

INTERNATIONAL STANDARD

NORME INTERNATIONALE



**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**



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2016 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 Varembe
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
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 corrigenda or an amendment might have been published.

IEC Catalogue - webstore.iec.ch/catalogue

The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

IEC publications search - www.iec.ch/searchpub

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 also once a month by email.

Electropedia - www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing 20 000 terms and definitions in English and French, with equivalent terms in 15 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary

65 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

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: csc@iec.ch.

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.

Catalogue IEC - webstore.iec.ch/catalogue

Application autonome pour consulter tous les renseignements bibliographiques sur les Normes internationales, Spécifications techniques, Rapports techniques et autres documents de l'IEC. Disponible pour PC, Mac OS, tablettes Android et iPad.

Recherche de publications IEC - www.iec.ch/searchpub

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 aussi une fois par mois par email.

Electropedia - www.electropedia.org

Le premier dictionnaire en ligne de termes électroniques et électriques. Il contient 20 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans 15 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

Glossaire IEC - std.iec.ch/glossary

65 000 entrées terminologiques électrotechniques, en anglais et en français, extraites des articles Termes et Définitions des publications IEC parues depuis 2002. Plus certaines entrées antérieures extraites des publications des CE 37, 77, 86 et CISPR de l'IEC.

Service Clients - webstore.iec.ch/csc

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

INTERNATIONAL STANDARD

NORME INTERNATIONALE



**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 978-2-8322-3480-8

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.

CONTENTS

FOREWORD.....	12
0 Introduction	14
0.1 General.....	14
0.2 Patent declaration	16
1 Scope.....	17
2 Normative references	17
3 Terms, definitions, symbols, abbreviated terms and conventions	19
3.1 Terms and definitions	19
3.1.1 Common terms and definitions	19
3.1.2 CPF 2: Additional terms and definitions	24
3.2 Symbols and abbreviated terms.....	24
3.2.1 Common symbols and abbreviated terms.....	24
3.2.2 CPF 2: Additional symbols and abbreviated terms.....	25
3.3 Conventions.....	26
4 Overview of FSCP 2/1 (CIP Safety™).....	26
4.1 General.....	26
4.2 FSCP 2/1	26
5 General	27
5.1 External documents providing specifications for the profile	27
5.2 Safety functional requirements	28
5.3 Safety measures	28
5.4 Safety communication layer structure	29
5.5 Relationships with FAL (and DLL, PhL).....	30
5.5.1 General	30
5.5.2 Data types	30
6 Safety communication layer services.....	30
6.1 Introduction.....	30
6.2 Connection object	31
6.2.1 General	31
6.2.2 Class attribute extensions	31
6.2.3 Service extensions.....	31
6.2.4 Explicit message response format for SafetyOpen and SafetyClose	32
6.3 Connection Manager object.....	32
6.3.1 General	32
6.3.2 ForwardOpen for safety.....	33
6.3.3 Safety network segment.....	35
6.3.4 Originator rules for calculating the connection parameter CRC.....	38
6.3.5 SafetyOpen processing flowcharts.....	38
6.3.6 Checks required by Multipoint producers with existing connections	41
6.3.7 Electronic key usage for safety.....	42
6.3.8 RPI vs. API in safety connections	42
6.3.9 Application path construction for safety	42
6.3.10 Safety Validator connection types.....	43
6.3.11 Application reply data in a successful SafetyOpen response	46
6.3.12 Unsuccessful SafetyOpen response	48
6.3.13 ForwardClose for safety	50

6.4	Identity object	50
6.4.1	General	50
6.4.2	Changes to common services	50
6.4.3	Extensions for CP 16/3 devices	51
6.5	Link objects	51
6.5.1	DeviceNet object changes	51
6.5.2	TCP/IP Interface object changes	52
6.5.3	SERCOS III Link object	52
6.6	Safety Supervisor object	53
6.6.1	General	53
6.6.2	Safety Supervisor class attributes	54
6.6.3	Subclasses	54
6.6.4	Safety Supervisor instance attributes	54
6.6.5	Semantics	58
6.6.6	Subclasses	64
6.6.7	Safety Supervisor common services	64
6.6.8	Safety Supervisor behavior	75
6.7	Safety Validator object	82
6.7.1	General	82
6.7.2	Class attributes	82
6.7.3	Instance attributes	83
6.7.4	Class services	88
6.7.5	Instance services	89
6.7.6	Object behavior	89
6.8	Connection Configuration Object	92
6.8.1	General	92
6.8.2	Class attribute extensions	92
6.8.3	Instance attributes, additions and extensions	92
6.8.4	Instance attribute semantics extensions or restrictions for safety	95
6.8.5	Special Safety Related Parameters – (Attribute 13)	99
6.8.6	Object-specific services	105
6.8.7	Common service extensions for safety	105
6.8.8	Object behavior	107
7	Safety communication layer protocol	108
7.1	Safety PDU format	108
7.1.1	Safety PDU encoding	108
7.1.2	Safety CRC	120
7.2	Communication protocol behavior	121
7.2.1	Sequence of safety checks	121
7.2.2	Connection termination	121
7.2.3	Cross checking error	121
7.3	Time stamp operation	122
7.4	Rollover counts in the EF	123
7.5	Protocol sequence diagrams	123
7.5.1	General	123
7.5.2	Normal safety transmission	123
7.5.3	Lost, corrupted and delayed message transmission	124
7.5.4	Lost, corrupted or delayed message transmission with production repeated	127

7.5.5	Point-to-point ping.....	129
7.5.6	Multipoint ping on CP 2/3 Safety.....	130
7.5.7	Multipoint ping on CP 2/2 safety networks	131
7.5.8	Multipoint ping – retry with success	132
7.5.9	Multipoint ping – retry with timeout	133
7.6	Safety protocol definition	134
7.6.1	General	134
7.6.2	High level view of a safety device	134
7.6.3	Safety Validator object	134
7.6.4	Relationship between SafetyValidatorServer and SafetyValidatorClient	135
7.6.5	Extended Format time stamp rollover handling.....	135
7.6.6	SafