_Last_Time_Coord_Msg_Count[Consumer_Num-1= 0x0000,

       // Producer Derived Variables
       // Time_Drift_Constant, the minimum value is 1
       //(Time_Drift_Constant is not
       // saved but is used in the calculation of the
       // Connection_Correction_Constant below.)
       Time_Drift_Constant =
      Roundup((Timeout_Multiplier[Consumer_Num-1] +1) × EPI ×
                      Ping_Interval_EPI_Multiplier / 320000),
      // Connection_Correction_Constant
       Connection_Correction_Constant[Consumer_Num-1] =
      Time_Drift_Constant + 1 – Time_Coord_Msg_Min_Multiplier
[Consumer_Num-1],
       // Time_Coord_Response_EPI_Limit
       Time_Coord_Response_EPI_Limit[Consumer_Num-1= Roundup((5000000 +
                 (Time_Coord_Msg_Min_Multiplier[Consumer_Num-1]×128) +
                 (EPI × ( Consumer_Num – 2))) / EPI),

       // Time_Coord_Response_EPI_Limit has a maximum value of 1000
       IF (Time_Coord_Response_EPI_Limit[Consumer_Num-1] > 1000),
       THEN
        {
             Time_Coord_Response_EPI_Limit[Consumer_Num-1] = 1000,
        }
       ENDIF
```

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

```
      }
ENDIF
}
```

7.6.6.7 Example combined data production

The following is the common required logic of the SafetyValidatorClient for all of safety connections.

```
////////////////////////////////////////////////////////////////
// start of EPI Safety Data production processing
////////////////////////////////////////////////////////////////
// This logic assumes that the application has passed the Safety
//  Data and Application_Run_Idle to the Safety Validator.
//
////////////////////////////////////////////////////////////////
// Capture the time to be used for the time stamp
Producer_Safe_Data_TS = Producer_Clk_Count,

// Check if it is time to increment the Ping Count
Ping_Interval_EPI_Count = Ping_Interval_EPI_Count + 1,

IF (Ping_Interval_EPI_Count >= Ping_Interval_EPI_Multiplier),
THEN
{
Increment Mode_Octet.Ping_Count,
Ping_Interval_EPI_Count = 0,
}
ENDIF

// Set the remainder of the Mode_Octet bits
Mode_Octet.Run_Idle = Application_Run_Idle,
Mode_Octet.TBD_Bit  = 0,
Mode_Octet.TBD_2_Bit  = 0,

// Execute the safety producer, connection type specific functions
IF (Connection_Type == multipoint),
THEN
{
multi_cast_producer_function(),
}
ELSE
{
single_cast_producer_function(),
}
ENDIF


// set Mode_Octet redundant bits (2:4) to the correct values
Mode_Octet = (Mode_Octet AND 0xe3)OR((Mode_Octet>>3) AND 0x1c XOR
0x14),
Calculate Data Section CRC,
Calculate Time_Stamp Section CRC,
Trigger the sending of the Data Message,

// If on FSCP 2 on CP 2/3 and Multipoint, send the Time Correction
//  Message if it is time.
IF ((Connection_Type == CP 2/3) AND
(Send_Time_Correction_Message == 1)),
THEN
{
```

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

```
Trigger the sending of the Time Correction Message,
Send_Time_Correction_Message = 0,
}
ENDIF
////////////////////////////////////////////////////////////////
// end of safety data production processing
////////////////////////////////////////////////////////////////


////////////////////////////////////////////////////////////////
// Start of point-to-point production function
////////////////////////////////////////////////////////////////
single_cast_producer_function()
// Check if a Time Coordination message has been received in
//  the allotted time.
IF (Ping_Interval_EPI_Count == 8),
THEN
{
Increment Ping_Int_Since_Last_Time_Coord_Msg_Count[0],
IF (Ping_Int_Since_Last_Time_Coord_Msg_Count[0]
>= (Timeout_Multiplier[0] + 2)),
      THEN
{
      S_Connection_Fault[0]=Faulted,
}
ENDIF
}
ENDIF

//Hold Data_Time_Stamp = 0 until time coordination msg received
IF(Consumer_Active_Idle[0] == Idle),
THEN
{
Mode_Octet.Run_Idle = Idle,
Time_Stamp_Section.Data_Time_Stamp = 0x0000,
}
ELSE
{
Time_Stamp_Section.Data_Time_Stamp = Producer_Safe_Data_TS +
Consumer_Time_Correction_Value[0],
}
ENDIF

END single_cast_ producer_function()
////////////////////////////////////////////////////////////////
// end of point-to-point processing
////////////////////////////////////////////////////////////////


////////////////////////////////////////////////////////////////
// Start of multipoint production function
////////////////////////////////////////////////////////////////
multi_cast_producer_function()
// Check if its time to start sending Time Correction messages
// Time Correction messages are sent starting at the 8th EPI
production
//  within the Ping interval
IF (Ping_Interval_EPI_Count == 8),
THEN
{
RR_Con_Num_Index_Pntr = 0,
}
ENDIF
```

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

```
// Check if a Time Coordination message has been received in
//  the allotted time.
IF (RR_Con_Num_Index_Pntr < Max_Consumer_Number),
THEN
{
Increment
Ping_Int_Since_Last_Time_Coord_Msg_Count[RR_Con_Num_Index_Pntr],
IF (Ping_Int_Since_Last_Time_Coord_Msg_Count[RR_Con_Num_Index_Pntr]
             >= (Timeout_Multiplier[RR_Con_Num_Index_Pntr] + 2)),
THEN
{
      Set S_Connection_Fault[RR_Con_Num_Index_Pntr]=Faulted,
}
ENDIF
ENDIF

// Check if its time to send an active non-error Time Correction
//  message
IF ((RR_Con_Num_Index_Pntr < Max_Consumer_Number) AND
   (Consumer_Active_Idle[RR_Con_Num_Index_Pntr] == Active)), AND
   (Consumer_Open[RR_Con_Num_Index_Pntr] == Open) AND
   (S_Connection_Fault[RR_Con_Num_Index_Pntr] == OK)
THEN
{
Send_Time_Correction_Message = 1,
Mcast_Octet.Consumer_# = RR_Con_Num_Index_Pntr + 1,
Mcast_Octet.Multi_Cast_Active_Idle =
Consumer_Active_Idle[RR_Con_Num_Index_Pntr],
Time_Correction_Section.Time_Correction_Value =
Consumer_Time_Correction_Value[RR_Con_Num_Index_Pntr],
 Set Mcast_Octet.Parity_Even to the correct value,
MCast_Octet_2 = ((MCast_Octet XOR 0xFF) AND 0x55) OR
(MCast_Octet AND 0xAA)
Calculate CRC of time correction message,
}
ELSE
{
//load null TIME_CORRECTION Section,
Mcast_Octet.Consumer_# = 0,
Mcast_Octet.Multi_Cast_Active_Idle = Idle,
Time_Correction_Section.Time_Correction_Value = 0,
 Set Mcast_Octet.Parity_Even to the correct value,
MCast_Octet_2 = ((MCast_Octet XOR 0xFF) AND 0x55) OR
 (MCast_Octet AND 0xAA)
Calculate CRC of time correction section,
}
ENDIF

// If Time Correction messages are being sent, increment to the
//  next consumer
IF (RR_Con_Num_Index_Pntr < Max_Consumer_Number),
THEN
{
RR_Con_Num_Index_Pntr = RR_Con_Num_Index_Pntr + 1,
}
ENDIF

// Set the time stamp value
Time_Stamp_Section.Data_Time_Stamp = Producer_Safe_Data_TS,
END multi_cast_producer_function()
////////////////////////////////////////////////////////////
// end of multipoint processing
```

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

```
////////////////////////////////////////////////////////////////
```

7.6.6.8 Example time coordination message reception logic

The SafetyValidatorClient shall complete the following steps for each time coordination message received. For point-to-point and multipoint safety connections, a Consumer_Time_Value is received in the time coordination message.

Producers shall allow Time Coordination responses to arrive during the Ping_Interval or Ping_Interval +1.

```
////////////////////////////////////////////////////////////////
//Time Coordination message reception processing
////////////////////////////////////////////////////////////////
// Consumer_Num equals 1 for point to point
// Consumer_Num equals the consumer the message
//  was received from for multipoint
////////////////////////////////////////////////////////////////
// This Logic should only be executed If Ack_Byte.Ping_Response
//  of the message is equal to 1 AND Consumer_Open[Consumer_Num-1]
//  is equal to Open. If Ack_Byte.Ping_Response is equal to 0 OR
//  Consumer_Open[Consumer_Num-1]is equal to Closed, this
//  message should be ignored.
////////////////////////////////////////////////////////////////
// reject Time Coordination packets if CONSUMER_TIMESTAMP has
// previously been captured AND this is not the first time
// coordination message from this consumer
IF (  (Consumer_Time_Value[Consumer_Num-1] ==
Time_Coordination_Section.Consumer_Time_Value)  AND
        (Consumer_Active_Idle[Consumer_Num-1] == Active) )
THEN
{
        // the only time this would be the case is if that Time
Coordination was already received
        Abort the processing of this packet. Do Not close the
connection.
}
ENDIF


// Capture the received time
Producer_Rcved_Time_Value[Consumer_Num-1] = Producer_Clk_Count,

// Perform the integrity checks
Check the CRC of the Time Coordination Section, based on format used,
Ack_Byte_Error = false,
IF ((Ack_Byte parity incorrect)
THEN
{
Ack_Byte_Error = true,
}
ENDIF
IF (BaseFormat)
THEN
{
//ckeck Ack_Byte_2 if BaseFormat
IF ((Ack_Byte parity incorrect) OR (Ack_Byte_2 !=
   (((Ack_Byte XOR 0xFF) AND 0x55) OR (Ack_Byte AND 0xAA))))
THEN
{
Ack_Byte_Error = true,
}
ELSE
```

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

```
{
Ack_Byte_Error = false,
}
ENDIF
ENDIF
IF ((CRC_Error based on format used) OR (Ack_Byte_Error = true) OR
// Ensure that the Time Coordination message returned
//  with the same ping interval or the next ping interval.
//  The next ping interval is allowed for the case that a
//  multipoint consumer connects to an existing producer.
//  If the new consumer receives its first message near the end
//  of the ping interval, the time coordination may arrive back
//  at the producer during the next ping interval.
     ((Ack_Byte.Ping_Count_Reply != Ping_Count) AND
      (Ack_Byte.Ping_Count_Reply != Ping_Count-1)) OR
// Ensure that the Time Coordination message returned
//  within the approximatley 5 second limit
((Consumer_Active_Idle[Consumer_Num-1] == Active) AND
 (Ping_Interval_EPI_Count >
           Time_Coord_Response_EPI_Limit[Consumer_Num-1])),
THEN
{
IF (ExtendedFormat),
THEN
{
//decide whether to close the connection or not
Increment Producer_Fault_Counter[Consumer_Num-1]
IF (Producer_Fault_Counter[Consumer_Num-1] >=
Max_Fault_Number[Counsumer_Num-1])
THEN
{
S_Connection_Fault[Consumer_Num-1] = Faulted,
Abort the processing of this packet. Close the connection.
}
ELSE
{
Abort the processing of this packet. Do Not close the connection.
}
ENDIF
}
ELSE
{
S_Connection_Fault[Consumer_Num-1] = Faulted,
Abort the processing of this packet. Close the connection.
}
ENDIF
}
ENDIF

// at this point we know we have a good, non-redundant time
coordination packet

// Capture the received CONSUMER time
Consumer_Time_Value[Consumer_Num-1] =
           Time_Coordination_Section.Consumer_Time_Value;

// Determine the worst case Consumer_Time_Correction_Value based on
the
//  received Time_Coordination section
Worst_Case_Consumer_Time_Correction_Value[Consumer_Num-1] =
      Time_Coordination_Section.Consumer_Time_Value
      - Producer_Rcved_Time_Value[Consumer_Num-1]
- Connection_Correction_Constant[Consumer_Num-1],
```

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

```
// Determine the worst case time drift since the last
//  Time Coordination information was received. This is equal to the
//  number of Ping Intervals since the last Time Coordination message
//  times the Time Drift per Ping Interval plus 1 for the asyncronous
//  clocks. This value will not be used until the second
//  Time_Coordination message is recived.

Time_Drift_Since_Last_Time_Coord =
({Ping_Int_Since_Last_Time_Coord_Msg_Count[Consumer_Num-1]+ 1}
  * Time_Drift_Per_Ping_Interval) + 1,

// If this Time_Coordination Transport delay is greater then the
//  last Time_Coordination Transport delay by more than the
appropriate
//  number of Time_Drift_Per_Ping_Intervals, then, use the previous
//  Correction value minus the appropriate number of
//  Time_Drift_Per_Ping_Intervals. This action is not taken until the
//  second Time_Coordination message is received.
// The math for this check should be 16 bit or greater
IF ((Consumer_Active_Idle[Consumer_Num-1] == Active) AND
((Consumer_Time_Correction_Value[Consumer_Num-1]-
      Worst_Case_Consumer_Time_Correction_Value[Consumer_Num-1] –
 Time_Drift_Since_Last_Time_Coord) AND 0x8000 == 0)),
THEN
{
Consumer_Time_Correction_Value[Consumer_Num-1] =
Consumer_Time_Correction_Value[Consumer_Num-1] -
Time_Drift_Since_Last_Time_Coord,
}
ELSE
{
Consumer_Time_Correction_Value[Consumer_Num-1] =
Worst_Case_Consumer_Time_Correction_Value[Consumer_Num-1],
}
ENDIF

// Set the flag indicating a Time_Coordination message has been
received
IF (S_Connection_Fault[Consumer_Num-1] = OK)
THEN
{
Consumer_Active_Idle[Consumer_Num-1] = Active,
}
ENDIF

// Reset the Time_Coordination message timer
Ping_Int_Since_Last_Time_Coord_Msg_Count[Consumer_Num-1] = 0,
////////////////////////////////////////////////////////////
// end producer time coordination information reception processing
////////////////////////////////////////////////////////////
```

7.6.7 SafetyValidatorServer function definition

7.6.7.1 General

The SafetyValidatorServer function is the safety layer that augments a standard connection on CP 2/3 or CP 2/2 to transmit safety data. It coordinates the reception of safety data with a peer instance of the SafetyValidatorClient class and delivers this data to the consuming safety-related application.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

7.6.7.2 Safety consumption

This Subclause 7.6.7 describes the consumption of data and the interfaces between the application, the SafetyValidatorServer and the underlying link layer.

There are two versions of safety data consumer monitoring. They are:

- SafetyValidatorServer – Link Triggered.
  This is appropriate for consuming applications that are synchronized to the reception of the data, or consuming applications that present a continuous delay from the reception of data.
- SafetyValidatorServer – Application Triggered.
  This is appropriate for consuming applications that are periodic in nature and not synchronized to the reception of the data.

In both versions, the SafetyValidatorServer shall perform the following aspects of the safety data monitoring:

- Time coordination with the producer;
- Time stamp section integrity checking;
- Data integrity checking;
- Network time expectation checking.

7.6.7.3 SafetyValidatorServer – link triggered

Figure 58 shows the data flows for the SafetyValidatorServer in the link triggered mode.

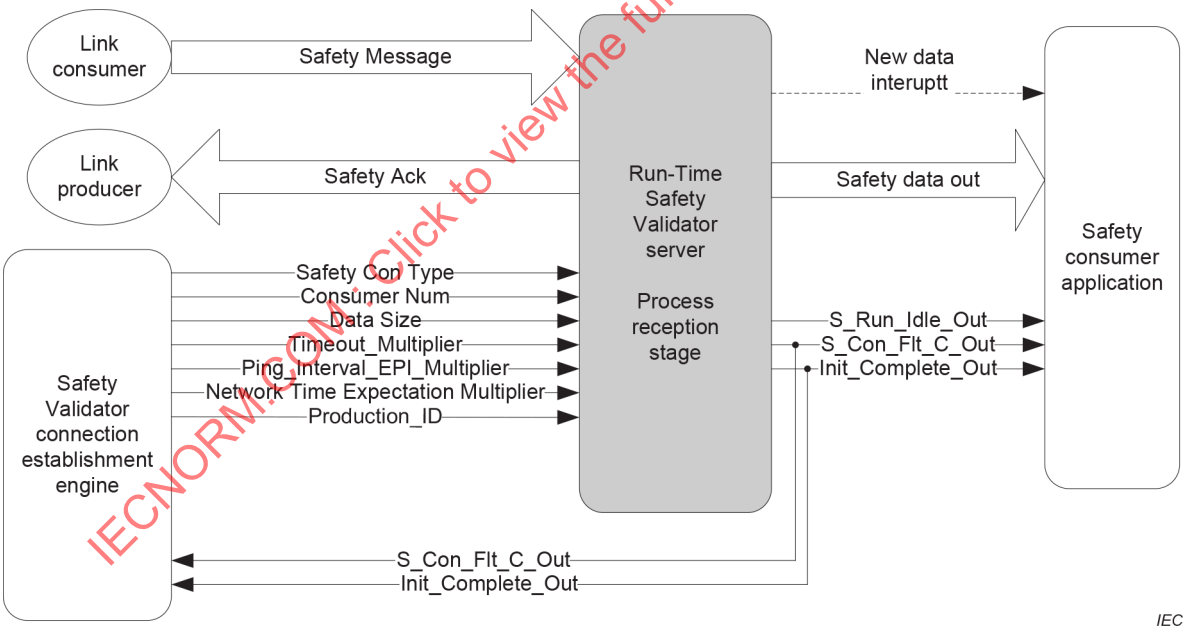


Figure 58 – Consumer safety data monitoring

The Link Triggered SafetyValidatorServer shall perform all aspects of the safety protocol on each message received.

For multipoint, the Link Triggered SafetyValidatorServer shall also perform all aspects of the safety protocol on each Time_Correction section received.

The SafetyValidatorServer shall insure that the safety data presented to the consuming application has been crosschecked and that the network time expectation is being met.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

The Link Triggered SafetyValidatorServer shall set the new data flag each time data is ready for consumption.

7.6.7.4 SafetyValidatorServer – application triggered

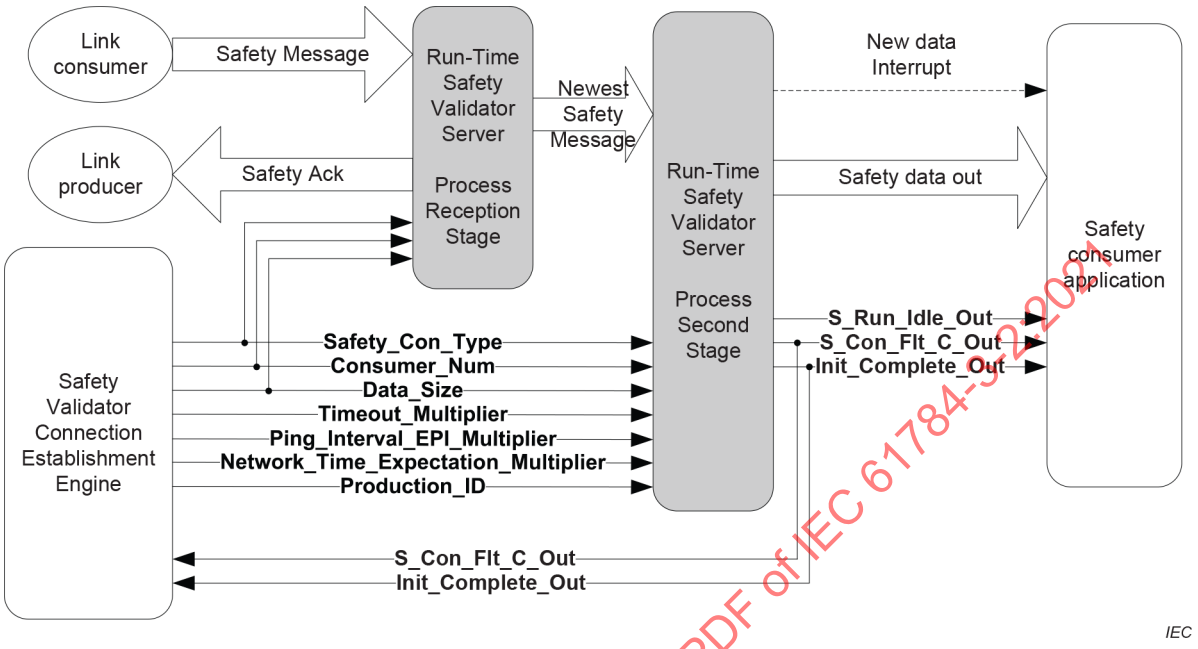


Figure 59 – SafetyValidatorServer – application triggered

The Application Triggered SafetyValidatorServer does not fully process each message.

The Process Reception Stage of the application triggered SafetyValidatorServer shall check the ping count for all incoming data messages.

For multipoint consumption in application triggered SafetyValidatorServers, the latest Time_Correction section received shall be forwarded to the consuming application.

The consuming safety-related application shall request new data from the SafetyValidatorServer in order to cause the SafetyValidatorServer to complete processing of a message.

For periodic applications that are not synchronized to the reception of the data, this reduces the processing burden, since the data section is only crosschecked (in Process Second Stage in Figure 59 for the safety data messages that are used. This is particularly useful for the case where the network EPIs are at a faster rate then the consuming application's periodic rate.

The consuming application shall ensure that it gets new data at least once every 2 s to ensure that the time stamp does not rollover.

7.6.7.5 Safety data reception logic

The safety data reception processing consists of:

- Ping_Count check;
- Time Stamp section checking;
- Data integrity checking;
- Time stamp checking;

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

- Deriving Run_Idle and fault status.

The definitions of the variables used in the safety data reception logic can be found in 7.7.7.6.

Table 95 defines the safety data processing steps that are performed by the Link Triggered SafetyValidatorServer.

Table 95 – Data reception – Link triggered

	Point-to-point	Multipoint
Check Ping_Response	No	No
Check Ping_Count	Yes	Yes
Check Time stamp section CRC	Yes	Yes
Check Run_Idle	Yes	Yes
Check TBD_Bit	Yes	Yes
Check Data CRCs	Yes	Yes
Check Data Actual/Complement	Yes	Yes
Derive Data_Time_Stamp	Yes	Yes

Table 96 defines the safety data processing steps that shall be performed by the Link Triggered SafetyValidatorServer for the reception of each Time Correction section.

Table 96 – Time_Correction reception – Link triggered

Multipoint	Multipoint
Check MCast_Octet and MCast_Octet_2	Yes, if consumer_# match
Check Time_Correction CRC	Yes, if consumer_# match
Get Time_Correction_Value	Yes, if consumer_# match
Check Multi_Cast_Active_Idle	Yes, if consumer_# match

Table 97 defines the safety data processing steps that are performed on each message reception by the application triggered SafetyValidatorServer.

Table 97 – Data reception – Application triggered

	Point-to-point	Multipoint
Check Ping_Response	No	No
Check Ping_Count	Yes	Yes
Check Time stamp section CRC	No	No
Check Run_Idle	No	No
Check TBD_Bit	No	No
Check Data CRCs	No	No
Check Data Actual/Complement	No	No
Derive Data_Time_Stamp	No	No

Table 98 defines the safety data processing steps that shall be performed on each Time_Correction section reception by the application triggered SafetyValidatorServers.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Table 98 – Time_Correction reception – Application triggered

	Multipoint
Check MCast_Octet and MCast_Octet_2	Forward message if consumer_# match
Check Time_Correction CRC	No
Get Time_Correction_Value	no
Check Multi_Cast_Active_Idle	No

Table 99 defines the safety data processing steps that are performed by the application triggered SafetyValidatorServer when safety data is requested.

Table 99 – Consuming application – Safety data monitoring

	Point-to-point	Multipoint
Check Ping_Response	NA	NA
Check Ping_Count	NA	NA
Check Time stamp section CRC	Yes	Yes
Check MCast_Octet and MCast_Octet_2	NA	Yes (from last time correction)
Check Time_Correction CRC	NA	Yes (from last time correction)
Get Time_Correction_Value	NA	Yes (from last time correction)
Check Multi_Cast_Active_Idle	NA	Yes (from last time correction)
Check Run_Idle	Yes	Yes
Check TBD_Bit	Yes	Yes
Check Data CRCs	Yes	Yes
Check Data Actual/Complement	Yes	Yes
Derive Data_Time_Stamp	Yes	Yes

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

7.6.7.6 Ping count checking

The SafetyValidatorServer shall perform Ping_Count checking on every message. Ping_Count checking checks the ping count to see if it has changed.

If a SafetyValidatorServer detects that the ping count has changed, it shall produce a time coordination message within that Ping Interval or within 5 s, whichever is less.

Ping_Count checking errors should not be treated as dangerous failures. The time stamp section CRC does not need to be checked to perform the Ping_Count checking.

7.6.7.7 Data and network time expectation checking maximum interval

The data integrity shall be checked at least once every 2 s.

The Time Stamp and Network Time Expectation (NTE) shall be checked at least once every 2 s.

7.6.7.8 Example cold start initialization

```
////////////////////////////////////////////////////////////////
// Cold start after connection establishment processing
////////////////////////////////////////////////////////////////
// This Logic should be executed at the transition of the
//  consuming connection from closed to open.
////////////////////////////////////////////////////////////////

S_Con_Flt_C_Out = OK,
Init_Complete_Out = 0,
S_Run_Idle_Out = Idle,

Last_Ping_Count = 3,
Time_Coordination_Count_Down = 0x0000,

Corrected_Data_Time_Stamp = 0x0000,
Last_Data_Time_Stamp = 0x0000,
Last_Rcved_Multi_Cast_Active_Idle  = Idle,
Last_Rcved_Time_Correction_Value  = 0x0000,
Time_Correction_Ping_Interval_Count = 0x0000,
Time_Correction_Received_Flag = 0,
Data_Age = 0x0000,
Max_Data_Age = 0x0000,
////////////////////////////////////////////////////////////////
// end, Cold start after connection establishment processing
////////////////////////////////////////////////////////////////
```

7.6.7.9 SafetyValidatorServer – link triggered logic

Subclauses 7.6.7.10 and 7.6.7.11 describe the consumer safety data reception logic for the SafetyValidatorServer – Link Triggered option. The term Link Triggered means that all the logic is executed on every reception.

Subclause 7.6.7.10 describes the combined logic associated with the Safety data packet reception for the point-to-point and multipoint safety connection types.

Subclause 7.6.7.11 describes the logic associated with the Time Correction Message reception for the multipoint safety connection type.

This logic shall only be executed if the connection is open with no errors.

7.6.7.10 Example combined reception logic – link triggered logic

The following is the required SafetyValidatorServer reception logic for the safety data packet reception of the point-to-point or multipoint safety connection type, for the SafetyValidatorServer – Link Triggered Logic.

Multipoint connections shall send a Time Coordination Message (Consumer_Num – 1) receptions after the ping count change.

Multipoint-consumers connecting to an existing producer shall send the Time_Coordination message immediately upon the first valid reception.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

```
////////////////////////////////////////////////////////////////
// Safety Data Consumption – link triggered logic
////////////////////////////////////////////////////////////////

// If the Extended  Format is being used, we shall determine a
rollover value to
// be used when calculating CRCs before we attempt to validate the
message
// (since the rollover is part of CRC values in the message).
IF (ExtendedFormat),
THEN
{
// For point to point, a time_stamp other than 0 or a Run
//  indication, indicate that the Time_Coordination_Message has been
//  received by the Client and the corrected time stamp is being used.
IF ((Point to point) AND  (Init_Complete_Out == 0) AND
(Time_Stamp_Section.Data_Time_Stamp == 0) AND
      (Mode_Byte.Run_Idle == IDLE)),
THEN
{
      RC_Used_in_CRC  = 0x0000,
}
ELSE
{
RC_Used_in_CRC  = TS_Rollover_Count,

// check for time stamp rollover
IF (unsigned compare(Time_Stamp_Section.Data_Time_Stamp <
       Last_Time_Stamp_For_Rollover))
THEN
{
          RC_Used_in_CRC = RC_Used_in_CRC  + 1,
}
ENDIF
}
ENDIF
  }
ENDIF

Temp_Fault_Flag = OK,

// check for data integrity faults
IF ((CRC Error based on format used)
OR (Complement_Data_Section CRC != OK)
OR (Mode_Byte.Run_Idle != not Mode_Byte.N_Run_Idle)
OR (Mode_Byte. TBD_2_Bit !=
Mode_Byte. TBD_2_Bit _Copy)
OR (Mode_Byte.TBD_Bit != not Mode_Byte.N_TBD_Bit)
OR (Actual_Data != not Complement_Data) [for > 2 bytes only]
),
THEN
{
      Temp_Fault_Flag = Faulted,
}
ENDIF

// Set up Time_Stamp_Delta, to be used to check for out of sequence
//  messages  Time_Stamp_Delta is not calculated until the EPI
//  reception after Init_Complete_Out is set to 1.
IF(Init_Complete_Out == 0),
THEN
{
      Time_Stamp_Delta = 1,
```

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

```
}
ELSE
{
      Time_Stamp_Delta = Time_Stamp_Section.Data_Time_Stamp –
Last_Data_Time_Stamp,
}
ENDIF

// Take a look at the time stamp delta and determine if it indicates
// the message was received in the right order.
IF ((Time_Stamp_Delta < 0) OR
      (Time_Stamp_Delta > Network_Time_Expectation_Multiplier)),
THEN
{
Temp_Fault_Flag = Faulted,
}
ENDIF

// If the Extended  Format is being used, we can drop some packets
with
// data integrity/message validation or out of order errors.
IF ((ExtendedFormat) AND (Temp_Fault_Flag == Faulted)),
THEN
 {
increment Consumer_Fault_Counter

// Calculate updated data age for the data in the last good packet
IF (Init_Complete_Out)
THEN
{
                     Data_Age = Consumer_Clk_Count –
Last_Corrected_Data_Time_Stamp,
}
ENDIF

// Calculate the maximum worst case age
IF (Data_Age > Max_Data_Age)
THEN
{
           Max_Data_Age = Data_Age,
}
ENDIF

// Is it OK to ignore this error?
// It is OK if the consumer fault counter is not greater than the
// maximum faults allowed and the updated data age from the
// last good packet still meets our data age criteria
// (less than the time expectation multiplier)
IF (
       (Consumer_Fault_Counter < Max_Fault_Number) AND
       (Data_Age <= Network_Time_Expectation_Multiplier)
     )
THEN
{
Abort the processing of this packet. Do Not close the connection.
Do not use the Data.
Do not update Last_Corrected_Data_Time_Stamp or Last_Data_Time_Stamp
           }
ELSE
{
                S_Con_Flt_C_Out = Faulted,
             Abort the processing of this packet. Close the
connection.
```

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

```
}
  ENDIF
}
ENDIF

// execute a function that checks for ping count changes and
// determines if it is time to produce a time coordination message
ping_count_check_in_consumer_function(),

Init_Complete_Out_Temp = 0,

// execute the safety connection type specific functions
IF (Connection_Type == Multipoint),
THEN
{
      multi_cast_consumer_function(),
}
ELSE
{
      single_cast_consumer_function(),
}
ENDIF

         // If we are using the ExtendedFormat, at this point we have
a properly formatted
// message that was received in the right order. With the Extended
Format
// update the rollover count and last timestamp for rollover.
IF (ExtendedFormat),
THEN
{
      // Only update the rollover count if this is a multipoint
connection
      // or if this is a point to point connection that is out of the
initialization
      // phase.
      IF ((Connection_Type == Multipoint) OR
            (Init_Complete_Out_Temp == 1)),
      THEN
      {
            // Check the timestamp value in the message to determine if
a
            // rollover has occurred, and if so, update the rollover
count
            // accordingly.
            IF (unsigned compare(Time_Stamp_Section.Data_Time_Stamp <
                  Last_Time_Stamp_For_Rollover))
            THEN
            {
            TS_Rollover_Count  = TS_Rollover_Count  + 1,
            }
            ENDIF

             Last_Time_Stamp_For_Rollover =
Time_Stamp_Section.Data_Time_Stamp,
      }
      ENDIF

      // Save the corrected data timestamp so we can recalculate a data
age
      // if the next packet has errors.
      Last_Corrected_Data_Time_Stamp = Corrected_Data_Time_Stamp,
}
```

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

```
        ENDIF

// Save Time stamp for next reception sequence check
Last_Data_Time_Stamp = Time_Stamp_Section.Data_Time_Stamp,

// Calculate the worst case age
IF (Init_Complete_Out_Temp == 1),
THEN
{
      Data_Age = Consumer_Clk_Count – Corrected_Data_Time_Stamp,
}
ENDIF

// Calculate the maximum worst case age
IF (Data_Age > Max_Data_Age)
THEN
{
      Max_Data_Age = Data_Age,
}
ENDIF

// Check for Age, Integrity, and out of sequence faults
IF (( unsigned int_16( Data_Age > Network_Time_Expectation_Multiplier)
AND (Init_Complete_Out_Temp == 1))
OR (Temp_Fault_Flag == Faulted))
         THEN
{
// The connection will be closed, the data should not be used
S_Con_Flt_C_Out_Temp = Faulted,
}
ENDIF

////////////////////////////////////////////////////////////
// The following information is passed on to the consuming application
//   with block integrity: Safety
Data,Init_Complete_Out,S_Run_Idle_Out
//   and S_Con_Flt_C_Out.
// The time between the checking of the age of the data and passing
//  the data off to the consuming application shall be protected under
//  the time_stamp check or the consuming application time checks.
////////////////////////////////////////////////////////////
Make Safety Data Available to Consuming Application
Init_Complete_Out = Init_Complete_Out_Temp,
S_Run_Idle_Out    = S_Run_Idle_Out_Temp,
S_Con_Flt_C_Out   = S_Con_Flt_C_Out_Temp,
 ////////////////////////////////////////////////////////////
// end Safety Data Consumption – link triggered logic
////////////////////////////////////////////////////////////

////////////////////////////////////////////////////////////
// Start of point to point consumer function
////////////////////////////////////////////////////////////
single_cast_consumer_function()
// For point to point multipoint, no time stamp correction is required
Corrected_Data_Time_Stamp = Time_Stamp_Section.Data_Time_Stamp,

// Determine the Init_Complete_Out state to be passed on to the
//  consuming application.
// For point to point or bi-dir, a time_stamp other than 0 or a Run
//  indication, indicate that the Time_Coordination_Message has been
//  received by the Client and the corrected time stamp is being used.
IF ((Init_Complete_Out == 1) OR
      (Corrected_Data_Time_Stamp != 0) OR
```

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

```
      (Mode_Byte.Run_Idle == Run)),
THEN
{
      Init_Complete_Out_Temp = 1,
}
ENDIF

// Determine the Run_Idle indication to be passed on to the consuming
//  application.
IF (((Mode_Byte.Run_Idle == Idle) OR (Init_Complete_Out_Temp == 0))
THEN
{
      S_Run_Idle_Out_Temp = Idle,
}
ELSE
{
      S_Run_Idle_Out_Temp = Run,
}
ENDIF

END single_cast_consumer_function()
////////////////////////////////////////////////////////////////
// end of point to point processing
////////////////////////////////////////////////////////////////

////////////////////////////////////////////////////////////////
// Start of multipoint consumer function
////////////////////////////////////////////////////////////////
multi_cast_consumer_function()
// If multipoint, check that a time correction message has been
//  received within the last Timeout_Multiplier.PI + 1 Ping Intervals
IF  (Time_Correction_Ping_Interval_Count > (Timeout_Multiplier.PI +
1))
THEN
{
      Temp_Fault_Flag = Faulted,
}
ENDIF

// If multipoint, add correction value to time stamp
Corrected_Data_Time_Stamp =  Time_Stamp_Section.Data_Time_Stamp +
 Last_Rcved_Time_Correction_Value
// Determine the Init_Complete_Out state to be passed on to the
//  consuming application.
// For multipoint, the reception of a Time_Coorection Message,
indicate
//  that data may be used.
IF (Time_Correction_Received_Flag == 1)
THEN
{
      Init_Complete_Out_Temp = 1,
}
ENDIF
// Determine the Run_Idle indication to be passed on to the consuming
//  application.
IF ((Mode_Byte.Run_Idle == Idle) OR
    (Init_Complete_Out_Temp == 0) OR
    (Time_Correction_Received_Flag == 0) OR   //used only on
multipoint
    (Last_Rcved_Multi_Cast_Active_Idle==Idle))//used only on
multipoint
THEN
{
```

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

```
      S_Run_Idle_Out_Temp = Idle,
}
ELSE
{
      S_Run_Idle_Out_Temp = Run,
}
ENDIF
end multi_cast_consumer_function()
////////////////////////////////////////////////////////////////
// end of multipoint processing
////////////////////////////////////////////////////////////////


////////////////////////////////////////////////////////////////////////
/////////
// Start of ping count check function
////////////////////////////////////////////////////////////////////////
/////////
ping_count_check_in_consumer_function()

// Check if its time to send a Time Coordination Message
// Multipoint connections send a Time Coordination Message
//   (Consumer_Num – 1) receptions after the ping count change.
IF (received Mode_Byte.Ping_Count != Last_Ping_Count),
THEN
{
      Time_Coordination_Count_Down = Consumer_Num,
       Increment Time_Correction_Ping_Interval_Count,
}
ENDIF

//    For multipoint-consumers connecting to an existing producer,
send
//    the Time_Coordination message immediately upon the 1st reception.
IF (It is the first data reception),
THEN
{
      Produce Time_Coordination_Message,
Time_Coordination_Count_Down = 0,
}
ENDIF

// Check if a ping count change has been detected and the Time
//   Coordination message has not been sent yet.
IF (Time_Coordination_Count_Down > 0),
THEN
{
decrement Time_Coordination_Count_Down,

               // Send the Time_Coordination_message if the decremented
//  Time_Coordination_Count_Down transitions to 0
IF (Time_Coordination_Count_Down == 0),
THEN
{
      Produce Time_Coordination_Message,
}
ENDIF
}
ENDIF

// Save ping count for next reception check
Last_Ping_Count = Mode_Byte.Ping_Count,
```

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

```
end ping_count_check_in_consumer_function()
////////////////////////////////////////////////////////////////////
////////////////////////////
// end of ping count check function
////////////////////////////////////////////////////////////////////
```

7.6.7.11 Example time correction message reception – link triggered logic

The following is the required SafetyValidatorServer logic associated with the Time Correction Message reception for the multipoint safety connection type, for the Consumer – Link Triggered.

```
////////////////////////////////////////////////////////////////
// Consumer processing – Time Correction Message reception
////////////////////////////////////////////////////////////////
// Is the Time Correction message for this Consumer ?
IF (MCast_Octet.Consumer_Num = Consumer_Num)
 // Perform integrity checks.
THEN
{
IF (Time Coordination message CRC incorrect)
OR (MCast_Octet parity incorrect)
OR {MCast_Octet_2 != (((MCast_Octet XOR0xFF)AND0x55)
           OR(MCast_Octet AND0xAA))}
                OR {(MCast_Octet.Multi_Cast_Active_Idle == Idle)
AND (Last_Rcved_Multi_Cast_Active_Idle == Active)},
      // only one transition from connection idle to active will
// be allowed, to prevent an erroneous idle indication,
// a transistion from active to idle will be latched into
// a fault state
      THEN
{
S_Con_Flt_C_Out = Faulted,
      }
ENDIF

      // Save the Time_Correction_Value.
      Last_Rcved_Time_Correction_Value =
Time_Correction_Section.Time_Correction_Value,

      // Save the Multi_Cast_Active_Idle bit.
      Last_Rcved_Multi_Cast_Active_Idle =
MCast_Octet.Multi_Cast_Active_Idle,

      // Set the Time_Correction_Received_Flag.
      Time_Correction_Received_Flag = 1,

      // Reset the Time Correction timeout counter
      Time_Correction_Ping_Interval_Count = 0,
ENDIF
////////////////////////////////////////////////////////////////
// end – Time Correction Message reception
////////////////////////////////////////////////////////////////
```

7.6.7.12 SafetyValidatorServer – application triggered logic

For SafetyValidatorServer – Application Triggered, the same logic described above shall be performed by the combination of the SafetyValidatorServer, but only when requested by the consuming application. Application Triggered implementations only process the safety packets when needed by the application. This implementation strategy is useful for applications that usually run slower than a typical EPI rate. The functions can be divided as defined in Table 96 and Table 99.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

The protocol processing steps defined in Table 99 only need to be performed on the messages used by the consuming application.

7.6.7.13 Example time coordination message production logic

The SafetyValidatorServer shall perform the following steps each time a time coordination message is sent. For point-to-point and multipoint safety connections, time coordination data is sent in the time coordination message. This logic is also described in the single_cast_function() of the combined production logic section.

```
////////////////////////////////////////////////////////////////
//Time Coordination message production processing
////////////////////////////////////////////////////////////////
// Set the Ping_Count_Reply to the value captured at the ping request
Ack_Octet.Ping_Count_Reply = Mode_Octet.Ping_Count,

// Set the Ping_Response bit to 1
Ack_Octet.Ping_Response = 1,

// Set the Consumer_Time_Value to the producers clock value
Time_Coordination_section.Consumer_Time_Value = Producer_Clk_Count,

// Add data integrity measures
Set Ack_Octet.Reserved(6:4) = 0,
Set Ack_Octet.Reserved(2) = 0,
Set Ack_Octet.Parity_Even bit to the correct value,
Ack_Octet_2 !=(((Ack_Octet XOR 0xFF)AND 0x55)OR
              (Ack_Octet AND 0xAA)),
Calculate CRC on Time Coordination message,
////////////////////////////////////////////////////////////////
// end time coordination message send logic
////////////////////////////////////////////////////////////////
```

7.7 Safety message and protocol data specifications

7.7.1 Mode octet

7.7.1.1 Mode_Octet.Run_Idle

The Run_Idle bit value of 0 shall indicate Idle, and the Run_Idle bit value of 1 shall indicate Run.

For point-to-point connections, the Run_Idle bit shall be set to idle if the producing application is Idle or if the producer is waiting for Time Coordination Message information to be received at the initiation of data production.

If Time Coordination Message information has been received, the Run_Idle bit shall be set to the Run_Idle status indicated by the producing application.

For multipoint connections, the Run_Idle bit shall be set to the Run_Idle status indicated by the producing application.

7.7.1.2 Mode_Octet.N_Run_Idle

The N_Run_Idle complement bit shall always be the complement of the Run_Idle bit.

7.7.1.3 Mode_Octet TBD_2_Bit

The Mode_Octet Reserved TBD_2_bit shall be set to 0 by the producer.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

7.7.1.4 Mode_Octet.TBD_2_Copy

The TBD_2_Copy bit shall always equal to the TBD_2 bit.

7.7.1.5 Mode_Octet.Ping_Count

The Ping_Count is used by the consumer to know when it needs to send a Time Coordination Message.

7.7.1.6 Mode_Octet.TBD_Bit

The Mode_Octet Reserved TBD_bit shall be set to 0 by the producer. The Reserved bits shall be ignored by the consumer except for CRC checking and Actual/Complement checking of the TBD_Bit/N_TBD_Bit pair.

7.7.1.7 Mode_Octet.N_TBD_Bit

The N_TBD_Bit complement bit shall always be the complement of the TBD_Bit.

7.7.2 Time Stamp Section

Time_Stamp_Section.Data_Time_Stamp: the Data_Time_Stamp is the time that the Data was sampled for this production.

For point-to-point, the Data_Time_Stamp is relative to the timer that is on the consumer. For multipoint, the Data_Time_Stamp is relative to the timer that is on the producer.

The Data_Time_Stamp is always in 128 µs increments.

7.7.3 Time Coordination Message

7.7.3.1 Ack_Octet.Ping_Response bit

The Ping_Response bit shall indicate that a ping response is being sent on this data production from the safety data consumer on this node.

If the Ping_Response bit is 1, it shall indicate that the Consumer_Time_Value, and Ping_Count_Reply, are valid on this production.

If the Ping_Response bit is 0, it shall indicate that the Consumer_Time_Value, and Ping_Count_Reply, are not valid on this production and shall be ignored.

7.7.3.2 Ack_Octet.Consumer_Time_Value

The Consumer_Time_Value shall be the safety data consumer's clock value at the time that the message is sent.

The Consumer Time Value is used to derive the Data_Time_Stamp for the other directions data production.

7.7.3.3 Ack_Octet.Ping_Count_Reply

The Ping_Count_Reply is used by each consumer to indicate the ping request that is being responded to.

The Ping_Count_Reply is equal to the value of the Ping_Count that is being responded to.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

7.7.3.4 Ack_Octet.Time Coordination Reserved bits

The Time Coordination Reserved bits shall be set to 0 by the consumer.

The Reserved bits shall be ignored by the producer except for CRC and Ack_Octet_2 checking.

7.7.4 Time correction message

7.7.4.1 Mcast_Octet.Consumer_#

For multipoint produced data the Multi_Cast_Active_Idle, and Consumer_Time_Correction_Value shall be directed to the consumer indicated by the Consumer_# field of the message.

The Consumer_# points to a specific consumer (1 to 15).

The Multi_Cast_Active_Idle, and the Consumer_Time_Correction_Value shall be applied by the consumer indicated by the Consumer_#.

A Consumer_# of 0 shall be used to indicate Multi_Cast_Active_Idle, and the Consumer_Time_Correction_Value are not being transferred if needed.

7.7.4.2 Time_Correction_Section.Consumer_Time_Correction_Value

The Consumer_Time_Correction_Value is used by the multipoint consumer to correct the Producer_Time_Stamp so the resultant time stamp is relative to the consumers' clock.

7.7.4.3 Mcast_Octet.Multi_Cast_Active_Idle

The Multi_Cast_Active_Idle bit value of 0 shall indicate Idle, and the Multi_Cast_Active_Idle bit value of 1 shall indicate Active.

Once the Multi_Cast_Active_Idle bit has been set to Active after 1st data production, this bit shall not be set back to idle until the safety connection is re-initialized.

If the consumer sees the Multipoint_Active_Idle bit transition from Active to Idle, it shall close the connection if the Base Format is used. If the Extended Format is used and the Max_Fault_Count has not been reached, the packet will be dropped, otherwise the connection will be closed.

For multipoint connections, the Run_Idle bit of the Mode_Octet shall be set to the Run_Idle status indicated by the producing application.

The consumer will need to look at both the Run_Idle bit and the Multi_Cast_Active_Idle bit.

7.7.4.4 Mcast_octet.time correction reserved bits

The Time Correction Reserved bits shall be set to 0 by the producer.

The Reserved bits shall be ignored by the consumer except for CRC checking and MC_Octet_2 checking.

7.7.5 Safety data production

7.7.5.1 Producing connection status

The producer connection status shall be determined by the combination of the S_Connection_Fault and the Consumer_Active_Idle flags (see Table 100 for definition).

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Table 100 – Producer connection status determination

S_Connection_Fault	Consumer_Active_Idle	Producer Connection status	Comment
Fault	Don't Care	Status = Faulted	Restart will be required
OK	Idle	Status = Idle	The safety connection has not been activated
OK	Active	Status = Active	The safety connection is active

7.7.5.2 Consumer_Open

For Safety Data producers, Consumer_Open from the Validator Connection Establishment Engine to the Run Time Validator shall be provided to indicate whether or not a particular consumer of the produced data has an active open connection.

If the producer is multipoint, Consumer_Open shall exist for each multipoint consumer, 1 to Max_Consumer_Number (indexed from 0 to Max_Consumer_Number – 1).

The Consumer_Open values are Open or Closed.

The Consumer_Open indication shall act as an enable to the Run Time Validator on a connection by connection basis. After successful connection establishment, Consumer_Open flags shall transition from Closed to Open.

The Validator Connection Establishment engine shall provide an array of consumer connection status resources for multipoint producers that shall be allocated when a consumer makes a connection.

The consumer numbers allocated to a Run-time Validator shall be the number sent to the consumer in the connection establishment reply.

The consumer connection numbers can be treated as an allocation pool that can be re-used and re-allocated as needed.

The Validator Connection Establishment Engine shall ensure that the Consumer_Open resource for any allocated consumer number is set to Closed for a minimum time of (Timeout_Multiplier.PI + 2) × Ping Interval prior to re-allocating that Consumer number to another connection. This is to ensure that any previously established connections have timed out prior to allocating the number to a new connection.

In other words, if the Validator Connection Establishment Engine sees S_Connection_Fault set, it shall set Consumer_Open to Closed for a minimum of (Timeout_Multiplier.PI + 2) × Ping Interval or optionally until that same consumer tries to re-establish the same connection.

7.7.5.3 Application_Run_Idle

If the producing application is actively controlling data the Run_Idle indication shall indicate Run. If the producing application is not actively controlling the data and the data need to be put in the safety state, the Run_Idle indication shall indicate Idle.

7.7.5.4 Consumer_Active_Idle [per consumer]

Consumer_Active_Idle is a run time flag to indicating if valid Time Coordination Message information has been received for this consumer.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

If a safety data producer is producing data and valid Time Coordination information has been received without errors the Consumer_Active_Idle flag shall be equal to Active, otherwise it will be Idle.

For multipoint producers, a Consumer_Active_Idle flag shall exist for each multipoint consumer, numbered 1 to Max_Consumer_Number.

The Consumer_Active_Idle values are idle and active.

At connection establishment, all Consumer_Active_Idle flags shall be initialized to Idle.

7.7.5.5 S_Connection_Fault [per consumer]

S_Connection_Fault is a run time flag that indicates whether the safety connection to the consumer is OK or Faulted.

An S_Connection_Fault indication of Fault, shall indicate that the producer has detected a problem with the safety connection to this consumer or the consumer has indicated an error back to the producer.

If the safety data producer has received invalid Time Coordination information, or a Time Coordination information timeout, the S_Connection_Fault flag shall be equal to Fault, otherwise it will be OK.

For multipoint producers, an S_Connection_Fault flag shall exists for each multipoint consumer, numbered 1 to Max_Consumer_Number.

The S_Connection_Fault values are OK and Faulted.

At connection establishment, all S_Connection_Fault variables shall be initialized to OK.

7.7.5.6 Producer input static variables

Producer input static variables are the configuration time parameters that define the operation of the safety protocol producer.

7.7.5.7 EPI

EPI is the expected packet interval. Safety data shall be produced at a rate not exceeding the EPI. The EPI is expressed as an integer value in microseconds. The legal range of values is from 100 µs to 1 000 000 µs.

For all safety connections, the producer and all consumers shall all have the same EPI.

7.7.5.8 Timeout_Multiplier [per consumer]

The Timeout_Multiplier indicates the number of data production retries to use in the connection failure detection equations.

The Base Format limited the Timeout_Multiplier parameter values from 1 to 4. For the Base Format, the Timeout_Multiplier value was used for two purposes. They are:

a) To calculate the Network Time Expectation;

b) To determine the number of ping intervals to wait without Time_Coordination or Time Correction before declaring a connection fault.

The Extended Format allows a larger Timeout_Multiplier parameter value to be used to calculate the Network Time Expectation, but the value used to determine the number of ping intervals to

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

wait without Time_Coordination or Time Correction before declaring a connection fault is still limited to a maximum value of 4. The ExtendedFormat allows the Timeout_Multiplier parameter value to be any value from 1 to 255.

Throughout this document "Timeout_Multiplier" will refer to the Timeout_Multiplier parameter value. "Timeout_Multiplier.PI" will refer to the value that is derived from "Timeout_Multiplier" to determine the number of Ping Intervals to wait without Time_Coordination or Time Correction before declaring a connection fault.

For the Base Format, Timeout_Multiplier.PI shall be equal to the Timeout_Multiplier. For the ExtendedFormat, Timeout_Multiplier.PI shall be equal to the smaller of Timeout_Multiplier or 4, whichever is lower.

The Timeout_Multiplier shall be used to determine how many ping intervals (Timeout_Multiplier.PI + 2) a producer will wait before faulting a consumer who has failed to send a Time Coordination response to a Ping request .

The legal range of the Base Format Timeout_Multiplier values shall be 1, 2, 3, or 4. The legal range of the Extended Format Timeout_Multiplier value shall be 1 to 255 so long as the Network Time Expectation value does not exceed 5,8 s.

For any producer, each consumer may have a different Timeout_Multiplier.

7.7.5.9 Connection_Type

The Connection_Type specifies whether the connection is point-to-point or multipoint.

For any producer, each producer connection and the corresponding consumer connection(s) shall be of the same Connection Type.

7.7.5.10 Ping_Interval_EPI_Multiplier

Ping_Interval_EPI_Multiplier is the number that defines the Ping_Count_Interval for a particular connection.

The Ping_Count_Interval shall be equal to the EPI times the Ping_Interval_EPI_Multiplier.

The Ping_Count_Interval shall define the rate at which Time Coordination Messages will be requested and sent.

The Ping_Count_Interval shall define the rate at which Time Correction sections are sent to each consumer.

A legal Ping_Interval_EPI_Multiplier shall have a minimum value determined from the equation Max_Consumer Number × Timeout_Multiplier.PI + 15, and a maximum less than 1 000. The default values shall be 100 for multipoint and 19 for point-to-point.

The Ping_Interval_EPI_Multiplier should be set large enough to allow the ping request to be recognized by the server(s), the server(s) to send the Time Coordination section(s), and all Time_Coordination section(s) to arrive and be processed by the client. All these steps shall occur before the Ping_Interval time expires.

All Time_Correction sections shall be sent out by the client within the Ping_Interval.

The Ping_Interval_EPI_Multiplier shall be set small enough to ensure that the Ping_Count_Interval is less than or equal to 100 s.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

A ping count interval of greater than 100 s may contribute greater than 0,5 s to the clock drift, depending upon the Timeout_Multiplier.PI for that connection. To prevent clock size wrap around, 0,5 s has been set at the maximum value that can be allocated to clock drift.

The following variables will be used to calculate the Ping_Interval_EPI_Multiplier.

- C_TO_S_Delay_Multiplier equals the time as a multiplier of the EPI time that is equal to the time for message initiation, transport delay, and reception processing delay of the Data Message or the Time_Correction Message from the client to the server.
- S_TO_C_Delay_Multiplier equals the time as a multiplier of the EPI time that is equal to the time for message initiation, transport delay, and reception processing delay of the Time_Coordination Message from the server to the client.
- Ping_Rcved_TO_Time_Coord_Sent_Multiplier equals the time as a multiplier of the EPI time that is allowed from the time that the EPI reception that needs to trigger the sending of the Time Coordination message until the message needs to be sent.
- Time_Coord_Rcved_TO_Time_Coord_Processed_Multiplier equals the time as a multiplier of the EPI time that is allowed from the time that the Time Coordination message is received until the Time Coordination message is processed.

For a single network it is reasonable to expect that C_TO_S_Delay_Multiplier and S_TO_C_Delay_Multiplier are less than 2 times the EPI.

For a bridged network depending upon the number of hops, it is reasonable to expect that C_TO_S_Delay_Multiplier and S_TO_C_Delay_Multiplier are less than 4 times the EPI. 4 will be used as the minimum value for C_TO_S_Delay_Multiplier and S_TO_C_Delay_Multiplier when calculating the minimum value for Ping_Interval_EPI_Multiplier.

The C_TO_S_Delay_Multiplier and S_TO_C_Delay_Multiplier EPI multipliers should not have to consider messages being lost on the network. The Timeout_Multiplier will account for lost messages.

Ping_Rcved_TO_Time_Coord_Sent_Multiplier should be less than 3 times the EPI.

Time_Coord_Rcved_TO_Time_Coord_Processed_Multiplier should be less than 3 times the EPI.

The equation to determine the minimum Ping_Interval_EPI_Multiplier is:

$$\begin{aligned}&[\{\text{the maximum Timeout_Multiplier.PI (C\#) for all consumers}\} \times \text{Max_Consumer_Num}]\\&\quad + \text{C_TO_S_Delay_Multiplier}\\&\quad + \text{S_TO_C_Delay_Multiplier}\\&\quad + \text{Ping_Rcved_TO_Time_Coord_Sent_Multiplier}\\&\quad + \text{Time_Coord_Rcved_TO_Time_Coord_Processed_Multiplier} + 1\end{aligned} \tag{1}$$

where

C# = Consumer_Number

Using 4 as the constant used for C_TO_S_Delay_Multiplier and S_TO_C_Delay_Multiplier and 3 as the constant used for Ping_Rcved_TO_Time_Coord_Sent_Multiplier and Time_Coord_Rcved_TO_Time_Coord_Processed_Multiplier:

The Ping_Interval_EPI_Multiplier shall be greater than or equal to:

$$[\{\text{the Max Timeout_Multiplier.PI (C\#) for all consumers}\} \times \text{Max_Consumer_Num}] + 15 \tag{2}$$

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

This relationship will be relied upon by the producer when sending Time Correction messages. For C_TO_S_Delay_Multiplier and S_TO_C_Delay_Multiplier values greater than 4, and Ping_Rcved_TO_Time_Coord_Sent_Multiplier and Time_Coord_Rcved_TO_Time_Coord_Processed_Multiplier greater than 3, the Ping_Interval_EPI_Multiplier should be increased accordingly.

The Ping_Interval_EPI_Multiplier shall be less than: 100 s / EPI.

The Ping_Interval_EPI_Multiplier range of 75 to 100 will meet the restrictions defined above for all legal values defined below:

- EPI, 0,000 1 s to 1 s;
- Timeout_Multiplier.PI, 1 to 4;
- Max_Consumer_Num, 1 to 15;
- C_TO_S_Delay_Multiplier and S_TO_C_Delay_Multiplier, 1 to 4;
- Ping_Rcved_TO_Time_Coord_Sent_Multiplier, 1 to 3;
- Time_Coord_Rcved_TO_Time_Coord_Processed_Multiplier, 1 to 3.

For any producer, the producer and all consumers shall have the same Ping_Interval_EPI_Multiplier.

7.7.5.11 Max_Consumer_Number

Max_Consumer_Number is the maximum number of consumers that may be configured.

If the connection type is point-to-point, the Max_Consumer_Number shall be equal to 1.

For multipoint connections, the legal range of Max_Consumer_Number values shall be from 1 to 15.

For any producer, the producer and all consumers shall have the same Max_Consumer_Number.

7.7.5.12 Time_Coord_Msg_Min_Multiplier [per consumer]

Time_Coord_Msg_Min_Multiplier is the minimum number of 128 µs increments it could take for a Time Coordination Message to traverse from the consumer to the producer. A value other than 0 for this variable will allow the time stamp to be more accurate. The default for the Time_Coord_Msg_Min_Multiplier shall be 0, and the legal range of values shall be from 0 to 7 813, which equates to 0 s to 1 s.

This is the minimum number of 128 µs increments it could take:

From:

> The consumer capturing Consumer_Time_Value from the Consumer_Clk_Count for the Time Coordination Message,

To:

> The producer capturing the Producer_Rcved_Time_Value upon reception of the Time Coordination Message

For any producer, each consumer may have a different Time_Coord_Msg_Min_Multiplier.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

7.7.5.13 Producer connection derived static variables

These static variables are derived from the input static variables. These static variables are derived at configuration time and are used during producer processing.

7.7.5.14 Time_Drift_Per_Ping_Interval [per consumer]

The Time_Drift_Per_Ping_Interval is a value in 128 µs increments that represents the worst-case time drift due to crystal inaccuracy during one Ping Interval.

The clocks in safety devices shall be accurate to within 0,02 % (0,000 2). Considering positive and negative drift the clocks will remain within 0,000 2 × 2 of each other or 0,004 (0,04 %).

The legal range of values is from 1 to 313, since the Ping Interval is limited to 100 s (100 000 000 µs).

The Time_Drift_Per_Ping_Interval calculation is done with time references in microseconds (EPI is the EPI in microsecond units). The Time_Drift_Per_Ping_Interval calculation is done in 32 bit integer math with the result being a 16 bit integer. The divide by 320 000 factor in the Time_Drift_Per_Ping_Interval calculation is equivalent to multiplying by the worst case clock drift of 0,000 4 and dividing by 128 µs.

Time_Drift_Per_Ping_Interval (C#) =
Roundup [EPI × Ping_Interval_EPI_Multiplier / 320 000]
OR 1 whichever is greater (3)

where

C# = Consumer_Number

EXAMPLE If EPI = 8 000 µs and Ping_Interval_EPI_Multiplier = 100, then Time_Drift_Per_Ping_Interval(C#) = 3 (384 µs)

7.7.5.15 Connection_Correction_Constant [per consumer]

Connection_Correction_Constant is a value in 128 µs increments that is subtracted from the time stamp to represent the worst case error due to:

- Time drift;
- The asynchronous nature of the producer and consumer clocks;
- The minimum time for the Time Coordination Message to traverse from the consumer to the producer.

Connection_Correction_Constant [C#] =
Time_Drift_Constant + 1 – Time_Coord_Msg_Min_Multiplier [C#] (4)

where

C# = Consumer_Number

The Time_Drift_Constant (which is part of the Connection_Correction_Constant calculation) is a value in 128 µs increments that is subtracted from the time stamp to represent the worst-case time drift due to crystal inaccuracy. The producer and consumer clocks shall be accurate to within 0,02 % (0,000 2). Considering positive and negative drift the clocks will remain within 0,000 2 × 2 of each other or 0,000 4 (0,04 %).

The legal range of values for the Time_Drift_Constant is from 1 to 1 563.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

The Time_Drift_Constant calculation is done with time references in microseconds (EPI is the EPI in microsecond units).

The Time_Drift_Constant calculation shall be done using at least 32 bit integer math with the result being a 16 bit integer.

The 1/320 000 factor in the Time_Drift_Constant calculation is equivalent to multiplying by the worst case clock drift of 0,000 4 and dividing by 128.

Time_Drift_Constant (in 128 µs counts) =
Roundup [(Timeout_Multiplier.PI
(C#) + 1) × EPI_in_µs × Ping_Interval_EPI_Multiplier / 320 000]
OR 1 whichever is greater. (5)

EXAMPLE Timeout_Multiplier.PI = 2, EPI(in microseconds) = 8 000, Ping_Interval_EPI_Multiplier = 100, Time_Drift_Constant = 8, Time_Coord_Msg_Min_Multiplier = 2, then Connection_Correction_Constant = 7

7.7.5.16 Time_Coord_Response_EPI_Limit [per consumer]

The Time_Coord_Response_EPI_Limit is used to ensure that a Time Coordination message that returns to the producer requesting it, arrives within a time sufficient to prevent the possibility of a 16 bit time stamp math rollover. There are other checks to insure that the Time_Coordination message returns within the Ping Interval and that not too many Time Coordination messages are dropped.

Time_Coord_Response_EPI_Limit (a value in EPI increments) is used to determine if the time between the incrementing of the Ping Count and the Time Coordination response is less than a time value that is equal to:

{5 + [Time_Coord_Msg_Min_Multiplier × 0,000 128] + [EPI × (Consumer_Num – 1)]}
in seconds. (6)

To keep the reaction time less than 5,8 s, the transport time of the safety message plus the transport time of the Time Coordination message minus the minimum Time Coordination message [Time_Coord_Msg_Min_Multiplier/0,000 128] shall be less than 5,0 s if the worst case drift of 0,5 s is considered. This procedure keeps the Connection_Correction_Constant within range to prevent rollover at the age check.

The legal range of values for Time_Coord_Response_EPI_Limit is between 5 to 1 000.

If the Consumer_Active_Idle[Consumer_Num-1] == Active, Producers shall check that Time Coordination Messages are received within the Time_Coord_Response_EPI_Limit and fault the connection if they are not.

The Time_Coord_Response_EPI_Limit calculation is done with time references in microseconds (EPI is the EPI in microsecond units).

The Time_Coord_Response_EPI_Limit calculation shall be done in 32 bit integer math with the result being a 16 bit integer.

Time_Coord_Response_EPI_Limit [C#] =
Roundup ({5 000 000 + [Time_Coord_Msg_Min_Multiplier[C#] × 128]
+ [EPI × (C# – 1)]} / EPI)
OR 1 000 whichever is lower. (7)

where

C# = Consumer_Number

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

EXAMPLE If Time_Coord_Msg_Min_Multiplier = 2 (256 µs), EPI = 8 000 µs, and Consumer_Number = 1, then Time_Coord_Response_EPI_Limit = 626.

7.7.6 Producer dynamic variables

7.7.6.1 Producer_Clk_Count

Each product that produces or consumes safety data shall derive a periodic timer that increments a counter (Producer_Clk_Count or Consumer_Clk_Count) every 128 µs.

Producer_Clk_Count shall have tolerances and stability within ± 0,02 %.

Producer_Clk_Count (and Consumer_Clk_Count) shall be 16 bits in length.

7.7.6.2 Producer_Safe_Data_TS

Producer_Safe_Data_TS is a variable that shall be set equal to Producer_Clk_Count at the point in time that the Safety_Data for a particular EPI data production is sampled and captured from the producing application.

This location that is sampled is the point where the producing applications time monitoring responsibilities end and the safety protocols time monitoring responsibilities begin. This value is used as the time stamp for the data that is relative to the producer's clock. The legal range of values is from 0 to 65 535.

7.7.6.3 Data_Time_Stamp

Data_Time_Stamp is the time that the safety data was sampled relative to the consumer's clock.

The Data_Time_Stamp value is derived by the producer for a point-to-point production.

The Data_Time_Stamp value is derived by the consumer in multipoint connections.

The legal range of values is from 0 to 65 535.

For point-to-point:

$$\text{Data_Time_Stamp} = \text{Producer_Safe_Data_TS} + \text{Consumer_Time_Correction_Value} \quad (8)$$

For multipoint:

$$\text{Data_Time_Stamp} = \text{Producer_Safe_Data_TS} \quad (9)$$

7.7.6.4 Ping_Interval_EPI_Count

Ping_Interval_EPI_Count is a count of the number of EPI time periods between the incrementing of the Ping_Count.

Ping_Interval_EPI_Count is used to control Ping Intervals and to control the sending of Time Correction messages for multipoint producers.

The Ping_Interval_EPI_Count is incremented at every data production. When Ping_Interval_EPI_Count reaches the Ping_Interval_EPI_Multiplier , it is reset to 0, and the Ping count is incremented.

For multipoint producers, Time Correction messages shall be sent to the n consumers (where n = 1 to Max_Consumer_Number), on the 9th to n+9 productions of the Ping Interval.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

The Time Correction message of consumer 1 shall be sent first, followed by 2, 3,…,n.

The intent of this logic is to distribute the Time Correction messages at a point within the Ping Interval, when the Time Coordination messages should have already arrived and been processed for this Ping Interval.

The legal range of values is from 0 to Ping_Interval_EPI_Multiplier.

At connection establishment, the Ping_Interval_EPI_Count variable shall be set to 0000_{hex}.

7.7.6.5 RR_Con_Num_Index_Pntr

RR_Con_Num_Index_Pntr is a variable used by the multipoint producer to control the checking of the timeout on the reception of Time Coordination messages, and to control the sending of Time Correction messages.

A value greater than or equal to Max_Consumer_Number, indicates that the Time Coordination timeouts are not being checked on this EPI, and no Time Corrections are being sent based on this EPI.

A value of 0 to (Max_Consumer_Number -1) indicates which Time Coordination timeouts will be checked (Consumer_Number = RR_Con_Num_Index_Pntr + 1) on this EPI and which Time Correction message (Consumer_Number = RR_Con_Num_Index_Pntr + 1) may be sent based on this EPI production.

7.7.6.6 Time_Drift_Since_Last_Time_Coord [per consumer]

Time_Drift_Since_Last_Time_Coord is a variable that contains the maximum time drift that could have occurred between the producer and the consumer since the last time that a Time Coordination message was received. This value is equal to the Ping_Int_Since_Last_Time_Coord_Msg_Count times Time_Drift_Per_Ping_Interval. The Ping_Int_Since_Last_Time_Coord_Msg_Count is the number of Ping Intervals since the last Time Coordination message.

The Time_Drift_Since_Last_Time_Coord shall be used to indirectly determine if the delay of the Time Coordination message received is significantly greater than the delay for the Time Coordination message previously being used.

The Delay of the Time Coordination message has an impact on the Consumer_Time_Correction_Value that will be used. Greater delays in the Time Coordination message cause the Time_Stamp to be compensated in a negative direction, causing the age of the data to be greater.

If the difference between the delays of two consecutive Time_Coordination messages is greater than the EPI time, the later Consumer_Time_Correction_Value may cause the Time_Stamp of the next EPI production to actually be less then the Time_Stamp of the previous EPI production. This would result in a sequence error at the consumer of the Time_Stamp.

Since the maximum time drift is controlled, either the Last Time_Correction_Value minus the Time_Drift_Since_Last_Time_Coord value, or the New Time_Correction_Value value, shall be sent to the consumer, whichever is better.

This prevents long delays in the delivery of a Time Correction messages from causing sequence errors in the Time Stamp checks.

For multipoint producers, a Time_Drift_Since_Last_Time_Coord shall exist for each multipoint consumer, 1 to Max_Consumer_Number.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

The legal range of values is from 0 to 3 910.

7.7.6.7 Worst_Case_Consumer_Time_Correction_Value

This a temporary value used to determine the Consumer_Time_Correction_Value.

7.7.7 Producer per consumer dynamic variables

7.7.7.1 General

The following dynamic variables are producer variables that exist for each consumer. For point-to-point connections there will be only one variable for each consumer. For multipoint there will be Max_Consumer_Number of variables, each representing an individual consumer.

7.7.7.2 Consumer_Time_Value[per consumer]

Consumer_Time_Value is the time value sent to the producer of a time stamp from the consumer or in the Time Coordination Message. A Consumer_Time_Value is received for each multipoint consumer, 1 to Max_Consumer_Number.

The legal range of values is from 0 to 65 535.

At connection establishment, all Consumer_Time_Value variables shall be set to 0000_{hex}.

When a Time Coordination Message is received, the producer shall check that the Time_Coordination_Section.Consumer_Time_Value is not the same as the last received Consumer_Time_Value. If it is, the Time Coordination message shall not be processed.

This check will prevent a producer from processing network generated duplicate Time Coordination messages.

7.7.7.3 Producer_Rcved_Time_Value[per consumer]

Producer_Rcved_Time_Value shall be set equal to Producer_Clk_Count at the point in time that the Time Coordination Message information is received from the time stamp consumer.

A Producer_Rcved_Time_Value shall exist for each multipoint consumer, 1 to Max_Consumer_Number.

The legal range of values is from 0 to 65 535.

At connection establishment, all Producer_Rcved_Time_Value variables shall be set to 0000_{hex}.

7.7.7.4 Consumer_Time_Correction_Value[per consumer]

The Consumer_Time_Correction_Value exists only for multipoint safety connections.

The Consumer_Time_Correction_Value is added to the producer's data time stamp to allow the result to indicate the worst-case earliest time that the data could have been sampled relative to the consumer's clock value.

A Consumer_Time_Correction_Value exists for each multipoint consumer, 1 to Max_Consumer_Number.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Consumer_Time_Correction_Value [Consumer_Number] =

Consumer_Time_Value [Consumer_Number] (10)
- Producer_Rcved_Time_Value [Consumer_Number]
- Connection_Correction_Constant [Consumer_Number]

The legal range of values is from 0 to 65 535.

At connection establishment, all Consumer_Time_Correction_Value variables shall be set to 0000_{hex}.

7.7.7.5 Ping_Int_Since_Last_Time_Coord_Msg_Count [per consumer]

Ping_Int_Since_Last_Time_Coord_Msg_Count is a run time count of the number of Ping Intervals between Time Coordination Messages for a particular consumer.

For point-to-point connections, the Ping_Int_Since_Last_Time_Coord_Msg_Count shall be incremented at the 8th EPI production of the Ping Interval.

For multipoint connections, Ping_Int_Since_Last_Time_Coord_Msg_Count shall be incremented every (8 + n)th EPI production of the Ping Interval, where n equals the consumer number – 1.

The Ping_Int_Since_Last_Time_Coord_Msg_Count for any particular consumer shall be reset upon the reception of a valid Time Coordination Message from that consumer.

If the Ping_Int_Since_Last_Time_Coord_Msg_Count ever exceeds the Timeout_Multiplier.PI plus 2 for a connection, that consumer shall be set to the faulted state.

If the producer is multipoint, Ping_Int_Since_Last_Time_Coord_Msg_Count exists for each multipoint consumer, 1 to Max_Consumer_Number.

The legal range of values is from 0 to 5.

At connection establishment, all Ping_Int_Since_Last_Time_Coord_Msg_Count variables shall be set to 0000_{hex}.

7.7.7.6 Producer_Fault_Counter

For the Extended Format, this is a temporary value used to track the number of data integrity errors the producer detects on the reception of Time Coordination messages. This value is incremented every time a Time Coordination message is detected with a data integrity error. This value will be reset to 0 every hour. If this value reaches the Max_Fault_Number for that consumer (SafetyOpen Parameter), the connection will be closed.

7.7.8 Consumer data variables

7.7.8.1 General

This Subclause 7.7.8 describes the data variables that will be used by a safety consumer to receive safety data. The internal variables are defined in an attempt to define the behavior of the safety data consumer upon the reception of safety data.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

7.7.8.2 Consuming connection status

The status of the safety data and the safety connections can be derived from the S_Con_Flt_C_Out, the S_Run_Idle_Out flags, and the Init_Complete_Out. Table 101 summarizes the logic that the consuming application can use to drive the safety data and status.

Table 101 – Consuming safety connection status

S_Con_Flt_C_Out	S_Run_Idle_Out	Init_Complete_Out	Connection Status	Description
Fault	Don't care	Don't care	Faulted	The safety connection is faulted. Restart will be required. Put the data in safety state
OK	Idle	0	Idle	The safety connection has not been activated. Put the data in safety state
OK	Idle	1	Idle	The safety connection has been activated and the producing application is in Idle Mode. Put the data in safety state
OK	Active	0	N/A	Illegal condition – can not occur
OK	Active	1	Run	The safety connection is active and the producing application is in Run Mode. Use the data

The Connection Status of consuming safety connections shall be indicated as defined in Table 101.

7.7.8.3 S_Con_Flt_C_Out

S_Con_Flt_C_Out indicates to the consuming application if it needs to put the safety data in a safety state because the safety validators have detected a safety connection fault. S_Con_Flt_C_Out_Temp is used as a temporary location for this variable.

The S_Con_Flt_C_Out values are OK and Fault.

At connection establishment, all S_Con_Flt_C_Out flags shall be set to OK.

7.7.8.4 S_Run_Idle_Out

S_Run_Idle_Out shall be used by a consuming application to determine if it needs to put the safety data in a safety state.

The S_Run_Idle_Out shall indicate Idle when either the producing application is Idle or the Safety Validators are not active. S_Run_Idle_Out_Temp is used as a temporary location for this variable.

The S_Run_Idle_Out values are IDLE or RUN.

At connection establishment, all S_Run_Idle_Out flags shall be set to Idle.

7.7.8.5 Init_Complete_Out

Init_Complete_Out indicates if the time stamp initialization is complete or not.

S_Run_Idle_Out shall be in Idle until Init_Complete_Out is set to a 1.

After the connection is first established, the consuming application shall close Base Format connections if initialization is not completed within 10 s. The consuming application shall close Extended connections if initialization is not completed within 8,3 s.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

The S_Run_Idle_Out will indicate Idle, regardless of this timeout. If the timeout is incorporated, the error shall be latched until the safety connection is closed and a re-open attempt is made.

For Point-to-point, the flag Init_Complete_Out shall indicates that the first time coordination message has been received by the producer, and the producer is producing data with the time stamp relative to the consumers clock.

For Multipoint, the flag Init_Complete_Out shall indicates that the first time coordination message has been received by the producer for this consumer, and the consumer has received the 1st time correction message based on the time coordination information.

For Point-to-point, the Data_Time_Stamp value shall be set to 0 by the producer until the first time coordination section is received.

If the consumer receives the Data_Time_Stamp as a value other than 0, the time stamp checking shall be enabled.

For Multipoint, the Data_Time_Stamp value shall always be set equal to the producers clock.

The Multipoint consumer shall enable time stamp checking upon the reception of the first time correction section.

For all consumed safety connections, time stamp checking shall be enabled if the mode of the data indicates Run.

Init_Complete_Out_Temp is used as a temporary location for this variable.

7.7.9 Consumer input static variables

7.7.9.1 Connection_Type

Connection_Type specifies whether the connection is point-to-point or multipoint. For any producer, the producer and all consumers shall have the same Connection_Type.

7.7.9.2 Consumer_Num

Consumer _Num is the number a Multipoint Consumer is assigned (1 to 15).

7.7.9.3 Network_Time_Expectation_Multiplier

Network_Time_Expectation_Multiplier is the maximum number of 128 µs increments that a consumer needs to allow the age of the safety data to reach.

If consumed safety data becomes older then Network_Time_Expectation_Multiplier, the safety data shall be put in the safety state.

The legal range of values is from 0 to 45 313, which equates to 0 s to 5,8 s. The 5,8 s limit, the requirement to check the Network_Time_Expectation at least once every 2 s, and the maximum Time_Correction value change (or maximum clock drift) for a Ping interval is 0,5 s, will ensure that the clock base value of 8,388 s ($FFFF_{hex}$ × 0,000 128) does not wrap around between checks.

The actual network reaction time may be this value in time plus 1 EPI if the producing application is asynchronous to the data production, since in this case the data may be one EPI old at the time that the time stamp was placed on the produced data.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

7.7.9.4 Timeout_Multiplier

Timeout_Multiplier is the number of data production retries to use for in network fault detection equations. This is the same value used by the producer.

7.7.9.5 Ping_Interval_EPI_Multiplier

Ping_Interval_EPI_Multiplier is the number that defines the Ping_Count_Interval for a particular connection. The Ping_Count_Interval is equal to the EPI times the Ping_Interval_EPI_Multiplier.

This is the same value used by the producer.

7.7.9.6 Consumer connection derived static variables

These static variables are derived from the input static variables. These static variables are derived at configuration time and are used during producer processing.

7.7.10 Consumer dynamic variables

7.7.10.1 Consumer_Clk_Count

Each product that consumes safety data will derive a periodic timer that increments a counter (Consumer_Clk_Count) every 128 µs.

Consumer_Clk_Count will have tolerances and stability within ± 0,02 % because safety devices are required to have clocks with this tolerance.

Consumer_Clk_Count shall be 16 bits in length.

If the difference between the Consumer_Clk_Count at the time that the data is given to the consuming application for use and the Data_Time_Stamp sent with the data exceeds the Network_Time_Expectation_Multiplier, the S_Con_Flt_C_Out flag shall be set to "Faulted" to indicate that the Reaction Time for the network has not been met.

7.7.10.2 Last_Ping_Count

A consumer of safety data shall be able to detect when the Ping_Count has changed. This 2 bit variable is used to hold the Ping_Count for comparison on the next reception.

Since the initial production of safety data needs to have a Ping_Count of 00, the Last_Ping_Count shall be initialized to 11.

7.7.10.3 Time_Coordination_Count_Down

The Time_Coordination_Count_Down shall be set equal to the Consumer_Number upon the reception of a multipoint ping request.

The consumer shall decrement the Time_Coordination_Count_Down value on subsequent reception of consumed data until the value is equal to 0.

If the value is equal to 1 during any reception of consumed data, the ping response for that consumer shall be sent.

The intent of this logic is to distribute the multipoint ping responses.

When a connection is first established, the Time_Coordination_Count_Down shall be initialized to 0.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

7.7.10.4 Corrected_Data_Time_Stamp

This value is the consumer copy of the received Data_Time_Stamp.

For multipoint, the Corrected_Data_Time_Stamp shall be a sum of the received time stamp and the Last_Rcved_Time_Correction_Value.

7.7.10.5 Last_Data_Time_Stamp

This value is the saved copy of the received Data_Time_Stamp.

The Last_Data_Time_Stamp shall be used to detect out of sequence messages.

When a connection is first established, the Last_Data_Time_Stamp shall be initialized to 0.

7.7.10.6 Last_Rcved_Multi_Cast_Active_Idle

This value is the saved copy of the received Multi_Cast_Active_Idle.

The Last_Rcved_Multi_Cast_Active_Idle shall be used to detect a change from active to idle, which would be considered a fault.

When a connection is first established, the Last_Rcved_Multi_Cast_Active_Idle shall be initialized to 0.

7.7.10.7 Last_Rcved_Time_Correction_Value

This value is the saved copy of the received Time_Correction_Value.

The Last_Rcved_Time_Correction_Value shall be used to correct the Time Stamp for each multipoint consumer.

When a connection is first established, the Last_Rcved_Time_Correction_Value shall be initialized to 0.

7.7.10.8 Time_Correction_Ping_Interval_Count

This value indicates the number of Ping Intervals that have occurred since the last reception of a Time Correction message.

If the Time_Correction_Ping_Interval_Count is greater than the Timeout_Multiplier.PI + 1, the connection shall be faulted.

7.7.10.9 Time_Correction_Received_Flag

This value indicates that a Time Correction message has been received for this multipoint consumer. This value indicates that a time correction message has been received and the time stamp can be corrected and checked.

When the Time_Correction_Received_Flag is set, the consumer shall begin the process of correcting and checking the time stamp.

7.7.10.10 Data_Age

This value indicates the worst case age of the data in 128 µs increment.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Data Age is determined at the point a Consuming Application samples the data. In Application-Triggered consumers, this sampling is asynchronous to the data reception. In Link-Triggered consumers, this sampling is done when the data is received.

Data age is defined as the difference between the Consumer_Clk_Count at the sample point and the Data Time Stamp when the data was last captured.

7.7.10.11 Max_Data_Age

This value indicates maximum value of Data_Age since the last time that it was reset.

7.7.10.12 Consumer_Fault_Counter

For the Extended Format, this a temporary value used to track the number of data integrity errors the consumer detects on the reception of Data and Time Correction messages. This value is incremented every time a Data and Time Correction message is detected with a data integrity error. This value will be reset to 0 every hour. If this value reaches the Max_Fault_Number (SafetyOpen Parameter), the connection will be closed.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

8 Safety communication layer management

8.1 Overview

Subclauses 8.1 to 8.7 do not attempt to provide a tutorial on every aspect of CPF 2, but rather a high-level overview of how CPF 2 connections are established on each network and across network types, highlighting the features used and extensions required to support Safety Connections.

All FSCP 2/1 connections shall be established using a Forward Open with a safety network segment (CP 2/2) or a SafetyOpen (CP 2/3). There are measures for detection of both system and user errors defined. Table 102 defines the errors and the measures to detect these errors.

Table 102 – Connection establishment errors and measures to detect errors

Connection establishment errors	Measures to detect connection establishment errors				
	User testing	OUNID verification	TUNID verification	CPCRC CRC	Configuration ID (SCID)
User misroutes connection request	X	X1	X		
System misroutes connection request			X		
Corrupted SafetyOpen				X	X
Corrupted or changed application configuration					X
Reconfiguration from wrong originator		X[a]			

[a] Only applies if ownership has been established.

8.2 Definition of the measures used during connection establishment

System-Wide Unique "Safety Network Number" (SNN) – Uniquely identifies a network across all networks in the safety system. The user safety manual shall contain an advisory that states

"The user should assign SNN numbers for each safety network or safety sub-net that are unique system-wide", or words to that effect.

The Safety Network Number makes up part of the UNID. This value is a 6 octet value that uses the CPF 2 DATE_AND_TIME format.

The DATE values of 1 to 11 687 decimal (1972-01-01 to 2002-12-31) are past time values that are reserved for Manual Setting values of the SNN.

The SNN may be one of two types:

- Manual Setting, or
- Software Tool Generated.

The Type of SNN can be determined from the DATE section, see Table 103 for details.

Table 103 – SNN Date/Time allocations

From DATE (Decimal)	To DATE (Decimal)	From DATE (Day)	To DATE (Day)	SNN Type
0	0	1972-01-01	1972-01-01	Null SNN (illegal value)
1	1	1972-01-02	1972-01-02	Manual setting – backplane
2	2	1972-01-03	1972-01-03	Manual setting – CP 2/1
3	3	1972-01-04	1972-01-04	Reserved for future use
4	4	1972-01-05	1972-01-05	Manual setting – CP 2/2
5	5	1972-01-06	1972-01-06	Manual setting – CP 2/3
6	6	1972-01-07	1972-01-07	Manual setting – CP 16/3
7	1 460	1972-01-07	1975-12-31	Reserved for future use
1 461	11 687	1976-01-01	2003-12-31	Vendor specific range
11 688	65 534	2004-01-01	2151-06-05	Software tool generated
65 535	65 535	2151-06-06	2151-06-06	Target indication that no SNN has been set

If a software tool reads a reserved SNN Type, it shall display it as a Hex value.

The legal Range of TIME values for the Type of SNN are listed in Table 104.

Table 104 – SNN legal range of time values

SNN type	From time hex	To time hex	From time d/h/min/s	To time d/h/min/s
Null SNN	00000000	00000000	00d00h00min00,000s	00d00h00min00,000s
Manual setting (DATE = 1 to 5)	00000001	0000270F (9 999 decimal)	00d00h00min00,001s	00d00h00min09,999s
Reserved for future use	-	-	-	-
Software tool generated	00000000	05265BFF	00d00h00min00,000s	00d23h59min59,999s
Target indication that no SNN has been set	FFFFFFFF	FFFFFFFF	-24d20h31min23,648s	-24d20h31min23,648s

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

System-Wide "Unique Node Identifier" (UNID) – Uniquely identifies a node across all networks in the safety system. This value is made up of the Safety Network Number (SNN) and the Node Address of the device. This value is a structure consisting of the 6 octet SNN and a 4 octet Node Address. The 4 octet node address is sized to accommodate all forms of CPF 2 network addresses.

```
struct UNID
{
DATE_AND_TIME    SNN;
UDINT                  NodeID;
};
```

NodeID smaller than 4 octets (i.e., CP 2/3) shall be aligned to the least significant octet in little endian order. The unused octets shall be zero filled.

Safety Function – The UNID is used to uniquely identify originators and/or targets during the connection establishment process.

Other uses of UNID:

TUNID = Target's Unique Network Identifier

Safety Function – Identifies the target in the SafetyOpen.

OUNID = Originator's Unique Network Identifier

Safety Function – Identifies the originator in the SafetyOpen.

OCPUNID = Output Connection Owning UNID

Safety Function – Identifies the owner of the output connection in the target, this shall be equal to the OUNID in normal operation.

CFUNID = Configuration Owning UNID

Safety Function – Identifies the owner of the safety configuration in the target, this shall be equal to the OUNID in normal operation.

Producer Identifier (PID) – Identifies the producer of the runtime data and Time Correction data.

The Producer Identifier (PID) shall be used as an initial seed value in the CRCs in the runtime protocol.

The Consumer shall obtain the Producer Identifier from either the SafetyOpen or SafetyOpen response (depending upon originator) and use the value as an initial seed in runtime checking the safety CRCs.

The value of the PID is Vendor ID + Device Serial Number + CIP Connection Serial Number.

Safety Function – The PID is used to ensure the correct routing of the produced/safety connection data and Time Correction data.

Consumer Identifier (CID) – Identifies the producer of the Time Coordination message.

The Consumer Identifier (CID) shall be used as an initial seed value in the CRC in the Time Coordination message.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

The Producer shall obtain the Consumer Identifier from either the SafetyOpen or the SafetyOpen Response (depending upon originator) and use the value as an initial seed in runtime checking the safety CRCs.

The value of the CID is Vendor ID + Device Serial Number + CIP Connection Serial Number.

Safety Function – The CID is used to ensure the correct routing of the Time Coordination data.

Connection Parameters CRC (CPCRC) – This is a safety related CRC covering the CPF 2 connection establishment data in the SafetyOpen. This CRC will also cover the additional parameters required by the safety protocol. The CRC used for the CPCRC is CRC-S4 and is defined in 7.1.2.

Safety Function – The CPCRC is used to ensure the integrity of the connection data contained within the SafetyOpen.

Safety Configuration CRC (SCCRC) – This is a CRC that covers the device configuration data that is contained in a SafetyOpen. The parameters covered by the CPCRC are not covered by the SCCRC. The CRC used for the SCCRC is CRC-S4 and is defined in 7.1.2.

The Safety Configuration Data CRC (SCCRC) shall be calculated over the entire application data section that is sent to the device being configured by the tool.

The SCCRC itself shall be included in the calculation of the CPCRC.

Safety Function – The SCCRC is used to ensure configuration data integrity while being transferred and to ensure configuration data integrity in storage.

Safety Configuration Time Stamp (SCTS) – This is a safety related signature that identifies the revision of the device configuration contained in either a SafetyOpen or in a safety device.

The SCTS shall be a Time/Date stamp marking the Time and Date of the configuration creation or change.

The SCTS parameter in the SafetyOpen shall be included in the calculation of the CPCRC.

The configuration software shall follow the CPF 2 defined Date and Time format (see IEC 61131-3) for setting the signature.

Safety Function – The SCTS is used to ensure the identity of the safety-related application data.

Safety Configuration Identifier (SCID) – The SCID is a combination of the SCCRC and the SCTS. The SCTS and SCCRC together serve to uniquely identify a configuration to the user and originator.

The SCID = 0 in a Type 2b SafetyOpen shall have special meaning to indicate that the SCID shall not be checked by a target before accepting the connection.

This special SCID value allows originators who are not concerned about the configuration of a device to make connections without knowing the SCID value.

The safety manual shall contain user instructions that state "If you choose to configure safety connections with an SCID = 0, you are responsible for ensuring that originators and targets have the correct configurations", or similar equivalent wording.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Initial Time Stamp – When the Extended Format safety message format is being used, the Extended Format safety segment and Extended Format SafetyOpen Response is used during connection establishment. Depending on the type of connection (see 7.6.5), the Initial Time Stamp is either sent in SafetyOpen or in the SafetyOpen Response. The Initial Time Stamp value is used to set up an initial time stamp parameter that is used to detect Time Stamp rollovers.

Initial Rollover Value – When the Extended Format safety message format is being used, the Extended Format safety segment and Extended Format SafetyOpen Response is used during connection establishment. Depending on the type of connection (see 7.6.5), the Initial Time Stamp is either sent in SafetyOpen or in the SafetyOpen Response. The Initial Rollover Value is used to set up the initial Rollover count parameter at the consumer. This value is included in the CRC calculations for the data packets. If the producer and consumer don't use the same value, the consumer CRC checks will fail. This feature provides additional detection capability for inserted messages and out-of-sequence packets.

8.3 Originator-Target relationship validation

In the CPF 2 framework, nodes are either originators (nodes that request connections) or targets (nodes that receive connection requests). Controllers are typically the connection originators. I/O modules (as well as other controllers or monitors) are typically the targets. Targets may support more than one application connection point.

Consider the system depicted in Figure 60. For the purposes of illustration, assume that all targets are the exact same.

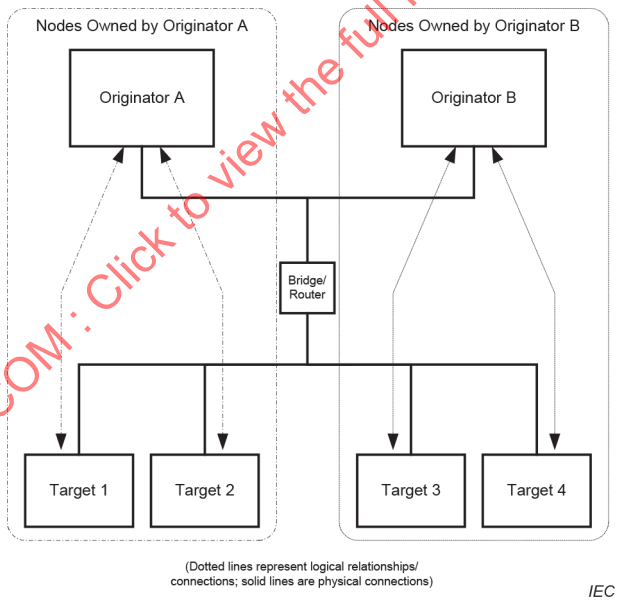


Figure 60 – Target ownership

Use of standard bridges/routers and standard lower-layer protocol stacks within the end-nodes offers the opportunity for additional errors that require protection measures that are more stringent than those applied in standard CPF 2 connection establishment. For instance, the bridge/router could mis-direct (for example corrupt the destination NodeID of) a connection request from originator A intended for Target 1 to Target 2, 3, or 4 instead. Or the source of the error could be the user mis-configuring originator B to connect to Target 1 while originator A is off-line and Target 1 is powered. Without a second level of comparison above the identical electronic key, the connection from originator B to Target 1 would be allowed; at which point originator B's application could place Target 1 (assuming it's an output device) into an incorrect operational state with respect to originator A's commissioned application.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

8.4 Detection of mis-routed connection requests

All SafetyOpen requests will contain the UNID of the target device. Upon the receipt of a SafetyOpen the target shall compare the SafetyOpen target UNID (TUNID) with its own UNID. If the TUNID to UNID comparison is successful than the SafetyOpen destination is deemed to be correct and processing shall continue.

8.5 SafetyOpen processing

There are two ways of processing the SafetyOpen (see Figure 61):

- Destination, Ownership, Configuration data processing and SCID checking;
- Destination, Ownership and SCID Checking (Optional).

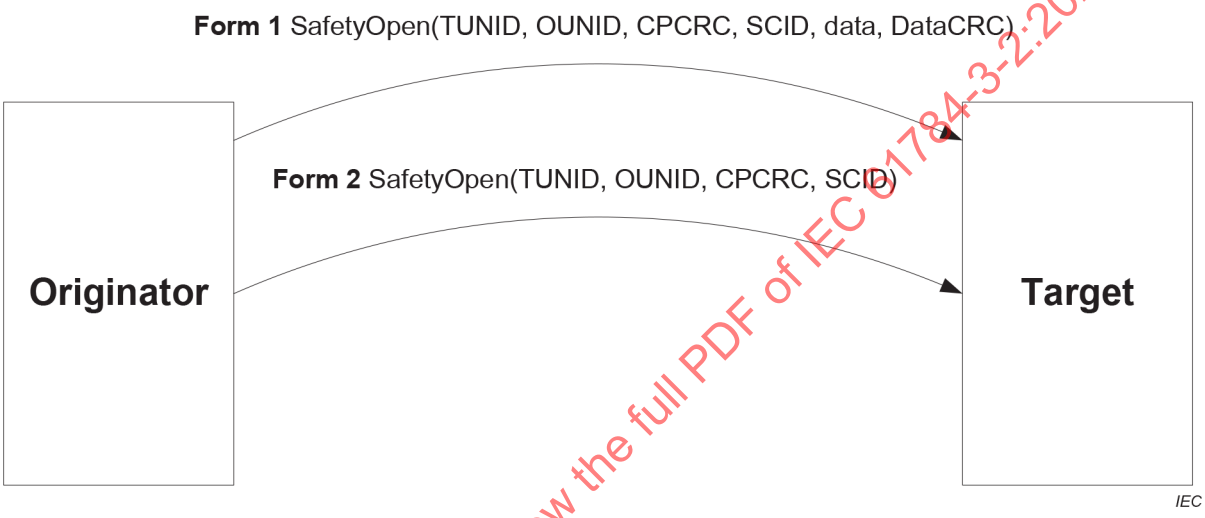


Figure 61 – SafetyOpen forms

8.6 Ownership management

There are two methods of establishing configuration and/or connection ownership, through the configuration tools or from the SafetyOpen. The tool can set the mode to be tool configuration only or originator configuration.

Any attempts to reconfigure a device via the SafetyOpen shall be rejected if the tool only configuration mode is selected.

If the originator configured mode is used, the OUNID of the selected originator can be set by the software tool during target device commissioning for added security. Figure 62 defines the ownership sates the methods of transitioning from ownership state to another ownership state.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

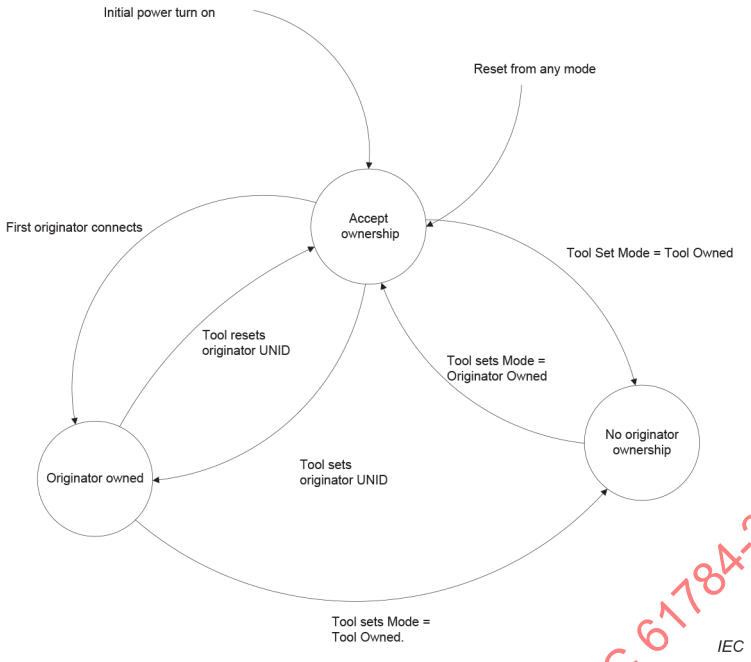


Figure 62 – Connection ownership state chart

To establish ownership of the configuration (and the connection in outputs), in targets the OUNID of the originating device shall be passed to the target in the SafetyOpen service.

The OUNID of the originating device shall be stored in non-volatile storage with the configuration to which it is associated.

Output devices shall store the OUNID associated with safety outputs to prevent other originators from hijacking outputs inadvertently. Keeping the originator OUNID associated with the configuration will allow multiple devices to connect to an input device and still maintain configuration ownership. Figure 63 defines the mapping of the SafetyOpen UNIDS to the target device originator ownership locations.

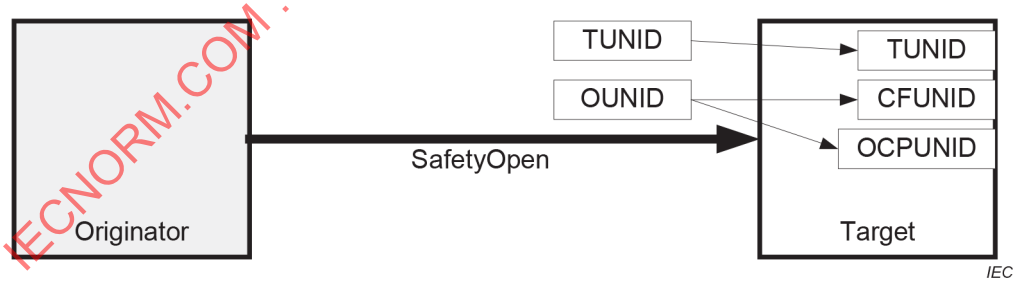


Figure 63 – SafetyOpen UNID mapping

8.7 Bridging different physical layers

CPF 2 nodes share a common application and user layer as defined in Figure 64.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

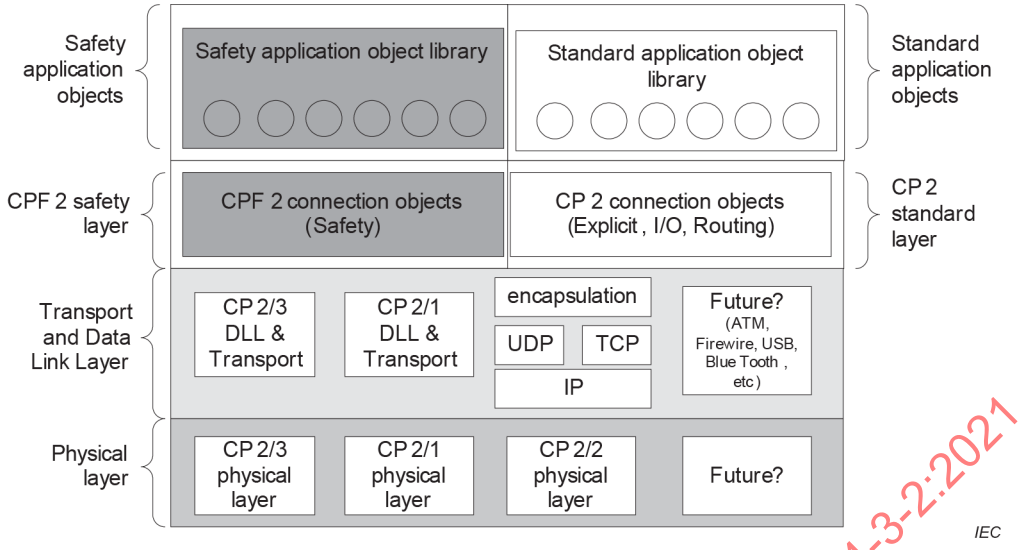


Figure 64 – Common CPF 2 application layer

The CPF 2 connection objects are the entities that reconcile the inherent differences between the capabilities and services provided by the underlying networks, exchanging safety data with the application objects above. For instance, CP 2/3 physical layer (i.e. CAN) data frames are limited to a maximum of 8 octets each. The CPF 2 connection object in a CP 2/3 node transports I/O packets larger than 8 octets via CP 2/3's I/O fragmentation protocol; whereas on the higher-capacity networks like CP 2/2, the maximum connection size of 511 octets fits into one physical layer data frame. Once a safety connection is established, the safety-related application layer exchanges safety data with the safety connection objects.

The safety protocol has been designed to enable end-to-end transport of the safety data without requiring specific knowledge of the safety protocol within or SIL 3 assessment of intermediate devices to have either specific knowledge of the safety protocol or safety certification. Figure 65 depicts an end-to-end connection between a safety node on CP 2/3 and a safety node on CP 2/1 routed across a CP 2/2 network. The safety connection endpoints enable the application level peers to share safety data.

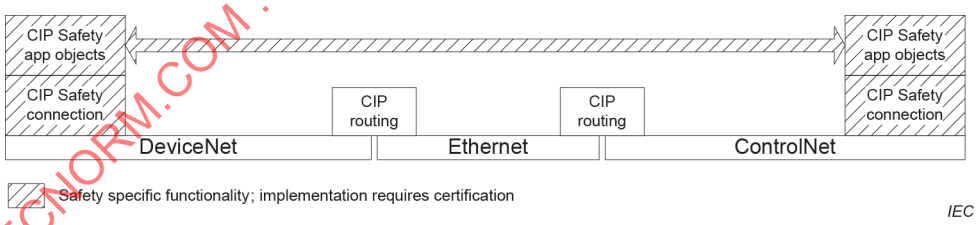


Figure 65 – End-to-End routing example

Safety connection establishment is dynamic on every network. CP 2/2 originators employ the ForwardOpen service of the connection manager object. The connection path of a ForwardOpen service's data includes a safety network segment for the end node. This safety network segment informs the recipient that a connection object capable of supporting a safety connection shall be available in order to accept the request. It also includes data used to specify Connection object attributes related to its safety behavior (for example expectation timers).

On CP 2/3 Safety, the originator shall establish an explicit messaging connection with the router or end-node to deliver the ForwardOpen or SafetyOpen service requests. The other CPF 2 networks (typically) deliver the ForwardOpen to the UCMM without a connection.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

8.8 Safety connection establishment

8.8.1 Overview

Establishing safety connections is a key system function. There are two safety elements that need to be addressed; setting up a connection relationship in an originator, and setting up a run-time connection. This Subclause 8.8 will describe the system requirements to perform both of these operations with integrity.

8.8.2 Basic facts for connection establishment

The basic facts for safety connection establishment are listed below.

- SafetyOpen is a service defined in the Connection object.
  - An explicit messaging connection is required with a path that targets the Connection object.
- ForwardOpen is a service defined in the Connection Manager object.
  - This is an unconnected message with a path that targets the Connection Manager object.
  - When originating from a CP 2/3 Safety originator, an explicit messaging connection is required with a path that targets the Connection Manager object.
- One additional set of connection parameters are required in the SafetyOpen to define the third connection point in CP 2/3 Safety nodes when the connection type is Multipoint. These parameters are contained in the Safety Segment.
- For devices that use object instances and/or connection points for their safety connection application paths:
  - A null application path is defined to mean either that a connection has no application data, or the SafetyOpen contains no configuration data. Each safety module vendor shall define a null path that is appropriate for their device. A null path shall always use a full path reference (i.e. 20 04 24 [vendor specific instance]). For EDS-based devices, the selected null instance shall be disclosed with an entry in the connection manager section of the EDS file (see ISO 15745-4:2003, Annex C).
  - The application path for the Time Coordination connection shall always be a null path.
  - Type 2 SafetyOpen (no configuration data) shall include a null application path for the configuration path.
- There is no path required for the Time Correction connection.
- The extra parameters of the third connection point are named and have values as follows:
  - Time Correction RPI;
  - Time Correction Network Connection ID;
  - Connection Type = Multipoint;
  - Priority = High Priority;
  - Fixed/Variable = Fixed;
  - Connection Size = 6 (fixed Time Correction size).
- The Time Correction Network Connection ID is not part of the CPCRC.
- The standard O-to-T and T-to-O connection sizes shall always reflect the 2-connection size for each. In other words, the connection that has the Data and Time Correction packets concatenated will have a size that reflects this combination. It will be the responsibility of bridges and the CP 2/3 Safety nodes to calculate the appropriate sizes for the connection resources on CP 2/3 Safety (this is made easier in that the size of the third connection point, provided in the SafetyOpen message, can be added or subtracted).

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

8.8.3 Configuring safety connections

This Subclause 8.8.3 defines the parameters needed to perform the safety protocol. It also defines the Safety Segment parameters needed to be passed in the SafetyOpen to properly set up a safety connection. This Subclause 8.8.3 will describe how these parameters get assigned and suggest reasonable defaults for a safety system.

The parameters that need to be configured for a safety connection are:

- Target UNID;
- Originator UNID;
- EPI;
- Ping Interval EPI Multiplier;
- Time Coord Msg Min Multiplier;
- Timeout_Multiplier;
- Max Consumer Number;
- Network Time Expectation Multiplier;
- ASYNC;
- Max_Fault_Number (Extended Format only).

All but the ASYNC parameter are included in the SafetyOpen service. The configuration Software for a Safety Connection Originator shall provide a means for the following parameters to either be configured or given default values: Expected Packet Interval, Target UNID, Originator UNID, Timeout_Multiplier, Ping Interval EPI Multiplier, Time Coord Msg Min Multiplier, Max Consumer Number, Network Time Expectation Multiplier, ASYNC and Max_Fault_Number (Extended Format only). The Max_Fault_Number is defined as a constant. Table 105 summarizes how these parameters and others will be obtained.

Safety originators shall use the value 02_{hex} for the Max_Fault_Number parameter in the SafetyOpen.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Table 105 – Safety connection parameters

Parameter	Suggested configuration method	Suggested default value
Data Expected Packet Interval (EPI)	User assigned or tool-based estimation	None, user shall provide one
Time Coordination EPI	Data EPI × Ping Interval EPI Multiplier	Software calculated
Time Correction EPI	Data EPI × Ping Interval EPI Multiplier	Software calculated
Target UNID	User assigned or obtained by software	None, user shall provide one
Originator UNID	User assigned	None, user shall provide one
Timeout_Multiplier	User assigned	2
Ping Interval EPI Multiplier	Default value for inputs or outputs	100 for inputs 19 for outputs
Time Coord Msg Min Multiplier	Default value on path	2 for non-bridged 3 for bridged
Max Consumer Number	Fixed value	15
Network Time Expectation Multiplier	Calculation	Calculated
ASYNC	EDS file input	1 (asynchronous)
Initial Time Stamp (Extended Format only)	Dynamic assignment	None, producer shall assign a value based on connection format and type
Initial Rollover Count (Extended Format only)	Dynamic assignment	None, producer shall assign a value based on connection format and type
Max_Fault_Number (Extended Format only)	Fixed value	2

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

8.8.4 Network time expectation multiplier

One of the primary calculations required of a Safety Configuration Tool or Connection Originator is the calculation of the Network Time Expectation Multiplier. This Subclause 8.8.4 provides a simplified way to do this calculation.

Subclause 9.3.2 defines the Network Time Expectation Multiplier as:

$$\text{Network_Time_Expectation_Multiplier} > [\text{EPI_in_sec} \times \text{Timeout_Multiplier} + \text{Safety_Message_Time(max)} + \text{Time_Coord_Message_Time(max)}] / 128\ \mu s + \text{Connection_Correction_Constant} \quad (11)$$

Some simplifying assumptions can be made as follows:

- Safety Message Time (max) = 1 EPI;
- Time Coordination Msg Time = Safety Message Time (max);
- Effect of Time_Drift_Constant is negligible (Connection Correction Constant can be ignored).

Under these assumptions, the generalized equation can be stated:

$$\text{Network Time Expectation Multiplier} = [\text{EPI_in_sec} \times (\text{Timeout_Multiplier} + 2)] / 128\ \mu s \quad (12)$$

Where:

The value does not exceed 5,8 s

The Network Time Expectation Multiplier parameter can now be determined by a common set of user inputs and one EDS file parameter.

Figure 66 shows where the various parameters defined in Table 105 are obtained. It also shows how these parameters are used by the software to construct the safety segment of a SafetyOpen.

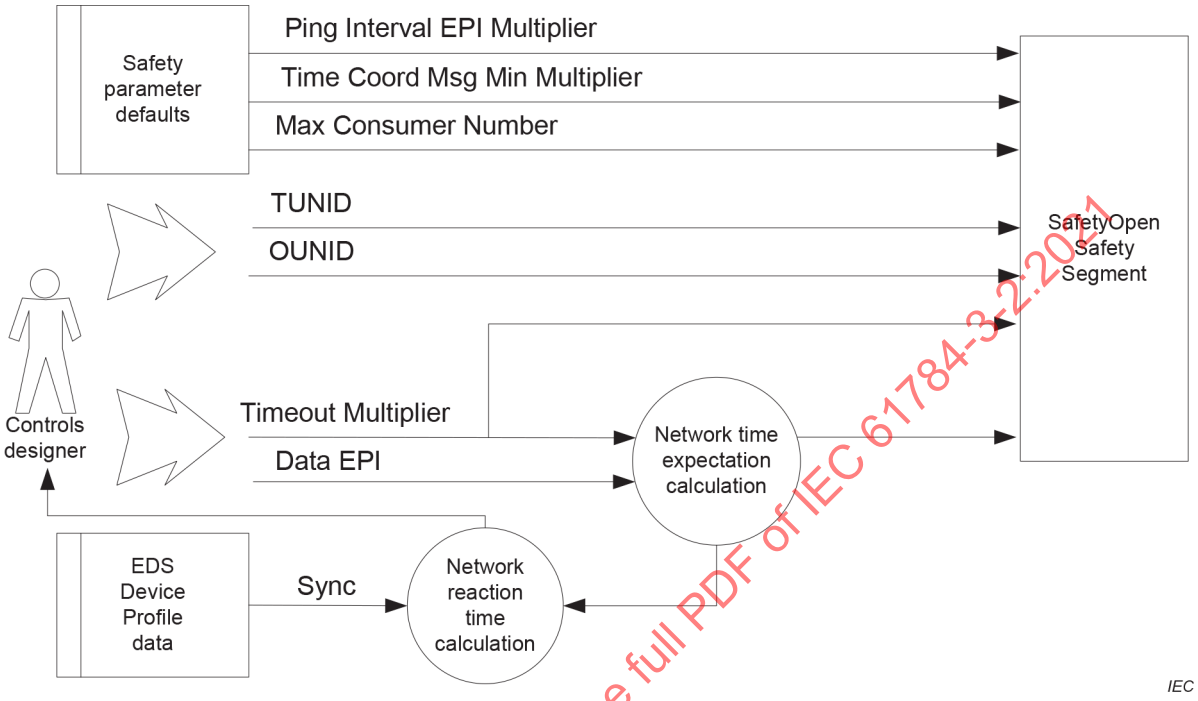


Figure 66 – Sources for safety related connection parameters

Figure 67 defines how the SafetyOpen parameters are mapped in Originators and Targets of a safety connection.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

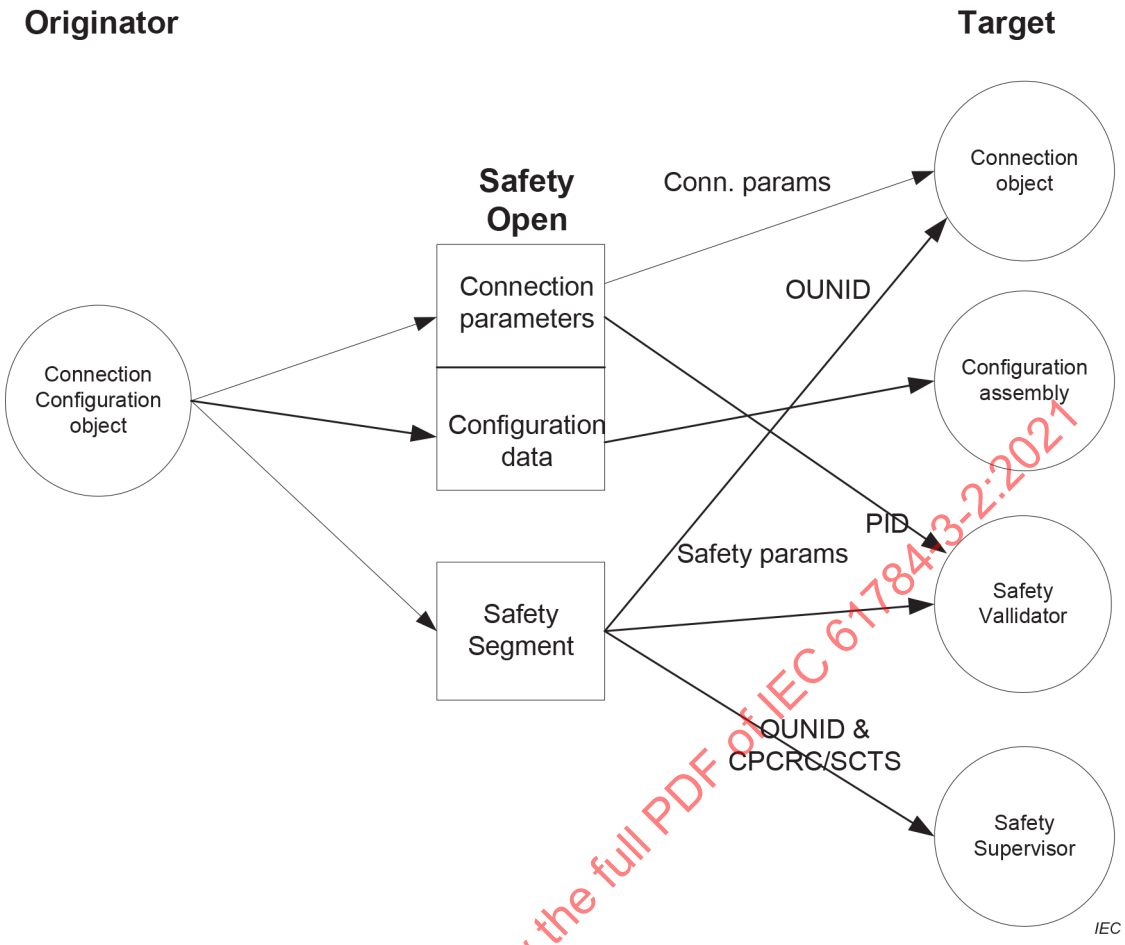


Figure 67 – Parameter mapping between originator and target

8.8.5 Establishing connections

When configuration data is transmitted within the SafetyOpen this is defined as a Type 1 SafetyOpen. When no configuration data is transmitted within the SafetyOpen this is defined as a Type 2 SafetyOpen. This is defined in Figure 68.

If a connection has configuration data, this configuration data shall only be sent when it is needed. Unless the configuration has been changed, this shall be accomplished by sending a Type 2 SafetyOpen, and only followed with a Type 1 SafetyOpen if the target responds with Device Not Configured error.

When a device receives a Type 1 SafetyOpen containing configuration data and an SCID that matches its existing configuration, it shall re-apply the configuration. All existing rules checks (i.e. OUNID and TUNID checks) shall still apply.

Since all safety nodes are required to have NV storage for configuration data, this is only likely on device replacement, initial start-up or when the configuration has changed. This process is illustrated in Figure 69.

Targets shall respond to a Type 2 SafetyOpen with an error code 01_{hex}, additional code 0110_{hex} (device not configured), when the device is not configured.

When an originator detects that the configuration data held for a device has changed, it shall always issue a Type 1 connection request the first time it connects. The SCID returned shall be validated against the value held.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

There are two kinds of Type 2 SafetyOpens: with and without the SCID.

- Type 2a: When a target receives a Type 2 SafetyOpen (no configuration data) accompanied by a non-zero Safety Configuration ID (SCID = SCCRC + SCTS), it shall compare it against the SCID of the configuration and only accept the connection if they match.
- Type 2b: When a target receives a Type 2 SafetyOpen (no configuration data) accompanied by a zero value SCID, it skips the check.

Table 106 provides a summary of the Forms of SafetyOpens.

Table 106 – SafetyOpen summary

	Type 1SafetyOpen with data	**Type 2aSafetyOpen with SCID check**	**Type 2bSafetyOpen without SCID check**
TUNID	X	X	X
OUNID	X	X	X
UPID[a]	X	X	X
CPCRC	X	X	X
SCID	X	X	= 0
Config. Data in SafetyOpen	Yes	No	No

[a] UPID is derived from components in the SafetyOpen or from application data returned in the SafetyOpen response. See 6.3.12.

The processing of SafetyOpens in Targets will differ depending on the Type of SafetyOpen message that is received. Figure 69 defines the message and event sequence for the Type 1 SafetyOpen and the objects that are responsible for the various processing steps. Figure 69 defines that the primary difference between processing Type 1 and Type 2 is the step where configuration data is passed to a configuration assembly and an owner assigned to that configuration.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

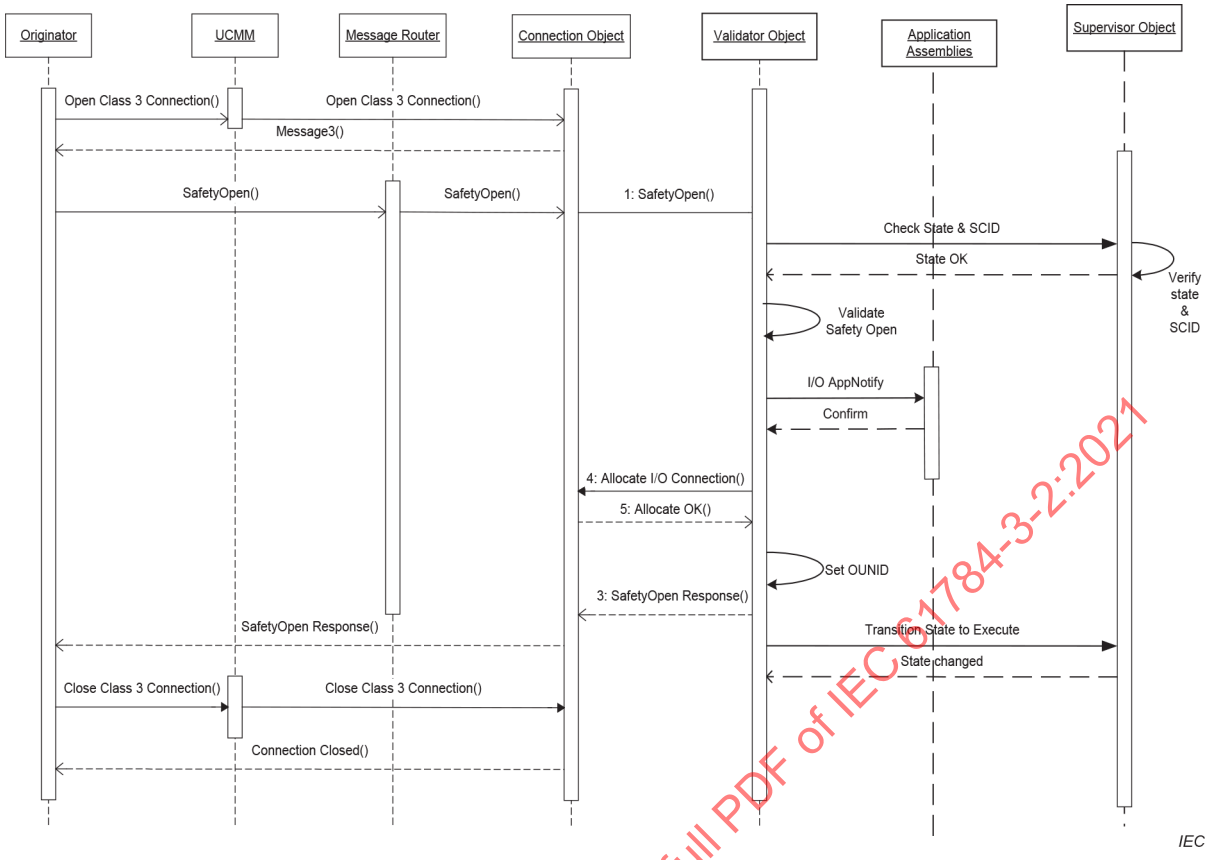


Figure 68 – CP 2/3 Safety connection establishment in targets for Type 2a SafetyOpen

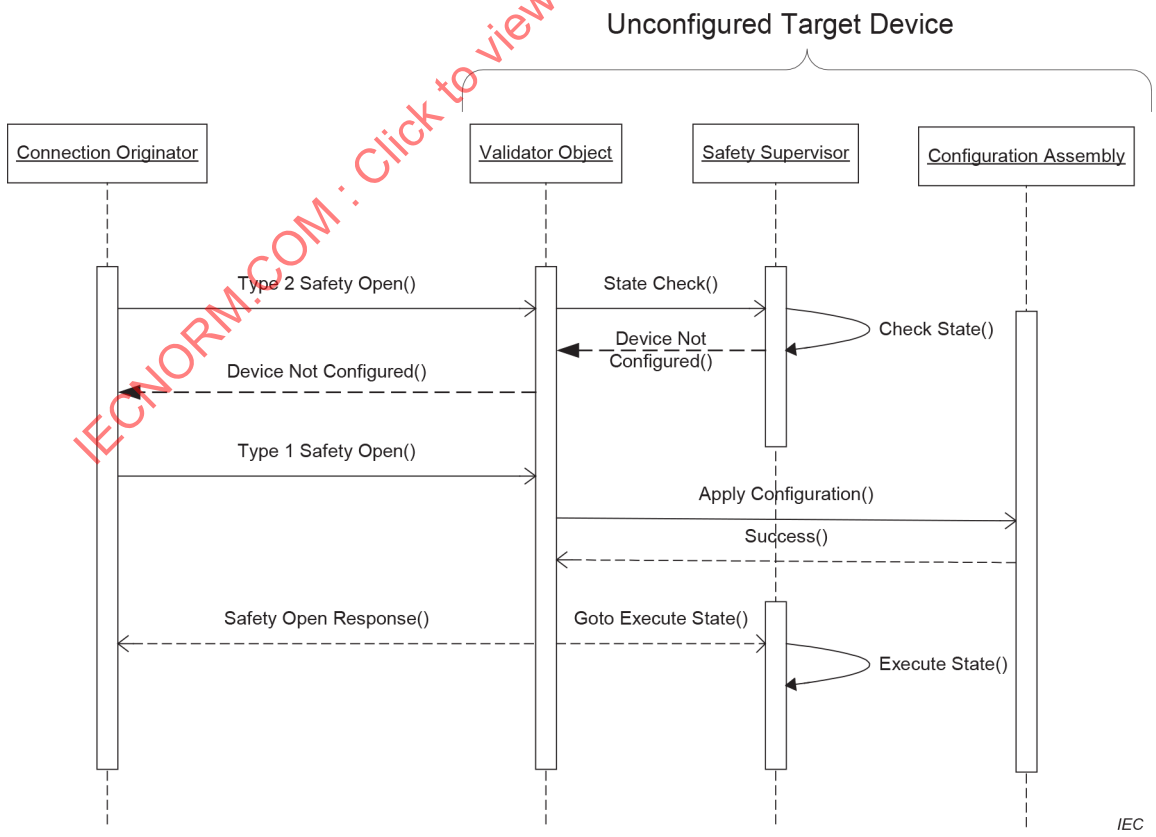


Figure 69 – General sequence to detect configuration is required

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

8.8.6 Recommendations for consumer number allocation

When a Multipoint connection is established, the producer of that connection shall allocate a unique consumer number to the consumer. The main difficulty with this process is not in the initial allocation, but in dealing with the case where a producer has closed a connection for some reason and now needs to decide when it is acceptable to re-assign that consumer number again.

Since multipoint producers will continue to produce data even though a connection to a particular consumer was closed (i.e. assumes other consumer connections still open), the only mechanism available for a multipoint consumer to detect the loss of the connection is by detecting that it has not gotten a Time Correction message within Timeout_Multiplier.PI + 1 ping intervals. During this period, the Consumer still thinks the connection is open, is still processing received data, and is still sending Time Coordination responses (even though the producer ignores them).

If a producer were to get a new connection request from another consumer and re-allocate this consumer number, there would be two consumers using the same number during this period. The producer would again start processing Time Coordination responses and sending Time Correction messages with that consumer number. In other words, if the timing were just right, the old consumer might never detect the connection has failed and there would exist two consumers with the same number sending conflicting clock information and using conflicting correction values. While this case will ultimately be detected by the producer through PID seeding, a means shall be employed to minimize the occurrence.

Multipoint producers shall quarantine consumer numbers that have been taken off-line for Timeout_Multiplier.PI + 2 ping intervals before it can be re-allocated to another connection. The only exception to this is when a Consumer issues a ForwardClose to notify the producer that the connection is being closed. In this case, the consumer number can be re-used immediately.

8.8.7 Recommendations for connection establishment

When a multipoint consumer decides to unilaterally close a connection, the only way for a producer to detect this event (other than getting a Forward Close from the consumer) is when it no longer receives a Time Coordination response for Timeout_Multiplier.PI + 2 Ping Intervals. During that time interval, the consumer number is still allocated to that consumer. There is a strong likelihood that while this connection is still open, that consumer will issue a new SafetyOpen. Producers have two options in this case:

- Search through the existing connections and see if a connection to this same consumer is already established and if so, re-issue the consumer number again;
- Allocate a new consumer and allow the old consumer number to time-out and go through quarantine.

The first option is the more complicated to code, but is the recommended option since it offers a more robust re-allocation scheme for consumer numbers. The advantage of the second option is that it is simpler to implement, but allows for consumer numbers to languish in quarantine longer than necessary. The second option can also make connection startup problematic for applications where the number of consumers is > 8.

If option one is used, the recommended scheme to match up connections should be to match up:

- OUNID, and
- Application data path.

If these match up with the parameters of an existing connection, then that device's consumer number can be re-issued.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

8.8.8 Ownership establishment

Subclause 8.9 discusses two methods of establishing connection ownership, through the software tools or from the SafetyOpen. It indicates that devices are required to support a facility to allow "tool only" configuration or originator configuration. It also implies that attempts to reconfigure a device via the SafetyOpen will be rejected if the configuration is locked. If the "tool only" state is not set, the OUNID of the selected originator can also be set by the software tool during target device commissioning for added security.

This Subclause 8.8.8 will define how this capability has been defined in the new Safety objects. The new Safety objects are required in devices that will be configured by the Safety Network Configuration Tool (SNCT).

To establish ownership of the configuration (and the connection in outputs), the OUNID of the originating device is passed to the target in the SafetyOpen message.

Safety devices shall NV-store the OUNID for the configuration in the device. Also, safety devices shall NV-store the signature for the configuration (SCID) in the device. The SCID is derived by concatenating the SCCRC and the SCTS in the SafetyOpen.

Output devices shall NV-store the OUNID associated with the safety output connection.

When the user has tested and verified the tool-generated configuration, they can lock the configuration from changes and flag it as "Locked". The "Configuration Lock" flag is an attribute of the Safety Supervisor. To modify it, a password can be provided which provides user defined security.

Devices which are configured by the SafetyOpen cannot have a "Configuration Lock" condition. The assumption is the Lock condition is set and controlled at the connection originator.

8.8.9 Ownership use cases

8.8.9.1 General

This Subclause 8.8.9 will present a series of connection scenarios where configuration is also being attempted. Each scenario will provide a brief description of how the device needs to deal with each case. Most of these cases utilize the SafetyOpen to configure the device. As such, the tool-based configuration features such as the "Configuration Lock" attribute shall not be in use.

8.8.9.2 The user-designated owner connects and configures an un-owned, un-configured input device – (OUNID assigned at first connection)

The Configuration Lock attribute in the target shall be "unlocked" and the Safety Supervisor shall be in Configure mode; device has no configuration. The SafetyOpen is validated by the target device as being correct and the originator OUNID is stored in the target and related to the configuration. A point-to-point or multipoint connection is established. Normal operation starts.

The originator of a Type 1 SafetyOpen that configures a previously unconfigured and unowned input device shall become the owner of the configuration.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

8.8.9.3 The user-designated owner connects and configures an un-owned, un-configured output device – (OUNID assigned at first connection)

The Configuration Locked attribute in the target shall be "unlocked" and the Safety Supervisor shall be in Configure mode; device has no configuration. The SafetyOpen is validated by the target device as being correct and the OUNID is stored in the target and related to the configuration and the connection. A point-to-point connection is established. Normal operation starts.

A Type 1 SafetyOpen that configures a previously unconfigured and unowned output device shall become the owner of both the connection and the configuration.

8.8.9.4 Owner connects and configures an owned, un-configured input device – (OUNID assigned by tool)

The Configuration Lock attribute in the target shall be "unlocked" and the Safety Supervisor shall be in Configure mode; device has no configuration. The SafetyOpen is validated by the target device as being correct and the SafetyOpen OUNID matches the stored OUNID. A point-to-point or multipoint connection is established. Normal operation starts.

8.8.9.5 Owner connects and configures an owned, unconfigured output device – (OUNID assigned by tool)

The Configuration Lock attribute in the target shall be "unlocked" and the Safety Supervisor shall be in Configure mode; device has no configuration. The SafetyOpen is validated by the target device as being correct and the SafetyOpen OUNID matches the stored OUNID for the configuration and the connection. The target stores the configuration. A point-to-point connection is established. Normal operation starts.

A second device attempts to connect to an owned point-to-point output connection.

If no connections are open the SafetyOpen will be evaluated by the target device. If a Type 1 SafetyOpen is sent where the originator OUNID is different than the OUNID that is stored with the connection the SafetyOpen shall be rejected and an error message, "O_UNID Mismatch" is returned.

8.8.9.6 Owner connects and attempts to re-configure a tool-owned, configured device – (Configuration Lock set)

If an originator attempts to configure a device with the Configuration Lock attribute set, the device shall reject the SafetyOpen and return an error message "Configuration Not Allowed" is returned.

8.8.9.7 Device reconfiguration – Input Device

The owner of a device sends a SafetyOpen with configuration data plus an SCID (SCCRC and SCTS) to the target device. The data is not necessarily the same as that which exists in the device and the SCID does not necessarily match the existing SCID. Regardless, as long as the following process is followed, it shall treat the message as a re-configuration.

A target input device that has an existing configuration shall (at a minimum) do the following when a Type 1 SafetyOpen is received:

- verify that the TUNID in the SafetyOpen matches the device TUNID;
- if configuration data in included (Type 1), verify that the OUNID in the SafetyOpen matches the stored OUNID;
- verify the Electronic Key matches the device;
- calculate the SCCRC over the received data and confirm that it obtains the same value;

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

- verify the CPCRC over the configuration is correct;
- start its reconfiguration process (enters Config State), close and inhibit connections during the reconfiguration (respond to connection requests with an error response, "Invalid Mode/State");
- update the configuration and SCID in NV Memory;
- verify and validate the connection parameters;
- validate the application path;
- confirm the safety connection requested is supported;
- safety parameters are within valid ranges;
- transition the connection to the established state, and the device to the executing state;
- new connections can now be accepted.

A connection of the requested type is established. While new connections can again be accepted, these other devices shall now either have the new SCID, or connect with an SCID = 0.

8.8.9.8 Device reconfiguration – Output Device

The owner of a device sends a SafetyOpen with configuration plus an SCID to the target device. The data is not necessarily the same as that which exists in the device and the SCID does not necessarily match the existing SCID. Regardless, as long as the following process is followed, it shall treat the message as a re-configuration.

A target output device that has an existing configuration shall (at a minimum) do the following when a Type 1 SafetyOpen is received:

- if the connection path is to an output resource, verifies that the OUNID in the SafetyOpen matches the OUNID for the connection;
- verify that the TUNID in the SafetyOpen matches the device TUNID;
- verify the Electronic Key matches the device;
- if configuration data in included (Type 1), verify that the OUNID in the SafetyOpen matches the stored OUNID for the configuration;
- calculate the SCCRC over the received data and confirm that it obtains the same value;
- verify the CPCRC over the configuration is correct;
- start its reconfiguration process by closing and inhibiting connections during the reconfiguration (respond to connection requests with an error response, "Invalid Mode/State");
- update the configuration and SCID in NV memory;
- verify and validate the connection parameters;
- validate the application path;
- confirm the safety connection requested is supported;
- safety parameters are within valid ranges;
- transition the connection to the established state, and the device to the executing state.

A connection of the requested type will now be established.

8.8.9.9 Connection establishment to a previously owned device (Changing OUNID)

When attempting to configure a device that has another owner, a SafetyOpen configuration request (i.e., Type 1) without a matching OUNID will be rejected with an error response, "OUNID Mismatch".

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

To clear an existing OUNID, safety targets shall support a "reset to out-of-box" using a reset switch on the device or using the special reset command defined in the Safety Supervisor.

If the device has a Safety I/O connection when a reset command is received, the reset command shall be rejected and an error message returned, "Invalid Mode/State". In order for a device to be reset by command it shall not have Safety I/O connections established.

A second device attempts to connect to an owned multipoint connection.

A second originator sends a SafetyOpen (i.e., Type 2a, or Type 2b) to a device that has a multipoint connection owned by another originator. If the SCID in the SafetyOpen is non-zero, the SCID is compared to the saved SCID. If the signatures match, the connection is established. If the signature does not match, the error response "SCID Mismatch" is returned. The owner does not need to be active during this process.

A target device that has an existing configuration shall (at a minimum) do the following when a Type 2a or 2b SafetyOpen is received:

- if the connection path is to an output resource, verifies that the OUNID in the SafetyOpen matches the OUNID for the connection;
- if the SCID is non-zero, confirm the SCID matches the device SCID;
- verify that the TUNID in the SafetyOpen matches the device TUNID;
- verify the Electronic Key matches the device;
- verify the CPCRC over the configuration is correct;
- verify and validate the connection parameters;
- validate the application path;
- confirm the safety connection requested is supported;
- safety parameters are within valid ranges;
- transition the connection to the established state.

8.8.10 PID/CID usage and establishment

The PID/CID seeding mechanism has been defined to detect message insertion from an invalid source. This insertion can occur from another producer sending Safety Data, another producer sending Time Correction messages, or an invalid consumer sending Time Coordination messages. All these cases will be covered by the PID/CID scheme in the Safety Protocol. The key to this is the exchange of PID/CID information during the connection establishment process. The Producer will provide its PID to all its consumers, and all the consumers shall provide their respective CID back to the producer. This exchange occurs regardless of who originates the connection, or what type of safety connection is being established.

During connection establishment the producing and consuming nodes shall exchange their respective PID/CID information (Vendor ID + Device Serial Number + Connection Serial Number). The originator sends its ID in the SafetyOpen request, and the target returns its ID as part of the SafetyOpen Success response. The two cases are defined in Figure 70.

The PID shall be used to seed Data production CRCs and Time Correction CRC, and the CID shall be used to seed the Time Coordination CRC.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

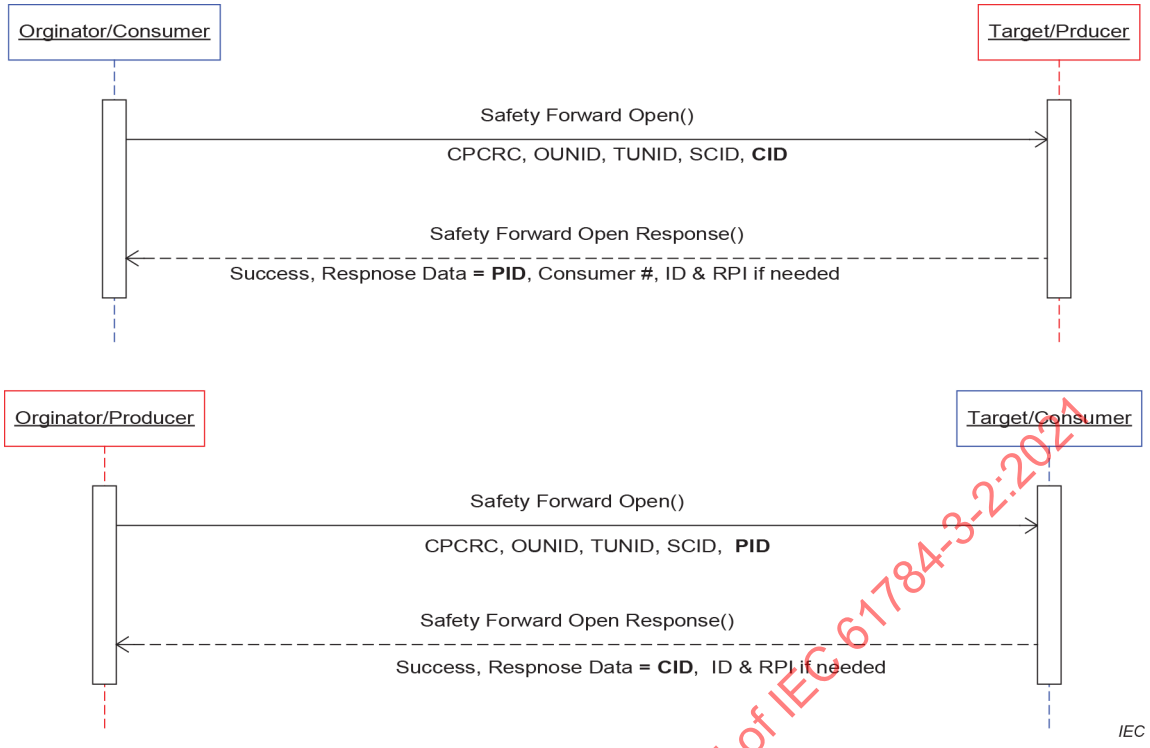
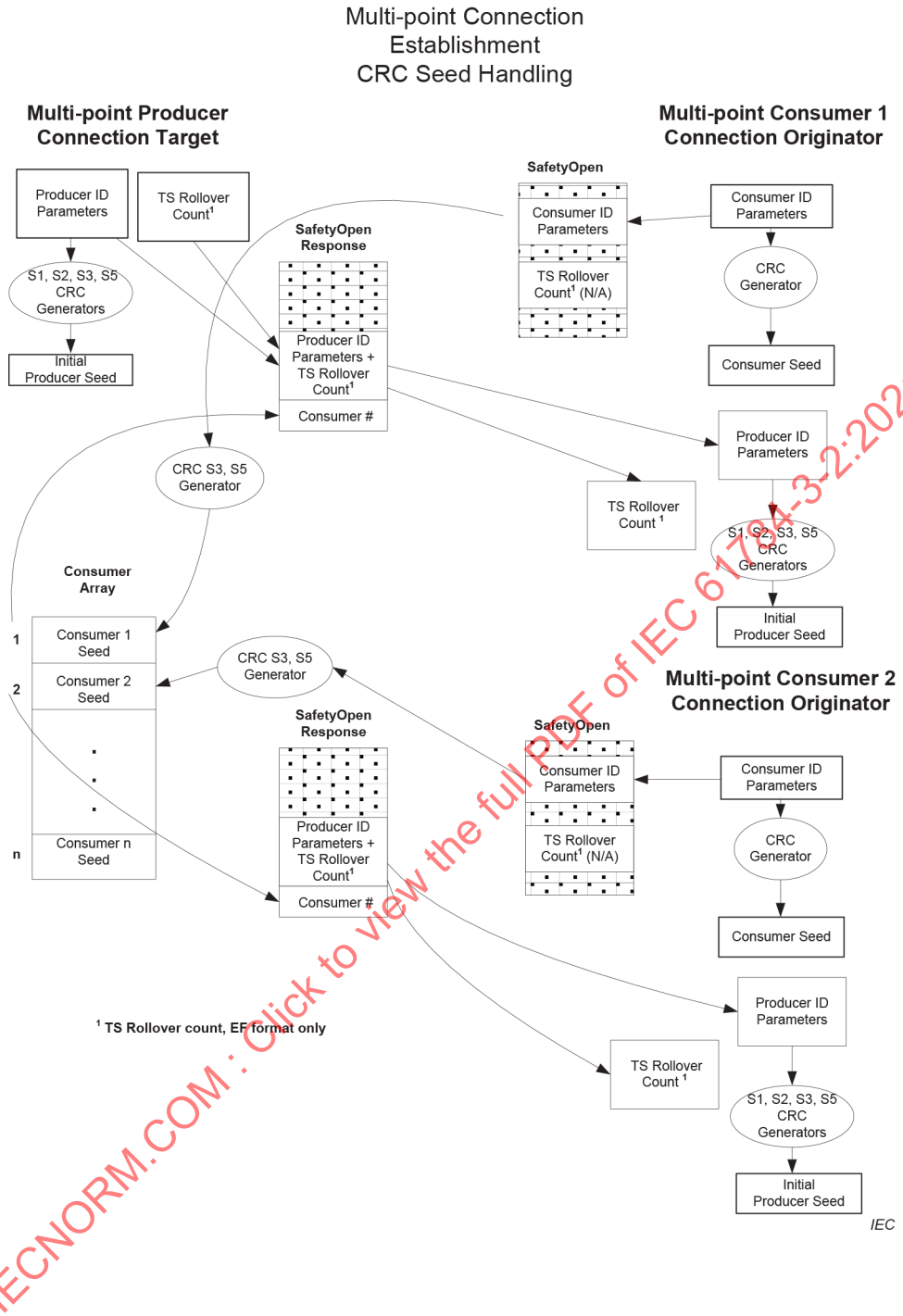


Figure 70 – PID/CID exchanges for two originator scenarios

8.8.11 Proper PID/CID usage in multipoint and point-to-point connections

The diagram shown in Figure 71 illustrates how the Producer and Consumer ID parameters are to be used to generate the CRC seed values for both the Base and Extended Format. This diagram defines the multipoint case, but it also applies to Point-to-point connections as well (this is done simply for consistency). References to TS _Rollover_Cnt and Rollover Detector only applies to the Extended Format is not used in the Base Formats. The producer seeds are generated using only the S1, S3 and S5 generators (i.e. same seed used for S1 and S2 CRC calculations) and the CID seed is generated with the S3 and S5 generator.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021



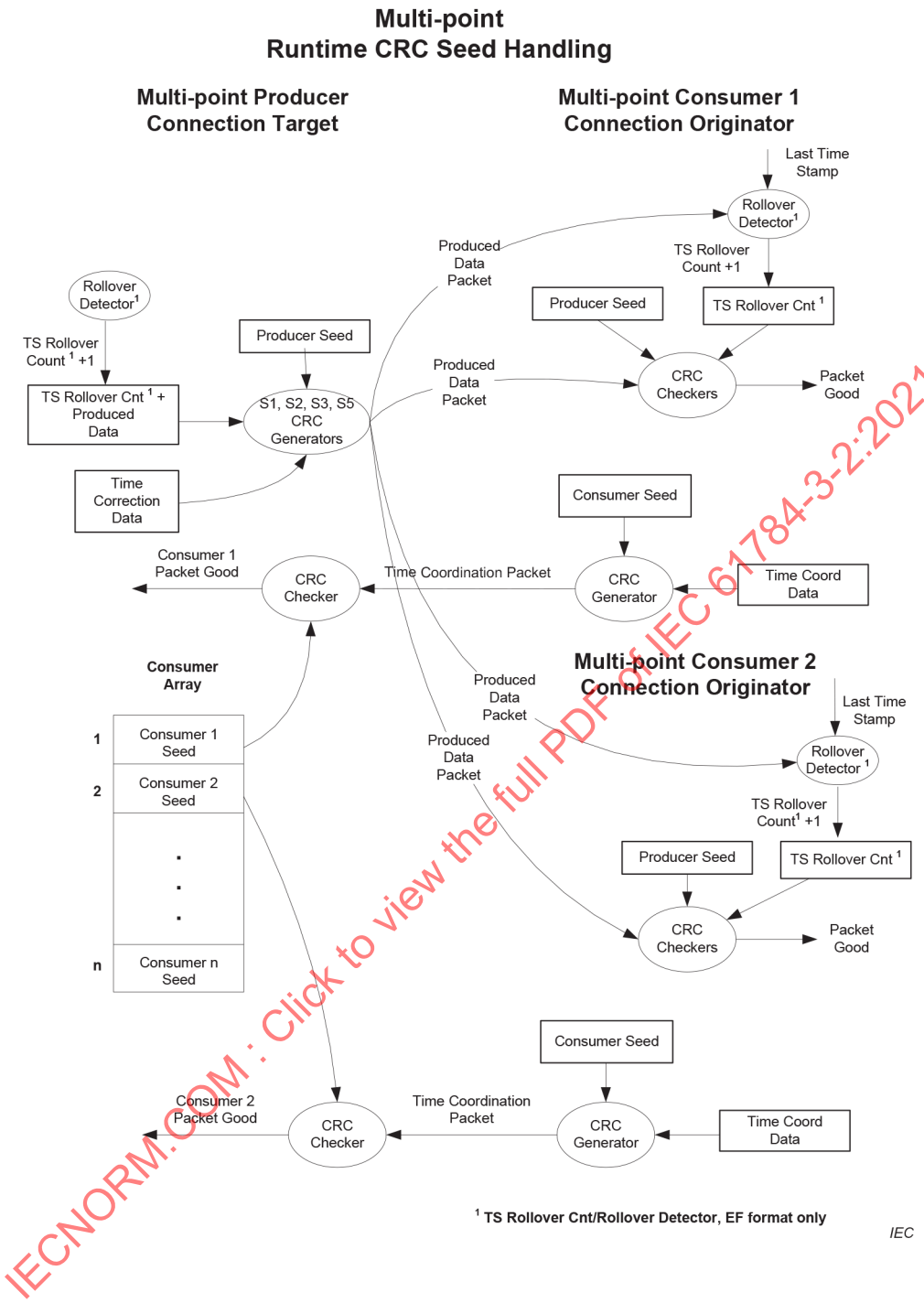
IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Figure 71 – Seed generation for multipoint connections

PID parameters shall be used to seed the CRCs for Produced Data messages and Time Correction messages, and CID parameters shall be used to seed the CRC for the Time Coordination responses.

As shown in the figure, multipoint producers will need to maintain a consumer array to keep track of the seed value for each allocated consumer number. The scheme shall also apply to Point-to-point connections except that only one consumer seed value needs to be maintained.

The diagram shown in Figure 72 illustrates how the seed values, set up during connection establishment, get used in the run-time data production.



IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Figure 72 – PID/CID runtime handling

8.8.12 Network supported services

The purpose of Subclauses 8.8.12 and 8.8.13 is to promote compatibility between devices developed to exchange safety data over the FSCP 2/1 Safety Networks. It defines guidelines on which safety services need to be supported by the different safety device types.

The goal is to allow the development of input and output devices which range from very simple discrete I/O to smart high functionality specialty I/O modules. When an input or output module reach a certain level of functional requirements, they may need to be viewed as embedding a safety Logic Device within the module.

8.8.13 FSCP 2/1 safety device type

8.8.13.1 General

To simplify the exchange of information and presentation of Safety Data to the users of multiple systems, the devices that participate on the safety network are divided into 4 device types. The device types are:

- Input Devices;
- Logic Devices;
- Output Devices;
- I/O Devices.

Input Devices are devices that translate user signals into safety data and send the safety data to Logic Devices. Input Devices do not receive safety data other than the safety connection status. If a device with input information needs to receive safety data from the other side of the safety connection, it should be considered an I/O Device or a Logic Device, and follow the guidelines of the I/O or Logic Safety Device Type.

Logic Devices are devices that process Safety Input Data and Produce Output Data. Direct communication between Input Devices and Output Devices is not supported. A Logic Device, no matter how simple, has to be between an Input Device and an Output Device.

Output Devices are devices that present some signal to the user's environment based on the safety data consumed by the device. Output Devices may have status that is produced back to the Logic Device.

I/O Devices are devices that have both Safety Inputs and Safety Outputs.

8.8.13.2 Safety connection category

All safety connections can be placed in one of four categories. They are:

- Input_Device_To_Logic_Device;
- Logic_Device_To_Output_Device;
- Logic_Device_To_I/O_Device (an Output device with Status is considered an I/O Device);
- Logic_Device_To_Logic_Device.

Logic devices may chose to support any or all of the safety connection categories. If a device does support a safety connection category, it shall support all the recommended services of that category.

8.8.13.3 Safety connection services

Table 107 defines all the defined Safety Validator Services that Connection Targets or Connection Originators can support.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Table 107 – Originator/Target service mapping

Connection originator or target	Safety connection types		Validator type
	Type	Use	
Target	Point-to-point	Producer	Type 1
Target	Point-to-point	Consumer	Type 2
Target	Multipoint	Producer	Type 3
Originator	Point-to-point	Producer	Type 1
Originator	Point-to-point	Consumer	Type 2
Originator	Multipoint	Consumer	Type 4

Table 108 defines the Safety Validator Services that Connection Targets or Connection Originators should not support. Multipoint producers are not required to initiate connections to its consumers; the consumers shall connect to it; Multipoint Consumers should be the connection Originator, and Multipoint Producers should be connection targets.

Table 108 – Unsupported originator/target service types

Connection originator or target	Safety connection types		Validator type
	Type	Use	
Target	Multipoint	Consumer	N/A
Originator	Multipoint	Producer	N/A

8.8.13.4 Services supported for each category

Figure 73 and Figure 75 list the preferred Safety Connection Services for various Connection Categories (see Figure 74 and Figure 76 for further clarification). For each Safety Connection Category, the different columns represent preferred methods of establishing safety connections between the two devices. For any particular device, only one column would be supported at one time.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

					Supported Services for Input or Output Type					
	Safety Connection Category				1		2	3		
	Safety Connection Service				Input Device To Logic Device		Logic Device To Output Device	Logic Device To I/O Device (Output with Status)		
	Originator or Target	Safety Connection Type			Op 1	Op 2		Op 1	Op 2	Op 3
Input and Output Devices	Target	Point-to-point	Producer			O			O	
	Target	Point-to-point	Consumer				R	R	O	
	Target	Multipoint	Producer		R			R		
Logic Devices	Originator	Point-to-point	Producer				R	R	O	
	Originator	Point-to-point	Consumer			O			O	
	Originator	Multipoint	Consumer		R			R		

Key

Op1, 2, 3 = Optional Combinations

R = Recommended Services for compatibility

O = Optional Service

Figure 73 – Connection categories and supported services

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

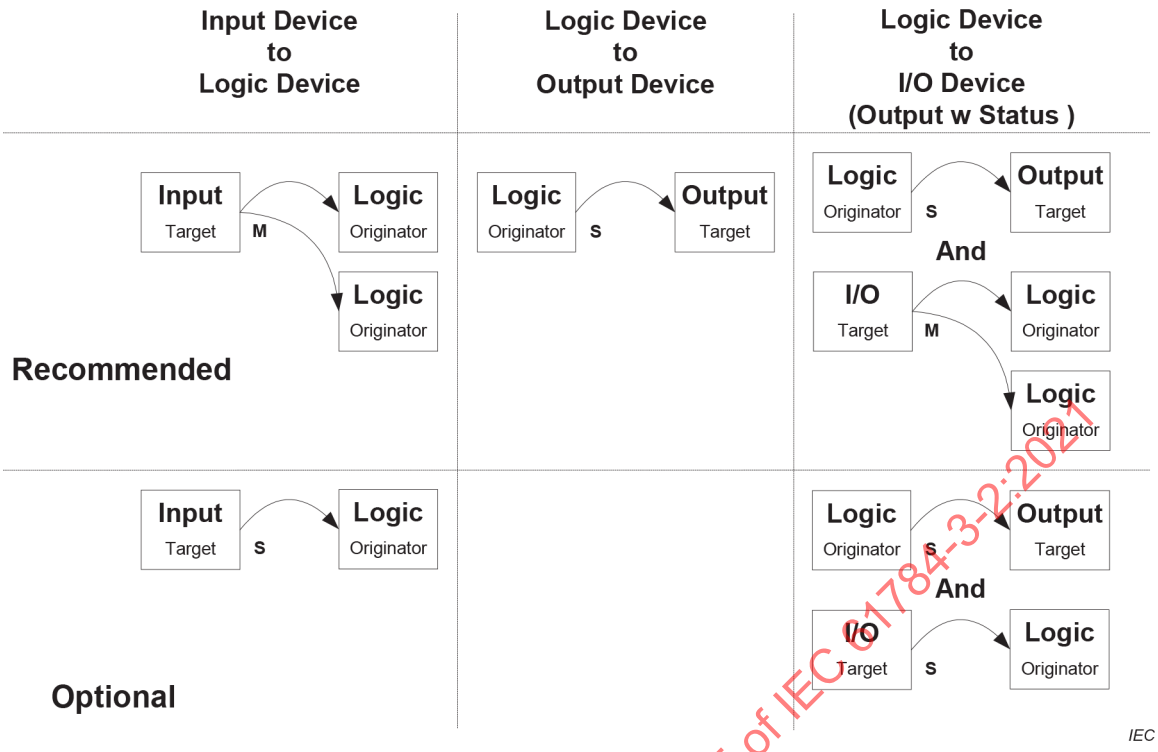


Figure 74 – Recommended connection types

	Safety connection service				Safety connection Category 4 Logic device to logic device			
	Originator or Target	Safety Validator type			Supported service combinations			
					Op 1	Op 2	Op 3	Op 4
Logic device target	Target	Point-to-point	Producer				O	
	Target	Point-to-point	Consumer			O		
	Target	Multipoint	Producer		R			
Logic device originator	Originator	Point-to-point	Producer			O		
	Originator	Point-to-point	Consumer				O	
	Originator	Multipoint	Consumer		R			

Key

Op1, 2, 3 = Optional Combinations

R = Recommended services for compatibility

O = Optional service

Figure 75 – Logic-to-logic supported services

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

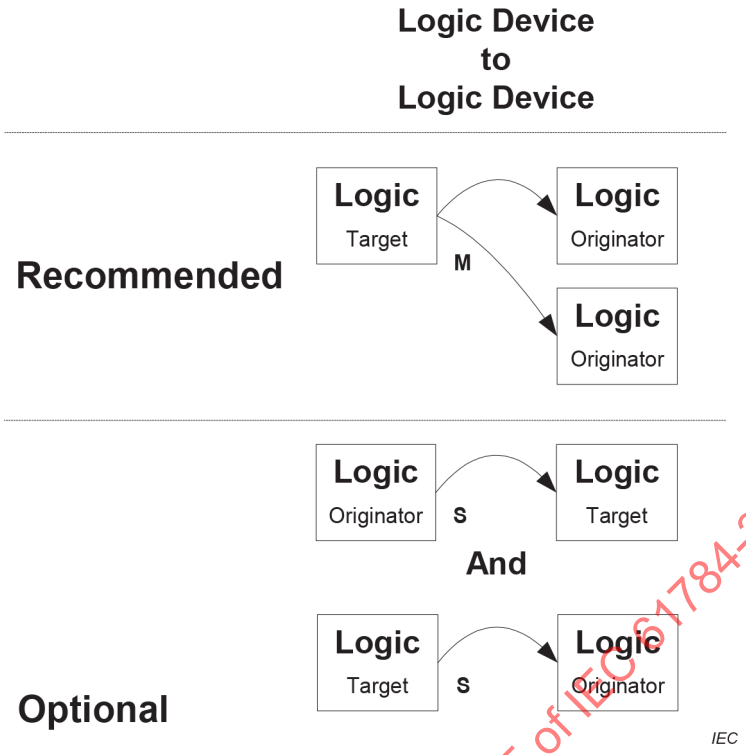


Figure 76 – Recommended connection types for logic to logic

8.9 Safety configuration process

8.9.1 Introduction to safety configuration

The purpose of this Subclause 8.9 is to identify the Safety Network Configuration process and the configuration data flows through the safety system. This Subclause 8.9 defines the system and the software requirements of the Safety Network Configuration interface and how data is protected to ensure the safety system meets the target SIL rating (up to SIL3).

The configuration process is comprised of two parts: 1) download and 2) testing and verification.

Download Process:

During the download portion of the configuration process the configuration data is transferred from one of the following two sources:

- The Safety Network Configuration Tool (SNCT) to the device being configured;
- From the originator to the target device.

Verification Process:

- During the verification stage the user will functionally test the device in the system, and visually verify that the correct configuration data has been transferred to the device being configured.
- Together the protections in these two parts ensure that devices are suitably configured for use in a safety system up to SIL3.

8.9.2 Configuration goals

The safety related goals for the configuration process for FSCP 2/1 safety devices are shown in Table 109.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Table 109 – Configuration goals

Goal	Description
Goal 1	To ensure with high integrity that the intended configuration created by the user with the software was correctly sent to and saved in the safety device
Goal 2	To have a common download process that is the same for the transfer of configuration data to all safety devices
Goal 3	To have a common download process that is the same for the transfer of configuration data from a software tool or an originating device during configuration
Goal 4	To ensure with the desired integrity level (up to SIL3) integrity that a target device has the intended configuration prior to opening a safety connection. The measures used during configuration download should be reused in the safety connection establishment process
Goal 5	To ensure unique identification of configuration with or without data being included within a connection establishment

8.9.3 Configuration overview

Safety configuration begins with the downloading of configuration data into a safety device. Figure 77 shows the possible configuration data transfers into safety devices. The numbers in the figure are references to the discussion numbering below.

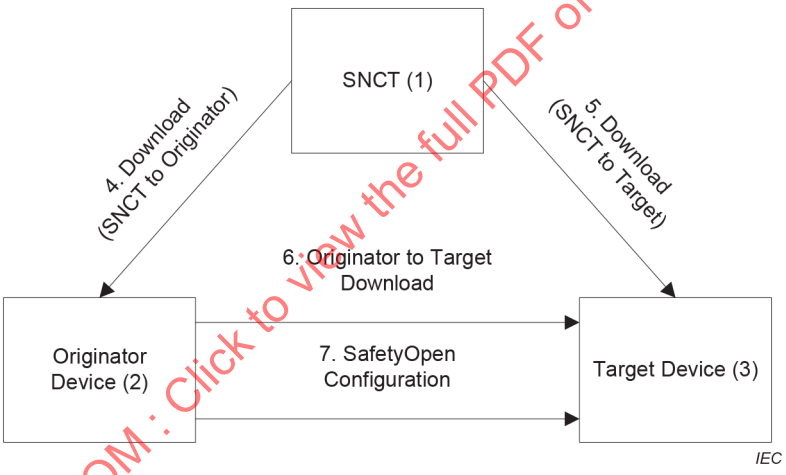


Figure 77 – Configuration data transfers

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

The devices involved in the configuration process are shown in Figure 77. The functions of items 1, 2, and 3 are described as follows:

- The SNCT (1) Safety Network Configuration Tool and the process described in this document allows this tool to be non-safety critical;
- The Originator (2) is a device that is capable of configuring Target devices (3) while initiating connections to them. Because these devices can hold configuration data for Targets (for targets that are not configured by the SNCT directly), they have additional procedures to complete the configuration process;
- The Target device (3) is one that can be either configured directly by the SNCT or can be configured by an Originator (2) owner. The ownership concept plays an important role in assuring the integrity of "originator configured" targets.

There are two basic configuration procedures (see Figure 77). The configuration procedures are described as follows:

- SNCT-to-Originator (flow 4) and SNCT-to-Target (flow 5). This procedure is one that configures a single device and these devices hold no configuration data for other devices;
- SNCT-to-Originator-to-Target (flow 4 plus flow 6 or 7). This special procedure is for configuring an originator device that holds configuration data for a target;
- Flow 6 is a procedure that duplicates the sequence of operations that would otherwise be done in flow 5;
- Flow 7 is a procedure by which the configuration is performed as part of the processing of a SafetyOpen.

There are two ways that a replacement device can be reconfigured from the originator and they are described as follows:

- Flow 6 is a procedure that duplicates the sequence of operations that would otherwise be done in flow 5;
- Flow 7 is a procedure by which the configuration is performed as part of the processing of a SafetyOpen.

8.9.4 User configuration guidelines

This Subclause 8.9.4 describes user configuration guidelines that assure a FSCP 2/1 safety system is properly configured and protected. These guidelines are used to define the safety manual requirements.

The user configuration data flows are defined in Figure 78.

a) The FSCP 2/1 safety system user shall assure that SNCT-configured-devices (2) are locked after verification.

   Devices that can be configured via the SNCT interface shall include a safety manual advisory that instructs the user to lock the device after verification has been completed.

b) The FSCP 2/1 safety system user shall assure that all originator-configured-devices (3) have ownership (7) assigned to the intended originator.

   Devices that can be configured by a Type 1 SafetyOpen shall include a safety manual advisory that instructs the user to verify that all originator-configured safety devices have their ownership assignments as part of the final verification process.

c) The user shall visually confirm (4) the sent configuration data and confirm it was downloaded correctly.

   All FSCP 2/1 safety devices shall include a safety manual advisory that instructs the user to visually verify that all configuration data was downloaded correctly.

d) The user shall functionally test their application.

e) The user shall assure the SCID (5) check by target and originator is done.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

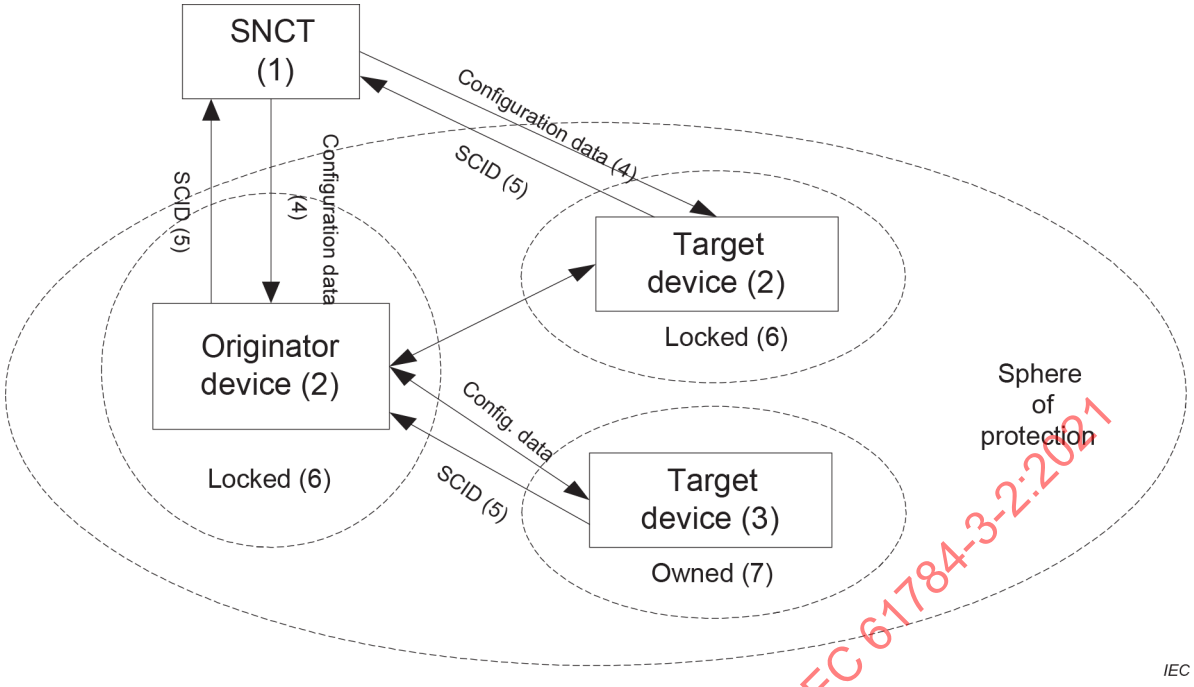


Figure 78 – Protection measures in safety devices

8.9.5 Configuration process justification

The FSCP 2/1 safety device being downloaded has safety measures defined which ensures integrity of data and data transfers as specified by IEC 61508 up to SIL3.

The SNCT on the other hand, will not be assessed due to the limitations of personal computer hardware, the operating system utilized, and the development tools. Because of these factors, the techniques employed to configure a safety device require that the safety device and user procedures, not the workstation software, enforce the protection measures.

SIL3 integrity is achieved by meeting the following requirements:

- A receiving safety device shall calculate a SCCRC with the device's targeted integrity level and SC3, and compare it to the SCCRC within the SCID;
- For Type 1 configured or tool configured devices, configuration validation of the downloaded safety-relevant data from the software (or originator) shall be performed with the device's targeted integrity level and SC3;
- When a safety device is configured directly from a workstation, the device safety manual shall instruct the user to compare the transferred SCID and configuration data with the SCID and configuration data originally viewed in the workstation;
- The SNCT software shall provide a facility to allow the user to confirm downloaded configurations are correct;
- Safety devices shall store/restore its configuration data with the device's targeted integrity level and SC3;
- Safety devices shall handle all device state transitions with the device's targeted integrity level and SC3.

Sub-systems that are required to be examined and certified:

- Target device configuration processing;
- Target device configuration storage;
- Target device configuration validation;

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

- Target device modes.

Sub-systems that are not required to be certified.

- Explicit messaging justification: The explicit messaging subsystem is simply a means of transferring the data, all integrity measures are performed by other system components and any errors such as corruption or loss of messages will be detected by the safety measures.
- Software user interface justification: The software interface is a means to display and enter data that will later be confirmed by other means. In itself, it does not require a conformity assessment, but it will be used in conjunction with a diverse read back and display mechanism to form a high integrity function.
- Software tool configuration storage justification: Any configuration data is stored with a safety related CRC that is verified to match the safety related CRC in the device. Any corruption of the data will be detected by the device with a CRC checking process consistent with the device's targeted integrity level and SC3.

8.9.6 Device functions for tool configuration

The process by which the SNCT interacts with originators and targets are controlled by facilities defined in the Safety Supervisor object. Features such as Password protection and the Configuration Lock attribute combine to provide security for this interface. Since the Safety Supervisor is provided in the baseline profile (see 6.5.3) for both safety targets and originators, the interface details are common. Subclauses 8.9.7 to 8.9.12 will define these features and how they are used by the SNCT.

8.9.7 Password security

The SNCT interface defines the following functions to optionally provide password security:

- Password functionality added.

  Support for one password shall be implemented by devices supporting the SNCT interface.

  Passwords submitted to devices supporting the SNCT interface shall be values obtained from running the encryption algorithm defined in 7.1.2.3.

  The default password value in devices supporting the SNCT interface shall be zero.

  Software shall transparently insert "zero" in all services which require one until a user sets it to something different.
- The SNCT interface shall support a Password service to set passwords which takes 2-password parameters; Old PW and New PW.
- The SNCT interface shall provide a Reset Password service which takes a vendor specific field to reset the password.

  Each vendor shall choose a method to reset passwords and instruct the user what to fill in to cause the device to reset the password. The software shall only insert whatever value the user enters into the reset field (see the Reset_Password service in the Safety Supervisor object definition in 6.5.3).

  The safety supervisor commands that have a password parameter define the processing requirements and error responses for these parameters.

8.9.8 SNCT interface services

The SNCT shall provide the following services.

- The SNCT interface shall provide a Configure Request service which requires password, TUNID, and OUNID to execute.
- In the SNCT interface, an unowned device shall capture the OUNID as the device owner when the first Configure_Request is received.
- The SNCT interface shall provide a Validate Configuration service which requires the SCID, SCCRC, and the SCTS to execute.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

- The SNCT interface shall provide an Apply service that causes the device to save the configuration to NV memory.
- The SNCT interface shall provide a special Reset service which requires the password and TUNID to execute and supports the 2 common Reset types along with one that can reset to the default but preserve the password.
- The SNCT interface defines an optional a Mode Change service which, if implemented, shall require a password to execute.

8.9.9 Configuration lock

The SNCT interface defines the following functions for Configuration Lock. Its intent is to provide a way for the user to flag that a tool-generated configuration has been tested and verified as valid. From that point, the signature (SCID) reflects a verified configuration. The configuration lock has the following characteristics.

- The SNCT interface shall provide a Configuration Lock service which requires the password and TUNID to execute.
- The SNCT Configuration Lock Attribute shall have a default value of "Unlocked".
- Safety devices which support the SNCT interface shall require that the "Configuration Lock" attribute be cleared before any command to change a safety device to the Configure State (Configure_Request) will be accepted.
- The Configuration Lock has two purposes:
  - Serves to indicate that the user has tested and confirmed the Tool-based configuration in this device is correct.
  - "Tool Only" mode requirement. When the Configuration Lock attribute is set, the device shall reject any Type 1 SafetyOpen messages.

These two features make it clear that for the SNCT to configure any safety node, it shall support features to set and clear the Configuration Lock attribute, and shall present the proper password to do so. These features are illustrated in the sequence diagram defined in Figure 81.

8.9.10 Effect of configuration lock on device behavior

Figure 79 defines the effect that the "configuration locked" condition has on the ability of a device to be configured; there are requirements defined in the Safety Supervisor object that cause safety devices to reject all attempts to change a locked configuration.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

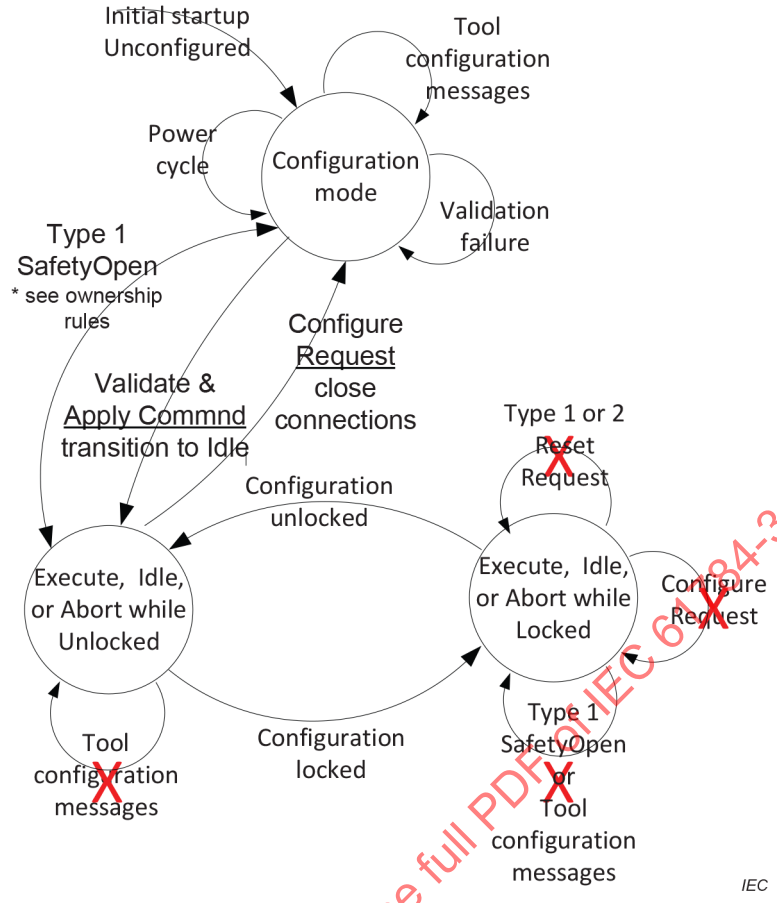


Figure 79 – Configuration, testing and locked relationships

Table 110 defines the effect that ownership has on a device's ability to be configured. It shows that owned devices can only be Type 1 configured by the originator that has the owner UNID. A locked device can never be configured regardless.

Table 110 – Configuration owner control vs. device state

Ownership rules	Configure mode	Execute/Idle Mode Unlocked	Execute/Idle Mode Locked
Configuration Un-owned	Tool configuration or Type 1 acceptance by anyone	Tool configuration or Type 1 acceptance by anyone	No Tool configuration, No Type 1 accepted
Originator Owned	Tool configuration or Type 1 by owner only	No Tool configuration (shall reset first) or Type 1 by owner only	No Tool configuration, No Type 1 accepted
Software Tool Owned	Tool configuration only No Type 1 accepted	Tool configuration only No Type 1 accepted	No Tool configuration, No Type 1 accepted

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

8.9.11 Configuration ownership

The SNCT interface defines functionality for handling the configuration owner identifier for a device. This function has been defined to allow a device to provide exclusive configuration rights to a particular configuration source. The source could also be assigned exclusively to a configuration tool. The following functions are provided:

- Configuration UNID attribute

  The default is to allow any device to be an owner.

  Devices are required to capture the first configuration source as the owner.

  Attributes and services in the Safety Supervisor are defined which allow Tools to be the exclusive configuration source.

- Even though an owner has been assigned as a configuration source, the SNCT tool has the ability to override a configuration. The SNCT shall provide protection measures to assure the user cannot perform an override without warnings and the proper password.

8.9.12 Configuration mode

All safety devices shall support a non-volatile configuration mode; this means that once a device is commanded to enter the configuration mode it shall remain in the configuration mode until the configuration is successfully validated.

8.9.13 Measures used to ensure integrity of configuration process

8.9.13.1 Safety Configuration Identifier (SCID)

In safety systems it is necessary to clearly identify the configuration. The identification is used during several operations:

Download from tools – This gives the user the ability to check that the tool and device agree on the information downloaded.

Device Replacement – If the tool is used for device replacement, the user has the ability to verify that the configuration is the correct one to download. If the originator is used to automatically reconfigure a device, the SCID is used to indicate that a reconfiguration is necessary and ensure the integrity of the operation.

Connection Establishment – The originator and target use the SCID to ensure that both devices are using the same configuration.

The SCID is a concatenation of the SCTS and the SCCRC described in 8.9.13.3 and 8.9.13.4 respectively.

8.9.13.2 Originator and Target SCID coverage

When originators are used to configure targets, Figure 80 illustrates how the SCIDs provide coverage of the various configurations. The SCID for targets that are configured by originators are not calculated in the originators, the calculation is performed in the workstation. The target configurations are protected by their respective SCIDs.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

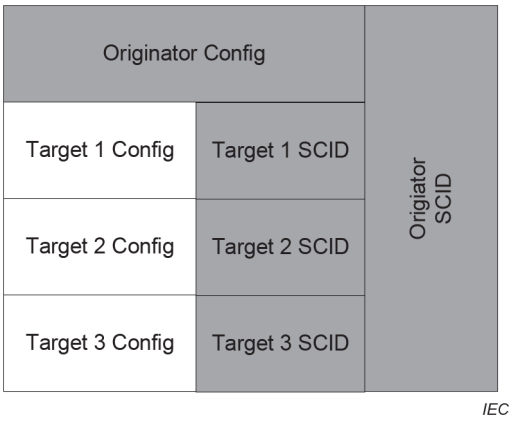


Figure 80 – Originator's configuration data

8.9.13.3 Safety Configuration CRC (SCCRC)

This is a CRC that covers the device configuration data that is contained in a SafetyOpen. It is part of the SCID for the device. The SCCRC is described in 8.2.

The safety function of the SCCRC is used to ensure the correctness of the safety-related application data.

8.9.13.4 Safety Configuration Timestamp (SCTS)

The Safety Configuration Time Stamp is a safety related signature that identifies the revision of the device configuration contained in either a SafetyOpen or in a safety device. It is part of the SCID for the device configuration.

The safety function of the SCTS is to ensure the uniqueness of the safety-related application data.

8.9.13.5 System-wide unique "Safety Network Number" (SNN)

The Safety Network Number uniquely identifies a network across all networks in the safety system. The end user is responsible for assigning a unique number to each safety network or safety sub-net within a system. This number shall be defined during node commissioning (i.e. set via the Propose_TUNID/Apply_TUNID process defined in 6.6.5.20 if the SNCT Interface is supported).

8.9.13.6 System-wide "Unique Node Identifier" (UNID)

Uniquely identifies a node across all networks in the safety system. This value is made up of the Safety Network Number (SNN) and the Node Address of the device. This value is a structure consisting of the 6 octet SNN and the 4 octet Node Address. The 4 octet node address is sized to accommodate all forms of CPF 2 network addresses.

```
struct UNID
{
DATE_AND_TIME    SNN;
UDINT      NodeID;
};
```

NodeIDs smaller than 4 octets (i.e. CP 2/3) shall be aligned to the least significant octet in little endian order. The unused octets shall be zero filled.

The safety function of the UNID is to uniquely identify originators and/or targets during the connection establishment process.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Other uses of UNID:

- TUNID = Target's Unique Network Identifier. The safety function of the TUNID is to dentify the target in the SafetyOpen and Configuration mode message.
- OUNID = Originator's Unique Network Identifier. The safety function of the OUNID is to identify the originator in the SafetyOpen.
- OCPUNID = Output Connection Point Owning UNID. The safety function of the OCPUNID is to identify the owner of the output connection in the target. Set to the OUNID of the originator in the SafetyOpen that obtains ownership of the output connection point. Used to prevent an unauthorized originator to obtain ownership of an output connection point.
- CFUNID = Configuration Owning UNID. The safety function of the CFUNID is to identify the owner of the safety configuration in the target, this should be equal to the OUNID in normal operation. This is set to the OUNID of the originator in the SafetyOpen that includes configuration data and is used to prevent an unauthorized originator from modifying the configuration.

8.9.13.7 Connection Parameters CRC (CPCRC)

The Connection Parameter CRC is a safety related CRC covering the CPF 2 connection establishment data in the SafetyOpen. This CRC will also cover the additional parameters required by the safety protocol. The CRC is defined in 7.1.2.3.

The safety fuction of the CPCRC is to ensure the integrity of the connection data contained within the SafetyOpen.

8.9.14 Download process

8.9.14.1 Overview

The safety download process ensures that the configuration data is transferred with high integrity from the SNCT or the Originator to the device being configured. At the successful completion of the download process the configuration is considered valid. There are two download processes used with safety devices:

- SNCT downloads to originators and targets;
- Originator downloads to targets using a Type 1 SafetyOpen.

The following subclauses will describe the details of the processes that are used for the download of safety devices.

8.9.14.2 SNCT download to originators and targets

Figure 81 shows the process of downloading a safety device from the SNCT. The download process between the SNCT and the Configured Device assures that the data is instantiated in the Configured Device's memory with high integrity.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

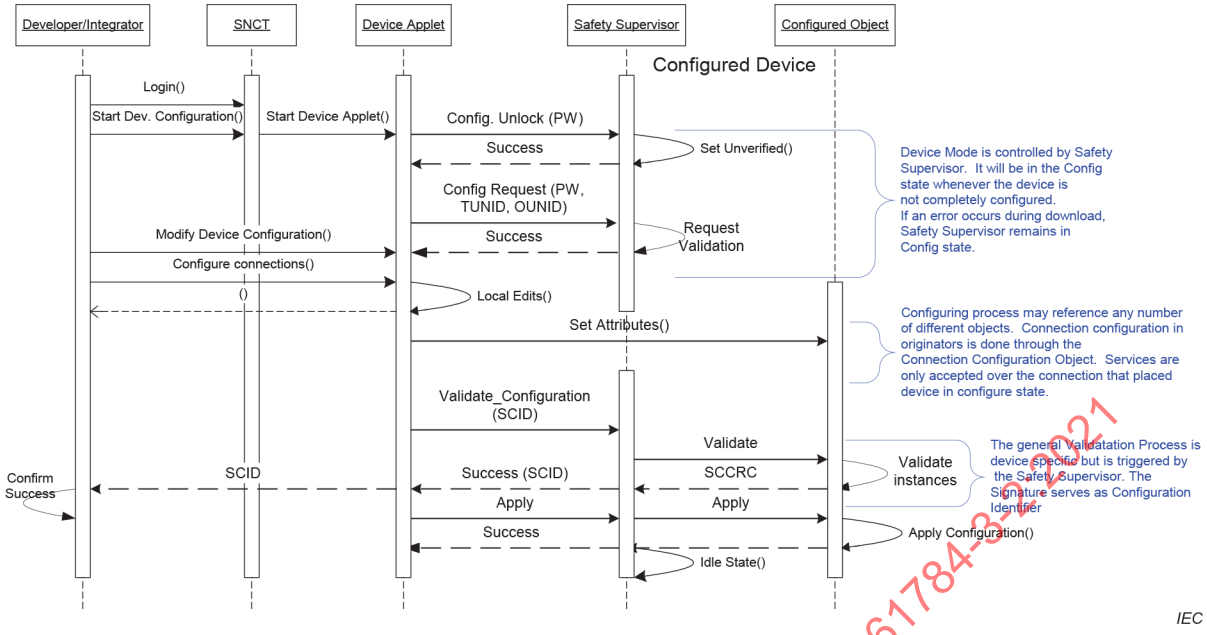


Figure 81 – SNCT to device download process

8.9.14.3 SNCT to device download process steps

The following are the process steps for the SNCT to device download process as shown in Figure 81.

a) Clear Configuration Lock Attribute
   i) Device: Configuration Lock Attribute cleared
b) Enter configuration state with password, TUNID, OUNID
   i) Device: No safety I/O connections can be active.
   ii) Device: Device saves Config mode to NV storage
      A) Until "Validate" and "Apply", power cycles go back to config mode
c) Transfer of configuration data
   i) Tool: Calculate "proposed SCCRC" for data (SCCRC part of SCID)
d) Validate configuration data
   i) Tool: Send Validate_Request with SCID (which contains proposed SCCRC)
   ii) Device: Analyze configuration data
   iii) Device: Calculates SCCRC value and compares to "proposed SCCRC"
   iv) Device: send SCID in Validate_Reply
   v) Tool: Compares returned SCCRC to "proposed SCCRC"
e) Apply Configuration
   i) Device: Save configuration to NV storage with SCID
   ii) Device: Mark configuration as valid
   iii) Device: Set mode to Idle
   iv) Tool: Capture and store the SCID with the configuration file.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

8.9.14.4 SNCT downloads to originators which do Type 1 target configuration

Figure 82 shows the process by which Originators are initially configured and how the Type 1 SafetyOpen is used to download Target devices. Once the user finishes defining the Originator and Target configurations in the SNCT, it is sent to the Originator. At this point the originator SCID can be confirmed by the user. This process ensures that the configuration data in the SNCT and originator match with a high degree of integrity.

Then the user shall place the Originator into execute mode to get the Target devices downloaded. If the connection is successful, the Target configuration/SCID was accepted by the target and confirmed by the originator. This action also established the Originator as the Target's owner and prevents the Target from being downloaded by any other device except the SNCT.

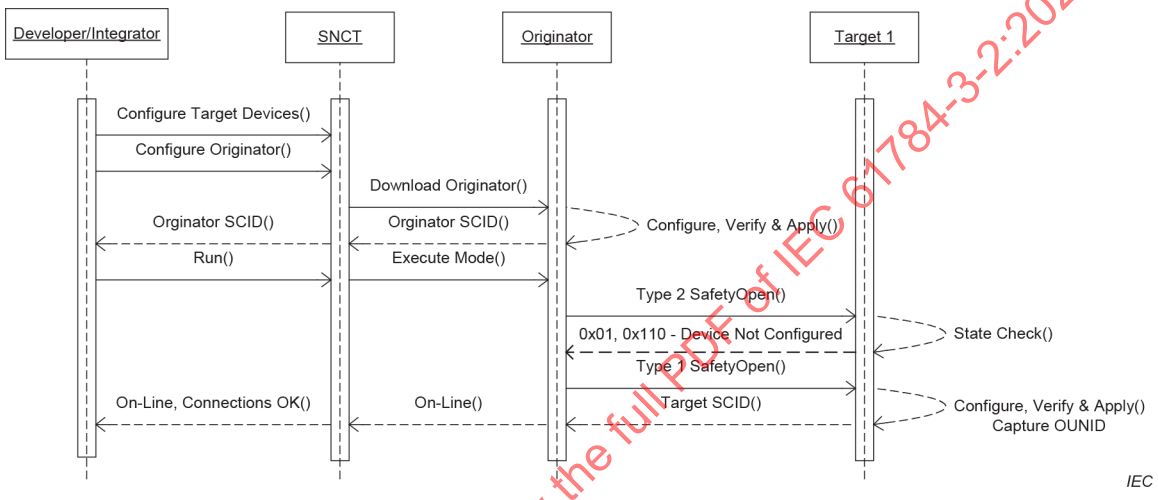


Figure 82 – SNCT Downloads to originators that perform Type 1 configuration

8.9.14.5 SNCT downloads to originators that perform Type 1 configuration

The following are the process steps for SNCT Downloads to originators that perform Type 1 configuration as shown in Figure 82.

a) Clear Configuration Lock Attribute on originator
   i) Device: Configuration Lock Attribute cleared
b) Enter configuration state with password, TUNID, OUNID
   i) Device: No safety I/O connections can be active
   ii) Device: Device saves "Configuring" mode to NV storage
   iii) Until "Validate" and "Apply", power cycles go back to "Configuring" mode
c) Transfer of configuration data
   i) Tool: Calculate "proposed SCCRC" for data (SCCRC part of SCID)
d) Validate configuration data
   i) Tool: Send Validate _Request with SCID (which contains proposed SCCRC)
   ii) Device: Analyze configuration data
   iii) Device: Calculates SCCRC value and compares to "proposed SCCRC"
   iv) Device: send SCID in Validate_Reply
   v) Tool: Compares returned SCCRC to "proposed SCCRC"

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

e) Apply Configuration
   i) Device: Save configuration to NV storage with SCID
   ii) Device: Mark configuration as valid
   iii) Device: Set mode to Idle
   iv) Tool: Capture and store the SCID with the configuration file.

f) Set Mode to Run
   i) Originator: Sends Type 2 SafetyOpens (see 8.8.5)
   ii) Target returns one of the following errors:
      A) Unconfigured: 01_{hex}, 0110_{hex} – Device Not Configured
      B) Prior configuration: 01_{hex}, $80C_{hex}$ – SCID Mismatch error
   iii) Originator: Sends Type 1 SafetyOpen
   iv) Targets: Verify and Apply the configuration data
   v) Targets: Return target SCID# to originators
   vi) Originator: Compare sent and received SCID#'s
   vii) Originator: Return On-Line status to SNCT

8.9.15 Verification process

8.9.15.1 Verification process overview

The verification process uses the data that was transferred during any of the download processes to allow the user to correctly verify that the downloaded data is correct, the system operation is correct and the system is ready for operation up to the targeted SIL rating. There are three main parts to the configuration process:

- Configuration Data Verification;
- Functional testing;
- Configuration Locking.

Key requirements for the safety manual:

- The device Safety Manual shall contain an advisory that user testing is the means by which all downloads are validated.
- The device Safety Manual shall contain an advisory that the signature should only be considered "verified" (and configuration locked) after user testing.

The device User manual shall contain an advisory that configuring an originator with connection data and/or target configuration data shall be downloaded to the target so it can be tested and verified. Only then can SCIDs from the target be confirmed.

As shown in Figure 83, when originators are tool-configured and targets are originator configured, only the originator is "locked" after verification and testing. The target in this case uses ownership assignments for protection. Also shown in Figure 83 is that Targets can also be tool-configured as well. In this case, these targets are also "locked" after verification and testing.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

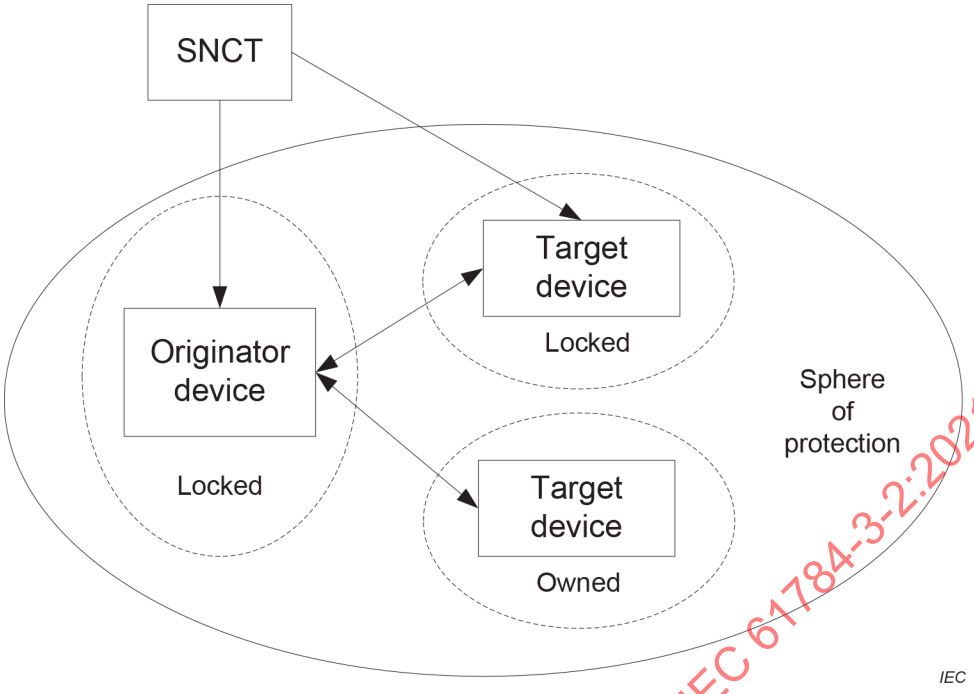


Figure 83 – Protection from locking and ownership

8.9.15.2 User configuration verification and alternatives

8.9.15.2.1 Overview

The user needs to visually verify that the downloaded configuration is correct and is the intended configuration for the device. This Subclause 8.9.15.2 presents three alternatives that will fulfill the requirements for user verification of the device configuration data. In all cases the user needs to verify the functionality of the devices being configured through some kind of functional testing.

- Alternative 1 – Immediate Read Back and Diverse Comparison
- Alternative 2 – Download and Verify, then Diverse Comparison
- Alternative 3 – Download and Test, then Diverse Comparison

8.9.15.2.2 Alternative 1 – immediate read back and diverse comparison

The device configuration data is read back by the work station immediately after download and presented to the user utilizing a diverse execution path in the workstation.

After a device receives its configuration, the data is read back and the User makes a comparison of the original software display, and the results of the read back. The data read back shall be displayed by a diverse means.

For example, reading back the entire configuration, comparing it to what the software has and providing a printout of the device configuration for the user to compare with what was previously entered.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

8.9.15.2.3 Alternative 2 download and verify, then diverse comparison

It is possible to achieve the same level of integrity at defined in 8.9.15.2.2 since it can be shown that the configuration data on the workstation storage is identical to the configuration data in the device. The verification of configuration data is accomplished by:

a) Writing the configuration data and CRC to the local drive in the workstation. The configuration data and CRC from the local drive are then sent to the device.

b) The device then verifies the correct transfer by comparing the data and CRC.

c) If the transfer to the device is correct, the device sends its calculated CRC back to the workstation to confirm that the data was sent correctly.

d) At that point the workstation compares the device CRC to the stored CRC (from step a).

e) For verification, the user shall view the "sent" configuration data using a diverse means to confirm that the correct configuration was sent to the device. Since the data on the workstation storage includes a CRC, a diverse means of display will allow the user to uncover any errors caused by the workstation when the data was entered into storage. This effectively duplicates the functionality of the full read back method without the overhead of doing a full data read back from the device to the workstation.

8.9.15.2.4 Alternative 3 – Download and test, then diverse comparison

In this method, the read back verification is delayed until all the configuration is downloaded and tested.

a) Initially the configuration of the devices in the system are unverified. The devices are configured and provided with the CRC which the devices use to verify the data. The user verification of the uploaded data is not done at this time.

b) Once the entire system is functionally tested by the user, the entire system will be verified by the software tool on the workstation. The verification step shall read back all of the configuration data from all of the devices, compare the read back data to the local drive copy, and present it to the user in a diverse manner for user examination. This read back of data shall be performed in the manner described in 6.6 but shall be performed for all devices in the system at the same time.

This method has the advantage of allowing the user to complete the onerous visual comparison once, with the final tested system.

8.9.15.3 Verification process

Figure 84 defines the complete process for verifying the configuration of safety devices. It is assumed that the data has be downloaded using the process described in 8.9.14, ensuring that the SNCT and the device have the same configuration data. One alternative shall be selected for the user verification of the configuration data. Upon completion of this process the devices and system are ready for operation up to the targeted SIL rating.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

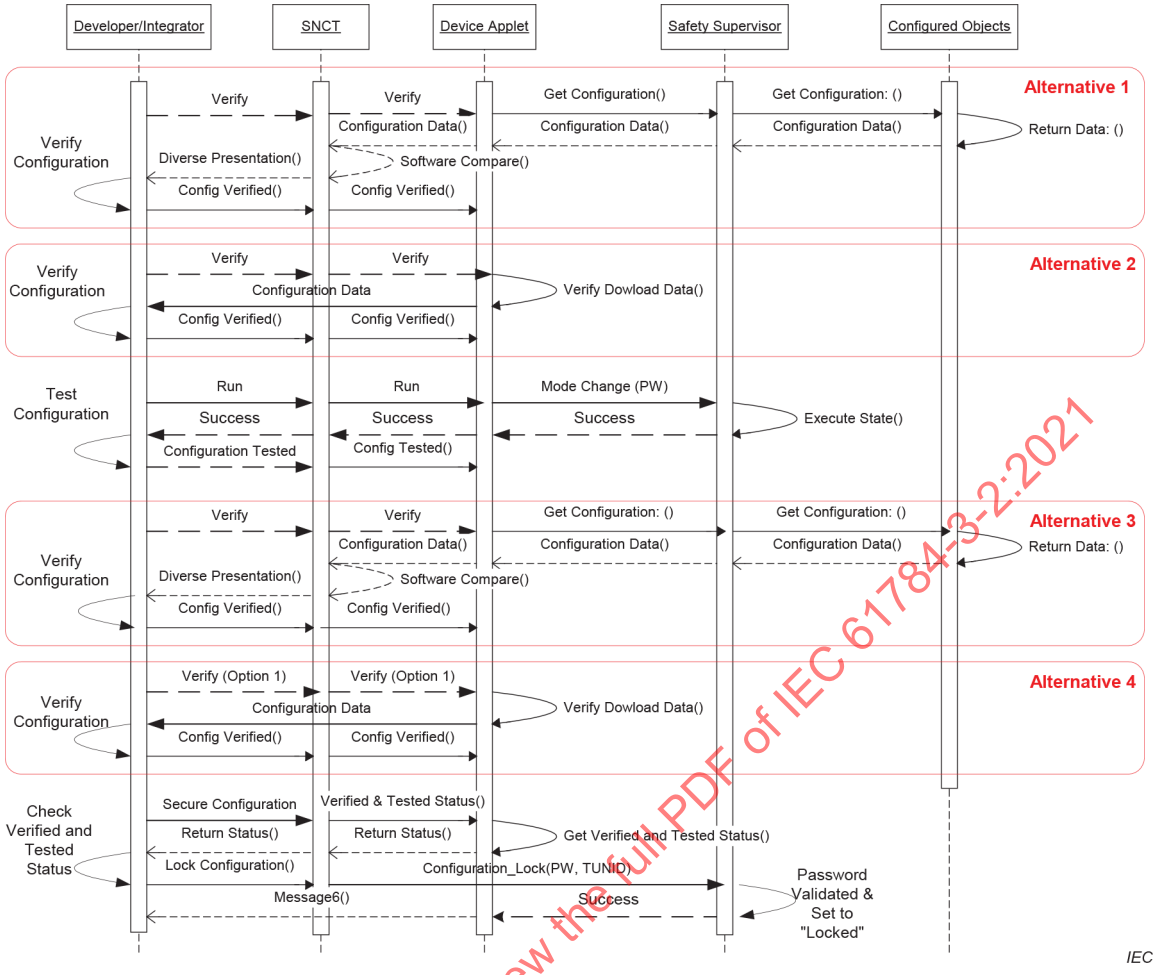


Figure 84 – Verification process including all alternatives

8.9.16 Configuration error analysis

8.9.16.1 Configuration errors and detection measures relationships

Table 111 defines the errors and detection measures that are considered for the download and configuration process defined by the SNCT interface.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Table 111 – Errors and detection measures

Errors	Detection measures							
	User Authentication [a]	Identification of configuration	Identification of target	SCCRC protection on configuration (Part of SCID)	Configuration Locking or Device Ownership	Configuration session control	User Functional Testing	Read back of the device configuration
User misdirected configuration	X				X		X	
System misrouted configuration	X		X		X		X	X
Lost Configuration Message				X			X	X
Corrupted configuration				X			X	X
Configuration at inappropriate time						X		
User loads wrong configuration		X					X	X
Configuration process is interrupted						X		

[a] User Authentication is an optional feature and only applies if the feature is used by the end user.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

8.9.16.2 Configuration errors

8.9.16.2.1 User misdirects configuration

The user is required to functionally test devices that are configured so user misdirection can be discovered during testing.

If the user configures a node unintentionally and it is not noticed, the originator connecting to the node will not have the matching signature and will either reconfigure the device with the correct signature or reject the connection. Either of these two actions will result in the system going to a safety state.

If the end user enables authentication features, users cannot configure nodes for which they do not have authorization. User authentication is an optional feature.

8.9.16.2.2 System misroutes configuration

There are two different cases for a system to misroute a configuration: configuration preformed during connection establishment by a Type 1 SafetyOpen, and configuration from a workstation or O-to-T configuration process. Both of these cases are explained in the following paragraphs.

- If a routing error occurs during the establishment of a configuration session the configuration mode message will be rejected by the device because of the wrong TUNID or OUNID in the mode message.

- If a configuration message is misrouted within a configuration session, it will be rejected by the receiving device if the device is not in the correct mode or is received on a connection other than the connection used to establish the configuration mode. If the device is in the correct mode the configuration message would have to be addressed to the correct class, instance, attribute to be accepted and would be discovered during the SCID validation steps. The device that was supposed to correctly receive the configuration message will also fail the SCID validation. The user will also discover this during the check of the configuration read back from the device.

8.9.16.2.3 Lost configuration message

The detections for a lost message are the same as those for a misrouted message.

8.9.16.2.4 The configuration is corrupted

If for any reason the configuration is corrupted, it will be detected by the SCID checks, the user functional testing, and the user configuration examination.

8.9.16.2.5 Configuration at an inappropriate time

Configuration of operating devices is prevented by the user authentication and setting of the configuration mode. If a user attempts to configure a device that the user is not authorized for the mode request will be rejected. If the user sends configuration messages to a device without the configuration mode set the device will reject the changes.

8.9.16.2.6 User loads the wrong configuration

Each configuration is uniquely identified by the SCID. Users are required to implement procedures to verify that the configuration being loaded is the correct one for the application.

8.9.16.2.7 Configuration process is interrupted

If the configuration process is interrupted for any reason the device will remain in the configuration mode until a valid configuration is loaded and the mode is changed.

When the configuration process is interrupted the process will need to be restarted on a new connection with a new configuration request.

8.9.16.3 Detection measures

8.9.16.3.1 User authentication

All safety devices have optional password protection. The Configuration Lock, Configuration Request, Mode Change, and Reset commands all require the use of a password to change the state.

8.9.16.3.2 Identification of configuration file

All safety configuration files are uniquely identified by the SCID.

8.9.16.3.3 Identification of target to be configured

The configuration mode message and the verify message both use the TUNID for identification of the target.

8.9.16.3.4 CRC protection on configuration

Part of the SCID is the SCCRC. The SCCRC is 32 bit CRC that is calculated over the safety configuration data.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

8.9.16.3.5 Configuration ownership

When an out-of-box target device is configured by an originator, the device captures the OUNID and subsequently prevents any other originator from configuring the device. Thus the ownership assignment (OUNID) provides a means of locking this device to a single configuration source.

8.9.16.3.6 Configuration session control

Prior to configuring a device it shall be placed into a configuration mode. The configuration mode is persistent in the device and remains in place until the device is set to another mode by a command. The configuration mode in safety devices implementing the SNCT interface shall persist through power cycles.

Upon entering the configuration mode, devices implementing the SNCT interface shall:

- Store the configuration mode in NV;
- Mark the existing configuration invalid;
- Lock out all configuration messages for connections other that the one that set the configuration mode;

To enter the configuration mode, devices implementing the SNCT interface shall:

- confirm User Password in the configuration mode command;
- confirm TUNID in the configuration mode command.

8.9.16.3.7 User functional testing

The user is required to functionally test new and replacement devices prior to utilizing the devices in a safety system (up to SIL3).

8.9.16.3.8 Configuration protection

After configuration, testing, and user verification has been completed by one of the procedures defined in 8.9.15.3, all tool-configured devices are locked. These are Targets, Originators, or both. This locked state can be read to provide an indication that the configuration has been verified and also guards against inadvertent configuration changes by requiring the user to first unlock the device.

As a result of user testing, originator-configured target devices have ownership assignments which binds these devices to their owners; effectively locking these devices from being inadvertently configured by some other source. As shown in Figure 83, the combination of locked tool-configured originators and owned targets provides a secure environment to protect the verified system from unauthorized changes.

8.9.16.3.9 Diagnostic software protections (not safety related)

The software may also implement data protection measures of the device configuration data as a data integrity measure and for the early error detection mechanism. It is important to understand that these measures are not safety related and therefore do not need to achieve any SIL level or be certified. These areas are defined here:

Storage of Configuration Data to Hard Disk, CD, etc shall include the SCID and be checked during a file load operation.

The transfer of Configuration Data across software interfaces shall include the SCID and be checked by the receiving software component.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

8.9.16.4 Device memory architecture considerations

It is important to understand the memory architecture that target devices could use to know how it could behave during configuration. All these architectures are supported by this document but will change the behavior for the user.

There are 3 distinct data areas defined with respect to configuration:

- NV stored copy – this is a valid configuration stored in Non-volatile memory and is what is used to set up a safety device on power-up;
- Working RAM copy – This is a valid configuration that is an exact copy of the configuration in NV memory, but is what is used during run-time operation;
- Editable RAM Copy – This is a data space that can be modified by software in the configuration mode, but has yet to be applied;

Product developers may choose to implement one or more of these data areas to increase user flexibility.

NV Copy Only – This design approach keeps configuration only in NV memory. When the configuration mode is entered, the entire configuration is invalidated and there is no possibility to restore the configuration. The software shall successfully download a complete and valid configuration to the device. Once it is validated and applied the NV copy is marked as good. The restore command is not supported in this type of device.

NV and Working Copy – This design approach keeps configuration in NV memory and a working copy in RAM. When the device enters the configuration state, the working copy is modified, but until the configuration is validated and applied, the old valid configuration is still available to be restored. A power cycle before the Apply would revert to the last configuration in NV memory. The restore command is supported and would re-copy the NV version into working RAM.

NV and Working Copy with Edit buffers – This design approach keeps a valid working configuration at all times until a "validate and apply" is done. If the configuring device quits without applying the changes, the restore command would allow the device to simply exit the configure state and run with what is in memory. The restore command is supported, but no copy from NV RAM is needed, the working copy can be used.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

8.10 Electronic Data Sheets extensions for safety

8.10.1 General rules for EDS based safety devices

8.10.1.1 General

The structure and rules for EDS are defined in ISO 15745-3:2003, Annex A and ISO 15745-4:2003, Annex C. The extensions for safety are defined in the following subclauses.

8.10.1.2 Safety configuration assembly definition

Safety devices can be configured from an EDS file definition. Safety devices that are configured via EDS file shall define a Configuration Assembly so that the software knows how to calculate the SCID. A standard EDS assembly section shall be used to define the various parameters contained in the Safety Configuration Assembly. A field and keyword has been defined in the [Parameter Class] section to identify the instance Id of the assembly. A connection manager entry shall also be used to reference this assembly if it is to be configurable with a Type 1 SafetyOpen.

8.10.1.3 Configuration CRC

The SNCT and EDS based safety device shall use the same method for calculating the SCCRC. EDS based safety devices shall use CRC-S4 with the seed value defined in 7.1.2.3. The data

input to the CRC algorithm is defined by the Configuration Assembly. Any padding in the configuration assembly will be assumed to be zero for purposes of calculating the SCCRC.

8.10.1.4 Password encryption for EDS devices

The SNCT and any other configuration software implementing the SNCT interface shall have a standardized method for encrypting passwords prior to presenting them to a safety device. Software tools implementing the SNCT interface shall use CRC-S4 with the seed value defined in 7.1.2.3.

When an encrypted password is smaller than the fixed-size password parameter, the method described under the Set_Password service in the Safety Supervisor object definition shall be used.

8.10.2 EDS extensions for safety

8.10.2.1 Additional Object Class sections

Table 112 identifies section keywords that are used to publicize Safety object class information. Each of the following EDS Section Keywords may contain any of the Common Object Class Entry Keyword(s) described in CPF 2. The following table contains Safety object class section names.

Table 112 – Object Class section keywords

CIP object	Class code	Section keyword name	Required/ Optional
Safety Supervisor object	39_{hex}	[Safety Supervisor Class]	Optional
Safety Validator object	$3A_{hex}$	[Safety Validator Class]	Optional
Safety Discrete Output Point object	$3B_{hex}$	[Safety Discrete Output Point Class]	Optional
Safety Discrete Output Group object	$3C_{hex}$	[Safety Discrete Output Group Class]	Optional
Safety Discrete Input Point object	$3D_{hex}$	[Safety Discrete Input Point Class]	Optional
Safety Discrete Input Group object	$3E_{hex}$	[Safety Discrete Input Group Class]	Optional
Safety Dual Channel Output object	$3F_{hex}$	[Safety Discrete Output Group Class]	Optional
Safety Analog Input Point object	49_{hex}	[Safety Analog Input Point Class]	Optional
Safety Analog Input Group object	$4A_{hex}$	[Safety Analog Input Group Class]	Optional
Safety Dual Channel Analog Input object	$4B_{hex}$	[Safety Dual Channel Analog Input Class]	Optional
SERCOS III Link object	$4C_{hex}$	[SERCOS III Link Class]	Optional

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

8.10.2.2 Extension to [File] section for safety

EDS Files for safety device shall be protected by a CRC. CRC-S4 with the seed value defined in 7.1.2.3 shall be used.

The EDS File CRC value shall be entered in the [file] section with the entry keyword "EDSFileCRC=". The EDSFileCRC entry keyword shall be contained on a single line.

The SNCT shall confirm the EDS file CRC prior to using the file contents as described below:

a) Open file as a binary file. Load the entire file into memory;

b) Remove the entire line including the carriage return that has the EDSFileCRC= entry;

c) Calculate the CRC over the remaining contents of the file;

d) Compare the calculated CRC to the EDSFileCRC= entry's value.

An "EDSFileCRC=" keyword and value shall be included in all safety device EDS files. If the [Device Classification] entry describes the device as having any Safety capabilities and the EDSFileCRC= entry keyword does not exist, then the SNCT shall not use the file.

8.10.2.3 Extension to [Device Classification] section for safety

The EDS file for safety devices shall include a [Device Classification] section which shall contain the line:

Classx = Safety;

where

x is a decimal value.

The Classx keyword, with the Classification field equal to Safety, is defined in Table 113.

Table 113 – Safety Classx entry format

Entry name	Field number	Data Type	Required/Optional
Classification	1	Field keyword	Required
Reserved	2,3	empty	
Port Instance	4,5,...n	UINT	Conditional[a]
[a] Required if the device supports more than 1 CIP port			

Classification shall be the value Safety.

The Port Instance fields are the Port Object instances that support safety.

8.10.2.4 Extension to [ParamClass] section for Safety

The SafetyCfgAssemby Keyword shall be used in the safety devices to identify the configuration assembly object instance. The keyword is defined in Table 114.

Table 114 – Parameter class keywords

Entry name	Entry keyword	Field number	Data Type	Required/Optional
Safety Assembly Instance	SafetyCfgAssembly	1	UINT	Conditional[a]
[a] Shall be in implementation for safety devices that are configured via EDS file				

SafetyCfgAssembly – Identifies the configuration assembly object instance number for safety-related parameters in this device.

A "SafetyCfgAssemby=" keyword entry shall be included for safety devices that are configured via EDS file. This value shall also match an AssemN entry keyword specified in the [Assembly] section.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

8.10.2.5 Extension to [Connection Manager] section for safety

8.10.2.5.1 General

There are four new keywords defined for safety that are described in this Subclause 8.10.2.5. The new keywords are summarized in Table 115.

Table 115 – New Connection Manager section keywords for safety

Entry name	Entry keyword	Field number	Data type	Required/Optional
Maximum Safety Connections	MaxSafetyConnections	1	USINT	Optional
Maximum Safety Input Connections	MaxSafetyInputCnxns	1	USINT	Optional
Maximum Safety Output Connections	MaxSafetyOutputCnxns	1	USINT	Optional
Default Safety Connections				
	Connection Instance 1	1	UINT	Required
	Connection Instance n	n	UINT	Conditional
Safety Format Support	SafetyFormat	1	USINT	Conditional[a]
[a] Required if the device supports the extended format, otherwise optional				

8.10.2.5.2 Max safety connections

Safety devices will typically support a large number of possible assemblies that mix and match different combinations of I/O data and/or status. At the same time, these devices have a limit on how many safety I/O connections can be established at any one time. These keywords in the [Connection Manager] section define these limits. If no entry exists in the EDS file, no limits exist.

8.10.2.5.3 Default safety connections

There will often be a set of connections that are most commonly used. Product developers can optionally define a default set of connections that allow the user to quickly and easily add these connections to an originator configuration. The DefaultSafetyConnections entry keyword specifies which connection manager entries are these "default" connections.

8.10.2.5.4 Safety Format Support

A device which supports the Extended Format shall declare that support by entering this keyword in the Connection Manager section of the device's EDS file. By making this declaration, connection configuration software algorithms can be enabled to configure a new format type attribute in the Connection Configuration object. When this keyword is not present in an EDS file, it will be assumed only the Base Format is supported (equivalent to SafetyFormat = BaseOnly). The possible options are:

- SafetyFormat = 1; supports Base Format only;
- SafetyFormat = 2; supports Extended Format only;
- SafetyFormat = 3; supports both base and Extended Format.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

8.10.2.5.5 Changes and additions to Connection Manager fields

8.10.2.5.5.1 Overview of changes and additions

Connection manager entry shall be defined for each safety component to which a connection can be established. The safety connections are defined using the existing Connection Manager section defined in ISO 15745-2:2003, Annex A with the following extensions. The SNCT shall use each entry to present the user with a set of connection options that can be connected to from an originator.

Table 116 lists the fields currently defined for the Connection Manager section.

Table 116 – Connection Manager field usage for safety

Field name	Field number	Data type	Usage for safety
Trigger and transport	1	DWORD	Class: shall be 0 Trigger: shall be application Transport Application type: all 0 producers shall be Input Only consumers shall be Exclusive Owner EXAMPLE producers (clients): 02040001_{hex} consumers (server): 84040001_{hex}
Connection parameters	2	DWORD	O-to-T size: shall only be fixed T-to-O size: shall only be fixed Octets per slot: always ignored Real Time Transfer format: 5 = Safety Priority: High or Scheduled Connection Type: Inputs: T-to-O Multipoint or Point-to-point O-to-T Point-to-point Outputs: O-to-T and T-to-O Point-to-Point EXAMPLE Multipoint Input (producer): 22645505_{hex} Point-to-point Output (consumer): 22445505_{hex}
O-to-T RPI	3	Param	Either leave blank or provide Param reference to define device capability
O-to-T size	4	UINT or Param	IF blank, will either assign the size from the associated ASSEM reference or the software will use the Time Coordination size
O-to-T format	5	Assem	For Safety output connections, this field shall indicate the Safety output assembly to which the connection is associated. For safety input connections, this field shall be empty
T-to-O RPI	6	Param	Either leave blank or provide Param reference to define device capability
T-to-O size	7	UINT or Param	If blank, will either assign the size from the ASSEM reference or the software will use the Time Coordination size
T-to-O format	8	Assem	For Safety input connections, this field shall indicate the Safety input assembly to which the connection is associated. For safety output connections, this field shall be empty

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Field name	Field number	Data type	Usage for safety
config #1 size	9	UINT or Param	Can optionally be used
config #1 format	10	Param or Assem	Can optionally be used
config #2 size	11	UINT or Param	Size of configuration assembly when device supports configuration via Type 1 SafetyOpen
config #2 format	12	Param or Assem	This field can indicate which assembly will hold the Type 1 SafetyOpen configuration data
Connection name string	13	Eds_Char Array	Unique name to allow a user to identify the application assembly to which this instance is associated
Help string	14	Eds_Char Array	User help message related to using the connection
Path	15	Padded EPATH	See 6.3.9 Application Path Construction Rules for Safety Connections.
ASYNC1	16	USINT	This is a FSCP 2/1 exclusive field Only applies to producing connections. Field shall be empty for consuming connections. Used to calculate Network Reaction Time
Max Consumer Number[a]	17	USINT	This is a FSCP 2/1 exclusive field When safety devices wish to define multipoint connections and need to restrict the max number of consumers to a value less than the default maximum of 15, this field can define the product limit. If this field is empty, the SNCT shall always use the default value of 15 for the maximum number of multipoint connections. This field can be left empty for point-to-point connections. See 7.7.5.11 (Max_Consumer_Number) for the definition of legal values for this field

[a] This field is specified only for safety related specifications and shall either be empty or omitted for non-safety related connection manager instances.

8.10.2.5.5.2 Trigger and Transport field

Safety devices define whether a connection is a producing (client) or consuming (server) connections by filling out this field. The other parts of the field will have fixed definitions as follows:

- Class: always 0;
- Trigger: always application;
- Transport type: all 0.

8.10.2.5.5.3 Connection Parameter field

Safety devices define what types of connections are possible for a connection by using this field. All the other fields will have fixed values. Table 117 provides the only valid values for Safety devices.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Table 117 – Connection parameter field settings for safety

Connection T\type	Connection parameter setting
Producing (client) input connection	22645505_{hex} (High piority, multipoint or point-to-point), 22445505_{hex} (High piority, no multipoint), 66645505_{hex} (Scheduled or High priority, multpoint or point-to-point), or 66445505_{hex} (Scheduled or High priority, no multipoint)
Consuming (server) output connection	22445505_{hex} (High piority, point-to-point), or 66445505_{hex} (Scheduled or High priority, point-to-piont)

8.10.2.5.5.4 Safety ASYNC field

This parameter is necessary to properly calculate the Network Reaction Time for a safety connection. This parameter is generally different for input connection and output connections but is design dependent. This field is required in the Connection Manager section for producing (client) connections. Devices which produce on input connections shall define a safety ASYNC value for those connections, and devices which produce on output connections (i.e. logic devices or scanners) shall define a safety ASYNC value for these connections. Any value provided on consuming (server) connections will be ignored by the software. If a safety ASYNC parameter is not defined in a producing connection, the software shall use a worst-case default value of 1. The values of the ASYNC parameter are:

- Safety ASYNC = 0 = synchronous;
- Safety ASYNC = 1 = asynchronous.

8.11 Requirements for CP 2/2

8.11.1 EPI rules for safety messages that travel over CP 2/2

Safety packets that shall travel over CP 2/2 have certain restrictions based on the Safety format used when establishing the connection.

Safety Connection using the Base Format and traveling over CP 2/2 are restricted to EPIs less than 100 ms. The method by which this restriction is enforced is a vendor specific decision. For example, the restriction could be enforced in the originator configuration software or in originator connection establishment checks. Vendors will be responsible for verifying that proper restrictions are in place.

Safety Connections using the Extended Format are able to use the higher range of 1 000 ms.

8.11.2 Default safety I/O service

Safety connections support both Point-to-point and Multipoint connection types, but CP 2/2 has a number of system complications when Multipoint services are used. It is highly recommended that when configuring safety connections in an originator, the safety configuration software should present point-to-point as the default service for all Safety configurations. The User shall be given the option to select Multipoint, but if this selection is not specifically made, point-to-point should be used.

Safety CP 2/2 devices should consider adding support for multiple point-to-point connections to the same safety input assembly to better facilitate the use of point-to-point.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

8.11.3 Duplicate IP detection

Safety devices that reside on CP 2/2 shall support the IPv4 Address Conflict Detection mechanism defined in CP 2/2.

8.11.4 Priority for safety connections

CP 2/2 safety devices shall utilize the standard CP 2/2 Quality of Service scheme; see IEC 61158-5-2 for implementation details. CP 2/2 safety devices shall implement the QoS services and support priority marking via DiffServ Code Points (DSCP). CP 2/2 safety devices shall use "scheduled" as the default priority for safety I/O devices.

8.12 Requirements for CP 2/3

8.12.1 Allocation of CP 2/3 identifiers

8.12.1.1 General

During connection processing of a SafetyOpen CP 2/3 safety identifiers shall be assigned from the available pool of CP 2/3 Group 1 identifiers.

In order to preserve connection ID's, the rules in Subclauses 8.12.1.2 to 8.12.1.10 shall be implemented for the allocation of connection ID's.

8.12.1.2 Basic CP 2/3 algorithm (general model)

Safety connection originators shall initially ask the target (via SafetyOpen) to allocate one, two, or three identifiers according to the rules stated in Table 118.

Table 118 – CP 2/3 ID assignment rules

Connection Type	Intermediate (First) Hop	Last (Only) Hop 1st attempt	Last (Only) Hop 2nd attempt	Last (Only) Hop 3rd attempt
Point to point	T ⇒ O: Target Router O ⇒ T: Originator or Originating Router	T ⇒ O: Target O ⇒ T: Target	Connection Fault, Connection cannot be established	Connection Fault, Connection cannot be established
Multipoint T ⇒ O (typical; input module, output module status)	T ⇒ O: Target Router O ⇒ T: Originator or Originating Router TC: Target Router	T ⇒ O: Target O ⇒ T: Conditional TC: Target	T ⇒ O: Target O ⇒ T: Originator (if first request was Target) TC: Target	Connection Fault, Connection cannot be established
Multipoint O ⇒ T	T ⇒ O: Target Router O ⇒ T: Originator or Originating Router TC: Originator or Originating Router	T ⇒ O: Target O ⇒ T: Originator TC: Originator or Originating Router	T ⇒ O: Originator O ⇒ T: Originator TC: Originator or Originating Router	Connection Fault, Connection cannot be established

This is accomplished by inserting 0xFFFFFFFF identifiers in the SafetyOpen request sent to the target.

If a safety target cannot or refuses to allocate the identifier(s), the target shall respond to the Safety Open request with a 0x01 general error status with extended status 0x031F indicating no connection resources are available.

The originator receives the SafetyOpen response.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

If the target has allocated identifiers from its pool, it shall insert them into the SafetyOpen success response.

The originator accepts these and the connection is completed.

If the target has not allocated identifiers from its pool then the originator has the option to allocate identifiers from its own pool. If the originator does allocate the identifier(s) then it shall convey this data to the target (via a second SafetyOpen)

If the originator cannot or refuses to allocate an identifier then the connection cannot be established.

8.12.1.3 Case 1 (target allocates identifiers)

This first scenario has the originator requesting that the target allocate the connection identifiers and the target agrees to do so.

The connection originator asks the target (via Safety Open) to allocate one, two or three identifiers.

- The target agrees to allocate the identifier(s) and responds to the Safety Open request with success.
- The originator receives the Safety Open response and accepts these identifiers and the connection is completed.

8.12.1.4 Case 2 (target cannot allocate identifiers)

This second scenario has the originator requesting that the target allocate the connection identifiers but the target cannot or refuses to do so.

- The connection originator asks the target (via Safety Open) to allocate one, two or three identifiers (identifier = 0xFFFFFFFF).
- The target chooses not to allocate the identifier(s) and responds to the Safety Open request with a 0x01 general error code with extended status 0x05 indicating that the resources are not available.
- The originator receives the Safety Open response, sees that target cannot allocate identifiers and then chooses to allocate identifiers from its own pool.
- The originator then constructs a second Safety Open with the identifiers specified.
- The target accepts this Safety Open and the connection is completed.

8.12.1.5 Case 3 (originator allocates identifiers)

This third scenario has the originator deciding to allocate its own identifiers with asking the target.

- The connection originator allocates the identifiers from its pool and enters these values into the Safety Open which is then sent to the target.
- The target accepts this Safety Open and responds with success.
- The originator receives the Safety Open response and the connection is completed.

8.12.1.6 Order of MSGID Allocation

As stated before each node has a total of 12 Group1 identifiers that can be used for safety connections. In order to provide consistency among producers and consumers, the following rule shall be used when allocating identifiers: The first MSGID to be allocated shall start at the highest available value and move downward.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Thus the first MSGID would be B(hex) or 1011(binary) and the next would be A(hex) or 1010(binary).

8.12.1.7 Rules for connection ID assignment

The following rules for CP 2/3 ID assignment shall be followed by Safety targets, originators and bridges. These rules provide repeatable ID allocation for a system where one or no routers are connected to CP 2/3. It effectively takes unused IDs from target devices and provides them to bridges. Because one resource, the router, is allowed to ask for these resources, it needs to work repeatably. But any attempt to extend this to other originators could result in a situation where repeatable power up was not achievable.

- Rule 1: All on-link multipoint originators provide the third group 1 ID when establishing a connection.
- Rule 2: All off-link multipoint connection originators (routers) request the third group 1 ID from the target
- Rule 3: The group 1 ID in targets are divided into 2 types, reserved and free.
  - The reserved IDs are equal to 2 × the maximum number of safety connections that a device can support. The maximum number of connections is specified when a device is configured.
  - The number of free IDs is equal to Max group 1 ID (12) – reserved IDs.
  - In most target devices, this could be a default value and the user would never need to change it.
- Rule 4: Each target would provide 2 reserved group 1 IDs to multipoint or point to point originators until its reserved IDs are depleted. Once its reserved IDs are depleted it would reject requests to establish new connections. But it would still allow originators to try to establish multipoint connection to multipoint productions that were already established.
- Rule 5: Each target would provide the third group1 ID to multipoint originators from its free pool. Once the free pool is exhausted, it would reject the request and the originator would need to supply the third ID.

8.12.1.8 Point to point message connections

The basic algorithm described in 8.12.1.2 to 8.12.1.7 applies to this connection types.

8.12.1.9 Multipoint message connections

Multipoint producers shall allocate an identifier from its own pool, i.e. the source MACID shall be that of the producer. Multipoint producers shall reject any connection request that attempts to assign IDs for its produced data or time correction data. The multipoint consumer may follow the basic algorithm described above.

8.12.1.10 CP 2/3 ID quarantining requirements

Target devices need to take care that they don't re-allocate any group 1 IDs until they are certain that the IDs are no longer being used by the device they had been previously allocated to. To assure that this condition will not occur, the following algorithm shall be followed.

When a safety device closes a connection in which group 1 IDs were allocated to another device, the group 1 ID shall be placed into quarantine for a period equal to the (connection_EPI × Ping_Interval_Multiplier) × (Timeout_Multiplier.PI + 2). During this time, the ID cannot be used or allocated to another device.

If an originator who borrowed an ID detects the communication failure and re-issues a new connection request before these IDs are removed from quarantine, devices can define schemes that detect these requests and pull the IDs from quarantine early and return them to the originator. However, care shall be taken to assure that this is done with integrity.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

8.12.2 Additional requirements

None.

8.13 CP 16/3 requirements

8.13.1 General architecture for CPF 2 on CP 16/3

The safety layer of FSCP 2/1 on CP 16/3 is implemented according to the FSCP 2/1 specification without any modifications. In particular, this means that

- FSCP 2/1 on CP 16/3 uses the safety message formats defined in this document,
- the same CRC polynomials, seed values and algorithms are used, and
- all FSCP 2/1 objects and services are implemented according to this document.

Therefore, FSCP 2/1 on CP 16/3 does not rely on any measures to ensure data integrity provided by the CP 16/3 transport layer. CP 16/3 may fully be regarded as being part of the black channel.

FSCP 2/1 relies on a basic set of standard CIP objects and services to establish transport connections and exchange cyclic data. As CP 16/3 does not provide an implementation of the CIP application layer, an adaptation layer is needed to fill the gap between the CP 16/3 transport layer and FSCP 2/1.

Although all mechanisms were adopted from the existing FSCP 2/1 specification, some additions and changes to the specification had to be made. All additions and changes do not affect the measures defined by FSCP 2/1 to ensure data integrity.

8.13.2 Baseline FSCP 2/1 on CP 16/3 device

The functionality needed to implement FSCP 2/1 in a CP 16/3 device is encapsulated in an adaptation layer on top of the standard CP 16/3 communication mechanisms. The CP 16/3 function group "S 0 1830 Safety Connection" provides the functionality for configuring both explicit and I/O connections, and for exchanging data via the CP 16/3 Messaging Protocol (SMP).

Figure 85 shows how the FSCP 2/1 Adaptation Layer provides CIP functionality similar to the Baseline Safety Device defined in 6.6.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

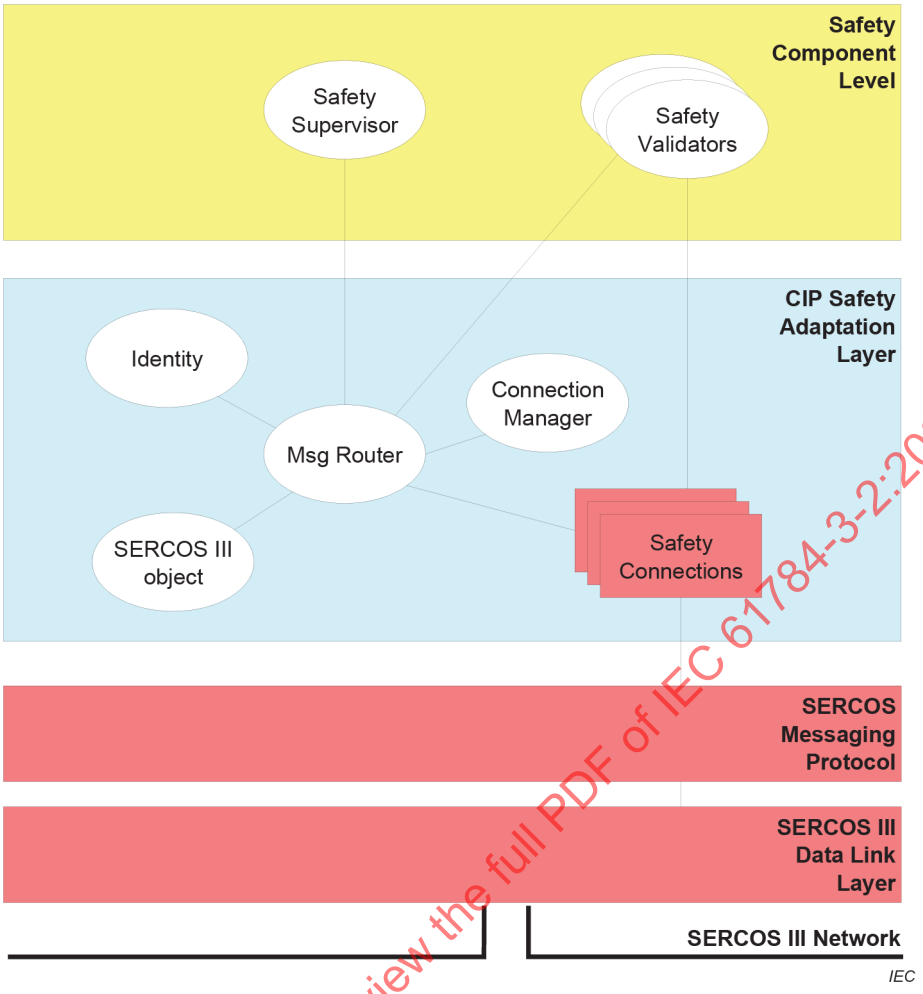


Figure 85 – Baseline FSCP 2/1 on CP 16/3 device

8.13.3 Supported objects and services in CP 16/3 devices

8.13.3.1 General

CP 16/3 devices shall support the CPF 2 objects as specified in 8.13.3.2 to 8.13.3.8.

8.13.3.2 Identity object (class code 0x01)

All required services shall be supported.

8.13.3.3 Connection Manager object (class code 0x06)

The Connection Manager object offers the services needed to open and close FSCP 2/1 connections:

- Forward Close (0x4E);
- Forward Open (0x54).

Although the Connection Manager object provides the interface to these services, most of the processing has to be done in the FSCP 2/1 layer to ensure high integrity. This is the purpose of the Validator Connection Establishment Engine shown in Figure 87. The FSCP 2/1 Adaptation Layer only takes care of preparing the black channel for the safety connection by setting up the necessary SMP sessions.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

8.13.3.4 Connection Configuration object (class code 0xF3)

The Connection Configuration object is usually only implemented for Connection Originators.

Each instance of this object keeps the configuration data for one connection that is needed to build a Forward Open service message to the Connection Target.

8.13.3.5 Message Router object (class code 0x02)

The Message Router object does not provide any accessible service. It distributes incoming explicit messages to all other objects in a device.

8.13.3.6 Safety Supervisor object (class code 0x39)

CP 16/3 devices shall support the Safety Supervisor object baseline level at a minimum.

8.13.3.7 Safety Validator object (class code 0x3A)

CP 16/3 devices shall support the Safety Validator object in its entirety.

8.13.3.8 SERCOS III Link object (class code 0x4C)

CP 16/3 devices shall support the SERCOS III Link object in its entirety.

8.13.4 Transport layer requirements

8.13.4.1 General

FSCP 2/1 on CP 16/3 devices shall use the CP 16/3 Messaging Protocol (SMP) to exchange safety messages. SMP defines a set of messaging containers that can be transported via CP 16/3 connections.

8.13.4.2 Transport layer considerations

CP 16/3 offers two basic mechanisms to exchange data between two devices.

- Cyclic connections

  A cyclic CP 16/3 connection transports a data package containing one or more data values from a producer to a consumer. The size of the data package, the contents and the production rate are usually configurable while a device is in parameterization level. When leaving the parameterization level, the configuration will remain static. The producer of the connection will then produce cyclic data at the configured rate.

- Service channel

  The service channel is an acyclic communication channel exclusively controlled by the CP 16/3 master. The master may send data to or retrieve data from a slave device.

Neither cyclic connections nor the service channel can fulfill all requirements of FSCP 2/1 on CP 16/3. Therefore, the FSCP 2/1 adaptation layer uses the CP 16/3 Messaging Protocol (SMP) to exchange FSCP 2/1 messages with other CP 16/3 devices. This protocol is layered on top of the cyclic CP 16/3 connections. It offers a send()/recv()-like API to the application layer (in this case, to the FSCP 2/1 Adaptation Layer). The application layer in the producer can send messages of arbitrary length to a consumer. SMP uses a fixed-length data container in a cyclic connection to transport these messages. Messages that are bigger than the data container will be split into several fragments which are then transported sequentially. A prioritization scheme allows high-priority messages to interrupt the transmission of long, fragmented messages of lower priority. This allows for an effective multiplexing of several logical communication channels on a single transport container.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Being a part of the CP 16/3 transport layer, the CP 16/3 Messaging Protocol stack is a part of the black channel. It does not affect any of the mechanisms and data integrity measures implemented by the FSCP 2/1 layer.

The example in Figure 86 shows a possible configuration of SMP for a single FSCP 2/1 connection. Two SMP containers are used, one being configured in the AT to transport messages from the CP 16/3 slave to the CP 16/3 master, while the other container is configured in the MDT to transport messages from the CP 16/3 master to the CP 16/3 slave. The CP 16/3 master, acting as the connection originator, will initiate the safety connection by sending a CIP Forward Open as an unconnected explicit message to the slave. This message is transported via the SMP container 2. The slave responds with a Forward Open Response message transported by SMP container 1. At the same time it starts producing FSCP 2/1 data messages which are transported in the same container. The use of a session with identifier allows an effective multiplexing of multiple logical communication channels on a single transport container.

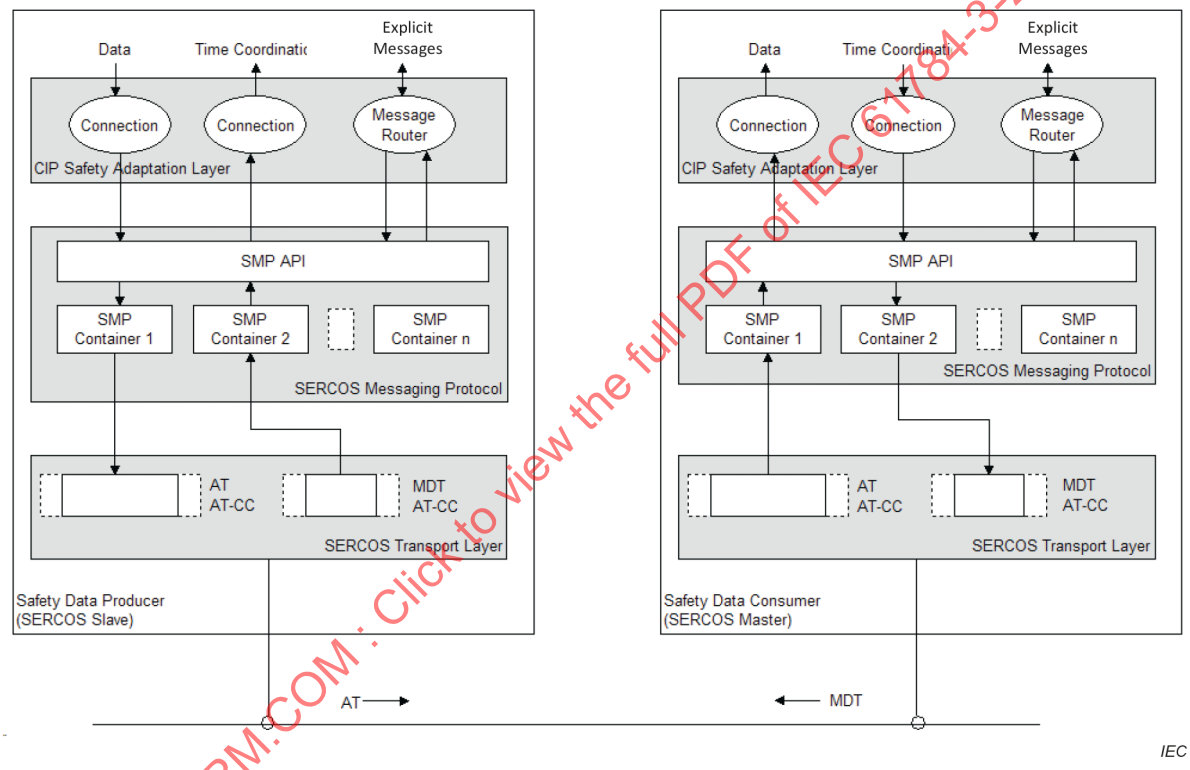


Figure 86 – FSCP 2/1 Adaptation Layer and SMP interaction

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

8.13.4.3 Multipoint connections

CP 16/3 MS (master-slave) connections shall only be used to build point-to-point safety connections. CP 16/3 CC (cross communication) connections may be used to build point-to-point or multipoint safety connections.

8.13.4.4 FSCP 2/1 Adaptation Layer for CIP Services

CP 16/3 does not support the Common Industrial Protocol (CIP). Therefore, the adoption of FSCP 2/1 as a safety layer for CP 16/3 devices raises the need for an adaptation layer that implements a basic set of CIP services and objects.

The objects and services offered by the FSCP 2/1 Adaptation Layer shown in Figure 87 are not part of the safety protocol itself. Therefore, these services do not need to be performed with high integrity. The FSCP 2/1 Adaptation Layer may be regarded as being part of the black channel.

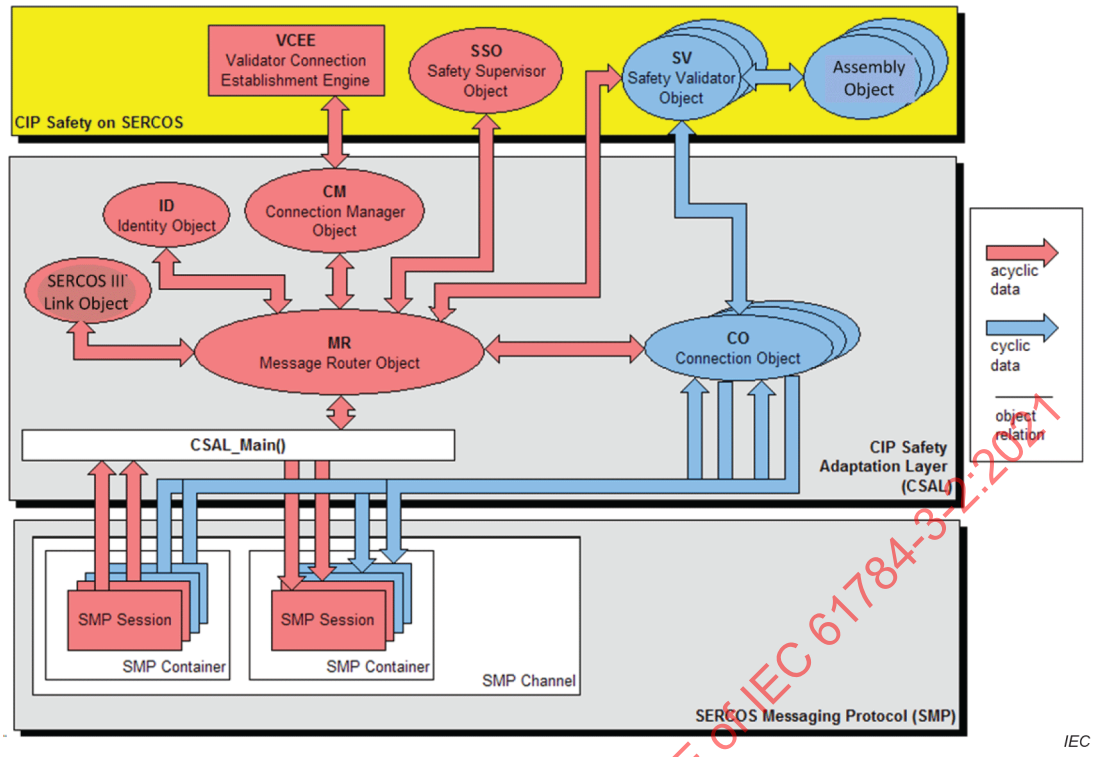


Figure 87 – FSCP 2/1 Adaptation

8.13.5 FSCP 2/1 and the CP 16/3 device model

Figure 88 shows the components of a generic CP 16/3 device. There is a clear separation into communication- and device-related components. The communication-related components are defined in the CP 16/3 communication profile (SCP). The CP 16/3 Interface component represents the physical interface to the CP 16/3 network, while the CP 16/3 Slave component provides a logical interface with a CP 16/3 Slave Address that is unique to the CP 16/3 Network. This structure allows for a modular device design with several subdevices sharing a single physical interface.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

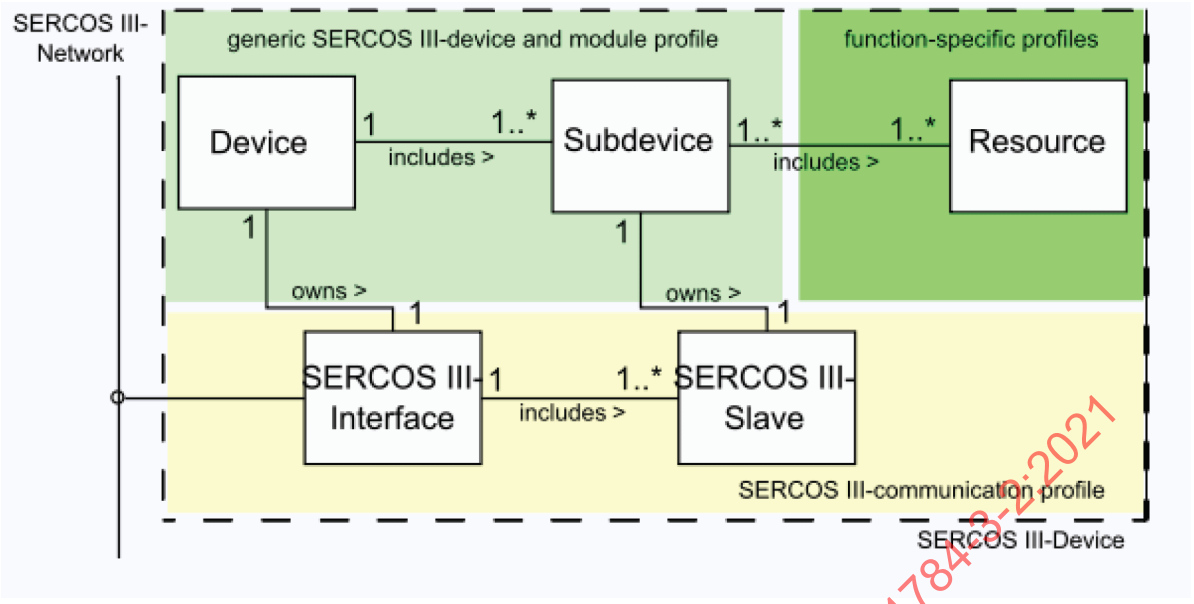


Figure 88 – CP 16/3 device model

In this context, "modular design" does not imply that the device hardware is modular as well. A monolithic device may internally be regarded as being modular if it features several independent subdevices. For example, a dual axis AC drive controller may internally be modeled as a single device containing two independent subdevices with two different CP 16/3 addresses that are connected to the CP 16/3 Network via the same interface.

In CP 16/3 terms, safety functionality is modeled as a function-specific profile that implements one or more resources in a subdevice. This implies that a CP 16/3 Device may contain several independent safety devices as defined by this document. As there is a substantial difference between a "device" and a "safety device" in the CP 16/3 context, care should be taken not to mix up these terms.

Modular I/O devices are modeled as a single CP 16/3 Device with usually one single subdevice. Each I/O module is represented by a set of function groups in this subdevice.

8.13.6 UNID assignment on CP 16/3

8.13.6.1 General

FSCP 2/1 requires the assignment of a plantwide Unique Node ID (UNID) to each safety device. The 10 octet UNID consists of a 6 octet Safety Network Number (SNN) combined with the node's 4 octet NodeID (MACID on CP 2/3, IP address on CP 2/2, SDID on CP 16/3).

For a CP 16/3 Safety Device, the SNN shall be readable as an attribute of the CP 16/3 object. The SDID is readable as part of the TUNID attribute of the supervisor object of the CP/3 safety device. Both the SDID and the SNN shall be stored as UNID struct in this TUNID attribute.

```
struct UNID
{
    S_SNNDate_AND_Time      SNN;
    UDINT                   SDID;
}
```

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

8.13.6.2 CP 16/3 Safety Device ID

Subclause 8.13.5 on the CP 16/3 device model showed that it is impossible to uniquely identify a safety module in a modular device by its network node address (CP 16/3 slave address).

On the other hand, excluding the network node address from the NodeID portion of the UNID leads to a better separation of the standard device configuration from the safety configuration. This facilitates device commissioning, because a module may be moved to a different physical location after the safety configuration has been verified and locked, as shown in Figure 89. Only the non-safety-relevant parts of the configuration have to be adjusted to the new network topology by changing the CP 16/3 addresses. The safety layer will still ensure that only safety connections configured for this safety device can be established.

Therefore, in a CP 16/3 network, the MACID portion of the UNID shall be chosen by the configuration tool or set in the safety device by other means (e.g. DIP switches), and shall not be related to neither the standard network node address, nor the physical position of a module on the device's local bus.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

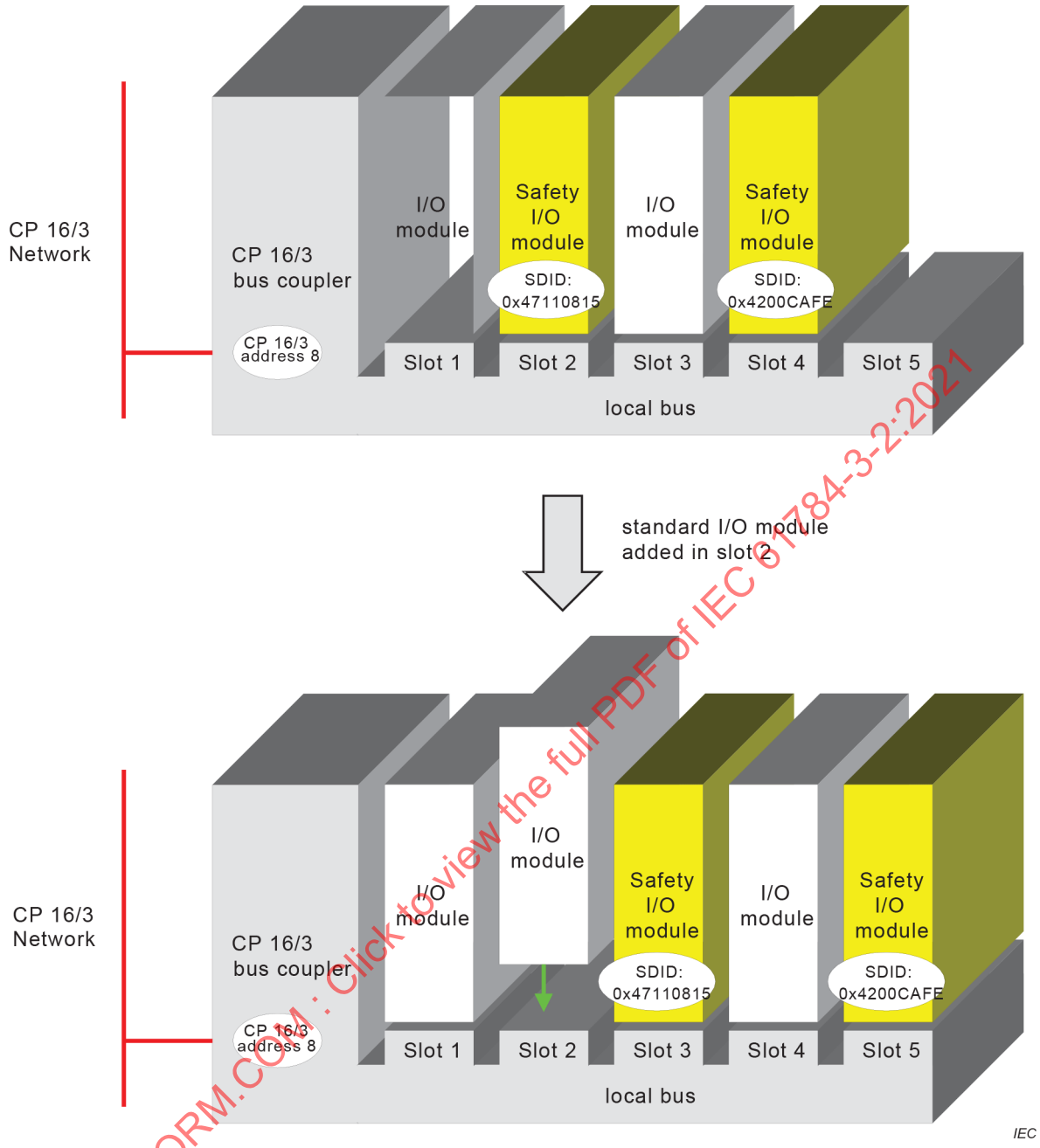


Figure 89 – Adding a standard module to a modular device

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

It has to be assured that the cabling attached to a module is also moved to the new location when moving a safety module without updating the safety network configuration. The manufacturer of a FSCP 2/1 on CP 16/3 device shall ensure this by appropriate means or by adding an appropriate advisory to the device's safety manual.

8.13.6.3 Safety Network Number assignment

FSCP 2/1 requires the assignment of Safety Network Numbers (SNN) in all FSCP 2/1 on CP 16/3 nodes. SNN and MACID together form the UNID that has to be unique for each device in a safety system. Because the SDID portion of the UNID is not related to the standard network address of a safety device, a SNN value is not limited to the boundaries of single CP 16/3 network. Several CP 16/3 networks may use the same SNN as long as they belong to the same configuration segment (a group of CP 16/3 networks configured by a single configuration tool). The configuration tool shall be responsible for assigning different SDID values to all safety devices in one configuration segment.

9 System requirements

9.1 Indicators and switches

9.1.1 General indicator requirements

FSCP 2/1 safety devices are required to have module and network indicators.

Device developers are free to have additional indicators on their products if they so desire.

Indicators are typically implemented as LEDs. If the device includes alternate status presentation means (e.g., LCD or HMI panels), then all references to LED contained in this specification may be considered to describe a visually or semantically equivalent indicator implemented using the alternate status presentation means.

Important: FSCP 2/1 safety devices shall provide a separate indicators for Module Status and a Network Status. In this case, these indicators provide important additional safety-related information to the user that cannot be accomplished with a combined Net/Mod Status indicator.

Important: If there is a conflict between turning an LED on Red versus Green, the LED shall be turned on Red.

9.1.2 LED indications for setting the device UNID

Table 119 defines the way the LED indications are used for setting the UNID. The LED behavior related to the Waiting for TUNID state in this table is not required for devices which do not support the Propose/Apply Safety Supervisor services.

Table 119 – LED indications for setting UNID

Safety Supervisor State/Event	MOD LED	NET LED
Self-test	Flash Red/Green	Off
Waiting for TUNID	Flash Red/Green	Connection dependent
Waiting for TUNID Proposed TUNID Rcvd	Flash Red/Green	Flash Red/Green using Fast 250 ms / 250 ms Reuse CP 2/3 Group 4 pattern
Configuring	Flash Red/Green	Connection dependent
Idle	Flashing Green	Connection dependent
Executing	Green	Connection dependent

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

9.1.3 Module Status LED

This bi–color (green/red) LED provides device status. It indicates whether or not the device has power and is operating properly. Table 120 defines the Module Status LED states. Table 120 defines the Module Status LED conditions for safety devices (which has to use the Safety Supervisor object). The states shown reflect the device states specified in the Identity object. These states are also mapped to the states defined in Safety Supervisor object.

For safety devices which use the SNCT interface, the states of the Safety Supervisor shall be what determine the Module LED status.

Table 120 – Module Status LED

For Safety Supervisor state:	LED is:	To indicate:
No Power	Off	There is no power applied to the device
Executing	Green	The device is operating in a normal condition
Idle state	Flashing Green[a]	The Device is in the Idle or Standby State. Reference the Identity object (6.4) or Safety Supervisor object (6.5.3)[b]
Abort	Flashing Red[a]	Recoverable Fault
Critical Fault	Red	The device has an unrecoverable fault, may need replacing
Device Self Testing, Waiting_for_TUNID or Configuring[b]	Flashing Red-Green[a]	The Device is in Self Test or the Device needs commissioning due to configuration or UNID missing, incomplete or incorrect[c]. Reference the Identity object (6.4) or Safety Supervisor object (6.5.3)[b]

[a] The flash rate for is approximately 1 flash per second. The LED should be on for 0,5 s on off for approximately 0,5 s.

[b] The state of safety devices is determined by the Safety Supervisor object.

[c] An Unconfigured/unowned safety device should not be allowed to persist while connected to an active safety system.

9.1.4 Indicator warning

The User Safety Manual shall provide a warning that states "LEDs are NOT reliable indicators and cannot be guaranteed to provide accurate information. They should ONLY be used for general diagnostics during commissioning or troubleshooting. Do not attempt to use LEDs as operational indicators".

9.1.5 Network Status LED

This bi–color (green/red) LED indicates the status of the communication link. The indications for this LED are defined in Table 121.

Table 121 – Network status LED states

Network Connection Status:	LED is:	To indicate:
Not Powered/Not On-line	Off	Device is not on–line. The device has not completed the Dup_MAC_ID test yet. The device is possibly not powered, look at Module Status LED

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Network Connection Status:	LED is:	To indicate:
On-line, Not Connected	Flashing Green [a]	Device is on–line but has no connections in the established state. The device has passed the Dup_MAC_ID test, is on–line, but has no established connections to other nodes. For a Group 2 Only device it means that this device is not allocated to a master. For a UCMM capable device it means that the device has no established connections. For safety devices, a connection may be established, but the Validator has not completed an initial Time Coordination exchange
Link OK, On-line, Connected	Green	The device is on–line and has connections in the established state.
Connection Time-out	Flashing Red [a]	One or more I/O Connections are in the Timed–Out state
Critical Link Failure	Red	Failed communication device. The device has detected an error that has rendered it incapable of communicating on the network
Communication Faulted and Received an Identify Comm Fault Request – Long Protocol or Propose_TUNID service received	Flashing Red-Green [a]	A specific Communication Faulted device. The device has detected a Network Access error and is in the Communication Faulted state. The device has subsequently received and accepted an Identify Communication Faulted Request – Long Protocol message. After Propose_TUNID service request, NET LED flashes Red/Green using Fast 250 ms/ 250 ms pattern until successful Apply_TUNID. Safety devices use this indication to allow maintenance personnel to commission the UNID in a safety device

[a] Unless otherwise indicated, the flash rate of the NET LED is approximately 1 flash per second. The LED should be on for approximately 0,5 s and off for approximately 0,5 s.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

9.1.6 Switches

9.1.6.1 NodeID switches

There are no safety-related diagnostic requirements for switch(es) because FSCP 2/1 assures integrity for NodeIDs through the TUNID setting mechanism. Therefore, the switch(es) need only be checked after power cycle, reset or during attribute setting. The logic for the two procedures is shown in Figure 90.

There is direct relationship between the NodeID setting and the NodeID portion of the Target UNID (TUNID) in the safety supervisor. See the Safety Supervisor (6.5.3) object for more information.

9.1.6.2 NodeID determination

During device initialization, the NodeID switches are read by the device firmware.

The NodeID attribute (if supported) in the CP 2/3 object shall always reflect the value in use.

The following logic is applied to CP 2/3:

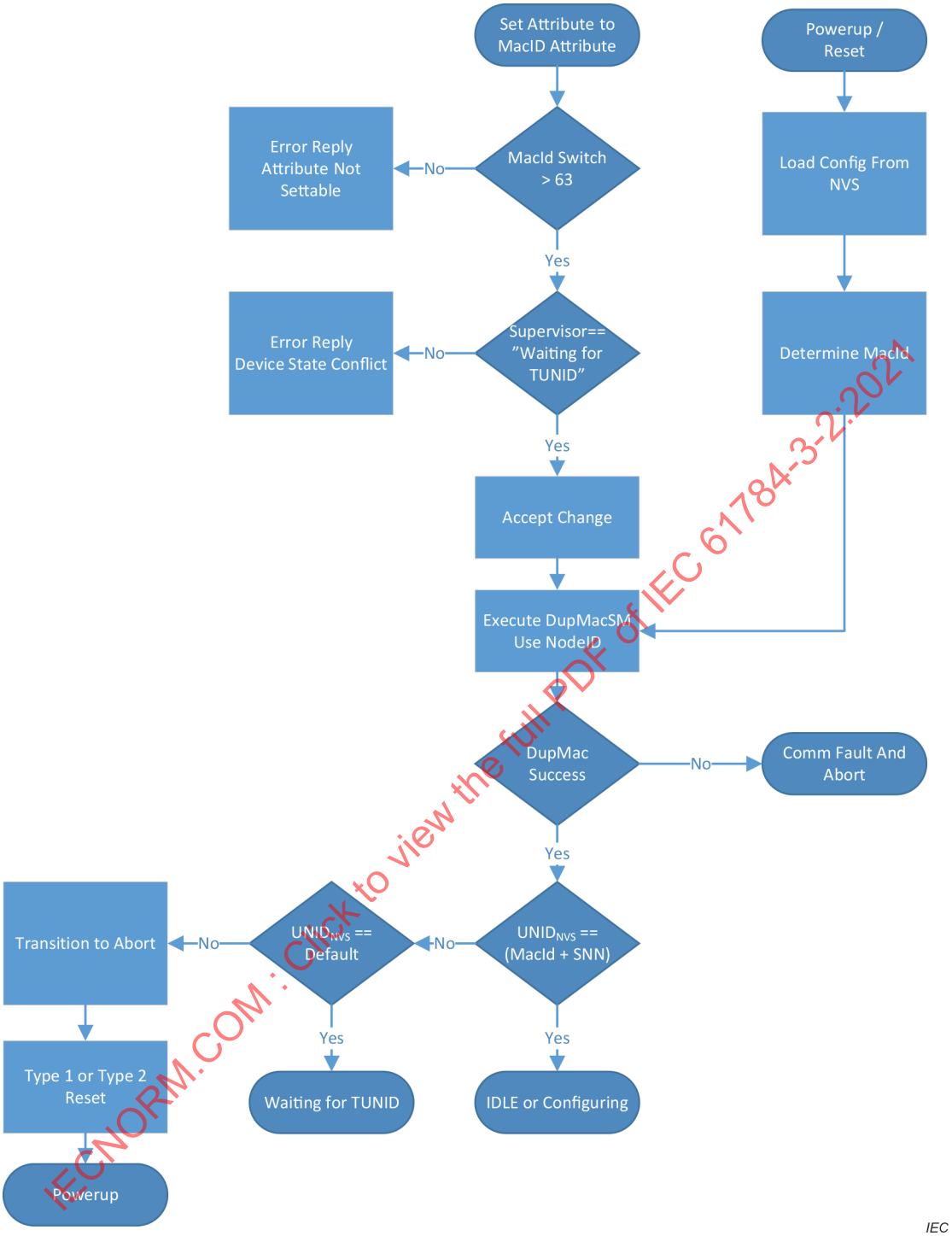
- When the switches are read, if the switches specify a valid NodeID, (a value from 0 to 63 for NodeID), this value shall be used as the NodeID;
- When the switches are read, if the specified NodeID differs from the value stored in the CP 2/3 object's NodeID Attribute (NVRAM values), the appropriate attribute/s shall be updated and saved to NVRAM;
- When the switches are read, if the switches specify an invalid NodeID, (a value greater than 63), the device should follow one of the recommended options in IEC 62026-3;
- When the switches are read, if the switches used to specify the NodeID are set to a valid value (a value from 0 to 63 for the NodeID), the NodeID attribute shall have Get Only access;
- When the switches are read, if the switches are set to the software programmable mode (>63 for the NodeID), the NodeID attribute shall have Set access;
- If a device has no switches it shall use default values for NodeID in its out-of-box configuration (63 for the NodeID).
- If the device is out-of-box it shall use the current NodeID switch settings if these are valid values.

When a FSCP 2/1 device supports the Propose_TUNID and Apply_TUNID or the Propose_TUNID_List and Apply_TUNID_List services and supports the Set_Attribute service to the NodeID attribute, and the NodeID switches are set to enable the Set_Attribute service, it shall only accept the Set_Attribute service while in the "Waiting for TUNID" state. Otherwise, it shall reply with a "Device State Conflict".

The rules for setting the NodeID attribute in devices which don't support the Propose_TUNID and Apply_TUNID or the Propose_TUNID_List and Apply_TUNID_List services is vendor-specific.

If a FSCP 2/1 device supports the Set_Attribute service to the Baud Rate attribute, Safety devices shall only accept the Set_Attribute while in the "Waiting for TUNID" state. Otherwise, it shall reply with a "Device State Conflict".

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021



IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Figure 90 – Safety device NodeID processing logic

9.1.6.3 Reset switch

If a reset switch is provided on a safety device, the safety device shall execute a Safety Supervisor Type 2 reset (i.e. reset to out-of-box, but preserve the password).

9.2 Installation guidelines

The installation guidelines of IEC 61918 and IEC 61784-5-2 for CPF 2 shall apply.

9.3 Safety function response time

9.3.1 Overview

The safety function response time is the worst-case time from a safety related event as input to the system or as a fault within the system, until the time that the system is in the safety state. The scope of the reaction time is defined in Figure 91.

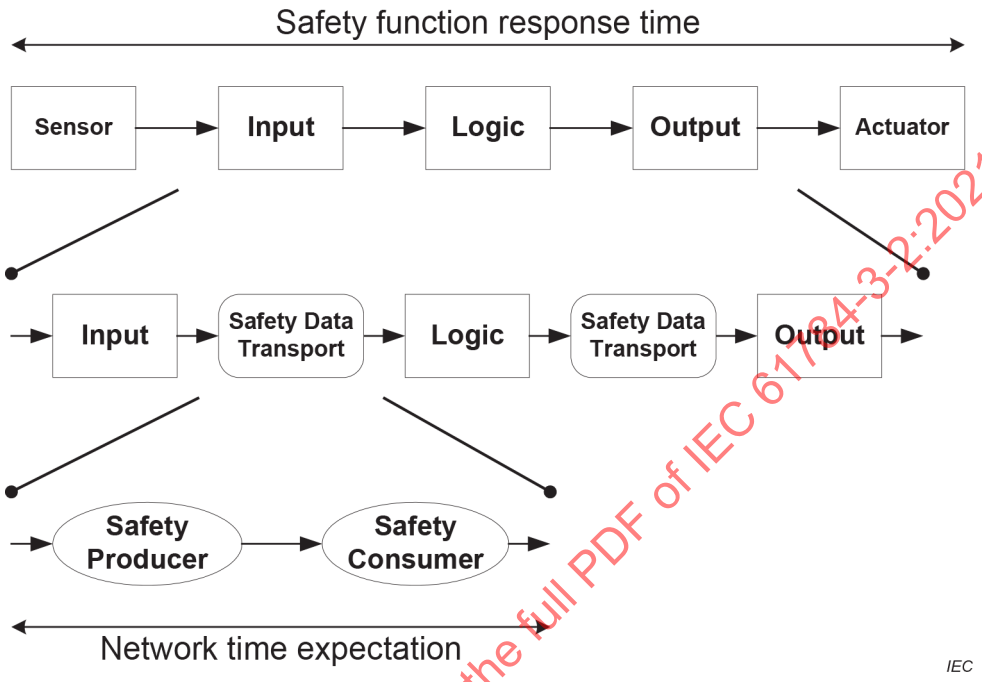


Figure 91 – Safety function response time

To determine the safety function time of any control chain the user shall add up the components of the safety chain.

Using the example in Figure 91, the safety function response time would be:

Safety function response time = Sensor reaction time (13)
+ Input reaction time
+ Network reaction time
+ Controller reaction time
+ Network reaction time
+ Output reaction time
+ Actuator reaction time

9.3.2 Network time expectation

The Network Time Expectation is a portion of the Safety function response time. The Network Time Expectation is the worst case time, from the time the data is captured by the safety data producer, until the consuming application recognizes a safety state. This also includes errors during production and consumption.

The Network_Time_Expectation_Multiplier used in the previous subclauses of this document, represents the worst case measured time from the time the data is captured by the safety data producer until the time that the consuming application recognizes a safety state indication.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

The Network_Time_Expectation_Multiplier value necessary to ensure a timeout error is not detected is:

$$\begin{aligned} \text{Network_Time_Expectation_Multiplier} > {} & \text{EPI} \times \text{Timeout_Multiplier} \\ & + \text{Safety_Message_Time(max)} \\ & + \text{Time_Coord_Message_Time(max))} / 128\ \mu\text{s} \\ & + \text{Connection_Correction_Constant} \end{aligned} \quad (14)$$

where:

Safety_Message_Time(max) is the actual time from the data being captured by the safety data producer until the time that the safety data is passed to the consuming application for use.

Time_Coord_Message_Time(max) is the maximum time it could take for the time coordination information to be sent from the consumer to the producer. This is measured from the time the Consumer_Clk_Count is captured to Consumer_Time_Value until the time Producer_Clk_Count is captured to Producer_Rcved_Time_Value.

Timeout_Multiplier is a parameter that is needed by the safety protocol processing. This value determines the number of messages that may be lost before declaring a connection error. A Timeout_Multiplier of 1 indicates that no messages may be lost. A Timeout_Multiplier of 2 indicates that 1 message may be lost, etc. In addition to the Timeout_Multiplier checks within the protocol, reaction time checks are also performed. A reasonable default for the Timeout_Multiplier would be 2. A reasonable limit would be for configuration software to restrict the Timeout_Multiplier to integer values from 1 to 4. For the ExtendedFormat the Timeout_Multiplier may be increased to 255 as long as the Network Time Expectation value does not exceed 5,8 s.

Connection_Correction_Constant is a value in 128 µs increments that is subtracted from the time stamp to represent the worst case error due to Time drift, the asynchronous nature of the producer and consumer clocks, and the minimum time for the Time Coordination Message to traverse from the consumer to the producer.

Timeout_Multiplier and Connection_Correction_Constant are described in 7.7.5.8 and 7.7.5.15 respectively.

9.3.3 Equations for calculating network reaction times

The most logical place for the user to set and determine the Network reaction times is at the logic device since it is very likely both the configuration holder and connection originator.

There are two cases of safety connection reaction times for most logic devices. They are:

- Input Connection reaction time;
- Output Connection reaction time.

Table 122 defines the producing application and consuming application for the Network reaction time cases above.

Table 122 – Connection reaction time type – producing/consuming applications

Connection reaction time type	Producing application	Consuming application
Safety Input	Input module	Controller
Safety Output	Controller	Output module

Figure 92 shows the analysis of the Safety Function Response Time components. The time enforcement analysis is done from the Output signal back to the Input signal. Doing the analysis from the Output signal back to the Input signal allows the effects of asynchronous productions to be seen.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

The analysis assumes that the output module will have an internal cycle that checks the age of the last received output data. The age of the output data will be maintained at less than the Network_Time_Expectation_Multiplier (NTEM) value.

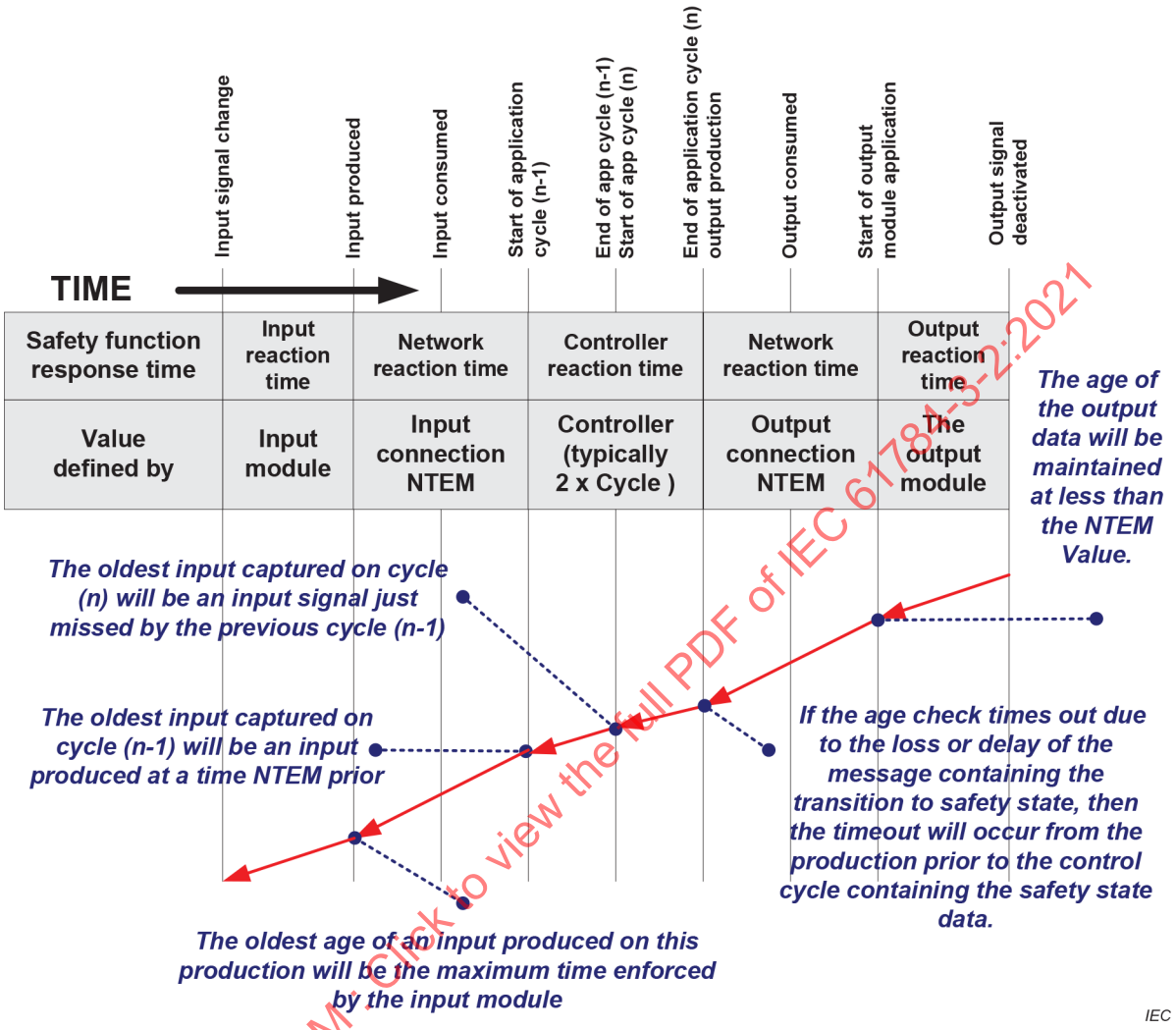


Figure 92 – Safety function response time components

From an analysis point of view, a controller to controller connection would be treated the same as an Input connection.

For an Input or Controller to Controller Connection:

$$\text{Network reaction time} = \text{Network_Time_Expectation_Multiplier} \times 128\ \mu\text{S} \quad (15)$$

For a Connection to an Output Module:

If the Output Production is Asynchronous to the Controller Cycle:

$$\text{Network reaction time} = \text{Network_Time_Expectation_Multiplier} \times 128\ \mu\text{S} + \text{EPI_in_Sec} \quad (16)$$

If the Output Production is Synchronous to the Controller Cycle:

$$\text{Network reaction time} = \text{Network_Time_Expectation_Multiplier} \times 128\ \mu\text{S} \quad (17)$$

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

The Output Connection cases can be simplified to:

$$\text{Network reaction time} = \text{Network Time Expectation Multiplier} \times 128\ \mu S + (\text{EPI_in_Sec} \times \text{ASYNC}) \quad (18)$$

where the ASYNC parameter is defined as follows:

ASYNC parameter

If the producing application is synchronous with data production, ASYNC = 0. If the producing application is asynchronous to the data production, ASYNC = 1. The net effect of this difference is that one additional EPI is added to the Network reaction time for asynchronous devices. This ASYNC parameter should be provided to the Safety Configuration software via and EDS file entry. The default value in cases where it is not provided shall be 0.

9.4 Duration of demands

The duration of demand by the safety-related application to the safety communication layer shall be sufficient in duration such that demand is detected by the longest EPI selected by the application.

9.5 Constraints for calculation of system characteristics

9.5.1 Number of nodes

CP 2/3 based implementations are limited to a maximum of 32 producing and 32 consuming nodes for this safety profile. CP 2/2 based implementations have no limitation on the number of producers and consumers for this safety profile.

9.5.2 Network PFH of Extended Format

This Subclause 9.5.2 describes the principal method used for the determination of the PFH value for each safety communication channel using Extended Format.

NOTE Base Format has been deprecated so network PFH is not calculated for Base Format.

The safety communication channel PFH shall meet the 1 % rule from IEC 61784-3. FSCP 2/1 is targeted at systems up to SIL 3, therefore the safety communication channel PFH shall not be more than 10^{-9} per hour.

FSCP 2/1 network protocol consists of four parts, safety data, time stamp information, the multipoint time correction information, and the time coordination ping response. Each of these parts has its own protection that contributes to the PFH. The protection of each part covers four types of errors: integrity error (I), authenticity error (A), timeliness error (T) and masquerade error (M).

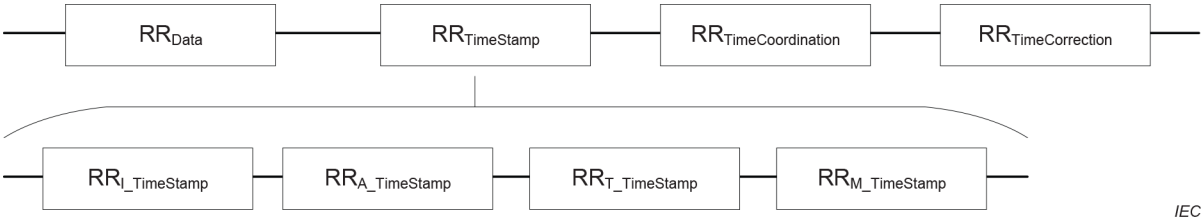


Figure 93 – Network protocol reliability block diagram (RBD)

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

As shown in Figure 93, the residual error rate per hour of each part can be divided into four sub residual error rate per hour elements which are corresponding to four error types. From the RBD in Figure 93, the equation for the total network residual error rate per hour of the safety communication channel is:

$$\lambda_{SC}(Pe) = RR_{Data} + RR_{TimeStamp} + RR_{TimeCoordination} + RR_{TimeCorrection} \quad (19)$$

$$= RR_{I_Data} + RR_{A_Data} + RR_{T_Data} + RR_{M_Data} + RR_{I_TimeStamp} + RR_{A_TimeStamp} + RR_{T_TimeStamp} + RR_{M_TimeStamp} + RR_{I_TimeCoordination} + RR_{A_TimeCoordination} + RR_{T_TimeCoordination} + RR_{M_TimeCoordination} + RR_{I_TimeCorrection} + RR_{A_TimeCorrection} + RR_{T_TimeCorrection} + RR_{M_TimeCorrection}$$

where

RR_I is residual error rate of integrity errors;

RR_A is residual error rate of authenticity errors;

RR_T is residual error rate of timeliness errors;

RR_M is residual error rate of masquerade errors.

The final network PFH value of the safety communication channel depends on how it is configured, e.g. point-to-point or multipoint, EPI_Timeout Multiplier and Ping Interval EPI Multiplier settings. With all settings in valid ranges as defined within this specification, the worst case PFH value of the safety communication channel (λ_{SC}) using Extended Format is $5{,}00 \times 10^{-10}$ per hour.

The overall PFH of each FSCP 2/1 device shall incorporate the worst-case network PFH value $5{,}00 \times 10^{-10}$ per hour. There is no need for additional Network PFH calculation.

9.5.3 Bit Error Rate (BER)

9.5.3.1 General

IEC 61784-3 requires a bit error rate (BER) of 0,01 be used in PDF/PFH calculations unless evidence is given that this BER is not practical. A BER of 0,01 means that 1 of every 100 bits transmitted is transmitted incorrectly. This of course, is an unrealistic condition for an industrial control system network where availability needs to be maintained.

9.5.3.2 CP 2/3 BER

The minimum packet size used in FSCP 2/1 on CP 2/3 is 108 bits. CP 2/3 has extensive error confinement and all nodes on a CP 2/3 system check all messages at every transmission. In the presence of persistent errors a CP 2/3 device will bus-off (i.e. the node ceases all network activity) and remain in the bus-off state until power cycled. Because of the extensive and diverse checking and the mandatory error handling a CP 2/3 system will stop operating in the presence of high bit errors. It can be shown that a CP 2/3 network will not operate with a BER above 0,001. The inability to operate is true for both CP 2/3 and FSCP 2/1.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

9.5.3.3 CP 2/2 BER

The minimum packet size for a FSCP 2/1 on CP 2/2 is 720 bits, which is much larger than the 108 bits on CP 2/3. Like CP 2/3, CP 2/2 will not operate with a BER above 0,001, though the checking mechanism is different in the case of CP 2/2. CP 2/2 uses the time expectation mechanism inherent in the FSCP 2/1 protocol to ensure messages are delivered on time. If a correct message is not delivered, within the expectation period, the connection will closed and the device will go to the safety state. If high BER (above 0,001) are present, the safety connection will be closed and the network will not be able to operate. It simply will not be available.

Rational for setting maximum BER at 0,001 for CP 2/2:

a) If the percent of packets not delivered correctly was high enough, some messages would not be delivered before the connection would time-out.

b) If the connections timed out frequently, the network would not be available and could not be used.

c) If a network is not available, it is in a safe condition.

9.5.3.4 Summary

A BER < 0,001 will cause the safety protocol to exceed the maximum 7 RPI time limit frequently enough for the network not to be available for practical use, therefore BER = 0,001 was used for all calculations.

9.6 Maintenance

There are no special maintenance requirements for this protocol.

9.7 Safety manual

Implementers of this document shall supply a safety manual with following information at a minimum:

a) The safety manual shall inform the users of constraints for calculation of system characteristics, see 9.5.

b) The safety manuals shall inform the users of their responsibilities in the proper parameterization of the device, see 8.9.

c) The safety manuals shall provide warning on the proper usage of LEDs, see 9.1.4.

In addition to the requirements of this Subclause 9.7 the safety manual shall follow all requirements in IEC 61508.

10 Assessment

It is highly recommended that implementers of FSCP 2/1 obtain verification for all functional safety aspects of the product, both the protocol and any application, in accordance with the independence and competence requirements of IEC 61508-1:2010, Clause 8. It is highly recommended that implementers of FSCP 2/1 obtain proof that a suitable assessment test has been performed.

NOTE Further information for assessment of FSCP 2/1 devices can be obtained from the organizations listed in Annex B.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Annex A
(informative)

Additional information for functional safety communication profiles of CPF 2

A.1 Hash function example code

```
#include "stdio.h"      //for printf
#include "memory.h"     //for memcmp

#define CRCS1_POLYNOMIAL  0x37
#define CRCS2_POLYNOMIAL  0x3b
#define CRCS3_POLYNOMIAL  0x080F
#define CRC32_POLYNOMIAL  0xedb88320  // not 0x04C11DB7
#define CRCS5_POLYNOMIAL  0x5D6DCB


// CRC32 (CRC-S4)
// polynomial 0xedb88320 = standard CRC-32 bit reversed from the
regular
// published polynomial of 0x04c11db7. This table should be used to
// replicate standard Ethernet CRC hardware algorithm. Thus the
software
// implementation of the Ethernet CRC should produce the same result
as the
// hardware. This table was generated via right shifting the LSB of
each
// byte
const unsigned long CRC32Table[256] =
{
0x00000000, 0x77073096, 0xEE0E612C, 0x990951BA,
0x076DC419, 0x706AF48F, 0xE963A535, 0x9E6495A3,
0x0EDB8832, 0x79DCB8A4, 0xE0D5E91E, 0x97D2D988,
0x09B64C2B, 0x7EB17CBD, 0xE7B82D07, 0x90BF1D91,
0x1DB71064, 0x6AB020F2, 0xF3B97148, 0x84BE41DE,
0x1ADAD47D, 0x6DDDE4EB, 0xF4D4B551, 0x83D385C7,
0x136C9856, 0x646BA8C0, 0xFD62F97A, 0x8A65C9EC,
0x14015C4F, 0x63066CD9, 0xFA0F3D63, 0x8D080DF5,
0x3B6E20C8, 0x4C69105E, 0xD56041E4, 0xA2677172,
0x3C03E4D1, 0x4B04D447, 0xD20D85FD, 0xA50AB56B,
0x35B5A8FA, 0x42B2986C, 0xDBBBC9D6, 0xACBCF940,
0x32D86CE3, 0x45DF5C75, 0xDCD60DCF, 0xABD13D59,
0x26D930AC, 0x51DE003A, 0xC8D75180, 0xBFD06116,
0x21B4F4B5, 0x56B3C423, 0xCFBA9599, 0xB8BDA50F,
0x2802B89E, 0x5F058808, 0xC60CD9B2, 0xB10BE924,
0x2F6F7C87, 0x58684C11, 0xC1611DAB, 0xB6662D3D,
0x76DC4190, 0x01DB7106, 0x98D220BC, 0xEFD5102A,
0x71B18589, 0x06B6B51F, 0x9FBFE4A5, 0xE8B8D433,
0x7807C9A2, 0x0F00F934, 0x9609A88E, 0xE10E9818,
0x7F6A0DBB, 0x086D3D2D, 0x91646C97, 0xE6635C01,
0x6B6B51F4, 0x1C6C6162, 0x856530D8, 0xF262004E,
0x6C0695ED, 0x1B01A57B, 0x8208F4C1, 0xF50FC457,
0x65B0D9C6, 0x12B7E950, 0x8BBEB8EA, 0xFCB9887C,
0x62DD1DDF, 0x15DA2D49, 0x8CD37CF3, 0xFBD44C65,
0x4DB26158, 0x3AB551CE, 0xA3BC0074, 0xD4BB30E2,
0x4ADFA541, 0x3DD895D7, 0xA4D1C46D, 0xD3D6F4FB,
0x4369E96A, 0x346ED9FC, 0xAD678846, 0xDA60B8D0,
0x44042D73, 0x33031DE5, 0xAA0A4C5F, 0xDD0D7CC9,
0x5005713C, 0x270241AA, 0xBE0B1010, 0xC90C2086,
0x5768B525, 0x206F85B3, 0xB966D409, 0xCE61E49F,
```

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

```
0x5EDEF90E, 0x29D9C998, 0xB0D09822, 0xC7D7A8B4,
0x59B33D17, 0x2EB40D81, 0xB7BD5C3B, 0xC0BA6CAD,
0xEDB88320, 0x9ABFB3B6, 0x03B6E20C, 0x74B1D29A,
0xEAD54739, 0x9DD277AF, 0x04DB2615, 0x73DC1683,
0xE3630B12, 0x94643B84, 0x0D6D6A3E, 0x7A6A5AA8,
0xE40ECF0B, 0x9309FF9D, 0x0A00AE27, 0x7D079EB1,
0xF00F9344, 0x8708A3D2, 0x1E01F268, 0x6906C2FE,
0xF762575D, 0x806567CB, 0x196C3671, 0x6E6B06E7,
0xFED41B76, 0x89D32BE0, 0x10DA7A5A, 0x67DD4ACC,
0xF9B9DF6F, 0x8EBEEFF9, 0x17B7BE43, 0x60B08ED5,
0xD6D6A3E8, 0xA1D1937E, 0x38D8C2C4, 0x4FDFF252,
0xD1BB67F1, 0xA6BC5767, 0x3FB506DD, 0x48B2364B,
0xD80D2BDA, 0xAF0A1B4C, 0x36034AF6, 0x41047A60,
0xDF60EFC3, 0xA867DF55, 0x316E8EEF, 0x4669BE79,
0xCB61B38C, 0xBC66831A, 0x256FD2A0, 0x5268E236,
0xCC0C7795, 0xBB0B4703, 0x220216B9, 0x5505262F,
0xC5BA3BBE, 0xB2BD0B28, 0x2BB45A92, 0x5CB36A04,
0xC2D7FFA7, 0xB5D0CF31, 0x2CD99E8B, 0x5BDEAE1D,
0x9B64C2B0, 0xEC63F226, 0x756AA39C, 0x026D930A,
0x9C0906A9, 0xEB0E363F, 0x72076785, 0x05005713,
0x95BF4A82, 0xE2B87A14, 0x7BB12BAE, 0x0CB61B38,
0x92D28E9B, 0xE5D5BE0D, 0x7CDCEFB7, 0x0BDBDF21,
0x86D3D2D4, 0xF1D4E242, 0x68DDB3F8, 0x1FDA836E,
0x81BE16CD, 0xF6B9265B, 0x6FB077E1, 0x18B74777,
0x88085AE6, 0xFF0F6A70, 0x66063BCA, 0x11010B5C,
0x8F659EFF, 0xF862AE69, 0x616BFFD3, 0x166CCF45,
0xA00AE278, 0xD70DD2EE, 0x4E048354, 0x3903B3C2,
0xA7672661, 0xD06016F7, 0x4969474D, 0x3E6E77DB,
0xAED16A4A, 0xD9D65ADC, 0x40DF0B66, 0x37D83BF0,
0xA9BCAE53, 0xDEBB9EC5, 0x47B2CF7F, 0x30B5FFE9,
0xBDBDF21C, 0xCABAC28A, 0x53B39330, 0x24B4A3A6,
0xBAD03605, 0xCDD70693, 0x54DE5729, 0x23D967BF,
0xB3667A2E, 0xC4614AB8, 0x5D681B02, 0x2A6F2B94,
0xB40BBE37, 0xC30C8EA1, 0x5A05DF1B, 0x2D02EF8D
};

//CRCS3_POLYNOMIAL = 0x080F
//This table was generated via left shifting the MSB of each byte
const unsigned short CRC16Table[256] =
{
0x0000, 0x080F, 0x101E, 0x1811, 0x203C, 0x2833, 0x3022, 0x382D,
0x4078, 0x4877, 0x5066, 0x5869, 0x6044, 0x684B, 0x705A, 0x7855,
0x80F0, 0x88FF, 0x90EE, 0x98E1, 0xA0CC, 0xA8C3, 0xB0D2, 0xB8DD,
0xC088, 0xC887, 0xD096, 0xD899, 0xE0B4, 0xE8BB, 0xF0AA, 0xF8A5,
0x09EF, 0x01E0, 0x19F1, 0x11FE, 0x29D3, 0x21DC, 0x39CD, 0x31C2,
0x4997, 0x4198, 0x5989, 0x5186, 0x69AB, 0x61A4, 0x79B5, 0x71BA,
0x891F, 0x8110, 0x9901, 0x910E, 0xA923, 0xA12C, 0xB93D, 0xB132,
0xC967, 0xC168, 0xD979, 0xD176, 0xE95B, 0xE154, 0xF945, 0xF14A,
0x13DE, 0x1BD1, 0x03C0, 0x0BCF, 0x33E2, 0x3BED, 0x23FC, 0x2BF3,
0x53A6, 0x5BA9, 0x43B8, 0x4BB7, 0x739A, 0x7B95, 0x6384, 0x6B8B,
0x932E, 0x9B21, 0x8330, 0x8B3F, 0xB312, 0xBB1D, 0xA30C, 0xAB03,
0xD356, 0xDB59, 0xC348, 0xCB47, 0xF36A, 0xFB65, 0xE374, 0xEB7B,
0x1A31, 0x123E, 0x0A2F, 0x0220, 0x3A0D, 0x3202, 0x2A13, 0x221C,
0x5A49, 0x5246, 0x4A57, 0x4258, 0x7A75, 0x727A, 0x6A6B, 0x6264,
0x9AC1, 0x92CE, 0x8ADF, 0x82D0, 0xBAFD, 0xB2F2, 0xAAE3, 0xA2EC,
0xDAB9, 0xD2B6, 0xCAA7, 0xC2A8, 0xFA85, 0xF28A, 0xEA9B, 0xE294,
0x27BC, 0x2FB3, 0x37A2, 0x3FAD, 0x0780, 0x0F8F, 0x179E, 0x1F91,
0x67C4, 0x6FCB, 0x77DA, 0x7FD5, 0x47F8, 0x4FF7, 0x57E6, 0x5FE9,
0xA74C, 0xAF43, 0xB752, 0xBF5D, 0x8770, 0x8F7F, 0x976E, 0x9F61,
0xE734, 0xEF3B, 0xF72A, 0xFF25, 0xC708, 0xCF07, 0xD716, 0xDF19,
0x2E53, 0x265C, 0x3E4D, 0x3642, 0x0E6F, 0x0660, 0x1E71, 0x167E,
0x6E2B, 0x6624, 0x7E35, 0x763A, 0x4E17, 0x4618, 0x5E09, 0x5606,
0xAEA3, 0xA6AC, 0xBEBD, 0xB6B2, 0x8E9F, 0x8690, 0x9E81, 0x968E,
```

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

```
0xEEDB, 0xE6D4, 0xFEC5, 0xF6CA, 0xCEE7, 0xC6E8, 0xDEF9, 0xD6F6,
0x3462, 0x3C6D, 0x247C, 0x2C73, 0x145E, 0x1C51, 0x0440, 0x0C4F,
0x741A, 0x7C15, 0x6404, 0x6C0B, 0x5426, 0x5C29, 0x4438, 0x4C37,
0xB492, 0xBC9D, 0xA48C, 0xAC83, 0x94AE, 0x9CA1, 0x84B0, 0x8CBF,
0xF4EA, 0xFCE5, 0xE4F4, 0xECFB, 0xD4D6, 0xDCD9, 0xC4C8, 0xCCC7,
0x3D8D, 0x3582, 0x2D93, 0x259C, 0x1DB1, 0x15BE, 0x0DAF, 0x05A0,
0x7DF5, 0x75FA, 0x6DEB, 0x65E4, 0x5DC9, 0x55C6, 0x4DD7, 0x45D8,
0xBD7D, 0xB572, 0xAD63, 0xA56C, 0x9D41, 0x954E, 0x8D5F, 0x8550,
0xFD05, 0xF50A, 0xED1B, 0xE514, 0xDD39, 0xD536, 0xCD27, 0xC528
};

//CRCS1_POLYNOMIAL=0x37
//This table was generated via left shifting the MSB of each byte
const unsigned char CRC8Table37[256] =
{
0x00, 0x37, 0x6e, 0x59, 0xdc, 0xeb, 0xb2, 0x85,
0x8f, 0xb8, 0xe1, 0xd6, 0x53, 0x64, 0x3d, 0x0a,
0x29, 0x1e, 0x47, 0x70, 0xf5, 0xc2, 0x9b, 0xac,
0xa6, 0x91, 0xc8, 0xff, 0x7a, 0x4d, 0x14, 0x23,
0x52, 0x65, 0x3c, 0x0b, 0x8e, 0xb9, 0xe0, 0xd7,
0xdd, 0xea, 0xb3, 0x84, 0x01, 0x36, 0x6f, 0x58,
0x7b, 0x4c, 0x15, 0x22, 0xa7, 0x90, 0xc9, 0xfe,
0xf4, 0xc3, 0x9a, 0xad, 0x28, 0x1f, 0x46, 0x71,
0xa4, 0x93, 0xca, 0xfd, 0x78, 0x4f, 0x16, 0x21,
0x2b, 0x1c, 0x45, 0x72, 0xf7, 0xc0, 0x99, 0xae,
0x8d, 0xba, 0xe3, 0xd4, 0x51, 0x66, 0x3f, 0x08,
0x02, 0x35, 0x6c, 0x5b, 0xde, 0xe9, 0xb0, 0x87,
0xf6, 0xc1, 0x98, 0xaf, 0x2a, 0x1d, 0x44, 0x73,
0x79, 0x4e, 0x17, 0x20, 0xa5, 0x92, 0xcb, 0xfc,
0xdf, 0xe8, 0xb1, 0x86, 0x03, 0x34, 0x6d, 0x5a,
0x50, 0x67, 0x3e, 0x09, 0x8c, 0xbb, 0xe2, 0xd5,
0x7f, 0x48, 0x11, 0x26, 0xa3, 0x94, 0xcd, 0xfa,
0xf0, 0xc7, 0x9e, 0xa9, 0x2c, 0x1b, 0x42, 0x75,
0x56, 0x61, 0x38, 0x0f, 0x8a, 0xbd, 0xe4, 0xd3,
0xd9, 0xee, 0xb7, 0x80, 0x05, 0x32, 0x6b, 0x5c,
0x2d, 0x1a, 0x43, 0x74, 0xf1, 0xc6, 0x9f, 0xa8,
0xa2, 0x95, 0xcc, 0xfb, 0x7e, 0x49, 0x10, 0x27,
0x04, 0x33, 0x6a, 0x5d, 0xd8, 0xef, 0xb6, 0x81,
0x8b, 0xbc, 0xe5, 0xd2, 0x57, 0x60, 0x39, 0x0e,
0xdb, 0xec, 0xb5, 0x82, 0x07, 0x30, 0x69, 0x5e,
0x54, 0x63, 0x3a, 0x0d, 0x88, 0xbf, 0xe6, 0xd1,
0xf2, 0xc5, 0x9c, 0xab, 0x2e, 0x19, 0x40, 0x77,
0x7d, 0x4a, 0x13, 0x24, 0xa1, 0x96, 0xcf, 0xf8,
0x89, 0xbe, 0xe7, 0xd0, 0x55, 0x62, 0x3b, 0x0c,
0x06, 0x31, 0x68, 0x5f, 0xda, 0xed, 0xb4, 0x83,
0xa0, 0x97, 0xce, 0xf9, 0x7c, 0x4b, 0x12, 0x25,
0x2f, 0x18, 0x41, 0x76, 0xf3, 0xc4, 0x9d, 0xaa,
};

//CRCS2_POLYNOMIAL = 0x3b
//This table was generated via left shifting the MSB of each byte
const unsigned char CRC8Table3b[256] =
{
0x00, 0x3b, 0x76, 0x4d, 0xec, 0xd7, 0x9a, 0xa1,
0xe3, 0xd8, 0x95, 0xae, 0x0f, 0x34, 0x79, 0x42,
0xfd, 0xc6, 0x8b, 0xb0, 0x11, 0x2a, 0x67, 0x5c,
0x1e, 0x25, 0x68, 0x53, 0xf2, 0xc9, 0x84, 0xbf,
0xc1, 0xfa, 0xb7, 0x8c, 0x2d, 0x16, 0x5b, 0x60,
0x22, 0x19, 0x54, 0x6f, 0xce, 0xf5, 0xb8, 0x83,
0x3c, 0x07, 0x4a, 0x71, 0xd0, 0xeb, 0xa6, 0x9d,
0xdf, 0xe4, 0xa9, 0x92, 0x33, 0x08, 0x45, 0x7e,
0xb9, 0x82, 0xcf, 0xf4, 0x55, 0x6e, 0x23, 0x18,
0x5a, 0x61, 0x2c, 0x17, 0xb6, 0x8d, 0xc0, 0xfb,
```

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

```
0x44, 0x7f, 0x32, 0x09, 0xa8, 0x93, 0xde, 0xe5,
0xa7, 0x9c, 0xd1, 0xea, 0x4b, 0x70, 0x3d, 0x06,
0x78, 0x43, 0x0e, 0x35, 0x94, 0xaf, 0xe2, 0xd9,
0x9b, 0xa0, 0xed, 0xd6, 0x77, 0x4c, 0x01, 0x3a,
0x85, 0xbe, 0xf3, 0xc8, 0x69, 0x52, 0x1f, 0x24,
0x66, 0x5d, 0x10, 0x2b, 0x8a, 0xb1, 0xfc, 0xc7,
0x49, 0x72, 0x3f, 0x04, 0xa5, 0x9e, 0xd3, 0xe8,
0xaa, 0x91, 0xdc, 0xe7, 0x46, 0x7d, 0x30, 0x0b,
0xb4, 0x8f, 0xc2, 0xf9, 0x58, 0x63, 0x2e, 0x15,
0x57, 0x6c, 0x21, 0x1a, 0xbb, 0x80, 0xcd, 0xf6,
0x88, 0xb3, 0xfe, 0xc5, 0x64, 0x5f, 0x12, 0x29,
0x6b, 0x50, 0x1d, 0x26, 0x87, 0xbc, 0xf1, 0xca,
0x75, 0x4e, 0x03, 0x38, 0x99, 0xa2, 0xef, 0xd4,
0x96, 0xad, 0xe0, 0xdb, 0x7a, 0x41, 0x0c, 0x37,
0xf0, 0xcb, 0x86, 0xbd, 0x1c, 0x27, 0x6a, 0x51,
0x13, 0x28, 0x65, 0x5e, 0xff, 0xc4, 0x89, 0xb2,
0x0d, 0x36, 0x7b, 0x40, 0xe1, 0xda, 0x97, 0xac,
0xee, 0xd5, 0x98, 0xa3, 0x02, 0x39, 0x74, 0x4f,
0x31, 0x0a, 0x47, 0x7c, 0xdd, 0xe6, 0xab, 0x90,
0xd2, 0xe9, 0xa4, 0x9f, 0x3e, 0x05, 0x48, 0x73,
0xcc, 0xf7, 0xba, 0x81, 0x20, 0x1b, 0x56, 0x6d,
0x2f, 0x14, 0x59, 0x62, 0xc3, 0xf8, 0xb5, 0x8e,
};

// polynominal 0x5D6DCB
// This table was generated via left shifting the MSB of each byte and
appending an
// additional byte to form a long word value. The MSB of the table
value will
// always be zero
const unsigned long CRCS5Table[256] =
{
0x00000000, 0x005d6dcb, 0x00badb96, 0x00e7b65d,
0x0028dae7, 0x0075b72c, 0x00920171, 0x00cf6cba,
0x0051b5ce, 0x000cd805, 0x00eb6e58, 0x00b60393,
0x00796f29, 0x002402e2, 0x00c3b4bf, 0x009ed974,
0x00a36b9c, 0x00fe0657, 0x0019b00a, 0x0044ddc1,
0x008bb17b, 0x00d6dcb0, 0x00316aed, 0x006c0726,
0x00f2de52, 0x00afb399, 0x004805c4, 0x0015680f,
0x00da04b5, 0x0087697e, 0x0060df23, 0x003db2e8,
0x001bbaf3, 0x0046d738, 0x00a16165, 0x00fc0cae,
0x00336014, 0x006e0ddf, 0x0089bb82, 0x00d4d649,
0x004a0f3d, 0x001762f6, 0x00f0d4ab, 0x00adb960,
0x0062d5da, 0x003fb811, 0x00d80e4c, 0x00856387,
0x00b8d16f, 0x00e5bca4, 0x00020af9, 0x005f6732,
0x00900b88, 0x00cd6643, 0x002ad01e, 0x0077bdd5,
0x00e964a1, 0x00b4096a, 0x0053bf37, 0x000ed2fc,
0x00c1be46, 0x009cd38d, 0x007b65d0, 0x0026081b,
0x003775e6, 0x006a182d, 0x008dae70, 0x00d0c3bb,
0x001faf01, 0x0042c2ca, 0x00a57497, 0x00f8195c,
0x0066c028, 0x003bade3, 0x00dc1bbe, 0x00817675,
0x004e1acf, 0x00137704, 0x00f4c159, 0x00a9ac92,
0x00941e7a, 0x00c973b1, 0x002ec5ec, 0x0073a827,
0x00bcc49d, 0x00e1a956, 0x00061f0b, 0x005b72c0,
0x00c5abb4, 0x0098c67f, 0x007f7022, 0x00221de9,
0x00ed7153, 0x00b01c98, 0x0057aac5, 0x000ac70e,
0x002ccf15, 0x0071a2de, 0x00961483, 0x00cb7948,
0x000415f2, 0x00597839, 0x00bece64, 0x00e3a3af,
0x007d7adb, 0x00201710, 0x00c7a14d, 0x009acc86,
0x0055a03c, 0x0008cdf7, 0x00ef7baa, 0x00b21661,
0x008fa489, 0x00d2c942, 0x00357f1f, 0x006812d4,
0x00a77e6e, 0x00fa13a5, 0x001da5f8, 0x0040c833,
0x00de1147, 0x00837c8c, 0x0064cad1, 0x0039a71a,
```

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

```
0x00f6cba0, 0x00aba66b, 0x004c1036, 0x00117dfd,
0x006eebcc, 0x00338607, 0x00d4305a, 0x00895d91,
0x0046312b, 0x001b5ce0, 0x00fceabd, 0x00a18776,
0x003f5e02, 0x006233c9, 0x00858594, 0x00d8e85f,
0x001784e5, 0x004ae92e, 0x00ad5f73, 0x00f032b8,
0x00cd8050, 0x0090ed9b, 0x00775bc6, 0x002a360d,
0x00e55ab7, 0x00b8377c, 0x005f8121, 0x0002ecea,
0x009c359e, 0x00c15855, 0x0026ee08, 0x007b83c3,
0x00b4ef79, 0x00e982b2, 0x000e34ef, 0x00535924,
0x0075513f, 0x00283cf4, 0x00cf8aa9, 0x0092e762,
0x005d8bd8, 0x0000e613, 0x00e7504e, 0x00ba3d85,
0x0024e4f1, 0x0079893a, 0x009e3f67, 0x00c352ac,
0x000c3e16, 0x005153dd, 0x00b6e580, 0x00eb884b,
0x00d63aa3, 0x008b5768, 0x006ce135, 0x00318cfe,
0x00fee044, 0x00a38d8f, 0x00443bd2, 0x00195619,
0x00878f6d, 0x00dae2a6, 0x003d54fb, 0x00603930,
0x00af558a, 0x00f23841, 0x00158e1c, 0x0048e3d7,
0x00599e2a, 0x0004f3e1, 0x00e345bc, 0x00be2877,
0x007144cd, 0x002c2906, 0x00cb9f5b, 0x0096f290,
0x00082be4, 0x0055462f, 0x00b2f072, 0x00ef9db9,
0x0020f103, 0x007d9cc8, 0x009a2a95, 0x00c7475e,
0x00faf5b6, 0x00a7987d, 0x00402e20, 0x001d43eb,
0x00d22f51, 0x008f429a, 0x0068f4c7, 0x0035990c,
0x00ab4078, 0x00f62db3, 0x00119bee, 0x004cf625,
0x00839a9f, 0x00def754, 0x00394109, 0x00642cc2,
0x004224d9, 0x001f4912, 0x00f8ff4f, 0x00a59284,
0x006afe3e, 0x003793f5, 0x00d025a8, 0x008d4863,
0x00139117, 0x004efcdc, 0x00a94a81, 0x00f4274a,
0x003b4bf0, 0x0066263b, 0x00819066, 0x00dcfdad,
0x00e14f45, 0x00bc228e, 0x005b94d3, 0x0006f918,
0x00c995a2, 0x0094f869, 0x00734e34, 0x002e23ff,
0x00b0fa8b, 0x00ed9740, 0x000a211d, 0x00574cd6,
0x0098206c, 0x00c54da7, 0x0022f6fa, 0x007f9631
};


/×× GetCRC32Ethernet

    \par Purpose:
    CRC32 calculation routine for polynomial 0xedb88320 which is bit
reversed
    from the regular polynomial of 0x04c11db7 thus the (crc >> 8)
below
    is right shifted.

    \note
    Doing incremental crc calculation is done with providing the
result
    from the previous block with preset.

    \note
    Restrictions:
        len > 0
        pStart points to valid memory with at least len bytes in size

    \param Input: \b pStart     Starting address to compute CRC over
    \param Input: \b len        Number of bytes
    \param Input: \b preset     Preset value for CRC

×/
unsigned long GetCRC32Ethernet(const void ×pStart, int len, unsigned
long preset)
{
```

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

```
    unsigned long crc = preset;
    unsigned char *buf = (unsigned char *)pStart;

    while (len-- > 0)
    {
        unsigned char data8 = *buf++;
        crc = CRC32Table[(crc ^ data8) & 0xff] ^ (crc >> 8);
    }
    return crc;
}   //GetCRC32Ethernet


/** ComputeCRCS1

    \par Purpose:
    CRC8 calculation routine for polynomial 0x37.
    Note that the CRC8Table37 was computed via left shift operations.

    \note
    Doing incremental crc calculation is done with providing the
result
    from the previous block with preset.

    \note
    Restrictions:
        len > 0
        pStart points to valid memory with at least len bytes in size

    \par Scope: public

    \param Input: \b pStart     Starting address to compute CRC over
    \param Input: \b len        Number of bytes
    \param Input: \b preset     Preset value for CRC

    \par Edit History:
*/
unsigned char ComputeCRCS1(const void *pStart, int len, unsigned char
preset)
{
    unsigned char crc = preset;
    unsigned char *buf = (unsigned char *)pStart;

      while (len-- > 0)
      {
          crc = CRC8Table37[(crc ^ *buf++)];
      }
      return (crc);
}   //ComputeCRCS1



/** ComputeCRCS2

    \par Purpose:
    CRC8 calculation routine for polynomial 0x3b.
    Note that the CRC8Table3b was computed via left shift operations.

    \note
    Doing incremental crc calculation is done with providing the
result
    from the previous block with preset.

    \note
```

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

```
    Restrictions:
        len > 0
        pStart points to valid memory with at least len bytes in size

    \par Scope: public

    \param Input: \b pStart     Starting address to compute CRC over
    \param Input: \b len        Number of bytes
    \param Input: \b preset     Preset value for CRC

    \par Edit History:
×/
unsigned char ComputeCRCS2(const void ×pStart, int len, unsigned char
preset)
{
    unsigned char crc = preset;
    unsigned char ×buf = (unsigned char ×)pStart;

      while (len-- > 0)
      {
            crc = CRC8Table3b[(crc ^ ×buf++)];
      }
      return (crc);
}   //ComputeCRCS2


/×× ComputeCRCS3

    \par Purpose:
    CRC16 calculation routine for polynomial 0x080F.
    The CRC16Table was computed via left shift operations and thus
will do
    a (crc << 8).

    \note
    Doing incremental crc calculation is done with providing the
result
    from the previous block with preset.

    \note
    Restrictions:
        len > 0
        pStart points to valid memory with at least len bytes in size

    \param Input: \b pStart     Starting address to compute CRC over
    \param Input: \b len        Number of bytes
    \param Input: \b preset     Preset value for CRC

×/
unsigned short ComputeCRCS3(const void ×pStart, int len, unsigned
short preset)
{
    unsigned short crc = preset;
    unsigned char ×buf = (unsigned char ×)pStart;

      while (len-- > 0)
      {
        unsigned char data = ×buf++;
        crc = CRC16Table[((crc >> 8) ^ data)] ^ (crc << 8);
      }
      return (crc);
}   //ComputeCRCS3
```

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

```
/×× ComputeCRCS3Ref4

    \par Purpose:
    Compute crc given 4 bytes of data and a preset for the crc.
    This assumes the input data is stored in native (little or big)
    endian format.

    \par Scope: public

    \param Input: \b data       Value to compute CRC on
    \param Input: \b preset     Preset value for CRC

    \par Edit History:
×/
unsigned short ComputeCRCS3Ref4(unsigned long data, unsigned short
preset)
{
    unsigned short crc = preset;
    crc = CRC16Table[(crc >> 8) ^ (data&0xff)]       ^ (crc << 8);
    crc = CRC16Table[(crc >> 8) ^ ((data>>8)&0xff)]  ^ (crc << 8);
    crc = CRC16Table[(crc >> 8) ^ ((data>>16)&0xff)] ^ (crc << 8);
    crc = CRC16Table[(crc >> 8) ^ ((data>>24)&0xff)] ^ (crc << 8);
    return crc;
}

/×× ComputeCRCS3Ref2

    \par Purpose:
    Compute crc given 2 bytes of data and a preset for the crc.
    This assumes the input data is stored in native (little or big)
endian format.

    \par Scope: public

    \param Input: \b data       Value to compute CRC on
    \param Input: \b preset     Preset value for CRC

    \par Edit History:
×/
unsigned short ComputeCRCS3Ref2(unsigned short data, unsigned short
preset)
{
    unsigned short crc = preset;
    crc = CRC16Table[(crc >> 8) ^ (data&0xff)]       ^ (crc << 8);
    crc = CRC16Table[(crc >> 8) ^ ((data>>8)&0xff)]  ^ (crc << 8);
    return crc;
}

/** ComputeCRCS5

    \par Purpose:
    CRCS5 calculation routine for polynomial 0x5D6DCB.
    The CRCS5Table was computed via left shift operations and thus
    will do a (crc << 8).
    \note
    Doing incremental crc calculation is done with providing the
    Result from the previous block with preset.

    \note
    Restrictions:
    len > 0
    pStart points to valid memory with at least len bytes in size.
```

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

```
    CRC value returned is a long with the MSB = 0

    \param Input: \b pStart     Starting address to compute CRC over
    \param Input: \b len        Number of bytes
    \param Input: \b preset     Preset value for CRC (unsigned long)

*/
unsigned long ComputeCRCS24(const void *pStart, int len, unsigned long
preset)
{
     unsigned long crc = preset;
     unsigned long temp;
     unsigned char *buf = (unsigned char *)pStart;

     while (len-- > 0)
     {
          unsigned char data = *buf++;
          // XOR data with CRC2, look up result, then XOR with CRC;
          crc = CRCS5Table[((crc >> 16) ^ data)&0xff] ^ (crc << 8);
      }
      return (crc & 0x00ffffff);
}   //ComputeCRCS5

/×× ComputeCRCS3Ref1

    \par Purpose:
    Compute crc given 1 bytes of data and a preset for the crc.

    \par Scope: public

    \param Input: \b data       Value to compute CRC on
    \param Input: \b preset     Preset value for CRC

    \par Edit History:
×/
unsigned short ComputeCRCS3Ref1(unsigned char data, unsigned short
preset)
{
    unsigned short crc = preset;
    crc = CRC16Table[(crc >> 8) ^ data] ^ (crc << 8);
    return crc;
}


//The following routines were used to generate the above tables.
//Just as a sanity check, rerun the calculations and test that the
//tables are correct
unsigned char  CRC8Table37Ref[256];
unsigned char  CRC8Table3bRef[256];
unsigned short CRC16TableRef[256];
unsigned long  CRC32TableRef[256];
unsigned long  CRCS5TableRef[256];

//left shift MSB
static void InitSafetyCRC8Table()
{
    unsigned short j;
    unsigned char i;
    unsigned char carry8=0;
    unsigned char entry8=0;

    //CRCS1_POLYNOMIAL
    for (j = 0; j < 256; j++)
```

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

```
    {
        entry8 = static_cast<unsigned char>(j);
        for (i = 0; i < 8; ++i)
        {
            carry8 = entry8 & 0x80;     // carry8 is the most
significant bit
            entry8 = entry8 << 1;
            if (carry8)               // if carry8 is nonzero
            {
                entry8 = entry8 ^ CRCS1_POLYNOMIAL;    // XOR by CRC
polynom
            }
        }
        CRC8Table37Ref[j] = entry8;
    }
    //CRCS2_POLYNOMIAL
    for (j = 0; j < 256; j++)
    {
        entry8 = static_cast<unsigned char>(j);
        for (i = 0; i < 8; ++i)
        {
            carry8 = entry8 & 0x80;     // carry8 is the most
significant bit
            entry8 = entry8 << 1;
            if (carry8)               // if carry8 is nonzero
            {
                entry8 = entry8 ^ CRCS2_POLYNOMIAL;    // XOR by CRC
polynom
            }
       }
        CRC8Table3bRef[j] = entry8;
    }
}  // end of initSafetyCRCTable8bit

//left shift MSB
static void InitSafetyCRC16Table()
{
    unsigned short j;
    unsigned char i;
    unsigned short carry16=0;
    unsigned short entry16=0;

    for (j = 0; j < 256; j++)
    {
        entry16 = j;
        for (i = 0; i < 16; ++i)
        {
            carry16 = entry16 & 0x8000;     // carry16 is the lowest
                                            // significant bit
            entry16 = entry16 << 1;
            if (carry16)               // if carry16 is nonzero
            {
                entry16 = entry16 ^ CRCS3_POLYNOMIAL;    // XOR by CRC
polynom
            }
        }
        CRC16TableRef[j] = entry16;
    }
}  // end of initSafetyCRC16Table()

//right shift LSB
static void InitSafetyCRC32Table()
{
```

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

```
    unsigned long j;
    unsigned char i;
    unsigned long carry32=0;
    unsigned long entry32=0;

    //right shift
    for (j = 0; j < 256; j++)
    {
        entry32 = j;
        for (i = 0; i < 8; ++i)
        {
            carry32 = entry32 & 1;      // carry16 is the lowest
                                        // significant bit
            entry32 = entry32 >> 1;
            if (carry32)                // if carry16 is nonzero
            {
                entry32 = entry32 ^ CRC32_POLYNOMIAL;     // XOR by
                                                          // CRC
polynom
            }
        }
        CRC32TableRef[j] = entry32;
    }
}  // end of initSafetyCRC32Table()


//left shift MSB
static void InitSafetyCRCS5Table()
{
   unsigned short j;
    unsigned char i;
    unsigned long carry24=0;
    unsigned long entry24=0;
    unsigned long poly = unsigned long(CRCS5_POLYNOMIAL);

    for (j = 0; j < 256; j++)
    {
        entry24 = (j<<16);
        for (i = 0; i < 8; ++i)
        {
            carry24 = entry24 & 0x800000;     // carry24 is the most
significant bit
            entry24 = entry24 << 1;
            if (carry24)                // if carry24 is nonzero
            {
                entry24 = entry24 ^ poly;    // XOR by CRC polynom
            }
        }
        CRCS5TableRef[j] = entry24 & 0x00ffffff;   // Upper byte is
don't care
    }
}  // end of initSafetyCRCS5Table()


//This is the reference model that the table driven routine shall
match
unsigned char Crc8ComputeSlow(const void× buffer, unsigned int count,
unsigned char poly, unsigned char preset)
{
    const unsigned char× ptr = (const unsigned char ×) buffer;
    unsigned char crc8=preset;
    unsigned char value=0;
```

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

```
    while (count--)
    {
        value = *ptr++;
        crc8 ^= value;
        for (int i = 0; i < 8; i++)
        {
            if (crc8 & 0x80)
            {
                crc8 = (crc8 << 1) ^ poly;
            }
            else
            {
                crc8 <<= 1;
            }
        }
    }
    return crc8;
}   //Crc8ComputeSlow

//This is the reference model that the table driven routine shall
match
unsigned short Crc16ComputeSlow(const void* buffer, unsigned int
count, unsigned short poly, unsigned short preset)
{
    const unsigned char* ptr = (const unsigned char *) buffer;
    unsigned short crc16=preset;
    unsigned short value=0;

    while (count--)
    {
        value = *ptr++;
        crc16 ^= (value << 8);
        for (int i = 0; i < 8; i++)
        {
            if (crc16 & 0x8000)
            {
                crc16 = (crc16 << 1) ^ poly;
            }
            else
            {
                crc16 <<= 1;
            }
        }
    }
    return crc16;
}   //Crc16ComputeSlow


//This is the reference model that the table driven routine shall
match
unsigned long Crc32ComputeSlow(const void* buffer, unsigned int count,
unsigned long poly, unsigned long preset)
{
    const unsigned char* ptr = (const unsigned char *) buffer;
    unsigned long crc32=preset;
    unsigned long value=0;

    while (count--)
    {
        value = *ptr++;
        crc32 ^= (value);
        for (int i = 0; i < 8; i++)
        {
```

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

```
            if (crc32 & 1)
            {
                crc32 = (crc32 >> 1) ^ poly;
            }
            else
            {
                crc32 >>= 1;
            }
        }
    }
    return crc32;
}   //Crc32ComputeSlow

//This is the reference model that the table driven routine shall
match
unsigned long CRCS5ComputeSlow(const void* buffer, unsigned int count,
unsigned long poly, unsigned long preset)
{
    const unsigned char* ptr = (const unsigned char *) buffer;
    unsigned long CRCS5 = preset;
    unsigned long value=0;

    while (count--)
    {
        value = *ptr++;
        CRCS5 ^= (value << 16);
        for (int i = 0; i < 8; i++)
        {
            if (CRCS5 & 0x800000)
            {
                CRCS5 = (CRCS5 << 1) ^ poly;

            }
            else
            {
                CRCS5 <<= 1;
            }
        }
    }
    return (CRCS5 & 0x00ffffff);
}   //CRCS5ComputeSlow


//define a structure such that it is 9 bytes long in packed format
//so as to equal the crc test string length (in DoCrcTest below)
struct SomeStruct
{
    unsigned char  aByte1;
    unsigned char  aByte2;
    unsigned char  aByte3;
    unsigned short aShort;
    unsigned long  aLong;
};


int DoCrcTest()
{
    const char *string = "123456789";
    int len = 9;            //length of "123456789"
    unsigned long  crc32;
    unsigned short crc16;
    unsigned char  crc8;
    SomeStruct aStruct;
```

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

```
    //fill aStruct with equivalent to "123456789" in
    //little endian memory order
    aStruct.aByte1  = 0x31;
    aStruct.aByte2  = 0x32;
    aStruct.aByte3  = 0x33;
    aStruct.aShort = 0x3534;
    aStruct.aLong  = 0x39383736;
    int crcMatch = 0;


    //the slow methods serve as the reference implementation
    //all other optimizations (ie table driven) shall match these
    crc8 = Crc8ComputeSlow(string, len, CRCS1_POLYNOMIAL, 0xff);
    if (crc8 != 0x4C)
    {
        crcMatch |= 1;
    }
    crc8 = Crc8ComputeSlow(string, len, CRCS2_POLYNOMIAL, 0xff);
    if (crc8 != 0xBF)
    {
        crcMatch |= 2;
    }
    crc16 = Crc16ComputeSlow(string, len, CRCS3_POLYNOMIAL, 0xffff);
    if (crc16 != 0x9516)
    {
        crcMatch |= 4;
    }

    crc32 = Crc32ComputeSlow(string, len, CRC32_POLYNOMIAL,
0xffffffff);
    if (crc32 != 0x340bc6d9)
    {
        crcMatch |= 8;
    }

    crc8 = ComputeCRCS1(string, len, 0xff);
    if (crc8 != 0x4C)
    {
        crcMatch |= 0x10;
    }
    crc8 = ComputeCRCS2(string, len, 0xff);
    if (crc8 != 0xBF)
    {
        crcMatch |= 0x20;
    }
    crc16 = ComputeCRCS3(string, len, 0xffff);
    if (crc16 != 0x9516)
    {
        crcMatch |= 0x40;
    }

    crc32 = GetCRC32Ethernet(string, len, 0xffffffff);
    if (crc32 != 0x340bc6d9)
    {
        crcMatch |= 0x80;
    }

    //retest that the tables are correct
    InitSafetyCRC8Table();
    InitSafetyCRC16Table();
    InitSafetyCRC32Table();
```

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

```
    if (memcmp(&CRC8Table37Ref[0], &CRC8Table37[0], 256) != 0)
    {
        crcMatch |= 0x200;
    }
    if (memcmp(&CRC8Table3bRef[0], &CRC8Table3b[0], 256) != 0)
    {
        crcMatch |= 0x400;
    }
    if (memcmp(&CRC16TableRef[0], &CRC16Table[0], 512) != 0)
    {
        crcMatch |= 0x800;
    }
    if (memcmp(&CRC32TableRef[0], &CRC32Table[0], 1024) != 0)
    {
        crcMatch |= 0x1000;
    }

    //should work on both big and little endian machine
    crc16 = 0xffff;
    crc16 = ComputeCRCS3Ref1(aStruct.aByte1, crc16);
    crc16 = ComputeCRCS3Ref1(aStruct.aByte2, crc16);
    crc16 = ComputeCRCS3Ref1(aStruct.aByte3, crc16);
    crc16 = ComputeCRCS3Ref2(aStruct.aShort, crc16);
    crc16 = ComputeCRCS3Ref4(aStruct.aLong,  crc16);
    if (crc16 != 0x9516)
    {
        crcMatch |= 0x2000;
    }

      return crcMatch;
}

int main(int argc, char× argv[])
{
    int result = DoCrcTest();
    if (result==0)
        printf("Tests passed!\n");
    else
        printf("Tests failed, result = 0x%x\n",result);
    return result;
}
```

A.2 Void

Void

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Annex B
(informative)

Information for assessment of the functional safety communication profiles of CPF 2

According to IEC rules, this document does not make a statement on how to validate conformance. However, test and validation of compliance of FSCP 2/1 devices with IEC 61784-3-2 may be required by law.

Corresponding information relative to the test and compliance with this document can be retrieved from the local National Committees of the IEC or from the relevant fieldbus organization.

NOTE For IEC 61784-3-2, the relevant fieldbus organization is ODVA, see www.odva.org.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Bibliography

[1] IEC 60050 (all parts), *International Electrotechnical Vocabulary (IEV)* (available at <http://www.electropedia.org/)

NOTE See also the IEC Multilingual Dictionary – Electricity, Electronics and Telecommunications (available on CD-ROM and at <http://www.electropedia.org>).

[2] IEC 60050-191:1990[9], *International Electrotechnical Vocabulary (IEV) – Chapter 191: Dependability and quality of service*

[3] IEC 61000-1-2, *Electromagnetic compatibility (EMC) – Part 1-2: General – Methodology for the achievement of functional safety of electrical and electronic systems including equipment with regard to electromagnetic phenomena*

[4] IEC 61000-6-7, *Electromagnetic compatibility (EMC) – Part 6-7: Generic standards – Immunity requirements for equipment intended to perform functions in a safety-related system (functional safety) in industrial locations*

[5] IEC 61010-2-201, *Safety requirements for electrical equipment for measurement, control and laboratory use – Part 2-201: Particular requirements for control equipment*

[6] IEC 61131-6, *Programmable controllers – Part 6: Functional safety*

[7] IEC 61158 (all parts), *Industrial communication networks – Fieldbus specifications*

[8] IEC 61158-5 (all parts), *Industrial communication networks – Fieldbus specifications – Part 5: Application layer service definition*

[9] IEC 61496 (all parts), *Safety of machinery – Electro-sensitive protective equipment*

[10] IEC 61508-1:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements*

[11] IEC 61508-4:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations*

[12] IEC 61508-5:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 5: Examples of methods for the determination of safety integrity levels*

[13] IEC 61511 (all parts), *Functional safety – Safety instrumented systems for the process industry sector*

[14] IEC 61784-3 (all parts), *Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses*

[15] IEC 61784-5 (all parts), *Industrial communication networks – Profiles – Part 5: Installation of fieldbuses – Installation profiles for CPF x*

[16] IEC 61800-5-2, *Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional*

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

9 Withdrawn.

[17] IEC 62061, *Safety of machinery – Functional safety of safety-related control systems*

[18] IEC 62280:2014, *Railway applications – Communication, signalling and processing systems – Safety related communication in transmission systems*

[19] IEC 62443 (all parts), *Industrial communication networks – Network and system security*

[20] ISO/IEC Guide 51:2014, *Safety aspects – Guidelines for their inclusion in standards*

[21] ISO/IEC 2382:2015, *Information technology – Vocabulary*

[22] ISO/IEC 7498-1, *Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model*

[23] ISO/IEC 19501:2005, *Information technology – Open Distributed Processing – Unified Modeling Language (UML) Version 1.4.2*

[24] ISO 10218-1, *Robots and robotic devices – Safety requirements for industrial robots – Part 1: Robots*

[25] ISO 13849 (all parts), *Safety of machinery – Safety-related parts of control systems*

[26] ANDREW S. TANENBAUM, DAVID J. WETHERALL, *Computer Networks*, 5th Edition, Prentice Hall, N.J., ISBN-10: 0132126958, ISBN-13: 978-0132126953

[27] W. WESLEY PETERSON, EDWARD J. WELDON, *Error-Correcting Codes*, 2nd Edition 1972, MIT-Press, ISBN 0-262-16-039-0

[28] GUY E. CASTAGNOLI, *On the Minimum Distance of Long Cyclic Codes and Cyclic Redundancy-Check Codes*, 1989, Dissertation No. 8979 of ETH Zurich, Switzerland

[29] GUY E. CASTAGNOLI, STEFAN BRÄUER, and MARTIN HERRMANN, *Optimization of Cyclic Redundancy-Check Codes with 24 and 32 Parity Bits*, June 1993, IEEE Transactions On Communications, Volume 41, No. 6

[30] The CIP Networks Library Volume 5: *CIP Safety Specification*, Edition 2.18, April 2019, available at http://www.odva.org [viewed 2020-12-22]

[31] The CIP Networks Library Volume 1: *CIP Common,* Edition 3.26, April 2019, available at http://www.odva.org [viewed 2020-12-22]

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

SOMMAIRE

AVANT-PROPOS 292
0 Introduction 294
0.1 Généralités 294
0.2 Déclaration de brevets 296
1 Domaine d'application 297
2 Références normatives 297
3 Termes, définitions, symboles, abréviations et conventions 299
3.1 Termes et définitions 299
3.1.1 Termes et définitions communs 299
3.1.2 CPF 2: Termes et définitions supplémentaires 305
3.2 Symboles et abréviations 306
3.2.1 Symboles et abréviations communs 306
3.2.2 CPF 2: Symboles et abréviations supplémentaires 307
3.3 Conventions 308
4 Présentation générale du FSCP 2/1 (CIP Safety™) 308
4.1 Généralités 308
4.2 FSCP 2/1 308
5 Généralités 310
5.1 Documents externes de spécifications applicables au profil 310
5.2 Exigences fonctionnelles de sécurité 310
5.3 Mesures de sécurité 310
5.4 Structure de la couche de communication de sécurité 311
5.5 Relations avec la FAL (et DLL, PhL) 312
5.5.1 Généralités 312
5.5.2 Types de données 312
6 Services de la couche de communication de sécurité 312
6.1 Généralités 312
6.2 Objet Connexion 313
6.2.1 Généralités 313
6.2.2 Extensions des attributs de classe 313
6.2.3 Extensions de services 314
6.2.4 Format de réponse de messages explicites pour SafetyOpen et SafetyClose 314
6.3 Objet Gestionnaire de connexion 315
6.3.1 Généralités 315
6.3.2 ForwardOpen pour la sécurité 315
6.3.3 Segment de réseau de sécurité 317
6.3.4 Règles du point d'origine pour le calcul du CRC de paramètre de connexion 321
6.3.5 Organigrammes de traitement de SafetyOpen 322
6.3.6 Contrôles exigés par les producteurs multipoints avec les connexions existantes 325
6.3.7 Utilisation de la clé électronique de sécurité 326
6.3.8 RPI en fonction d'API dans les connexions de sécurité 326
6.3.9 Règles d'élaboration du chemin d'application pour les connexions de sécurité 327

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

6.3.10 Types de connexions de l'objet de validation de sécurité 329
6.3.11 Données de réponse d'application dans une réponse SafetyOpen satisfaisante 333
6.3.12 Réponse SafetyOpen non satisfaisante 335
6.3.13 Service ForwardClose de sécurité 337
6.4 Objet Identité 338
6.4.1 Généralités 338
6.4.2 Modifications apportées aux services communs 338
6.4.3 Extensions pour les appareils CP 16/3 338
6.5 Objets de liaison 339
6.5.1 Modifications apportées à l'objet DeviceNet 339
6.5.2 Modifications apportées à l'objet Interface TCP/IP 340
6.5.3 Objet Liaison SERCOS III 340
6.6 Objet Programme de contrôle de sécurité 341
6.6.1 Généralités 341
6.6.2 Attributs de classe du programme de contrôle de sécurité 342
6.6.3 Sous-classes 343
6.6.4 Attributs instance du Programme de contrôle de sécurité 343
6.6.5 Sémantique 347
6.6.6 Sous-classes 355
6.6.7 Services communs du programme de contrôle de sécurité 355
6.6.8 Comportement du Programme de contrôle de sécurité 369
6.7 Objet de validation de sécurité 377
6.7.1 Généralités 377
6.7.2 Attributs de classe 378
6.7.3 Attributs instance 378
6.7.4 Services de classes 385
6.7.5 Services instance 386
6.7.6 Comportement d'objet 386
6.8 Connection Configuration Object (Objet de configuration de connexion) 389
6.8.1 Généralités 389
6.8.2 Extensions des attributs de classe 389
6.8.3 Attributs instance, ajouts et extensions 389
6.8.4 Extensions ou restrictions de sémantique des attributs instance pour des raisons de sécurité 392
6.8.5 Paramètres spéciaux relatifs à la sécurité – (attribut 13) 398
6.8.6 Services spécifiques à l'objet 403
6.8.7 Extensions des services communs pour la sécurité 404
6.8.8 Comportement d'objet 405
7 Protocole de couche de communication de sécurité 407
7.1 Format PDU de sécurité 407
7.1.1 Codage PDU de sécurité 407
7.1.2 CRC de sécurité 419
7.2 Comportement du protocole de communication 420
7.2.1 Séquence des contrôles de sécurité 420
7.2.2 Fin de connexion 421
7.2.3 Erreur de contre-vérification 421
7.3 Opération de datation 421
7.4 Comptages de remplacement dans l'EF 423

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

7.5 Diagrammes séquentiels de protocoles 423
7.5.1 Généralités 423
7.5.2 Transmission de sécurité normale 423
7.5.3 Transmission de messages perdus, corrompus et retardés 425
7.5.4 Transmission de messages perdus, corrompus ou retardés avec production répétée 427
7.5.5 Demande Ping point à point 429
7.5.6 Demande Ping multipoint avec sécurité CP 2/3 430
7.5.7 Demande Ping multipoint sur les réseaux de sécurité CP 2/2 432
7.5.8 Demande Ping multipoint – Retransmission aboutie 432
7.5.9 Demande Ping multipoint – Retransmission avec temporisation 433
7.6 Définition du protocole de sécurité 434
7.6.1 Généralités 434
7.6.2 Vue de haut niveau d'un appareil de sécurité 434
7.6.3 Objet de validation de sécurité 435
7.6.4 Relation entre SafetyValidatorServer et SafetyValidatorClient 436
7.6.5 Gestion du remplacement de la datation de format étendu 437
7.6.6 Définition de la fonction SafetyValidatorClient 443
7.6.7 Définition de la fonction SafetyValidatorServer 452
7.7 Spécifications des messages de sécurité et des données de protocole 465
7.7.1 Octet Mode 465
7.7.2 Section de datation 466
7.7.3 Message de coordination temporelle 466
7.7.4 Message de correction de temps 466
7.7.5 Production des données de sécurité 467
7.7.6 Variables dynamiques du producteur 475
7.7.7 Variables dynamiques de producteur par consommateur 477
7.7.8 Variables de données du consommateur 479
7.7.9 Variables statiques d'entrée du consommateur 481
7.7.10 Variables dynamiques du consommateur 482
8 Gestion de la couche de communication de sécurité 484
8.1 Présentation générale 484
8.2 Définition des mesures utilisées lors de l'établissement d'une connexion 484
8.3 Validation de la relation point d'origine cible 488
8.4 Détection des demandes de connexion mal acheminées 489
8.5 Traitement de SafetyOpen 489
8.6 Gestion de propriété 489
8.7 Pontage de différentes couches physiques 490
8.8 Etablissement de connexion de sécurité 492
8.8.1 Présentation générale 492
8.8.2 Faits de base pour l'établissement d'une connexion 492
8.8.3 Configuration des connexions de sécurité 493
8.8.4 Multiplicateur de délai du réseau 494
8.8.5 Etablissement de connexions 496
8.8.6 Recommandations pour l'attribution d'un numéro de consommateur 499
8.8.7 Recommandations pour l'établissement d'une connexion 499
8.8.8 Etablissement de propriété 500
8.8.9 Cas d'utilisation de la propriété 500
8.8.10 Utilisation et établissement de la relation PID/CID 504

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

8.8.11 Utilisation PID/CID correcte dans les connexions multipoints et point à point 505
8.8.12 Services pris en charge par le réseau 507
8.8.13 Type d'appareil de sécurité FSCP 2/1 507
8.9 Processus de configuration de sécurité 511
8.9.1 Introduction à la configuration de sécurité 511
8.9.2 Objectifs de configuration 511
8.9.3 Présentation générale de la configuration 512
8.9.4 Lignes directrices pour la configuration par l'utilisateur 513
8.9.5 Justification du processus de configuration 514
8.9.6 Fonctions d'appareils pour configuration par outil 515
8.9.7 Sécurité par mot de passe 515
8.9.8 Services d'interface SNCT 516
8.9.9 Verrouillage de configuration 516
8.9.10 Influence du verrouillage de configuration sur le comportement des appareils 516
8.9.11 Propriété de configuration 518
8.9.12 Mode de configuration 518
8.9.13 Mesures d'assurance de l'intégrité du processus de configuration 518
8.9.14 Processus de téléchargement aval 520
8.9.15 Processus de vérification 523
8.9.16 Analyse des erreurs de configuration 526
8.10 Extensions de fiches techniques électroniques à des fins de sécurité 531
8.10.1 Règles générales applicables aux appareils de sécurité EDS 531
8.10.2 Extensions EDS à des fins de sécurité 531
8.11 Exigences pour le CP 2/2 537
8.11.1 Règles EPI applicables aux messages de sécurité acheminés par le CP 2/2 537
8.11.2 Service E/S de sécurité par défaut 538
8.11.3 Duplication de détection IP 538
8.11.4 Priorité pour les connexions de sécurité 538
8.12 Exigences pour le CP 2/3 538
8.12.1 Attribution des identifiants CP 2/3 538
8.12.2 Exigences supplémentaires 541
8.13 Exigences pour le CP 16/3 541
8.13.1 Architecture générale de la CPF 2 sur le CP 16/3 541
8.13.2 FSCP 2/1 de référence des appareils CP 16/3 542
8.13.3 Objets et services pris en charge dans les appareils CP 16/3 543
8.13.4 Exigences relatives aux couches de transport 544
8.13.5 FSCP 2/1 et modèle d'appareil CP 16/3 546
8.13.6 Attribution d'un UNID sur le CP 16/3 547
9 Exigences système 550
9.1 Indicateurs et commutateurs 550
9.1.1 Exigences générales concernant les indicateurs 550
9.1.2 Indications LED pour le paramétrage de l'UNID des appareils 550
9.1.3 LED d'état du module 551
9.1.4 Avertissement lié aux indicateurs 551
9.1.5 LED d'état du réseau 551
9.1.6 Commutateurs 553

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

9.2 Lignes directrices relatives à l'installation 555
9.3 Temps de réponse de la fonction de sécurité 555
9.3.1 Présentation générale 555
9.3.2 Délai du réseau 556
9.3.3 Equations de calcul des temps de réaction du réseau 556
9.4 Durée des demandes (ou sollicitations) 559
9.5 Contraintes liées au calcul des caractéristiques du système 559
9.5.1 Nombre de nœuds 559
9.5.2 PFH de réseau du format étendu 559
9.5.3 Taux d'erreurs sur les bits (BER) 560
9.6 Maintenance 561
9.7 Manuel de sécurité 561
10 Evaluation 561
Annexe A (informative) Informations supplémentaires pour les profils de communication de sécurité fonctionnelle de la CPF 2 562
A.1 Exemple de code de fonction de hachage 562
A.2 Vide 576
Annexe B (informative) Information pour l'évaluation des profils de communication de sécurité fonctionnelle de la CPF 2 577
Bibliographie 578

Figure 1 – Relations entre l'IEC 61784-3 et d'autres normes (machines) 294
Figure 2 – Relations entre l'IEC 61784-3 et d'autres normes (transformation) 295
Figure 3 – Relation des Objets de validation de sécurité 309
Figure 4 – Couches de communication 312
Figure 5 – ForwardOpen avec segment de réseau de sécurité 316
Figure 6 – Format cible de réseau de sécurité 319
Figure 7 – Service SafetyOpen de traitement de cible sans données de configuration (SafetyOpen de type 2) 323
Figure 8 – Service SafetyOpen de traitement de cible avec données de configuration (SafetyOpen de type 1) 324
Figure 9 – Logique du point d'origine permettant de déterminer le format à utiliser 325
Figure 10 – Application de configuration d'appareil 360
Figure 11 – Organigrammes de traitement de Configuration et Validation 361
Figure 12 – Traitement d'UNID pendant l'état "Attente du TUNID" 368
Figure 13 – Diagramme d'états du Programme de contrôle de sécurité 370
Figure 14 – Relations entre configuration, essais et verrouillage 375
Figure 15 – Types de connexions de sécurité 383
Figure 16 – Diagramme de transitions d'état de l'Objet de validation de sécurité 387
Figure 17 – Logique pour le type de format Autodétection 402
Figure 18 – Diagramme d'états de l'objet Configuration de connexion 406
Figure 19 – Flux de données de l'objet Configuration de connexion 406
Figure 20 – Format de l'octet Mode 409
Figure 21 – Section de données à 1 ou 2 octets, format de base 410
Figure 22 – Section de données à 1 ou 2 octets, format étendu 410
Figure 23 – Format de section de données de 3 à 250 octets, format de base 411

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Figure 24 – Format de section de données de 3 à 250 octets, format étendu 411
Figure 25 – Format de section de datation, format de base 412
Figure 26 – Codage du message de coordination temporelle BF 413
Figure 27 – Codage du message de coordination temporelle EF 413
Figure 28 – Codage du message de correction de temps BF 415
Figure 29 – Codage du message de correction de temps EF 415
Figure 30 – Codage PDU point à point à 1 ou 2 octets 416
Figure 31 – Codage PDU multipoint à 1 ou 2 octets 417
Figure 32 – Format de connexion de sécurité de format 2 multipoint à 1 ou 2 octets 417
Figure 33 – Codage PDU point à point de 3 à 250 octets 418
Figure 34 – Codage PDU multipoint de 3 à 248 octets 418
Figure 35 – Format de connexion de sécurité multipoint de 3 à 248 octets 419
Figure 36 – Ordre de calcul du CRC pour les messages de format étendu 419
Figure 37 – Séquence de datation 422
Figure 38 – Diagramme d'une séquence de sécurité producteur/consommateur normale 423
Figure 39 – Diagramme d'une séquence de sécurité producteur/consommateur normale (production répétée) 424
Figure 40 – Diagramme séquentiel d'un message producteur vers consommateur corrompu 425
Figure 41 – Diagramme séquentiel d'un message producteur vers consommateur perdu 426
Figure 42 – Diagramme séquentiel d'un message retardé 427
Figure 43 – Diagramme séquentiel d'un message producteur vers consommateur corrompu avec production répétée 427
Figure 44 – Diagramme séquentiel d'une fin de connexion occasionnée par des retards 428
Figure 45 – Diagramme séquentiel d'un contrôle CRC de sécurité non satisfaisant 429
Figure 46 – Diagramme séquentiel d'une demande Ping point à point – réponse normale 429
Figure 47 – Diagramme séquentiel d'une demande Ping multipoint satisfaisante, sécurité CP 2/3 431
Figure 48 – Diagramme séquentiel d'une demande Ping multipoint satisfaisante, sécurité CP 2/2 432
Figure 49 – Diagramme séquentiel d'une retransmission de demande Ping multipoint 433
Figure 50 – Diagramme séquentiel d'une temporisation de demande Ping multipoint 433
Figure 51 – Architectures de sécurité possibles pour le FSCP 2/1 434
Figure 52 – Diagramme de relations des entités de modèle de référence d'un appareil de sécurité 435
Figure 53 – Deux appareils qui échangent des données de sécurité par l'intermédiaire des fonctions SafetyValidatorClient et SafetyValidatorServer 436
Figure 54 – Consommateur d'origine et producteur cible point à point 438
Figure 55 – Producteur d'origine et consommateur cible point à point 440
Figure 56 – Consommateur d'origine et producteur cible multipoint 441
Figure 57 – Flux de données de production de sécurité 443
Figure 58 – Contrôle des données de sécurité de consommation 453
Figure 59 – SafetyValidatorServer – déclenchée par l'application 453

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Figure 60 – Propriété cible 488
Figure 61 – Formes de SafetyOpen 489
Figure 62 – Diagramme d'états de la propriété de connexion 490
Figure 63 – Mapping de l'UNID de service SafetyOpen 490
Figure 64 – Couche application CPF 2 commune 491
Figure 65 – Exemple d'acheminement de bout en bout 491
Figure 66 – Sources des paramètres de connexion relative à la sécurité 495
Figure 67 – Mapping des paramètres entre le point d'origine et la cible 496
Figure 68 – Etablissement d'une connexion de sécurité CP 2/3 dans les cibles pour un service SafetyOpen de type 2a 498
Figure 69 – Séquence générale de détection de l'exigence d'une configuration 498
Figure 70 – Echanges PID/CID pour deux scénarios de point d'origine 504
Figure 71 – Génération des valeurs de départ pour les connexions multipoints 505
Figure 72 – Traitement d'exécution PID/CID 506
Figure 73 – Catégories de connexions et services pris en charge 509
Figure 74 – Types de connexions recommandés 510
Figure 75 – Services logique à logique pris en charge 510
Figure 76 – Types de connexions recommandés pour les services logique à logique 511
Figure 77 – Transferts de données de configuration 512
Figure 78 – Mesures de protection des appareils de sécurité 514
Figure 79 – Relations entre configuration, essais et verrouillage 517
Figure 80 – Données de configuration du point d'origine 519
Figure 81 – Processus de téléchargement aval du SNCT à l'appareil 521
Figure 82 – Téléchargements aval du SNCT vers les points d'origine qui réalisent la configuration de type 1 522
Figure 83 – Protection contre le verrouillage et propriété 524
Figure 84 – Processus de vérification comprenant toutes les méthodes alternatives 526
Figure 85 – FSCP 2/1 de référence des appareils CP 16/3 543
Figure 86 – Interaction entre couches d'adaptation FSCP 2/1 et SMP 545
Figure 87 – Couche d'adaptation FSCP 2/1 546
Figure 88 – Modèle d'appareil CP 16/3 547
Figure 89 – Ajout d'un module normalisé à un appareil modulaire 549
Figure 90 – Logique de traitement du NodeID des appareils de sécurité 554
Figure 91 – Temps de réponse de la fonction de sécurité 555
Figure 92 – Composantes du temps de réponse de la fonction de sécurité 558
Figure 93 – Schéma de principe de fiabilité (RBD) de protocole de réseau 559

Tableau 1 – Erreurs de communication et matrice de mesures de détection 311
Tableau 2 – Nouveaux attributs de classe 313
Tableau 3 – Extensions de services 314
Tableau 4 – Format de réponse SafetyOpen et SafetyClose 314
Tableau 5 – Identifiant de segment de réseau de sécurité 317
Tableau 6 – Définition du segment de réseau de sécurité 317
Tableau 7 – Format de routage de segment de réseau de sécurité 320

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Tableau 8 – Format étendu de segment de réseau de sécurité 320
Tableau 9 – Règles d'évaluation des paramètres de production multipoint 326
Tableau 10 – Options de paramétrage du service ForwardOpen pour les connexions de sécurité qui comportent des chemins d'application qui reposent sur des objets 330
Tableau 11 – Options de paramétrage du service ForwardOpen pour les connexions de sécurité qui comportent un chemin d'application de segment de symbole étendu ANSI 332
Tableau 12 – Paramètres de connexion de réseau pour les connexions de sécurité 333
Tableau 13 – Réponse d'application de cible SafetyOpen (taille: 10 octets) 333
Tableau 14 – Réponse d'application de cible SafetyOpen EF CP 2/2 ou CP 16/3 (taille: 14 octets) 334
Tableau 15 – Réponse d'application de cible SafetyOpen BF CP 2/3 (taille: 18 octets) 334
Tableau 16 – Réponse d'application de cible SafetyOpen EF CP 2/3 (taille: 22 octets) 335
Tableau 17 – Nouveaux codes d'erreurs étendus de sécurité 335
Tableau 18 – Tableau de recommandations concernant les événements d'erreur SafetyOpen 336
Tableau 19 – Modifications apportées aux services communs de l'objet Identité 338
Tableau 20 – Extensions de l'objet Identité pour les appareils CP 16/3 339
Tableau 21 – Nouvel attribut instance de l'objet DeviceNet 339
Tableau 22 – Nouvel attribut instance de l'objet Interface TCP/IP 340
Tableau 23 – Attributs de classe de l'objet Liaison SERCOS III 340
Tableau 24 – Attributs instance de l'objet Liaison SERCOS III 341
Tableau 25 – Services communs de l'objet Liaison SERCOS III 341
Tableau 26 – Attributs de classe du Programme de contrôle de sécurité 342
Tableau 27 – Attributs instance du Programme de contrôle de sécurité 343
Tableau 28 – Valeurs d'indication de l'attribut Etat de l'appareil 348
Tableau 29 – Format de l'attribut Etat d'exception 349
Tableau 30 – Valeurs de l'attribut Détail d'exception commun 350
Tableau 31 – Synthèse du format de détail d'exception 351
Tableau 32 – Synthèse du comportement des appareils pour différentes valeurs CFUNID 353
Tableau 33 – Services communs du Programme de contrôle de sécurité 355
Tableau 34 – Services spécifiques de l'objet Programme de contrôle de sécurité 356
Tableau 35 – Structure de message Configure_Request 358
Tableau 36 – Structure de message Validate_Configuration 358
Tableau 37 – Structure de message de réussite Validate_Configuration 359
Tableau 38 – Code d'erreur de Validate_Configuration 359
Tableau 39 – Codes étendus de Validate_Configuration 359
Tableau 40 – Structure de message Set_Password 362
Tableau 41 – Structure de message Reset_Password 362
Tableau 42 – Structure de message Configuration_Lock/Unlock 363
Tableau 43 – Structure de message Mode_Change 363
Tableau 44 – Structure de message Safety_Reset 364
Tableau 45 – Types de réinitialisations de sécurité du Programme de contrôle de sécurité 364
Tableau 46 – Paramètre d'attribut Mode point 365

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Tableau 47 – Règles de traitement applicables aux types de réinitialisations 365
Tableau 48 – Service Propose_TUNID 366
Tableau 49 – Service Apply_TUNID 366
Tableau 50 – Service Propose_TUNID_List 369
Tableau 51 – Service Apply_TUNID_List 369
Tableau 52 – Evénements liés au Programme de contrôle de sécurité 370
Tableau 53 – Matrice d'événements d'état du Programme de contrôle de sécurité 371
Tableau 54 – Contrôle de la propriété de configuration en fonction de l'état de l'appareil 375
Tableau 55 – Mapping des états du Programme de contrôle de sécurité vers l'objet Identité 376
Tableau 56 – Mapping des événements de l'objet Programme de contrôle de sécurité 376
Tableau 57 – Mapping des événements de l'objet Identité 377
Tableau 58 – Attributs de classe de l'Objet de validation de sécurité 378
Tableau 59 – Attributs instance de l'Objet de validation de sécurité 378
Tableau 60 – Attributions d'états de l'Objet de validation de sécurité 382
Tableau 61 – Type d'Objet de validation de sécurité, attributions de champs de bits 382
Tableau 62 – Règles d'évaluation du paramètre SafetyOpen des producteurs multipoints 384
Tableau 63 – Services de classes de l'Objet de validation de sécurité 385
Tableau 64 – Services instance de l'Objet de validation de sécurité 386
Tableau 65 – Données du service Get_Attributes_All de l'Objet de validation de sécurité 386
Tableau 66 – Matrice d'événements d'état de l'Objet de validation de sécurité 388
Tableau 67 – Mapping des états entre le Programme de contrôle de sécurité et l'Objet de validation de sécurité 389
Tableau 68 – Extensions des attributs de classe de l'objet Configuration de connexion 389
Tableau 69 – Ajouts/extensions d'attributs instance de l'objet Configuration de connexion 390
Tableau 70 – Définition des bits de drapeaux de connexion 393
Tableau 71 – Paramètres de connexion O-to-T 394
Tableau 72 – Paramètres de connexion T-to-O 395
Tableau 73 – Formats de mapping des données 396
Tableau 74 – Format 0 de mapping des données 397
Tableau 75 – Format 1 de mapping des données 397
Tableau 76 – Valeurs SCCRC de l'appareil cible 400
Tableau 77 – Valeurs SCTS de l'appareil cible 400
Tableau 78 – Paramètres de connexion de correction de temps pour une connexion multipoint 401
Tableau 79 – Signification de l'attribut Type de format 402
Tableau 80 – Signification de l'attribut Etat du format 403
Tableau 81 – Services spécifiques à l'objet Configuration de connexion 403
Tableau 82 – Données du service de réponse Get_Attributes_All (attributs ajoutés) 404
Tableau 83 – Données du service de réponse Get_Attributes_All (paramètres ajoutés) 404
Tableau 84 – Données du service de demande Set_Attributes_All (attributs ajoutés) 405

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Tableau 85 – Données du service de réponse Set_Attributes_All (paramètres ajoutés) 405
Tableau 86 – Mapping des états entre le Programme de contrôle de sécurité et les objets CCO 406
Tableau 87 – Sections de connexion et formats PDU 408
Tableau 88 – Sections de connexion et format de message 408
Tableau 89 – Variables de l'octet Mode 409
Tableau 90 – Variables de datation 412
Tableau 91 – Variables du message de coordination temporelle 413
Tableau 92 – Variables du message de correction de temps 415
Tableau 93 – Polynômes de CRC utilisés 420
Tableau 94 – Utilisation des CRC pour la connexion et la configuration 420
Tableau 95 – Réception des données – Déclenchée par la liaison 454
Tableau 96 – Réception de Time_Correction – Déclenchée par la liaison 455
Tableau 97 – Réception des données – Déclenchée par l'application 455
Tableau 98 – Réception de Time_Correction – Déclenchée par l'application 455
Tableau 99 – Application de consommation – Contrôle des données de sécurité 456
Tableau 100 – Détermination de l'état de la connexion du producteur 467
Tableau 101 – Etat de la connexion de sécurité de consommation 479
Tableau 102 – Erreurs d'établissement de connexion et mesures de détection des erreurs 484
Tableau 103 – Attributions de Date/Heure SNN 485
Tableau 104 – Plage légale de SNN des valeurs temporelles 485
Tableau 105 – Paramètres de connexion de sécurité 494
Tableau 106 – Récapitulatif SafetyOpen 497
Tableau 107 – Mapping des services point d'origine/cible 508
Tableau 108 – Types de services point d'origine/cible non pris en charge 508
Tableau 109 – Objectifs de configuration 512
Tableau 110 – Contrôle de la propriété de configuration en fonction de l'état de l'appareil 517
Tableau 111 – Erreurs et mesures de détection 527
Tableau 112 – Mots clés des sections de classe d'objet 532
Tableau 113 – Format d'entrée Classex de sécurité 533
Tableau 114 – Mots clés de classes de paramètres 533
Tableau 115 – Nouveaux mots clés de la section Gestionnaire de connexion à des fins de sécurité 534
Tableau 116 – Utilisation du champ Gestionnaire de connexion à des fins de sécurité 535
Tableau 117 – Paramétrages du champ Paramètres de connexion à des fins de sécurité 537
Tableau 118 – Règles d'attribution d'ID CP 2/3 539
Tableau 119 – Indications LED pour le paramétrage de l'UNID 550
Tableau 120 – LED d'état du module 551
Tableau 121 – Etats de la LED d'état du réseau 552
Tableau 122 – Type de temps de réaction de connexion – applications de production/consommation 557

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

RÉSEAUX DE COMMUNICATION INDUSTRIELS – PROFILS –

Partie 3-2: Bus de terrain de sécurité fonctionnelle – Spécifications supplémentaires pour CPF 2

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

L'IEC 61784-3-2 a été établie par le sous-comité 65C: Réseaux industriels, du comité d'études 65 de l'IEC: Mesure, commande et automation dans les processus industriels. Il s'agit d'une Norme internationale.

Cette quatrième édition annule et remplace la troisième édition parue en 2016. Cette édition constitue une révision technique.

Cette édition inclut les modifications techniques majeures suivantes par rapport à l'édition précédente:

- ajout de deux nouveaux états de l'objet Programme de contrôle de sécurité en 6.6.5.5;

- ajout de l'exigence relative au comportement des LED réseau pour le processus de proposition de TUNID en 6.6.8, 9.1.2 et 9.1.5;
- ajout de la prise en charge du chemin d'application pour les variables de processus en 6.3.9 et 6.3.10;
- ajout de la prise en charge des appareils multiports en 6.6.4, 6.6.5, 6.6.7 et en différents endroits;
- correction des équations de temps de réaction du réseau en 9.3.3;
- ajout de la prise en charge SIL jusqu'au niveau SIL3 en 7.6, 8.7, 8.9, 9.5 et en différents endroits;
- reprise des lignes directrices relatives à la procédure de configuration en 8.9.14 et 8.9.15;
- détection des modifications de commutateur en 9.1.6;
- utilisation déconseillée du format de base en 3.1.2, 7.1.1.1 et 6.3.3.2;
- définition de la valeur Max_Fault_Number sur 2 en 6.3.3.4, 6.8.3 et 8.8.3;
- mise à jour du calcul de la PFH de réseau en 9.5.2;
- apport de diverses corrections mineures depuis la dernière publication.

Le texte de cette Norme internationale est issu des documents suivants:

FDIS	Rapport de vote
65C/1083/FDIS	65C/1087/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à son approbation.

La version française de cette norme n'a pas été soumise au vote.

La langue employée pour l'élaboration de cette Norme internationale est l'anglais.

Le présent document a été rédigé selon les Directives ISO/IEC, Partie 2, il a été développé selon les Directives ISO/IEC, Partie 1 et les Directives ISO/IEC, Supplément IEC, disponibles sous www.iec.ch/members_experts/refdocs. Les principaux types de documents développés par l'IEC sont décrits plus en détail sous www.iec.ch/standardsdev/publications.

Une liste de toutes les parties de la série IEC 61784-3, publiées sous le titre général *Réseaux de communication industriels – Profils – Bus de terrain de sécurité fonctionnelle*, peut être consultée sur le site web de l'IEC.

Le comité a décidé que le contenu du présent document ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous "webstore.iec.ch" dans les données relatives au document recherché. A cette date, le document sera

- reconduit,
- supprimé,
- remplacé par une édition révisée, ou
- amendé.

IMPORTANT – Le logo "colour inside" qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

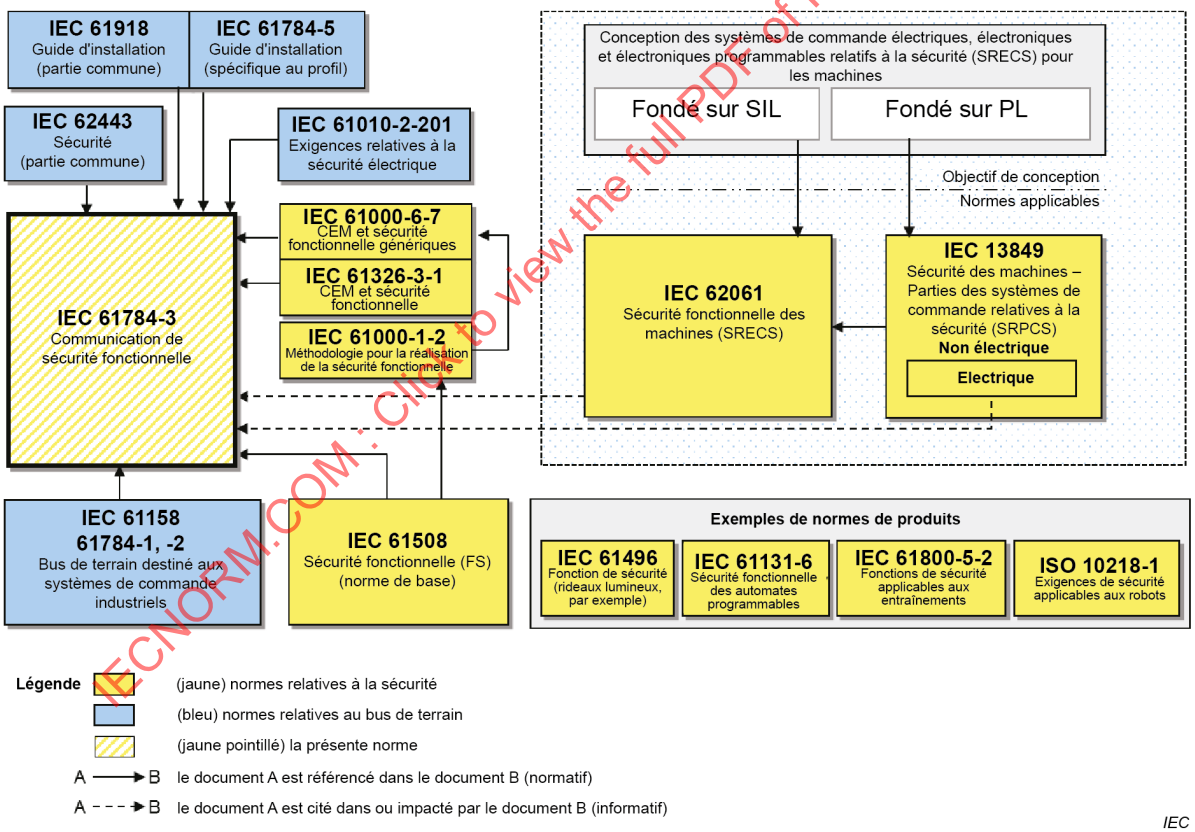
0 Introduction

0.1 Généralités

L'IEC 61158 (toutes les parties), relative aux bus de terrain, ainsi que ses normes associées IEC 61784-1 et IEC 61784-2, définissent un ensemble de protocoles de communication qui assurent la commande répartie d'applications automatisées. La technologie de bus de terrain est désormais reconnue et bien éprouvée. Les améliorations des bus de terrain se poursuivent; elles couvrent des applications pour des domaines comme les applications en temps réel relatives à la sécurité.

La série IEC 61784-3 (toutes les parties) explique les principes pertinents pour les communications de sécurité fonctionnelle en référence à l'IEC 61508 (toutes les parties) et spécifie plusieurs couches de communication de sécurité (profils et protocoles correspondants) qui reposent sur les profils de communication et les couches de protocole de l'IEC 61784-1, l'IEC 61784-2 et l'IEC 61158 (toutes les parties). Elle ne couvre pas les aspects relatifs à la sécurité électrique et à la sécurité intrinsèque. Elle ne couvre pas non plus les aspects relatifs à la sûreté et ne prévoit aucune exigence en matière de sûreté.

La Figure 1 représente les relations entre l'IEC 61784-3 (toutes les parties) et les normes pertinentes relatives à la sécurité et aux bus de terrain dans un environnement de machines.

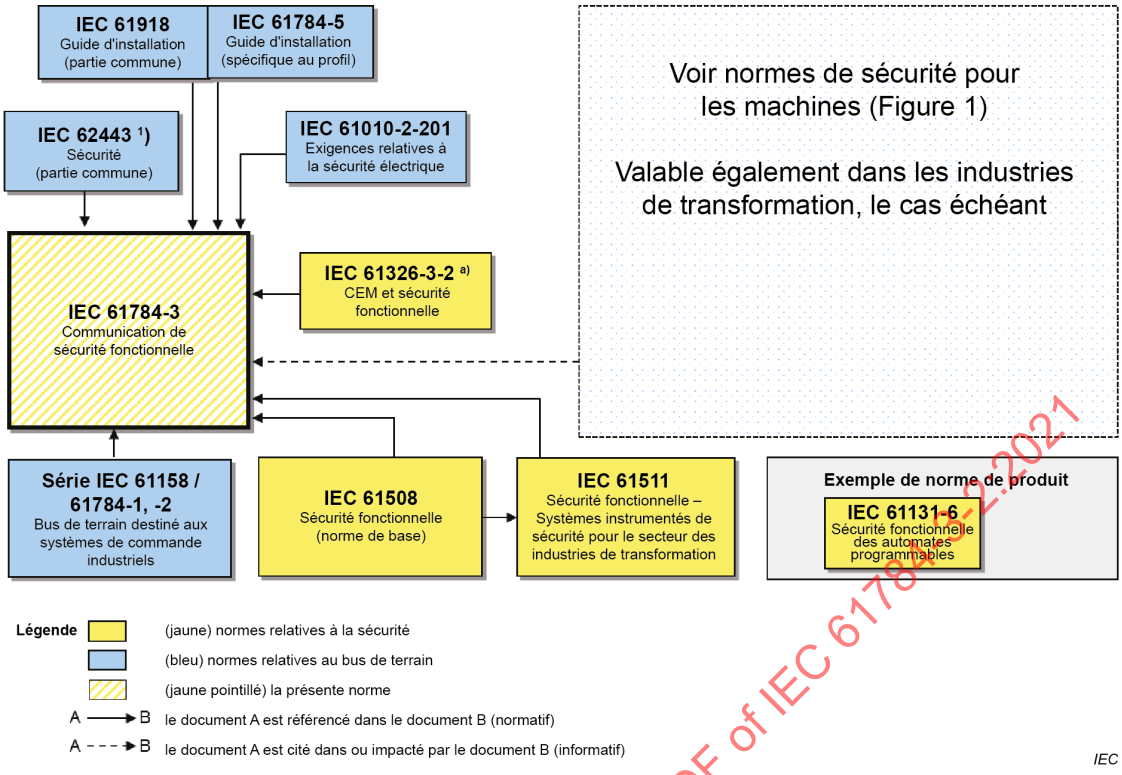


NOTE L'IEC 62061 spécifie la relation entre PL (Catégorie) et SIL.

Figure 1 – Relations entre l'IEC 61784-3 et d'autres normes (machines)

La Figure 2 représente les relations entre l'IEC 61784-3 (toutes les parties) et les normes pertinentes relatives à la sécurité et aux bus de terrain dans un environnement de processus.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021



[a] Pour les environnements électromagnétiques spécifiés; sinon, l'IEC 61326-3-1 ou l'IEC 61000-6-7 s'applique.

Figure 2 – Relations entre l'IEC 61784-3 et d'autres normes (transformation)

Les couches de communication de sécurité mises en œuvre dans le cadre de systèmes relatifs à la sécurité conformément à l'IEC 61508 (toutes les parties) assurent la confiance nécessaire à accorder à la transmission de messages (informations) entre plusieurs participants sur un bus de terrain dans un système relatif à la sécurité ou une fiabilité suffisante dans le comportement de sécurité en cas d'erreurs ou de défaillances du bus de terrain.

Les couches de communication de sécurité spécifiées dans l'IEC 61784-3 (toutes les parties) permettent de s'assurer qu'un bus de terrain peut être utilisé dans des applications qui nécessitent une sécurité fonctionnelle jusqu'au niveau d'intégrité de sécurité (SIL) spécifié par son profil de communication de sécurité fonctionnelle correspondant.

La revendication du SIL qui en résulte pour un système dépend de la mise en œuvre du profil de communication de sécurité fonctionnelle (FSCP) retenu au sein du système (la mise en œuvre du profil de communication de sécurité fonctionnelle dans un appareil normal ne suffit pas à le qualifier d'appareil de sécurité).

L'IEC 61784-3 (toutes les parties) décrit:

- les principes de base de la mise en œuvre des exigences de l'IEC 61508 (toutes les parties) pour les communications de données relatives à la sécurité, y compris les anomalies de transmission potentielles, les mesures correctives et des considérations relatives à l'intégrité des données;
- les profils de communication de sécurité fonctionnelle pour plusieurs familles de profils de communication dans l'IEC 61784-1 et l'IEC 61784-2, y compris les extensions de la couche de sécurité aux sections relatives au service et aux protocoles de communication de l'IEC 61158 (toutes les parties).

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

0.2 Déclaration de brevets

La Commission Electrotechnique Internationale (IEC) attire l'attention sur le fait qu'il est déclaré que la conformité avec les dispositions du présent document peut impliquer l'utilisation de brevets intéressant les profils de communication de sécurité fonctionnelle pour la famille 2. L'IEC ne prend pas position quant à la preuve, à la validité et à la portée de ces droits de propriété.

Le détenteur de ces droits de propriété a donné l'assurance à l'IEC qu'il consent à négocier des licences avec des demandeurs du monde entier à des termes et conditions raisonnables et non discriminatoires. A ce propos, la déclaration du détenteur des droits de propriété est enregistrée à l'IEC. Des informations peuvent être obtenues dans la base de données des droits de propriété, disponible à l'adresse suivante: http://patents.iec.ch.

L'attention est d'autre part attirée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété autres que ceux qui ont été enregistrés dans la base de données des droits de propriété. L'IEC ne saurait être tenue pour responsable de l'identification de ces droits de propriété en tout ou partie.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

RÉSEAUX DE COMMUNICATION INDUSTRIELS – PROFILS –

Partie 3-2: Bus de terrain de sécurité fonctionnelle – Spécifications supplémentaires pour CPF 2

1 Domaine d'application

La présente partie de l'IEC 61784-3 (toutes les parties) spécifie une couche de communication de sécurité (services et protocole) qui repose sur la CPF 2 de l'IEC 61784-1, l'IEC 61784-2 et l'IEC 61158, Type 2. Elle identifie les principes applicables aux communications de sécurité fonctionnelle définies dans l'IEC 61784-3, qui correspondent à cette couche de communication de sécurité. Cette couche de communication de sécurité est destinée à être mise en œuvre uniquement sur les appareils de sécurité.

NOTE 1 Elle ne couvre pas les aspects relatifs à la sécurité électrique et à la sécurité intrinsèque. La sécurité électrique concerne les dangers tels que les chocs électriques. La sécurité intrinsèque concerne les dangers associés aux atmosphères explosibles.

Le présent document définit les mécanismes de transmission des messages relatifs à la sécurité entre les participants d'un réseau réparti, en utilisant la technologie de bus de terrain conformément aux exigences de la série IEC 61508 (toutes les parties) [1] concernant la sécurité fonctionnelle. Ces mécanismes peuvent être utilisés dans différentes applications industrielles, par exemple la commande de processus, l'usinage automatique et les machines.

Le présent document fournit des lignes directrices aux développeurs, ainsi qu'aux évaluateurs d'appareils et de systèmes conformes.

NOTE 2 La revendication du SIL qui en résulte pour un système dépend de la mise en œuvre du profil de communication de sécurité fonctionnelle retenu au sein du système (la mise en œuvre d'un profil de communication de sécurité fonctionnelle conforme au présent document dans un appareil normal ne suffit pas à le qualifier d'appareil de sécurité).

2 Références normatives

Les documents suivants sont cités dans le texte de sorte qu'ils constituent, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

IEC 61131-2, *Mesurage et contrôle des processus industriels – Automates programmables – Partie 2: Exigences et essais des équipements*

IEC 61131-3, *Automates programmes – Partie 3: Langages de programmation*

IEC 61158-2:2014, *Réseaux de communications industriels – Spécifications des bus de terrain – Partie 2: Spécification et définition des services de la couche physique*

IEC 61158-3-2, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 3-2: Définition des services de la couche liaison de données – Eléments de type 2*

[1] Dans les pages suivantes du présent document, "IEC 61508" remplace "IEC 61508 (toutes les parties)".

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

IEC 61158-3-19, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 3-19: Définition des services de la couche liaison de données – Eléments de type 19*

IEC 61158-4-2:2019, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 4-2: Spécification du protocole de la couche de liaison de données – Eléments de Type 2*

IEC 61158-4-19, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 4-19: Spécification du protocole de la couche de liaison de données – Eléments de type 19*

IEC 61158-5-2, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 5-2: Définition des services de la couche application – Eléments de type 2*

IEC 61158-5-19, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 5-19: Définition des services de la couche application – Eléments de type 19*

IEC 61158-6-2, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 6-2: Spécification de protocole de couche application – Eléments de type 2*

IEC 61158-6-19, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 6-19: Spécification de protocole de la couche application – Eléments de type 19*

IEC 61326-3-1, *Matériel électrique de mesure, de commande et de laboratoire – Exigences relatives à la CEM – Partie 3-1: Exigences d'immunité pour les systèmes relatifs à la sécurité et pour les matériels destinés à réaliser des fonctions relatives à la sécurité (sécurité fonctionnelle) – Applications industrielles générales*

IEC 61326-3-2, *Matériel électrique de mesure, de commande et de laboratoire – Exigences relatives à la CEM – Partie 3-2: Exigences d'immunité pour les systèmes relatifs à la sécurité et pour les matériels destinés à réaliser des fonctions relatives à la sécurité (sécurité fonctionnelle) – Applications industrielles dont l'environnement électromagnétique est spécifié*

IEC 61508 (toutes les parties), *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité*

IEC 61784-1, *Réseaux de communication industriels – Profils – Partie 1: Profils de bus de terrain*

IEC 61784-2, *Réseaux de communication industriels – Profils – Partie 2: Profils de bus de terrain supplémentaires pour les réseaux en temps réel fondés sur l'ISO/IEC/IEEE 8802-3*

IEC 61784-3:2021, *Réseaux de communication industriels – Profils – Partie 3: Bus de terrain de sécurité fonctionnelle – Règles générales et définitions de profils*

IEC 61784-5-2, *Réseaux de communication industriels – Profils – Partie 5-2: Installation des bus de terrain – Profils d'installation pour CPF 2*

IEC 61918, *Réseaux de communication industriels – Installation de réseaux de communication dans des locaux industriels*

IEC 62026-3, *Appareillage à basse tension – Interfaces appareil de commande-appareil (CDI) – Partie 3: DeviceNet*

ISO 13849-1:2015, *Sécurité des machines – Parties des systèmes de commande relatives à la sécurité – Partie 1: Principes généraux de conception*

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

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

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

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

3 Termes, définitions, symboles, abréviations et conventions

3.1 Termes et définitions

Pour les besoins du présent document, les termes et définitions de l'IEC 61784-3 ainsi que les suivants s'appliquent.

L'ISO et l'IEC tiennent à jour des bases de données terminologiques destinées à être utilisées en normalisation, consultables aux adresses suivantes:

- IEC Electropedia: disponible à l'adresse http://www.electropedia.org/
- ISO Online browsing platform: disponible à l'adresse http://www.iso.org/obp

NOTE L'italique est utilisé dans les définitions pour mettre en évidence les termes définis en 3.1.

3.1.1 Termes et définitions communs

NOTE Ces termes et définitions communs sont issus de l'IEC 61784-3:2021.

3.1.1.1
probabilité d'erreurs sur les éléments binaires
Pe
probabilité de réception d'un bit donné avec la valeur incorrecte

3.1.1.2
canal noir
système de communication défini qui contient un ou plusieurs éléments sans preuve de conception ou de validation conformément à l'IEC 61508

Note 1 à l'article: Cette définition étend la signification habituelle du canal pour inclure le système qui contient le canal.

3.1.1.3
pont
appareil abstrait qui relie plusieurs segments de réseau le long de la couche de liaison de données

3.1.1.4
système de communication fermé
nombre fixe ou nombre maximal fixe d'éléments reliés par un *système de communication* dont les propriétés sont connues et fixées et où le *risque* d'accès non autorisé est considéré comme négligeable

[SOURCE: IEC 62280:2014, 3.1.6, modifié – "transmission" remplacé par "communication"]

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

3.1.1.5
canal de communication
connexion logique entre deux points limites d'un *système de communication*

3.1.1.6
système de communication
ensemble de matériels, de logiciels et de supports de propagation qui permet la transmission de *messages* (ISO/IEC 7498-1, couche d'application) d'une application à une autre

3.1.1.7
connexion
liaison logique entre deux objets d'application d'appareils identiques ou différents

3.1.1.8
contrôle de redondance cyclique
CRC
<valeur> donnée redondante déduite, et enregistrée ou transmise simultanément, d'un bloc de données afin de détecter toute corruption des données

<méthode> procédure utilisée pour calculer les données redondantes

Note 1 à l'article: Les termes "code CRC" et "signature CRC", ainsi que les étiquettes comme CRC1, CRC2, peuvent également être utilisés dans le présent document pour se référer aux données redondantes.

Note 2 à l'article: Voir également [26], [27] [2].

3.1.1.9
système de communication défini
canal défini
nombre fixe ou nombre maximal fixe d'éléments reliés par un *système de communication* à *bus de terrain*, dont les propriétés sont connues et fixées, par exemple les conditions d'installation, l'immunité électromagnétique, les *éléments (actifs) de réseau* industriel, et où le *risque* d'accès non autorisé est réduit à un niveau toléré conformément au modèle de cycle de vie de l'IEC 62443 (toutes les parties), en utilisant par exemple des zones et des conduits

3.1.1.10
appareil
entité physique connectée au bus de terrain, constituée d'un élément de communication et éventuellement d'autres éléments fonctionnels

[SOURCE: IEC 61158-2:2014, 3.1.13, modifié – Note à l'article et certaines informations supprimées]

3.1.1.11
DLPDU
DÉCONSEILLÉ: trame
unité de données de protocole de liaison de données

Note 1 à l'article: L'abréviation "DLPDU" est dérivée du terme anglais développé correspondant "Data Link Protocol Data Unit".

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

2 Les chiffres entre crochets renvoient à la bibliographie.

3.1.1.12
erreur
écart ou discordance entre une valeur ou une condition calculée, observée ou mesurée et la valeur ou la condition vraie, prescrite ou théoriquement correcte

Note 1 à l'article: Les erreurs peuvent être causées par des erreurs de conception du matériel/logiciel et/ou des informations altérées du fait d'un brouillage électromagnétique et/ou autres effets.

Note 2 à l'article: Les erreurs ne produisent pas nécessairement une *défaillance* ou une *anomalie*.

[SOURCE: IEC 61508-4:2010, 3.6.11, modifié – notes ajoutées]

3.1.1.13
défaillance
cessation de l'aptitude d'une unité fonctionnelle à accomplir une fonction requise ou à fonctionner comme prévu

Note 1 à l'article: Une défaillance peut être causée par une *erreur* (problème de conception matérielle/logicielle ou rupture de message, par exemple).

[SOURCE: IEC 61508-4:2010, 3.6.4, modifié – notes et figures remplacées]

3.1.1.14
anomalie
condition anormale qui peut entraîner une réduction ou la perte de capacité d'une unité fonctionnelle à accomplir une fonction requise

Note 1 à l'article: L'IEC 60050-191:1990, 191-05-01, définit le terme "fault" (en français "panne") comme un état d'inaptitude à accomplir une fonction requise, en excluant l'inaptitude due à la maintenance préventive, à d'autres actions programmées ou à un manque de ressources extérieures.

[SOURCE: IEC 61508-4:2010, 3.6.1, modifié – référence à la figure supprimée]

3.1.1.15
bus de terrain
système de communication fondé sur le transfert de données en série et utilisé dans des applications d'automatisation industrielle ou de commande de processus

3.1.1.16
profil de communication de sécurité fonctionnelle
FSCP
spécification de technologie pour la mise en œuvre d'une SCL

Note 1 à l'article: L'abréviation "FSCP" est dérivée du terme anglais développé correspondant "functional safety communication profile".

3.1.1.17
fonction de hachage
fonction (mathématique) de mapping des valeurs d'un ensemble (éventuellement) très grand de valeurs en une plage de valeurs (habituellement) plus petite

Note 1 à l'article: Les fonctions de hachage peuvent être utilisées pour déterminer l'altération des données.

Note 2 à l'article: Les fonctions de hachage communes incluent la parité, la somme de contrôle ou le CRC.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

3.1.1.18
danger
source potentielle de dommage

Note 1 à l'article: Ce terme comprend le danger sur des personnes survenant dans un laps de temps très court (par exemple, feu et explosion), mais aussi le danger à long terme sur la santé d'une personne (par exemple, dégagement d'une substance toxique).

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

3.1.1.19
maître
entité de communication capable d'initier et de programmer des activités de communication effectuées par d'autres stations qui peuvent être des maîtres ou des esclaves

3.1.1.20
message
<théorie de l'information et théorie des communications> suite ordonnée de caractères (généralement des octets) destinée à communiquer des informations

[SOURCE: ISO/IEC 2382:2015, 2123205, modifié – insertion de "(généralement des octets)", suppression des notes et de la source]

3.1.1.21
niveau de performance
PL
niveau discret d'aptitude de parties relatives à la sécurité à réaliser une *fonction de sécurité* dans des conditions prévisibles

Note 1 à l'article: L'abréviation "PL" est dérivée du terme anglais développé correspondant "performance level".

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

3.1.1.22
redondance
existence de plusieurs moyens pour accomplir une fonction requise ou pour représenter des informations

[SOURCE: IEC 61508-4:2010, 3.4.6, modifié – exemple et notes supprimés]

3.1.1.23
taux d'erreurs résiduelles
taux statistique de défaut de détection d'*erreurs* par les *mesures de sécurité* SCL

3.1.1.24
risque
combinaison de la probabilité d'un dommage et de sa gravité

Note 1 à l'article: Pour plus d'informations sur ce concept, voir Annexe A de l'IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6, et Guide ISO/IEC 51:2014, définition 3.9, modifiée – note différente]

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

3.1.1.25
canal de communication de sécurité
canal de communication qui commence au sommet de la SCL de la source et qui se termine au sommet de la SCL du collecteur

Note 1 à l'article: Le canal peut être modélisé sous la forme de deux SCL reliées par un *canal noir*, un *système de communication défini* ou un *canal défini*.

3.1.1.26
couche de communication de sécurité
SCL
couche de communication située au-dessus de la FAL qui comprend toutes les mesures supplémentaires nécessaires qui permettent d'assurer la transmission de données en toute sécurité conformément aux exigences de l'IEC 61508

Note 1 à l'article: L'abréviation "SCL" est dérivée du terme anglais développé correspondant "safety communication layer".

3.1.1.27
connexion de sécurité
connexion qui utilise le protocole de sécurité pour des transactions de communications

3.1.1.28
données de sécurité
données transmises par un réseau de sécurité qui utilise un protocole de sécurité

Note 1 à l'article: La *couche de communication de sécurité* n'assure pas la sécurité des données proprement dites, mais uniquement la transmission en toute sécurité de ces dernières.

3.1.1.29
appareil de sécurité
appareil conçu conformément à l'IEC 61508 et qui met en œuvre le profil de communication de sécurité fonctionnelle

3.1.1.30
fonction de sécurité
fonction à réaliser par un *système* E/E/PE *relatif à la sécurité* ou par un dispositif externe de réduction de *risque*, prévue pour assurer ou maintenir un état de sécurité de l'EUC par rapport à un événement dangereux spécifique

[SOURCE: IEC 61508-4:2010, 3.5.1, modifié – références et exemples supprimés]

3.1.1.31
temps de réponse de la fonction de sécurité
temps écoulé dans le cas le plus défavorable à la suite de l'activation d'un capteur de sécurité relié à un *bus de terrain*, avant d'atteindre l'état de sécurité correspondant de ses actionneurs de sécurité, du fait d'*erreurs* ou de *défaillances* dans la *fonction de sécurité*

Note 1 à l'article: Ce concept, introduit dans l'IEC 61784-3:2021, 5.2.4, est traité par les profils de communication de sécurité fonctionnelle définis dans le présent document.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

3.1.1.32
niveau d'intégrité de sécurité
SIL
niveau discret (parmi quatre possibles) correspondant à une gamme de valeurs d'intégrité de sécurité où le niveau 4 d'intégrité de sécurité possède le plus haut degré d'intégrité et le niveau 1 possède le plus bas

Note 1 à l'article: Les objectifs chiffrés de *défaillance* (voir l'IEC 61508-4:2010, 3.5.17) pour les quatre niveaux d'intégrité de sécurité sont indiqués dans les Tableaux 2 et 3 de l'IEC 61508-1:2010.

Note 2 à l'article: Les niveaux d'intégrité de sécurité sont utilisés pour spécifier les exigences concernant l'intégrité de sécurité des *fonctions de sécurité* à allouer aux *systèmes* E/E/PE *relatifs à la sécurité*.

Note 3 à l'article: Un niveau d'intégrité de sécurité (SIL) ne constitue pas une propriété d'un système, sous-système, élément ou composant. L'interprétation correcte de l'expression "*système relatif à la sécurité* à SIL*n*" (où *n* est 1, 2, 3 ou 4) signifie que le système est potentiellement capable de prendre en charge des *fonctions de sécurité* avec un niveau d'intégrité de sécurité jusqu'à *n*.

Note 4 à l'article: L'abréviation "SIL" est dérivée du terme anglais développé correspondant "safety integrity level".

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

3.1.1.33
mesure de sécurité
mesure qui permet de contrôler les *erreurs* de communication éventuelles, qui est conçue et mise en œuvre conformément aux exigences de l'IEC 61508

Note 1 à l'article: Dans la pratique, plusieurs mesures de sécurité sont combinées pour atteindre le *niveau d'intégrité de sécurité* exigé.

Note 2 à l'article: Les *erreurs* de communication et les mesures de sécurité associées sont décrites dans l'IEC 61784-3:2021, 5.3 et 5.4.

3.1.1.34
PDU de sécurité
SPDU
PDU transféré par le *canal de communication de sécurité*

Note 1 à l'article: Le SPDU peut comporter plusieurs exemplaires des *données de sécurité* qui utilisent des structures de codage et des *fonctions de hachage* différentes, associées à des parties explicites de protections supplémentaires, par exemple une clé, un nombre de séquences ou un mécanisme de *datation*.

Note 2 à l'article: Les SCL redondantes peuvent fournir deux versions différentes du SPDU en vue de son insertion dans des champs séparés de la *trame de bus de terrain*.

Note 3 to entry: L'abréviation "SPDU" est dérivée du terme anglais développé correspondant "safety PDU".

3.1.1.35
application relative à la sécurité
programmes conçus conformément à l'IEC 61508 pour satisfaire aux exigences SIL de l'application

3.1.1.36
système relatif à la sécurité
système qui exécute les *fonctions de sécurité* conformément à l'IEC 61508

3.1.1.37
esclave
entité de communication capable de recevoir des *messages* et de les envoyer en réponse à une autre entité de communication qui peut être *maître* ou esclave, mais pas d'initier des activités de communication

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

3.1.1.38
déclenchement parasite
déclenchement provoqué par le système de sécurité sans injonction du processus

3.1.1.39
datation
information temporelle incluse dans un *message*

3.1.2 CPF 2: Termes et définitions supplémentaires

3.1.2.1
format de base
format utilisé pour les RPI de connexion d'une durée inférieure à 100 ms ou pour des applications dans lesquelles des connexions interrompues peuvent être admises

3.1.2.2
déconseiller
action qui consiste à ne plus reconnaître officiellement ou à déconseiller l'utilisation d'une entité (un produit logiciel, par exemple) au profit d'une alternative plus récente ou mieux adaptée

3.1.2.3
format étendu
format utilisé pour les RPI de connexion d'une durée supérieure à 100 ms ou pour des applications dans lesquelles il est nécessaire d'éviter des connexions interrompues

3.1.2.4
demande Ping (demande d'acquittement)
demande d'acquittement de la réception d'un message par le consommateur

3.1.2.5
réponse à demande Ping
réponse à une demande Ping

3.1.2.6
point d'origine
nœud qui demande la création d'une connexion

3.1.2.7
signature
méthode d'identification unique d'un ensemble de données

Note 1 à l'article: Ceci peut prendre la forme d'une révision, d'une somme de contrôle ou d'une toute autre méthode fixée par accord entre les appareils d'origine et cibles.

3.1.2.8
appareil à un seul port de sécurité
appareil d'origine, appareil cible ou appareil mixte d'origine/cible qui réalise des communications de sécurité sur un seul et unique port CIP

3.1.2.9
capabilité systématique
mesure (exprimée sur une échelle de SC 1 à SC 4) de la confiance dans le fait que l'intégrité de sécurité systématique d'un élément satisfait aux exigences du niveau SIL spécifié, par rapport à la fonction de sécurité spécifiée de l'élément, lorsque l'élément est appliqué conformément aux instructions spécifiées dans le manuel de sécurité d'articles conformes pour l'élément

[SOURCE: IEC 61508-4:2010, 3.5.9, modifié – notes supprimées]

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

3.1.2.10
intégrité de sécurité systématique
partie de l'intégrité de sécurité d'un système relatif à la sécurité qui se rapporte aux défaillances systématiques dans un mode de défaillance dangereux

[SOURCE: IEC 61508-4:2010, 3.5.6, modifié – note supprimée]

3.1.2.11
cible
nœud qui reçoit une demande de création de connexion

3.2 Symboles et abréviations

3.2.1 Symboles et abréviations communs

CP	Communication Profile (Profil de communication)	[IEC 61784-1]
CPF	Communication Profile Family (Famille de profils de communication)	[IEC 61784-1]
CRC	Contrôle de redondance cyclique	
DLL	Data Link Layer (Couche de liaison de données)	[ISO/IEC 7498-1]
DLPDU	Data Link Protocol Data Unit (Unité de données de protocole de liaison de données)	
CEM	Compatibilité électromagnétique	
EUC	Equipment Under Control (Equipement commandé)	[IEC 61508-4:2010]
E/E/PE	Electrical/Electronic/Programmable Electronic (Electrique/électronique/électronique programmable)	[IEC 61508-4:2010]
FAL	Fieldbus Application Layer (Couche application de bus de terrain)	[IEC 61158-5 (toutes les parties)]
FS	Functional Safety (Sécurité fonctionnelle)	
FSCP	Functional Safety Communication Profile (Profil de communication de sécurité fonctionnelle)	
MTBF	Mean Time Between Failures (Durée moyenne de bon fonctionnement)	
MTTF	Mean Time To Failure (Durée moyenne de fonctionnement avant défaillance)	
PDU	Protocol Data Unit (Unité de données de protocole)	[ISO/IEC 7498-1]
PFD	Probability of dangerous Failure on Demand (Probabilité de défaillance dangereuse sur sollicitation)	[IEC 61508-4:2010]
PFH	Fréquence moyenne de défaillance dangereuse [h^{-1}] par heure	[IEC 61508-4:2010]
PhL	Physical Layer (Couche physique)	[ISO/IEC 7498-1]
PL	Performance Level (Niveau de performance)	[ISO 13849-1]
PLC	Programmable Logic Controller (Automate programmable)	

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

SCL Safety Communication Layer
(Couche de communication de sécurité)

SIL Safety Integrity Level [IEC 61508-4:2010]
(Niveau d'intégrité de sécurité)

3.2.2 CPF 2: Symboles et abréviations supplémentaires

AIRS Already In Requested Mode/State (Déjà en mode/état sollicité)

BER Bit Error Rate (Taux d'erreurs sur les bits)

BF Base Format (Format de base)

CCO Connection Configuration Object (Objet de configuration de connexion)

CFUNID Configuration UNID (UNID de configuration)

CNP Connection Point (Point de connexion)

CID Consumer ID (ID consommateur)

CIP™[3] Common Industrial Protocol (Protocole industriel commun) (cadre d'application partagé parmi les profils de communication CPF 2)

CPCRC Connection Parameter CRC (CRC de paramètre de connexion)

CTM Connection Timeout Multiplier
(Multiplicateur de temporisation de connexion)

EDS Electronic Data Sheet (Fiche technique électronique)

EF Extended Format (Format étendu)

EPI Expected Packet Interval (Intervalle de paquets attendus)

LED Light Emitting Diode (Diode électroluminescente)

MACID Adresse physique d'appareil (CP 2/3)

MOD Module

NodeID Pour les appareils de sécurité CP 2/3, il s'agit de la MACID de l'appareil sur le réseau. Pour les appareils de sécurité CP 2/2, il s'agit de l'adresse IP de l'appareil sur le réseau. Pour les appareils de sécurité CP 16/3, il s'agit du SDID de l'appareil sur le réseau.

NV Non volatil

NVS Non-Volatile Storage (Mémoire non volatile)

OCPUNID Output Connection Owner UNID
(UNID du propriétaire de connexion de sortie)

OSC Object State Conflict (Conflit d'état d'objet)

O-to-T Originator to Target (Point d'origine vers Cible)

OUNID Originator UNID (UNID du point d'origine)

PID Producer Identifier (Identifiant de producteur)

PS Power Supply (Alimentation)

Rés. Réservé

RPI Requested Packet Interval (Intervalle de paquets sollicités)

SCCRC Safety Configuration Data CRC
(CRC de données de configuration de sécurité)

SCID Safety Configuration Identified (Configuration de sécurité identifiée)

SCTS Safety Configuration Time Stamp (Datation de configuration de sécurité)

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

[3] Pour les déclarations d'appellation commerciale, voir Article 4.

SNCT	Safety Network Configuration Tool (Outil de configuration de réseau de sécurité)	
SNN	Safety Network Number (Numéro de réseau de sécurité)	
T-to-O	Target to Originator (Cible vers Point d'origine)	
TBD	To Be Defined (A définir)	
TNS	TUNID Not Set (TUNID non défini)	
TUNID	Target UNID (UNID cible)	
UML	Universal Modeling Language (Langage de modélisation unifié)	[ISO/IEC 19501]
UNID	Unique Network Identifier (Identifiant de réseau unique)	

3.3 Conventions

Les conventions utilisées pour les descriptions des objets, services et protocoles sont décrites dans l'IEC 61158-3-2, l'IEC 61158-4-2, l'IEC 61158-5-2 et l'IEC 61158-6-2.

Le cas échéant, le présent document utilise des organigrammes, des diagrammes séquentiels UML et un pseudo-code "C" pour la description des concepts.

4 Présentation générale du FSCP 2/1 (CIP Safety™)

4.1 Généralités

La famille de profils de communication 2 (communément appelée CIP™[4]) définit des profils de communication qui reposent sur l'IEC 61158-2 Type 2, l'IEC 61158-3-2, l'IEC 61158-4-2, l'IEC 61158-5-2 et l'IEC 61158-6-2.

La famille de profils de communication 16 (communément appelée SERCOS®[5]) définit un profil de communication CP 16/3 qui repose sur l'IEC 61158-3-19, l'IEC 61158-4-19, l'IEC 61158-5-19 et l'IEC 61158-6-19.

Les profils de base CP 2/1, CP 2/2, CP 2/3 et CP 16/3 sont définis dans l'IEC 61784-1 et l'IEC 61784-2. Le profil de communication de sécurité fonctionnelle CPF 2 FSCP 2/1 (CIP Safety™[4]) repose sur les profils de base CPF 2 définis dans l'IEC 61784-1 et l'IEC 61784-2, le profil de base CP 16/3 défini dans l'IEC 61784-2, ainsi que sur les spécifications de la couche de communication de sécurité définies dans le présent document.

4.2 FSCP 2/1

Le FSCP 2/1 repose sur le modèle producteur/consommateur de la CPF 2. L'association des producteurs et des consommateurs constitue un élément important de la relation qui assure la haute intégrité nécessaire aux applications relatives à la sécurité.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

---

4 CIP™ (Common Industrial Protocol) et CIP Safety™ sont des appellations commerciales de l'organisme à but non lucratif ODVA, Inc. Cette information est donnée à l'intention des utilisateurs de la présente Norme internationale et ne signifie nullement que l'IEC approuve ou recommande le détenteur de la marque ou de l'un de ses produits. La conformité au présent document n'exige pas l'emploi des appellations commerciales CIP™ ou CIP Safety™. L'emploi des appellations commerciales CIP™ ou CIP Safety™ exige l'autorisation d'ODVA et la conformité aux conditions d'utilisation (essais et validation).

5 SERCOS® est une appellation commerciale de SERCOS International e.V. Cette information est donnée à l'intention des utilisateurs du présent document et ne signifie nullement que l'IEC approuve ou recommande le détenteur de la marque ou de l'un de ses produits. La conformité au présent document n'exige pas l'emploi de l'appellation commerciale SERCOS®. L'emploi de l'appellation commerciale SERCOS® exige l'autorisation du détenteur de cette appellation et la conformité aux conditions d'utilisation (essais et validation).

La couche de communication de sécurité FSCP 2/1 est spécifiée à l'aide d'un Objet de validation de sécurité. Cet objet est chargé de la gestion des connexions de sécurité FSCP 2/1 et constitue l'interface entre les objets d'application relatifs à la sécurité et les connexions de couches de liaison, comme le montre la Figure 3. L'Objet de validation de sécurité assure l'intégrité des transferts de données de sécurité.

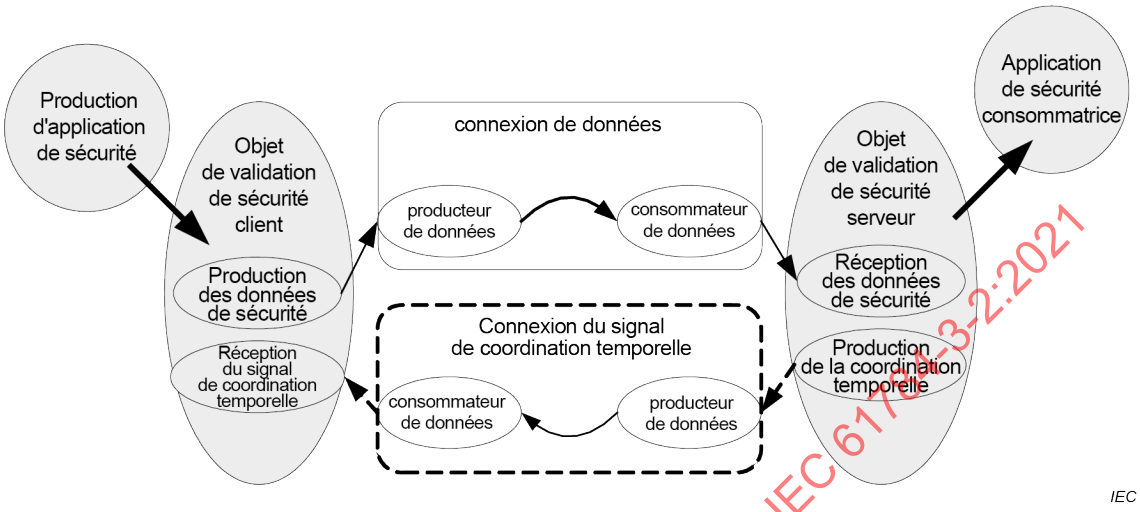


Figure 3 – Relation des Objets de validation de sécurité

L'intégrité des transferts de données de sécurité est assurée comme suit:

- l'application relative à la sécurité productrice utilise une instance d'Objet de validation de sécurité client pour générer des données de sécurité et assurer la coordination temporelle;
- le client utilise un producteur de données de liaison pour transmettre les données et un consommateur de liaison pour recevoir des messages de coordination temporelle;
- l'application relative à la sécurité consommatrice utilise un Objet de validation de sécurité serveur pour recevoir et vérifier les données;
- le serveur utilise un consommateur de liaison pour recevoir les données et un producteur de liaison pour transmettre des messages de coordination temporelle.

Le FSCP 2/1 utilise le concept de canal noir. Les producteurs et consommateurs de données de liaison n'ont aucune connaissance sur le paquet de données de sécurité et ne mettent en œuvre aucune fonction de sécurité. Les Objets de validation de sécurité sont responsables du transfert à haute intégrité et du contrôle des données de sécurité.

Le FSCP 2/1 applique les mesures suivantes pour assurer l'intégrité des messages de sécurité:

- datation;
- authentification de connexion;
- assurance d'intégrité des données;
- redondance avec contre-vérification;
- différents systèmes d'assurance d'intégrité des données.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Les messages sont produits avec une datation qui permet au consommateur de vérifier l'âge des données transmises. L'identification fait l'objet d'un codage dans chaque message relatif à la sécurité afin de s'assurer que le bon consommateur utilise le message. Tous les messages relatifs à la sécurité utilisent un CRC unique. La transmission des données relatives à la sécurité est redondante. Plusieurs mesures de production de messages relatifs à la sécurité permettent de s'assurer que les messages CPF 2 normalisés ne sont pas interprétés comme des messages de sécurité.

5 Généralités

5.1 Documents externes de spécifications applicables au profil

Les documents [30] et [31] fournissent des spécifications supplémentaires applicables en cas de mise en œuvre de la SCL définie dans le présent document.

5.2 Exigences fonctionnelles de sécurité

Les exigences suivantes doivent s'appliquer pour le développement d'appareils qui mettent en œuvre le protocole FSCP 2/1. Les mêmes exigences ont été appliquées pour le développement de ce protocole.

- Le protocole FSCP 2/1 est conçu de manière à prendre en charge le niveau d'intégrité de sécurité 3 (SIL3) (voir l'IEC 61508), et le PLe/catégorie 4 (voir l'ISO 13849-1).
- L'état de sécurité des données discrètes est l'état hors tension (0). Pour les valeurs analogiques, l'état hors tension doit être défini par l'application relative à la sécurité.
- Les exigences de base qui s'appliquent au développement du protocole FSCP 2/1 sont spécifiées dans l'IEC 61784-3.
- Le protocole FSCP 2/1 est mis en œuvre en appliquant la méthode du canal noir; aucune dépendance relative à la sécurité ne s'applique aux profils de communication CPF 2 normaux.
- Les mises en œuvre du FSCP 2/1 doivent être conformes à l'IEC 61508.
- Les conditions environnementales doivent être conformes à l'IEC 61131-2 pour les niveaux de base et à l'IEC 61326-3-1 et l'IEC 61326-3-2 pour les essais de marge de sécurité, à moins que des normes de produits spécifiques existent.
- Les communications de sécurité et normale doivent être indépendantes. Les appareils de sécurité et normaux doivent cependant être capables d'utiliser le même canal de communication.
- Sauf spécification dans le présent document, les exigences relatives à la CPF 2 ne doivent pas être modifiées pour la sécurité.

5.3 Mesures de sécurité

Le Tableau 1 comprend les mesures appliquées pour détecter les erreurs de communication, ainsi que la couverture fournie par chaque mesure utilisée.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Tableau 1 – Erreurs de communication et matrice de mesures de détection

Erreurs de communication	Mesures de sécurité							
	Numéro de séquence	Datation	Délai	Authentification de connexion	Message de réaction	Assurance d'intégrité des données	Redondance avec contre-vérification	Différents systèmes d'assurance d'intégrité des données
Corruption						X	X	
Répétition non prévue		X				X[a]	(X)[e]	
Séquence incorrecte		X				X[a]	(X)[e]	
Perte			X[c]			X[a]	(X)[e]	
Retard inacceptable		(X)[e]	X					
Insertion		X[d]		X		X[a]	(X)[e]	
Déguisement		X[d]		X		X[b]	X[f]	X
Adressage				X		X[b]		

[a] Le CRC relatif à la sécurité fournit une protection supplémentaire pour les erreurs de communication dans les messages.

[b] Le codage de l'identifiant unique dans le CRC relatif à la sécurité évite les erreurs de déguisement et d'adressage.

[c] Un message non reçu dans le délai prévu est détecté.

[d] Les messages de déguisement ou insérés ne présentent pas la datation prévue.

[e] Non revendiqué pour le profil FSCP 2/1.

[f] Il est vraisemblable que le déguisement ne comporte pas de données redondantes, et qu'il ne satisfasse pas à la contre-vérification.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

5.4 Structure de la couche de communication de sécurité

Le protocole de sécurité est superposé au protocole de réseau normalisé (la pile de protocoles normalisés est un canal noir). La Figure 4 représente la relation entre la couche de communication de sécurité et les couches CPF 2 existantes.

Les couches de sécurité acceptent les données de sécurité qui proviennent du circuit d'application relatif à la sécurité. Les couches de sécurité élaborent ensuite un message de sécurité, transmettent ce message, et reçoivent et décodent ce même message. Lorsque le message de sécurité est décodé et vérifié, les données sont présentées au circuit d'application relatif à la sécurité du récepteur.

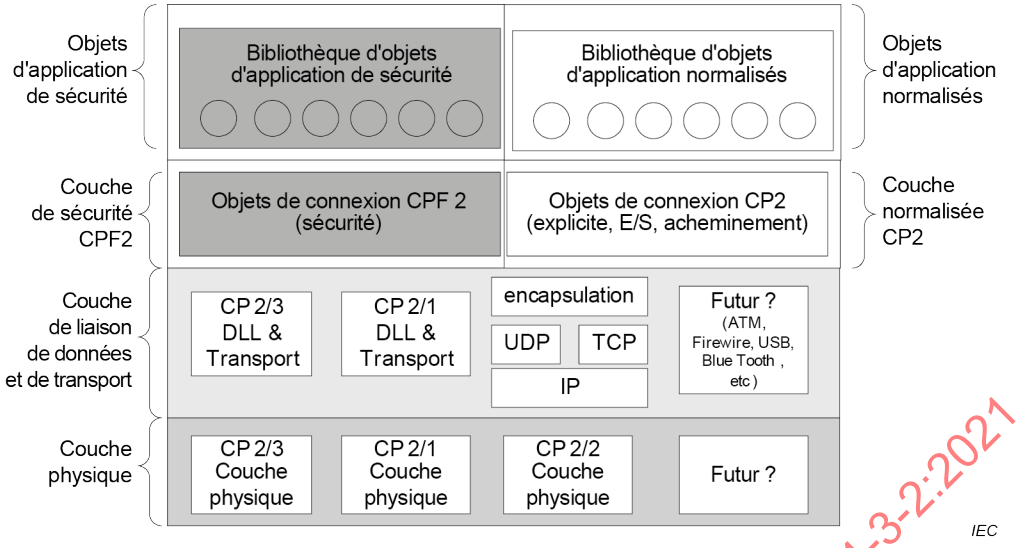


Figure 4 – Couches de communication

5.5 Relations avec la FAL (et DLL, PhL)

5.5.1 Généralités

Cette couche de communication de sécurité ne doit être utilisée qu'avec les profils de communication CPF 2 (CP 2/3 (DeviceNet™ [6]), CP 2/2 (EtherNet/IP™ [7]) et CP 16/3 (SERCOS III™[8])). Il n'existe aucune exigence concernant les profils de communication CPF 2 autres que celles définies dans le présent document.

5.5.2 Types de données

Les profils définis dans le présent document prennent en charge tous les types de données CPF 2 définis dans l'IEC 61158-5-2.

6 Services de la couche de communication de sécurité

6.1 Généralités

Le présent Article 6 définit les extensions des objets CPF 2 existants, ainsi que les nouveaux objets de sécurité. Les connexions de sécurité utilisent les connexions de classe 0 pour les messages E/S. Les connexions de messages explicites normaux sont utilisées pour l'établissement des connexions E/S de sécurité.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

---

6 DeviceNet™ est une appellation commerciale de l'organisme à but non lucratif ODVA, Inc. Cette information est donnée à l'intention des utilisateurs du présent document et ne signifie nullement que l'IEC approuve ou recommande le détenteur de la marque ou de l'un de ses produits. La conformité au présent document n'exige pas l'emploi de l'appellation commerciale DeviceNet™. L'emploi de l'appellation commerciale DeviceNet™ exige l'autorisation d'ODVA.

7 EtherNet/IP™ est une appellation commerciale d'ODVA, Inc. Cette information est donnée à l'intention des utilisateurs du présent document et ne signifie nullement que l'IEC approuve ou recommande le détenteur de la marque ou de l'un de ses produits. La conformité au présent document n'exige pas l'emploi de l'appellation commerciale EtherNet/IP™. L'emploi de l'appellation commerciale EtherNet/IP™ exige l'autorisation d'ODVA.

8 SERCOS® et l'interface SERCOS® sont des appellations commerciales de SERCOS International e.V. Cette information est donnée à l'intention des utilisateurs du présent document et ne signifie nullement que l'IEC approuve ou recommande le détenteur de la marque ou de l'un de ses produits. La conformité à ce profil n'exige pas l'emploi de l'appellation commerciale SERCOS®. L'emploi de l'appellation commerciale SERCOS® exige l'autorisation du détenteur de cette appellation.

6.2 Objet Connexion

6.2.1 Généralités

Plusieurs attributs et services de classes spécifiques à la sécurité sont définis pour prendre en charge la sécurité. Les nœuds de sécurité CP 2/3 contenus dans le protocole FSCP 2/1 doivent mettre en œuvre les services SafetyOpen et SafetyClose de l'objet Connexion.

6.2.2 Extensions des attributs de classe

Le Tableau 2 définit les attributs de classe utilisés par les appareils de sécurité.

Tableau 2 – Nouveaux attributs de classe

ID d'attribut	Mise en œuvre nécessaire	Règle d'accès	NV	Nom	Type de données	Description de l'attribut
8	Facultatif	Obtenir	V	Comptage d'erreurs de demandes de connexion	UINT	Compteur de diagnostic qui représente le cumul des anomalies SafetyOpen ou SafetyClose[a]
9	Facultatif	Obtenir	V	Compteurs des connexions de sécurité	STRUCT de:	Compteurs d'états
				Comptage de demandes SafetyOpen abouties	UINT	Comptage de demandes SafetyOpen abouties émises par ce nœud vers une autre cible
				Comptage de demandes SafetyOpen non abouties	UINT	Comptage de demandes SafetyOpen non abouties émises par ce nœud vers une autre cible
				Comptage de demandes SafetyClose abouties	UINT	Comptage de demandes SafetyClose abouties émises par ce nœud vers une autre cible
				Comptage de demandes SafetyClose non abouties[b]	UINT	Comptage de demandes SafetyClose non abouties émises par ce nœud vers une autre cible
				Comptage des indications SafetyOpen abouties	UINT	Comptage de demandes SafetyOpen abouties émises par un point d'origine externe vers ce nœud
				Comptage des indications SafetyOpen non abouties[b]	UINT	Comptage de demandes SafetyOpen non abouties émises par un point d'origine externe vers ce nœud
				Comptage des indications SafetyClose abouties	UINT	Comptage de demandes SafetyClose abouties émises par un point d'origine externe vers ce nœud
				Comptage des indications SafetyClose non abouties[b]	UINT	Comptage de demandes SafetyClose non abouties émises par un point d'origine externe vers ce nœud

[a] L'attribut 8 est la somme des 4 compteurs de défaillance dans l'attribut 9. La représentation des erreurs de connexion par cet attribut unique peut être utilisée dans les logiciels de surveillance afin de contrôler de manière efficace les erreurs sans interroger les structures supplémentaires de l'attribut 9. Lorsque l'attribut 8 a été défini comme non nul, le logiciel de surveillance peut examiner l'attribut 9 pour plus de détails.

[b] Inclus dans l'attribut de classe 8.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

6.2.3 Extensions de services

Le Tableau 3 définit les services utilisés par les appareils de sécurité CP 2/3 sur le FSCP 2/1. Ces services doivent être pris en charge par un appareil cible sur le FSCP 2/1. Les services SafetyOpen et SafetyClose, utilisés en lieu et place des services ForwardOpen et ForwardClose de l'objet Gestionnaire de connexion, héritent du même comportement que ces services de Gestionnaire de connexion.

Tableau 3 – Extensions de services

Code de service	Mise en œuvre nécessaire		Nom du service	Description du service
	Classe	Instance		
$4D_{hex}$	Facultatif	N/A	Compteurs de réinitialisation	Ce service remet à zéro les attributs de classe 8 et 9
$4E_{hex}$	Exigé	N/A	SafetyClose	Utilisé pour fermer une connexion E/S de sécurité. Voir le service ForwardClose de l'objet Gestionnaire de connexion en 6.3.13
54_{hex}	Exigé	N/A	SafetyOpen[a]	Utilisé pour établir une connexion E/S de sécurité. Voir le service ForwardOpen de l'objet Gestionnaire de connexion en 6.3.2

[a] Les données du service SafetyOpen doivent contenir un segment de réseau de sécurité dans le champ Connection_Path.

6.2.4 Format de réponse de messages explicites pour SafetyOpen et SafetyClose

Les réponses des services SafetyOpen et SafetyClose ont un format commun. Ce format contient des informations d'état pour des conditions de réussite et d'échec. Des données de réponse spécifiques à chaque service sont transmises si la réponse du service est positive. Si la réponse du service est une erreur, un état FSCP 2/1 satisfaisant indiqué par le code d'erreur général FF_{hex} est transmis, accompagné d'une quantité variable d'informations qui portent sur l'erreur étendue.

Le format de réponse pour les services spécifiques aux objets SafetyOpen et SafetyClose est défini dans le Tableau 4.

Tableau 4 – Format de réponse SafetyOpen et SafetyClose

Nom de paramètre	Type de données	Description du paramètre de réponse
Réservé	USINT	Réservé
Etat général	USINT	Un des codes d'état général énumérés dans l'IEC 61158-6-2 (codes d'état)
Taille de l'état supplémentaire	USINT	Nombre de mots de 16 bits dans la matrice d'états supplémentaires
Etat supplémentaire	MATRICE de UINT	Etat supplémentaire
Données de réponse	MATRICE d'OCTETS	Données de réponse émises par la demande ou données d'erreurs supplémentaires si l'état général a indiqué une erreur

Les données de réponse et les états généraux/supplémentaires pour les services SafetyOpen et SafetyClose doivent correspondre aux données de réponse et états généraux/supplémentaires pour les services ForwardOpen et ForwardClose de l'objet Gestionnaire de connexion, respectivement.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

6.3 Objet Gestionnaire de connexion

6.3.1 Généralités

Les appareils de sécurité CP 2/2 et CP 16/3 doivent utiliser un service ForwardOpen avec un segment de réseau de sécurité pour établir des connexions de sécurité. Ce segment identifie de manière unique le service ForwardOpen comme un service ForwardOpen de sécurité. Dans l'ensemble du présent 6.3, le terme "SafetyOpen" doit faire référence tant au service ForwardOpen de l'objet Gestionnaire de connexion (lorsqu'il contient un segment de réseau de sécurité) qu'au service SafetyOpen de l'objet Connexion.

6.3.2 ForwardOpen pour la sécurité

6.3.2.1 Contenu de ForwardOpen pour la sécurité

Le contenu du service ForwardOpen de l'objet Gestionnaire de connexion, y compris le segment de réseau de sécurité, est représenté sur la Figure 5 ci-dessous. Les réglages appropriés des différents paramètres du service ForwardOpen sont indiqués à la Figure 5.

Nom de paramètre		Type de données / Taille	Destination cible et sémantique
Priorité/Time_tick		OCTET	Demande de maintenance du gestionnaire de connexion
Time-out_ticks		USINT	Demande de maintenance du gestionnaire de connexion
ID de connexion de réseau O-to-T		UDINT	Instance de connexion de consommation:: ID de connexion consommée CIP
ID de connexion de réseau T-to-O		UDINT	Instance de connexion de production:: ID de connexion de production CIP
Numéro de série de connexion		UINT	Valeur: Numéro à 16 bits unique (pour le point d'origine) Destinataire: Demande de maintenance du gestionnaire de connexion
ID du fournisseur d'origine		UINT	Demande de maintenance du gestionnaire de connexion
Numéro de série du point d'origine		UDINT	Demande de maintenance du gestionnaire de connexion
Connection Timeout Multiplier (Multiplicateur de temporisation de connexion)		USINT	Instance de connexion de production et de consommation: Multiplicateur de temporisation
Réservé		3 OCTETS	
RPI O-to-T		UDINT	Instance de connexion de consommation: EPR
Paramètres de connexion de réseau O-to-T	Propriétaire redondant	WORD	Valeur: 0 (les connexions de sécurité ne prennent pas en charge la redondance); Destinataire: Gestionnaire de connexion
	Type de connexion		Valeur: Point à point; Destinataire: Gestionnaire de connexion
	Priorité		Valeur: 1 (Elevée "01") ou 2 (Programmée "10"); Destinataire: Gestionnaire de connexion
	Fixe/Variable		Valeur: Fixe; Destinataire: Gestionnaire de connexion
	Taille de connexion (en octets)		Valeur: Taille du PDU de sécurité, y compris les sections Octet Mode, Réel, Complémentaire et Datation Destinataire: Instance de connexion de consommation: Attribut de taille de connexion consommée
RPI T-to-O		UDINT	Instance de connexion de production: EPR
Paramètres de connexion de réseau T-to-O	Propriétaire redondant	WORD	Valeur: 0 (les connexions de sécurité ne prennent pas en charge la redondance); Destinataire: Gestionnaire de connexion
	Type de connexion		Valeur: Point à point; Destinataire: Gestionnaire de connexion

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Nom de paramètre			Type de données / Taille	Destination cible et sémantique
	Priorité			Valeur: 1 (Elevée "01") ou 2 (Programmée "10"); Destinataire: Gestionnaire de connexion
	Fixe/Variable			Valeur: Fixe; Destinataire: Gestionnaire de connexion
	Taille de connexion (en octets)			Valeur: Taille du PDU de sécurité, y compris les sections Octet Mode, Réel, Complémentaire et Datation Destinataire: Instance de connexion de production: Taille de connexion produite
Type de transport/Déclencheur			SWORD	Valeur: Valeur de sécurité simple ou multipoint Destinataire: Instance d'objet de validation Déclencheur toujours réglé sur Application Client/Serveur: selon la direction
Connection_Path_Size			USINT	Nombre de mots de 16 bits dans le champ Connection_Path – le destinataire est la demande de maintenance du gestionnaire de connexion. NOTE Chaque routeur supprime les segments d'acheminement contenus dans le Connection_Path qui s'y appliquent, avant de transférer la demande au saut/à la cible suivant(e). La zone Segments de réseau cible est réservée aux segments de réseau cible à canal gris/noir. Par conséquent, la valeur Connection_Path_Size incluse dans le calcul du CRC du paramètre de connexion n'inclut pas les mots utilisés pour les segments d'acheminement et les segments de réseau cible présents dans le champ Connection_Path du point d'origine.
Connection_Path (EPATH complété)				
	Groupe(s) de segments Port		Variable	Consommé par le ou les gestionnaires de connexion d'acheminement intermédiaires. Voir l'IEC 61158-6-2. NOTE Chaque segment Format de routage-Réseau de sécurité suit immédiatement le segment Port du pont (CPF 2 vers CP 2/3) auquel il est destiné.
	Segment logique: Clé électronique	ID du fournisseur	UINT	Valeur: Clé électronique de la cible exigée. Maintenance du gestionnaire de connexion ou de l'objet Connexion
		Type de prod.	UINT	
		Code de prod.	UINT	
		Compatible/ Rév. principale	SWORD	
		Rév. secondaire	USINT	
	Segments de réseau cible		Variable	Voir l'IEC 61158-6-2 pour plus d'informations. Noter que le segment de sécurité cible est placé après le ou les chemins d'application et toutes les données de configuration (facultatives). Cette position est réservée aux segments de réseau cible à canal noir.
	Chemin(s) d'application		Voir 6.3.9 pour les règles d'élaboration du chemin d'application de connexion de sécurité.	
	Données de configuration	Segment de données: Données simples	Variable	Données de configuration à utiliser pour l'objet d'application relatif à la sécurité identifié par le chemin de configuration
	Segment de sécurité cible		50_{hex}	Segment de réseau de sécurité pour la cible; voir 6.3.3.

Légende

= Champs Connexion/Objet de validation de sécurité couverts par le CRC des paramètres de connexion

= Segment de données de configuration couvert par SCCV

Figure 5 – ForwardOpen avec segment de réseau de sécurité

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

6.3.2.2 ForwardOpen pour la sécurité pour format étendu

Les points d'origine de sécurité qui prennent en charge le format étendu peuvent se connecter à des cibles avec des RPI d'une durée inférieure ou égale à 100 ms avec le format étendu (EF) ou le format de base (BF).

Les points d'origine de sécurité qui se connectent à une cible CP 2/2, à une cible CP 16/3 ou à une cible CP 2/3 avec un saut CP 2/2 ou un saut CP 16/3 sur le chemin et ont un RPI d'une durée supérieure à 100 ms doivent utiliser le format étendu.

Différentes méthodes peuvent être utilisées pour y parvenir. Les fichiers EDS et les logiciels de configuration peuvent préconfigurer le choix, ou le point d'origine peut utiliser un algorithme dynamique pour effectuer les déterminations.

Le mécanisme utilisé par le point d'origine pour indiquer à une cible que le format étendu fait l'objet d'une demande présente un nouveau format de segment de réseau de sécurité défini en 6.3.3.

6.3.3 Segment de réseau de sécurité

6.3.3.1 Format commun

Le type de segment de paramètres de connexion de sécurité a été ajouté à la définition du segment de réseau CPF 2 comme type de segment 10_{hex} (qui produit une valeur de segment de 50_{hex}). La définition actualisée de Segment de réseau est donnée dans le Tableau 5.

Tableau 5 – Identifiant de segment de réseau de sécurité

Type de segment de réseau	Nom de segment de réseau
50_{hex}	Segment de sécurité

Le format du segment de réseau de sécurité est défini dans le Tableau 6. Ce type de segment se situe dans la plage des types de segments de réseau, qui comporte un champ de taille de données. Le paramètre de format de segment de sécurité, à savoir le premier paramètre dans la zone de données, indique les données qui suivent.

Tableau 6 – Définition du segment de réseau de sécurité

Décalage d'octet	Nom de champ	Type de données	Description
0	Type de segment	SWORD	Indique le segment de réseau de sécurité (50_{hex})
1	Longueur des données du segment de réseau	SWORD	Longueur des données de segment à suivre (en mots)
2	Format du segment de réseau de sécurité	USINT	Indique le type de segment de réseau de sécurité 0 = Format cible 1 = Format de routage 2 = Format EF 3 – 255 = Réservé
3 – n	Données du segment de réseau de sécurité	MATRICE d'OCTETS	Données du segment de réseau de sécurité, définies par le format du segment

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

6.3.3.2 Segment de réseau de sécurité: format cible (00_{hex}) – déconseillé

Il n'est plus exigé que les appareils mettent en œuvre le format de base. Les appareils qui ne prennent plus en charge ce format doivent répondre aux demandes de connexion de sécurité en utilisant le format cible avec Erreur de paramètre de sécurité – Format de connexion de sécurité invalide, 01_{hex}, 0803_{hex}. Les points d'origine peuvent continuer à prendre en charge ce format cible à des fins de rétrocompatibilité avec les appareils existants.

Le format cible est orienté vers la cible de la connexion. La valeur du paramètre Longueur des données de segment de réseau doit être 27 ($1b_{hex}$), ce qui correspond à 27 MOTS. La Figure 6 définit le format cible de réseau de sécurité.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Nom de champ	Type de données	Description
Réservé	SWORD	Remplissage
CRC de configuration (SCCRC)	UDINT	CRC-S4 du segment de données de configuration cible. Une valeur de 0 indique que le contrôle SCID peut être omis.
Datation de configuration (SCTS)	DATE_AND_TIME	Date et heure de la configuration. Une valeur de 0 indique que le contrôle SCID peut être omis. Valeur de 6 octets (Date: 2 octets, Heure: 4 octets)
EPI de correction de temps	UDINT	Non utilisé: 0 Utilisé: Instance de connexion de correction de temps: EPI
Paramètres de connexion de réseau de correction de temps	WORD	Paramètres de connexion de réseau pour la connexion de correction de temps. Ce champ utilise la même définition que le paramètre de connexion de réseau contenu dans l'objet Gestionnaire de connexion. Non utilisé: 0 (Nul). Utilisé: Fixe, priorité élevée, multipoint
Target_UNID (TUNID)	STRUCT de: 10 OCTETS	UNID de l'appareil cible. Cette valeur est une valeur de 10 octets constituée de l'identifiant de réseau de sécurité (6 octets) et de l'adresse de nœud (adresse de 4 octets)
UNID du point d'origine (OUNID)	STRUCT de: 10 OCTETS	UNID de l'appareil d'origine. Cette valeur est une valeur de 10 octets constituée de l'identifiant de réseau de sécurité (6 octets) et de l'adresse de nœud (adresse de 4 octets)
Ping_Interval_EPI_Multiplier	UINT	Nombre qui définit le Ping_Count_Interval pour la connexion. La plage de valeurs valides est donnée en 7.7.5.10
Time_Coord_Msg_Min_Multiplier	UINT	Pour l'instance de connexion de production. Plage valide comprise entre 0 et 7 813
Network_Time_Expectation_Multiplier	UINT	Pour l'instance de connexion de consommation. Plage valide comprise entre 1 et 45 313
Timeout_Multiplier	USINT	Utilisé par le producteur et le consommateur pour la temporisation des connexions. Plage valide comprise entre 1 et 4
Max_Consumer_Number	USINT	Valeur: 1 (point à point), 2-15 (multipoint)
CRC des paramètres de connexion (CPCRC)	UDINT	CRC-S4 des paramètres de connexion cible dans cette demande
ID de connexion de correction de temps	UDINT	Non utilisé: $FFFFFFFF_{hex}$ Utilisé: Instance de connexion de correction de temps: ID de connexion

Légende

= Champs de segment de sécurité couverts par le CRC des paramètres de connexion

Figure 6 – Format cible de réseau de sécurité

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

6.3.3.3 Segment de réseau de sécurité: format de routage (01_{hex})

Le format de routage est orienté vers un routeur intermédiaire le long du chemin de connexion, lorsqu'il est nécessaire que ce routeur sache qu'il s'agit d'un service ForwardOpen de sécurité. Actuellement, seuls les routeurs CP 2/3 nécessitent que ce segment de réseau soit orienté vers eux. Le segment de réseau est appliqué au sous-réseau qui a émis la demande de connexion. Les segments de réseau de sécurité du format de routage apparaissent uniquement dans la partie du chemin du Connection_Path d'un service ForwardOpen de sécurité. La longueur de segment totale est de 6 mots. Le format de routage de segment de réseau de sécurité est défini dans le Tableau 7.

Tableau 7 – Format de routage de segment de réseau de sécurité

Nom de champ	Type de données	Description
Réservé	SWORD	Réservé, valeur = 0
ID de connexion de correction de temps	UDINT	Non utilisé: $FFFFFFFF_{hex}$ Utilisé: Instance de connexion de correction de temps: ID de connexion
EPI de correction de temps	UDINT	Non utilisé: 0 Utilisé: Instance de connexion de correction de temps:: EPI
Paramètres de connexion de réseau de correction de temps	WORD	Paramètres de connexion de réseau pour la connexion de correction de temps. Ce champ utilise la même définition que le paramètre de connexion de réseau contenu dans l'objet Gestionnaire de connexion. Non utilisé: 0 (Nul). Utilisé: Fixe, priorité élevée, multipoint

6.3.3.4 Segment de réseau de sécurité: format étendu (0x02)

Le format étendu est orienté vers la cible de la connexion et présenté dans le Tableau 8.

Toutes les connexions de sécurité EF doivent être établies au moyen du segment de réseau de sécurité de format étendu dans un service Forward Open (CP 2/2 ou CP 16/3) ou SafetyOpen (CP 2/3).

Tableau 8 – Format étendu de segment de réseau de sécurité

Nom de champ	Type de données	Description
Réservé	octet	Remplissage
CRC de configuration (SCCRC)	UDINT	CRC-S32 du segment de données de configuration cible. Une valeur de 0 indique que le contrôle SCID peut être omis.
Datation de configuration (SCTS)	DATE_AND_TIME	Date et heure de la configuration. Une valeur de 0 indique que le contrôle SCID peut être omis. Valeur de 6 octets (Date: 2 octets, Heure: 4 octets)
EPI de correction de temps	UDINT	Non utilisé: 0 Utilisé: Instance de connexion de correction de temps:: EPI
Paramètres de connexion de réseau de correction de temps	WORD	Paramètres de connexion de réseau pour la connexion de correction de temps. Ce champ utilise la même définition que le paramètre de connexion de réseau contenu dans l'objet Gestionnaire de connexion. Non utilisé: 0 (Nul). Utilisé: Fixe, priorité élevée, multipoint

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Nom de champ	Type de données	Description
Target_UNID (TUNID)	STRUCT de: UINT 10: octets	UNID de l'appareil cible. Cette valeur est une valeur de 10 octets constituée de l'identifiant de réseau de sécurité (6 octets) et de l'adresse de nœud (adresse de 4 octets)
UNID du point d'origine (OUNID)	STRUCT de: UINT 10: octets	UNID de l'appareil d'origine. Cette valeur est une valeur de 10 octets constituée de l'identifiant de réseau de sécurité (6 octets) et de l'adresse de nœud (adresse de 4 octets)
Ping_Interval_EPI_Multiplier	UINT	Nombre qui définit le Ping_Count_Interval pour la connexion. La plage de valeurs valides est donnée en 7.7.5.10
Time_Coord_Msg_Min_Multiplier	UINT	Pour l'instance de connexion de production. Plage valide comprise entre 0 et 7 813
Network_Time_Expectation_ Multiplier	UINT	Pour l'instance de connexion de consommation. Plage valide comprise entre 1 et 45 313
Timeout_Multiplier	USINT	Utilisé par le producteur et le consommateur pour la temporisation des connexions. Plage valide comprise entre 1 et 255 pour le format étendu
Max_Consumer_Number	USINT	Valeur: 1 (point à point), 2-15 (multipoint)
Max_Fault_Number	UINT	Nombre de paquets erronés sur une période d'une heure à l'issue de laquelle une connexion est fermée. Utilisé par les producteurs et les consommateurs. Valeur = 2
CRC des paramètres de connexion (CPCRC)	UDINT	CRC-S32 des paramètres de connexion cible dans cette demande
ID de connexion de correction de temps[a]	UDINT	Non utilisé: 0xFFFFFFFF Utilisé: Instance de connexion de correction de temps: ID de connexion
Datation initiale[a]	UINT	Utilisé par le consommateur pour initialiser Last_Time_Stamp_for_Rollover. Réglage du point d'origine de consommation sur 0xFFFF
Valeur de remplacement initiale[a]	UINT	Utilisé par le consommateur pour initialiser TS_Rollover_Count. Réglage du point d'origine de consommation sur 0xFFFF

[a] Ces champs NE sont PAS inclus dans le CPCRC.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

6.3.4 Règles du point d'origine pour le calcul du CRC de paramètre de connexion

Le CRC de paramètre de connexion (CPCRC) est calculé uniquement lors de la première configuration d'une connexion ou lors de la modification de cette configuration. Dans les autres cas, cette valeur reste statique dans le point d'origine.

La taille du chemin de connexion dans le service SafetyOpen change de valeur selon qu'un point d'origine envoie ou non des données de configuration. Dans la mesure où ce champ est inclus dans le calcul du CPCRC, il est nécessaire que les points d'origine calculent et conservent deux valeurs lorsqu'ils prennent en charge la fonction de configuration SafetyOpen. Une valeur permet de configurer un appareil tout en ouvrant la connexion, l'autre valeur permettant l'ouverture strictement dite de la connexion (aucune donnée de configuration n'est incluse).

La taille du chemin doit également être "préajustée" afin de supprimer les entrées de chemin "dépouillées" par les routeurs au moment où le service ForwardOpen de sécurité transite par chaque sous-réseau. L'exigence qui s'applique impose que le point d'origine soit chargé de calculer la valeur CPCRC sur la base de l'état réel du service SafetyOpen ou ForwardOpen au moment où la cible le reçoit, de sorte que cette dernière puisse effectuer un calcul simple dans tous les cas.

6.3.5 Organigrammes de traitement de SafetyOpen

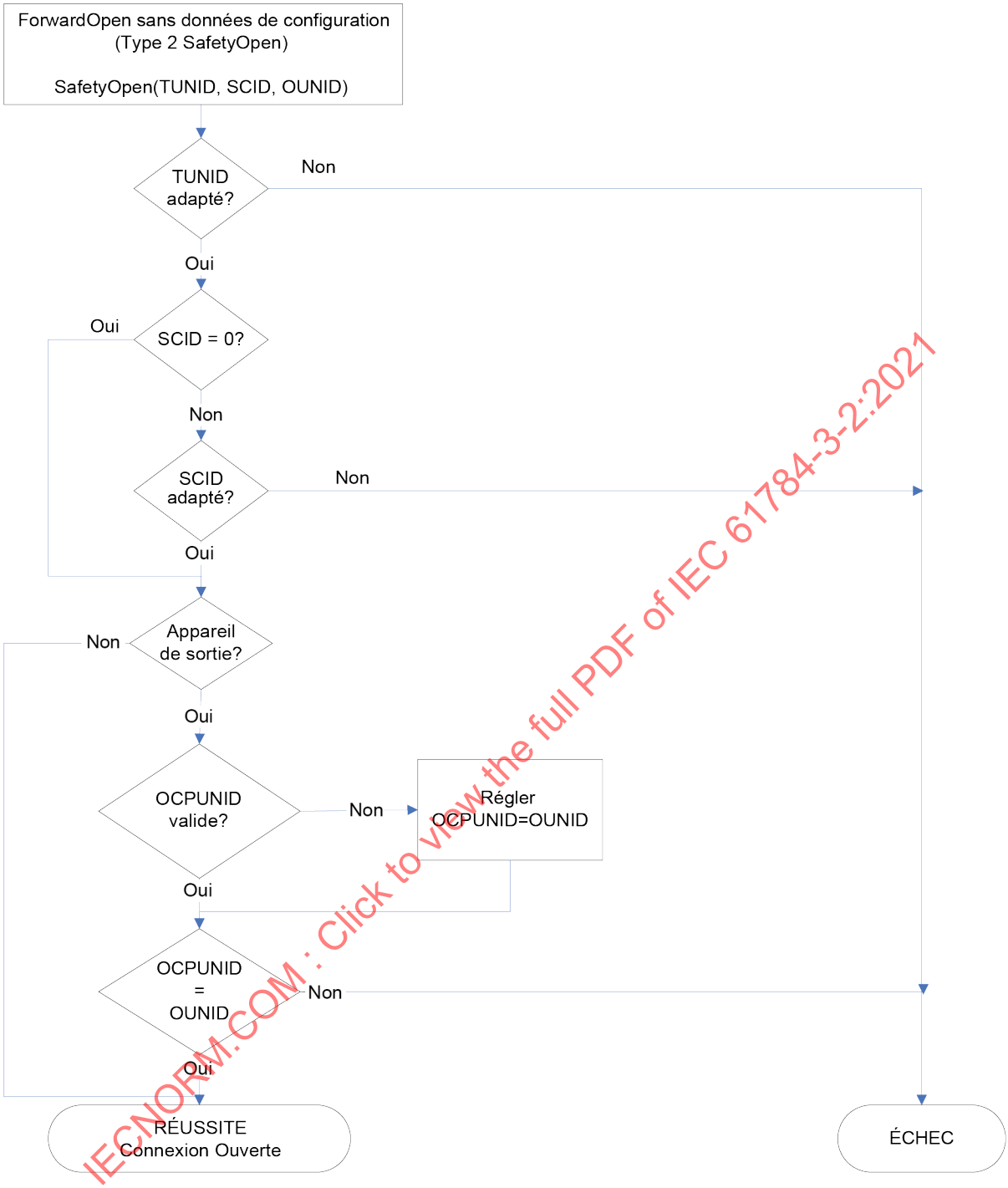
Les organigrammes suivants présentent le comportement exigé d'une cible à réception d'un service SafetyOpen:

a) vérifier le CRC de paramètre de connexion. Comme le représente la Figure 6, le CRC de paramètre de connexion couvre les champs SafetyOpen utilisés par la cible. Les routeurs disposés le long du chemin ne doivent pas modifier ces champs;

b) la cible vérifie la concordance du segment de clé électronique (voir 6.3.7);

c) selon le type de connexion de sécurité, la logique définie à la Figure 7 ou à la Figure 8 doit être observée.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021



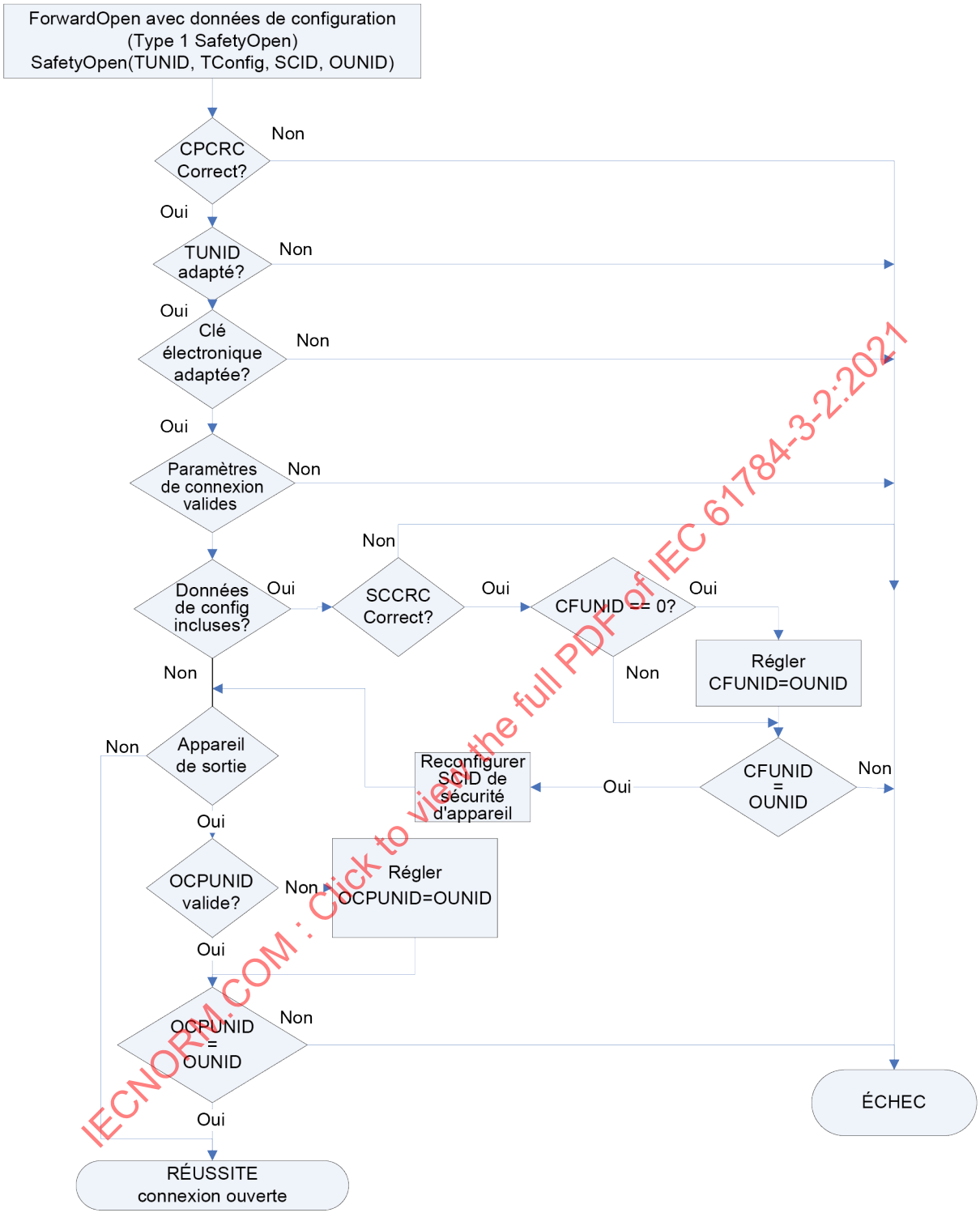
Légende :

UNID = Identifiant de réseau unique
SCID = ID de configuration de sécurité de la cible
OCP = Point de connexion de sortie
CFUNID = UNID de propriétaire de la configuration
TUNID = Identifiant de réseau unique de la cible
OUNID = Identifiant de réseau unique du point d'origine
OCPUNID = UNID de propriétaire de la connexion de sortie

IEC

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Figure 7 – Service SafetyOpen de traitement de cible sans données de configuration (SafetyOpen de type 2)



IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

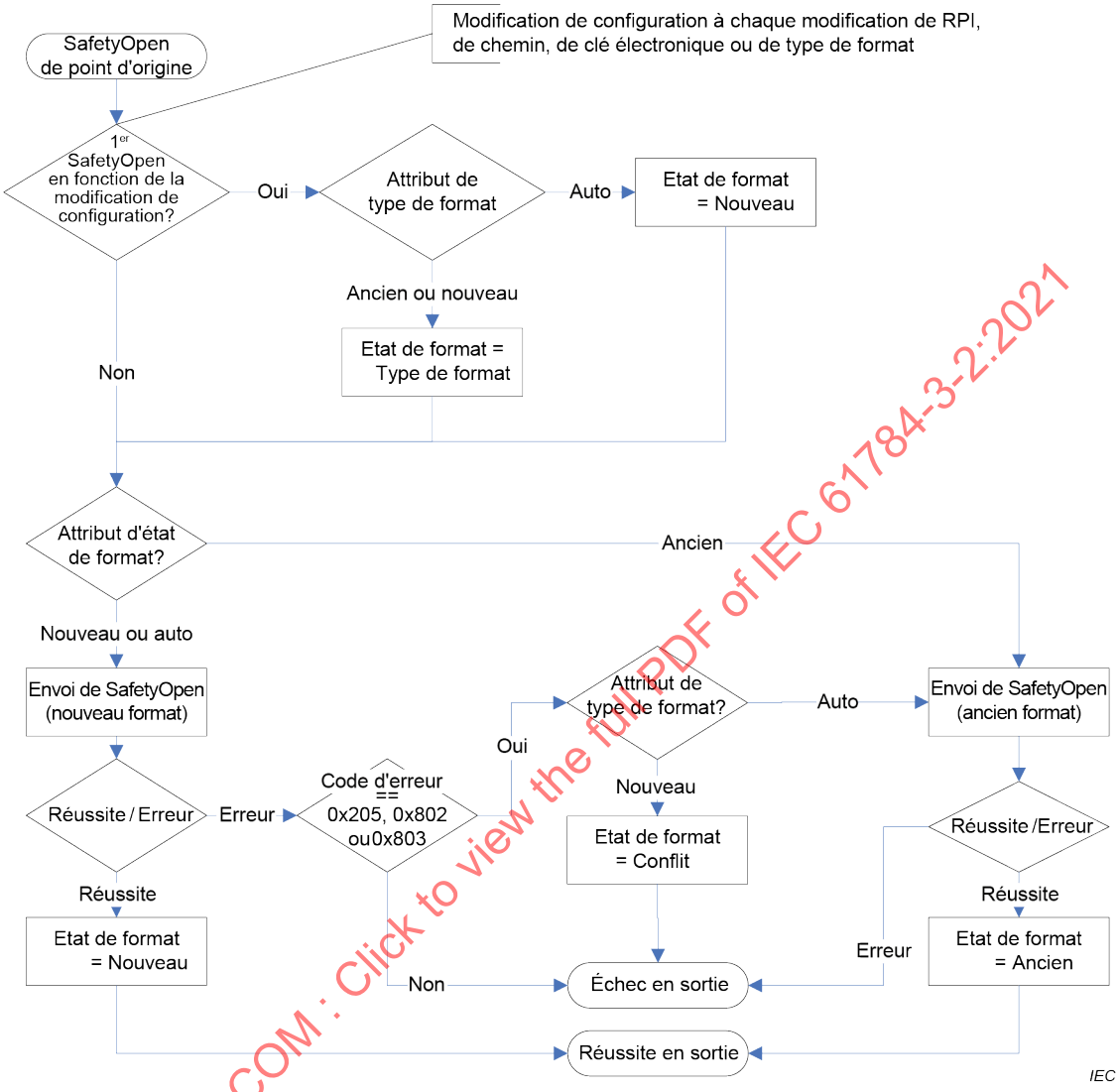
Légende :

UNID = Identifiant de réseau unique
CPCRC = CRC de paramètre de connexion
SCCRC= Partie CRC de SCID
OCPUNID = UNID de propriétaire de la connexion de sortie
TUNID = Identifiant de réseau unique de la cible
SCID = ID de configuration de sécurité de la cible
OUNID = Identifiant de réseau unique du point d'origine
CFUNID = UNID de propriétaire de la configuration

IEC

Figure 8 – Service SafetyOpen de traitement de cible avec données de configuration (SafetyOpen de type 1)

Les points d'origine de sécurité qui ne prennent en charge aucun autre moyen permettant de déterminer le format de connexion peuvent mettre en œuvre la logique représentée à la Figure 9 afin de déterminer le format de manière dynamique.



IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Figure 9 – Logique du point d'origine permettant de déterminer le format à utiliser

6.3.6 Contrôles exigés par les producteurs multipoints avec les connexions existantes

Il est visiblement possible que les paramètres de sécurité utilisés dans un service ForwardOpen ou SafetyOpen de différents points d'origine de consommation ne soient pas toujours identiques. Un ensemble cohérent de règles doit permettre de déterminer la méthode d'évaluation de ces paramètres par une cible de production multipoint, lorsque lesdits paramètres sont en contradiction avec d'autres connexions de consommation déjà établies. Le Tableau 9 définit les règles d'évaluation des paramètres de production multipoint.

Tableau 9 – Règles d'évaluation des paramètres de production multipoint

Paramètre de sécurité	Règle d'évaluation de production si la connexion existe	Réponse d'erreur[a] (le cas échéant)	
		Générale	Etendue
Multiplicateur EPI de Ping_Interval	Doit correspondre au P.I.E.M. existant	01_{hex}	0815_{hex}
Multiplicateur minimal de messages de coordination temporelle	Accepte n'importe lequel (peuvent être tous différents)	N/A	
Multiplicateur de délai du réseau	Accepte n'importe lequel (peuvent être tous différents)	N/A	
Timeout_Multiplier	Accepte n'importe lequel (peuvent être tous différents)	N/A	
Max_Consumer_Number	Doit correspondre au Max_Consumer_Number existant	01_{hex}	0816_{hex}
RPI T-to-O, RPI O-to-T	Doit correspondre aux RPI de connexion existants	01_{hex}	0112_{hex}
RPI de correction de temps	Doit correspondre aux RPI de correction de temps de connexion existants	01_{hex}	0801_{hex}
Type de segment de réseau de sécurité	Doit correspondre au format de connexion existant[b]	0x01	$0x817_{hex}$
Max_Fault_Number	Accepte n'importe lequel (peuvent être tous différents)	N/A	

[a] Une autre connexion peut également être ouverte en lieu et place de la transmission d'une réponse d'erreur, au choix du développeur d'appareils; cette flexibilité diffère des exigences spécifiées pour les connexions multipoints normalisées de la CPF 2.

[b] Les demandes de connexion ultérieures formulées sur une connexion multipoint existante doivent toutes avoir le même format que la connexion existante.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

6.3.7 Utilisation de la clé électronique de sécurité

Les points d'origine et cibles de sécurité doivent satisfaire aux exigences suivantes d'utilisation du segment Clé électronique dans un service SafetyOpen.

Ce segment doit être présent dans toutes les demandes de service SafetyOpen ou ForwardOpen de sécurité.

La clé électronique doit toujours être traitée par les appareils cibles avec intégrité (ne peut être confirmée de manière externe).

Le bit de compatibilité et le comportement de la clé électronique doivent être pris en charge par les points d'origine et cibles de sécurité, comme cela est défini. Les caractères de remplacement (champs définis sur 0) pour chaque champ interne de la clé électronique ne doivent pas être pris en charge.

6.3.8 RPI en fonction d'API dans les connexions de sécurité

Les appareils de sécurité n'ont pas la capacité de négocier la valeur RPI. Les cibles de sécurité acceptent le RPI demandé dans la mesure où il peut être pris en charge, ou le rejettent dans son intégralité. La tolérance relative à une demande RPI acceptable doit être de ± 128 µs.

Les intervalles API T-to-O, O-to-T et de correction de temps dans une réponse satisfaisante doivent toujours avoir la même valeur que celle reçue dans le service SafetyOpen.

6.3.9 Règles d'élaboration du chemin d'application pour les connexions de sécurité

6.3.9.1 Généralités

Les règles d'utilisation des trois chemins d'application cibles possibles contenus dans le paramètre Chemin de connexion d'un service ForwardOpen pour une connexion normale reposent sur les valeurs de type de connexion du paramètre de connexion réseau et la présence du segment de données défini dans l'IEC 61158-6-2.

Etant donné que les valeurs de type de connexion du paramètre de connexion réseau ne sont jamais nulles pour les connexions de sécurité, les règles d'élaboration du chemin d'application spécifiques aux connexions de sécurité sont fournies du 6.3.9.2 au 6.3.9.3.

6.3.9.2 Chemins d'application d'instance d'objet et/ou de point de connexion de l'ensemble

Les cibles E/S utilisent habituellement une combinaison d'instances d'objet et/ou de points de connexion pour identifier les données d'application disponibles sur une connexion cible donnée.

Lorsque des instances d'objet et/ou des points de connexion de l'ensemble sont utilisés pour identifier une cible de connexion de sécurité, 3 références (une pour la configuration, une pour les données consommées et une pour les données produites) doivent être fournies.

Les types de chemins possibles sont identifiés comme suit:

A. - [Classe] [Ensemble] [Instance] [Instance-configuration]

B. - [Classe] [Ensemble] [Instance] [Instance-producteur]

C. - [Classe] [Ensemble] [Instance] [Instance-consommateur]

D. - [Classe] [Ensemble] [Instance] [Instance NULLE définie par l'appareil]

E. - [CNP] [CNP consommateur]

F. - [CNP] [CNP producteur]

G. - [CNP] [CNP NUL défini par l'appareil]

Lorsque la classe de référence des 3 chemins est identique, leur format est souvent comprimé: (CNP désigne le Point de connexion).

[Classe] [N° classe] [Instance] [N° instance] [CNP] [CNP Consommateur] [CNP] [CNP Producteur]

Dans la mesure où la classe de référence des trois chemins doit être identique, une valeur d'instance NULLE doit être réservée dans cette classe (par les développeurs d'appareils) afin d'utiliser le format comprimé de sécurité. La valeur NULLE est utilisée pour la partie du chemin de référence de la connexion de coordination temporelle et de la connexion de configuration (dans les points d'origine de non-configuration). Lorsque la pratique ne permet pas l'utilisation d'une référence de classe commune, la forme longue doit être utilisée.

Les règles suivantes s'appliquent à l'élaboration du chemin SafetyOpen:

- tous les appareils doivent au minimum prendre en charge la forme longue;
- un chemin Nul ou un point de connexion Nul doit permettre de représenter la connexion de coordination temporelle;
- un chemin Nul ou un point de connexion Nul doit être utilisé pour le chemin de configuration lorsqu'aucune donnée de configuration ne peut être transmise sur la connexion;

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

- les points d'origine doivent toujours transmettre un chemin de configuration valide sur toutes les connexions qui peuvent accepter un service SafetyOpen de type 1, et ce, même en l'absence de toute donnée de configuration (c'est-à-dire type 2a).

Le chemin ou le point de connexion "Nul" utilisé doit relever du choix du module. La méthode qui permet d'effectuer ce choix dans un fichier EDS utilise le champ "Chemin de données" dans la section Gestionnaire de connexion. Les appareils configurés au moyen d'un applet de configuration doivent également fournir ce chemin.

Les concepteurs d'appareils de sécurité peuvent choisir le format de chemin à spécifier dans leurs fichiers EDS, parmi les options suivantes. Les combinaisons de trois chemins possibles pour les services SafetyOpen des types 1, 2a utilisés sur les connexions, qui acceptent les données de configuration, sont les suivantes:

- [A, D, B] pour les connexions d'entrée;
- format comprimé [A, G, F] pour les connexions d'entrée;
- [A, C, D] pour les connexions de sortie;
- format comprimé [A, E, G] pour les connexions de sortie.

Les combinaisons de trois chemins possibles pour les services SafetyOpen des types 2a, 2b utilisés sur les connexions, qui n'acceptent pas les données de configuration, sont les suivantes:

- [D, D, B] pour les connexions d'entrée;
- format comprimé [D, G, F] pour les connexions d'entrée;
- [D, C, D] pour les connexions de sortie;
- format comprimé [D, E, G] pour les connexions de sortie.

6.3.9.3 Chemins d'application de segment de symbole étendu ANSI

Les chaînes de caractères permettent fréquemment de fournir l'accès aux variables de processus définies par l'utilisateur sur les appareils qui les prennent en charge.

Lorsqu'un appareil prend en charge la production de données d'une variable de processus de sécurité sur une connexion d'entrée de sécurité, un seul chemin d'application qui comprend un segment de symbole étendu ANSI (voir l'IEC 61158-6-2) doit être utilisé pour coder le nom de chaîne de la variable de processus de sécurité.

Les règles suivantes s'appliquent à l'élaboration du chemin d'application du segment de symbole étendu ANSI.

- Aucune donnée de configuration ne peut être envoyée, car aucun chemin de configuration ne peut être spécifié.
- Aucune définition d'ensemble d'entrée n'est exigée, car le format de données de la variable de processus est défini par l'utilisateur.
- La connexion O-to-T est la connexion de coordination temporelle.
- La connexion T-to-O contient les données de la variable de processus de sécurité. Le format de chemin EDS du chemin d'application unique est "SYMBOL_ANSI" (voir l'IEC 61158-6-2 pour plus d'informations) pour les connexions SafetyOpen de type 2a, 2b.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

6.3.10 Types de connexions de l'objet de validation de sécurité

La fonction Objet de validation de sécurité, selon le type de connexion de sécurité prévu dans le service SafetyOpen, exige toujours entre deux et trois ressources de connexion. Le service SafetyOpen comporte les informations de connexion qui permettent à une cible d'établir ces connexions de manière appropriée. Le présent 6.3.10 indique de quelle manière sont déterminés les types de connexions, ainsi que la manière dont le service SafetyOpen doit être rempli.

Une hypothèse de base repose sur le fait que les connexions pour les messages de coordination et de correction de temps n'exigent aucune entrée de chemin, dans la mesure où elles comportent un chemin implicite d'accès à l'Objet de validation de sécurité qui coordonne la connexion de sécurité. Les différents scénarios de connexion sont décrits dans l'Objet de validation en 6.7.

La fonction Objet de validation de sécurité peut déterminer le type de ressources de connexion exigé en observant le paramètre du service SafetyOpen. Les différents paramètres de service SafetyOpen, ainsi que les paramètres clés dont a besoin la fonction de sécurité pour déterminer les types de connexions sont définis dans le Tableau 10 pour les connexions qui comportent des chemins d'application d'instances d'objet et/ou de point de connexion, et dans le Tableau 11 pour les connexions qui comportent un chemin d'application de segment de symbole étendu ANSI.

Les instances d'objet de connexion peuvent être indisponibles en raison de la capacité ou des limites de l'identifiant de cible; il est possible que les identifiants de connexion non attribués ne soient pas disponibles. L'appareil peut également ne pas disposer de la capacité suffisante nécessaire au traitement de la connexion supplémentaire; etc. Les objets Connexion de sécurité exigent des ressources similaires aux connexions E/S normalisées.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Tableau 10 – Options de paramétrage du service ForwardOpen pour les connexions de sécurité qui comportent des chemins d'application qui reposent sur des objets

Type de connexion O-to-T	Type de connexion T-to-O	Type de transport/ déclencheur	Chemin d'application 1	Chemin d'application 2[a]	Chemin d'application 3[a]	Nombre maximal de consommateurs	Type de connexion de l'objet de validation de sécurité	Facteurs de décision clés	Rôle cible
Point à point	Point à point	Application, classe 0, client	Chemin nul défini par le fournisseur [b]	Chemin nul défini par le fournisseur	Objet d'application d'entrée de sécurité	1	Point à point Producteur (Entrée)	2-point à point + Client	Connexion de production: Données de sécurité Connexion de consommation: Coordination
Point à point	Point à point	Application, classe 0, serveur	Chemin nul défini par le fournisseur	Objet d'application de sortie de sécurité	Chemin nul défini par le fournisseur	1	Point à point Consommateur (Sortie)	2-point à point + Serveur	Connexion de consommation: Données de sécurité Connexion de production: Coordination
Point à point	Multi-point	Application, classe 0, client	Chemin nul défini par le fournisseur	Chemin nul défini par le fournisseur	Objet d'application d'entrée de sécurité	2-15	Producteur multi-point CP 2/3	2 – Multipoint + 1 point à point + Client	Connexion de production: Données de sécurité Connexion de production: Correction Connexion de consommation: coordination

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Type de connexion O-to-T	Type de connexion T-to-O	Type de transport/ déclencheur	Chemin d'application 1	Chemin d'application 2[a]	Chemin d'application 3[a]	Nombre maximal de consommateurs	Type de connexion de l'objet de validation de sécurité	Facteurs de décision clés	Rôle cible
Point à point	Multipoint	Application, classe 0, client	Chemin nul défini par le fournisseur	Chemin nul défini par le fournisseur	Objet d'application d'entrée de sécurité	2-15	Producteur multipoint CP 2/2	1 – Multipoint + 1 point à point + Client	Connexion de production: Données de sécurité + correction Connexion de consommation: Coordination
Multipoint	Point à point	Application, classe 0, serveur	Chemin nul défini par le fournisseur	Objet d'application de sortie de sécurité	Chemin nul défini par le fournisseur	2-15	Consommateur multipoint CP 2/3	2 – Multipoint + 1 point à point + Serveur	Connexion de consommation: Données de sécurité Connexion de consommation: Correction Connexion de production: coordination
Multipoint	Point à point	Application, classe 0, serveur	Chemin nul défini par le fournisseur	Objet d'application de sortie de sécurité	Chemin nul défini par le fournisseur	2-15	Consommateur multipoint CP 2/2	1 – Multipoint + 1 point à point + Serveur	Connexion de consommation: Données de sécurité + correction Connexion de production: coordination

[a] Entrée et sortie par rapport au réseau.

[b] Les appareils configurables par EDS doivent définir un chemin nul d'application dans le fichier EDS.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Tableau 11 – Options de paramétrage du service ForwardOpen pour les connexions de sécurité qui comportent un chemin d'application de segment de symbole étendu ANSI

Type de connexion O-to-T	Type de connexion T-to-O	Type de transport/ déclencheur	Chemin d'application	Nombre maximal de consom-mateurs	Type de connexion de l'objet de validation de sécurité	Facteurs de décision clés	Rôle cible
Point à point	Point à point	Application, classe 0, client	Segment de symbole étendu ANSI	1	Point à point Producteur (Entrée)	2-point à point + Client	Connexion de production: Données de sécurité Connexion de consom-mation: Coordina-tion
Point à point	Multipoint	Application, classe 0, client	Segment de symbole étendu ANSI	2-15	Producteur multipoint CP 2/3	2 – Multipoint + 1 point à point + Client	Connexion de production: Données de sécurité Connexion de production: Correction Connexion de consom-mation: coordina-tion
Point à point	Multipoint	Application, classe 0, client	Objet d'application d'entrée de sécurité	2-15	Producteur multipoint CP 2/2	1 – Multipoint + 1 point à point + Client	Connexion de production: Données de sécurité + correction Connexion de consomma tion: Coordina-tion

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Le Tableau 12 définit les paramètres de connexion de réseau à utiliser pour l'ensemble des trois connexions associées à chaque type de connexion de sécurité.

Tableau 12 – Paramètres de connexion de réseau pour les connexions de sécurité

Type de cible	Paramètre de connexion de réseau	Valeur de paramètre correcte	Description
Producteur point à point	O-to-T	4406_{hex}	Priorité élevée point à point, fixe
	T-to-O	4408_{hex}	Priorité élevée point à point, fixe
	Correction de temps	0000_{hex}	Non utilisé
Producteur point à point	O-to-T	4408_{hex}	Priorité élevée point à point, fixe
	T-to-O	4406_{hex}	Priorité élevée point à point, fixe
	Correction de temps	0000_{hex}	Non utilisé
Producteur multipoint	O-to-T	4406_{hex}	Priorité élevée point à point, fixe
	T-to-O	$240E_{hex}$	Priorité élevée multipoint, fixe
	Correction de temps	2406_{hex}	Priorité élevée multipoint, fixe

Les réponses SafetyOpen satisfaisantes doivent renvoyer les identifiants de connexion utilisés, ainsi que le Consumer_Number attribué au point d'origine (toujours $FFFF_{hex}$ pour les connexions point à point).

6.3.11 Données de réponse d'application dans une réponse SafetyOpen satisfaisante

Le format d'une réponse SafetyOpen satisfaisante est identique à celui de la Forward_Open_Reply défini dans l'IEC 61158-6-2. La transmission des données en retour est définie dans le Tableau 13.

La cible d'une fonction SafetyOpen doit renvoyer les données, définies du Tableau 13 au Tableau 16, dans le champ Réponse d'application de la réponse SafetyOpen. Le nombre de consommateurs et les données de réponse PID ne sont importants que lorsque le point d'origine est le consommateur.

Tableau 13 – Réponse d'application de cible SafetyOpen (taille: 10 octets)

Nom de paramètre	Type de données	Description
Consumer_Number	UINT	
PID/CID	STRUCT de:	Identifiant de cible qui permet de générer une valeur de départ du PID ou du CID
ID du fournisseur cible	UINT	ID du fournisseur de cible
Numéro de série de l'appareil cible	UDINT	Numéro de série de l'appareil cible
Numéro de série de connexion cible	UINT	Numéro de série de connexion cible attribué à la connexion. L'identifiant d'instance de l'objet de validation de sécurité doit être utilisé

Lorsque la cible d'une connexion utilise le format étendu avec les liaisons CP 2/2 ou CP 16/3, elle doit utiliser la réponse d'application de cible SafetyOpen EF de 14 octets définie dans le Tableau 14.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Tableau 14 – Réponse d'application de cible SafetyOpen EF CP 2/2 ou CP 16/3 (taille: 14 octets)

Nom de paramètre	Type de données	Description
Consumer_Number	UINT	
PID/CID	STRUCT de:	Identifiant de cible qui permet de générer une valeur de départ du PID ou du CID
ID du fournisseur cible	UINT	ID du fournisseur de cible
Numéro de série de l'appareil cible	UDINT	Numéro de série de l'appareil cible
Numéro de série de connexion cible	UINT	Numéro de série de connexion cible attribué à la connexion. L'identifiant d'instance de l'objet de validation de sécurité doit être utilisé
Datation initiale[a]	UINT	Utilisé par le consommateur pour initialiser Last_Time_Stamp_for_Rollover
Valeur de remplacement initiale[a]	UINT	Utilisé par le consommateur pour initialiser TS_Rollover_Count

[a] Les producteurs point à point renvoient les valeurs reçues dans la fonction SafetyOpen. Les producteurs multipoints ainsi que les consommateurs point à point répondent avec leurs valeurs internes (par exemple, Clock_Count_RC_Offset).

Tableau 15 – Réponse d'application de cible SafetyOpen BF CP 2/3 (taille: 18 octets)

Nom de paramètre	Type de données	Description
Consumer_Number[a]	UINT	
PID/CID	STRUCT de:	Identifiant de cible qui permet de générer une valeur de départ du PID ou du CID
ID du fournisseur cible	UINT	ID du fournisseur de cible
Numéro de série de l'appareil cible	UDINT	Numéro de série de l'appareil cible
Numéro de série de connexion cible	UINT	Numéro de série de connexion cible attribué à la connexion. L'identifiant d'instance de l'objet de validation de sécurité doit être utilisé
Time_Correction_Connection_ID[a]	UDINT	Identifiant de connexion choisi par la cible pour la connexion de correction de temps. La valeur est retournée si elle est choisie par le point d'origine
Time_Correction_API	UDINT	Renvoie la même valeur reçue dans le paquet Demande

[a] Lorsqu'une cible de sécurité CP 2/3 reçoit une fonction SafetyOpen qui n'est pas multipoint (aucune connexion de correction de temps n'est alors établie), le paramètre Time_Correction_Connection_ID doit être défini sur $FFFF_{hex}$. Si la cible n'est pas un producteur multipoint, le nombre de consommateurs est défini sur $FFFF_{hex}$.

Lorsque la cible d'une connexion utilise le format étendu sur le CP 2/3, elle doit utiliser la réponse d'application de cible SafetyOpen EF de 22 octets définie dans le Tableau 16.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Tableau 16 – Réponse d'application de cible SafetyOpen EF CP 2/3 (taille: 22 octets)

Nom de paramètre	Type de données	Description
Consumer_Number[a]	UINT	
PID/CID	STRUCT de:	Identifiant de cible qui permet de générer une valeur de départ du PID ou du CID
ID du fournisseur cible	UINT	ID du fournisseur de cible
Numéro de série de l'appareil cible	UDINT	Numéro de série de l'appareil cible
Numéro de série de connexion cible	UINT	Numéro de série de connexion cible attribué à la connexion. L'identifiant d'instance de l'objet de validation de sécurité doit être utilisé
Time_Correction_Connection_ID[a]	UDINT	Identifiant de connexion choisi par la cible pour la connexion de correction de temps. La valeur est retournée si elle est choisie par le point d'origine
Time_Correction_API	UDINT	Renvoie la même valeur reçue dans le paquet Demande
Datation initiale[b]	UINT	Utilisé par le consommateur pour initialiser Last_Time_Stamp_for_Rollover
Valeur de remplacement initiale[b]	UINT	Utilisé par le consommateur pour initialiser TS_Rollover_Count

[a] Lorsqu'une cible de sécurité CP 2/3 reçoit une fonction SafetyOpen qui n'est pas multipoint (aucune connexion de correction de temps n'est alors établie), le paramètre Time_Correction_Connection_ID doit être défini sur $FFFF_{hex}$. Si la cible n'est pas un producteur multipoint, le nombre de consommateurs est défini sur $FFFF_{hex}$.

[b] Les producteurs point à point renvoient les valeurs reçues dans la fonction SafetyOpen. Les producteurs multipoints ainsi que les consommateurs point à point répondent avec leurs valeurs internes (par exemple, Clock_Count_RC_Offset).

6.3.12 Réponse SafetyOpen non satisfaisante

La fonction SafetyOpen comporte certains cas d'erreurs spéciaux qui ne sont pas mappés avec l'ensemble existant de codes d'erreurs, et étend la définition des codes d'erreurs existants.

Le Tableau 17 définit de nouveaux codes d'erreurs étendus de sécurité et présente la définition étendue des codes d'erreurs existants.

Tableau 17 – Nouveaux codes d'erreurs étendus de sécurité

Etat général	Etat étendu	Explication
01_{hex}	0105_{hex}	Conflit de propriété ou non-concordance de l'OUNID. La configuration est déjà propriété d'un autre point d'origine
01_{hex}	0106_{hex}	Conflit de propriété ou non-concordance de l'OUNID. La connexion de sortie était déjà propriété d'un autre point d'origine
01_{hex}	0205_{hex}	Erreur de paramètre dans le service Unconnected Send (Envoi non connecté) ou Erreur de paramètre dans le service SafetyOpen ou SafetyClose
01_{hex}	0801_{hex}	RPI multipoint incompatible. Une connexion existante a été établie à un RPI différent
01_{hex}	0802_{hex}	Taille de connexion de sécurité invalide
01_{hex}	0803_{hex}	Format de connexion de sécurité invalide
01_{hex}	0804_{hex}	Paramètres de connexion de correction de temps invalides
01_{hex}	0805_{hex}	Multiplicateur EPI d'intervalles Ping invalide
01_{hex}	0806_{hex}	Multiplicateur minimal de messages de coordination temporelle

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Etat général	Etat étendu	Explication
01_{hex}	0807_{hex}	Multiplicateur de délai du réseau
01_{hex}	0808_{hex}	Multiplicateur de temporisation
01_{hex}	0809_{hex}	Nombre maximal de consommateurs invalide
01_{hex}	$080A_{hex}$	CPRC invalide
01_{hex}	$080B_{hex}$	ID de connexion de correction de temps invalide
01_{hex}	$080C_{hex}$	Non-concordance du SCID. La valeur de SCID était non nulle et ne correspondait pas à la valeur de la cible
01_{hex}	$080D_{hex}$	TUNID non défini. L'appareil est sorti d'usine et le TUNID n'a pas été défini, les connexions ne sont donc pas admises
01_{hex}	$080E_{hex}$	Non-concordance du TUNID. Le TUNID fourni ne correspond pas. Le message a été vraisemblablement acheminé vers ce nœud par erreur
01_{hex}	$080F_{hex}$	Opération de configuration non admise
01_{hex}	0815_{hex}	Multiplicateur EPI d'intervalles Ping multipoints incompatible. Une connexion existante a été établie avec un multiplicateur EPI d'intervalles Ping différent.
01_{hex}	0816_{hex}	Nombre maximal de consommateurs multipoints incompatible. Une connexion existante a été établie avec un nombre maximal de consommateurs différent.
01_{hex}	0817_{hex}	Type de segment de réseau de sécurité multipoint incompatible. Une connexion existante a été établie avec un type de segment de réseau de sécurité différent.

[a] Les plages de codes d'état étendus réservés pour FSCP 2/1 sont définies de 0801_{hex} à $080F_{hex}$ et de 0815_{hex} à 0834_{hex} (voir CPF 2).

Le Tableau 18 de matrice d'événements/erreurs fournit des recommandations concernant les codes d'erreurs à appliquer pour les erreurs potentielles détectées lors du traitement d'un service SafetyOpen. Ces recommandations ne sont pas censées constituer une liste exhaustive.

Tableau 18 – Tableau de recommandations concernant les événements d'erreur SafetyOpen

Evénement	Type d'erreur	Etat général	Etat étendu
L'appareil cible a reçu une demande SafetyOpen dans des états de l'objet Programme de contrôle de sécurité autres que l'état Repos et l'état Exécution	Opération de configuration non admise	01_{hex}	$080F_{hex}$
	Appareil non configuré	01_{hex}	110_{hex}
Type (nom) de connexion de sécurité invalide	Erreur de paramètre de sécurité – Type de connexion invalide	01_{hex}	315_{hex}
Taille de connexion de sécurité invalide	Erreur de paramètre de sécurité – Taille de connexion de sécurité invalide	01_{hex}	0802_{hex}
Format de connexion de sécurité invalide	Erreur de paramètre de sécurité – Format de connexion de sécurité invalide	01_{hex}	0803_{hex}
Paramètres de connexion de correction de temps invalides	Erreur de paramètre de sécurité – Paramètres de connexion de correction de temps invalides	01_{hex}	0804_{hex}
Multiplicateur EPI d'intervalles Ping hors plage	Erreur de paramètre de sécurité – Multiplicateur EPI d'intervalles Ping invalide	01_{hex}	0805_{hex}

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Evénement	Type d'erreur	Etat général	Etat étendu
Multiplicateur minimal de messages de coordination temporelle hors plage	Erreur de paramètre de sécurité – Multiplicateur minimal de messages de coordination temporelle	01_{hex}	0806_{hex}
Multiplicateur de délai hors plage	Erreur de paramètre de sécurité – Multiplicateur de délai	01_{hex}	0807_{hex}
Multiplicateur de temporisation hors plage	Erreur de paramètre de sécurité – Multiplicateur de temporisation	01_{hex}	0808_{hex}
Nombre maximal de consommateurs non compris dans les limites du producteur multipoint	Erreur de paramètre de sécurité – Nombre maximal de consommateurs invalide	01_{hex}	0809_{hex}
Valeur CPCRC dans SafetyOpen et valeur CPCRC calculée	Erreur de paramètre de sécurité – CPRC invalide	01_{hex}	$080A_{hex}$
ID de connexion de correction de temps Invalide	Erreur de paramètre de sécurité – ID de connexion de correction de temps invalide	01_{hex}	$080B_{hex}$
Le RPI demandé n'est pas compatible avec les connexions multipoints établies précédemment	RPI multipoint incompatible	01_{hex}	801_{hex}
RPI O-to-T, RPI T-to-O, ou RPI de correction de temps non pris en charge	RPI non pris en charge	01_{hex}	0111_{hex}
Toutes les instances de l'objet de validation de sécurité sont utilisées	Le gestionnaire de connexion ou l'objet de connexion ne peut pas prendre en charge davantage de connexions	01_{hex}	0113_{hex}

6.3.13 Service ForwardClose de sécurité

Aucun comportement supplémentaire n'est défini pour le service ForwardClose lorsqu'il est utilisé pour fermer une connexion de sécurité. Dans les exigences de sécurité suivantes, le terme "SafetyClose" fait référence tant au service ForwardClose de l'objet Gestionnaire de connexion, qu'au service SafetyClose de l'objet Connexion.

Le service SafetyClose doit être utilisé pour fermer les connexions avec une cible de sécurité (et tous les autres nœuds du chemin de connexion dans le cas d'un service ForwardClose).

La demande SafetyClose doit supprimer une connexion parmi tous les nœuds qui participent à la connexion d'origine.

La demande SafetyClose doit occasionner la désaffectation de toutes les ressources dans l'ensemble des nœuds qui participent à la connexion, y compris les ID de connexion, la largeur de bande et les mémoires tampons internes.

Les cibles qui reçoivent la demande de service SafetyClose doivent fermer la connexion pour laquelle les paramètres de l'ID du fournisseur du point d'origine, du numéro de série de connexion et du numéro de série du point d'origine correspondent. Les informations supplémentaires fournies par ce service (c'est-à-dire le chemin de connexion) doivent être ignorées par la cible.

Une réponse SafetyClose satisfaisante doit être transmise après suppression de la connexion au niveau de la cible.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

A réception d'une réponse SafetyClose satisfaisante, le point d'origine et chaque nœud intermédiaire le long du chemin, ferment la connexion et libèrent les ressources associées à cette connexion. Toutefois, le point d'origine doit également fermer la connexion si aucune réponse n'est reçue au cours d'une période d'attente choisie par le fournisseur.

6.4 Objet Identité

6.4.1 Généralités

Code de classe: 01_{hex}

Le présent 6.4 décrit les modifications apportées à l'objet Identité pour prendre en charge la sécurité.

Tous les appareils de sécurité CPF 2 doivent substituer le comportement défini dans l'objet Programme de contrôle de sécurité au comportement d'état de l'objet Identité.

6.4.2 Modifications apportées aux services communs

Le Tableau 19 définit les services de l'objet Identité qui exigent des actualisations.

Tableau 19 – Modifications apportées aux services communs de l'objet Identité

Code de service	Mise en œuvre nécessaire		Nom du service	Description du service
	Classe	Instance		
05_{hex}	n/a	Facultatif[a]	Réinitialisation	Appelle éventuellement le service Réinitialisation de type 0 pour l'appareil.

[a] Conditionnel – Les appareils de sécurité ne sont autorisés à prendre en charge, de manière facultative, le service Réinitialisation d'identité de type 0 qu'en l'absence de connexions E/S de sécurité ou normales. Si des connexions E/S sont établies, l'appareil doit répondre par une erreur "Etat de l'appareil". Ce service, lorsqu'il est exécuté, doit agir sur l'intégralité de l'appareil. Lorsqu'un appareil prend en charge le type de réinitialisation 0, tous les autres types de réinitialisations d'identité ne doivent pas être pris en charge et doivent répondre à toute demande qui comporte une erreur "Paramètre invalide (0x20)".

6.4.3 Extensions pour les appareils CP 16/3

Les extensions de l'objet Identité des appareils CP 16/3 sont spécifiées dans le Tableau 20.

Certains attributs des extensions de l'objet pour CP 16/3 renvoient à des IDN (Numéros d'identification) de CP 16/3 qui utilisent la nomenclature de CP 16/3, par exemple S-0-1300. Ces IDN de CP 16/3 sont décrits en détail dans l'IEC 61158-4-19.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Tableau 20 – Extensions de l'objet Identité pour les appareils CP 16/3

ID d'attribut	Mise en œuvre nécessaire	Règle d'accès	Nom	Type de données	Description de l'attribut	Sémantique de la valeur
1	Exigé	Obtenir	ID du fournisseur	Voir l'IEC 61158-5-2		
2	Exigé	Obtenir	Type d'appareil	Voir l'IEC 61158-5-2		
3	Exigé	Obtenir	Code produit	Voir l'IEC 61158-5-2		
4	Exigé	Obtenir	Révision	Voir l'IEC 61158-5-2		
5	Exigé	Obtenir	Etat	Voir l'IEC 61158-5-2		
6	Exigé	Obtenir	Numéro de série	Voir l'IEC 61158-5-2		
7	Exigé	Obtenir	Nom du produit	Voir l'IEC 61158-5-2		Les 32 premiers caractères de CP 16/3 S-0-1300.x.4
8-18	Facultatif	Voir l'IEC 61158-5-2				

6.5 Objets de liaison

6.5.1 Modifications apportées à l'objet DeviceNet

6.5.1.1 Attribut supplémentaire de sécurité

Code de classe: 03_{hex}

Le présent 6.5.1 définit les modifications et ajouts exigés de l'objet DeviceNet pour prendre en charge la sécurité. Un attribut doit être ajouté pour permettre la lecture du numéro de réseau de sécurité (SNN). La définition de cet attribut est donnée dans le Tableau 21.

Tableau 21 – Nouvel attribut instance de l'objet DeviceNet

ID d'attribut	Mise en œuvre nécessaire	Règle d'accès	Nom	Type de données	Description de l'attribut	Sémantique de la valeur
11	Exigé	Obtenir	Safety Network Number (Numéro de réseau de sécurité)	6 OCTETS	Numéro unique dans l'ensemble du système pour le sous-réseau sur lequel repose cet appareil	L'attribut doit contenir la partie SNN du TUNID dans le programme de contrôle de sécurité. Voir 8.2 pour une définition plus précise de cet attribut

Les appareils qui mettent en œuvre le FSCP 2/1 sur le CP 2/3 doivent prendre en charge l'attribut 11 de l'objet DeviceNet.

6.5.1.2 Limitation de connexion rapide de sécurité

Tous les appareils de sécurité CP 2/3 ne doivent pas prendre en charge la fonction Connexion rapide. L'attribut Connexion Rapide ne doit pas être pris en charge et doit répondre à tout service d'attribut Obtenir/Définir avec le code d'erreur "Attribut non pris en charge".

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

6.5.2 Modifications apportées à l'objet Interface TCP/IP

Code de classe: $F5_{hex}$

Le présent 6.5.2 définit les modifications et ajouts exigés de l'objet Interface TCP/IP pour prendre en charge la sécurité. Un attribut doit être ajouté pour permettre la lecture du numéro de réseau de sécurité (SNN). La définition de cet attribut est donnée dans le Tableau 22.

Tableau 22 – Nouvel attribut instance de l'objet Interface TCP/IP

ID d'attribut	Mise en œuvre nécessaire	Règle d'accès	Nom	Type de données	Description de l'attribut	Sémantique de la valeur
7	Exigé	Obtenir	Safety Network Number (Numéro de réseau de sécurité)	6 OCTETS	Numéro unique dans l'ensemble du système pour le sous-réseau sur lequel repose cet appareil	L'attribut doit contenir la partie SNN du TUNID dans le programme de contrôle de sécurité. Voir 8.2 pour une définition plus précise de cet attribut

Les appareils qui mettent en œuvre le FSCP 2/1 sur le CP 2/2 Sécurité doivent prendre en charge l'attribut 7 de l'objet Interface TCP/IP.

6.5.3 Objet Liaison SERCOS III

6.5.3.1 Généralités

Code de classe: $4C_{hex}$

Le présent 6.5.3 fournit des informations sur l'objet Liaison SERCOS III. Cet objet doit être présent dans tous les produits qui prennent en charge le FSCP 2/1 sur le CP 16/3. Si des liaisons CP 16/3 multiples existent dans un appareil, plusieurs instances de l'objet Liaison SERCOS III doivent être utilisées. L'attribut 1 permet de lire le numéro de réseau de sécurité (SNN).

6.5.3.2 Attributs de classe

Les attributs de classe de l'objet Liaison SERCOS III sont définis dans le Tableau 23.

Tableau 23 – Attributs de classe de l'objet Liaison SERCOS III

ID d'attribut	Mise en œuvre nécessaire	Règle d'accès	Nom	Type de données	Description de l'attribut	Sémantique de la valeur
1	Cet attribut est facultatif et est décrit dans l'IEC 61158-5-2					
2	Conditionnel[a]	Obtenir	Instance maximale	UINT	Nombre maximal d'instances d'un objet actuellement créé à ce niveau de hiérarchie de classe de l'appareil	Nombre le plus élevé d'instances d'un objet créé à ce niveau de hiérarchie de classe
3 à 7	Cet attribut est facultatif et est décrit dans l'IEC 61158-5-2					

[a] Si l'appareil a plusieurs liaisons d'interface CP 16/3, cet attribut doit être pris en charge.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

6.5.3.3 Attributs instance

Les attributs instance de l'objet Liaison SERCOS III sont définis dans le Tableau 24.

Tableau 24 – Attributs instance de l'objet Liaison SERCOS III

ID d'attribut	Mise en œuvre nécessaire	Règle d'accès	Nom	Type de données	Description de l'attribut	Sémantique de la valeur
1	Exigé	Obtenir	Safety Network Number (Numéro de réseau de sécurité)	6 OCTETS	Numéro unique dans l'ensemble du système pour le sous-réseau sur lequel repose cet appareil	L'attribut doit contenir la partie SNN du TUNID dans le programme de contrôle de sécurité. Voir 8.2 pour une définition plus précise de cet attribut
2	Facultatif	Obtenir	Durée du cycle de communication	UDINT	CP 16/3 S-0-1002	
3	Facultatif	Obtenir	Etat d'interface	WORD	CP 16/3 S-0-1014	
4	Facultatif	Obtenir	Compteur d'erreurs MST-P/S	UINT	CP 16/3 S-0-1028	
5	Facultatif	Obtenir	Compteur d'erreurs Port1 et Port2	Struct de:	CP 16/3 S-0-1035	
			Compteur d'erreurs Port1	UINT		
			Compteur d'erreurs Port2	UINT		
6	Facultatif	Obtenir	Adresse SERCOS®	UINT	CP 16/3 S-0-1040	

6.5.3.4 Services communs

La définition des services communs de l'objet Liaison SERCOS III est donnée dans le Tableau 25.

Tableau 25 – Services communs de l'objet Liaison SERCOS III

Code de service	Mise en œuvre nécessaire		Nom du service	Description du service
	Classe	Instance		
$0E_{hex}$	Conditionnel[a]	Exigé	Get_Attribute_Single	Utilisé pour lire un attribut d'objet

[a] Conditionnel – Exigé si un attribut de classe est pris en charge.

6.6 Objet Programme de contrôle de sécurité

6.6.1 Généralités

Code de classe: 39_{hex}

Le programme de contrôle de sécurité constitue l'objet central des appareils de sécurité FSCP 2/1. Deux mises en œuvre fondamentales du programme de contrôle de sécurité sont définies:

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

- programme de contrôle de référence – défini comme une mise en œuvre de contrôle qui prend en charge tous les attributs et services "exigé" définis par cette définition d'objet. Ce programme de référence inclut tous les comportements de diagrammes d'états, à l'exclusion du traitement des événements d'état pour les services non exigés (voir 6.6.8);
- programme de contrôle SNCT – défini comme une mise en œuvre de contrôle qui prend en charge la fonctionnalité de référence dans son intégralité, ainsi que les attributs et services qui portent le marquage "conditionnel" sur le support SNCT.

Tous les appareils de sécurité installés sur un réseau de sécurité FSCP 2/1 doivent prendre en charge la définition du Programme de contrôle de sécurité de référence.

De nombreux paramètres de l'objet Programme de contrôle de sécurité étant jugés critiques pour la sécurité, les attributs de cet objet doivent avoir une intégrité plus élevée que les données d'objet normalisées.

Le comportement d'état de l'objet Programme de contrôle de sécurité doit contrôler l'état de l'appareil complet. Tous les objets d'un appareil de sécurité doivent être asservis aux états et commandes du Programme de contrôle de sécurité afin de gérer ses fonctions et ses comportements.

L'objet Programme de contrôle de sécurité centralise les définitions d'état d'objet d'application et les informations d'état associées, les indications d'état d'exception (alarmes et avertissements), et définit un modèle de comportement retenu par hypothèse par les objets identifiés comme appartenant à des appareils de sécurité. En d'autres termes, si l'instance d'objet Programme de contrôle de sécurité est soumise à une demande de réinitialisation, la réinitialisation est effectuée par cette instance d'objet, ainsi que par l'ensemble des objets d'application associés.

L'objet Programme de contrôle de sécurité doit fournir à l'objet Identité ses informations d'état. Une demande de réinitialisation à l'intention de l'objet Identité n'est pas prise en charge par les appareils de sécurité FSCP 2/1 (voir 6.4) et doit être remplacée par une demande de réinitialisation à l'intention de l'objet Programme de contrôle de sécurité qui comporte des qualificatifs supplémentaires capables d'exécuter la demande. D'autres relations sont spécifiées en 6.6.8.

De plus, certains attributs instance sont réservés pour permettre une extension future destinée à mettre en œuvre les profils définis pour l'industrie des semiconducteurs.

6.6.2 Attributs de classe du programme de contrôle de sécurité

Les attributs de classe utilisés par le programme de contrôle de sécurité sont définis dans le Tableau 26.

Tableau 26 – Attributs de classe du Programme de contrôle de sécurité

ID d'attribut	Mise en œuvre nécessaire	Règle d'accès	Nom	Type de données	Description de l'attribut
1 – 96	Ces attributs de classe sont décrits dans l'IEC 61158-6-2				
97-98	Réservé par le FSCP 2/1 pour une utilisation future				
99	Conditionnel[a]	Obtenir	Sous-classe	UINT	Identifie un sous-ensemble d'attributs de classe, de services et de comportements supplémentaires

[a] Si la valeur de sous-classe est 00, qui identifie "aucune sous-classe", il convient d'appliquer cet attribut. Dans le cas contraire, cet attribut doit être appliqué.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

6.6.3 Sous-classes

Chaque sous-classe de niveau de classe donne une signification unique pour une plage de recouvrement d'identifiants d'attributs de classe et/ou de services de classe. La plage des définitions de sous-classes commence à la valeur ID 96_{hex} avec une numérotation descendante pour les attributs, et à la valeur ID 63_{hex} avec une numérotation descendante pour les services. La sous-classe d'une classe donnée est identifiée par la valeur de son attribut de classe de sous-classe. Aucune sous-classe n'est actuellement définie pour l'instance de classe.

6.6.4 Attributs instance du Programme de contrôle de sécurité

Les attributs instance utilisés par le programme de contrôle de sécurité sont définis dans le Tableau 27.

Tableau 27 – Attributs instance du Programme de contrôle de sécurité

ID d'attribut	Mise en œuvre nécessaire	Règle d'accès	NV	Nom	Type de données	Description de l'attribut
1	Facultatif	Obtenir	NV	Nombre d'attributs	USINT	Nombre d'attributs pris en charge par l'instance d'objet
2	Facultatif	Obtenir	NV	Liste d'attributs	MATRICE de USINT	Liste d'attributs pris en charge par l'instance d'objet
3	Réservé					
4	Réservé					
5	Facultatif	Obtenir	NV	Nom du fabricant	Chaîne courte	Texte ASCII, 20 caractères max.; voir 6.6.5.1
6	Facultatif	Obtenir	NV	Numéro de modèle du fabricant	Chaîne courte	Texte ASCII, 20 caractères max., spécifié par le fabricant
7	Facultatif	Obtenir	NV	Niveau de révision logicielle	Chaîne courte	Texte ASCII, 6 caractères max.; voir 6.6.5.2
8	Facultatif	Obtenir	NV	Niveau de révision matérielle	Chaîne courte	Texte ASCII, 6 caractères max.; voir 6.6.5.3
9	Facultatif	Obtenir	NV	Numéro de série du fabricant	Chaîne courte	Texte ASCII, 30 caractères max., spécifié par le fabricant; voir 6.6.5.4
10	Facultatif	Obtenir	NV	Configuration d'appareil	Chaîne courte	Texte ASCII, 50 caractères max., spécifié par le fabricant. Informations supplémentaires facultatives concernant la configuration de l'appareil
11	Exigé	Obtenir	V	Etat de l'appareil	USINT	Voir 6.6.5.5
12	Exigé	Obtenir	V	Etat d'exception	SWORD	Voir 6.6.5.6

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

ID d'attribut	Mise en œuvre nécessaire	Règle d'accès	NV	Nom	Type de données	Description de l'attribut
13	Conditionnel, repose sur le bit 7 d'état d'exception	Obtenir	V	Alarme de détail d'exception	STRUCT de:	Structure de 3 éléments qui contient une représentation en mode point du détail de l'alarme
				Détail d'exception commun	STRUCT de:	
				Taille	USINT	Nombre d'octets de détail d'exception commun
	Conditionnel, repose sur la taille [f]			Détail	MATRICE de:	Voir 6.6.5.7
				Détail	SWORD	Voir 6.6.5.7
				Détail d'exception de l'appareil	STRUCT de:	
				Taille	USINT	Nombre d'octets de détail d'exception de l'appareil
	Conditionnel, repose sur la taille [f]			Détail	MATRICE de:	Spécifié par le fabricant
				Détail n	SWORD	Spécifié par le fabricant
				Détail d'exception du fabricant	STRUCT de:	
				Taille	USINT	Nombre d'octets de détail d'exception du fabricant
				Détail	MATRICE de:	Spécifié par le fabricant
				Détail n	SWORD	Spécifié par le fabricant
14	Conditionnel, repose sur le bit 7 d'état d'exception	Obtenir	V	Avertissement de détail d'exception	STRUCT de:	Structure de 3 éléments qui contient une représentation en mode point du détail de l'avertissement
				Détail d'exception commun	STRUCT de:	
				Taille	USINT	Nombre d'octets de détail commun
	Conditionnel, repose sur la taille [f]			Détail	MATRICE de:	Voir 6.6.5.8
				Détail n	SWORD	Voir 6.6.5.8
				Détail d'exception de l'appareil	STRUCT de:	
				Taille	USINT	Nombre d'octets de détail de l'appareil
	Conditionnel, repose sur la taille [f]			Détail	MATRICE de:	Spécifié par le fabricant
				Détail n	SWORD	Spécifié par le fabricant
				Détail d'exception du fabricant	STRUCT de:	
				Taille	USINT	Nombre d'octets de détail du fabricant
				Détail	MATRICE de:	Spécifié par le fabricant
				Détail n	SWORD	Spécifié par le fabricant
15	Conditionnel [e]	Définir	NV	Activation d'alarme	BOOL	Voir 6.6.5.12

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

ID d'attribut	Mise en œuvre nécessaire	Règle d'accès	NV	Nom	Type de données	Description de l'attribut
16	Conditionnel [e]	Définir	NV	Activation d'avertissement	BOOL	Voir 6.6.5.12
17	Facultatif	Définir	V/ NV [a]	Temps	DATE_ AND_ TIME	Valeur de l'horloge temps réel interne de l'appareil
18	Conditionnel [g]	Obtenir	NV	Comportement de l'horloge pendant un cycle d'alimentation	USINT	Décrit le comportement de l'horloge temps réel interne de l'appareil (attribut "Temps") pendant un cycle d'alimentation: 0 = [par défaut] l'horloge se réinitialise toujours pendant un cycle d'alimentation 1 = la valeur de l'horloge est archivée dans la mémoire non volatile hors tension 2 = horloge à pile de secours qui fonctionne hors alimentation de l'appareil 3 – 255 = Réservé
19	Facultatif	Obtenir	NV	Date de dernière maintenance	DATE	Date de dernier entretien de l'appareil
20	Facultatif	Obtenir	NV	Date de prochaine maintenance programmée	DATE	Date de recommandation du prochain entretien de l'appareil
21	Facultatif	Obtenir	NV	Temporisateur d'expiration de maintenance programmée	INT	Voir 6.6.5.14
22	Conditionnel [h]	Définir	NV	Activation d'avertissement de l'expiration de maintenance programmée	BOOL	Voir 6.6.5.15
23	Facultatif	Obtenir	NV	Heures de fonctionnement	UDINT	Indication du nombre d'heures de mise sous tension de l'appareil
24	Conditionnel [c]	Définir [i]	NV	Verrouillage de configuration	BOOL	Marque la configuration d'appareil interne comme vérifiée et verrouillée, ou alternativement comme non vérifiée, non verrouillée et modifiable
25	Conditionnel [c]	Obtenir	NV	Configuration UNID	10 octets	CFUNID – Identifie le propriétaire de la configuration d'un appareil: Ensemble des $Ffhex_{hex}$ = configuration par outil uniquement. 0 = sans propriétaire, accepte tout propriétaire
26	Exigé	Obtenir	NV	Identifiant de configuration de sécurité	10 octets	Le SCID est constitué du CRC de configuration de sécurité + datation de la configuration de sécurité. Il s'agit de la signature de la configuration
27	Conditionnel [j]	Obtenir	NV	Target UNID (UNID cible)	10 octets	UNID courant de l'appareil

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

ID d'attribut	Mise en œuvre nécessaire	Règle d'accès	NV	Nom	Type de données	Description de l'attribut
28	Conditionnel[d]	Obtenir	NV	Propriétaires des points de connexion de sortie		
				Nombre d'entrées de matrice	UINT	Nombre d'entrées OCPUNID STRUCT
				Propriétaires de sorties	MATRICE de STRUCT	
				OCPUNID	10 octets	UNID du propriétaire des ressources de sortie. 0 = sans propriétaire, accepte tout propriétaire (par défaut)
				Taille de l'ePath	USINT	Taille du chemin, nombre d'octets
				Ressource d'application	ePath compact	Chemin vers la ressource "avec propriétaire" (c'est-à-dire 20 04 24 01 – classe d'ensemble, instance 1)
29	Conditionnel [k]	Obtenir	V	Proposition de TUNID	10 octets	Valeur UNID qu'un point d'origine tente de définir dans l'appareil
30	Conditionnel [j]	Obtenir	NV	Liste d'UNID cibles	STRUCT de	
				Nombre d'UNID cibles	USINT	Nombre d'entrées dans la liste d'UNID cibles
				UNID cibles	MATRICE de STRUCT	Liste de paires (Numéro de port, UNID cible)
				Numéro de port	UINT	Voir l'IEC 61158-4-2:2019, 7.11.4.3
				Target UNID (UNID cible)	10 OCTETS	UNID cible associé à un numéro de port CIP spécifique
31	Conditionnel [k]	Obtenir	V	Liste de propositions d'UNID	STRUCT de	
				Nombre de propositions de TUNID	USINT	Nombre d'entrées dans la liste de propositions d'UNID cibles
				Propositions de TUNID	MATRICE de STRUCT	Liste de paires (Numéro de port, Proposition d'UNID cible)
				Numéro de port	UINT	Voir l'IEC 61158-4-2:2019, 7.11.4.3
				Proposition de TUNID	10 OCTETS	Proposition d'UNID cible associée à un numéro de port CIP spécifique
97-98	Réservé par le FSCP 2/1 pour une utilisation future					
99	Conditionnel [b]	Obtenir	NV	Sous-classe	UINT	Identifie un sous-ensemble d'attributs instance, de services et de comportements supplémentaires

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

[a]	Le comportement non volatil de l'attribut Temps est conditionnel: l'attribut 17 est NV si l'attribut 18 = 1, sinon il est V.
[b]	Si la valeur de sous-classe est 00, qui identifie "aucune sous-classe", il convient d'appliquer cet attribut. Dans le cas contraire, cet attribut doit être appliqué.
[c]	Les appareils de sécurité qui prennent en charge l'interface SNCT (c'est-à-dire non configurée par la fonction SafetyOpen ou tout moyen spécifique au fournisseur) doivent prendre en charge cet attribut.
[d]	Conditionnel – L'attribut Propriétaire de Connexion de sortie doit être pris en charge pour tous les ensembles de sorties de sécurité.
[e]	Conditionnel – Exigé pour les appareils FSCP 2/1, mais facultatif pour le FSCP 2/1 sur les appareils CP 16/3.
[f]	"Conditionnel, repose sur la taille" signifie que le détail de l'exception est présent lorsque la taille est supérieure à zéro.
[g]	Exigé si Temps (attribut 17) est pris en charge.
[h]	Exigé si Temporisateur d'expiration de maintenance programmée (attribut 21) est pris en charge.
[i]	Défini uniquement par le service "Verrouillage/Déverrouillage de configuration".
[j]	Les appareils à un seul port de sécurité doivent prendre en charge l'attribut 27 (UNID cible). Les appareils à plusieurs ports de sécurité ne doivent prendre en charge que l'attribut 40 (Liste d'UNID cibles).
[k]	Les appareils à un seul port de sécurité qui prennent en charge le SNCT doivent prendre en charge l'attribut 29 (Proposition de TUNID), à moins qu'ils ne soient configurés par des moyens spécifiques au fournisseur. Les appareils à plusieurs ports de sécurité qui prennent en charge le SNCT ne doivent prendre en charge que l'attribut 31 (Liste de propositions de TUNID), à moins qu'ils ne soient configurés par des moyens spécifiques au fournisseur.

6.6.5 Sémantique

6.6.5.1 Nom du fabricant

L'attribut Nom du fabricant identifie le fabricant de l'appareil.

Il n'est pas assuré par spécification que cet attribut soit unique. Par conséquent, il ne constitue pas un attribut de substitution à l'attribut correspondant de l'objet Identité, et il convient de ne pas l'utiliser à des fins d'identification.

6.6.5.2 Niveau de révision logicielle

Il s'agit d'une chaîne de texte en code ASCII qui représente la révision du logiciel correspondant à l'appareil spécifique identifié par l'objet Identité.

6.6.5.3 Niveau de révision matérielle

Il s'agit d'une chaîne de texte en code ASCII qui représente la révision du matériel identifié par l'objet Identité. Le fabricant de l'appareil doit contrôler cette révision de manière à pouvoir assurer la traçabilité des modifications apportées au matériel de l'appareil.

6.6.5.4 Numéro de série du fabricant

Cet attribut est une représentation de chaîne du numéro de série du fournisseur de l'appareil, qui est formatée pour s'ajuster à la plupart des systèmes de suivi de fabrication. Il n'est pas nécessaire que cet attribut corresponde au numéro de série de l'objet Identité qui permet d'identifier de manière unique l'appareil dans l'environnement réseau.

6.6.5.5 Etat de l'appareil

Cet attribut représente l'état courant de l'appareil. Sa valeur change conjointement au changement de l'état de l'appareil. Les valeurs d'indication de l'attribut Etat de l'appareil sont définies dans le Tableau 28.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Tableau 28 – Valeurs d'indication de l'attribut Etat de l'appareil

Valeur d'attribut	Etat
0	Non défini
1	Autovérification
2	Repos
3	Exception d'autovérification
4	Exécution
5	Abandon
6	Anomalie critique
7	Configuration
8	Attente du TUNID
9-50	Réservé par le FSCP 2/1
51	Attente du TUNID avec le couple admis[a]
52	Exécution avec le couple admis[a]
53-99	Spécifique à l'appareil
100-255	Spécifique au fournisseur

[a] Admis et défini uniquement dans une spécification de profil d'appareil appropriée.

6.6.5.6 Etat d'exception

Attribut à un seul octet dont la valeur indique l'état des alarmes et des avertissements pour l'appareil. Cette indication peut être fournie par l'une des deux méthodes suivantes: de base ou étendue.

Dans le cas de la méthode de base, le bit 7 de l'attribut Etat d'exception est défini sur zéro; la communication de cet attribut permet de consigner de manière exclusive toutes les exceptions. Le format des bits 0 à 6 dans ce mode est spécifique à l'appareil; il peut toutefois être précisé davantage dans une spécification de profil de l'appareil appropriée. Si le format n'est pas spécifié, il est alors équivalent à celui spécifié pour la méthode étendue.

Dans le cas de la méthode étendue, le bit 7 de l'attribut Etat d'exception est défini sur 1; la communication de cet attribut permet de consigner les exceptions, le format étant spécifié dans le Tableau 29. De plus, les attributs Détail d'exception sont pris en charge. Les bits de l'attribut Etat d'exception sont déterminés par un élément logique "OR" des bits associés de l'attribut Détail d'exception, tel qu'indiqué.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Tableau 29 – Format de l'attribut Etat d'exception

Bit	Mode point de l'état d'exception, bit 7 défini sur 0 fonction	Mode point de l'état d'exception, bit 7 défini sur 1 fonction
0	Définition spécifique à l'appareil (voir Profil de l'appareil)	ALARME/commune aux appareils[a]
1		ALARME/spécifique à l'appareil
2		ALARME/spécifique au fabricant
3		Réservé – défini sur 0
4		AVERTISSEMENT/commun aux appareils[a]
5		AVERTISSEMENT/spécifique à l'appareil
6		AVERTISSEMENT/spécifique au fabricant
7	0 = méthode de base	1 = méthode étendue

[a] L'alarme ou l'avertissement n'est pas spécifique au type d'appareil ou au fabricant de ce dernier.

6.6.5.7 Alarme et avertissement relatifs au détail d'exception

Les formats de ces deux attributs sont identiques. Ils sont ainsi décrits conjointement dans le présent paragraphe.

Les attributs relatifs à l'état décrit des alarmes ou des avertissements sont associés à l'appareil. Chaque attribut est une structure qui contient trois membres, chacun de ces membres étant relatif respectivement à l'état décrit des exceptions communes (c'est-à-dire non spécifiques à l'appareil), spécifiques à l'appareil, mais non spécifiques au fabricant, et spécifiques au fabricant. Le détail commun est défini en 6.6.5.8 et en 6.6.5.9. Le détail spécifique à l'appareil est défini dans le profil d'appareil approprié. Le détail spécifique au fabricant est défini par ce dernier. Une valeur de TAILLE nulle indique qu'aucun détail n'est défini pour la structure du détail d'exception associée.

Chacun des trois membres de la structure est défini comme une structure qui contient une liste ordonnée (c'est-à-dire une matrice) d'OCTETS de longueur TAILLE, et un entier non signé dont la valeur est TAILLE. Chaque octet de chaque matrice a un mapping spécifique. Ce mapping est formaté sous la forme de 8 bits qui représentent 8 conditions indépendantes, tandis qu'une valeur de 1 indique l'établissement (ou l'existence) de la condition, et qu'une valeur de 0 indique la suppression (ou l'absence) de la condition. Si un appareil ne prend pas en charge un détail d'exception, le bit correspondant n'est jamais défini. Les modes points dédiés aux alarmes et avertissements dans les attributs correspondants sont structurés en parallèle, de sorte que l'établissement d'une alarme ou d'un avertissement d'une condition peut être fonction de la gravité. Si une condition ne peut pas être intrinsèquement à la fois une alarme et un avertissement, la position de bits parallèle correspondant à l'autre état doit rester "0".

L'existence d'une structure variable du détail d'exception dépend de la valeur de l'attribut Etat d'exception. L'existence d'une structure variable du détail d'exception n'est exigée que si le bit 7 de l'attribut Etat d'exception est défini sur 1 (indiquant la consignation de la méthode étendue), le bit (parmi les bits 0 à 6) dudit attribut correspondant au type d'exception particulier étant également défini sur 1.

6.6.5.8 Détail d'exception commun

Cette structure se rapporte aux conditions d'exception (c'est-à-dire alarmes ou avertissements) communes à tous les appareils. L'élément de détail de la structure est une liste ordonnée (c'est-à-dire une matrice) d'octets de longueur TAILLE qui constitue la valeur de l'élément de structure Taille. Pour chaque octet du champ Détail, tous les bits non identifiés sont réservés pour une future normalisation.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Le premier octet de cet attribut est CommonExceptionDetail[0]. Les détails d'exception supplémentaires, s'ils sont fournis, sont appelés CommonExceptionDetail[1] et CommonExceptionDetail[TAILLE]. L'exception spécifique associée à chacun des modes points est donnée dans le Tableau 30. La TAILLE pour cette révision est de deux (2). Les détails des critères propres à chaque condition d'exception ne relèvent pas du domaine d'application du présent document.

6.6.5.9 Valeurs de l'attribut Détail d'exception commun

Tableau 30 – Valeurs de l'attribut Détail d'exception commun

Détail d'exception commun [0] [a]	Détail d'exception commun [1] [a]
Exception de diagnostic interne	surintensité d'alimentation
Exception de microprocesseur	alimentation réservée
Exception EPROM	tension de sortie d'alimentation
Exception EEPROM	tension d'entrée d'alimentation
Exception RAM	date de maintenance programmée
Réservé	notification au fabricant
Exception temps réel interne	réinitialisation de l'exception
Réservé	Réservé

[a] Si un appareil ne prend pas en charge un détail d'exception, le bit correspondant n'est jamais défini.

6.6.5.10 Détail d'exception de l'appareil

Cette structure, de forme similaire au détail d'exception commun, se rapporte aux conditions d'exception spécifiques aux appareils individuels installés sur le réseau, et qui sont définies dans leurs profils d'appareil respectifs. L'élément de détail de la structure est une liste ordonnée (c'est-à-dire une matrice) d'octets de longueur TAILLE qui constitue la valeur de l'élément de structure Taille. Pour une description détaillée de cet attribut, consulter le profil d'appareil spécifique approprié.

6.6.5.11 Détail d'exception du fabricant

Cette structure (voir Tableau 31), de forme similaire au détail d'exception commun, se rapporte aux conditions d'exception spécifiques aux fabricants des appareils individuels installés sur le réseau, et qui sont définies par ces derniers dans leur documentation de produit. L'élément de détail de la structure est une liste ordonnée (c'est-à-dire une matrice) d'octets de longueur TAILLE qui constitue la valeur de l'élément de structure Taille. Pour une description détaillée de cet attribut, consulter la documentation du fabricant d'appareils spécifiques appropriée.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Tableau 31 – Synthèse du format de détail d'exception

Composante de détail	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Taille du détail d'exception commun	0	0	0	0	0	0	0	0
Détail d'exception commun 0	Rés.	Anomalie en temps réel	Rés.	Mémoire données	Mémoire non volatile	Mémoire codage	Microprocesseur	Diagnostic
Détail d'exception commun 1	Rés.	Réinitialisation de l'exception	Notification au fournisseur	Date de maintenance programmée	Tension d'entrée d'alimentation	Tension de sortie d'alimentation	Rés.	Surintensité d'alimentation
Taille du détail d'exception de l'appareil	TBD[a]	TBD[a]	TBD[a]	TBD[a]	TBD[a]	TBD[a]	TBD[a]	TBD[a]
Détail d'exception de l'appareil 0	--	--	--	--	--	--	--	--
Détail d'exception de l'appareil n	--	--	--	--	--	--	--	--
Taille du détail d'exception du fabricant	TBD[a]	TBD[a]	TBD[a]	TBD[a]	TBD[a]	TBD[a]	TBD[a]	TBD[a]
Détail du fabricant 0	--	--	--	--	--	--	--	--
Détail du fabricant n	--	--	--	--	--	--	--	--

[a] Consulter la documentation appropriée du fabricant d'appareils spécifiques pour une définition complète.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

6.6.5.12 Activation des alarmes et avertissements

Ces attributs booléens permettent d'activer (1) ou de désactiver (0) le processus de paramétrage des bits d'exception de l'objet Programme de contrôle de sécurité. La désactivation signifie l'absence de réglage des bits correspondants, cette désactivation contribuant à la suppression de ces bits s'ils avaient été définis. Les états d'alarme et d'avertissement ne sont également pas conservés; lorsqu'ils sont activés, les bits doivent être définis uniquement si la condition correspondante est vraie.

L'état par défaut de ces attributs d'activation est activé (1).

6.6.5.13 Temps

Cet attribut facultatif représente la valeur de l'heure et de la date conservée par l'horloge temps réel de l'appareil avec une résolution d'une milliseconde.

La valeur par défaut de l'attribut Temps est zéro (0), ce qui correspond à 00:00:00 le 01/01/1970.

6.6.5.14 Temporisateur d'expiration de maintenance programmée

Cet attribut, qui comporte une résolution d'une heure, permet d'engendrer un avertissement qui signifie qu'un étalonnage de l'appareil est attendu. Un temporisateur du Programme de contrôle de sécurité décrémente cet attribut une fois par heure sous tension. Lorsque l'attribut n'est plus positif et l'attribut Activation d'avertissement de l'expiration de maintenance programmée est défini sur activé, cette situation génère la condition Avertissement de l'expiration de maintenance programmée. Ceci entraîne le réglage du bit Avertissement de maintenance programmée.

L'attribut Temporisateur d'expiration de maintenance programmée, lorsqu'il est mis en œuvre, ne doit pas retomber à zéro; l'attribut ne décrémente plus lorsqu'il atteint sa valeur la plus négative. Le Temporisateur d'expiration de maintenance programmée, lorsqu'il est mis en œuvre, doit poursuivre sa décrémentation indépendamment de l'état de l'attribut Activation d'avertissement de l'expiration de maintenance programmée. Ce même temporisateur, toujours lorsqu'il est mis en œuvre, doit être conservé dans la mémoire non volatile.

6.6.5.15 Activation d'avertissement de l'expiration de maintenance programmée

Cet attribut booléen permet d'activer (1) ou de désactiver (0) le processus de paramétrage du bit d'exception de maintenance programmée de l'objet Programme de contrôle de sécurité. La désactivation signifie l'absence de réglage du bit correspondant, cette désactivation contribuant à la suppression de ce bit s'il avait été défini. Lorsqu'il est activé, le bit doit être défini uniquement si la condition correspondante est vraie.

L'état par défaut de cet attribut d'activation est activé (1).

6.6.5.16 Verrouillage de configuration

L'attribut Verrouillage de configuration, lorsqu'il est mis en œuvre avec l'interface SNCT, doit être utilisé pour marquer la configuration de l'appareil comme étant vérifiée, et pour verrouiller cette dernière; 0 = Non verrouillé (non vérifié et modifiable), 1 = Verrouillé (vérifié et non modifiable).

La valeur par défaut de l'attribut Verrouillage de configuration est 0 = non verrouillé. Elle est utilisée principalement pour les appareils de sécurité configurés par l'interface SNCT (c'est-à-dire non configurés par SafetyOpen). Après configuration de l'appareil par outil et sa validation par l'utilisateur, le logiciel définit ce drapeau afin de "neutraliser" les modifications ultérieures éventuelles. Il est possible de protéger ce drapeau par un mot de passe qui nécessite une vérification de l'utilisateur avant de pouvoir déverrouiller et modifier la configuration.

Le réglage de l'attribut Verrouillage de configuration d'un appareil doit entraîner parallèlement le refus des Configure_Requests, de la fonction Réinitialisation de sécurité de types 1 et 2 et de toute fonction SafetyOpen de type 1 valide.

6.6.5.17 UNID de configuration (CFUNID)

L'attribut UNID de configuration doit être mis en œuvre comme partie intégrante de l'interface SNCT. L'UNID de configuration identifie le propriétaire de la configuration dans cet appareil de sécurité. L'attribut UNID de configuration peut être défini par différents moyens. Les significations spéciales suivantes doivent être attribuées à l'attribut UNID de configuration:

- tous les octets définis sur 00_{hex} = pas de propriétaire, accepte tout propriétaire;
- tous les octets définis sur FF_{hex} = l'outil logiciel est le propriétaire attribué.

La valeur par défaut de l'UNID de configuration doit correspondre au réglage de tous les octets sur 00_{hex}.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Lorsque l'attribut UNID de configuration est défini sur "Pas de propriétaire, accepte tout propriétaire", les appareils de sécurité FSCP 2/1 doivent saisir la première source de configuration (Type 1 et/ou Configure_Request) comme étant le propriétaire (voir Tableau 32).

La valeur CFUNID est utilisée conjointement à la valeur OUNID qui accompagne la Configure_Request ou une fonction SafetyOpen de type 1. Voir Tableau 32 pour la définition de la méthode utilisée par les appareils pour répondre aux différents services qui sont fonction de la valeur de réglage de l'attribut CFUNID au moment de la réception du service. L'interface SNCT doit toujours utiliser toutes les valeurs FF_{hex} pour l'attribut OUNID.

EXEMPLE Si l'attribut CFUNID est défini sur toutes les valeurs FF_{hex}, l'attribut OUNID de Configure_Request doit être égal à cette valeur pour traiter la commande.

Tableau 32 – Synthèse du comportement des appareils pour différentes valeurs CFUNID

Service	Valeur de CFUNID		
	FF_{hex}	00_{hex}	OUNID
Configure_Request (FF_{hex}) de SNCT	Acceptation	Acceptation Définir CFUNID = FF_{hex}	Echec
Configure_Request (OUNID)	Echec	Acceptation Définir CFUNID = OUNID	Accepter uniquement si CFUNID = OUNID Echec sinon
SafetyOpen de type 1	Echec	Acceptation Définir CFUNID = OUNID	Accepter uniquement si CFUNID = OUNID Echec sinon

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

6.6.5.18 Identifiant de configuration de sécurité (SCID)

L'attribut Identifiant de configuration de sécurité est la signature de la configuration de sécurité. Cet attribut est une concaténation du CRC de configuration de sécurité (SCCRC) et de la datation de la configuration de sécurité (SCTS). Ces valeurs sont issues de la fonction SafetyOpen ou du logiciel de configuration de sécurité au cours de la validation de configuration.

La valeur par défaut de l'attribut SCID du Programme de contrôle de sécurité doit être 0.

Lorsqu'un appareil adopte le mode Configuration, l'attribut SCID doit être défini sur 0 et maintenu à cette valeur (tout au long des cycles d'alimentation) jusqu'à exécution satisfaisante de la Validation.

```
typedef struct _S_SCID
{
DWORD            dwCRC;   //calculated by device
DWORD            dwTime;  // set by software
WORD             wDate;
} S_SCID;
```

6.6.5.19 UNID cible (TUNID)

Il s'agit d'un attribut NV qui reflète l'UNID que la configuration a sauvegardé.

Pour les appareils à un seul port de sécurité, l'attribut UNID cible du Programme de contrôle de sécurité doit toujours refléter l'UNID cible par défaut ou courant que le processus de paramétrage de l'UNID a sauvegardé. Pour les appareils à plusieurs ports de sécurité, l'attribut Liste d'UNID cibles (attribut 30) du Programme de contrôle de sécurité doit toujours refléter les UNID cibles par défaut ou courants que le processus de paramétrage de la liste d'UNID a sauvegardés.

L'UNID ou les UNID d'un appareil doivent être archivés dans la mémoire non volatile comme partie intégrante de la procédure de paramétrage des UNID.

L'UNID ou les UNID d'un appareil doivent être archivés dans l'objet DeviceNet, l'objet Interface TCP/IP ou l'attribut SNN de l'objet SERCOS III comme partie intégrante de la procédure de paramétrage des UNID.

La mémoire non volatile d'un appareil qui présente un état par défaut du fabricant doit comporter une valeur d'UNID cible non valide (par exemple 10 octets de FF_{hex}) pour chacun de ses ports de sécurité.

L'UNID ou les UNID d'un appareil doivent être lus à partir de la mémoire non volatile lors de la mise sous tension, puis chargés dans un attribut de l'objet Programme de contrôle de sécurité et dans l'attribut Safety_Network_Number de l'objet DeviceNet, de l'objet Interface TCP/IP ou de l'objet SERCOS III.

Si l'UNID représente un nombre valide (non égal à la valeur de l'appareil à la sortie d'usine), ce nombre doit être comparé au NodeID. En cas de concordance, la procédure de démarrage de l'appareil se poursuit. En cas de non-concordance, l'appareil passe à l'état Abandon.

Lorsque la défaillance d'un appareil a pour origine la non-concordance du paramètre Commutation mémoire non volatile, cet appareil doit permettre soit une réinitialisation à l'état d'usine, soit la transmission d'une demande Récupération au Programme de contrôle de sécurité afin de supprimer l'abandon. Dans les deux cas, l'appareil doit passer à l'état "Attente du TUNID".

La lecture de l'attribut UNID dans le Programme de contrôle de sécurité doit être effectuée avec une intégrité de sécurité.

L'application des données de configuration et de l'UNID à la mémoire non volatile doit s'effectuer avec une intégrité de sécurité.

6.6.5.20 Proposition de TUNID

La valeur par défaut de l'attribut Proposition de TUNID doit correspondre à toutes les valeurs FF_{hex}.

Cet attribut reflète la valeur proposée lorsque l'appareil suit le processus "ProposeTUNIG/ApplyTUNID". Lorsque l'application est achevée, cet attribut doit de nouveau être défini sur la valeur par défaut d'usine de toutes les valeurs FF_{hex}.

6.6.5.21 Propriétaire de connexion de sortie (OCPUNID)

Cet attribut n'est utilisé que pour les connexions de sécurité sur les sorties. Les connexions de sécurité aux sorties définissent un propriétaire afin d'éviter que des connexions errantes ne détournent une ressource de sortie dans un système de sécurité validé. Cet identifiant de propriétaire identifie l'appareil de sécurité d'origine auquel ont été conférés les droits de propriété pour cette connexion de sortie de sécurité. Ce paramètre provient des paramètres du Segment de sécurité de la fonction SafetyOpen. La valeur OCPUNID peut être identique à celle de l'attribut 25 du Programme de contrôle de sécurité (CFUNID) lorsque l'appareil est également configuré comme partie intégrante de SafetyOpen. Dans la mesure où un appareil peut comporter deux ressources de sortie ou plus, et peut admettre l'existence de propriétaires distincts pour chaque ressource, cet attribut prend la forme d'une structure qui permet le maintien séparé de chaque ressource. La ressource est identifiée par une adresse de Segment logique.

La valeur par défaut de tous les OCPUNID doit être 0 (accepte tout propriétaire), chaque ePath étant dirigé vers la ressource respective.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

6.6.5.22 Liste d'UNID cibles

Voir 6.6.5.19 pour la définition des membres d'UNID cible de cet attribut.

6.6.5.23 Liste de propositions de TUNID

Voir 6.6.5.20 pour la définition des membres de Proposition de TUNID de cet attribut.

6.6.6 Sous-classes

Chaque sous-classe de niveau d'instance donne une signification unique pour une plage de recouvrement d'identifiants d'attributs instance et/ou de services instance. La plage des définitions de sous-classes commence à la valeur ID 96_{hex} avec une numérotation descendante pour les attributs, et à la valeur ID 63_{hex} avec une numérotation descendante pour les services. La sous-classe d'une instance donnée est identifiée par la valeur de son attribut instance Sous-classe. Aucune sous-classe n'est actuellement définie pour les instances.

6.6.7 Services communs du programme de contrôle de sécurité

6.6.7.1 Présentation générale des services communs

Les services communs pris en charge par le Programme de contrôle de sécurité sont définis dans le Tableau 33. Les services spécifiques de l'objet Programme de contrôle de sécurité sont définis dans le Tableau 34.

Tableau 33 – Services communs du Programme de contrôle de sécurité

Code de service	Mise en œuvre nécessaire		Nom du service	Description du service
	Classe	Instance		
$0E_{hex}$	Conditionnel	Exigé	Get_Attribute_Single	Renvoie le contenu de l'attribut spécifié
010_{hex}	n/a	Exigé	Set_Attribute_Single	Modifie une valeur d'attribut
$0D_{hex}$	n/a	Conditionnel [a]	Application	Applique une configuration en attente à la mémoire non volatile, et dirige l'appareil vers l'état Repos
15_{hex}	n/a	Facultatif	Restauration	Restaure la dernière configuration appliquée dans les appareils qui la prennent en charge

[a] Les appareils de sécurité qui prennent en charge l'interface SNCT (c'est-à-dire non configurée par SafetyOpen ou tout moyen spécifique au fournisseur) doivent prendre en charge ce service.

L'appareil peut solliciter l'existence d'un service instance de Programme de contrôle de sécurité en interne, spécifié par le fabricant.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Tableau 34 – Services spécifiques de l'objet Programme de contrôle de sécurité

Code de service	Mise en œuvre nécessaire		Nom du service	Description du service
	Classe	Instance		
$4B_{hex}$			Réservé	
$4C_{hex}$	n/a	Facultatif	Récupération	Retire l'appareil de l'état Abandon
$4E_{hex}$	n/a	Facultatif	Perform_Diagnostics	Contribue à l'exécution d'un ensemble de routines de diagnostic par l'appareil, le cas échéant
$4F_{hex}$	n/a	Conditionnel[a]	Configure_Request	Dirige l'appareil vers l'état Configuration, le cas échéant. Ce service exige la saisie d'un mot de passe pour son exécution
50_{hex}	n/a	Conditionnel[a]	Validate_Configuration	Contribue à l'exécution d'un contrôle de validation de la configuration en attente par l'appareil. Ce service exige du logiciel qu'il fournisse le SCID (CRC + datation)
51_{hex}	n/a	Conditionnel[a]	Set_Password	Permet de définir un attribut de mot de passe dans l'objet Programme de contrôle
52_{hex}	n/a	Conditionnel[a]	Configuration_Lock/ Unlock	Ce service intervient après la présence de l'attribut Verrouillage de configuration dans le Programme de contrôle de sécurité. Ce service exige la saisie d'un mot de passe pour son exécution
53_{hex}	n/a	Conditionnel[c]	Changement de mode	Doit être mis en œuvre pour les appareils logiques qui prennent en charge l'exécution, indépendamment des connexions E/S. L'exécution des changements de mode dans les appareils de sécurité exige un mot de passe
54_{hex}	n/a	Type 0 conditionnel [e], Types 1 et 2 conditionnels[a]	Réinitialisation de sécurité	Réinitialise l'appareil d'une manière similaire à l'objet Identité, à l'exception du fait que l'exécution exige un mot de passe
55_{hex}	n/a	Conditionnel[b]	Réinitialisation de mot de passe	Permet de réinitialiser le mot de passe dans un appareil. Le contenu des données de ce message est spécifique au fournisseur
56_{hex}	n/a	Conditionnel [d]	Propose_TUNID	Permet d'initier le paramétrage du TUNID dans un appareil à la sortie d'usine
57_{hex}	n/a	Conditionnel [d]	Apply_TUNID	Permet d'achever le paramétrage du TUNID
58_{hex}	n/a	Conditionnel [f]	Propose_TUNID_List	Permet d'initier le paramétrage de la liste de TUNID dans un appareil à la sortie d'usine
59_{hex}	n/a	Conditionnel [f]	Apply_TUNID_List	Permet d'achever le paramétrage de la liste de TUNID

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

[a]	Doit être mis en œuvre pour les appareils de sécurité FSCP 2/1 qui prennent en charge l'interface SNCT.
[b]	Conditionné par la prise en charge du service de mot de passe comme partie intégrante de l'interface SNCT.
[c]	Doit être mis en œuvre pour les appareils de sécurité FSCP 2/1 qui prennent en charge l'interface SNCT et qui sont des appareils logiques qui prennent en charge l'exécution, indépendamment des connexions E/S. L'exécution des changements de mode dans les appareils de sécurité exige un mot de passe.
[d]	Ne doit être mis en œuvre pour les appareils FSCP 2/1 à un seul port de sécurité qui prennent en charge l'interface SNCT, et vivement recommandé pour les appareils configurables par la fonction SafetyOpen de type 1. Facultatif pour les appareils qui utilisent une configuration spécifique au fournisseur. Les appareils à plusieurs ports de sécurité ne doivent pas mettre en œuvre les services Propose_TUNID et Apply_TUNID.
[e]	Conditionnel – Exigé pour les appareils FSCP 2/1, mais facultatif pour les appareils FSCP 2/1 sur le CP 16/3 et les appareils de sécurité qui utilisent une configuration spécifique au fournisseur.
[f]	Conditionnel – Les appareils à plusieurs ports de sécurité qui prennent en charge l'interface SNCT doivent prendre en charge les services Propose_TUNID_List et Apply_TUNID_List. Les appareils à un seul port de sécurité ne doivent pas prendre en charge les services Propose_TUNID_List et Apply_TUNID_List. Les appareils à plusieurs ports de sécurité dotés d'une configuration spécifique au fournisseur peuvent prendre en charge les services Propose_TUNID_List et Apply_TUNID_List.

L'appareil peut solliciter l'existence d'un service instance de Programme de contrôle de sécurité en interne, spécifié par le fabricant. Généralement, ces demandes sont générées après un événement tel que l'activation d'un bouton ou la fermeture d'un contact externe.

6.6.7.2 Service de récupération

Ce service permet de faire passer les objets d'application de l'appareil de l'état d'anomalie récupérable à l'état de repos. Cette demande de service peut être émise en interne par les objets d'application.

6.6.7.3 Service Perform_Diagnostics

Le service Perform_Diagnotics permet d'indiquer à l'objet Programme de contrôle de sécurité d'effectuer un essai de diagnostic. Cet essai est de type commun ou dépendant de l'appareil. Les essais de diagnostic communs peuvent comprendre les éléments suivants: RAM, EPROM, mémoire non volatile et communications. La structure des essais de diagnostic de type commun est spécifique à la mise en œuvre. Les détails des diagnostics dépendants de l'appareil ne relèvent pas du domaine d'application du présent document.

6.6.7.4 Service Configure_Request

Le service Configure_Request permet de faire passer les objets d'application de l'appareil de l'état Abandon, Exécution ou Repos à l'état Configuration.

En cas de réception d'une Configure_Request, une erreur "Conflit d'état d'objet (0Chex)" doit être renvoyée si l'attribut Configuration_Lock est défini. La demande contient trois paramètres, à savoir le paramètre du mot de passe contenu dans le Programme de contrôle de sécurité, l'UNID de l'appareil cible et l'UNID du point d'origine. Ces valeurs sont mappées avec le mot de passe, le TUNID et le CFUNID de l'appareil. La présence de l'UNID est nécessaire pour permettre à l'appareil de déterminer si la source est un outil logiciel ou un point d'origine de capacité ACR.

En cas d'acceptation de la commande Configure_Request, l'appareil ne doit accepter que les messages de configuration destinés aux objets relatifs à la sécurité sur "cette seule connexion". Les tentatives d'écriture de messages destinés aux objets relatifs à la sécurité par d'autres connexions doivent être rejetées.

En cas d'échec d'une connexion de configuration pour quelque motif que ce soit, une autre Configure_Request doit être reçue (établissant ainsi une nouvelle source de connexion) avant de pouvoir effectuer des modifications de configuration (même après un cycle d'alimentation).

La structure de Configure_Request est définie dans le Tableau 35.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Tableau 35 – Structure de message Configure_Request

Nom	Type de données	Description
Code de service	USINT	$4F_{hex}$
Mot de passe	MATRICE de 16 OCTETS	
TUNID	MATRICE de 10 OCTETS	UNID de l'appareil cible. Permet de détecter les demandes mal acheminées
OUNID	MATRICE de 10 OCTETS	UNID de l'appareil d'origine. Si le point d'origine est un outil logiciel, ce paramètre doit être réglé sur toutes les valeurs FF_{hex}. Si le point d'origine est un appareil de capacité ACR, ce paramètre doit être l'OUNID de l'appareil

Un code d'erreur "Paramètre invalide" (20_{hex}) doit être renvoyé en cas de non-concordance du TUNID ou de l'OUNID lors du traitement d'une demande de configuration du Programme de contrôle de sécurité.

Un code d'erreur "Violation de privilège" ($0F_{hex}$) doit être renvoyé en cas de non-concordance du mot de passe lors du traitement d'une demande de configuration du Programme de contrôle de sécurité.

6.6.7.5 Service Validate_Configuration

Ce service conduit l'appareil à valider une configuration en attente, par la réalisation d'un calcul CRC avec ces données et en le comparant au CRC associé au message. Si le CRC ne produit pas le même résultat, une réponse d'erreur telle que définie ci-dessous est renvoyée. Dans le cas contraire, une réponse "réussite" est renvoyée. Voir Figure 10 et Figure 11 pour les détails de traitement de ce service. Cette commande ne peut être reçue que sur la connexion qui a placé l'appareil en mode configuration. La mémoire non volatile de l'appareil enregistre le SCID final dans l'attribut 26 du Programme de contrôle de sécurité.

La structure du message Validate_Configuration est définie dans le Tableau 36.

Tableau 36 – Structure de message Validate_Configuration

Nom	Type de données	Description
Code de service	USINT	50_{hex}
SCID	STRUCT de:	ID de configuration de sécurité
SCCRC	4 OCTETS	Proposition de CRC de configuration de sécurité calculé par le logiciel. Cette proposition est validée par l'appareil
SCTS	6 OCTETS	Datation de la configuration de sécurité. Cette valeur marque la date et l'heure de la configuration, qui est utilisée comme mécanisme de détection des modifications

La structure de la Réponse de validation satisfaisante est définie dans le Tableau 37.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Tableau 37 – Structure de message de réussite Validate_Configuration

Nom	Type de données	Description
Code de service	USINT	50_{hex}
SCID	STRUCT de:	ID de configuration de sécurité
SCCRC	4 OCTETS	CRC de configuration de sécurité calculé par l'appareil
SCTS	6 OCTETS	Datation de la configuration de sécurité. Cette valeur reflète les données transmises dans la demande Validation

En cas d'échec de la commande Validate_Configuration du Programme de contrôle de sécurité, la réponse doit transmettre une "erreur de validation" définie par la classe ($D0_{hex}$). Le code d'erreur suivant présenté dans le Tableau 38 est défini comme une erreur de validation dans le Programme de contrôle de sécurité; les codes d'erreur supplémentaires sont définis dans le Tableau 39.

Tableau 38 – Code d'erreur de Validate_Configuration

Code d'erreur général	Code d'erreur supplémentaire	Nom d'erreur	Description
$D0_{hex}$	Voir Tableau 39	Erreur de validation	Cette erreur est une erreur spécifique de classe pour le Programme de contrôle de sécurité; elle est transmise en réponse à une erreur Validate_Configuration

Tableau 39 – Codes étendus de Validate_Configuration

Codes d'erreur supplémentaires	Code de raison	Description
1	Non-concordance du CRC	Il s'agit du code supplémentaire non spécifique par défaut, en l'absence de toute autre information supplémentaire et lorsque le CRC de configuration ne correspond pas à la valeur transmise
2	Paramètre de configuration invalide	Ce code peut être utilisé pour indiquer une erreur de paramètre si un appareil procède à une validation spécifique des données de configuration. NOTE Il peut se produire même en cas de concordance du CRC.
3	TUNID Not Set (TUNID non défini)	Ce code peut être utilisé pour indiquer que l'appareil est à l'état "Attente du TUNID" et qu'il est nécessaire de définir son TUNID

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

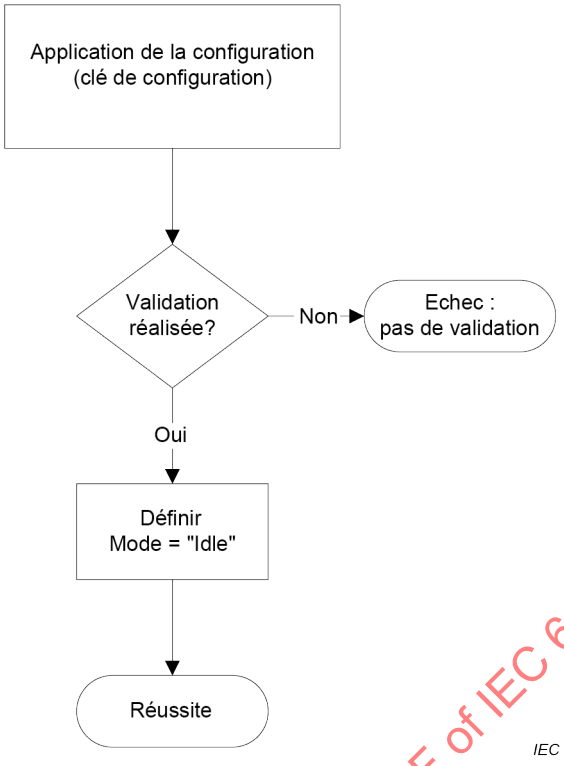
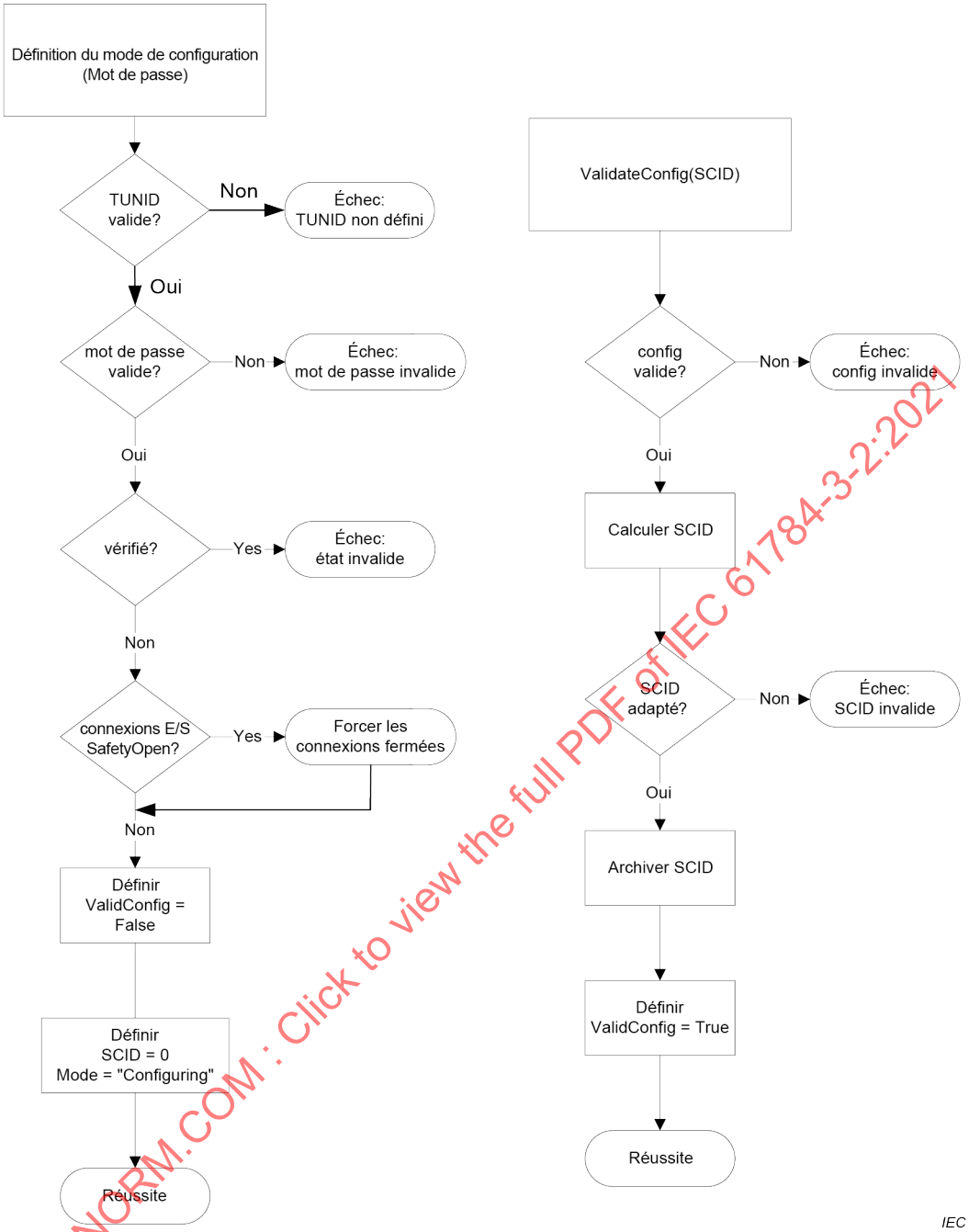


Figure 10 – Application de configuration d'appareil

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021



IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Figure 11 – Organigrammes de traitement de Configuration et Validation

6.6.7.6 Service Set_Password

Le service Set_Password conduit l'appareil à définir un mot de passe dans le Programme de contrôle. Ce service utilise 2 paramètres. Le premier d'entre eux est un paramètre qui représente le mot de passe existant, le second étant un paramètre qui représente le nouveau paramètre. Lors du premier paramétrage d'un mot de passe, le paramètre Mot de passe courant est défini sur la valeur par défaut d'usine (zéro).

La structure de Set_Password est définie dans le Tableau 40.

Tableau 40 – Structure de message Set_Password

Nom	Type de données	Description
Code de service	USINT	51_{hex}
Mot de passe courant	16 OCTETS	
Nouveau mot de passe	16 OCTETS	

Un code d'erreur "Violation de privilège" ($0F_{hex}$) doit être renvoyé en cas de non-concordance du mot de passe courant lors du traitement d'une commande Définition du mot de passe du Programme de contrôle de sécurité.

Un mot de passe dont le nombre de caractères est inférieur à celui défini dans le paramètre de mot de passe doit être aligné à droite en ordre petit-boutiste selon l'octet de poids faible du paramètre de mot de passe de 16 octets. Les octets supérieurs inutilisés du paramètre de mot de passe doivent être remplis de zéros.

6.6.7.7 Service Reset_Password

Ce service permet la réinitialisation des mots de passe d'un appareil. Le contenu exact et l'usage sont spécifiques au fournisseur afin de protéger l'intégrité des mots de passe. Ce service exige l'utilisation d'un paramètre et d'un champ de données spécifique au fournisseur. Le paramètre exigé est un champ de taille de données qui permet d'identifier la taille du champ de données spécifique au fournisseur. L'hypothèse retenue est que le contenu des données du fournisseur est spécifique à l'appareil, et le moyen d'utilisation de ce service doit être prévu par chaque fournisseur.

La structure de Reset_Password est définie dans le Tableau 41.

Tableau 41 – Structure de message Reset_Password

Nom	Type de données	Description
Code de service	USINT	55_{hex}
Taille des données	USINT	Nombre d'octets de données spécifiques au fournisseur
Données du fournisseur	Taille des données	Données du fournisseur qui contiennent d'autres données nécessaires à la réinitialisation du mot de passe

En cas d'erreur "Taille de données" pour la commande Reset_Password du Programme de contrôle de sécurité, le code d'erreur 15_{hex} (trop grand nombre de données) ou 13_{hex} (trop faible nombre de données) doit être renvoyé.

Un code d'erreur "Violation de privilège" ($0F_{hex}$) doit être renvoyé en cas de non-concordance des données du fournisseur lors du traitement d'une commande Reset_Password du Programme de contrôle de sécurité.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

6.6.7.8 Service Configuration_Lock/Unlock

Le service Configuration_Lock/Unlock conduit l'appareil à modifier l'attribut Configuration_Lock dans le Programme de contrôle de sécurité. Ce service exige un paramètre de valeur (0 = déverrouillé, 1 = verrouillé) et le paramètre de mot de passe. Le paramètre de mot de passe est comparé au mot de passe archivé et est exécuté uniquement en cas de concordance du mot de passe. Une erreur "Non-concordance du mot de passe" est renvoyée en cas de non-concordance du mot de passe.

La structure de Configuration_Lock/Unlock est définie dans le Tableau 42.

Tableau 42 – Structure de message Configuration_Lock/Unlock

Nom	Type de données	Description
Code de service	USINT	52_{hex}
Valeur	BOOL	0 = déverrouillé, 1 = verrouillé
Mot de passe	16 OCTETS	
TUNID	10 OCTETS	UNID de l'appareil cible. Permet de détecter les demandes mal acheminées

En cas de non-concordance du TUNID de la commande Configuration_Lock/Unlock du Programme de contrôle de sécurité, le code d'erreur "Paramètre invalide" (020_{hex}) doit être renvoyé.

Un code d'erreur "Violation de privilège" ($0F_{hex}$) doit être renvoyé en cas de non-concordance du mot de passe lors du traitement d'une commande Configuration_Lock/Unlock du Programme de contrôle de sécurité.

6.6.7.9 Service Changement de mode

Le service Changement de mode est utilisé par les appareils qui ont besoin de passer de l'état Repos à l'état Exécution, indépendamment de l'état de connexion. L'exécution de cette commande exige une autorisation appropriée, d'où la nécessité du mot de passe.

La structure du service Changement de mode est définie dans le Tableau 43.

Tableau 43 – Structure de message Mode_Change

Nom	Type de données	Description
Code de service	USINT	53_{hex}
Valeur	BOOL	0 = Repos, 1 = Exécution
Mot de passe	16 OCTETS	

Un code d'erreur "Violation de privilège" ($0F_{hex}$) doit être renvoyé en cas de non-concordance du mot de passe de la commande Changement de mode du Programme de contrôle de sécurité.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

6.6.7.10 Service Safety_Reset

Le service Safety_Reset permet de réinitialiser l'appareil. Le service Safety_Reset se substitue au service de réinitialisation normalisé défini, de telle sorte qu'il peut être qualifié par le mot de passe.

En cas de réception d'une Réinitialisation de sécurité de type 1 ou 2, une erreur "Conflit d'état d'objet ($0C_{hex}$)" doit être renvoyée si l'attribut Configuration_Lock est défini.

La structure de Safety_Reset est définie dans le Tableau 44.

Tableau 44 – Structure de message Safety_Reset

Nom	Type de données	Description
Code de service	USINT	54_{hex}
Type de réinitialisation	USINT	Voir Tableau 45
Mot de passe	16 OCTETS	
TUNID	10 OCTETS	UNID de l'appareil cible. Permet de détecter les demandes mal acheminées
Attribute_Bit_Map	USINT	Paramètre en mode point qui indique quels attributs doivent être préservés pour la réinitialisation. Ce paramètre n'est inclus que lorsque la réinitialisation est de type 2. Voir Tableau 46

En cas de non-concordance du TUNID lors de la transmission de la commande Réinitialisation de sécurité du Programme de contrôle de sécurité, le code d'erreur "Paramètre invalide" (20_{hex}) doit être renvoyé.

Un code d'erreur "Violation de privilège" ($0F_{hex}$) doit être renvoyé en cas de non-concordance du mot de passe lors du traitement d'une commande Réinitialisation de sécurité du Programme de contrôle de sécurité.

Tableau 45 – Types de réinitialisations de sécurité du Programme de contrôle de sécurité

Valeur:	Type de réinitialisation
0	Emule le mieux possible la puissance d'itération (des cycles) de l'appareil
1	Revient le plus précisément possible à la configuration par défaut, puis émule le mieux possible la puissance d'itération (des cycles)
2	Revient le plus précisément possible à la configuration d'usine, sauf pour protéger les paramètres indiqués par l'attribut Mode point, puis émule le mieux possible la puissance d'itération (des cycles)

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Tableau 46 – Paramètre d'attribut Mode point

Bit	Affectations de l'attribut Mode point
0	Lorsque défini, conserve la MACID définie par le logiciel
1	Lorsque défini, conserve le débit en bauds défini par le logiciel
2	Lorsque défini, conserve le TUNID
3	Lorsque défini, conserve le mot de passe
4	Lorsque défini, conserve le CFUNID
5	Lorsque défini, conserve l'OCPUNID
6	Réservé, toujours 0
7	Utilise le mapping étendu (à définir ultérieurement)

Le Tableau 47 indique de quelle manière un appareil de sécurité doit traiter les différents types de réinitialisations selon la condition Verrouillage/Déverrouillage et l'état de connexion de sécurité.

Tableau 47 – Règles de traitement applicables aux types de réinitialisations

Type de réinitialisation	Conditions potentielles à réception d'une réinitialisation			
	Ouverture / Verrouillage de la connexion de sécurité	Ouverture / Déverrouillage de la connexion de sécurité	Aucune connexion de sécurité / Verrouillé	Aucune connexion de sécurité / Déverrouillé
Type 0	Réponse d'erreur de mode/d'état	Réponse d'erreur de mode/d'état	Traitement et réponse	Traitement et réponse
Type 1	Réponse d'erreur de mode/d'état	Réponse d'erreur de mode/d'état	Réponse d'erreur de mode/d'état	Traitement et réponse
Type 2	Réponse d'erreur de mode/d'état	Réponse d'erreur de mode/d'état	Réponse d'erreur de mode/d'état	Traitement et réponse

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

6.6.7.11 Service Propose_TUNID

Le service Propose_TUNID établit une proposition de paramétrage du TUNID dans l'appareil. La valeur n'est pas archivée dans la mémoire non volatile ou dans l'attribut TUNID jusqu'à réception du service d'application.

Le service Propose_TUNID ne doit être accepté que lorsque l'appareil cible est dans l'état "Waiting_for_TUNID".

Lorsque le TUNID est défini avec succès, il peut passer à l'état Configuration.

Le NodeID du TUNID doit être comparé à la MACID de l'objet DeviceNet ou à l'attribut IP de l'objet TCP/IP ou au SDID de l'objet Liaison SERCOS III.

La valeur de l'attribut NodeID est le résultat de la lecture des commutateurs ou du réglage par outil. Dans chaque cas, la partie MACID/IP de Proposed_TUNID doit correspondre à ce résultat.

La structure du service Propose_TUNID est définie dans le Tableau 48.

Tableau 48 – Service Propose_TUNID

Nom	Type de données	Description
Code de service	USINT	56hex
TUNID	10 OCTETS	Proposition de valeur d'UNID de l'appareil cible

Si un point d'origine souhaite annuler une proposition/application, la transmission d'une proposition de service avec un TUNID de toutes les valeurs FF_{hex} doit annuler la proposition/application.

Le pseudo-code suivant définit le comportement du service Propose_TUNID:

```
TUNIDProposedHandler()
{
IF (Device_State=Waiting_for_TUNID)
   THEN IF (Propose_TUNID[TUNID] != all FFhex)
         THEN IF (Propose_TUNID[TUNID_MACID] == NodeID)
              THEN
    TUNIDProposedAttr = Propose_TUNID[TUNID]
                   NET LED Flash sequence is started
                   Return Success Reply
              ELSE

   Error Code “Invalid Parameter” is returned
   ELSE // cancel propose_apply operation, returns att. to all FFhex
       Stop NET LED Flash Sequence
      TUNIDProposedAttr = Propose_TUNID[TUNID]
       Return Success Reply
ELSE
      Error Code “Object State Conflict” is returned
}
```

6.6.7.12 Service Apply_TUNID

La structure du service Apply_TUNID est définie dans le Tableau 49 et un organigramme de traitement est défini à la Figure 12.

Tableau 49 – Service Apply_TUNID

Nom	Type de données	Description
Code de service	USINT	57_{hex}
TUNID	10 OCTETS	Proposition de valeur d'UNID de l'appareil cible

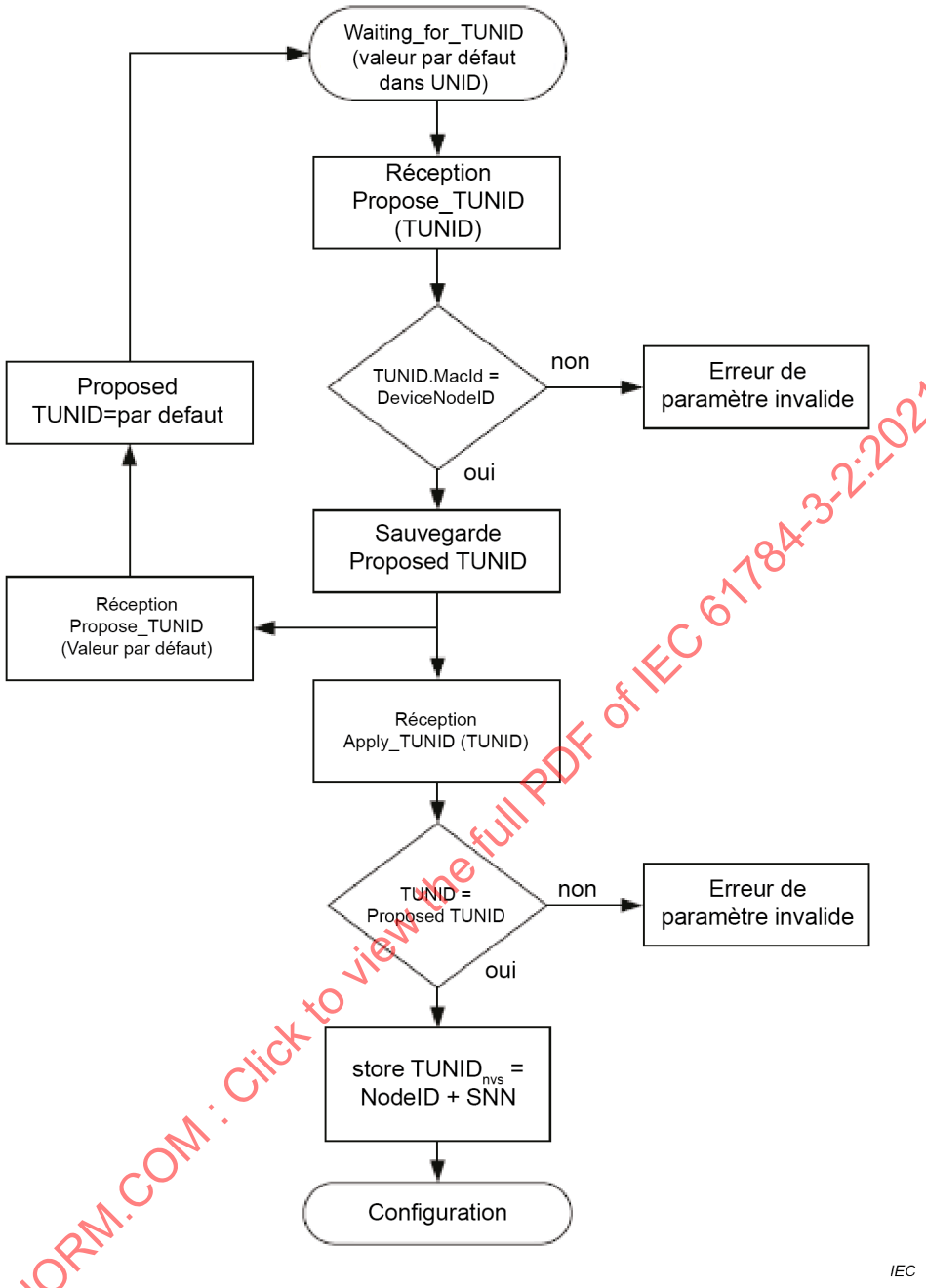
Le service Apply_TUNID doit valider le TUNID par rapport à la valeur proposée. Il interrompt également le clignotement de la LED, sauvegarde le TUNID dans la mémoire non volatile, actualise l'attribut TUNID dans le Programme de contrôle et définit l'attribut proposed_TUNID sur toutes les valeurs FF_{hex}. Le Programme de contrôle doit alors passer à l'état Configuration.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Le pseudo-code suivant définit le comportement du service Apply_TUNID:

```
Apply_TUNIDHandler()
{
IF (Device_State=Waiting_for_TUNID)
   THEN IF {(Apply_TUNID[TUNID] != all FF_hex)
                  AND (TUNIDProposedAttr == Apply_TUNID[TUNID])
        THEN
            Stop Flash Sequence
            Target_UNID = TUNIDProposedVar[TUNID]
//NV Memory operation
// Set SNN attribute in DeviceNet, SERCOS III Link object or TCP/IP
object, NV Memory operation
              Safety_Network_Number = TUNIDProposedVar[SNN]
              TUNIDProposedVar[TUNID] = TUNID_OUT_OF_BOX_DEFAULT
              Return Success Reply
              Device_State = CONFIGURING
         ELSE
              Error Code “Invalid Parameter” is returned
   ELSE
      Error Code “Object State Conflict” is returned
}
```

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021



IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Figure 12 – Traitement d'UNID pendant l'état "Attente du TUNID"

6.6.7.13 Service Propose_TUNID_List

Le service Propose_TUNID_List établit le paramétrage du TUNID pour chaque port d'un appareil. Appliquer le 6.6.7.11 à chaque proposition de TUNID dans la liste. La structure du service Propose_TUNID est définie dans le Tableau 50.

Tableau 50 – Service Propose_TUNID_List

Nom	Type de données	Description
Code de service	USINT	57_{hex}
Nombre de propositions de TUNID	USINT	Nombre d'entrées dans la liste de propositions d'UNID cibles
Propositions de TUNID	MATRICE de STRUCT	Liste de paires (Numéro de port, Proposition de TUNID)
Numéro de port	UINT	Voir l'IEC 61158-4-2:2019, 7.11.4.3
Proposition de TUNID	10 OCTETS	Proposition de TUNID associée à un numéro de port CIP spécifique

6.6.7.14 Service Apply_TUNID_List

Le service Apply_TUNID_List valide la proposition de paramétrage du TUNID pour chaque port d'un appareil. Appliquer le 6.6.7.12 à chaque proposition de TUNID dans la liste. La structure du service Apply_TUNID est définie dans le Tableau 51.

Tableau 51 – Service Apply_TUNID_List

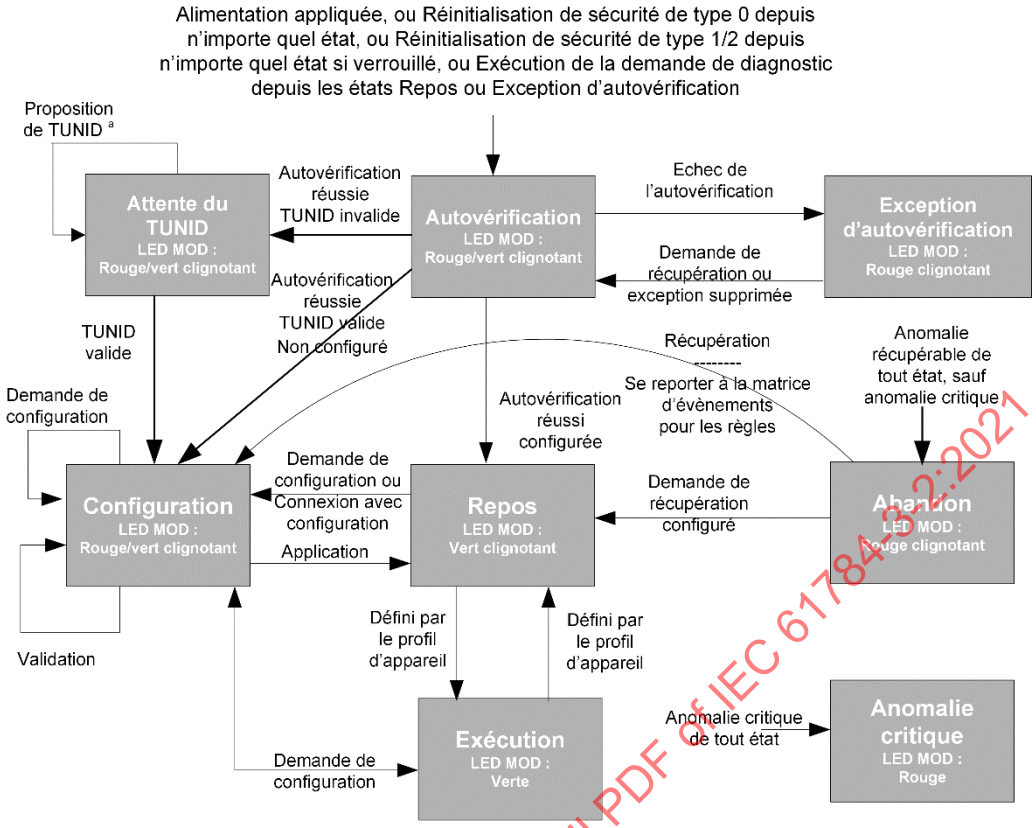
Nom	Type de données	Description
Code de service	USINT	57_{hex}
TUNID	10 OCTETS	Proposition de valeur d'UNID de l'appareil cible

6.6.8 Comportement du Programme de contrôle de sécurité

6.6.8.1 Etats de l'objet Programme de contrôle de sécurité

La Figure 13 représente le diagramme d'états qui définit le comportement de l'objet Programme de contrôle de sécurité. Des informations complémentaires concernant les événements liés audit programme sont données dans le Tableau 52. Le comportement de la LED d'état du module est régi par les états du Programme de contrôle de sécurité comme indiqué dans le diagramme. Les extensions d'état spécifiques au type d'appareil sont admises et explicitement définies dans le profil des appareils de sécurité. Les modifications spécifiques à un appareil du comportement de la LED d'état du module sont également admises et explicitement définies dans le profil des appareils de sécurité. L'état "Attente du TUNID" et le comportement associé de la LED sont spécifiques au fournisseur pour les appareils qui ne prennent pas en charge les services de proposition/d'application du TUNID.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021



a Après une demande de service Propose_TUNID, la LED réseau clignote rouge/vert en utilisant le modèle rapide 250 ms/250 ms jusqu'à la réussite d'Apply_TUNID.

Figure 13 – Diagramme d'états du Programme de contrôle de sécurité

Tableau 52 – Evénements liés au Programme de contrôle de sécurité

Etat	Description
Exécution	L'appareil est en cours d'exécution (par exemple, est en phase de configuration complète, ne comporte pas d'erreurs et a satisfait aux critères définis par le fournisseur). Cet état, et les transitions vers ou hors de cet état, doivent être spécifiés davantage dans une spécification de profil d'appareil appropriée
Autovérification	L'instance objet existe et a été initialisée; tous les attributs ont des valeurs initiales appropriées (tel qu'indiqué dans le présent document et dans la spécification de profil d'appareil applicable). Les bits d'Etat d'exception ont été réinitialisés. L'appareil effectue un essai spécifique à l'appareil et spécifique au type d'appareil afin de déterminer s'il est qualifié pour exécuter son processus d'application
Exception d'autovérification	L'objet a détecté une condition d'exception au cours de l'autovérification. Les détails de l'exception sont archivés dans les valeurs d'attribut appropriées de l'objet Programme de contrôle de sécurité
Repos	L'objet et l'appareil ont été initialisés, ont effectué une autovérification satisfaisante et ont une configuration valide. De plus, l'appareil n'utilise pas les composants opérationnels de ses fonctions spécifiques. La configuration et le repos sont des états persistants conservés tout au long des cycles d'alimentation
Abandon	L'instance objet est dans l'état Abandon; cet état ne peut être adopté qu'en l'occurrence d'événements à génération interne. Les conditions nécessaires à la sortie d'un état d'anomalie récupérable sont définies dans la matrice d'événements
Attente du TUNID	L'appareil quitte l'état Autovérification et détermine que le TUNID archivé dans la mémoire non volatile a une valeur par défaut d'usine. Il reste dans cet état jusqu'à l'achèvement satisfaisant de la séquence de paramétrage du TUNID (opération de proposition/application dans l'interface SNCT). L'appareil peut alors être configuré

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Etat	Description
Configuration	L'objet et l'appareil ont été initialisés, ont effectué une autovérification satisfaisante, mais n'ont PAS de configuration valide. La configuration et le repos sont des états conservés tout au long des cycles d'alimentation
Anomalie critique	L'objet (et l'appareil) est dans un état d'anomalie, où aucune récupération n'est réalisée. Le traitement de services d'objet particuliers peut être impossible dans cet état. Les éventuelles autres conditions nécessaires à la sortie d'un état d'anomalie critique ne relèvent pas du domaine d'application du présent document

La valeur de l'attribut Etat du Programme de contrôle de sécurité indique l'état général de l'appareil. Elle est actualisée par rapport aux transitions d'état appropriées dans l'objet Programme de contrôle de sécurité. Les valeurs d'attribut 1 à 8 représentent des états valides. Une valeur nulle indique que l'état du Programme de contrôle de sécurité n'est pas connu; les conditions dans lesquelles une valeur nulle peut exister ne relèvent pas du domaine d'application du présent document.

6.6.8.2 Matrice d'événements d'état du Programme de contrôle de sécurité

Le Tableau 53 définit les états et événements applicables au Programme de contrôle de sécurité.

Tableau 53 – Matrice d'événements d'état du Programme de contrôle de sécurité

Evénement	Etat							
	Attente du TUNID	Configu-ration (Etat de sécurité)	Repos (Etat de sécurité)	Autovéri-fication (Etat de sécurité)	Exception d'autovéri-fication (Etat de sécurité)	Exécution	Abandon (Etat de sécurité)	Anomalie critique (Etat de sécurité)
Alimentation appliquée			--	Le point d'entrée par défaut effectue son processus d'applica-tion d'autovéri-fication	--	--	--	Transition vers l'état AUTOVÉ-RIFICA-TION
Autovérifica-tion réussie			Non applicable	Transition vers le dernier état sauvegar-dé s'il ne s'agit pas de l'état d'usine Sinon, Attente du TUNID	Non applicable	Non applicable	Non applicable	Non applicable
Echec de l'autovérifi-cation			Non applicable	Définition des bits d'état d'exception appropriés et transition vers l'état EXCEP-TION D'AUTO-VÉRIFI-CATION	Non applicable	Non applicable	Non applicable	Non applicable

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Evénement	Etat							
	Attente du TUNID	**Configuration (Etat de sécurité)**	**Repos (Etat de sécurité)**	**Autovérification (Etat de sécurité)**	**Exception d'autovérification (Etat de sécurité)**	**Exécution**	**Abandon (Etat de sécurité)**	**Anomalie critique (Etat de sécurité)**
Proposition de TUNID	Validation des réglages et de la LED réseau clignotante rouge/vert à l'aide d'un modèle rapide 250 ms/250 ms	Erreur OSC[b]	Erreur OSC[b]	Erreur OSC[b]	Erreur OSC[b]	Erreur OSC[b]	Erreur OSC[b]	Erreur OSC[b]
Application du TUNID	Sauvegarde du TUNID dans la mémoire non volatile, Transition vers l'état Configuration	Erreur OSC[b]	Erreur OSC[b]	Erreur OSC[b]	Erreur OSC[b]	Erreur OSC[b]	Erreur OSC[b]	Erreur OSC[b]
Condition d'exception supprimée			Non applicable	Non applicable	Définition des bits d'état d'exception appropriés et transition vers l'état AUTOVÉRIFICATION	Non applicable	Non applicable	Non applicable
Anomalie critique	Transition vers l'état ANOMALIE CRITIQUE	Transition vers l'état ANOMALIE CRITIQUE	Transition vers l'état ANOMALIE CRITIQUE	Transition vers l'état ANOMALIE CRITIQUE	Transition vers l'état ANOMALIE CRITIQUE	Transition vers l'état ANOMALIE CRITIQUE	Transition vers l'état ANOMALIE CRITIQUE	Non prise en compte de l'événement
Demande de configuration	Erreur TNS[c]	Maintien dans l'état Validation et acceptation	Si non verrouillé, Transition vers l'état Configuration	Erreur OSC[b]	Erreur OSC[b]	Si non verrouillé, Retrait des connexions Application de l'état de sécurité Transition vers l'état Configuration	Si configuré: Transition vers l'état REPOS --- Non configuré: Transition vers l'état Configuration --- Si non-concordance Commutateur/TUNID Erreur OSC[b]	Erreur OSC[b]

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Evénement	Etat							
	Attente du TUNID	**Configuration (Etat de sécurité)**	**Repos (Etat de sécurité)**	**Autovérification (Etat de sécurité)**	**Exception d'autovérification (Etat de sécurité)**	**Exécution**	**Abandon (Etat de sécurité)**	**Anomalie critique (Etat de sécurité)**
Validation Configuration	Erreur OSC[b]	Maintien dans l'état – Archivage du résultat	Erreur OSC[b]	Erreur OSC[b]	Erreur OSC[b]	Erreur OSC[b]	Erreur OSC[b]	Erreur OSC[b]
Demande d'application	Erreur OSC[b]	Transition vers l'état Repos si valide	Erreur OSC[b]	Erreur OSC[b]	Erreur OSC[b]	Erreur OSC[b]	Erreur OSC[b]	Erreur OSC[b]
SafetyOpen de type 1	Erreur TNS[c]	Application de la transition de configuration vers l'état Exécution si configuration valide	Transition vers l'état Configuration, Adoption de l'état REPOS/ EXÉCUTION en fonction du profil	Erreur OSC[b]	Erreur OSC[b]	Retrait des connexions, transition vers l'état Configuration, adoption de l'état REPOS/ EXÉCUTION en fonction du profil	Erreur OSC[c]	Erreur OSC[b]
Réinitialisation de sécurité de type 0	Transition vers l'état AUTOVÉRIFICATION	Transition vers l'état AUTOVÉRIFICATION	Transition vers l'état AUTOVÉRIFICATION	Transition vers l'état AUTOVÉRIFICATION	Transition vers l'état AUTOVÉRIFICATION	Transition vers l'état AUTOVÉRIFICATION (SRS15)	Transition vers l'état AUTOVÉRIFICATION	Transition vers l'état AUTOVÉRIFICATION si possible
Réinitialisation de sécurité de type 1/2	Si non verrouillé, Traitement de type Transition vers l'état AUTOVÉRIFICATION	Si non verrouillé, Traitement de type Transition vers l'état AUTOVÉRIFICATION	Si non verrouillé, Traitement de type Transition vers l'état AUTOVÉRIFICATION	Si non verrouillé, Traitement de type Transition vers l'état AUTOVÉRIFICATION	Si non verrouillé, Traitement de type Transition vers l'état AUTOVÉRIFICATION	Si non verrouillé, Traitement de type Transition vers l'état AUTOVÉRIFICATION (SRS15)	Si non verrouillé, Traitement de type Transition vers l'état AUTOVÉRIFICATION	Si non verrouillé, Traitement de type Transition vers l'état AUTOVÉRIFICATION
Demande d'abandon interne	Transition vers l'état Abandon	Transition vers l'état Abandon	Transition vers l'état Abandon	Erreur OSC[b]	Erreur OSC[b]	Transition vers l'état Abandon	Erreur AIRS[a]	Erreur OSC[b]
Demande de récupération	Erreur OSC[b]	Erreur OSC[b]	Erreur OSC[b]	Redémarrage AUTOVÉRIFICATION	Transition vers l'état AUTOVÉRIFICATION	Erreur OSC[b]	Si configuré: Transition vers l'état REPOS --- Non configuré: Transition vers l'état Configuration --- Si non-concordance Commutateur/ TUNID Erreur OSC[b]	Erreur OSC[b]

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Evénement	Etat							
	Attente du TUNID	**Configuration (Etat de sécurité)**	**Repos (Etat de sécurité)**	**Autovérification (Etat de sécurité)**	**Exception d'autovérification (Etat de sécurité)**	**Exécution**	**Abandon (Etat de sécurité)**	**Anomalie critique (Etat de sécurité)**
Exécution de la demande de diagnostic	Erreur OSC[b]	Erreur OSC[b]	Transition vers l'état AUTOVÉRIFICATION	Redémarrage AUTOVÉRIFICATION	Transition vers l'état AUTOVÉRIFICATION	Erreur OSC[b]	Exécution de tous les essais de diagnostic	Erreur OSC[b]
Echec de la connexion de sécurité	Non prise en compte de l'événement	Non prise en compte de l'événement	Non prise en compte de l'événement	Non prise en compte de l'événement[d]	Non prise en compte de l'événement	Profil d'appareil défini	Non prise en compte de l'événement[d]	Non prise en compte de l'événement[d]
Connexion E/S de sécurité établie	Impossible	Impossible	Profil d'appareil défini	Non prise en compte de l'événement[d]	Impossible	Profil d'appareil défini	Impossible	Impossible
Connexion E/S de sécurité supprimée	Non prise en compte de l'événement[d]	Non prise en compte de l'événement[d]	Non prise en compte de l'événement[d]	Non prise en compte de l'événement[d]	Impossible	Profil d'appareil défini	Non prise en compte de l'événement[d]	Erreur OSC[b]
Changement de mode	Erreur OSC[b]	Erreur OSC[b]	Profil d'appareil défini	Erreur OSC[b]	Erreur OSC[b]	Profil d'appareil défini	Erreur OSC[b]	Erreur OSC[b]
Restauration	Erreur OSC[b]	Restauration de la configuration précédente	Erreur OSC[b]	Erreur OSC[b]	Erreur OSC[b]	Non prise en compte de l'événement[d]	Erreur OSC[b]	Erreur OSC[b]
Verrouillage/ Déverrouillage	Erreur OSC[b]	Erreur OSC[b]	Si valide, exécution et réponse	Erreur OSC[b]	Erreur OSC[b]	Si valide, exécution et réponse	Si valide, exécution et réponse	Si valide, exécution et réponse si possible
Définitions des LED applicables aux états								
LED d'état du module	Rouge/Vert clignotant	Rouge/ Vert clignotant	Vert clignotant	Rouge/Vert clignotant	Rouge clignotant	Vert fixe	Rouge clignotant	Rouge fixe

[a] Erreur AIRS = Réponse d'erreur "Déjà en mode/état sollicité" (code $0B_{hex}$).

[b] Erreur OSC = Réponse d'erreur "Conflit d'état d'objet" (code $0Ch_{hex}$) dans toute la mesure du possible.

[c] Erreur TNS = Réponse d'erreur "TUNID non défini", code étendu 01_{hex} ou code étendu spécifique à l'objet $80D_{hex}$.

[d] Non prise en compte de l'événement: défini comme "l'événement n'a pas d'influence sur l'état", aucune réponse nécessaire.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

L'appareil peut solliciter l'existence d'un service instance de Programme de contrôle de sécurité en interne, spécifié par le fabricant. Généralement, ces demandes sont générées après un événement tel qu'un échec de diagnostic.

6.6.8.3 Influence du verrouillage sur le comportement de l'appareil

La Figure 14 définit l'influence de la condition "verrouillée" sur la capacité de configuration d'un appareil; les appareils verrouillés rejettent toutes les tentatives de modification des données de configuration qui affectent le SCID.

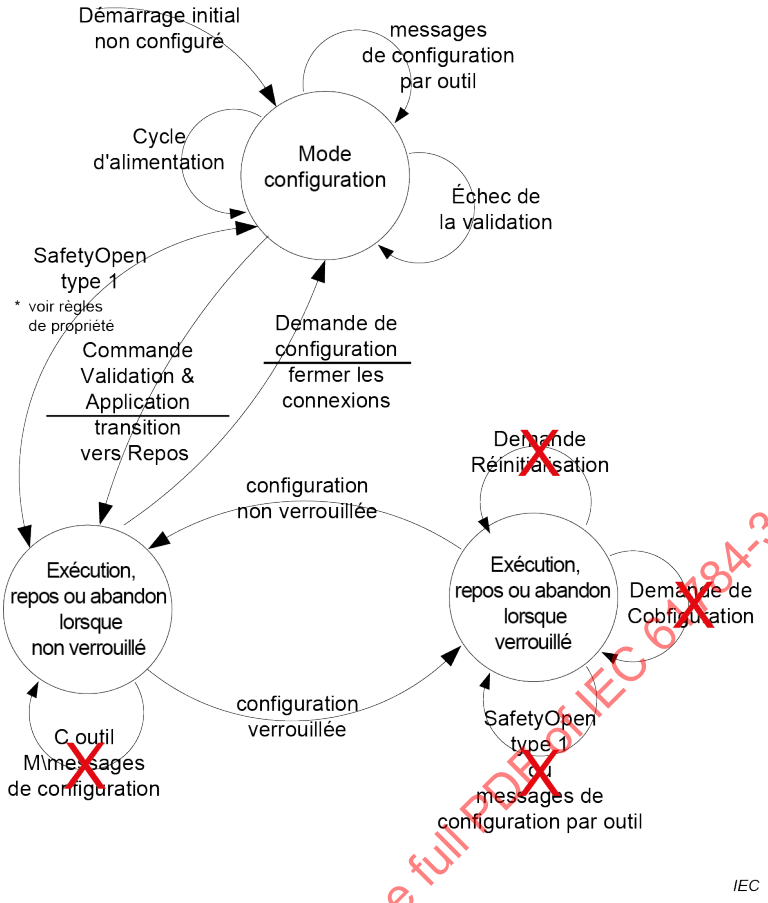


Figure 14 – Relations entre configuration, essais et verrouillage

Le Tableau 54 définit l'influence de la propriété sur la capacité de configuration d'un appareil. Il indique que la configuration des appareils avec propriétaire peut être uniquement de type 1, ladite configuration étant effectuée par le point d'origine qui possède l'UNID du propriétaire. Un appareil verrouillé ne peut jamais être configuré, quel que soit son propriétaire.

Tableau 54 – Contrôle de la propriété de configuration en fonction de l'état de l'appareil

Règles de propriété	Mode de configuration	Mode Exécution/Repos non verrouillé	Mode Exécution/Repos verrouillé
Configuration avec propriétaire (OUNID de configuration = UNID du propriétaire)	Type 1 accepté par le propriétaire uniquement	Type 1 accepté par le propriétaire uniquement	Tous les types 1 refusés
Configuration sans propriétaire (OUNID de configuration = 0)	Type 1 accepté par quiconque	Type 1 accepté par quiconque	Tous les types 1 refusés
Outil logiciel avec propriétaire (OUNID de configuration = toutes les valeurs FF_{hex})	Aucun type 1 accepté	Aucun type 1 accepté	Tous les types 1 refusés

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

6.6.8.4 Mapping des états de l'objet Programme de contrôle de sécurité vers l'objet Identité

Le Tableau 55 définit le mapping des états du Programme de contrôle de sécurité vers les états définis pour l'objet Identité. Ce mapping des états définit l'interface entre ces trois objets. L'attribut d'état de l'objet Identité (si pris en charge) doit suivre ce tableau.

Tableau 55 – Mapping des états du Programme de contrôle de sécurité vers l'objet Identité

Programme de contrôle de sécurité	Identité
Autovérification	Autovérification de l'appareil
Exception d'autovérification	Principalement non récupérable
Repos	En attente
Configuration	En attente
Attente du TUNID	En attente
Exécution	Opérationnel
Abandon	Principalement récupérable
Anomalie critique	Principalement non récupérable

6.6.8.5 Mapping d'un événement de l'objet Programme de contrôle de sécurité vers un événement de l'objet Identité

Le Tableau 56 décrit le mapping d'événements définis du Programme de contrôle de sécurité vers des événements équivalents définis pour l'objet Identité. Ce mapping des événements définit l'interface entre ces objets. Ce mapping est fourni à des fins de référence.

Tableau 56 – Mapping des événements de l'objet Programme de contrôle de sécurité

Mapping des événements d'état du Programme de contrôle de sécurité vers ->	Evénement d'Identité équivalent
Alimentation appliquée	Alimentation appliquée
Echec de l'autovérification	Essais non réussis
Autovérification réussie	Essais réussis
Proposition de TUNID	Aucun événement équivalent
Application du TUNID	Aucun événement équivalent
Condition d'exception supprimée	Anomalie corrigée
Anomalie critique	Anomalie principale non récupérable
Demande de configuration	Désactivé
Validation de configuration	Aucun événement équivalent
Application de la configuration	Activé
SafetyOpen de type 1	Aucun événement équivalent
Réinitialisation de sécurité	Réinitialisation
Abandon (Interne)	Anomalie principale récupérable
Demande de récupération	Anomalie corrigée
Exécution de la demande de diagnostic	Aucun événement équivalent
Echec de la connexion de sécurité	Désactivé
Connexion de sécurité établie	Activé
Connexion de sécurité supprimée	Aucun événement équivalent

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Mapping des événements d'état du Programme de contrôle de sécurité vers ->	Evénement d'Identité équivalent
Changement de mode	Aucun événement équivalent
Restauration	Aucun événement équivalent
Verrouillage/Déverrouillage	Aucun événement équivalent

6.6.8.6 Mapping d'un événement de l'objet Identité vers un événement du Programme de contrôle de sécurité

Le Tableau 57 décrit le mapping de conditions d'événements définies des objets Identité vers des événements équivalents définis pour l'objet Programme de contrôle de sécurité. Ce mapping des événements définit les événements équivalents entre ces objets. Ce mapping n'est fourni qu'à des fins de référence; l'objet Programme de contrôle de sécurité est l'objet de contrôle des appareils de sécurité et seuls les événements définis par le programme de contrôle doivent être mis en œuvre dans ces mêmes appareils.

Tableau 57 – Mapping des événements de l'objet Identité

Mapping des événements d'Identité vers ->	Evénements du Programme de contrôle de sécurité
Alimentation appliquée	Alimentation appliquée
Essais non réussis	Echec de l'autovérification
Essais réussis	Autovérification réussie
Désactivé	Demande de configuration
Activé	Application de la configuration
Anomalie principale récupérable	Abandon (interne)
Anomalie principale non récupérable	Anomalie critique
Anomalie secondaire	Aucune influence
Anomalie corrigée	Condition d'exception supprimée
Réinitialisation	Erreur Service non pris en charge

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

6.7 Objet de validation de sécurité

6.7.1 Généralités

Code de classe: $3A_{hex}$

L'Objet de validation de sécurité est conçu pour être utilisé dans les appareils de sécurité sur tous les réseaux FSCP 2/1. Cet objet contient les informations nécessaires à la coordination et au maintien de connexions de sécurité fiables entre les applications relatives à la sécurité client et serveur. Le rôle principal de la fonction Objet de validation de sécurité est d'agir comme un gestionnaire de transport de sécurité des multiples connexions CPF 2 de faible niveau qui ensemble constituent une connexion de sécurité complète.

L'appareil qui contient l'Objet de validation de sécurité peut créer plusieurs instances de cet objet pour chaque point de connexion d'application relative à la sécurité (par exemple, ensemble de données d'application) pris en charge par l'appareil.

L'Objet de validation de sécurité prend en charge deux types fondamentaux de transport de sécurité: le point à point et le multipoint. Chaque type de transport de sécurité comprend un ensemble défini de connexions CPF 2 de faible niveau qui doit être attribué avec l'Objet de validation de sécurité en cas d'instanciation d'une connexion de sécurité par une fonction SafetyOpen.

6.7.2 Attributs de classe

Les attributs de classe destinés au programme de contrôle de sécurité sont définis dans le Tableau 58.

Tableau 58 – Attributs de classe de l'Objet de validation de sécurité

ID d'attribut	Mise en œuvre nécessaire	Règle d'accès	Nom	Type de données	Description de l'attribut	Sémantique de la valeur
1 – 7	Facultatif	Obtenir			Voir l'IEC 61158-5-2 et l'IEC 61158-6-2 pour une description des attributs de classe réservés facultatifs	
8	Exigé	Obtenir	Comptage des anomalies de connexion de sécurité	UINT	Compteur de diagnostics qui représente le cumul des anomalies de connexion de sécurité	

Comptage des anomalies de connexion de sécurité: cet attribut de l'Objet de validation de sécurité doit représenter le cumul (avec autoremplacement) du nombre d'anomalies de connexions de sécurité, pour quelque motif que ce soit.

6.7.3 Attributs instance

6.7.3.1 Présentation générale des attributs instance

La plupart des valeurs d'attributs sont figées dans le code ou issues du processus d'établissement des connexions dynamiques. La seule valeur d'attribut définissable est le diagnostic de l'âge maximal des données. La liste complète des attributs instance est définie dans le Tableau 59.

Tableau 59 – Attributs instance de l'Objet de validation de sécurité

ID d'attribut	Mise en œuvre nécessaire	Règle d'accès	NV	Nom	Type de données	Description de l'attribut	Sémantique de la valeur
1	Exigé	Obtenir		Etat de l'Objet de validation de sécurité	USINT	Etat de la connexion de sécurité	
2	Exigé	Obtenir		Type d'Objet de validation de sécurité	USINT	Type d'Objet de validation de sécurité utilisé dans cette instance	Voir 6.7.3.3
3	Facultatif	Obtenir		Multiplicateur EPI d'intervalles Ping	UINT	Nombre qui définit le Ping_Count_Interval pour une connexion particulière	16 à 1 000

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

ID d'attribut	Mise en œuvre nécessaire	Règle d'accès	NV	Nom	Type de données	Description de l'attribut	Sémantique de la valeur
4	Facultatif	Obtenir		Multiplicateur minimal de messages de coordination temporelle	STRUCT de:		
				Taille de matrice de Multiplicateur minimal de messages de coordination temporelle	USINT	La taille de la matrice est égale au nombre maximal de consommateurs pour les producteurs multipoints, et à 1 pour le consommateur point à point et multipoint	
				Multiplicateur minimal de messages de coordination temporelle	MATRICE de: UINT	Nombre minimal d'incréments de 128 µs susceptibles d'être utilisés pour transmettre un message de coordination temporelle du consommateur au producteur	0 – 7 813
5	Facultatif	Obtenir		Multiplicateur de délai du réseau	STRUCT de:		
				Taille de matrice Multiplicateur de délai du réseau	USINT	La taille de la matrice est égale au nombre maximal de consommateurs pour les producteurs multipoints, et à 1 pour le consommateur point à point et multipoint	
				Multiplicateur de délai du réseau	MATRICE de: UINT	Nombre maximal d'incréments de 128 µs qu'un consommateur doit permettre à l'âge des données de sécurité d'atteindre	0 – 45 313

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

ID d'attribut	Mise en œuvre nécessaire	Règle d'accès	NV	Nom	Type de données	Description de l'attribut	Sémantique de la valeur
6	Facultatif	Obtenir		Multiplicateur de temporisa-tion	STRUCT de:		
				Taille de matrice de Multiplicateur de temporisa-tion	USINT	La taille de la matrice est égale au nombre maximal de consommateurs pour les producteurs multipoints, et à 1 pour le consommateur point à point et multipoint	
				Multiplicateur de temporisa-tion	MATRICE de: USINT	Détermine le nombre de messages qui peut être perdu préalablement à toute déclaration d'erreur de connexion	Format de base: 1-4 Format étendu: 1-255
7	Facultatif	Obtenir		Nombre maximal de consomma-teurs	USINT	Nombre maximal de consommateurs admis pour la connexion	1 (Point à point) 2 – 15 (Multipoint)
8	Facultatif[a]	Obtenir		Instance de connexion de données	UINT	ID d'instance de la connexion de données de sécurité	
9	Facultatif[a]	Obtenir		Instance de connexion de coordination	STRUCT de:	ID d'instance de la connexion de coordination de sécurité	1-nombre maximal de connexions de l'appareil
				Taille de matrice d'Instance de connexion de coordination	USINT	La taille de la matrice est égale au nombre maximal de consommateurs pour les producteurs multipoints, et à 1 pour le consommateur point à point et multipoint	
				Instance de connexion de coordination	MATRICE de: UINT		
10	Facultatif[a]	Obtenir		Instance de connexion de correction	UINT	ID d'instance de la connexion de correction de temps	0 (lorsque non utilisé) 1-nombre maximal de connexions de l'appareil
11	Facultatif[a]	Obtenir		Rattache-ment CCO	UINT	ID d'instance d'un CCO qui détient les paramètres d'établissement de connexion pour cette connexion. Utilisé uniquement par les points d'origine de la connexion de sécurité	0 (lorsque non utilisé ou en l'absence de rattache-ment)

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

ID d'attribut	Mise en œuvre nécessaire	Règle d'accès	NV	Nom	Type de données	Description de l'attribut	Sémantique de la valeur
12	Exigé	Définir		Age maximal des données	UINT	Diagnostic qui détient l'âge des données le plus élevé détecté par incréments de 128 µs. Attribut utilisé uniquement pour les consommateurs de sécurité	L'ensemble ne doit être pris en charge que par le consomma-teur. Zéro est la seule valeur valide pour l'ensemble. Voir 6.7.3.13.
13	Exigé	Obtenir		Chemin de données d'application	EPATH compact	Points de liaison avec les données d'application associées à cette connexion de sécurité	
14	Facultatif	Obtenir	V	Code d'erreur	UINT	Motif d'erreur dans cette instance	0 en l'absence d'erreur; dans les autres cas, code d'erreur spécifique à la mise en œuvre
15	Conditionnel[b]	Obtenir	V	Compteurs des anomalies Producteur/ Consomma-teur	STRUCT de:		
				Taille de matrice de Compteurs Producteur /Consomma-teur	USINT	La taille de la matrice est égale au nombre maximal de consommateurs pour les producteurs multipoints, et à 1 pour le consommateur point à point et multipoint	
				Compteur des anomalies Producteur/ Consomma-teur	MATRICE de: USINT	Nombre d'anomalies détectées par ce compteur	Voir 6.7.3.14

[a] La publication de ces paramètres est facultative. Cependant, toutes les instances d'Objet de validation doivent avoir des paramètres internes qui représentent ces variables.

[b] Si l'appareil prend en charge le format étendu, cet attribut est exigé.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

6.7.3.2 Etat de l'Objet de validation de sécurité

Cet attribut définit l'état courant de l'instance Objet de validation de sécurité. Les transitions propres à cet attribut d'état reflètent l'état courant de l'objet. Les définitions sont données dans le Tableau 60. Cet attribut peut être utilisé pour déterminer la condition des connexions de sécurité établies

Tableau 60 – Attributions d'états de l'Objet de validation de sécurité

Valeur	Nom d'état	Description
0	Non attribué	Dans cet état, l'Objet de validation de sécurité n'a pas été attribué à une connexion, ou a été fermé
1	Initialisation	Dans cet état, l'Objet de validation de sécurité se situe dans le processus d'échange des informations de coordination temporelle sur la connexion. La connexion "de sécurité" n'est pas encore pleinement établie
2	Etabli	Dans cet état, l'instance Objet de validation de sécurité est pleinement établie et produit/consomme des données de sécurité pour le compte de l'application relative à la sécurité
3	Connection_Failed	Cet état est actif lorsque toutes les connexions associées à cet Objet de validation ont échoué pour quelque raison que ce soit. Dans le cas des producteurs, toutes les connexions de consommateur multipoint doivent avoir échoué. Le producteur reste dans l'état Etabli tant qu'un consommateur est toujours actif
4-255	Réservé	

6.7.3.3 Type d'Objet de validation de sécurité

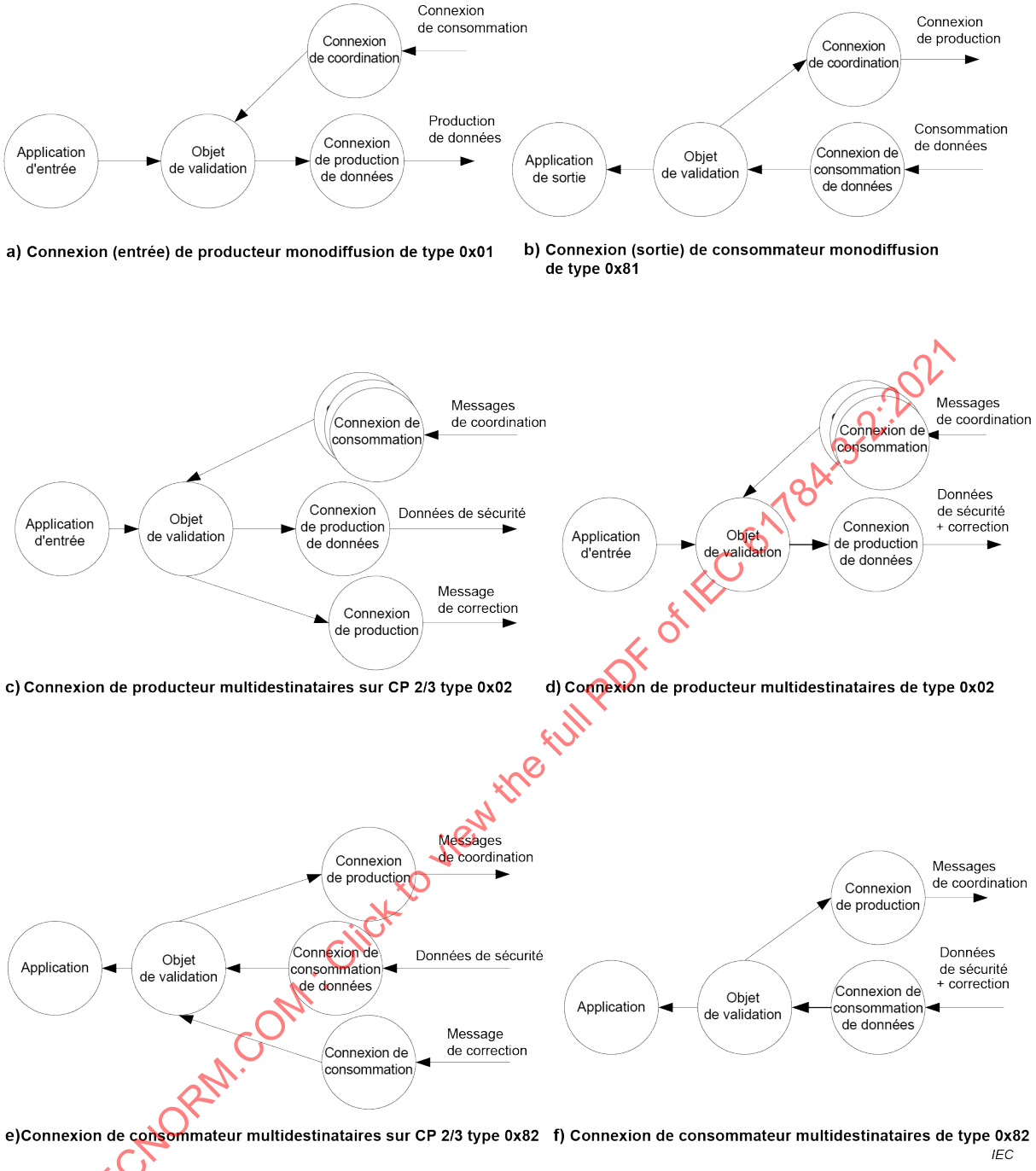
Cet attribut définit le type de transport utilisé par l'Objet de validation de sécurité, dont la définition est donnée dans le Tableau 61. Les cibles doivent déduire cette valeur des paramètres de connexion de sécurité de la fonction SafetyOpen.

Tableau 61 – Type d'Objet de validation de sécurité, attributions de champs de bits

Bit 7	Bits 0 – 6
Producteur (client) = 0/ Consommateur (serveur) = 1	Type de connexion de sécurité: 0 = non attribué 1 = Point à point 2 = Multipoint 3 – 127 = Réservé

Les transports propres à chaque type d'Objet de validation de sécurité sont représentés à la Figure 15. Cet attribut peut être utilisé pour demander à un appareil de déterminer le type de connexion qui a été établie.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021



a) Connexion (entrée) de producteur monodiffusion de type 0x01

b) Connexion (sortie) de consommateur monodiffusion de type 0x81

c) Connexion de producteur multidestinataires sur CP 2/3 type 0x02

d) Connexion de producteur multidestinataires de type 0x02

e)Connexion de consommateur multidestinataires sur CP 2/3 type 0x82

f) Connexion de consommateur multidestinataires de type 0x82

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Figure 15 – Types de connexions de sécurité

6.7.3.4 Multiplicateur EPI d'intervalles Ping

Cet attribut est utilisé comme partie intégrante de la fonction Objet de validation de sécurité. Ce paramètre provient des paramètres du Segment de sécurité de la fonction SafetyOpen. Les règles que doivent suivre les producteurs multipoints pour l'évaluation de ce paramètre provenant de consommateurs multiples sont définies dans le Tableau 62.

6.7.3.5 Multiplicateur minimal de messages de coordination temporelle

Cet attribut est utilisé comme partie intégrante de la fonction Objet de validation de sécurité. Ce paramètre provient des paramètres du Segment de sécurité de la fonction SafetyOpen. Les règles que doivent suivre les producteurs multipoints pour l'évaluation de ce paramètre provenant de consommateurs multiples sont définies dans le Tableau 62.

Tableau 62 – Règles d'évaluation du paramètre SafetyOpen des producteurs multipoints

Paramètre de sécurité	Règle d'évaluation des producteurs	Réponse d'erreur (le cas échéant)
Multiplicateur EPI d'intervalles Ping	Doit correspondre au P.I.E.M. existant (le consommateur le définit en premier lieu)	Paramètre invalide
Multiplicateur minimal de messages Time_Coord	Accepter tout multiplicateur (peuvent être tous différents)	NA
Multiplicateur de délai du réseau	Accepter tout multiplicateur (peuvent être tous différents)	NA
Multiplicateur de temporisation	Accepter tout multiplicateur (peuvent être tous différents)	NA
Nombre maximal de consommateurs	Doit correspondre au Max_Consumer_Number existant (le consommateur le définit en premier lieu)	Paramètre invalide

6.7.3.6 Multiplicateur de délai du réseau

Cet attribut définit le temps de réaction de connexion associé à cette connexion. Ce paramètre provient des paramètres du Segment de sécurité de la fonction SafetyOpen. Les règles que doivent suivre les producteurs multipoints pour l'évaluation de ce paramètre provenant de consommateurs multiples sont définies dans le Tableau 62.

6.7.3.7 Multiplicateur de temporisation

Cet attribut définit la tolérance sur l'Objet de validation de sécurité pour les messages perdus préalablement à la défaillance d'une connexion et à l'application d'une mesure de sécurité. Ce paramètre provient des paramètres du Segment de sécurité de la fonction SafetyOpen. Les règles que doivent suivre les producteurs multipoints pour l'évaluation de ce paramètre qui provient de consommateurs multiples sont définies dans le Tableau 62.

6.7.3.8 Nombre maximal de consommateurs

Cet attribut définit le nombre maximal de consommateurs qui sont autorisés à se connecter à un producteur multipoint (type 82). Les consommateurs et producteurs multipoints ont besoin tous deux de connaître cette valeur pour fonctionner correctement. Ce paramètre provient des paramètres du Segment de sécurité de la fonction SafetyOpen. Les règles que doivent suivre les producteurs multipoints pour l'évaluation de ce paramètre qui provient de consommateurs multiples sont définies dans le Tableau 62.

6.7.3.9 Instance de connexion de données

Cet attribut identifie l'instance de l'objet de connexion responsable de la connexion Données de sécurité. Cet attribut est affecté comme partie intégrante du processus d'établissement de la connexion.

6.7.3.10 Instance de connexion de coordination

Cet attribut identifie l'instance de l'objet de connexion responsable de la connexion de coordination temporelle. Cet attribut est affecté comme partie intégrante du processus d'établissement de la connexion.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

6.7.3.11 Instance de connexion de correction

Cet attribut identifie l'instance de l'objet de connexion responsable de la connexion Correction de temps si elle est utilisée. Cet attribut est affecté comme partie intégrante du processus d'établissement de la connexion.

6.7.3.12 Rattachement CCO

Cet attribut identifie l'instance Configuration de connexion utilisée pour l'établissement de cette connexion de sécurité. Ce rattachement est nécessaire pour indiquer à la fonction CCO la fermeture de la connexion, de sorte qu'elle puisse tenter de rétablir la connexion. Cet attribut n'est utilisé qu'avec les points d'origine de connexion. Cet attribut peut être attribué comme partie intégrante du processus d'établissement des connexions ou figé dans le code lors de la conception.

6.7.3.13 Age maximal des données

L'âge des données de paquets reçues est défini comme la différence entre l'horloge de 128 µs du consommateur et la datation reçue au moment de la réception du paquet. L'attribut Age maximal des données est la valeur maximale de cet âge lorsque la connexion est/a été établie. La valeur peut être utilisée par des outils de diagnostic afin d'accorder le multiplicateur de délai du réseau.

L'attribut Age maximal des données doit toujours refléter la plus grande valeur atteinte par l'âge des données de connexion, sans dépasser la valeur du multiplicateur de délai.

En cas d'anomalie et de fermeture d'une connexion de sécurité, l'attribut Age maximal des données doit être réinitialisé à la valeur 0, lorsque la connexion est rétablie.

6.7.3.14 Compteur des anomalies Producteur/Consommateur

Cet attribut reflète les compteurs d'anomalies de producteur ou de consommateur internes, dans le cas des connexions qui utilisent le format étendu.

Lorsque la connexion est une connexion de consommation EF, l'attribut Compteur des anomalies Producteur/Consommateur doit refléter les Consumer_Fault_Counters. Lorsque la connexion est une connexion de production EF, l'attribut doit refléter le Producer_Fault_Counter.

L'attribut est utilisé dans les essais d'évaluation qui vérifient le bon fonctionnement du comportement de détection des anomalies EF.

6.7.4 Services de classes

Les services de classes pris en charge par l'Objet de validation de sécurité sont définis dans le Tableau 63.

Tableau 63 – Services de classes de l'Objet de validation de sécurité

Code de service	Mise en œuvre nécessaire	Nom	Description du service
$0E_{hex}$	Exigé	Get_Attribute_Single	Utilisé pour la lecture d'une valeur d'attribut de classe de l'Objet de validation de sécurité
$4B_{hex}$	Facultatif	Réinitialisation de tous les compteurs d'erreurs	Utilisé pour réinitialiser l'attribut de classe 8 dans toutes les instances

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

6.7.5 Services instance

6.7.5.1 Présentation générale des services instance

Les services instance pris en charge par l'Objet de validation de sécurité sont définis dans le Tableau 64.

Tableau 64 – Services instance de l'Objet de validation de sécurité

Code de service	Mise en œuvre nécessaire	Nom	Description du service
01_{hex}	Facultatif	Get_Attribute_All	Renvoie les valeurs de tous les attributs instance
$0E_{hex}$	Exigé	Get_Attribute_Single	Utilisé pour la lecture d'une valeur d'attribut de l'Objet de validation de sécurité
10_{hex}	Exigé	Set_Attribute_Single	Utilisé pour la réinitialisation de l'attribut Age maximal des données
$4B_{hex}$	Facultatif	Réinitialisation du code d'erreur	Utilisé pour la réinitialisation de l'attribut instance 14

6.7.5.2 Réponse Get_Attributes_All

Les données de réponse au service Get_Attributes_All sont définies dans le Tableau 65.

Tableau 65 – Données du service Get_Attributes_All de l'Objet de validation de sécurité

ID d'attribut	Nombre d'octets	Nom	Type de données
1	0	Etat de l'Objet de validation de sécurité	USINT
2	1	Type d'Objet de validation de sécurité	USINT
3	2,3	Multiplicateur EPI d'intervalles Ping	UINT
4	variable	Multiplicateur minimal de messages de coordination temporelle	STRUCT
5	variable	Délai du réseau	STRUCT
6	variable	Multiplicateur de temporisation	STRUCT
7	variable	Nombre maximal de consommateurs	USINT
8	variable	Instance de connexion de données	UINT = 0 si non pris en charge
9	variable	Instance de connexion de coordination	UINT = 0 si non pris en charge
10	variable	Instance de connexion de correction	STRUCT
11	variable	Rattachement CCO	UINT = 0 si non pris en charge
12	variable	Age maximal des données	UINT
13	variable	Chemin d'application	EPATH compact
14		Code d'erreur	UINT

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

6.7.6 Comportement d'objet

6.7.6.1 Diagramme de transitions d'état

Le comportement de l'Objet de validation de sécurité est représenté à la Figure 16 et dans le Tableau 66.

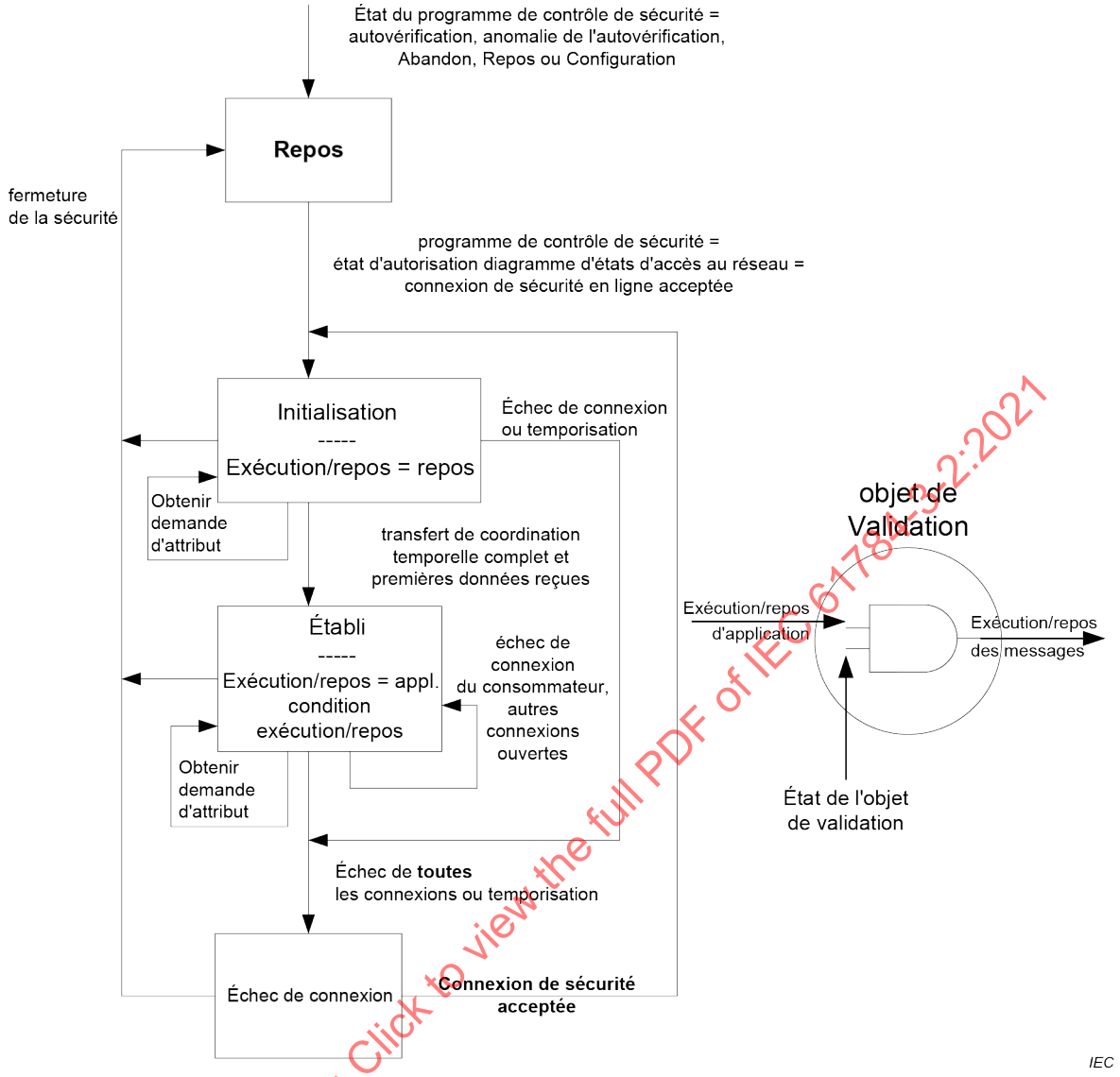


Figure 16 – Diagramme de transitions d'état de l'Objet de validation de sécurité

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

6.7.6.2 REPOS

L'état Repos est l'état initial saisi après la mise sous tension/l'autovérification. Cet état correspond à l'état normal en l'absence d'ouverture ou d'échec de connexions.

6.7.6.3 Initialisation

Pour les producteurs multipoints, cet état est effectif pour chaque connexion de consommateur traitée par le producteur. Pour les producteurs point à point et l'ensemble des consommateurs, cet état se rapporte à la connexion Objet de validation de sécurité complète.

6.7.6.4 Etabli

Pour les producteurs multipoints, cet état est effectif pour chaque connexion de consommateur traitée par le producteur. Pour les producteurs point à point et l'ensemble des consommateurs, cet état se rapporte à la connexion Objet de validation de sécurité complète.

6.7.6.5 Connection_Failed

Cet état est actif lorsque toutes les connexions associées à l'Objet de validation de sécurité ont échoué. Cet état peut perdurer jusqu'à réception d'un SafetyClose, ou jusqu'au rétablissement de la connexion à partir d'un point d'origine concordant (c'est-à-dire que l'OUNID et le chemin d'application correspondent à une ressource de connexion).

6.7.6.6 Matrice d'événements d'état

Le Tableau 66 présente la matrice d'événements d'état qui définit le comportement de l'Objet de validation de sécurité. Le Tableau 67 associe par mapping les états de l'Objet de validation de sécurité et ceux du Programme de contrôle de sécurité.

Tableau 66 – Matrice d'événements d'état de l'Objet de validation de sécurité

Evénement	Etat			
	Repos	Initialisation	Exécution	Echec de connexion
Alimentation appliquée et autovérification effectuée	Etat initial	--	--	
Programme de contrôle de sécurité = état d'autorisation, Diagramme d'états d'accès au réseau = en ligne, Nouvelle connexion de sécurité demandée	Demande de validation et Transition vers l'état Initialisation	Si producteur multipoint, Initialisation de la connexion de sécurité	Si producteur multipoint, initialisation de la connexion de sécurité	Mapping de l'OUNID et du chemin d'application, Si concordance, transition vers l'état Initialisation
Transfert de coordination temporelle achevé	--	Transition vers l'état Exécution	Si producteur multipoint, Nouveau consommateur en ligne	--
Echec du consommateur dans un producteur multipoint tandis que d'autres consommateurs sont toujours en ligne	--	LED d'état du réseau rouge clignotant	LED d'état du réseau rouge clignotant	--
Echec de toutes les connexions	--	Echec de la transition vers l'état Connexion	Echec de la transition vers l'état Connexion	LED d'état du réseau rouge clignotant
Mapping de la demande de connexion du consommateur (c'est-à-dire que l'OUNID et le chemin d'application correspondent à une connexion de consommateur non aboutie)	--	Transition du consommateur vers l'état Initialisation	Transition du consommateur vers l'état Initialisation	Transition vers l'état Initialisation
Réception de SafetyClose	Réponse satisfaisante, maintien dans l'état Repos	Réponse satisfaisante, Transition vers l'état Repos	Réponse satisfaisante, Transition vers l'état Repos	Réponse satisfaisante, Transition vers l'état Repos

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Tableau 67 – Mapping des états entre le Programme de contrôle de sécurité et l'Objet de validation de sécurité

Programme de contrôle de sécurité	Objet de validation de sécurité
Autovérification	Repos
Exception d'autovérification	Repos
Attente du TUNID	Repos
Repos	Repos[a], Initialisation, Exécution, ou Connection_Failed
Configuration	Repos
Exécution	Repos[a], Initialisation ou Exécution, ou Connection_Failed
Abandon	Repos
Anomalie critique	Repos

[a] Un Objet de validation de sécurité ne doit accepter des connexions que lorsque le Programme de contrôle de sécurité est dans un état qui peut accepter les connexions dépendant de l'appareil (c'est-à-dire l'état Exécution uniquement ou Exécution/Repos). Un Objet de validation de sécurité peut être au repos tandis qu'un autre est toujours actif.

6.8 Connection Configuration Object (Objet de configuration de connexion)

6.8.1 Généralités

Le présent 6.8 définit les extensions de l'objet Configuration de connexion, de classe $F3_{hex}$ pour le FSCP 2/1. Voir l'IEC 61158-4-2 pour une définition complète.

Code de classe: F3hex

6.8.2 Extensions des attributs de classe

Les attributs de classe destinés à être utilisés par les appareils FSCP 2/1 sont définis dans le Tableau 68.

Tableau 68 – Extensions des attributs de classe de l'objet Configuration de connexion

ID d'attribut	Mise en œuvre nécessaire	Règle d'accès	Nom	Type de données	Description de l'attribut
9	Conditionnel[a]	Définir	Signature de modification	UDINT	Créé et utilisé par le logiciel de configuration pour détecter les modifications apportées aux valeurs d'attributs instance

[a] Cet attribut n'est exigé qu'avec les appareils qui n'utilisent pas l'interface SNCT de sécurité.

6.8.3 Attributs instance, ajouts et extensions

Le Tableau 69 définit les attributs instance et les modifications destinés à être utilisés par les appareils FSCP 2/1.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Tableau 69 – Ajouts/extensions d'attributs instance de l'objet Configuration de connexion

ID d'attribut	Mise en œuvre nécessaire	Règle d'accès	NV	Nom	Type de données	Description de l'attribut	Sémantique de la valeur
9	Exigé	Définir	NV	Mapping des données	STRUCT de:		
				format_number	UINT	Ce numéro détermine le format de mapping utilisé	2 – 99 Réservé 100 – 199 Spécifiques au fournisseur. Toutes les autres valeurs sont réservées
				Data_Map data_size	UINT	Taille, en octets, des informations de mapping	
				Data_Map_data	Matrice d'octets	Données de format de mapping des données fondées sur le numéro de format	
10	Facultatif	Définir	NV	Config #2 Data2	STRUCT de:		
				config_data_size	UINT	Longueur de config_data en octets	
				config_data	Matrice d'octets	Données de la configuration n° 2	
11	Facultatif	Définir	NV	ID d'appareil du proxy	STRUCT de:		
				vendor_id	UINT	ID du fournisseur	
				product_type	UINT	Type d'appareil	
				product_code	UINT	Code produit	
				major_rev	USINT	Révision principale	
				minor_rev	USINT	Révision secondaire	
12	Conditionnel[a]	Définir	NV	Désactivation de connexion	BOOL		0 – connexion activée. 1 – connexion désactivée. En cas de réception d'un service Ouverture, cette valeur doit être définie sur 0. En cas de réception d'un service Fermeture ou Arrêt, cette valeur doit être définie sur 1

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

ID d'attribut	Mise en œuvre nécessaire	Règle d'accès	NV	Nom	Type de données	Description de l'attribut	Sémantique de la valeur
13	Conditionnel[a]	Définir	NV	Paramètres de sécurité	STRUCT de:		
				Réservé	USINT	Réservé	Doit être égal à zéro
				Réservé	USINT	Réservé	Doit être égal à zéro
				CRC de configuration	UDINT	CRC-S4 qui porte sur les données de configuration de l'appareil cible dans les attributs 7 et 10	Cette valeur est calculée par le logiciel de configuration sur la base des données des attributs 7 et 10 après application de la configuration
				Signature de configuration	DATE ET HEURE		
				EPI de correction de temps	UDINT		
				Paramètres de connexion de correction de temps	WORD		
				Target UNID (UNID cible)	10 octets		UNID de l'appareil cible
				Espace réservé pour l'UNID du point d'origine	10 octets	Tous les zéros	Permet à FW de remplir facilement l'OUNID dans le segment de sécurité
				Multiplicateur EPI d'intervalles Ping	UINT		
				Multiplicateur minimal de messages de coordination temporelle	UINT		
				Multiplicateur de délai du réseau	UINT		
				Multiplicateur de temporisation	USINT		
				Nombre maximal de consommateurs	USINT		
14	Conditionnel[a]	Obtenir	NV	CRC de paramètre de connexion	UDINT	CRC-S4 qui porte sur les paramètres de connexion utilisés dans un service SafetyOpen	Cette valeur est calculée par cet appareil une seule fois, lorsque la configuration est appliquée. Elle doit pouvoir être lue par le logiciel de configuration

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

ID d'attribut	Mise en œuvre nécessaire	Règle d'accès	NV	Nom	Type de données	Description de l'attribut	Sémantique de la valeur
15	Conditionnel[a]	Définir	NV	Instance de configuration	UINT	Objet configuré pour ce nœud	= 0 lorsqu'aucun objet n'est attribué
16	Conditionnel[a]	Définir	NV	Attribution d'ID	BOOL	Lorsque supprimé, le point d'origine attribue les ID de réseau pour les connexions qu'il a produites	0: attribution de l'ID pour les connexions produites (par défaut) 1: sollicitation de la cible concernant les ID produits
17	Conditionnel[a]	Obtenir		Numéro de série de connexion cible	UINT	Numéro instance de l'Objet de validation de sécurité de la cible. Renvoi du Numéro de série de connexion de cible au cours de l'établissement de la connexion. Lecture par les outils de diagnostic	0 lorsque la connexion n'est pas établie
20	Conditionnel[b]	Définir	NV	Type de format	USINT	Définit le format à utiliser pour la connexion avec une cible	0 = Auto (par défaut) 1 = "De base" 2 = "Etendu"
21	Conditionnel[b]	Obtenir	NV	Etat du format	USINT	Indique le format actuellement utilisé lorsque le type de format est Auto (ou lorsqu'aucun accord sur un format n'a pu être obtenu)	0 = Auto 1 = "De base" 2 = "Etendu" 0xFF = "détection de conflit"
22	Conditionnel[b]	Définir	NV	Nombre maximal d'anomalies	UINT	Nombre de paquets erronés sur une période d'une heure à l'issue de laquelle une connexion est fermée. Utilisé par les producteurs et les consommateurs.	Par défaut = 5 Une valeur de 0 indique que les connexions doivent être fermées dès qu'une erreur est détectée

[a] Cet attribut est exigé pour un appareil qui prend en charge les connexions de sécurité; il est facultatif dans les autres cas.

[b] Cet attribut est exigé pour un appareil qui prend en charge le format étendu; il est facultatif dans les autres cas.

6.8.4 Extensions ou restrictions de sémantique des attributs instance pour des raisons de sécurité

6.8.4.1 Drapeaux de connexion – (Attribut 2)

Les drapeaux de connexion sont définis dans le Tableau 70.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Tableau 70 – Définition des bits de drapeaux de connexion

Bits	Définition pour les appareils de sécurité
Bit 0:	Direction de connexion Toujours 0 = Point d'origine de la connexion
Bits 1-3:	Format de transfert en temps réel O-to-T Toujours 101 = Format de sécurité
Bits 4-6:	Format de transfert en temps réel T-to-O Toujours 101 = Format de sécurité
Bits 7-15:	Non utilisé. Toujours 0
Valeur:	$005A_{hex}$ = Point d'origine $005B_{hex}$ = Cible

6.8.4.2 Indice de données CS – (attribut 4)

L'indice de données CS n'est pas utilisé; il doit être égal à FFFF $FFFF_{hex}$.

6.8.4.3 Multiplicateur de temporisation de connexion – (partie de l'attribut 5)

Le producteur et le consommateur utilisent le multiplicateur de temporisation de connexion afin de temporiser les 3 connexions normalisées. Le multiplicateur est utilisé par le consommateur de la connexion pour déterminer s'il est nécessaire de temporiser la connexion.

La valeur de temporisation de la connexion est définie comme suit:

RPI de connexion × (CTM + 1) × 4

Plage: 0 à 7

où

0 = (0x4);

1 = (0x8);

2 = (0x12);

3 = (0x16);

4 = (0x20);

5 = (0x24);

6 = (0x28);

7 = (0x32).

Valeur: Toujours 1 (x8)

6.8.4.4 Classe de transport et déclencheur – (partie de l'attribut 5)

La valeur de la classe de transport et du déclencheur pour la sécurité est de 20_{hex} pour une connexion d'entrée ou de $A0_{hex}$ pour une connexion de sortie.

6.8.4.5 RPI O-to-T – (partie de l'attribut 5)

Si la direction est 0 (Client/T-to-O), il s'agit du RPI de la coordination temporelle et le RPI T6to-O est le RPI de production des données.

Si la direction est 1 (Serveur/O-to-T), il s'agit du RPI de production des données et le RPI T6to-O est le RPI de coordination temporelle.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Le RPI de coordination temporelle est défini comme suit:

Plage: 100 µs à 100 000 000 µs

Multiplicateur EPI d'intervalles Ping × RPI de production de données

RPI de production de données

Plage: 100 µs à 1 000 000 µs

6.8.4.6 Paramètres de connexion O-to-T – (partie de l'attribut 5)

Les paramètres de connexion O-to-T sont définis dans le Tableau 71.

Tableau 71 – Paramètres de connexion O-to-T

Bits	Paramètre	Valeur
0-8	Taille de connexion (en octets)	Si la direction est 1 (Serveur/O-to-T), il s'agit de la taille du message de sécurité: Si la taille des données est de 1 à 2 octets: Taille des données d'application + 6 Si la taille des données est de 3 à 250 octets: (Taille des données d'application × 2) + 8 Si la direction est 0 (Client/T-to-O), il s'agit de la taille du message de coordination temporelle (6 octets) Plage: 7-510
9	Fixe/Variable	Toujours 0 (Fixe)
10-11	Priorité	Toujours 01 (Elevée)
12	Réservé	Toujours 0
13-14	Type de connexion	Toujours 10 (Point à point)
15	Propriétaire redondant	Toujours 0 (la sécurité ne prend pas en charge la redondance)

6.8.4.7 RPI T-to-O – (partie de l'attribut 5)

Si la direction est 0 (Client/T-to-O), il s'agit du RPI de la production des données et le RPI O-to-T est le RPI de coordination temporelle.

Si la direction est 1 (Serveur/O-to-T), il s'agit du RPI de coordination temporelle et le RPI O-to-T est le RPI de production des données.

Valeur: voir RPI O-to-T.

6.8.4.8 Paramètres de connexion T-to-O – (partie de l'attribut 5)

Les paramètres de connexion T-to-O sont définis dans le Tableau 72.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Tableau 72 – Paramètres de connexion T-to-O

Bits	Paramètre	Valeur
0-8	Taille de connexion (en octets)	Si la direction est 0 (Client/T-to-O), il s'agit de la taille du message de sécurité. Pour une connexion point à point, voir les paramètres de connexion O-to-T. Pour les connexions multipoints avec une taille de données de 1 à 2 octets: Taille des données d'application + 12 Pour les connexions multipoints avec une taille de données de 3 à 248 octets: (Taille des données d'application × 2) + 14 Les calculs de connexions multipoints doivent inclure la section de correction de temps. Ceci est exigé pour toutes les connexions multipoints afin de s'assurer du calcul correct du CPCRC dans le service SafetyOpen. La valeur est déterminée par l'appareil cible. Si la direction est 1 (Serveur/O-to-T), il s'agit de la taille du message de coordination temporelle (6 octets). Plage: 7-508
9	Fixe/Variable	Toujours 0 (Fixe)
10-11	Priorité	Toujours 01 (Elevée)
12	Réservé	Toujours 0
13-14	Type de connexion	01 (Multipoint) 10 (Point à point) Valeur par défaut: 10 (Point à point)
15	Propriétaire redondant	Toujours 0 (la sécurité ne prend pas en charge la redondance)

6.8.4.9 Chemin de connexion (attribut 6)

6.8.4.9.1 Taille du chemin de connexion

Il s'agit du nombre de mots à 16 bits archivés dans le Chemin de connexion. Ce chemin doit être ajusté afin de retirer la taille des éléments de chemin du pont lors du calcul du CPCRC (c'est-à-dire que la taille utilisée pour le calcul doit être la valeur que la cible pourra observer lorsque le ou les ponts auront retiré leurs segments et ajusté cette taille de manière appropriée).

6.8.4.9.2 Chemin de connexion

Les chemins de connexion sont associés à la connexion dans l'ordre suivant: (1) Chemin de Pont, (2) Chemin de configuration, (3) Chemin de consommation et (4) Chemin de production.

Le chemin de pont (1) doit être séparé, par le point d'origine, des chemins d'application 2, 3 et 4 au moment de la constitution du service SafetyOpen et lors du calcul du CPCRC.

6.8.4.9.3 Chemin de pont

Chemin valide construit pour le parcours entre le point d'origine et la cible.

6.8.4.9.4 Chemin de configuration

Le chemin est valide si l'attribut 7 ou 8 comporte des données de configuration, ce chemin étant nul dans les autres cas. Le chemin provient dans tous les cas de l'applet cible (c'est-à-dire le fichier EDS).

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

6.8.4.9.5 Chemin de consommation cible

Le chemin est valide s'il s'agit de la direction 1 (Serveur/O-to-T) ou est nul dans les autres cas. Le chemin provient dans tous les cas de l'applet cible (c'est-à-dire le fichier EDS).

6.8.4.9.6 Chemin de production cible

Le chemin est valide s'il s'agit de la direction 0 (Client/T-to-O) ou est nul dans les autres cas. Le chemin provient dans tous les cas de l'applet cible (c'est-à-dire le fichier EDS).

6.8.4.10 Taille des données de configuration nº 1 (partie de l'attribut 7)

Son utilisation est facultative pour la sécurité, la taille des données étant nulle en cas de non-utilisation.

6.8.4.11 Données de configuration nº 1 (partie de l'attribut 7)

Son utilisation est facultative pour la sécurité, et doit par ailleurs être concaténée avec le contenu des données de configuration nº 2.

6.8.4.12 Taille des données de configuration nº 2 (partie de l'attribut 10)

Nombre d'octets stockés dans les données de configuration nº 2 (ci-dessous).

Plage: 1 à < Taille de configuration maximale admissible>

6.8.4.13 Données de configuration nº 2 (partie de l'attribut 10)

Utilisées pour stocker les données de configuration de l'appareil cible.

6.8.4.14 Mapping des données (attribut 9)

6.8.4.14.1 Attribution de format de mapping

Le Tableau 73 définit un ensemble de formats de mapping actuellement définis dans la plage normalisée. La plage spécifique au fournisseur est toujours disponible pour être utilisée pour des formats de mapping spéciaux.

Tableau 73 – Formats de mapping des données

Numéro de format	Nom de format	Taille S des données de mapping des données (en octets)	Données de mapping des données	Commentaire
0	Format de scrutation ouvert	4 octets	Voir Tableau 74	Format simple qui associe par mapping les données sous forme de granularité de mots dans les tableaux d'images d'entrée et de sortie
1	Format de scrutation à index d'octet	4 octets	Voir Tableau 75	Format simple qui associe par mapping les données sous forme de granularité d'octets dans les tableaux d'images d'entrée et de sortie
2-99	Réservé			
100-199	Spécifique au fournisseur			
200 – 65 535	Réservé			

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

6.8.4.14.2 Utilisation du format 0 pour les scrutateurs de sécurité

Le format 0 de mapping des données contient la structure des données de mapping qui utilise le format décrit dans le type de format de mapping, défini dans le Tableau 74.

Tableau 74 – Format 0 de mapping des données

Nom	Type de données	Description	Valeur
Décalage des images de données du point d'origine à la cible	UINT	Décalage, en unités de 16 bits, dans le tableau d'images du point d'origine à la cible	Si la direction est 0 (Client/T-to-O): Toujours 0. Si la direction est 1 (Serveur/O-to-T): Décalage de mots dans le tableau des données de sortie de sécurité
Décalage des images de données de la cible au point d'origine	UINT	Décalage, en unités de 16 bits, dans le tableau d'images de la cible au point d'origine	Si la direction est 0 (Client/T-to-O): Décalage de mots dans le tableau des données d'entrée de sécurité Si la direction est 1 (Serveur/O-to-T): Toujours 0

6.8.4.14.3 Utilisation du format 1 pour les scrutateurs de sécurité

Le format 1 de mapping des données contient la structure des données de mapping qui utilise le format décrit dans le type de format de mapping, défini dans le Tableau 75.

Tableau 75 – Format 1 de mapping des données

Nom	Type de données	Description	Valeur
Décalage des images de données du point d'origine à la cible	UINT	Décalage, en unités de 8 bits, dans le tableau d'images du point d'origine à la cible	Si la direction est 0 (Client/T-to-O): Toujours 0. Si la direction est 1 (Serveur/O-to-T): Décalage d'octets dans le tableau des données de sortie de sécurité
Décalage des images de données de la cible au point d'origine	UINT	Décalage, en unités de 8 bits, dans le tableau d'images de la cible au point d'origine	Si la direction est 0 (Client/T-to-O): Décalage d'octets dans le tableau des données d'entrée de sécurité. Si la direction est 1 (Serveur/O-to-T): Toujours 0

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

6.8.4.15 ID d'appareil du proxy

N'est jamais utilisé.

6.8.4.16 Désactivation de connexion (attribut 12)

Lorsque l'attribut Désactivation de connexion dans l'objet CCO est TRUE, la connexion doit rester désactivée tout au long des cycles d'alimentation. Lorsque l'attribut Désactivation de connexion dans l'objet CCO est FALSE, la connexion doit rester activée tout au long des cycles d'alimentation.

6.8.5 Paramètres spéciaux relatifs à la sécurité – (attribut 13)

6.8.5.1 Multiplicateur EPI d'intervalles Ping

Cet attribut est utilisé comme partie intégrante de la fonction Objet de validation de sécurité. Ce paramètre fait partie intégrante des paramètres du Segment de sécurité de la fonction SafetyOpen. Ping_Interval_EPI_Multiplier est le nombre qui définit le Ping_Count_Interval pour la connexion de sécurité.

Les appareils qui mettent en œuvre les extensions de sécurité de l'objet CCO doivent effectuer un contrôle des plages qui porte sur le multiplicateur EPI d'intervalles Ping au cours d'une demande Validate_Configuration.

L'emploi du multiplicateur EPI d'intervalles Ping est défini comme suit:

Plage: [Max_Consumer_Number × Timeout_Multiplier.PI + 15] à 1 000.

Valeur par défaut:

Si la direction est 0 (Client/T-to-O): 100

Si la direction est 1 (Serveur/O-to-T): 19

6.8.5.2 Multiplicateur minimal de messages de coordination temporelle

Cet attribut est utilisé comme partie intégrante de la fonction Objet de validation de sécurité. Ce paramètre provient des paramètres du Segment de sécurité de la fonction SafetyOpen. Le Time_Coord_Msg_Min_Multiplier est le nombre minimal d'incréments de 128 µs susceptibles d'être utilisés pour transmettre un message de coordination temporelle du consommateur au producteur. La valeur par défaut est 0.

Les appareils qui mettent en œuvre les extensions de sécurité de l'objet CCO doivent effectuer un contrôle des plages qui porte sur le Time_Coord_Msg_Min_Mulitiplier au cours d'une demande Validate_Configuration.

L'emploi du multiplicateur minimal de messages de coordination temporelle est défini comme suit:

Plage: 0 à 7 813, ce qui équivaut à 0 s à 1 s.

Valeur par défaut: 2 en l'absence de pont; 3 ou plus avec ajout d'un pontage.

6.8.5.3 Multiplicateur de délai du réseau

Cet attribut est utilisé comme partie intégrante de la fonction Objet de validation de sécurité. Ce paramètre fait partie intégrante des paramètres du Segment de sécurité de la fonction SafetyOpen. Network_Time_Expectation_Multiplier est le nombre maximal d'incréments de 128 µs qu'un consommateur doit permettre à l'âge des données de sécurité d'atteindre.

Les appareils qui mettent en œuvre les extensions de sécurité de l'objet CCO doivent effectuer un contrôle des plages qui porte sur le Network_Time_Expectation_Multiplier au cours d'une demande Validate_Configuration.

L'emploi du multiplicateur de délai du réseau est défini comme suit:

Plage 0 à 45 313, ce qui équivaut à 0 s à 5,8 s.

Equation Voir détails en 8.8.4.

6.8.5.4 Multiplicateur de temporisation

Cet attribut est utilisé comme partie intégrante de la fonction Objet de validation de sécurité. Ce paramètre fait partie intégrante des paramètres du Segment de sécurité de la fonction SafetyOpen.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Les appareils qui mettent en œuvre les extensions de sécurité de l'objet CCO doivent effectuer un contrôle des plages qui porte sur le Timeout_Multiplier au cours d'une demande Validate_Configuration.

L'emploi du multiplicateur de temporisation est défini comme suit:

Format de base de plage	1 à 4
Format étendu de plage	1 à 255
Valeur par défaut	2

6.8.5.5 Nombre maximal de consommateurs

Cet attribut définit le nombre maximal de consommateurs qui sont autorisés à se connecter à un producteur multipoint (type 2). Il est nécessaire que les consommateurs et producteurs multipoints connaissent tous deux cette valeur pour fonctionner correctement. Cet attribut est utilisé comme partie intégrante de la fonction Objet de validation de sécurité. Ce paramètre fait partie intégrante des paramètres du Segment de sécurité de la fonction SafetyOpen.

Les appareils qui mettent en œuvre les extensions de sécurité de l'objet CCO doivent effectuer un contrôle des plages qui porte sur le Nombre max. de consommateurs au cours d'une demande Validate_Configuration.

L'emploi du nombre maximal de consommateurs est défini comme suit:

Plage:	1 à 15
Valeur par défaut:	15
Valeur:	est issue de l'applet cible (c'est-à-dire le fichier EDS).

6.8.5.6 UNID de connexion cible

Cet attribut constitue l'UNID de l'appareil de sécurité cible pour cette connexion. Ce paramètre fait partie intégrante des paramètres du segment de sécurité de la fonction SafetyOpen. Il est vérifié par l'appareil cible afin de confirmer que la demande n'a pas fait l'objet d'un mauvais acheminement. L'essai de la connexion par l'utilisateur constitue la seule méthode qui permet de confirmer que cette valeur est correcte.

Le format UNID cible avec le CP 2/3 est défini comme suit:

OCTET 0-5:	Safety Network Number (Numéro de réseau de sécurité)
OCTET 6:	MACID du CP 2/3
OCTET 7-9:	Toujours 0 pour le CP 2/3

6.8.5.7 CRC de configuration de sécurité (SCCRC)

Le SCCRC est utilisé comme signature de la configuration de l'appareil et peut servir à confirmer l'intégrité de la configuration dans la durée. Le logiciel de configuration doit calculer le SCCRC sur les données de configuration dans leur ordre exact d'apparition dans le message SafetyOpen. Le même calcul est effectué par les appareils cibles et comparé avec cette valeur.

Le SCCRC doit être calculé sur les données de configuration par l'appareil, à chaque validation de la configuration de ce dernier (c'est-à-dire Demande Validate_Configuration au Programme de contrôle de sécurité ou connexion de sécurité de type 1).

Le SCCRC doit être archivé dans la mémoire non volatile avec les autres attributs NV à chaque application d'une configuration (c'est-à-dire demande d'application au Programme de contrôle de sécurité).

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Le manuel de sécurité doit indiquer à l'utilisateur de soumettre à l'essai les configurations de connexion de sécurité après leur application à un point d'origine, afin de confirmer que la connexion cible fonctionne tel que prévu.

L'utilisation du SCCRC de l'appareil cible est présentée dans le Tableau 76.

Tableau 76 – Valeurs SCCRC de l'appareil cible

Type de connexion de sécurité	Valeur SCCRC
Type 1	SCCRC qui identifie les données de configuration dans les données de configuration n° 2
Type 2a	SCCRC qui identifie la configuration prévue de l'appareil cible
Type 2b	0

6.8.5.8 Signature de configuration de sécurité (Datation)

Les valeurs SCTS de l'appareil cible sont présentées dans le Tableau 77.

Tableau 77 – Valeurs SCTS de l'appareil cible

Type de connexion de sécurité	Valeur SCTS
Type 1	SCTS qui identifie les données de configuration dans les données de configuration n° 1
Type 2a	SCTS qui identifie la configuration prévue de l'appareil cible
Type 2b	0

6.8.5.9 EPI de correction de temps

Ce paramètre définit l'EPI du message de correction de temps utilisé dans une connexion multipoint.

La valeur d'une connexion multipoint est la suivante:

Multiplicateur EPI d'intervalles Ping × RPI de production de données.

Dans les autres cas, la valeur est 0.

6.8.5.10 Paramètres de connexion de correction de temps

Définit les paramètres de connexion utilisés dans le message de correction de temps d'une connexion multipoint.

La valeur est 0000_{hex} pour une connexion non multipoint ou 2406_{hex} pour une connexion multipoint, comme défini dans le Tableau 78.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Tableau 78 – Paramètres de connexion de correction de temps pour une connexion multipoint

Bits	Paramètre	Valeur
0-8	Taille de connexion (en octets)	Taille du message de correction de temps de 6 octets
9	Fixe/Variable	Toujours 0 (Fixe)
10-11	Priorité	Toujours 01 (Elevée)
12	Réservé	Toujours 0
13-14	Type de connexion	01 (Multipoint)
15	Propriétaire redondant	Toujours 0 (la sécurité ne prend pas en charge la redondance)

6.8.5.11 CRC des paramètres de connexion (CPCRC) – (attribut 14)

L'attribut CRC des paramètres de connexion doit être calculé par cet appareil d'origine à chaque validation de la configuration du point d'origine (c'est-à-dire Demande Validate_Configuration au programme de contrôle de sécurité).

Le CPCRC doit être archivé dans la mémoire non volatile avec les autres attributs NV à chaque application d'une configuration (c'est-à-dire demande d'application au Programme de contrôle de sécurité).

Il convient d'exiger de l'utilisateur qu'il soumette à l'essai cette connexion, après son application, afin de confirmer la configuration de connexion. A partir de là, le CPCRC est utilisé comme signature de cette configuration de connexion et peut servir à confirmer l'intégrité de la configuration dans la durée. Le calcul proprement dit est effectué avec les paramètres de connexion de la fonction SafetyOpen dans l'ordre exact de leur apparition dans le message. Le même calcul est effectué par les appareils cibles et comparé avec cette valeur: l'ordre exact doit donc être respecté.

6.8.5.12 Instance de configuration – (attribut 15)

Cet attribut assure la liaison avec l'instance de l'objet attribué à cette connexion. L'attribut peut être utilisé lorsque la fonction SafetyOpen ne permet pas de transmettre les données de configuration de la cible. Une valeur de 0 (valeur par défaut) pour cet attribut indique l'absence d'attribution d'objet.

6.8.5.13 Attribution d'ID

Cet attribut booléen permet d'accorder à l'utilisateur une certaine souplesse concernant la méthode d'attribution d'identifiants par les points d'origine à l'établissement d'une connexion. Ceci est particulièrement important pour le FSCP 2/1 sur le CP 2/3. Le comportement par défaut du point d'origine consiste à fournir des identifiants aux connexions dans lesquelles il est le producteur. Si l'utilisateur définit cet attribut, le point d'origine demande en revanche à la cible de fournir un identifiant à ces connexions générées. Un utilisateur peut souhaiter effectuer cette opération lorsque le point d'origine comporte un grand nombre de connexions, mais ne comporte pas un nombre suffisant d'éléments pour procéder à l'application. Cet attribut s'applique uniquement aux productions non multipoints (ces dernières doivent toujours être attribuées par le producteur). Cette fonction étant considérée comme une fonction avancée, il convient de la présenter à un utilisateur avec la plus grande attention. Il doit être recommandé à l'utilisateur qu'il convient d'utiliser cette fonction uniquement dans des scénarios d'application limités où une répétabilité de connexion peut être assurée.

6.8.5.14 Type de format

Le Tableau 79 définit la signification de l'attribut Type de format.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Tableau 79 – Signification de l'attribut Type de format

Nom de valeur du type de format	Signification
Auto	Le point d'origine détermine le format à utiliser pour l'établissement de la première connexion
De base	Le point d'origine utilise le format existant pour l'établissement de la connexion suivante
Etendue	Le point d'origine utilise le format étendu pour l'établissement de la connexion suivante

Si la valeur "Auto" n'est pas définie comme la valeur par défaut de l'attribut Type de format, le point d'origine détermine le format à utiliser. Si la valeur "De base" est la valeur de configuration facultative de l'attribut Type de format, le point d'origine utilise uniquement le format "De base". Si la valeur "Etendu" est la valeur de configuration facultative de l'attribut Type de format, le point d'origine utilise uniquement le format "Etendu".

L'attribut Etat du format doit être défini sur la valeur 0xFF (Détection de conflit) si le type de format est "De base" ou "Etendu" et si une cible répond par une erreur "Format de connexion de sécurité invalide" (0x01, 0x803) ou une erreur "Taille de connexion de sécurité invalide" (0x01, 0x802).

L'attribut Type de format ne peut pas être modifié lorsque la connexion est active. Lorsque le format est réglé sur "Auto", la logique suivante représentée à la Figure 17 doit être utilisée:

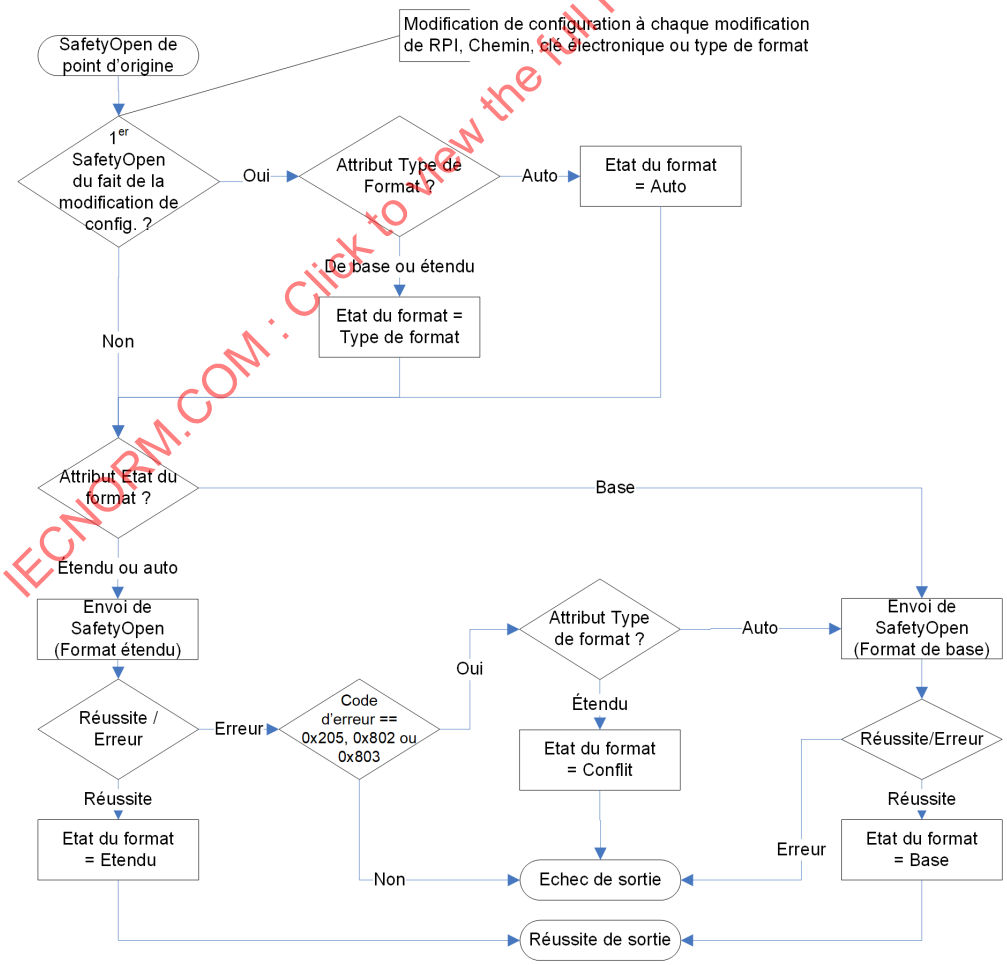


Figure 17 – Logique pour le type de format Autodétection

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

6.8.5.15 Etat du format

Le Tableau 80 définit la signification de l'attribut Etat du format.

Tableau 80 – Signification de l'attribut Etat du format

Nom de valeur de l'état du format	Signification du point d'origine	Signification de la cible
Auto	Le point d'origine n'a pas encore déterminé le type de format à utiliser	NA
"De base"	Si le type de format est "Auto" Le point d'origine a déterminé que la cible exige un ancien format Si le type de format est "De base" Le point d'origine se connecte uniquement avec l'ancien format Si le type de format est "Etendu" Il convient que cette condition ne se produise jamais	La cible utilise le format "De base"
"Etendu"	Si le type de format est "Auto" Le point d'origine a déterminé que la cible accepte un nouveau format Si le type de format est "De base" Il convient que la condition ne se produise jamais Si le type de format est "Etendu" Le point d'origine se connecte uniquement avec le nouveau format	La cible utilise le format "Etendu"
"Détection de conflit"	Si le type de format est "De base" ou "Etendu" et en cas de réception d'erreurs de type de segment, il existe un conflit de paramétrage entre la cible et le point d'origine. Cet état identifie cette condition par un drapeau	La cible reçoit des demandes SafetyOpen pour un format qu'elle ne prend pas en charge

6.8.6 Services spécifiques à l'objet

L'objet Configuration de connexion fournit les services spécifiques à l'objet suivants, définis dans le Tableau 81.

Tableau 81 – Services spécifiques à l'objet Configuration de connexion

Service	Mise en œuvre nécessaire		Nom du service	Description du service
	Classe	Instance		
$4B_{hex}$	Conditionnel[a]	N/A	Stimulateur de temporisateur	Stimule l'édition du temporisateur de chien de garde
$4C_{hex}$	Facultatif	Conditionnel[b]	Ouverture	Ouvre les connexions
$4D_{hex}$	Facultatif	Conditionnel[b]	Fermeture	Ferme les connexions
$4E_{hex}$	Facultatif	Conditionnel[b]	Arrêt	Interrompt les connexions
$4F_{hex}$	Conditionnel[a]	N/A	Modification démarrage	Gère l'édition de sessions
50_{hex}	Exigé	N/A	Obtenir état	Obtient l'état pour des connexions multiples
51_{hex}	Conditionnel[a]	N/A	Modification achevée	Achève l'édition de sessions
52_{hex}	Conditionnel[a]	N/A	Vérification des modifications	Vérifie les modifications en attente

[a] Les appareils de sécurité ne doivent pas mettre en œuvre ces services, dans la mesure où l'outil de configuration logicielle coordonne la configuration par l'intermédiaire du Programme de contrôle de sécurité.

[b] Les appareils de sécurité doivent prendre en charge les services Ouverture, Fermeture et Arrêt. Ces services ne doivent être acceptés qu'en cas de déverrouillage de l'appareil. Si l'appareil est verrouillé, il doit répondre par une erreur "Conflit d'état de l'appareil".

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

6.8.7 Extensions des services communs pour la sécurité

6.8.7.1 Get_Attribute_All (Code de service 01_{hex})

Les attributs ajoutés à la fin de la réponse Get_Attribute_All sont définis dans le Tableau 82 et le Tableau 83. Tous les autres paramètres de ce service sont définis dans l'objet CCO normalisé dans l'IEC 61158-5-2 et l'IEC 61158-6-2.

Tableau 82 – Données du service de réponse Get_Attributes_All (attributs ajoutés)

Nom	Type de données	Description
Paramètres de sécurité	STRUCT de:	
	USINT	Remplissage, défini sur zéro
	USINT	Remplissage, défini sur zéro
	UDINT	CRC de configuration (SCCRC)
	DATE ET HEURE	Datation de configuration (SCTS)
	UDINT	EPI de correction de temps
	WORD	Paramètres de connexion de correction de temps
	10 octets	Target UNID (UNID cible)
	10 octets	Remplissage, défini sur zéro
	UINT	Multiplicateur EPI d'intervalles Ping
	UINT	Multiplicateur minimal de messages de coordination temporelle
	UINT	Multiplicateur de délai du réseau
	USINT	Multiplicateur de temporisation
	USINT	Nombre maximal de consommateurs
CRC de paramètre de connexion	UDINT	CRC-32 qui porte sur les paramètres de connexion utilisés dans un service SafetyOpen
Instance de configuration	UINT	
Drapeau d'attribution d'ID	BOOL	
Numéro de série de connexion cible	UINT	Instance d'Objet de validation de sécurité renvoyée par la cible lors de l'établissement de la connexion

Tableau 83 – Données du service de réponse Get_Attributes_All (paramètres ajoutés)

Nom	Type de données	Description
Longueur	USINT	Longueur des paramètres de sécurité supplémentaires = 4
Type de format	USINT	
Etat du format	USINT	
Nombre maximal d'anomalies	UINT	

6.8.7.2 Set_Attribute_All (Code de service 02_{hex})

Les attributs ajoutés à la fin de la réponse Set_Attribute_All doivent être étendus, tel que cela est défini dans le Tableau 84 et le Tableau 85. Tous les autres paramètres de ce service sont définis dans l'objet CCO normalisé dans l'IEC 61158-5-2 et l'IEC 61158-6-2.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Tableau 84 – Données du service de demande Set_Attributes_All (attributs ajoutés)

Nom	Type de données	Description
Paramètres de sécurité	STRUCT de:	
	USINT	Remplissage, défini sur zéro
	USINT	Remplissage, défini sur zéro
	UDINT	CRC de configuration (SCCRC) (valeur définie = 0, l'appareil effectue ce calcul)
	DATE ET HEURE	Datation de configuration (SCTS) (le cas échéant, sinon = 0)
	UDINT	EPI de correction de temps
	WORD	Paramètres de connexion de correction de temps
	10 octets	Target UNID (UNID cible)
	10 octets	Remplissage, défini sur zéro
	UINT	Multiplicateur EPI d'intervalles Ping
	UINT	Multiplicateur minimal de messages de coordination temporelle
	UINT	Multiplicateur de délai du réseau
	USINT	Multiplicateur de temporisation
	USINT	Nombre maximal de consommateurs
Instance de configuration	UINT	
Drapeau d'attribution d'ID	BOOL	

Tableau 85 – Données du service de réponse Set_Attributes_All (paramètres ajoutés)

Nom	Type de données	Description
Longueur	USINT	Longueur des paramètres de sécurité supplémentaires = 3
Type de format	USINT	
Nombre maximal d'anomalies	UINT	

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

6.8.7.3 Restauration (Code de service 15_{hex})

Les appareils de sécurité ne doivent pas mettre en œuvre le service Restauration au niveau de la classe ou de l'instance, dans la mesure où l'outil de configuration coordonne la configuration par l'intermédiaire du Programme de contrôle de sécurité.

6.8.8 Comportement d'objet

Le comportement de l'objet Configuration de connexion pour les appareils de sécurité doit être contrôlé par le Programme de contrôle de sécurité et respecter le comportement défini dans le Tableau 86, à la Figure 18 et à la Figure 19.

Tableau 86 – Mapping des états entre le Programme de contrôle de sécurité et les objets CCO

Programme de contrôle de sécurité	Configuration de connexion
Autovérification	Editions non admises
Exception d'autovérification	Editions non admises
Repos	Editions non admises
Configuration	Editions admises
Exécution	Editions non admises
Abandon	Editions non admises
Anomalie critique	Editions non admises

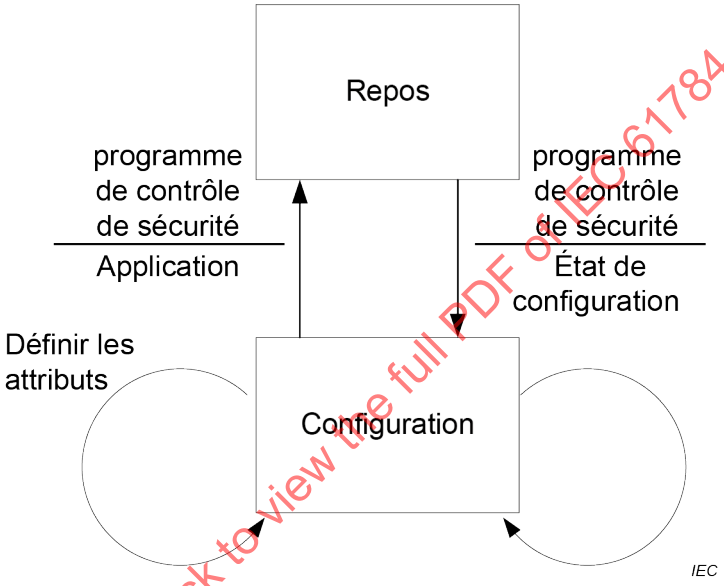


Figure 18 – Diagramme d'états de l'objet Configuration de connexion

Le flux de données applicable à l'objet Configuration de connexion dans l'état Configuration est défini à la Figure 19.

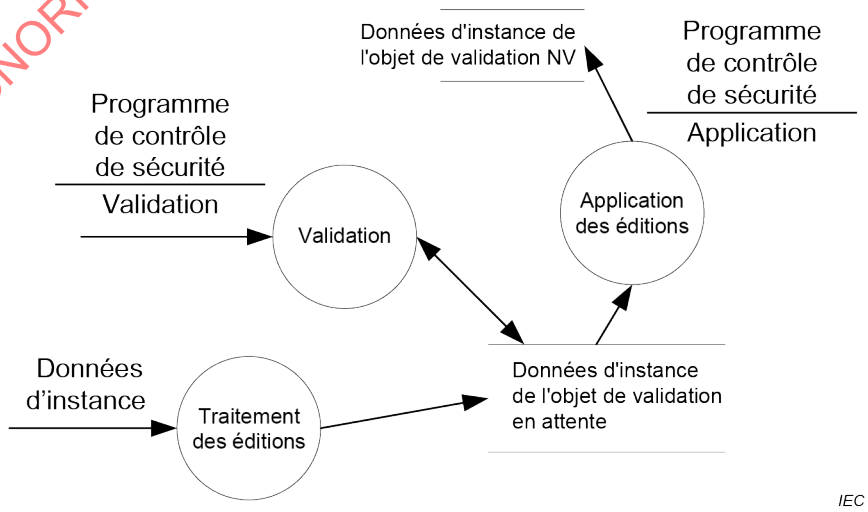


Figure 19 – Flux de données de l'objet Configuration de connexion

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

7 Protocole de couche de communication de sécurité

7.1 Format PDU de sécurité

7.1.1 Codage PDU de sécurité

7.1.1.1 Règles générales de codage

Le protocole de sécurité définit neuf formats de codage de section utilisés dans des combinaisons différentes pour les messages de sécurité. Les neuf types de formats de codage de section sont les suivants:

- section de données BF à 1 ou 2 octets (voir 7.1.1.4);
- section de données EF à 1 ou 2 octets (voir 7.1.1.4);
- section de données BF de 3 à 250 octets (voir 7.1.1.6);
- section de données EF de 3 à 250 octets (voir 7.1.1.6);
- section BT de datation (voir 7.1.1.8);
- section BF de coordination temporelle (voir 7.1.1.9);
- section EF de coordination temporelle (voir 7.1.1.9);
- section BT de correction de temps (voir 7.1.1.9);
- section EF de correction de temps (voir 7.1.1.9).

Ces codages de section permettent de constituer six types de messages de sécurité des formats de connexion. Les deux formats, de base et étendu, peuvent être utilisés dans les six types de messages. Les six types de formats de connexion sont les suivants:

- point à point à 1 ou 2 octets (voir 7.1.1.13);
- multipoint à 1 ou 2 octets, format 1 (voir 7.1.1.14);
- multipoint à 1 ou 2 octets, format 2 (voir 7.1.1.15);
- multipoint de 3 à 248 octets, format 1 (voir 7.1.1.16);
- multipoint de 3 à 248 octets, format 1 (voir 7.1.1.17);
- multipoint de 3 à 248 octets, format 2 (voir 7.1.1.18).

Le Tableau 87 définit les sections utilisées dans les différents types de messages pour les six types de formats de connexion différents:

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Tableau 87 – Sections de connexion et formats PDU

Format de connexion de sécurité			Types de messages					
			Message de données[b]				Message de coordination temporelle[b]	Message de correction de temps
Taille des données	Type de connexion de sécurité	Type de saut de réseau	Section de données à 1 ou 2 octets	Section de données de 3 à 250 octets	Section de datation[a]	Section de correction de temps	Section de coordination temporelle	Section de correction de temps
1 ou 2 octets	Point à point	Tous	X		X[a]		X	
	Multipoint	CP 2/3	X		X[a]		X	X
		CP 2/2	X		X[a]	X	X	
3 à 248 octets	Point à point	Tous		X	X[a]		X	
	Multipoint	CP 2/3		X	X[a]		X	X
		CP 2/2		X	X[a]	X	X	

[a] Le format de base comprend une section indépendante pour la datation; il fait partie intégrante de la section de données dans le format étendu.

[b] Le message peut utiliser soit le format de base, soit le format étendu.

Les points d'origines et les cibles doivent satisfaire aux critères de sélection présentés dans le Tableau 88 pour l'utilisation des formats de base et étendu.

Le format de base est déconseillé à partir du FSCP 2/1. FSCP 2/1 exige d'utiliser uniquement le format étendu.

Tableau 88 – Sections de connexion et format de message

Type	Base Format (Format de base)	Extended Format (Format étendu)
Point d'origine	Déconseillé[a]	Exigé
Cible	Déconseillé[a]	Exigé

[a] Facultatif pour prendre en charge la rétrocompatibilité.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

7.1.1.2 Octet Mode

L'octet Mode est décrit en dehors des définitions de sections, étant donné que les différentes parties sont incluses dans les différents CRC de sections. La disposition de l'octet Mode est définie à la Figure 20. Dans le format de base, les bits 0 à 4 de l'octet Mode font partie intégrante de la section de datation, tandis que les bits 5 à 7 font partie intégrante des sections de données. Dans le format étendu à paquets courts, les bits 5 à 7 font partie intégrante du CRC des données. Dans le format étendu à paquets longs, les bits 0 à 4 de l'octet Mode font partie intégrante du CRC des données complémentaires, tandis que les bits 5 à 7 font partie intégrante du CRC des données vraies. Les variables utilisées dans l'octet Mode, les descriptions succinctes et les références qui visent à compléter les descriptions sont données dans le Tableau 89.

Octet Mode							
7	6	5	4	3	2	1	0
Run_Idle	TBD_2_Bit	TBD_Bit	N_Run_Idle	TBD_2_Bit_Copy	N_TBD_Bit	Ping_Count	
N_Run_Idle[a]	N_TBD_2_Bit[a]	N_TBD_Bit[a]					
[a] Les valeurs ne sont pas transmises dans le paquet de données, elles sont déduites par le consommateur.							

Figure 20 – Format de l'octet Mode

Tableau 89 – Variables de l'octet Mode

Nom	Description	Référence
Run_Idle	Run_Idle doit être utilisé pour indiquer la convivialité des données telle que déterminée par l'application relative à la sécurité du producteur	7.7.1.1
N_Run_Idle	Complément de Run_Idle	7.7.1.2
TBD_2_Bit	Réservé pour une utilisation future	7.7.1.3
TBD_2_Bit Copy	Copie du TBD_2_Bit	7.7.1.4
TBD_Bit	Réservé pour une utilisation future. Le TBD_Bit doit être défini sur 0 par l'Objet de validation de sécurité	7.7.1.6
N_TBD_Bit	Complément du TBD_Bit	7.7.1.7
Ping_Count	Le nombre de demandes Ping permet de déterminer le moment auquel un consommateur doit envoyer un message de coordination temporelle	7.7.1.5

7.1.1.3 Traitement CRC de l'octet Mode pour le format de base

Le traitement de l'octet Mode dans les CRC BF doit être effectué comme suit:

- logique de l'octet Mode de type CRC préalablement à l'inclusion dans le CRC;
- CRC des données réelles: octet Mode AND $E0_{hex}$;
- CRC des données complémentaires: (octet Mode XOR FF_{hex}) AND $E0_{hex}$;
- CRC de la section de datation octet Mode AND $1F_{hex}$.

7.1.1.4 Section de données à 1 ou 2 octets, format de base

La section de données à 1 ou 2 octets doit comporter l'octet ou les octets des données réelles, l'octet Mode, le CRC réel et le CRC complémentaire. La disposition de la section de données à 1 ou 2 octets est définie à la Figure 21.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Section de données à 1 ou 2 octets																															
Données réelles																Octet Mode								CRC réel								CRC complémentaire							
7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
1 – 2 octets																								CRC-S1								CRC-S2							

Légende

= Couvert par le CRC de données réelles

= Couvert par le CRC de données complémentaires

= Couvert par le CRC de la section de datation

Figure 21 – Section de données à 1 ou 2 octets, format de base

Le calcul du CRC des données réelles BF à 1 ou 2 octets doit inclure:

- l'identifiant du producteur (PID) (par CRC-S1);
- l'(octet Mode) AND ($E0_{hex}$) (par CRC-S1);
- Loctet ou les octets des données réelles (par CRC-S1).

Le calcul du CRC des données complémentaires BF à 1 ou 2 octets doit inclure:

- l'identifiant du producteur (PID) (par CRC-S1);
- (octet Mode XOR FF_{hex}) AND ($E0_{hex}$) (par CRC-S2);
- les octets des données complémentaires XOR FF_{hex} (par CRC-S2).

NOTE Le PID utilise le CRC-S1 pour le calcul du CRC réel et complémentaire.

7.1.1.5 Section de données à 1 ou 2 octets, format étendu

La section de données à 1 ou 2 octets applicable au format étendu doit comprendre l'octet ou les octets des données réelles, l'octet Mode, la datation et le CRC-S5 calculé sur l'ensemble du paquet. Le format étendu de la section de données à 1 ou 2 octets est représenté à la Figure 22.

Section de données à 1 ou 2 octets, format étendu						
Données réelles	Octet Mode[a]		CRC S5		Datation	CRC S5
2 octets	1 octet		2 octets		2 octets	1 octet
1 – 2 octets			CRC-S5_0	CRC-S5_1	Datation	CRC-S5_2

[a] Les bits 0 à 4 ne sont pas inclus dans le calcul du CRC.

Légende

= Couvert par le CRC-S5

Figure 22 – Section de données à 1 ou 2 octets, format étendu

Le calcul du CRC de la section de données EF à 1 ou 2 octets doit utiliser CRC-S5 et inclure:

- l'identifiant de producteur (PID);
- le comptage de remplacement à 16 bits;
- l'octet Mode AND ($E0_{hex}$);

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

- l'octet ou les octets des données réelles;
- la datation.

7.1.1.6 Section de données de 3 à 250 octets, format de base

La section de données de 3 à 250 octets doit comporter les octets des données réelles, l'octet Mode, le CRC réel, les octets des données complémentaires et le CRC complémentaire. La disposition de la section de données de 3 à 250 octets est définie à la Figure 23.

Section de données de 3 à 250 octets				
Données réelles	Octet Mode	CRC réel	Données complémentaires	CRC complémentaire
3 – 250 octets		CRC-S3	3 – 250 octets	CRC-S3

Légende

= Couvert par le CRC de données réelles

= Couvert par le CRC de données complémentaires

= Couvert par le CRC de la section de datation

Figure 23 – Format de section de données de 3 à 250 octets, format de base

Le calcul du CRC des données réelles BF de 3 à 250 octets doit inclure:

- l'identifiant du producteur (PID) (par CRC-S3);
- l'(octet Mode) AND ($E0_{hex}$) (par CRC-S3);
- l'octet ou les octets des données réelles (par CRC-S3).

Le calcul du CRC des données complémentaires BF de 3 à 250 octets doit inclure:

- l'identifiant du producteur (PID) (par CRC-S3);
- (octet Mode XOR FF_{hex}) AND ($E0_{hex}$) (par CRC-S3);
- les octets des données complémentaires XOR FF_{hex} (par CRC-S3).

7.1.1.7 Section de données de 3 à 250 octets, format étendu

La section de données EF de 3 à 250 octets doit comprendre les octets des données réelles, l'octet Mode, le CRC-S3, les octets des données complémentaires, la datation et le CRC-S5. La section de données EF de 3 à 250 octets est représentée à la Figure 24.

De 3 à 250 octets, format étendu							
Données réelles	Octet Mode	CRC de données réelles	Données complémentaires	CRC de données complémentaires		Datation	CRC de données complémentaires
3 – 250 octets	1 octet	2 octets	3 – 250 octets	2 octets		2 octets	1 octet
3 – 250 octets		CRC-S3	Complémentaires 3 – 250 octets	CRC-S5_0	CRC-S5_1	Datation	CRC-S5_2

Figure 24 – Format de section de données de 3 à 250 octets, format étendu

Le calcul du CRC des données réelles EF de 3 à 250 octets doit inclure:

- l'identifiant du producteur (PID) *(par CRC-S3)*;
- le comptage de remplacement *(par CRC-S3)*;

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

- l'(octet Mode) **AND** (0xE0) *(par CRC-S3)*;
- l'octet ou les octets des données réelles *(par CRC-S3)*.

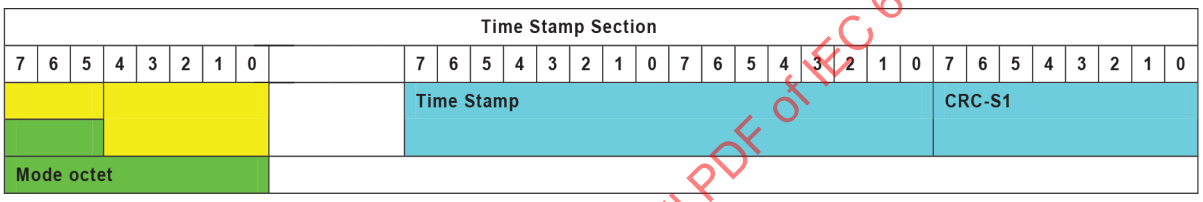
Le calcul du CRC des données complémentaires EF de 3 à 250 octets doit inclure:

- l'identifiant du producteur (PID) *(par CRC-S5)*;
- le comptage de remplacement *(par CRC-S5)*;
- l'octet Mode **AND** 0x1F *(par CRC-S5)*;
- les octets des données réelles **XOR** 0xFF *(par CRC-S5)*;
- la datation *(par CRC-S5)*.

7.1.1.8 Section de datation, format de base

La section de datation se compose de l'octet Mode, de Time_Stamp et du CRC de datation. La disposition de la section de datation est définie à la Figure 25.

Les descriptions des variables de la section de datation sont définies dans le Tableau 90.



IEC

Légende

= Couvert par le CRC de données réelles
= Couvert par le CRC de données complémentaires
= Couvert par le CRC de la section de datation

Figure 25 – Format de section de datation, format de base

Tableau 90 – Variables de datation

Nom	Description	Référence
Data_Time_Stamp	Point à point -- Data_Time_Stamp représente la datation de l'échantillonnage des données pour production, par rapport à l'horloge du consommateur. Multipoint -- Data_Time_Stamp représente la datation de l'échantillonnage des données pour production, par rapport à l'horloge du producteur.	7.7.2

Le calcul du CRC de datation BF doit inclure:

- l'octet Identifiant du producteur (PID) (par CRC-S1);
- l'(octet Mode) AND ($1F_{hex}$) (par CRC-S1);
- l'octet ou les octets de datation (par CRC-S1).

7.1.1.9 Section de coordination temporelle

La section de coordination temporelle doit être transmise au producteur par le consommateur en réponse à une modification dans le nombre de demandes Ping.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

La section de coordination temporelle est utilisée comme Message de coordination temporelle pour toutes les demandes de coordination temporelle point à point et multipoint. Il existe deux formats: le format de base (BF) et le format étendu (EF).

Le codage applicable à la section de coordination temporelle BF est défini à la Figure 26, celui applicable à la section de coordination temporelle EF étant défini à la Figure 27. Les variables utilisées dans la section de coordination temporelle, les descriptions succinctes et les références qui visent à compléter les descriptions sont données dans le Tableau 91.

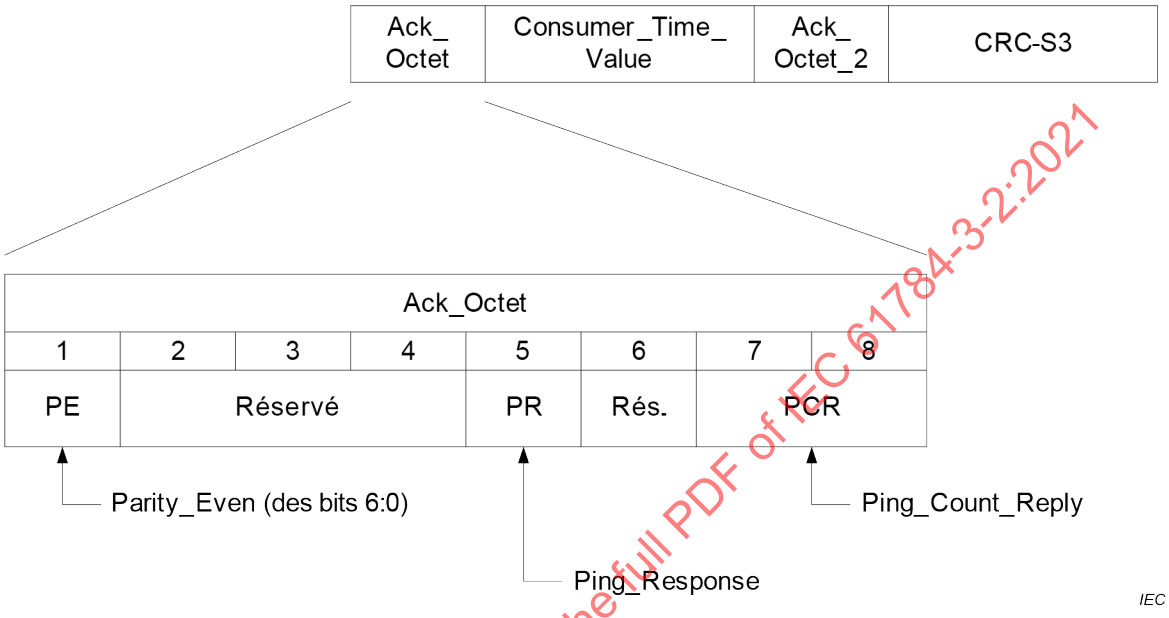


Figure 26 – Codage du message de coordination temporelle BF

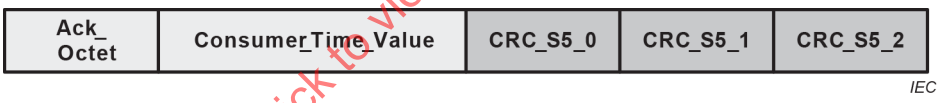


Figure 27 – Codage du message de coordination temporelle EF

Tableau 91 – Variables du message de coordination temporelle

Nom	Description	Référence
Consumer_Time_Value	Consumer_Time_Value dans le message de coordination temporelle doit marquer (le plus précisément possible) l'heure à laquelle le consommateur transmet un message de réponse aux demandes Ping	7.7.3.2
Ack_Octet	Se compose de:	
Parity_Even	Le bit Parity_Even dans le message de coordination temporelle doit constituer la parité paire des bits 0 à 6 du message	
Ping_Response_Bit	Le Ping_Response_Bit dans le message de coordination temporelle doit indiquer la transmission d'une réponse aux demandes Ping	7.7.3.1
Ping_Count_Reply	Le Ping_Count_Reply dans le message de coordination temporelle doit indiquer la demande Ping à laquelle répond le consommateur	7.7.3.3
Réservé	Réservé, défini sur zéro	
CRC-S3	CRC qui couvre les données contenues dans le message de coordination temporelle BF	
CRC-S5	CRC qui couvre les données contenues dans le message de coordination temporelle EF	

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

La règle suivante doit être utilisée pour le calcul du bit de parité dans le message de coordination temporelle:

Bit 7 de parité paire de forme Ack_Octet sur le Ack_Octet.

La règle suivante doit être utilisée pour le réglage des bits dans le Ack_Octet_2 du message de Coordination temporelle:

Ack_Octet_2 = ((Ack_Octet XOR FF_{hex}) AND 55_{hex}) OR (Ack_Octet AND AA_{hex}).

Le format de coordination temporelle EF doit être utilisé lors de l'établissement d'une connexion avec le format étendu. Dans les autres cas, le format de coordination temporelle BF doit être utilisé.

7.1.1.10 Calcul du CRC de coordination temporelle

Le calcul du CRC de coordination temporelle doit inclure:

- l'identifiant de consommateur (CID) (par CRC-S3 ou CRC-S5);
- l'octet Accusé de réception (par CRC-S3 CRC-S5);
- la Consumer_Time_Value (par CRC-S3 CRC-S5).

Ack_Octet_2 dans le message de Coordination temporelle ne doit pas être inclus dans le CRC de sécurité.

7.1.1.11 Section de correction de temps

Le message de correction de temps doit être transmis par un producteur multipoint à chaque consommateur multipoint, pour chaque intervalle Ping. Le message de correction de temps, qui contient les informations spécifiques au consommateur, est transmis par le producteur au consommateur à un débit inférieur à celui des données produites. Le message de correction de temps transmet les informations spécifiques au consommateur, à ce même consommateur à un débit inférieur à celui des données produites. Le codage du message de correction de temps BF est représenté à la Figure 28 et la section de correction de temps EF est définie à la Figure 29. Les variables utilisées dans la section de correction de temps sont définies dans le Tableau 92.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

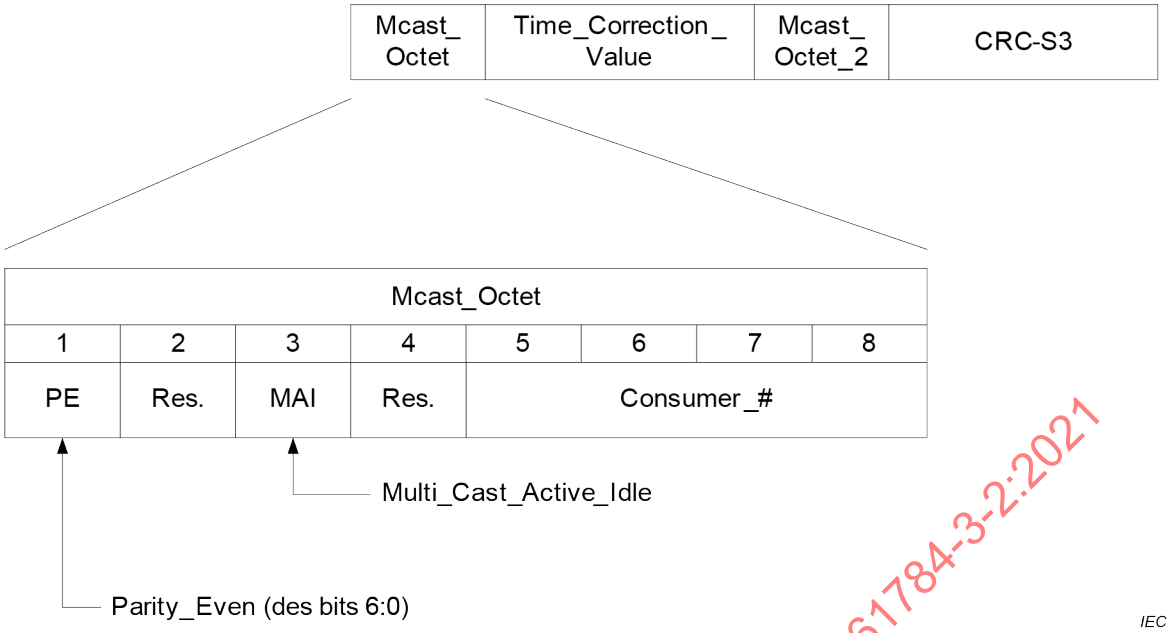


Figure 28 – Codage du message de correction de temps BF



Figure 29 – Codage du message de correction de temps EF

Tableau 92 – Variables du message de correction de temps

Nom	Description	Référence
Consumer_Time_Correction_Value	Consumer_Time_Correction_Value dans le message de correction de temps doit être utilisée pour corriger la datation des données et évaluer l'heure par rapport à l'horloge des consommateurs multipoints	7.7.4.2
MCast_Octet	Se compose de:	
Parity_Even	Le bit Parity_Even dans le message de correction de temps doit constituer la parité paire des bits 0 à 6 du message	
Multi_Cast_Active_Idle	Multi_Cast_Active_Idle dans le message de correction de temps doit indiquer "Repos" si la transmission précède la réponse de ce consommateur avec un message de coordination temporelle valide	7.7.4.3
Consumer_#	Consumer_# dans le message de correction de temps doit indiquer le numéro de consommateur auquel s'adresse ce message	7.7.4.1
Réservé	Réservé, défini sur zéro	7.7.4.4
CRC-S3	CRC qui couvre les données contenues dans le message de correction de temps BF	
CRC-S5	CRC qui couvre les données contenues dans le message de correction de temps EF	

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

La règle suivante doit être utilisée pour le calcul du bit de parité dans le message de correction de temps:

Bit 7 de la parité paire de forme MCast_Octet dans le MCast_Octet.

La règle suivante doit être utilisée pour le réglage des bits dans le Mcast_Octet_2 du message de correction de temps:

MCast_Octet_2 = ((MCast_Octet XOR FF_{hex}) AND 55_{hex}) OR (MCast_Octet AND AA_{hex}).

Le format de correction de temps EF doit être utilisé lors de l'établissement d'une connexion avec le format étendu. Dans les autres cas, le format de correction de temps BF doit être utilisé.

7.1.1.12 Calcul du CRC de correction de temps

Le calcul du CRC de correction de temps doit inclure:

- l'identifiant du producteur (PID) (par CRC-S3);
- Mcast_Octet (par CRC-S3);
- Time_Correction_Value (par CRC-S3).

MCast_Octet_2 du message de correction de temps ne doit pas être inclus dans le CRC de sécurité.

7.1.1.13 Format de connexion de sécurité point à point à 1 ou 2 octets

La Figure 30 définit l'organisation de la section pour le format de connexion de sécurité point à point à 1 ou 2 octets.

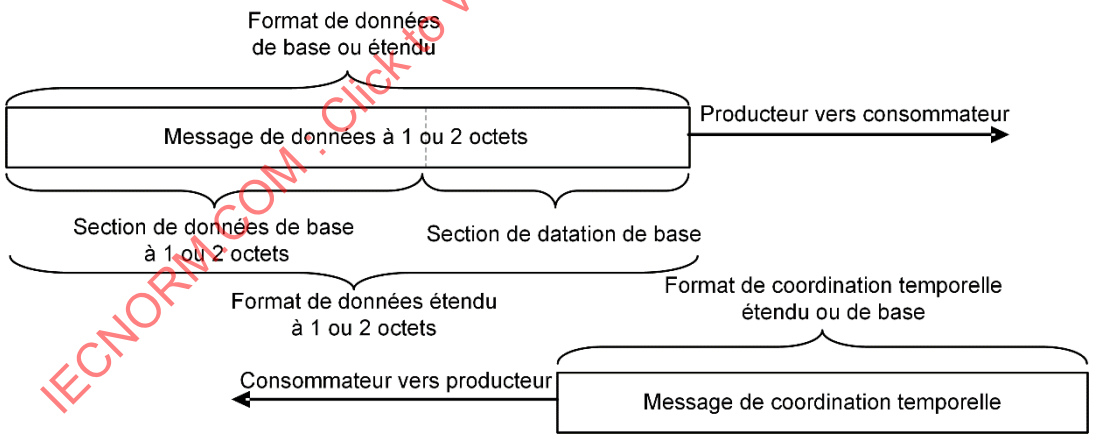


Figure 30 – Codage PDU point à point à 1 ou 2 octets

7.1.1.14 Format de connexion de format 1 multipoint à 1 ou 2 octets

La Figure 31 définit l'organisation de la section pour le format de connexion multipoint de format 1 à 1 ou 2 octets.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

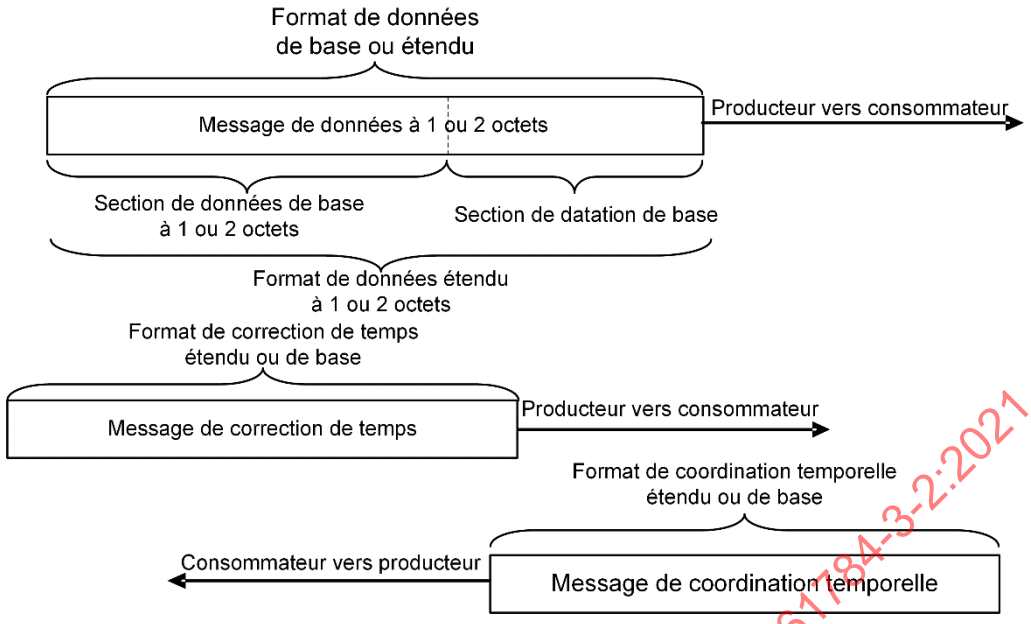
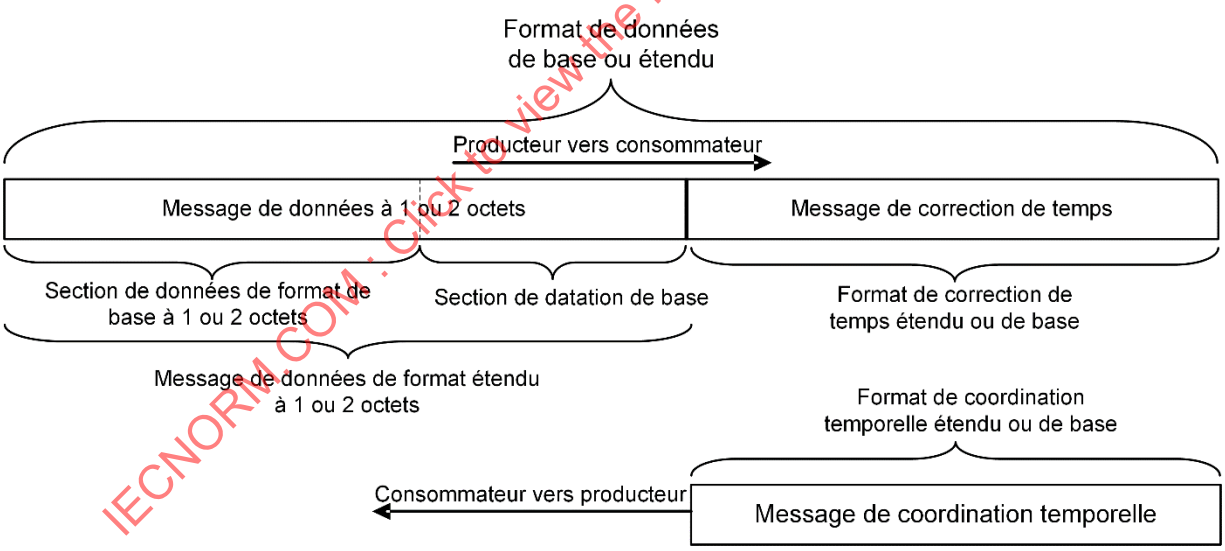


Figure 31 – Codage PDU multipoint à 1 ou 2 octets

7.1.1.15 Format de connexion de sécurité de format 2 multipoint à 1 ou 2 octets

La Figure 32 définit l'organisation de la section pour le format de connexion de sécurité de format 2 multipoint à 1 ou 2 octets.



IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Figure 32 – Format de connexion de sécurité de format 2 multipoint à 1 ou 2 octets

7.1.1.16 Format de connexion de sécurité point à point de 3 à 250 octets

La Figure 33 définit l'organisation de la section pour le format de connexion de sécurité point à point de 3 à 250 octets.

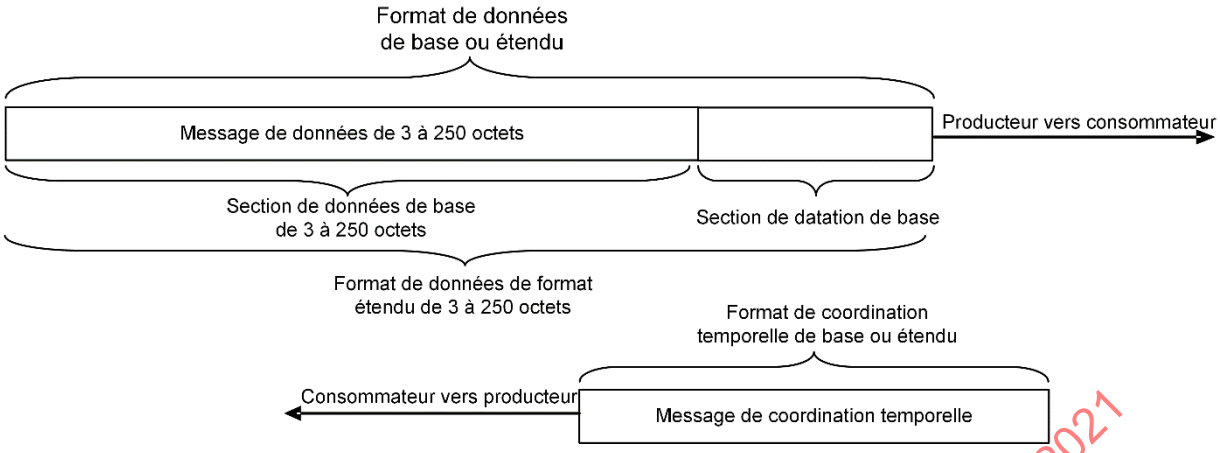
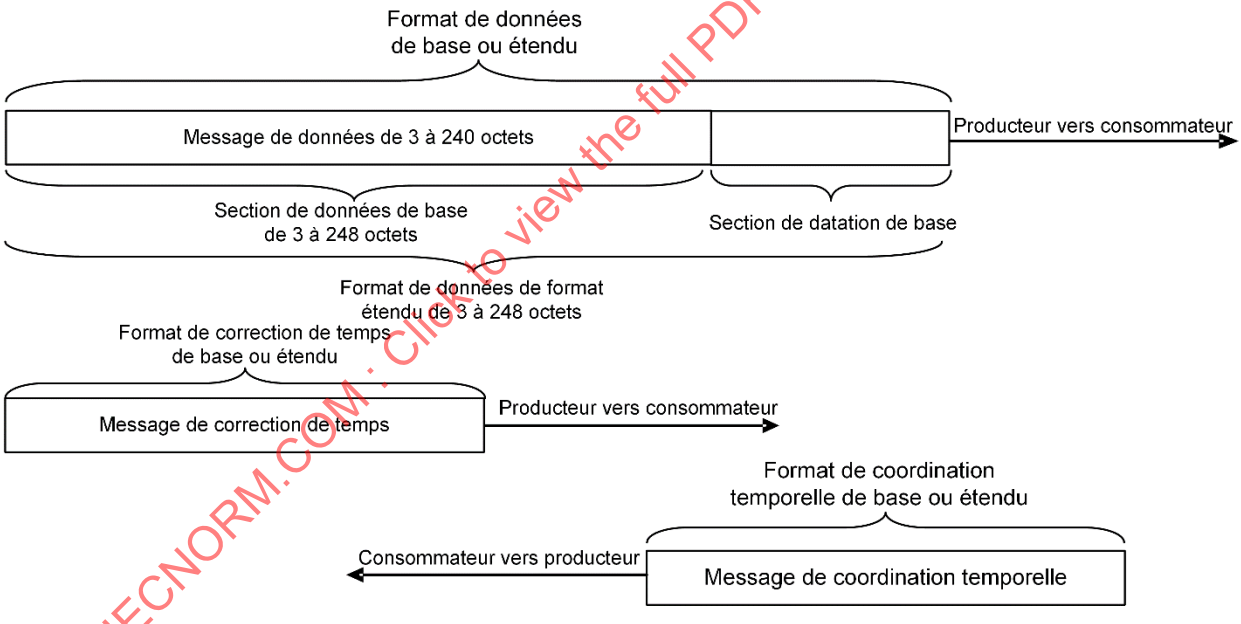


Figure 33 – Codage PDU point à point de 3 à 250 octets

7.1.1.17 Format PDU de sécurité de format 1 multipoint de 3 à 248 octets

La Figure 34 définit l'organisation de la section pour le format de connexion de sécurité multipoint de 3 à 248 octets.



IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Figure 34 – Codage PDU multipoint de 3 à 248 octets

7.1.1.18 Format PDU de sécurité de format 2 multipoint de 3 à 248 octets

La Figure 35 définit l'organisation de la section pour le format de connexion de sécurité multipoint de 3 à 248 octets.

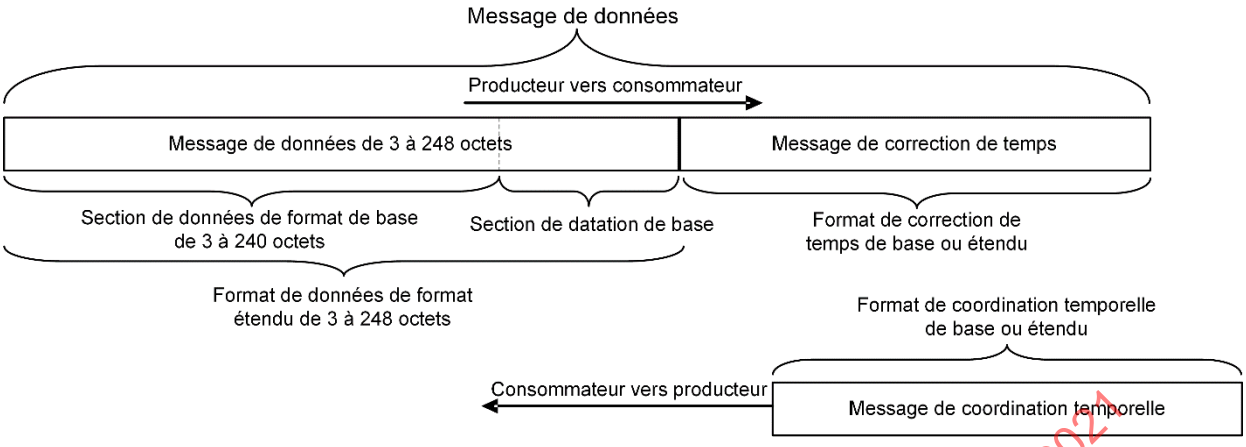
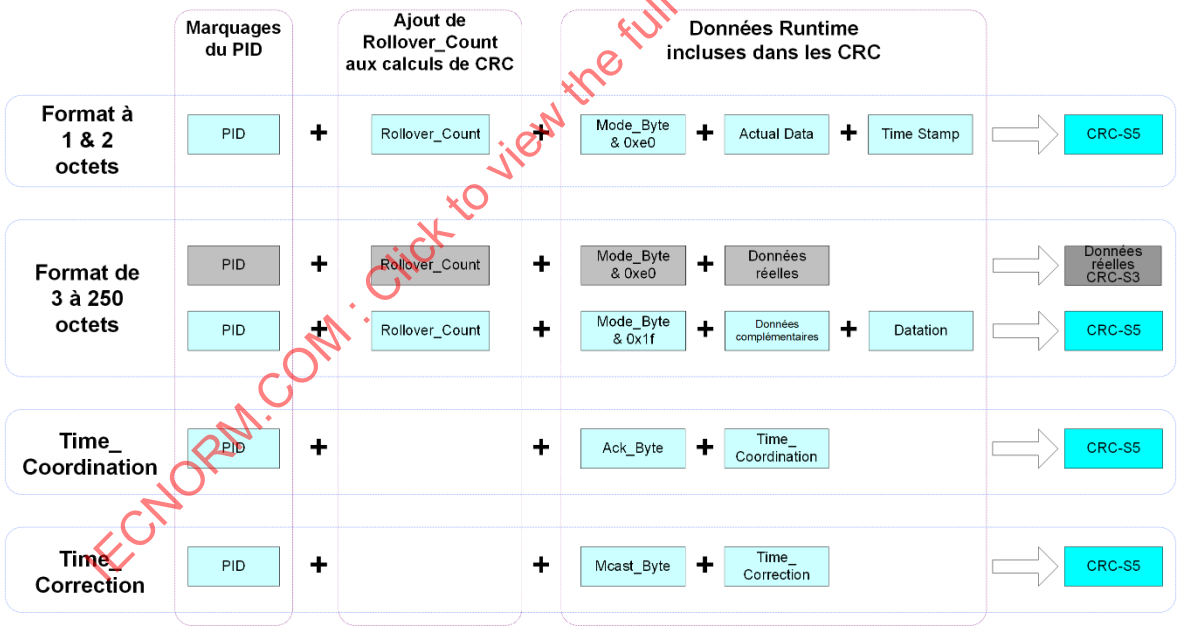


Figure 35 – Format de connexion de sécurité multipoint de 3 à 248 octets

7.1.1.19 Ordre des calculs du CRC pour le format étendu

La Figure 36 représente le point d'ajustement du comptage de remplacement aux calculs du CRC pour les messages de format étendu.

NOTE La valeur de départ du CRC est toujours fondée sur le PID/CID comme dans le format de base; le comptage de remplacement est traité comme un paramètre de donnée supplémentaire.



IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Figure 36 – Ordre de calcul du CRC pour les messages de format étendu

7.1.2 CRC de sécurité

7.1.2.1 Présentation générale du CRC de sécurité

Les différentes sections du FSCP 2/1 utilisent cinq CRC de sécurité.

- Un CRC de 8 bits (CRC-S1 ou CRC-S2) est utilisé pour les sections de données BF qui contiennent jusqu'à deux octets de données de sécurité, ainsi que pour les sections de datation.

- Un CRC de 16 bits (CRC-S3) est utilisé pour les sections de données BF et EF de 3 à 250 octets et pour les messages de correction de temps et de coordination temporelle BF.
- Un CRC de 24 bits (CRC-S5) est utilisé pour le format de données EF qui contient jusqu'à deux octets de données de sécurité et pour les sections de données complémentaires EF de 3 à 250 octets. Le CRC de 24 bits est également utilisé pour les messages de correction de temps et de coordination temporelle EF.
- Un CRC de 32 bits (CRC-S4), est utilisé pour l'établissement d'une connexion, la configuration et l'extension de sécurité de la définition du fichier EDS.

Les calculs de ces CRC sont décrits à l'Annexe A.

7.1.2.2 Polynômes de CRC

Le Tableau 93 définit les polynômes utilisés dans le FSCP 2/1.

Tableau 93 – Polynômes de CRC utilisés

Nom	Valeur hex de polynôme
CRC-S1	37_{hex}
CRC-S2	$3B_{hex}$
CRC-S3	$080F_{hex}$
CRC-S4	$EDB88320_{hex}$
CRC-S5	$5D6DCB_{hex}$

7.1.2.3 Spécifications d'utilisation des CRC

L'utilisation du CRC de messagerie E/S est définie en 7.1, avec application des CRC-S1, CRC-S2 et CRC-S3, de nombreux autres CRC étant toutefois définis dans le FSCP 2/1 pour l'établissement d'une connexion, la configuration et l'extension de sécurité de la définition du fichier EDS. Le Tableau 94 définit le type d'algorithme utilisé et la valeur de départ pour chaque utilisation.

Tableau 94 – Utilisation des CRC pour la connexion et la configuration

Nom du CRC	Algorithme utilisé	Valeur de départ	Description
SCCRC	CRC-S4 (voir Article A.1)	$FFFFFFFF_{hex}$	CRC de configuration de sécurité
CPCRC	CRC-S4 (voir Article A.1)	$FFFFFFFF_{hex}$	CRC de paramètre de connexion
CRC de mot de passe	CRC-S4 (voir Article A.1)	$FDFDFDFD_{hex}$	Utilisé pour le cryptage des mots de passe avant transmission
CRC du fichier EDS	CRC-S4 (voir Article A.1)	$FDFDFDFD_{hex}$	Utilisé pour assurer l'intégrité des fichiers EDS utilisés par les appareils de sécurité

7.2 Comportement du protocole de communication

7.2.1 Séquence des contrôles de sécurité

La séquence suivante des contrôles doit être utilisée pour vérifier les messages:

a) contrôle des comptages de demandes Ping;

b) évaluation du CRC de la section de datation;

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

c) évaluation des datations;

d) évaluation du CRC des données réelles;

e) évaluation du CRC des données complémentaires;

f) réalisation d'une contre-vérification.

7.2.2 Fin de connexion

Lorsqu'un producteur détecte une erreur qui exige de mettre fin à une connexion (c'est-à-dire une réponse aux demandes Ping hors de l'intervalle Ping du producteur), il doit mettre fin à la connexion et notifier l'application de l'action.

Tous les consommateurs doivent surveiller la transmission périodique des données et passer à un état de sécurité en cas d'arrêt des transmissions périodiques. Si le consommateur détecte une erreur, il doit passer à un état de sécurité et mettre fin à la connexion de consommation associée à cette erreur.

Lorsque la couche de sécurité détecte une erreur qui exige de mettre fin à une connexion, la séquence suivante doit être suivie pour effectuer ladite terminaison.

a) La couche de sécurité détecte une erreur qui exige de mettre fin à une connexion.

b) La couche de sécurité notifie le programme d'application par le réglage de l'état de connexion, afin d'indiquer une anomalie de sécurité des communications.

c) L'application relative à la sécurité doit transférer les données et les E/S (par exemple, réglage des sorties sur l'état de sécurité) associées à la connexion vers un état de sécurité.

d) La couche de sécurité doit notifier le système de communications sous-jacent d'une erreur et solliciter la fin de la connexion par le réglage de son état de manière à indiquer une erreur de sécurité des communications.

e) La couche de sécurité doit maintenir son état de sécurité jusqu'à la suppression de l'anomalie et jusqu'au lancement d'une séquence de redémarrage de connexion.

7.2.3 Erreur de contre-vérification

Lorsque des données de sécurité ayant fait l'objet d'une contre-vérification se révèlent différentes, les données sont traitées comme des données erronées. Le consommateur BF doit mettre fin à la connexion (voir 7.2.2) et le consommateur EF incrémente le Consumer_Fault_Count et rejette le paquet si le comptage est inférieur à Max_Fault_Number ou met fin à la connexion s'il est égal ou supérieur à Max_Fault_Number.

7.3 Opération de datation

La datation permet de calculer l'actualité de réception des données dans le consommateur. La Figure 37 représente la séquence de datation des opérations pour une paire producteur/consommateur point à point simple.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

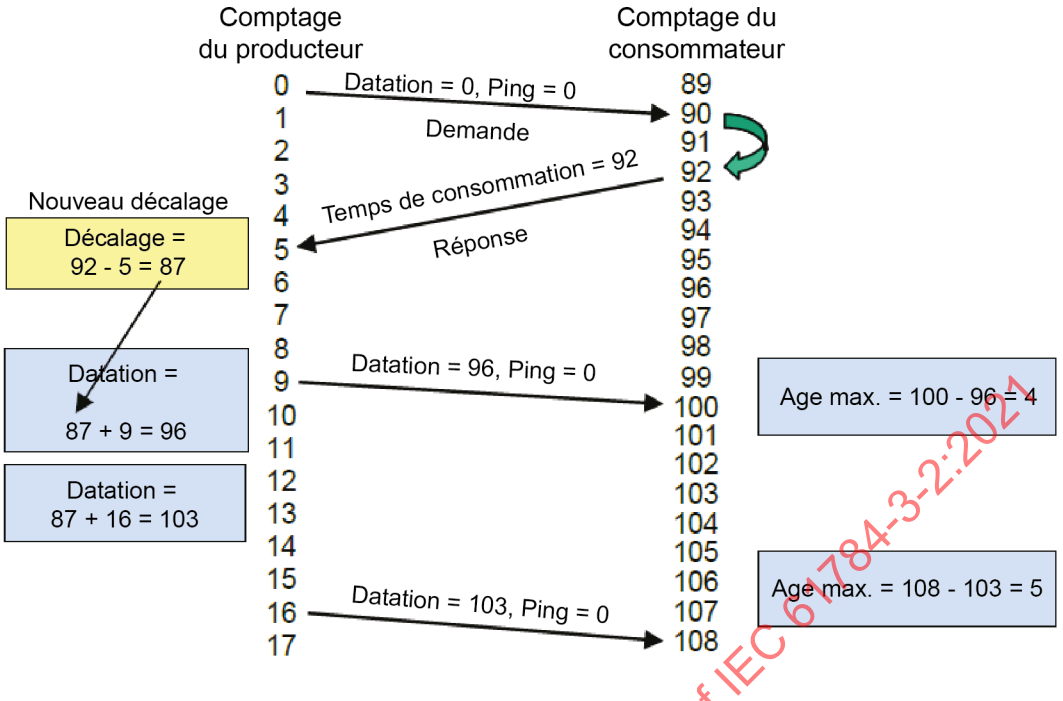


Figure 37 – Séquence de datation

A l'établissement de la connexion, le producteur doit solliciter une réponse à la demande Ping initiale.

Lorsque le consommateur constate une modification dans le comptage des demandes Ping, il doit préparer un message de réponse de coordination temporelle qui contient la valeur de consommation de son comptage d'horloge.

Le producteur doit utiliser le comptage d'horloge dans la réponse de coordination temporelle afin de calculer un décalage qui sera appliqué aux productions futures.

Pour chaque production ordonnancée, le producteur doit utiliser la valeur de son propre comptage d'horloge, ainsi que le décalage pour calculer la datation, et transmettre ces informations au consommateur avec les données.

Le consommateur doit utiliser la valeur reçue par le producteur pour calculer l'âge des données, par soustraction de la datation du producteur de son comptage d'horloge courant. Si le delta calculé est inférieur au delta maximal spécifié par l'utilisateur, les données sont correctes et sont utilisées par l'application interne à l'appareil. Si le delta est supérieur à la valeur spécifiée par l'utilisateur, les données sont jugées trop anciennes pour être utilisées, ce qui entraîne la fin de la connexion.

Le producteur doit solliciter une autre réponse à la demande Ping du consommateur pour chaque intervalle Ping. Ceci occasionne un nouveau calcul du décalage du producteur et empêche le vieillissement lent des données provoqué par des erreurs de temps.

Un facteur de correction de temps est ajouté afin de tenir compte de l'obliquité et de la dérive maximales des horloges dans un système asynchrone. Ce message permet d'ajuster le décalage du producteur.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

7.4 Comptages de remplacement dans l'EF

Un comptage de remplacement est utilisé en liaison avec la datation transmise pour étendre jusqu'à 32 bits la plage de fonctionnement réelle de la datation. Le comptage de remplacement n'est toutefois pas transmis avec la datation. Les valeurs initiales du comptage de remplacement sont définies à l'établissement d'une connexion et maintenues de façon indépendante à la fois par le producteur et le consommateur. La valeur du comptage de remplacement est incluse dans le calcul du CRC des données; ainsi les deux extrémités doivent s'accorder à tout moment sur la valeur en cours des paquets à recevoir de manière satisfaisante.

7.5 Diagrammes séquentiels de protocoles

7.5.1 Généralités

Les diagrammes séquentiels de protocoles représentent la relation entre producteurs et consommateurs par rapport à la datation et aux événements. L'écoulement du temps s'effectue du haut vers le bas de chaque figure. Les messages normaux reçus par le producteur ou le consommateur sont présentés dans les zones de texte normal. Les messages anormaux sont présentés dans les zones de texte en gras. Les messages attendus, mais non reçus sont présentés sous forme de texte libre.

7.5.2 Transmission de sécurité normale

Une communication normale entre un producteur et un consommateur de sécurité exige une séquence de messages périodiques. Lorsque le consommateur reçoit un message valide, la transaction s'effectue comme défini à la Figure 38.

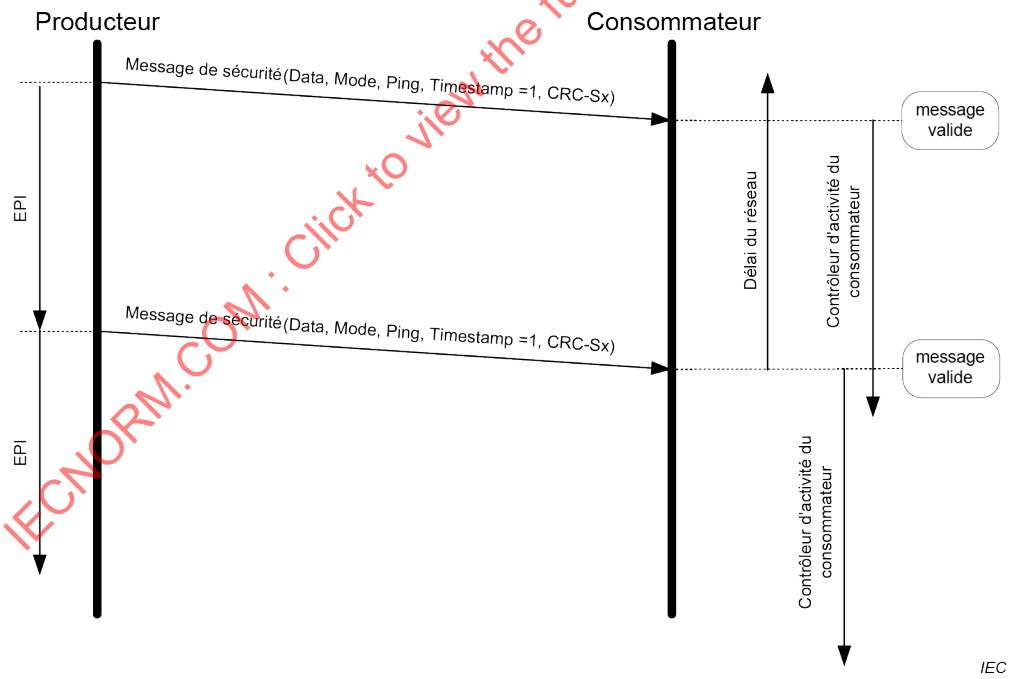


Figure 38 – Diagramme d'une séquence de sécurité producteur/consommateur normale

Le producteur de sécurité génère des données à une fréquence fixe appelée Intervalle de paquets attendu (EPI).

Les consommateurs déclenchés par la liaison doivent maintenir un temporisateur d'activité réinitialisé après réception d'un message attendu valide.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Si un message valide n'a pas été reçu avant expiration du temporisateur d'activité, le consommateur déclenché par la liaison doit mettre fin à la connexion (voir 7.2.2) et passer à l'état de sécurité défini.

Les consommateurs doivent vérifier l'âge des données reçues par un contrôle des datations reçues.

Si l'âge des données se révèle supérieur au délai du réseau, le consommateur doit mettre fin à la connexion (voir 7.2.2) et passer à l'état de sécurité défini.

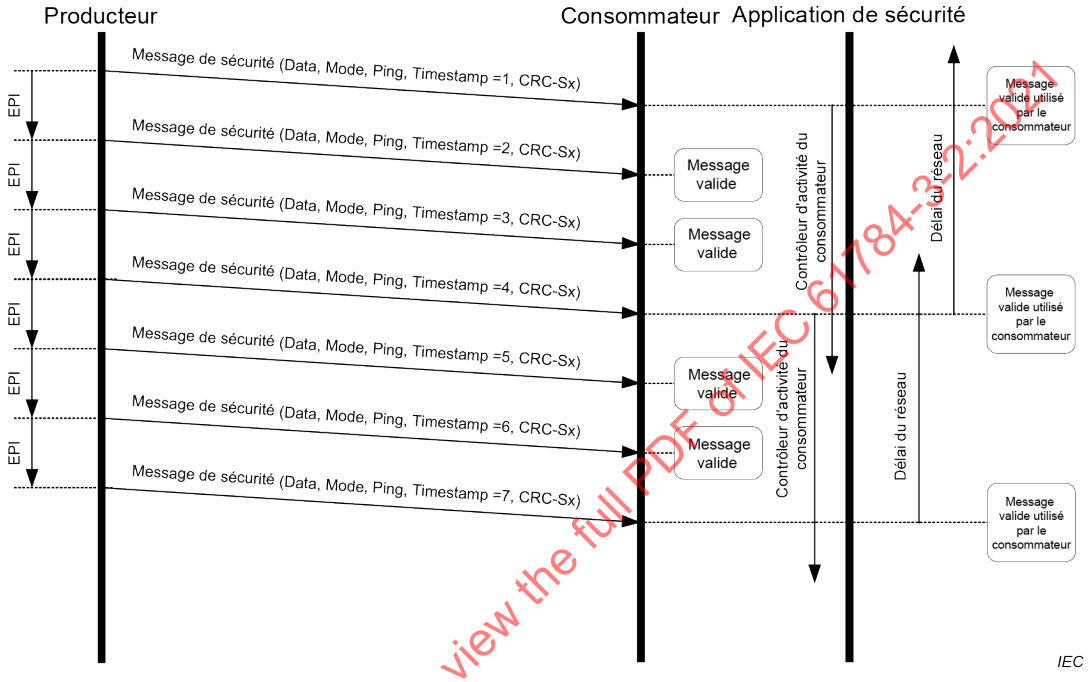


Figure 39 – Diagramme d'une séquence de sécurité producteur/consommateur normale (production répétée)

Les communications de sécurité doivent être configurables avec la production répétée. Dans ce cas, le consommateur n'utilise pas chaque paquet qui lui est transmis.

Lorsqu'une communication de sécurité est transmise avec une production répétée, les consommateurs déclenchés par l'application doivent utiliser le dernier paquet reçu pour achever la transaction, comme représenté à la Figure 39.

Les consommateurs qui utilisent les connexions de format de base doivent constater l'augmentation de la datation pour chaque période successive; à défaut, il doit être mis fin à la connexion (voir 7.2.2).

Les consommateurs qui utilisent les connexions de format étendu doivent constater l'augmentation de la datation pour chaque période successive. Si le consommateur reçoit un paquet avec une datation hors séquence, il doit rejeter ce dernier à moins que le compteur d'anomalies du consommateur n'ait atteint le nombre maximal d'anomalies; auquel cas, il doit être mis fin à la connexion.

L'envoi d'un message avec une production répétée offre l'avantage supplémentaire d'utiliser les données les plus récentes.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

7.5.3 Transmission de messages perdus, corrompus et retardés

Il est possible, en raison de perturbations extérieures, que le message transmis du producteur au consommateur puisse être corrompu, comme défini à la Figure 40. Si un message corrompu est détecté au niveau de la couche normalisée, il doit être éliminé et non présenté à l'application. Ceci entraîne une expiration du contrôleur d'activité du consommateur ou l'âge des données dépasse le délai du réseau. Le consommateur met alors fin à la connexion (voir 7.2.2) et passe à l'état de sécurité défini.

Si les CRC-Sx et les données transmises sont vérifiés et s'il est constaté que l'un ou l'autre comporte une erreur, ou que la contre-vérification des données comporte une erreur, le consommateur doit alors éliminer le paquet (format étendu AND ((Consumer_Fault_Count < Max_Fault_Number)), ou mettre fin à la connexion et passer à l'état de sécurité défini (format de base OR format étendu) AND ((Consumer_Fault_Count ≥ Max_Fault_Number) (voir 7.2.2).

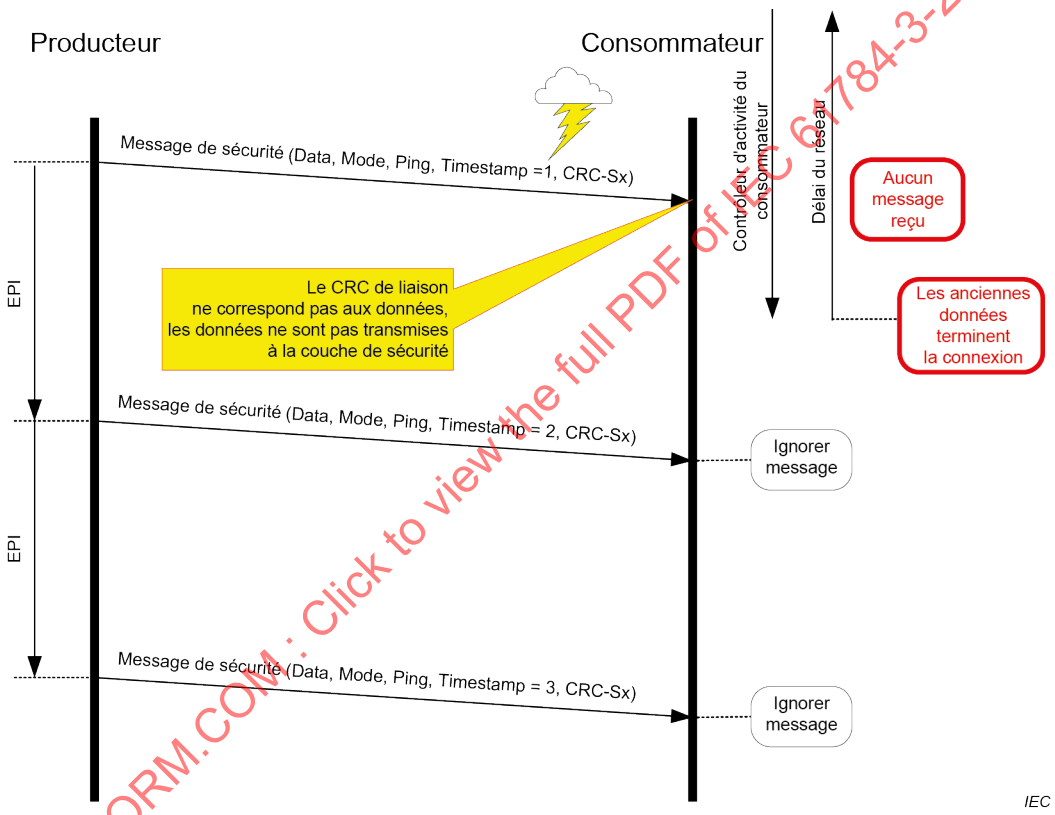


Figure 40 – Diagramme séquentiel d'un message producteur vers consommateur corrompu

Il est possible, en raison de perturbations extérieures, que le message transmis du producteur au consommateur puisse être perdu, comme défini à la Figure 41. Ceci entraîne une expiration du contrôleur d'activité du consommateur ou l'âge des données dépasse le délai du réseau. Le consommateur met alors fin à la connexion (voir 7.2.2) et passe à l'état de sécurité défini.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

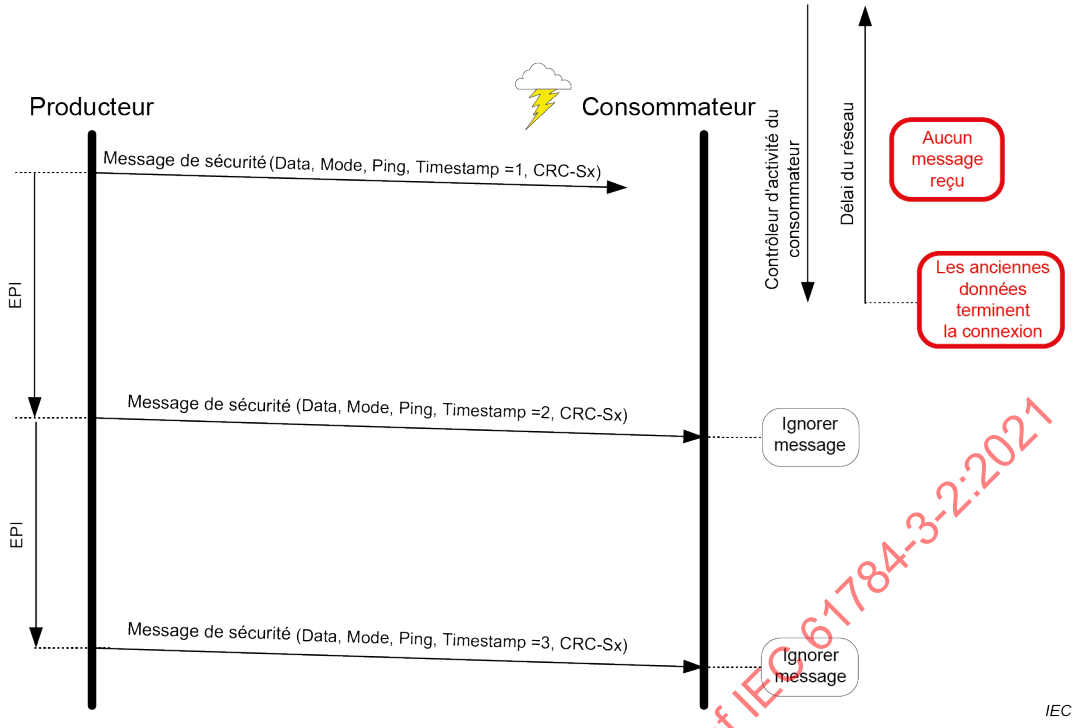


Figure 41 – Diagramme séquentiel d'un message producteur vers consommateur perdu

La transmission des messages peut être retardée. Si un message est retardé de sorte

- qu'il est reçu après le délai du contrôleur d'activité du consommateur (application déclenchée par la liaison), ou
- que l'âge des données dépasse le délai du réseau,

alors tous les messages ultérieurs sont ignorés, et il doit être mis fin à la connexion.

Dans les deux cas, le consommateur met fin à la connexion (voir 7.2.2) et passe à l'état de sécurité défini. Ce comportement est défini à la Figure 42.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

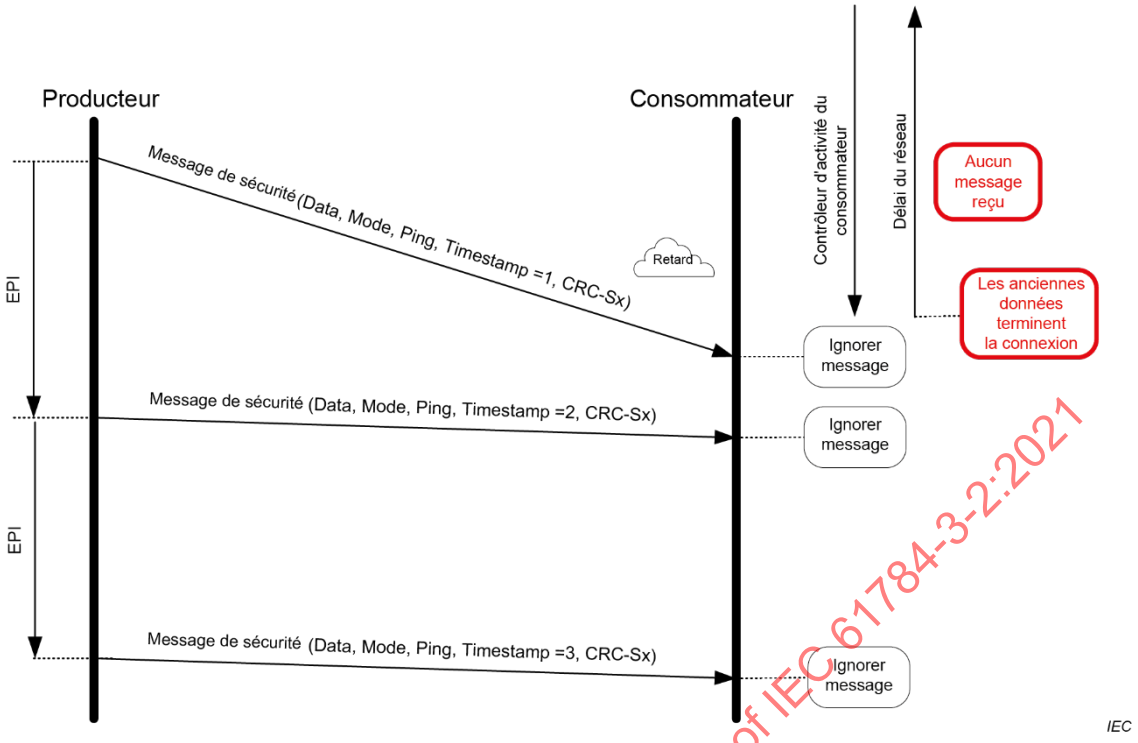


Figure 42 – Diagramme séquentiel d'un message retardé

7.5.4 Transmission de messages perdus, corrompus ou retardés avec production répétée

Il est possible, en raison de perturbations extérieures, que le message transmis du producteur au consommateur puisse être corrompu, comme défini à la Figure 43. La production peut être répétée afin de réduire le plus possible les déclenchements parasites et accroître la disponibilité du système entier.

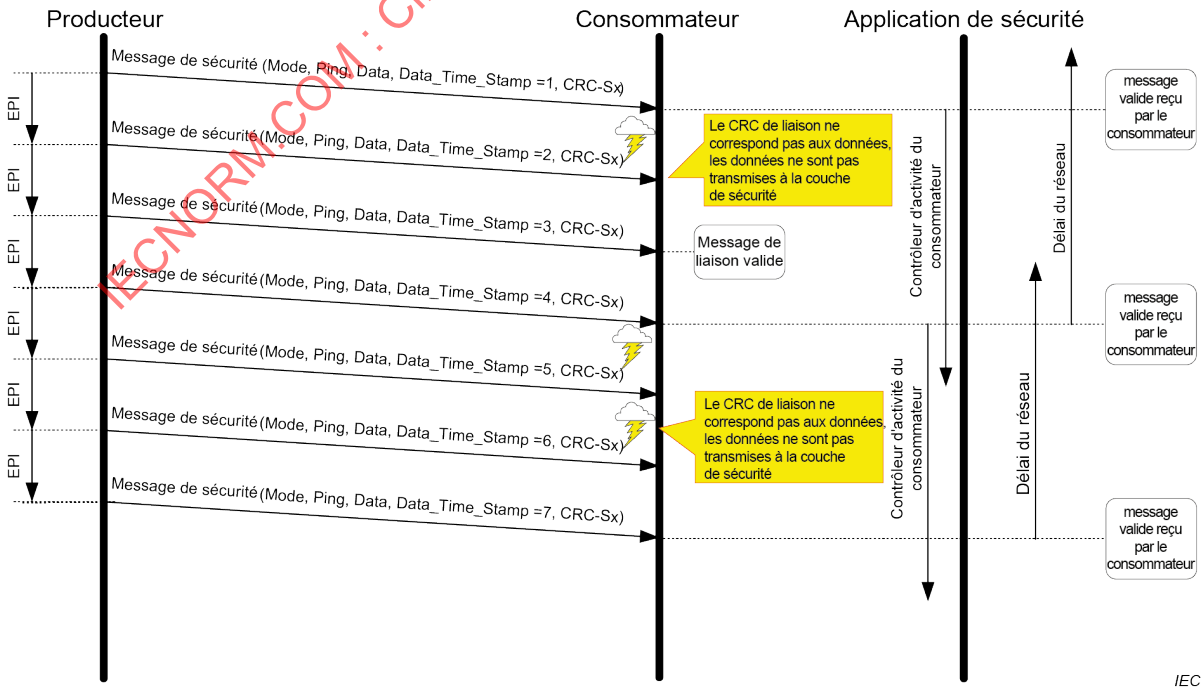


Figure 43 – Diagramme séquentiel d'un message producteur vers consommateur corrompu avec production répétée

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Si des erreurs sont détectées dans les couches normalisées, les messages peuvent être éliminés, tant qu'un message attendu valide est reçu dans le contrôleur d'activité du consommateur et que l'âge des données ne dépasse pas le délai du réseau.

Les messages répétés valides doivent être écrasés. L'application utilise le message valide le plus récent.

Il peut être possible, en raison de perturbations extérieures, qu'une série de messages soit retardée, ce qui entraîne la perte de la connexion. Cette séquence est définie à la Figure 44. Il est mis fin à la connexion si aucun message valide n'est reçu avant expiration du temporisateur périodique du consommateur (voir 7.2.2).

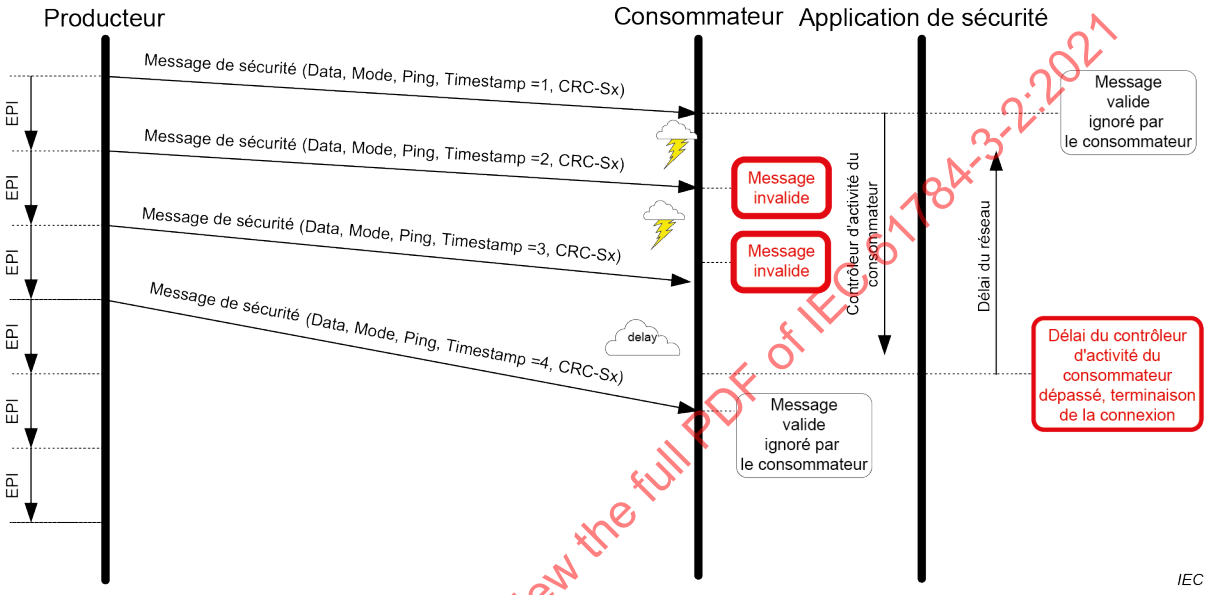


Figure 44 – Diagramme séquentiel d'une fin de connexion occasionnée par des retards

Un message de liaison valide qui ne satisfait pas au contrôle CRC de sécurité conduit le consommateur à prendre pour hypothèse que la liaison sous-jacente n'est pas fiable et, selon le format utilisé et/ou le nombre d'occurrences, peut provoquer la fin de la connexion. Cette séquence est définie à la Figure 45.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

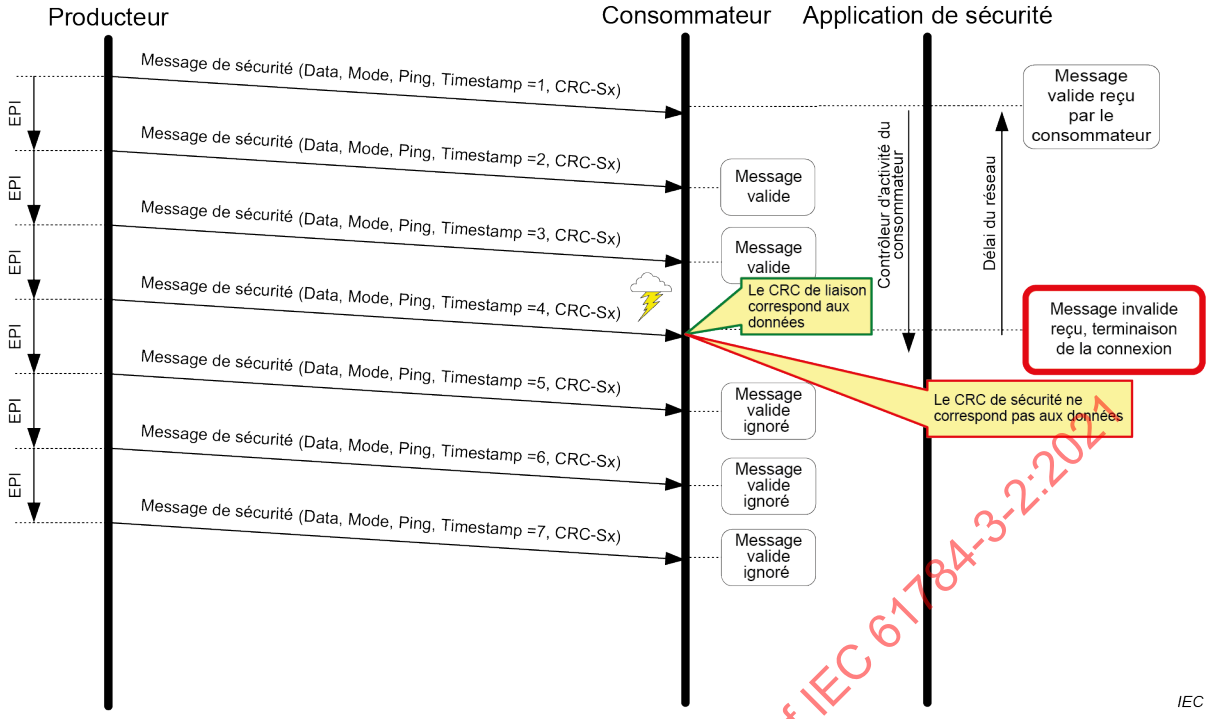


Figure 45 – Diagramme séquentiel d'un contrôle CRC de sécurité non satisfaisant

7.5.5 Demande Ping point à point

Une séquence de transaction de messages de demande et de réponse Ping permet de maintenir une temporisation cohérente entre producteurs et consommateurs. La description complète du producteur est donnée en 7.6.6 et celle du consommateur est donnée en 7.6.7. Cette séquence de messages pour une demande Ping point à point est définie à la Figure 46.

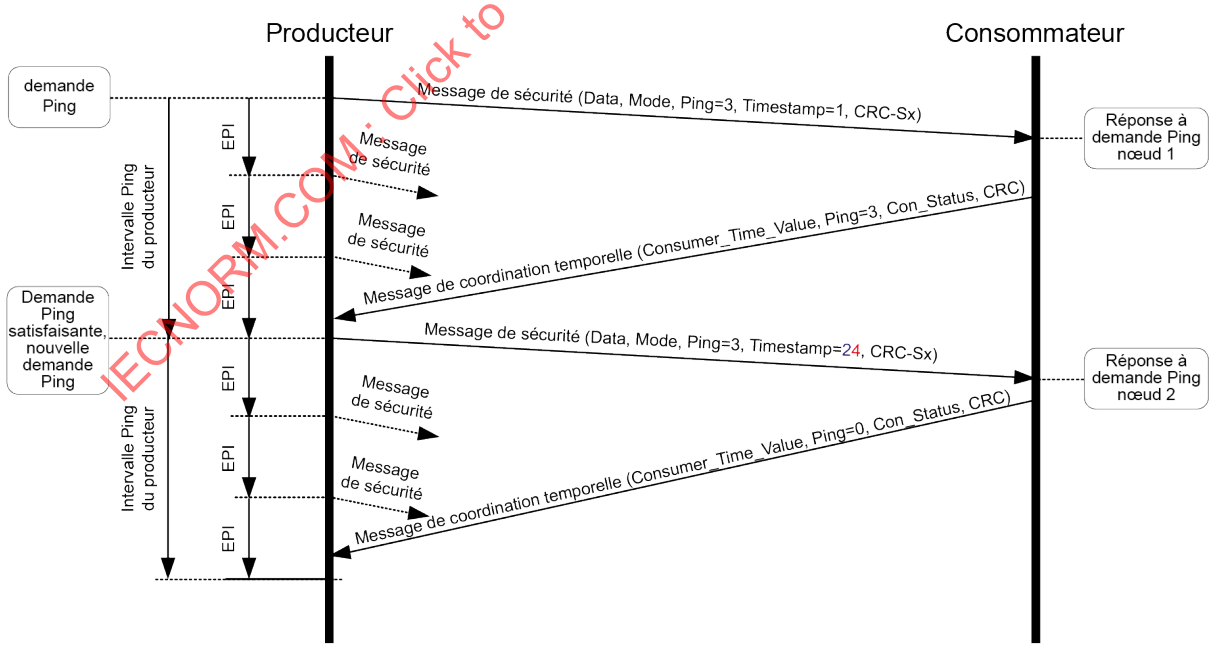


Figure 46 – Diagramme séquentiel d'une demande Ping point à point – réponse normale

A chaque intervalle Ping de producteur point à point, le nombre de demandes Ping doit être incrémenté dans l'en-tête de message de sécurité disponible suivant.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

L'intervalle Ping de producteur point à point doit être un multiple de l'EPI; les demandes Ping doivent être formulées à une fréquence qui repose sur le Ping_Interval_EPI_Mulitplier.

Lorsqu'un consommateur point à point constate une modification dans le nombre de demandes Ping, il génère un message de coordination temporelle.

Le message de coordination temporelle (voir 7.5.2) doit être reçu par le producteur dans un délai prescrit. Si le message de coordination temporelle n'est pas reçu dans ce délai, le producteur doit mettre fin à la connexion (voir 7.2.2).

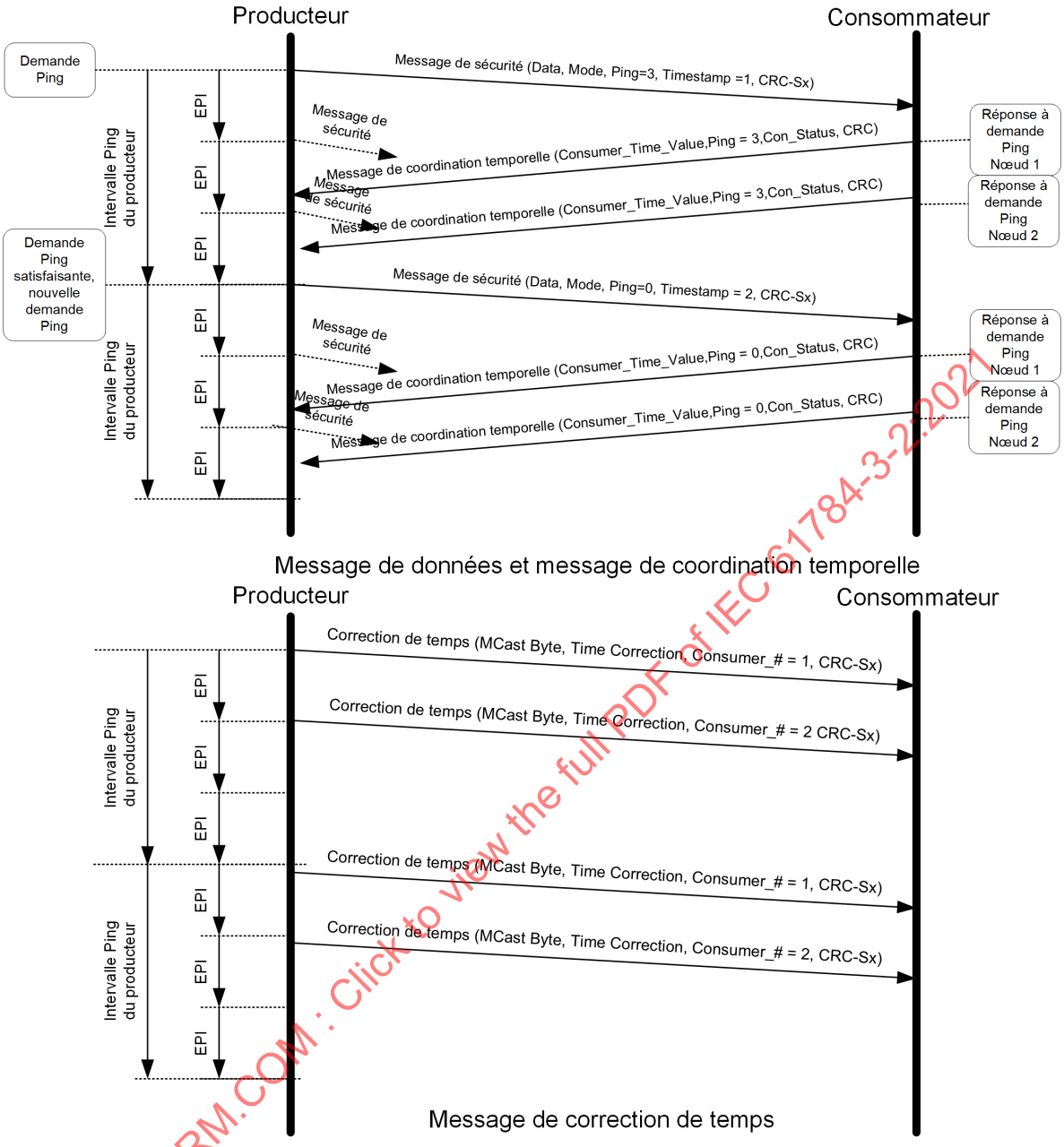
7.5.6 Demande Ping multipoint avec sécurité CP 2/3

Une séquence de transaction de messages de demande et de réponse Ping permet de maintenir une temporisation cohérente entre producteurs et consommateurs.

Pour les connexions multipoints de sécurité CP 2/3, un message distinct doit être utilisé pour communiquer les informations de correction de temps du producteur à chaque consommateur multipoint.

La description complète du producteur est donnée en 7.6.6 et celle du consommateur est donnée en 7.6.7. Cette séquence de messages pour une demande Ping multipoint est définie à la Figure 47. Le message de correction de temps est défini sur un autre diagramme pour des raisons de clarté.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021



IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Figure 47 – Diagramme séquentiel d'une demande Ping multipoint satisfaisante, sécurité CP 2/3

Pendant chaque intervalle Ping de producteur multipoint, une demande Ping est transmise par les producteurs multipoints aux consommateurs multipoints qui sollicitent une réponse.

Tous les consommateurs multipoints doivent répondre à une modification de la valeur de demande Ping, et les consommateurs autres que le consommateur 1 doivent attendre (Consumer_Number - 1) fois l'EPI pour répondre.

Tous les consommateurs multipoints doivent répondre dans le délai de l'intervalle Ping de la demande ou dans le délai de l'intervalle suivant.

Les messages de correction de temps doivent être transmis aux consommateurs multipoints à une fréquence qui permet d'assurer que chaque consommateur obtient un message de correction de temps dans un intervalle Ping de producteur unique.

7.5.7 Demande Ping multipoint sur les réseaux de sécurité CP 2/2

Une demande et une réponse à une demande Ping sont utilisées pour maintenir une temporisation entre les producteurs multipoints et leurs consommateurs. Pour les réseaux de sécurité CP 2/2, le message de correction de temps doit être concaténé au message de données de sécurité et transmis comme message unique. La description complète du producteur est donnée en 7.6.6 et celle du consommateur est donnée en 7.6.7. Cette séquence de messages pour une demande Ping multipoint est définie à la Figure 48.

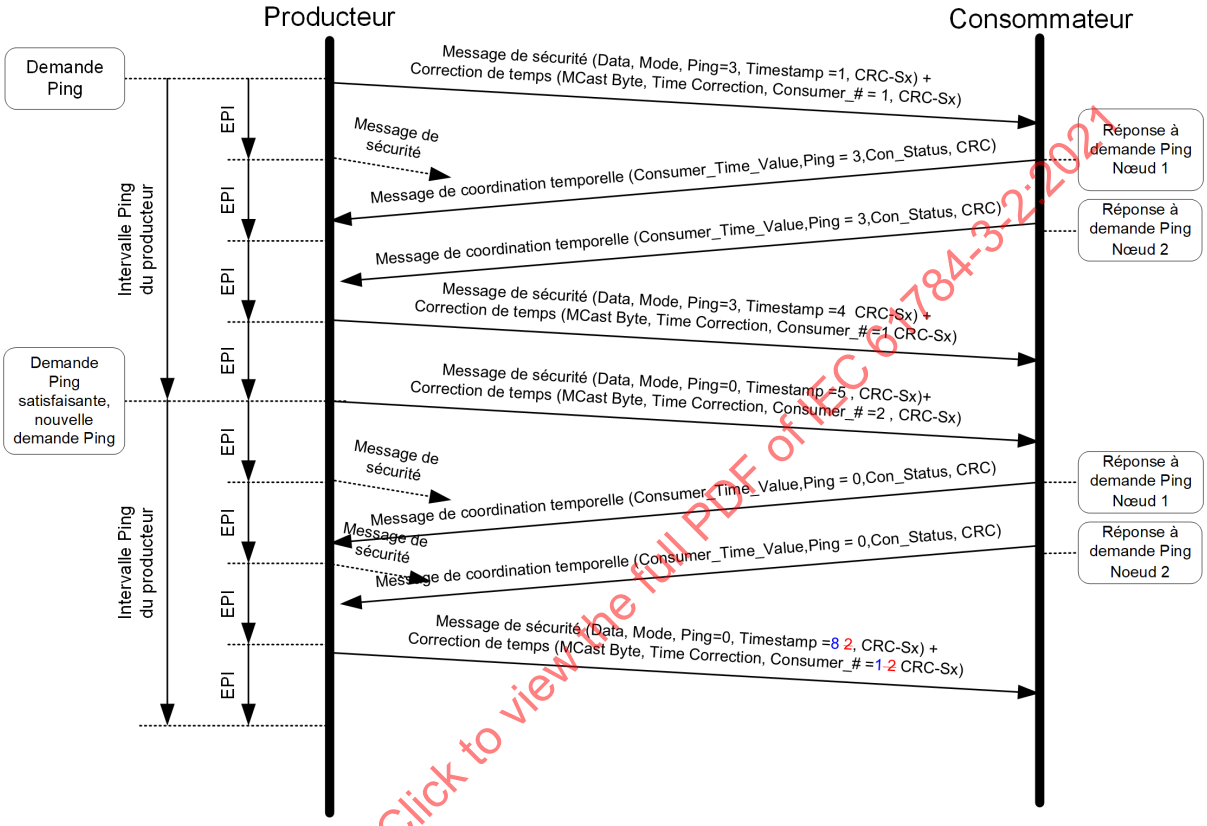


Figure 48 – Diagramme séquentiel d'une demande Ping multipoint satisfaisante, sécurité CP 2/2

Pendant chaque intervalle Ping de producteur, une demande Ping est transmise par les producteurs multipoints aux consommateurs multipoints qui sollicitent une réponse.

7.5.8 Demande Ping multipoint – Retransmission aboutie

Cette séquence de messages pour une demande Ping multipoint avec retransmissions est définie à la Figure 49. La connexion de correction de temps n'est pas définie pour des raisons de clarté.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

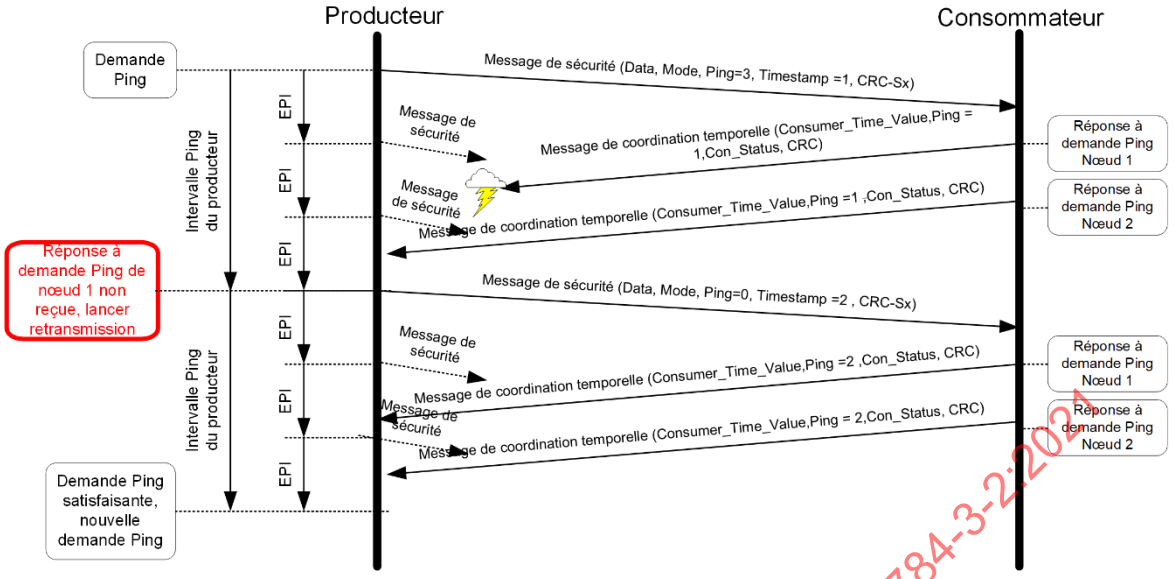


Figure 49 – Diagramme séquentiel d'une retransmission de demande Ping multipoint

Les pertes ou les retards de message de coordination temporelle multipoint après les intervalles Ping (Timeout_Multiplier.PI + 2) doivent entraîner la génération d'une erreur et la fermeture de la connexion.

7.5.9 Demande Ping multipoint – Retransmission avec temporisation

Cette séquence de messages pour une demande Ping multipoint avec retransmissions et temporisation est définie à la Figure 50. La connexion de correction de temps n'est pas définie pour des raisons de clarté.

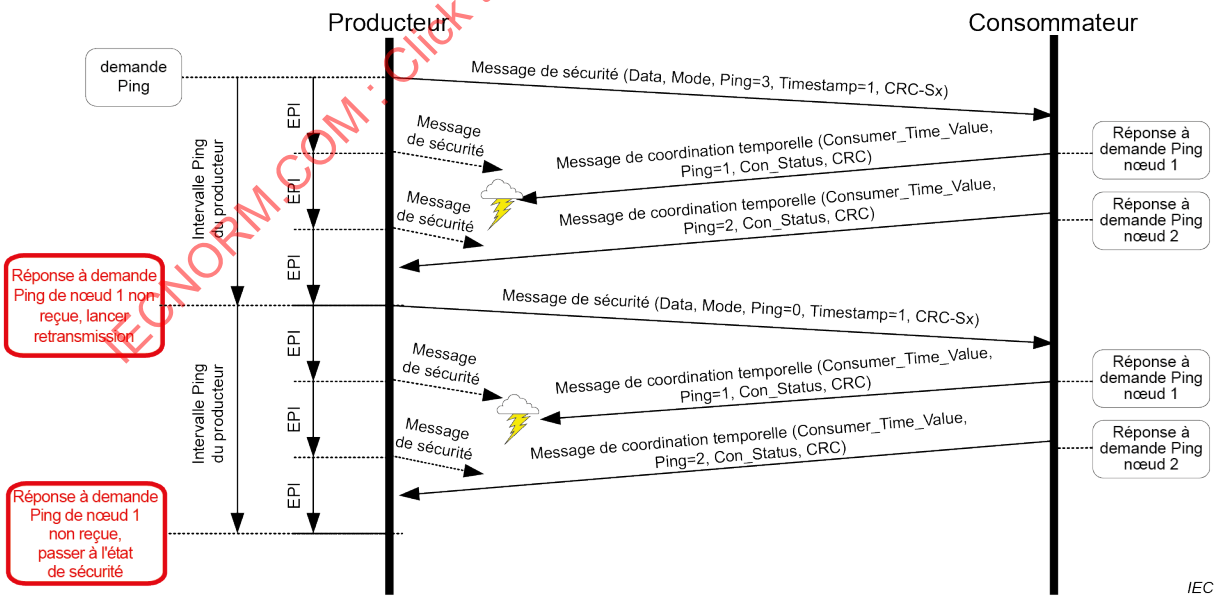


Figure 50 – Diagramme séquentiel d'une temporisation de demande Ping multipoint

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Si la réponse à une demande Ping demeure retardée, le producteur indique une anomalie de son état à destination du consommateur spécifique et le consommateur passe à l'état de sécurité défini. Si la demande Ping a été retardée en raison d'une anomalie du consommateur, ce dernier est déjà passé à un état de sécurité.

7.6 Définition du protocole de sécurité

7.6.1 Généralités

La couche de sécurité est une couche de service située entre la couche de transport CPF 2 normalisée et la couche d'application relative à la sécurité, comme cela est défini à la Figure 52. Il n'est pas nécessaire que cette couche de sécurité soit directement adressable dans le cadre CPF 2; il s'agit en revanche d'un comportement associé à une connexion entre les applications qui échangent des données de sécurité dans une application SIL3. Ce comportement est mis en œuvre en tant qu'Objet de validation de sécurité comme décrit en 6.7.

Plusieurs méthodes peuvent permettre de réaliser ce comportement souhaité. Les objets indiqués dans le présent 7.6 doivent être pris comme modèles de référence. Des produits et des applications individuels peuvent choisir de mettre en œuvre ce comportement, s'ils le jugent nécessaire. Cependant, il est nécessaire d'exprimer ce comportement ici de manière à constituer la base de développement des produits.

7.6.2 Vue de haut niveau d'un appareil de sécurité

La Figure 51 représente un certain nombre d'architectures de sécurité possibles qui peuvent utiliser le FSCP 2/1. Elle informe qu'il est possible d'utiliser n'importe quel niveau SIL de 1 à 3 avec le FSCP 2/1. Cependant, elle informe aussi que, dans tous les cas, la pile d'exécution et la configuration du FSCP 2/1 sont développées avec un processus de développement SC3. L'évaluation de la capabilité systématique, des exigences de niveau SIL et des mesures de non-interférence appropriées est effectuée par l'organisme de certification de sécurité.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

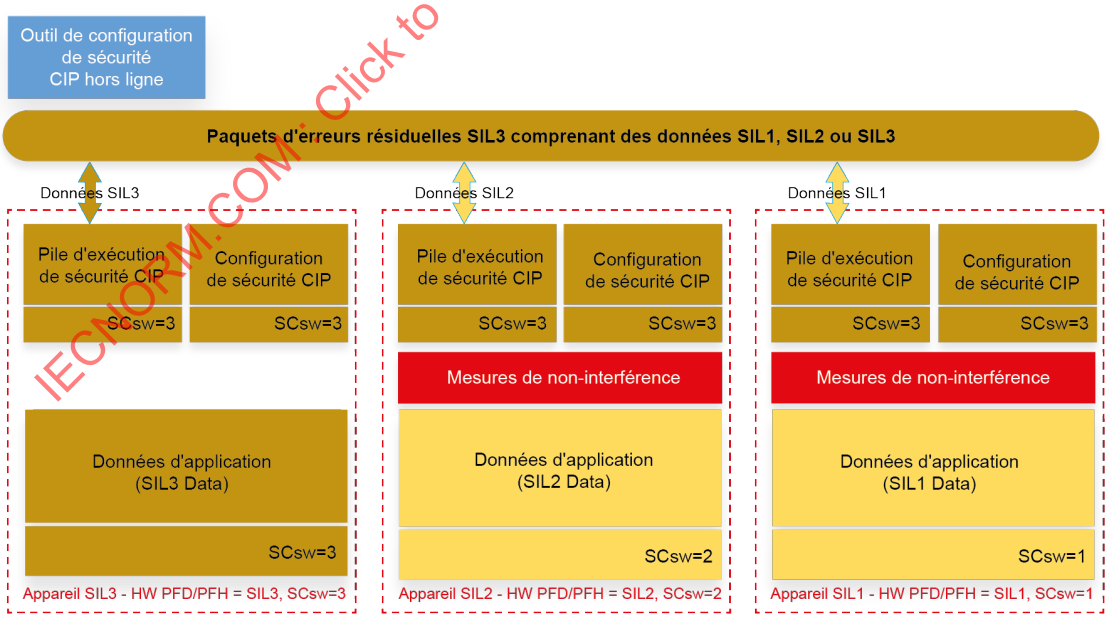


Figure 51 – Architectures de sécurité possibles pour le FSCP 2/1

La Figure 52 représente un exemple de modèle d'un appareil de sécurité SIL3 qui contient un ou plusieurs objets d'application relative à la sécurité. Chaque objet d'application relative à la sécurité fonctionne avec une paire d'objets de validation de sécurité afin d'échanger les données de sécurité entre la couche de transport CPF 2 et les circuits électroniques E/S de sécurité. Ces circuits électroniques sont conçus de manière à fournir un niveau de détection d'erreur et de localisation des anomalies adapté aux applications SIL3. Chacun des deux objets de validation de sécurité est associé à un canal de communication de réseau tel qu'un CP 2/3 ou CP 2/2. Cet exemple de modèle prend pour hypothèse une topologie de sécurité 1oo2 dans laquelle deux CPU indépendants participent au protocole de sécurité. Cependant, pour plusieurs architectures matérielles, la technologie FSCP 2/1 peut convenir à une utilisation dans des applications de sécurité inférieures au niveau SIL3.

Toutes les mises en œuvre de la technologie FSCP 2/1 doivent passer par un organisme de certification de la sécurité pour s'assurer que la conception et la mise en œuvre du protocole FSCP 2/1 (logiciel de communication lié à la sécurité) fournissent une capabilité systématique de niveau 3 (SC3) conformément à l'IEC 61508.

Le protocole FSCP 2/1 doit être considéré comme faisant partie d'un appareil complet, et l'intégration du protocole FSCP 2/1 dans l'appareil doit être achevée pour atteindre/maintenir la SC3. Par exemple, un fournisseur ne peut pas utiliser une pile FSCP 2/1 certifiée de manière distincte (une pile qui fournit un SIL3 et une SC3) dans son produit sans tenir compte de la nécessité de fournir une SC3 pour l'intégration du logiciel de communication de sécurité dans le produit intégré.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

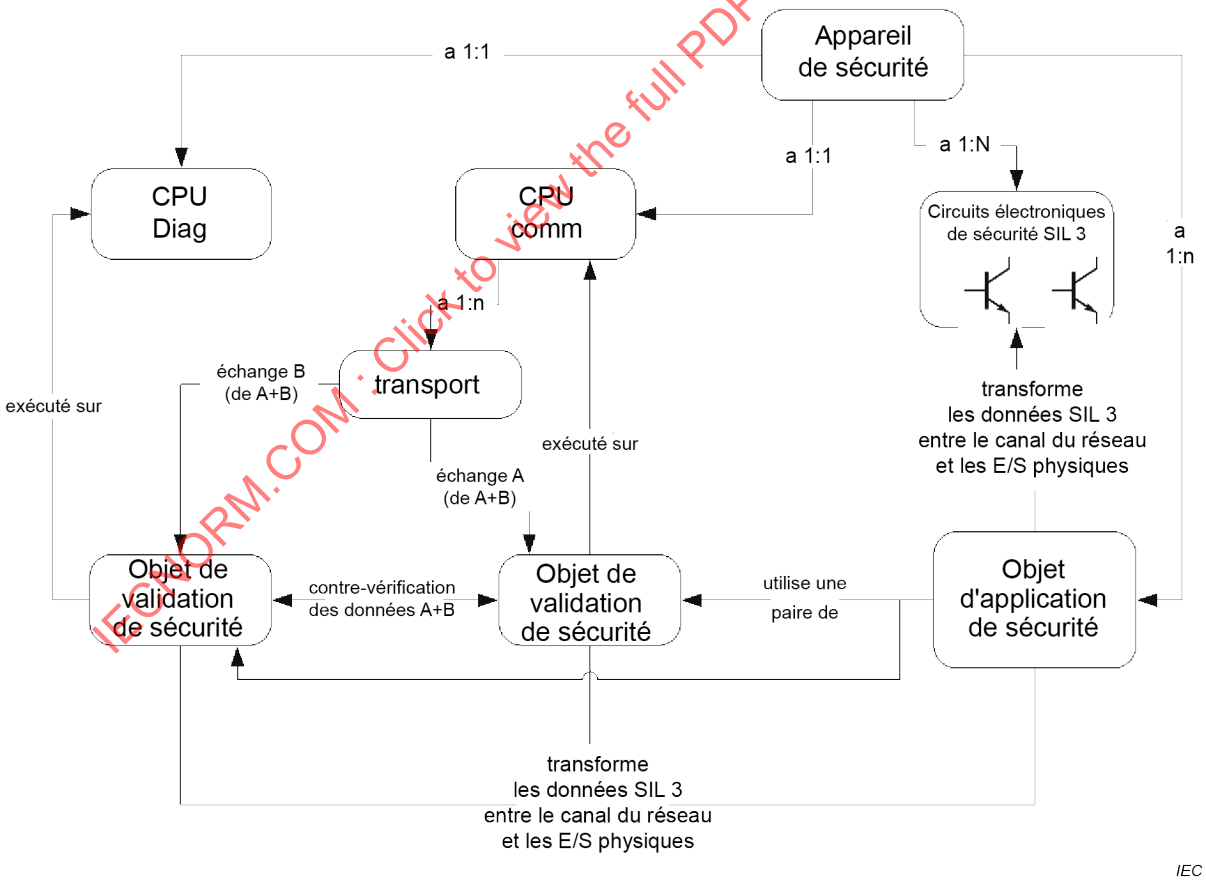


Figure 52 – Diagramme de relations des entités de modèle de référence d'un appareil de sécurité

7.6.3 Objet de validation de sécurité

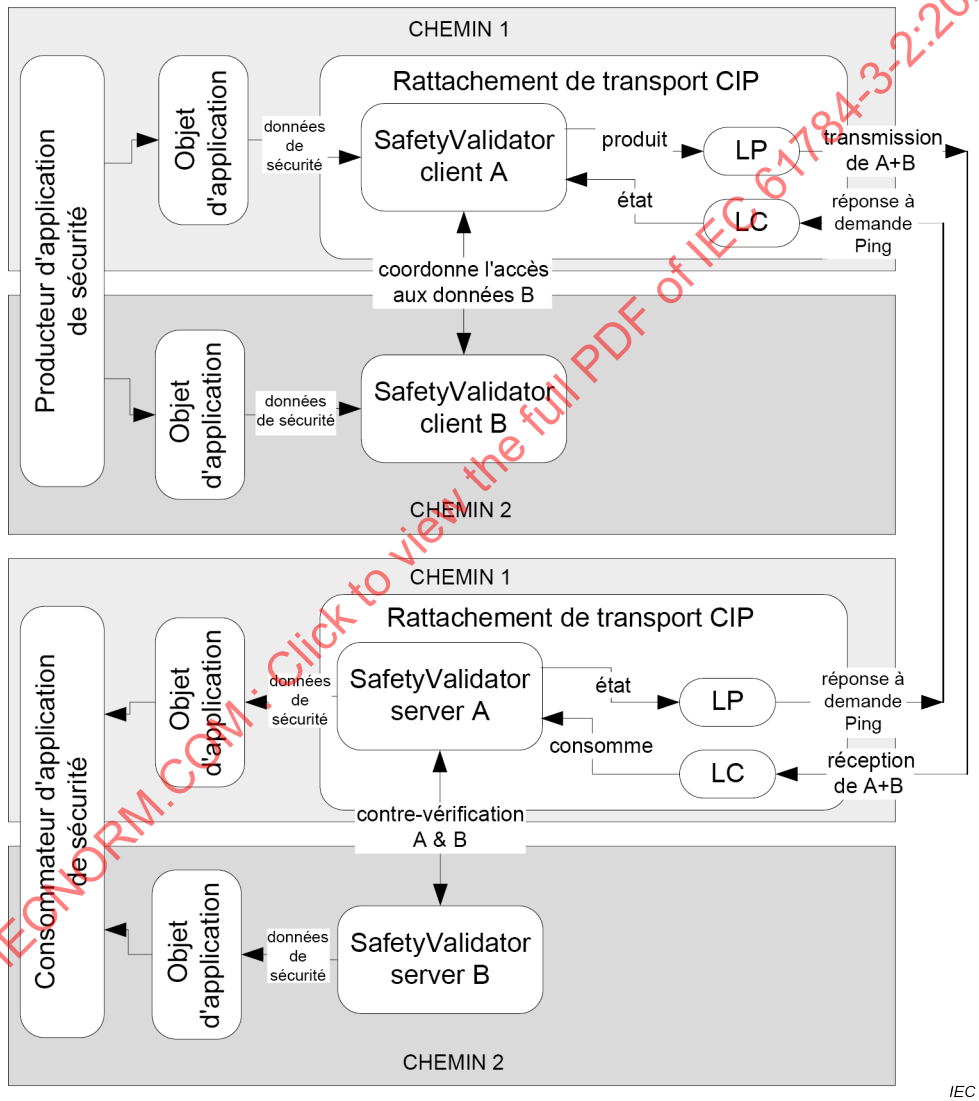
Le 6.7 définit un Objet de validation de sécurité à partir duquel les fonctions SafetyValidatorServer et SafetyValidatorClient sont mises en œuvre.

Les principes généraux et les attributs communs de ces deux fonctions de couche de sécurité sont définis en 7.6.4.

7.6.4 Relation entre SafetyValidatorServer et SafetyValidatorClient

La Figure 53 représente une vue de haut niveau de deux appareils qui échangent des données par l'intermédiaire des fonctions SafetyValidatorClient et SafetyValidatorServer. Une application de production de sécurité utilise une fonction SafetyValidatorClient pour transmettre des données de sécurité à une application de consommation de sécurité qui utilise une fonction SafetyValidatorServer.

NOTE Seul un des chemins redondants assure l'interface avec la couche de transport CPF 2. Les données A+B (réelles et complémentaires) sont encapsulées dans une trame de transport unique, et un seul processeur est impliqué dans la réception et la transmission des trames de données.



IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Figure 53 – Deux appareils qui échangent des données de sécurité par l'intermédiaire des fonctions SafetyValidatorClient et SafetyValidatorServer

7.6.5 Gestion du remplacement de la datation de format étendu

7.6.5.1 Généralités

Le format étendu exige une synchronisation coordonnée entre les producteurs et les consommateurs lors de l'établissement d'une connexion associée à des opérations de maintenance, afin de détecter et de gérer les événements de remplacement de datation. Ces opérations sont présentées de manière graphique pour chaque cas unique du 7.6.5.2 au 7.6.5.4. L'exemple de code présente également ces opérations dans leur ordre d'apparition dans le code.

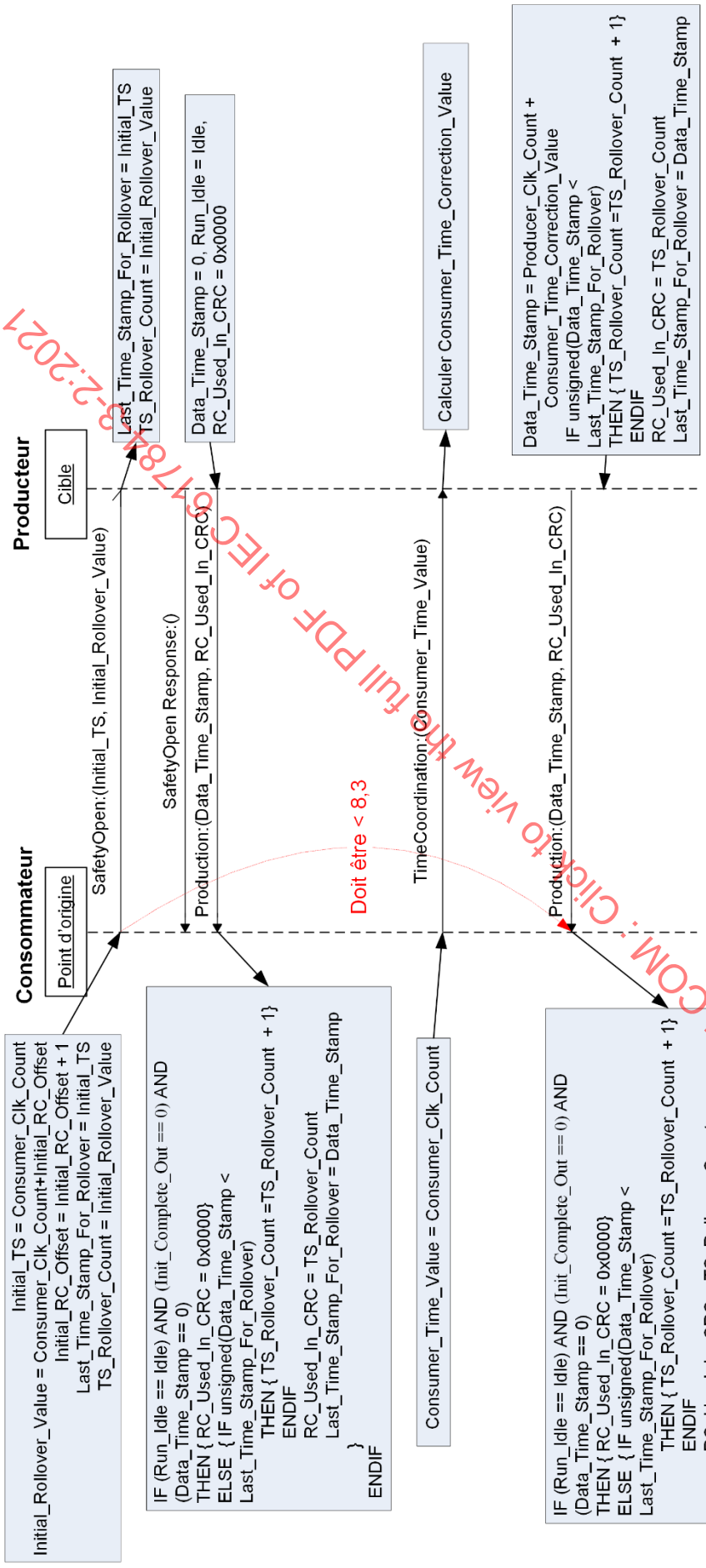
7.6.5.2 Consommateur d'origine et producteur cible point à point

Lorsque le consommateur est à l'origine des connexions point à point, il faut que le point d'origine fournisse des valeurs d'initialisation dans le service SafetyOpen. La cible utilise ces valeurs pour initialiser les paramètres de production.

Le comptage de remplacement utilisé dans le CRC point à point de format étendu doit être nul jusqu'à réalisation de l'échange de coordination temporelle initial.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Le processus complet est représenté à la Figure 54.



IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Figure 54 – Consommateur d'origine et producteur cible point à point

Le temps qui s'écoule entre la génération du service SafetyOpen et le traitement par les consommateurs du premier paquet produit après la réception par les producteurs du message Time_Coordination doit être inférieur à 8,3 s.

7.6.5.3 Producteur d'origine et consommateur cible point à point

Lorsque le producteur est à l'origine des connexions point à point de format étendu, le consommateur cible doit fournir les valeurs d'initialisation dans la réponse SafetyOpen. Le producteur d'origine utilise ces valeurs pour initialiser les paramètres de production.

Le processus complet est représenté à la Figure 55.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

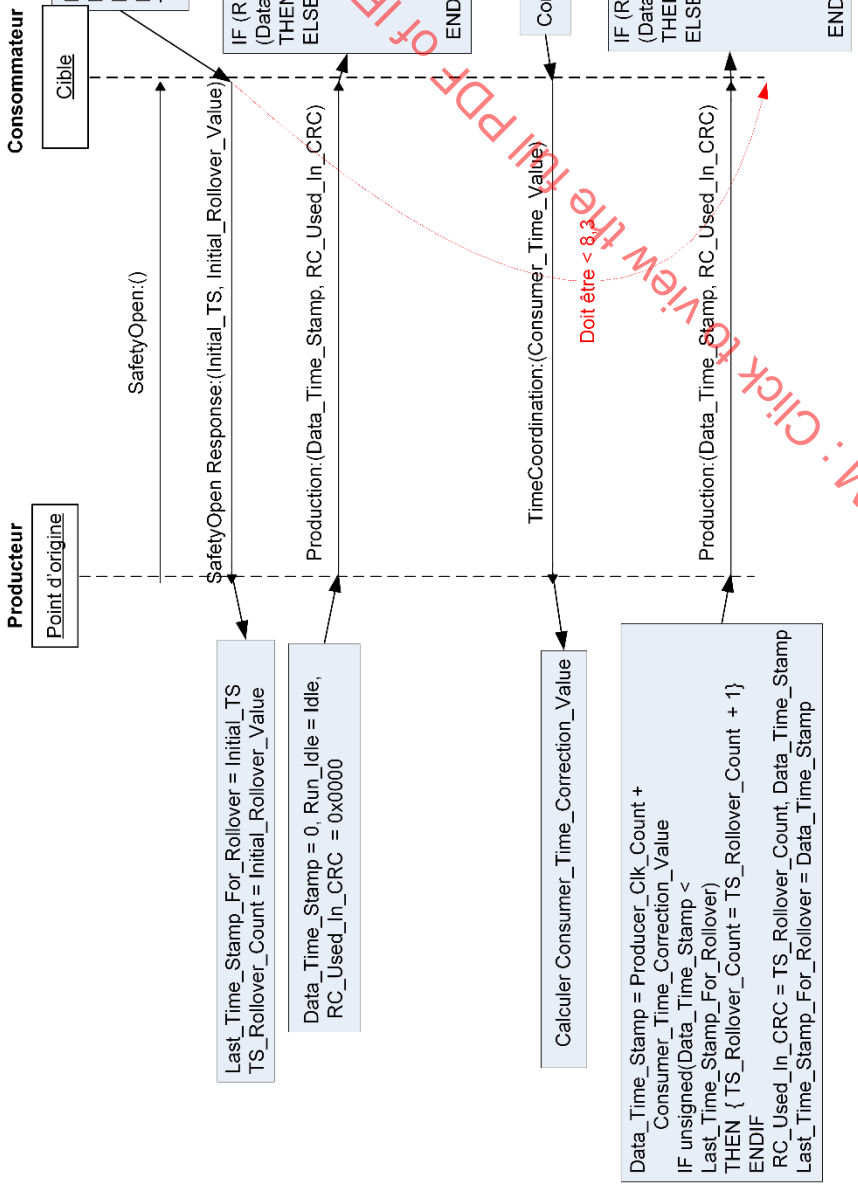


Figure 55 – Producteur d'origine et consommateur cible point à point

Le temps qui s'écoule entre la génération de la réponse SafetyOpen et le traitement par les consommateurs du premier paquet produit après la réception par les producteurs du message Time_Coordination doit être inférieur à 8,3 s.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

7.6.5.4 Consommateur d'origine et producteur cible multipoint

Lorsque le consommateur est à l'origine des connexions multipoints de format étendu, le producteur cible doit fournir les valeurs d'initialisation dans la réponse SafetyOpen. Le consommateur cible utilise ces valeurs pour initialiser les paramètres de production. Les valeurs que le producteur cible transmet dans la réponse SafetyOpen diffèrent selon que le premier consommateur sollicite ou non une connexion.

L'attribution active d'une valeur de départ au CRC par le comptage de remplacement dans les messages multipoints de format étendu doit commencer immédiatement à la première production.

Le processus complet est représenté à la Figure 56.

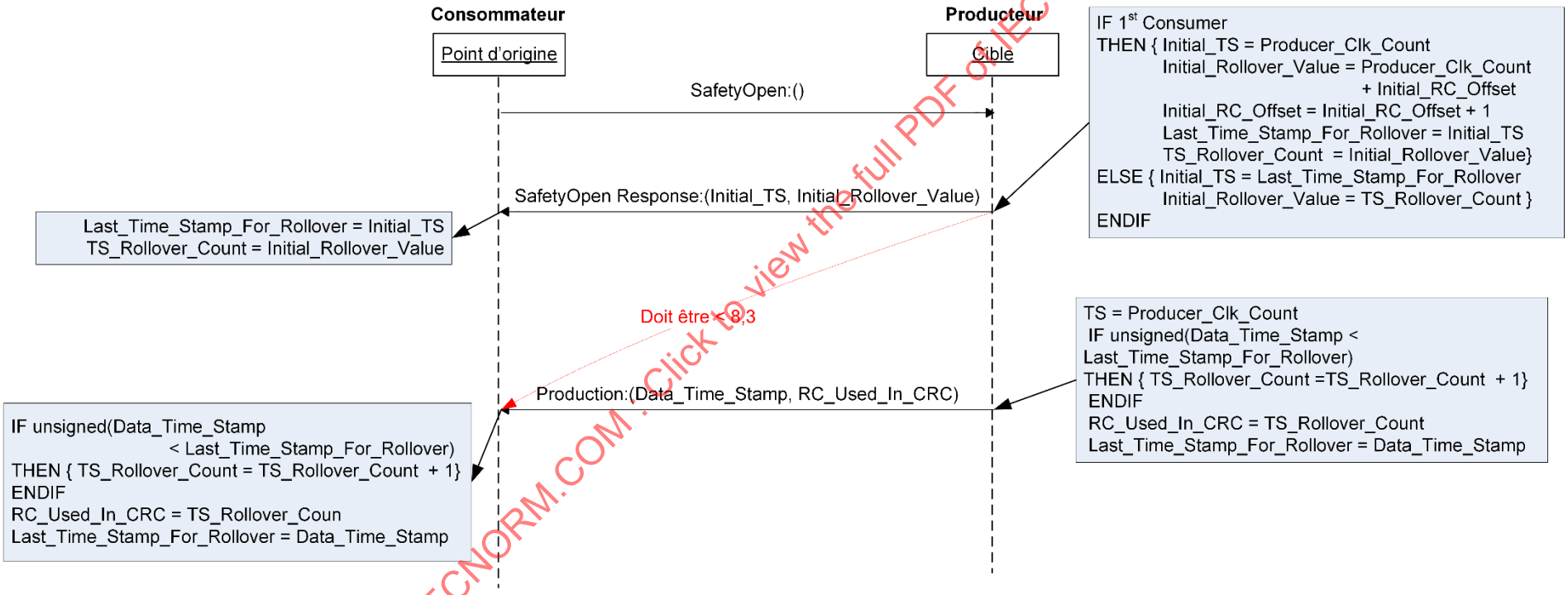


Figure 56 – Consommateur d'origine et producteur cible multipoint

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Le temps qui s'écoule entre la génération de la réponse SafetyOpen et le traitement par les consommateurs du premier paquet doit être inférieur à 8,3 s.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

7.6.6 Définition de la fonction SafetyValidatorClient

7.6.6.1 Généralités

La fonction SafetyValidatorClient constitue la représentation de la couche de sécurité qui augmente une connexion normalisée sur le CP 2/3 ou CP 2/2 afin de transmettre les données de sécurité. Elle coordonne la production des données d'application avec une instance homologue de la fonction SafetyValidatorServer.

7.6.6.2 Production de sécurité

Le présent 7.6.6 décrit la production des données et les interfaces entre l'application, la fonction SafetyValidatorClient et la couche de liaison sous-jacente. Le comportement d'exécution de SafetyValidatorClient et de ses interfaces constitue l'objet du présent paragraphe. L'application proprement dite doit présenter une intégrité élevée pour satisfaire le niveau SIL cible, ce qui peut être accompli de nombreuses manières et constitue une décision de conception finale du fournisseur.

La Figure 57 représente graphiquement le flux de données entre la fonction SafetyValidatorClient et une application relative à la sécurité de production. Safety_Data_Out est produit à une fréquence périodique, désignée comme l'Intervalle de paquets attendu (EPI). La fonction SafetyValidatorClient doit échantillonner, saisir et horodater les données à transmettre à chaque période EPI.

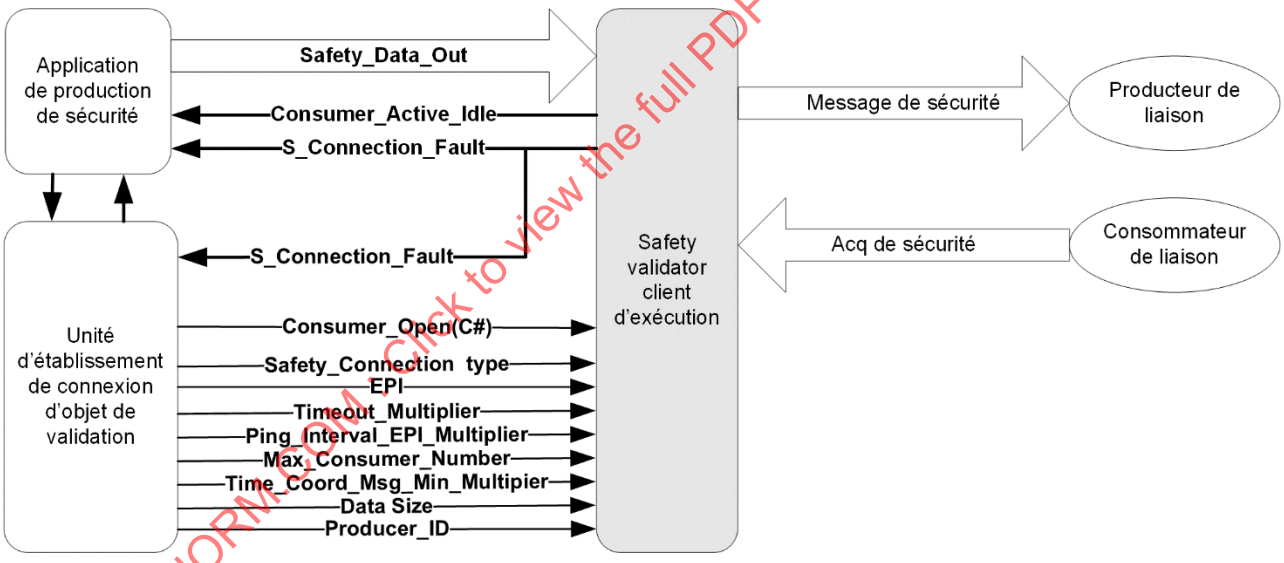


Figure 57 – Flux de données de production de sécurité

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

7.6.6.3 Interface d'application de production

L'application de production fournit Safety_Data_Out à la fonction SafetyValidatorClient. La fonction SafetyValidatorClient doit générer les Mode_Octet, Actual_Data et Complement_Data, ainsi que la section de datation.

La fonction SafetyValidatorClient doit renvoyer l'état de connexion de sécurité à l'application de production pour chaque consommateur.

7.6.6.4 Logique de production des données de sécurité

La logique que tous les producteurs de données de sécurité doivent suivre est décrite du 7.6.6.4 au 7.6.6.8. La mise en œuvre réelle de la logique peut varier, mais des résultats équivalents doivent être obtenus. Il est admis par hypothèse que la logique définie dans le présent document présente une application de production asynchrone qui met les données de sécurité à disposition de la fonction SafetyValidatorClient.

Les définitions relatives aux variables utilisées dans la logique de production de données de sécurité peuvent être consultées en 7.7.

7.6.6.5 Exemple de logique d'amorçage (démarrage) à froid pour la production des données de sécurité

La logique de production dédiée à l'initiation d'un amorçage à froid d'une connexion est la suivante:

```
////////////////////////////////////////////////////////////////
// Cold start after connection establishment processing
////////////////////////////////////////////////////////////////
// This Logic should be executed at the transition of the
//  producing connection from closed to open.
// For Point-to-point connections this logic may
//  be performed any time the connection is Opened or Re-Opened.
////////////////////////////////////////////////////////////////

Ping_Interval_EPI_Count = 0,
RR_Con_Num_Index_Pntr = Max_Consumer_Number,

// Initialize the ping count in the safety message to 0
Mode_Octet.Ping_Count = 0,

// Time_Drift_Per_Ping_Interval, the minimum value is 1
Time_Drift_Per_Ping_Interval =
Roundup(EPI × Ping_Interval_EPI_Multiplier / 320000,

FOR (Consumer_Num = 1 to Max_Consumer_Number),
{
      // Producer Dynamic Variables
      Consumer_Active_Idle[Consumer_Num-1] = Idle,
      S_Connection_Fault[Consumer_Num-1] = OK,
      Producer_Rcved_Time_Value[Consumer_Num-1] = 0x0000,
      Consumer_Time_Correction_Value[Consumer_Num-1] = 0x0000,
     Ping_Int_Since_Last_Time_Coord_Msg_Count[Consumer_Num-1] = 0x0000,
      Consumer_Time_Value[Consumer_Num-1] = 0x0000

      // Producer Derived Variables

      // Time_Drift_Constant, the minimum value is 1.
(Time_Drift_Constant is not
      // saved but is used in the calculation of the
      // Connection_Correction_Constant below.)
      Time_Drift_Constant =
                  Roundup((Timeout_Multiplier[Consumer_Num-1] +1)×EPI ×
                        Ping_Interval_EPI_Multiplier / 320000),

      // Connection_Correction_Constant
      Connection_Correction_Constant[Consumer_Num-1] =
Time_Drift_Constant + 1 – Time_Coord_Msg_Min_Multiplier [Consumer_Num-
1],

      // Time_Coord_Response_EPI_Limit
```

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

```
      Time_Coord_Response_EPI_Limit[Consumer_Num-1]= Roundup((5000000 +
                  (Time_Coord_Msg_Min_Multiplier[Consumer_Num-1]×128) +
                  (EPI × ( Consumer_Num – 1))) / EPI),

      // Time_Coord_Response_EPI_Limit has a maximum value of 1000
      IF (Time_Coord_Response_EPI_Limit[Consumer_Num-1] > 1000),
      THEN
      {
            Time_Coord_Response_EPI_Limit[Consumer_Num-1] = 1000,
      }
      ENDIF
}
ENDFOR

////////////////////////////////////////////////////////////////////
// end, Cold start after connection establishment processing
////////////////////////////////////////////////////////////////////
```

7.6.6.6 Exemple de logique de réamorçage d'un consommateur multipoint pour la production des données de sécurité

Cette logique permet l'arrêt et le réamorçage de chaque consommateur multipoint, tandis que la production multipoint destinée à d'autres consommateurs se poursuit.

Le présent 7.6.6.6 définit la logique nécessaire pour réamorcer un consommateur individuel, mais il ne représente pas une mise en œuvre efficace de la méthode de détection du réamorçage de la connexion individuelle.

```
////////////////////////////////////////////////////////////////
// Re-initialization of Multipoint production to individual consumers
////////////////////////////////////////////////////////////////
// This Logic should be executed after a multipoint consumer performs
//  a successful open to a multipoint producer while the production
//  is in process to re-initialize production to that consumer number
////////////////////////////////////////////////////////////////
FOR (Consumer_Num = 1 to Max_Consumer_Number),
{
IF (Consumer_Open(Consumer_Num-1)transitions from Closed to Open)
  THEN
  {
      // Producer Dynamic Variables
       Consumer_Active_Idle[Consumer_Num-1] = Idle,
       S_Connection_Fault[Consumer_Num-1] = OK,
       Producer_Rcved_Time_Value[Consumer_Num-1] = 0x0000,
       Consumer_Time_Correction_Value[Consumer_Num-1] = 0x0000,
       Ping_Int_Since_Last_Time_Coord_Msg_Count[Consumer_Num-1= 0x0000,

       // Producer Derived Variables
       // Time_Drift_Constant, the minimum value is 1
       //(Time_Drift_Constant is not
       // saved but is used in the calculation of the
       // Connection_Correction_Constant below.)
       Time_Drift_Constant =
      Roundup((Timeout_Multiplier[Consumer_Num-1] +1) × EPI ×
                        Ping_Interval_EPI_Multiplier / 320000),
      // Connection_Correction_Constant
       Connection_Correction_Constant[Consumer_Num-1] =
```

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

```
      Time_Drift_Constant + 1 – Time_Coord_Msg_Min_Multiplier
[Consumer_Num-1],
       // Time_Coord_Response_EPI_Limit
       Time_Coord_Response_EPI_Limit[Consumer_Num-1= Roundup((5000000 +
                 (Time_Coord_Msg_Min_Multiplier[Consumer_Num-1]×128) +
                 (EPI × ( Consumer_Num – 2))) / EPI),

       // Time_Coord_Response_EPI_Limit has a maximum value of 1000
       IF (Time_Coord_Response_EPI_Limit[Consumer_Num-1] > 1000),
       THEN
        {
             Time_Coord_Response_EPI_Limit[Consumer_Num-1] = 1000,
        }
       ENDIF
      }
ENDIF
}
```

7.6.6.7 Exemple de production de données combinée

La logique exigée commune de la fonction SafetyValidatorClient pour toutes les connexions de sécurité est présentée ci-dessous.

```
////////////////////////////////////////////////////////////////
// start of EPI Safety Data production processing
////////////////////////////////////////////////////////////////
// This logic assumes that the application has passed the Safety
//  Data and Application_Run_Idle to the Safety Validator.
//
////////////////////////////////////////////////////////////////
// Capture the time to be used for the time stamp
Producer_Safe_Data_TS = Producer_Clk_Count,

// Check if it is time to increment the Ping Count
Ping_Interval_EPI_Count = Ping_Interval_EPI_Count + 1,

IF (Ping_Interval_EPI_Count >= Ping_Interval_EPI_Multiplier),
THEN
{
Increment Mode_Octet.Ping_Count,
Ping_Interval_EPI_Count = 0,
}
ENDIF

// Set the remainder of the Mode_Octet bits
Mode_Octet.Run_Idle = Application_Run_Idle,
Mode_Octet.TBD_Bit  = 0,
Mode_Octet.TBD_2_Bit  = 0,

// Execute the safety producer, connection type specific functions
IF (Connection_Type == multipoint),
THEN
{
multi_cast_producer_function(),
}
ELSE
{
single_cast_producer_function(),
}
ENDIF
```

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

```
// set Mode_Octet redundant bits (2:4) to the correct values
Mode_Octet = (Mode_Octet AND 0xe3)OR((Mode_Octet>>3) AND 0x1c XOR
0x14),
Calculate Data Section CRC,
Calculate Time_Stamp Section CRC,
Trigger the sending of the Data Message,

// If on FSCP 2 on CP 2/3 and Multipoint, send the Time Correction
//  Message if it is time.
IF ((Connection_Type == CP 2/3) AND
(Send_Time_Correction_Message == 1)),
THEN
{
Trigger the sending of the Time Correction Message,
Send_Time_Correction_Message = 0,
}
ENDIF
////////////////////////////////////////////////////////////////
// end of safety data production processing
////////////////////////////////////////////////////////////////


////////////////////////////////////////////////////////////////
// Start of point-to-point production function
////////////////////////////////////////////////////////////////
single_cast_producer_function()
// Check if a Time Coordination message has been received in
//  the allotted time.
IF (Ping_Interval_EPI_Count == 8),
THEN
{
Increment Ping_Int_Since_Last_Time_Coord_Msg_Count[0],
IF (Ping_Int_Since_Last_Time_Coord_Msg_Count[0]
>= (Timeout_Multiplier[0] + 2)),
     THEN
{
     S_Connection_Fault[0]=Faulted,
}
ENDIF
}
ENDIF

//Hold Data_Time_Stamp = 0 until time coordination msg received
IF(Consumer_Active_Idle[0] == Idle),
THEN
{
Mode_Octet.Run_Idle = Idle,
Time_Stamp_Section.Data_Time_Stamp = 0x0000,
}
ELSE
{
Time_Stamp_Section.Data_Time_Stamp = Producer_Safe_Data_TS +
Consumer_Time_Correction_Value[0],
}
ENDIF

END single_cast_ producer_function()
////////////////////////////////////////////////////////////////
// end of point-to-point processing
////////////////////////////////////////////////////////////////
```

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

```
////////////////////////////////////////////////////////////////
// Start of multipoint production function
////////////////////////////////////////////////////////////////
multi_cast_producer_function()
// Check if its time to start sending Time Correction messages
// Time Correction messages are sent starting at the 8th EPI
production
//  within the Ping interval
IF (Ping_Interval_EPI_Count == 8),
THEN
{
RR_Con_Num_Index_Pntr = 0,
}
ENDIF

// Check if a Time Coordination message has been received in
//  the allotted time.
IF (RR_Con_Num_Index_Pntr < Max_Consumer_Number),
THEN
{
Increment
Ping_Int_Since_Last_Time_Coord_Msg_Count[RR_Con_Num_Index_Pntr],
IF (Ping_Int_Since_Last_Time_Coord_Msg_Count[RR_Con_Num_Index_Pntr]
            >= (Timeout_Multiplier[RR_Con_Num_Index_Pntr] + 2)),
THEN
{
     Set S_Connection_Fault[RR_Con_Num_Index_Pntr]=Faulted,
}
ENDIF
ENDIF

// Check if its time to send an active non-error Time Correction
//  message
IF ((RR_Con_Num_Index_Pntr < Max_Consumer_Number) AND
   (Consumer_Active_Idle[RR_Con_Num_Index_Pntr] == Active)), AND
   (Consumer_Open[RR_Con_Num_Index_Pntr] == Open) AND
   (S_Connection_Fault[RR_Con_Num_Index_Pntr] == OK)
THEN
{
Send_Time_Correction_Message = 1,
Mcast_Octet.Consumer_# = RR_Con_Num_Index_Pntr + 1,
Mcast_Octet.Multi_Cast_Active_Idle =
Consumer_Active_Idle[RR_Con_Num_Index_Pntr],
Time_Correction_Section.Time_Correction_Value =
Consumer_Time_Correction_Value[RR_Con_Num_Index_Pntr],
 Set Mcast_Octet.Parity_Even to the correct value,
MCast_Octet_2 = ((MCast_Octet XOR 0xFF) AND 0x55) OR
(MCast_Octet AND 0xAA)
Calculate CRC of time correction message,
}
ELSE
{
//load null TIME_CORRECTION Section,
Mcast_Octet.Consumer_# = 0,
Mcast_Octet.Multi_Cast_Active_Idle = Idle,
Time_Correction_Section.Time_Correction_Value = 0,
 Set Mcast_Octet.Parity_Even to the correct value,
MCast_Octet_2 = ((MCast_Octet XOR 0xFF) AND 0x55) OR
 (MCast_Octet AND 0xAA)
Calculate CRC of time correction section,
}
ENDIF
```

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

```
// If Time Correction messages are being sent, increment to the
//  next consumer
IF (RR_Con_Num_Index_Pntr < Max_Consumer_Number),
THEN
{
RR_Con_Num_Index_Pntr = RR_Con_Num_Index_Pntr + 1,
}
ENDIF

// Set the time stamp value
Time_Stamp_Section.Data_Time_Stamp = Producer_Safe_Data_TS,
END multi_cast_producer_function()
////////////////////////////////////////////////////////////////
// end of multipoint processing
////////////////////////////////////////////////////////////////
```

7.6.6.8 Exemple de logique de réception des messages de coordination temporelle

La fonction SafetyValidatorClient doit accomplir les étapes suivantes pour chaque message de coordination temporelle reçu. Pour les connexions de sécurité point à point et multipoints, le message de coordination temporelle reçoit une Consumer_Time_Value.

Les producteurs doivent permettre la réception des réponses de coordination temporelle au cours du Ping_Interval ou du Ping_Interval + 1.

```
////////////////////////////////////////////////////////////////
//Time Coordination message reception processing
////////////////////////////////////////////////////////////////
// Consumer_Num equals 1 for point to point
// Consumer_Num equals the consumer the message
//  was received from for multipoint
////////////////////////////////////////////////////////////////
// This Logic should only be executed If Ack_Byte.Ping_Response
//  of the message is equal to 1 AND Consumer_Open[Consumer_Num-1]
//  is equal to Open. If Ack_Byte.Ping_Response is equal to 0 OR
//  Consumer_Open[Consumer_Num-1]is equal to Closed, this
//  message should be ignored.
////////////////////////////////////////////////////////////////
// reject Time Coordination packets if CONSUMER_TIMESTAMP has
// previously been captured AND this is not the first time
// coordination message from this consumer
IF (  (Consumer_Time_Value[Consumer_Num-1] ==
Time_Coordination_Section.Consumer_Time_Value)  AND
        (Consumer_Active_Idle[Consumer_Num-1] == Active) )
THEN
{
        // the only time this would be the case is if that Time
Coordination was already received
        Abort the processing of this packet. Do Not close the
connection.
}
ENDIF


// Capture the received time
Producer_Rcved_Time_Value[Consumer_Num-1] = Producer_Clk_Count,

// Perform the integrity checks
Check the CRC of the Time Coordination Section, based on format used,
Ack_Byte_Error = false,
IF ((Ack_Byte parity incorrect)
THEN
{
```

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

```
Ack_Byte_Error = true,
}
ENDIF
IF (BaseFormat)
THEN
{
//ckeck Ack_Byte_2 if BaseFormat
IF ((Ack_Byte parity incorrect) OR (Ack_Byte_2 !=
   (((Ack_Byte XOR 0xFF) AND 0x55) OR (Ack_Byte AND 0xAA))))
THEN
{
Ack_Byte_Error = true,
}
ELSE
{
Ack_Byte_Error = false,
}
ENDIF
ENDIF
IF ((CRC_Error based on format used) OR (Ack_Byte_Error = true) OR
// Ensure that the Time Coordination message returned
//  with the same ping interval or the next ping interval.
//  The next ping interval is allowed for the case that a
//  multipoint consumer connects to an existing producer.
//  If the new consumer receives its first message near the end
//  of the ping interval, the time coordination may arrive back
//  at the producer during the next ping interval.
     ((Ack_Byte.Ping_Count_Reply != Ping_Count) AND
      (Ack_Byte.Ping_Count_Reply != Ping_Count-1)) OR
// Ensure that the Time Coordination message returned
//  within the approximatley 5 second limit
((Consumer_Active_Idle[Consumer_Num-1] == Active) AND
 (Ping_Interval_EPI_Count >
           Time_Coord_Response_EPI_Limit[Consumer_Num-1])),
THEN
{
IF (ExtendedFormat),
THEN
{
//decide whether to close the connection or not
Increment Producer_Fault_Counter[Consumer_Num-1]
IF (Producer_Fault_Counter[Consumer_Num-1] >=
Max_Fault_Number[Counsumer_Num-1])
THEN
{
S_Connection_Fault[Consumer_Num-1] = Faulted,
Abort the processing of this packet. Close the connection.
}
ELSE
{
Abort the processing of this packet. Do Not close the connection.
}
ENDIF
}
ELSE
{
S_Connection_Fault[Consumer_Num-1] = Faulted,
Abort the processing of this packet. Close the connection.
}
ENDIF
}
ENDIF
```

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

```
// at this point we know we have a good, non-redundant time
coordination packet

// Capture the received CONSUMER time
Consumer_Time_Value[Consumer_Num-1] =
           Time_Coordination_Section.Consumer_Time_Value;

// Determine the worst case Consumer_Time_Correction_Value based on
the
//  received Time_Coordination section
Worst_Case_Consumer_Time_Correction_Value[Consumer_Num-1] =
      Time_Coordination_Section.Consumer_Time_Value
      - Producer_Rcved_Time_Value[Consumer_Num-1]
- Connection_Correction_Constant[Consumer_Num-1],

// Determine the worst case time drift since the last
//  Time Coordination information was received. This is equal to the
//  number of Ping Intervals since the last Time Coordination message
//  times the Time Drift per Ping Interval plus 1 for the asyncronous
//  clocks. This value will not be used until the second
//  Time_Coordination message is recived.

Time_Drift_Since_Last_Time_Coord =
({Ping_Int_Since_Last_Time_Coord_Msg_Count[Consumer_Num-1]+ 1}
  * Time_Drift_Per_Ping_Interval) + 1,

// If this Time_Coordination Transport delay is greater then the
//  last Time_Coordination Transport delay by more than the
appropriate
//  number of Time_Drift_Per_Ping_Intervals, then, use the previous
//  Correction value minus the appropriate number of
//  Time_Drift_Per_Ping_Intervals. This action is not taken until the
//  second Time_Coordination message is received.
// The math for this check should be 16 bit or greater
IF ((Consumer_Active_Idle[Consumer_Num-1] == Active) AND
((Consumer_Time_Correction_Value[Consumer_Num-1]-
       Worst_Case_Consumer_Time_Correction_Value[Consumer_Num-1] –
 Time_Drift_Since_Last_Time_Coord) AND 0x8000 == 0)),
THEN
{
Consumer_Time_Correction_Value[Consumer_Num-1] =
Consumer_Time_Correction_Value[Consumer_Num-1] -
Time_Drift_Since_Last_Time_Coord,
}
ELSE
{
Consumer_Time_Correction_Value[Consumer_Num-1] =
Worst_Case_Consumer_Time_Correction_Value[Consumer_Num-1],
}
ENDIF

// Set the flag indicating a Time_Coordination message has been
received
IF (S_Connection_Fault[Consumer_Num-1] = OK)
THEN
{
Consumer_Active_Idle[Consumer_Num-1] = Active,
}
ENDIF

// Reset the Time_Coordination message timer
Ping_Int_Since_Last_Time_Coord_Msg_Count[Consumer_Num-1] = 0,
////////////////////////////////////////////////////////////////
```

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

```
// end producer time coordination information reception processing
//////////////////////////////////////////////////////////////////
```

7.6.7 Définition de la fonction SafetyValidatorServer

7.6.7.1 Généralités

La fonction SafetyValidatorServer constitue la couche de sécurité qui augmente une connexion normalisée sur le CP 2/3 ou CP 2/2 afin de transmettre les données de sécurité. Elle coordonne la réception des données de sécurité avec une instance homologue de la classe SafetyValidatorClient et fournit ces données à l'application relative à la sécurité de consommation.

7.6.7.2 Consommation de sécurité

Le présent 7.6.7 décrit la consommation des données et les interfaces entre l'application, la fonction SafetyValidatorServer et la couche de liaison sous-jacente.

Il existe deux versions de contrôle des consommateurs de données de sécurité. A savoir:

- SafetyValidatorServer – déclenchée par la liaison.
  Ceci convient aux applications de consommation synchronisées sur la réception des données, ou aux applications de consommation qui présentent un retard continu par rapport à la réception des données;
- SafetyValidatorServer – déclenchée par l'application.
  Ceci convient aux applications de consommation à caractère périodique et non synchronisées sur la réception des données.

Dans les deux versions, la fonction SafetyValidatorServer doit exécuter les aspects suivants du contrôle des données de sécurité:

- coordination temporelle avec le producteur;
- vérification de l'intégrité de la section de datation;
- vérification de l'intégrité des données;
- vérification du délai du réseau.

7.6.7.3 SafetyValidatorServer – déclenchée par la liaison

La Figure 58 représente les flux de données applicables à la fonction SafetyValidatorServer dans le mode déclenché par la liaison.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

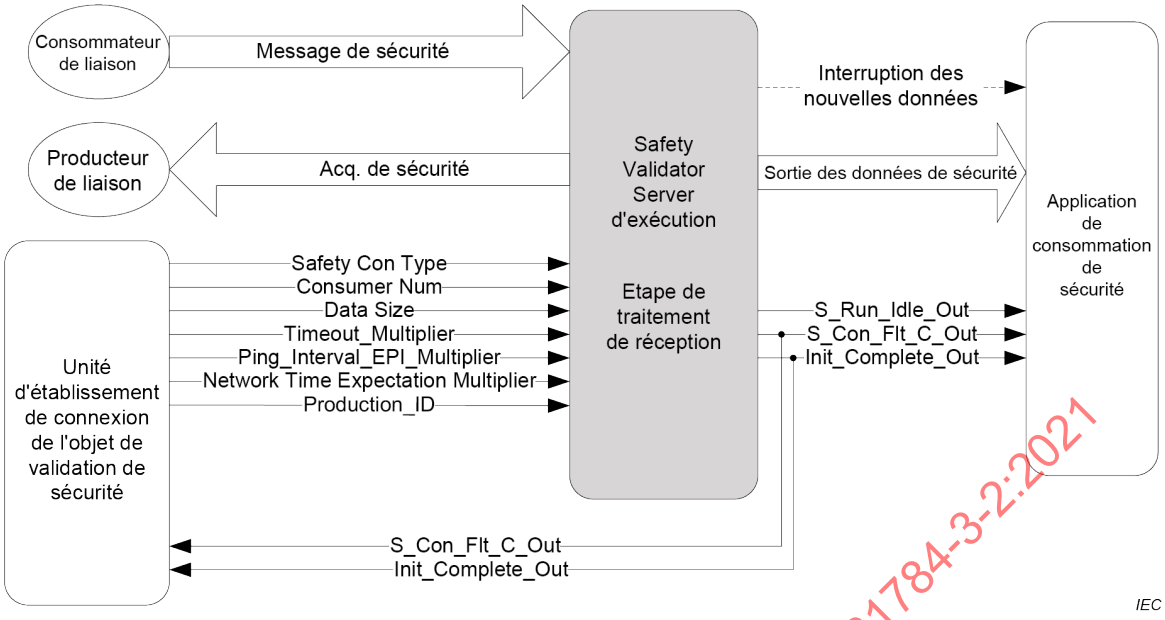


Figure 58 – Contrôle des données de sécurité de consommation

La fonction SafetyValidatorServer déclenchée par la liaison doit exécuter tous les aspects du protocole de sécurité sur chaque message reçu.

Pour les connexions multipoints, la fonction SafetyValidatorServer déclenchée par la liaison doit également exécuter tous les aspects du protocole de sécurité sur chaque section Time_Correction reçue.

La fonction SafetyValidatorServer doit s'assurer de la contre-vérification des données de sécurité présentées à l'application de consommation et du respect du délai du réseau.

La fonction SafetyValidatorServer déclenchée par la liaison doit définir le nouveau drapeau de données chaque fois que les données sont prêtes à être utilisées.

7.6.7.4 SafetyValidatorServer – déclenchée par l'application

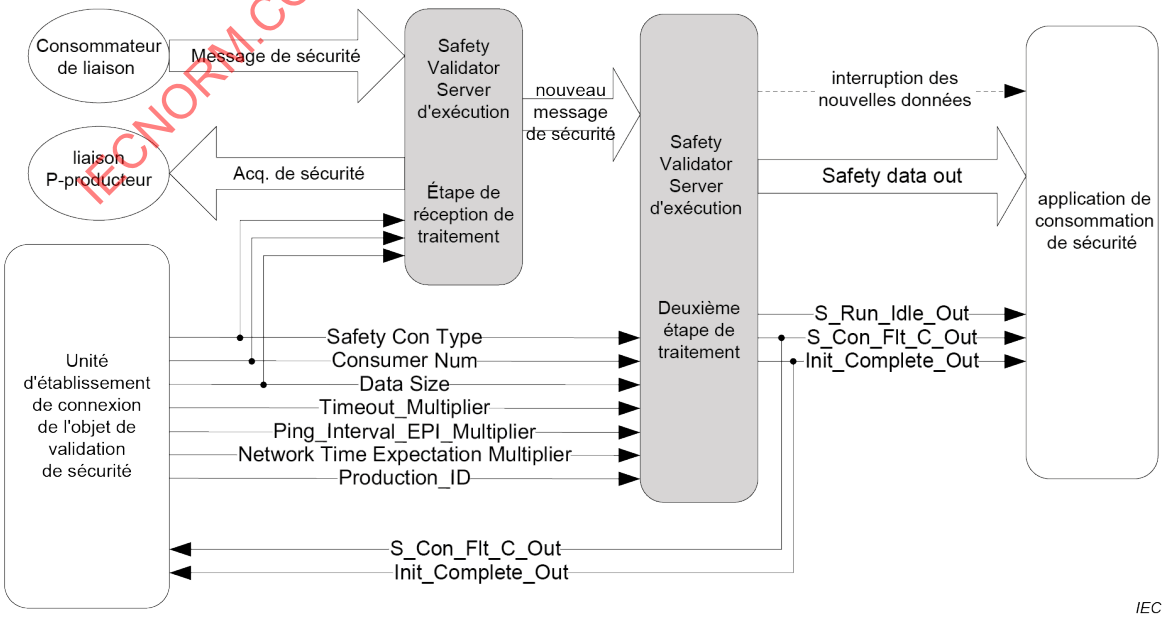


Figure 59 – SafetyValidatorServer – déclenchée par l'application

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

La fonction SafetyValidatorServer déclenchée par l'application ne traite pas entièrement chaque message.

L'étape de réception de traitement de la fonction SafetyValidatorServer déclenchée par l'application doit vérifier le nombre de demandes Ping pour tous les messages de données entrants.

Pour la consommation multipoint des fonctions SafetyValidatorServer déclenchées par l'application, la toute dernière section Time_Correction reçue doit être transmise à l'application de consommation.

L'application de consommation relative à la sécurité doit solliciter de nouvelles données auprès de la fonction SafetyValidatorServer afin que ce dernier effectue le traitement d'un message.

Dans le cas des applications périodiques non synchronisées sur la réception des données, ceci réduit la charge de traitement, dans la mesure où la section de données fait uniquement l'objet d'une contre-vérification (dans la deuxième étape de traitement de la Figure 59 pour les messages de données de sécurité utilisés). Ceci est particulièrement utile pour le cas où les EPI de réseau présentent une fréquence plus rapide que la fréquence périodique de l'application de consommation.

L'application de consommation doit s'assurer qu'elle obtient de nouvelles données au moins une fois toutes les 2 s afin de s'assurer que la datation n'est pas remplacée.

7.6.7.5 Logique de réception des données de sécurité

Le processus de réception des données de sécurité comprend:

- un contrôle Ping_Count;
- un contrôle de la section de datation;
- vérification de l'intégrité des données;
- un contrôle de la datation;
- la déduction de Run_Idle et de l'état d'anomalie.

Les définitions des variables utilisées dans la logique de réception des données de sécurité peuvent être consultées en 7.7.7.6.

Le Tableau 95 définit les étapes de traitement des données de sécurité exécutées par la fonction SafetyValidatorServer déclenchée par la liaison.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Tableau 95 – Réception des données – Déclenchée par la liaison

	Point à point	Multipoint
Contrôle de Ping_Response	Non	Non
Contrôle de Ping_Count	Oui	Oui
Contrôle du CRC de la section de datation	Oui	Oui
Contrôle de Run_Idle	Oui	Oui
Contrôle de TBD_Bit	Oui	Oui
Contrôle des CRC de données	Oui	Oui
Contrôle des données réelles/complémentaires	Oui	Oui
Déduction de Data_Time_Stamp	Oui	Oui

Le Tableau 96 définit les étapes de traitement des données de sécurité qui doivent être exécutées par la fonction SafetyValidatorServer déclenchée par la liaison pour la réception de chaque section de correction de temps.

Tableau 96 – Réception de Time_Correction – Déclenchée par la liaison

Multipoint	Multipoint
Contrôle de MCast_Octet et MCast_Octet_2	Oui, si concordance de consumer_#
Contrôle du CRC de Time_Correction	Oui, si concordance de consumer_#
Obtention de Time_Correction_Value	Oui, si concordance de consumer_#
Contrôle de Multi_Cast_Active_Idle	Oui, si concordance de consumer_#

Le Tableau 97 définit les étapes de traitement des données de sécurité exécutées à la réception de chaque message par la fonction SafetyValidatorServer déclenchée par l'application.

Tableau 97 – Réception des données – Déclenchée par l'application

	Point à point	Multipoint
Contrôle de Ping_Response	Non	Non
Contrôle de Ping_Count	Oui	Oui
Contrôle du CRC de la section de datation	Non	Non
Contrôle de Run_Idle	Non	Non
Contrôle de TBD_Bit	Non	Non
Contrôle des CRC de données	Non	Non
Contrôle des données réelles/complémentaires	Non	Non
Déduction de Data_Time_Stamp	Non	Non

Le Tableau 98 définit les étapes de traitement des données de sécurité qui doivent être exécutées à réception de chaque section Time_Correction par les fonctions SafetyValidatorServer déclenchées par l'application.

Tableau 98 – Réception de Time_Correction – Déclenchée par l'application

	Multipoint
Contrôle de MCast_Octet et MCast_Octet_2	Transmission du message si concordance de consumer_#
Contrôle du CRC de Time_Correction	Non
Obtention de Time_Correction_Value	Non
Contrôle de Multi_Cast_Active_Idle	Non

Le Tableau 99 définit les étapes de traitement des données de sécurité exécutées par la fonction SafetyValidatorServer déclenchée par l'application, en cas de sollicitation des données de sécurité.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

Tableau 99 – Application de consommation – Contrôle des données de sécurité

	Point à point	Multipoint
Contrôle de Ping_Response	NA	NA
Contrôle de Ping_Count	NA	NA
Contrôle du CRC de la section de datation	Oui	Oui
Contrôle de MCast_Octet et MCast_Octet_2	NA	Oui (à partir de la dernière correction de temps)
Contrôle du CRC de Time_Correction	NA	Oui (à partir de la dernière correction de temps)
Obtention de Time_Correction_Value	NA	Oui (à partir de la dernière correction de temps)
Contrôle de Multi_Cast_Active_Idle	NA	Oui (à partir de la dernière correction de temps)
Contrôle de Run_Idle	Oui	Oui
Contrôle de TBD_Bit	Oui	Oui
Contrôle des CRC de données	Oui	Oui
Contrôle des données réelles/complémentaires	Oui	Oui
Déduction de Data_Time_Stamp	Oui	Oui

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

7.6.7.6 Contrôle des comptages de demandes Ping

La fonction SafetyValidatorServer doit contrôler le Ping_Count à chaque message. Le contrôle de Ping_Count vérifie le comptage des demandes Ping pour déterminer s'il a varié.

Si une fonction SafetyValidatorServer détecte une variation du comptage des demandes Ping, il doit produire un message de coordination temporelle dans cet intervalle Ping ou dans un délai de 5 s, selon la plus courte durée.

Il convient de ne pas traiter les erreurs de contrôle de Ping_Count comme des défaillances dangereuses. Il n'est pas nécessaire de vérifier le CRC de la section de datation pour effectuer le contrôle du Ping_Count.

7.6.7.7 Intervalle maximal de vérification des données et du délai du réseau

L'intégrité des données doit faire l'objet d'un contrôle au moins une fois toutes les 2 s.

La datation et le délai du réseau (NTE) doivent faire l'objet d'un contrôle au moins une fois toutes les 2 s.

7.6.7.8 Exemple d'initialisation d'amorçage à froid

```
////////////////////////////////////////////////////////////////
// Cold start after connection establishment processing
////////////////////////////////////////////////////////////////
// This Logic should be executed at the transition of the
//  consuming connection from closed to open.
////////////////////////////////////////////////////////////////

S_Con_Flt_C_Out = OK,
Init_Complete_Out = 0,
S_Run_Idle_Out = Idle,

Last_Ping_Count = 3,
Time_Coordination_Count_Down = 0x0000,
```

```
Corrected_Data_Time_Stamp = 0x0000,
Last_Data_Time_Stamp = 0x0000,
Last_Rcved_Multi_Cast_Active_Idle  = Idle,
Last_Rcved_Time_Correction_Value  = 0x0000,
Time_Correction_Ping_Interval_Count = 0x0000,
Time_Correction_Received_Flag = 0,
Data_Age = 0x0000,
Max_Data_Age = 0x0000,
////////////////////////////////////////////////////////////////
// end, Cold start after connection establishment processing
////////////////////////////////////////////////////////////////
```

7.6.7.9 SafetyValidatorServer – logique déclenchée par la liaison

Les 7.6.7.10 et 7.6.7.11 décrivent la logique de réception des données de sécurité du consommateur pour la fonction SafetyValidatorServer déclenchée par la liaison. L'expression "déclenchée par la liaison" signifie que la logique dans son ensemble est exécutée à chaque réception.

Le 7.6.7.10 décrit la logique combinée associée à la réception des paquets de données de sécurité pour les types de connexions de sécurité point à point et multipoints.

Le 7.6.7.11 décrit la logique associée à la réception des messages de correction de temps pour le type de connexion de sécurité multipoint.

Cette logique ne doit être exécutée qu'en cas d'ouverture de la connexion sans aucune erreur.

7.6.7.10 Exemple de logique de réception combinée – logique déclenchée par la liaison

La logique suivante est la logique de réception de SafetyValidatorServer exigée pour la réception des paquets de données de sécurité du type de connexion de sécurité point à point ou multipoint, pour la logique SafetyValidatorServer déclenchée par la liaison.

Les connexions multipoints doivent transmettre un message de coordination temporelle (Consumer_Num – 1) réceptions après variation du nombre de demandes Ping.

Les consommateurs multipoints qui se connectent à un producteur existant doivent transmettre le message Time_Coordination immédiatement à la première réception valide.

```
////////////////////////////////////////////////////////////////
// Safety Data Consumption – link triggered logic
////////////////////////////////////////////////////////////////

// If the Extended  Format is being used, we shall determine a
rollover value to
// be used when calculating CRCs before we attempt to validate the
message
// (since the rollover is part of CRC values in the message).
IF (ExtendedFormat),
THEN
{
// For point to point, a time_stamp other than 0 or a Run
//  indication, indicate that the Time_Coordination_Message has been
//  received by the Client and the corrected time stamp is being used.
IF ((Point to point) AND  (Init_Complete_Out == 0) AND
(Time_Stamp_Section.Data_Time_Stamp == 0) AND
      (Mode_Byte.Run_Idle == IDLE)),
```

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

```
THEN
{
      RC_Used_in_CRC  = 0x0000,
}
ELSE
{
RC_Used_in_CRC  = TS_Rollover_Count,

// check for time stamp rollover
IF (unsigned compare(Time_Stamp_Section.Data_Time_Stamp <
       Last_Time_Stamp_For_Rollover))
THEN
{
          RC_Used_in_CRC = RC_Used_in_CRC  + 1,
}
ENDIF
}
ENDIF
  }
ENDIF

Temp_Fault_Flag = OK,

// check for data integrity faults
IF ((CRC Error based on format used)
OR (Complement_Data_Section CRC != OK)
OR (Mode_Byte.Run_Idle != not Mode_Byte.N_Run_Idle)
OR (Mode_Byte. TBD_2_Bit !=
Mode_Byte. TBD_2_Bit _Copy)
OR (Mode_Byte.TBD_Bit != not Mode_Byte.N_TBD_Bit)
OR (Actual_Data != not Complement_Data) [for > 2 bytes only]
),
THEN
{
      Temp_Fault_Flag = Faulted,
}
ENDIF

// Set up Time_Stamp_Delta, to be used to check for out of sequence
//  messages  Time_Stamp_Delta is not calculated until the EPI
//  reception after Init_Complete_Out is set to 1.
IF(Init_Complete_Out == 0),
THEN
{
      Time_Stamp_Delta = 1,
}
ELSE
{
      Time_Stamp_Delta = Time_Stamp_Section.Data_Time_Stamp –
Last_Data_Time_Stamp,
}
ENDIF

// Take a look at the time stamp delta and determine if it indicates
// the message was received in the right order.
IF ((Time_Stamp_Delta < 0) OR
      (Time_Stamp_Delta > Network_Time_Expectation_Multiplier)),
THEN
{
Temp_Fault_Flag = Faulted,
}
ENDIF
```

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

```
// If the Extended  Format is being used, we can drop some packets
with
// data integrity/message validation or out of order errors.
IF ((ExtendedFormat) AND (Temp_Fault_Flag == Faulted)),
THEN
 {
increment Consumer_Fault_Counter

// Calculate updated data age for the data in the last good packet
IF (Init_Complete_Out)
THEN
{
                      Data_Age = Consumer_Clk_Count –
Last_Corrected_Data_Time_Stamp,
}
ENDIF

// Calculate the maximum worst case age
IF (Data_Age > Max_Data_Age)
THEN
{
           Max_Data_Age = Data_Age,
}
ENDIF

// Is it OK to ignore this error?
// It is OK if the consumer fault counter is not greater than the
// maximum faults allowed and the updated data age from the
// last good packet still meets our data age criteria
// (less than the time expectation multiplier)
IF (
       (Consumer_Fault_Counter < Max_Fault_Number) AND
       (Data_Age <= Network_Time_Expectation_Multiplier)
     )
THEN
{
Abort the processing of this packet. Do Not close the connection.
Do not use the Data.
Do not update Last_Corrected_Data_Time_Stamp or Last_Data_Time_Stamp
           }
ELSE
{
              S_Con_Flt_C_Out = Faulted,
           Abort the processing of this packet. Close the connection.
}
  ENDIF
}
ENDIF

// execute a function that checks for ping count changes and
// determines if it is time to produce a time coordination message
ping_count_check_in_consumer_function(),

Init_Complete_Out_Temp = 0,

// execute the safety connection type specific functions
IF (Connection_Type == Multipoint),
THEN
{
      multi_cast_consumer_function(),
}
ELSE
{
```

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

```
      single_cast_consumer_function(),
}
ENDIF

         // If we are using the ExtendedFormat, at this point we have
a properly formatted
// message that was received in the right order. With the Extended
Format
// update the rollover count and last timestamp for rollover.
IF (ExtendedFormat),
THEN
{
      // Only update the rollover count if this is a multipoint
connection
      // or if this is a point to point connection that is out of the
initialization
      // phase.
      IF ((Connection_Type == Multipoint) OR
            (Init_Complete_Out_Temp == 1)),
      THEN
      {
            // Check the timestamp value in the message to determine if
a
            // rollover has occurred, and if so, update the rollover
count
            // accordingly.
            IF (unsigned compare(Time_Stamp_Section.Data_Time_Stamp <
                  Last_Time_Stamp_For_Rollover))
            THEN
            {
            TS_Rollover_Count  = TS_Rollover_Count  + 1,
            }
            ENDIF

            Last_Time_Stamp_For_Rollover =
Time_Stamp_Section.Data_Time_Stamp,
      }
      ENDIF

      // Save the corrected data timestamp so we can recalculate a data
age
      // if the next packet has errors.
      Last_Corrected_Data_Time_Stamp = Corrected_Data_Time_Stamp,
}
         ENDIF

// Save Time stamp for next reception sequence check
Last_Data_Time_Stamp = Time_Stamp_Section.Data_Time_Stamp,

// Calculate the worst case age
IF (Init_Complete_Out_Temp == 1),
THEN
{
      Data_Age = Consumer_Clk_Count – Corrected_Data_Time_Stamp,
}
ENDIF

// Calculate the maximum worst case age
IF (Data_Age > Max_Data_Age)
THEN
{
      Max_Data_Age = Data_Age,
}
```

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

```
ENDIF

// Check for Age, Integrity, and out of sequence faults
IF (( unsigned int_16( Data_Age > Network_Time_Expectation_Multiplier)
AND (Init_Complete_Out_Temp == 1))
OR (Temp_Fault_Flag == Faulted))
        THEN
{
// The connection will be closed, the data should not be used
S_Con_Flt_C_Out_Temp = Faulted,
}
ENDIF

////////////////////////////////////////////////////////////////
// The following information is passed on to the consuming application
//   with block integrity: Safety
Data,Init_Complete_Out,S_Run_Idle_Out
//   and S_Con_Flt_C_Out.
// The time between the checking of the age of the data and passing
//  the data off to the consuming application shall be protected under
//  the time_stamp check or the consuming application time checks.
////////////////////////////////////////////////////////////////
Make Safety Data Available to Consuming Application
Init_Complete_Out = Init_Complete_Out_Temp,
S_Run_Idle_Out    = S_Run_Idle_Out_Temp,
S_Con_Flt_C_Out   = S_Con_Flt_C_Out_Temp,
 ////////////////////////////////////////////////////////////////
// end Safety Data Consumption – link triggered logic
////////////////////////////////////////////////////////////////

////////////////////////////////////////////////////////////////
// Start of point to point consumer function
////////////////////////////////////////////////////////////////
single_cast_consumer_function()
// For point to point multipoint, no time stamp correction is required
Corrected_Data_Time_Stamp = Time_Stamp_Section.Data_Time_Stamp,

// Determine the Init_Complete_Out state to be passed on to the
//  consuming application.
// For point to point or bi-dir, a time_stamp other than 0 or a Run
//  indication, indicate that the Time_Coordination_Message has been
//  received by the Client and the corrected time stamp is being used.
IF ((Init_Complete_Out == 1) OR
      (Corrected_Data_Time_Stamp != 0) OR
      (Mode_Byte.Run_Idle == Run)),
THEN
{
     Init_Complete_Out_Temp = 1,
}
ENDIF

// Determine the Run_Idle indication to be passed on to the consuming
//  application.
IF (((Mode_Byte.Run_Idle == Idle) OR (Init_Complete_Out_Temp == 0))
THEN
{
     S_Run_Idle_Out_Temp = Idle,
}
ELSE
{
     S_Run_Idle_Out_Temp = Run,
}
ENDIF
```

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

```
END single_cast_consumer_function()
////////////////////////////////////////////////////////////////
// end of point to point processing
////////////////////////////////////////////////////////////////

////////////////////////////////////////////////////////////////
// Start of multipoint consumer function
////////////////////////////////////////////////////////////////
multi_cast_consumer_function()
// If multipoint, check that a time correction message has been
//  received within the last Timeout_Multiplier.PI + 1 Ping Intervals
IF  (Time_Correction_Ping_Interval_Count > (Timeout_Multiplier.PI + 1))
THEN
{
      Temp_Fault_Flag = Faulted,
}
ENDIF

// If multipoint, add correction value to time stamp
Corrected_Data_Time_Stamp =  Time_Stamp_Section.Data_Time_Stamp +
 Last_Rcved_Time_Correction_Value
// Determine the Init_Complete_Out state to be passed on to the
//  consuming application.
// For multipoint, the reception of a Time_Correction Message,
indicate
//  that data may be used.
IF (Time_Correction_Received_Flag == 1)
THEN
{
      Init_Complete_Out_Temp = 1,
}
ENDIF
// Determine the Run_Idle indication to be passed on to the consuming
//  application.
IF ((Mode_Byte.Run_Idle == Idle) OR
    (Init_Complete_Out_Temp == 0) OR
    (Time_Correction_Received_Flag == 0) OR   //used only on
multipoint
    (Last_Rcved_Multi_Cast_Active_Idle==Idle))//used only on
multipoint
THEN
{
      S_Run_Idle_Out_Temp = Idle,
}
ELSE
{
      S_Run_Idle_Out_Temp = Run,
}
ENDIF
end multi_cast_consumer_function()
////////////////////////////////////////////////////////////////
// end of multipoint processing
////////////////////////////////////////////////////////////////


////////////////////////////////////////////////////////////////
////////
// Start of ping count check function
////////////////////////////////////////////////////////////////
////////
ping_count_check_in_consumer_function()
```

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

```
// Check if its time to send a Time Coordination Message
// Multipoint connections send a Time Coordination Message
//   (Consumer_Num – 1) receptions after the ping count change.
IF (received Mode_Byte.Ping_Count != Last_Ping_Count),
THEN
{
      Time_Coordination_Count_Down = Consumer_Num,
       Increment Time_Correction_Ping_Interval_Count,
}
ENDIF

//    For multipoint-consumers connecting to an existing producer,
send
//    the Time_Coordination message immediately upon the 1st reception.
IF (It is the first data reception),
THEN
{
      Produce Time_Coordination_Message,
Time_Coordination_Count_Down = 0,
}
ENDIF

// Check if a ping count change has been detected and the Time
//   Coordination message has not been sent yet.
IF (Time_Coordination_Count_Down > 0),
THEN
{
decrement Time_Coordination_Count_Down,

               // Send the Time_Coordination_message if the decremented
//  Time_Coordination_Count_Down transitions to 0
IF (Time_Coordination_Count_Down == 0),
THEN
{
      Produce Time_Coordination_Message,
}
ENDIF
}
ENDIF

// Save ping count for next reception check
Last_Ping_Count = Mode_Byte.Ping_Count,

end ping_count_check_in_consumer_function()
////////////////////////////////////////////////////////////////////
////////////////////////////
// end of ping count check function
////////////////////////////////////////////////////////////////////
```

7.6.7.11 Exemple de réception d'un message de correction de temps – logique déclenchée par la liaison

La logique suivante est la logique SafetyValidatorServer exigée associée à la réception du message de correction de temps pour le type de connexion de sécurité multipoint, pour le consommateur – déclenchée par la liaison.

```
////////////////////////////////////////////////////////////
// Consumer processing – Time Correction Message reception
////////////////////////////////////////////////////////////
// Is the Time Correction message for this Consumer ?
IF (MCast_Octet.Consumer_Num = Consumer_Num)
 // Perform integrity checks.
```

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

```
THEN
{
IF (Time Coordination message CRC incorrect)
OR (MCast_Octet parity incorrect)
OR {MCast_Octet_2 != (((MCast_Octet XOR0xFF)AND0x55)
           OR(MCast_Octet AND0xAA))}
                OR {(MCast_Octet.Multi_Cast_Active_Idle == Idle)
AND (Last_Rcved_Multi_Cast_Active_Idle == Active)},
      // only one transition from connection idle to active will
// be allowed, to prevent an erroneous idle indication,
// a transistion from active to idle will be latched into
// a fault state
      THEN
{
S_Con_Flt_C_Out = Faulted,
      }
ENDIF

      // Save the Time_Correction_Value.
      Last_Rcved_Time_Correction_Value =
Time_Correction_Section.Time_Correction_Value,

      // Save the Multi_Cast_Active_Idle bit.
      Last_Rcved_Multi_Cast_Active_Idle =
MCast_Octet.Multi_Cast_Active_Idle,

      // Set the Time_Correction_Received_Flag.
      Time_Correction_Received_Flag = 1,

      // Reset the Time Correction timeout counter
      Time_Correction_Ping_Interval_Count = 0,
ENDIF
////////////////////////////////////////////////////////////
// end – Time Correction Message reception
////////////////////////////////////////////////////////////
```

7.6.7.12 SafetyValidatorServer – logique déclenchée par l'application

Pour la fonction SafetyValidatorServer déclenchée par l'application, la même logique décrite ci-avant doit être appliquée par la combinaison de la fonction SafetyValidatorServer, mais uniquement lorsqu'elle est sollicitée par l'application de consommation. Les mises en œuvre déclenchées par l'application traitent uniquement les paquets de sécurité lorsque l'application le nécessite. Cette stratégie de mise en œuvre est utile pour les applications dont la fréquence d'exécution est habituellement inférieure à une fréquence d'EPI type. Les fonctions peuvent être réparties, tel que cela est défini dans le Tableau 96 et le Tableau 99.

Les étapes de traitement de protocoles définies dans le Tableau 99 nécessitent de n'être exécutées qu'avec les messages utilisés par l'application de consommation.

7.6.7.13 Exemple de logique de production des messages de coordination temporelle

La fonction SafetyValidatorServer doit exécuter les étapes suivantes à chaque envoi d'un message de coordination temporelle. Pour les connexions de sécurité point à point et multipoints, les données de coordination temporelle sont transmises dans le message de coordination temporelle. Cette logique est également décrite dans la single_cast_function() de la section de logique de production combinée.

```
////////////////////////////////////////////////////////////
//Time Coordination message production processing
////////////////////////////////////////////////////////////
// Set the Ping_Count_Reply to the value captured at the ping request
Ack_Octet.Ping_Count_Reply = Mode_Octet.Ping_Count,
```

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021

```
// Set the Ping_Response bit to 1
Ack_Octet.Ping_Response = 1,

// Set the Consumer_Time_Value to the producers clock value
Time_Coordination_section.Consumer_Time_Value = Producer_Clk_Count,

// Add data integrity measures
Set Ack_Octet.Reserved(6:4) = 0,
Set Ack_Octet.Reserved(2) = 0,
Set Ack_Octet.Parity_Even bit to the correct value,
Ack_Octet_2 !=(((Ack_Octet XOR 0xFF)AND 0x55)OR
              (Ack_Octet AND 0xAA)),
Calculate CRC on Time Coordination message,
////////////////////////////////////////////////////////////////
// end time coordination message send logic
////////////////////////////////////////////////////////////////
```

7.7 Spécifications des messages de sécurité et des données de protocole

7.7.1 Octet Mode

7.7.1.1 Mode_Octet.Run_Idle

Le bit Run_Idle doit prendre la valeur 0 pour indiquer l'état Repos (Idle) et la valeur 1 pour indiquer l'état Exécution (Run).

Pour les connexions point à point, le bit Run_Idle doit être défini sur l'état Repos si l'application de production est "au repos" ou si le producteur attend les informations concernant les messages de coordination temporelle qui doivent être reçues au démarrage de la production des données.

Si ces informations ont été reçues, le bit Run_Idle doit être défini sur l'état Run_Idle indiqué par l'application de production.

Pour les connexions multipoints, le bit Run_Idle doit être défini sur l'état Run_Idle indiqué par l'application de production.

7.7.1.2 Mode_Octet.N_Run_Idle

Le bit complémentaire N_Run_Idle doit toujours venir en complément du bit Run_Idle.

7.7.1.3 Mode_Octet.TBD_2_Bit

Le Mode_Octet.TBD_2_Bit réservé doit être défini sur 0 par le producteur.

7.7.1.4 Mode_Octet.TBD_2_Copy

Le bit TBD_2_Copy doit toujours être égal au bit TBD_2_Bit.

7.7.1.5 Mode_Octet.Ping_Count

Le consommateur utilise le Ping_Count pour déterminer le moment où il est nécessaire d'envoyer un message de coordination temporelle.

7.7.1.6 Mode_Octet.TBD_Bit

Le Mode_Octet.TBD_Bit réservé doit être défini sur 0 par le producteur. Les bits réservés doivent être ignorés par le consommateur, sauf pour le contrôle du CRC et le contrôle réel/complémentaire de la paire TBD_Bit/N_TBD_Bit.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-2:2021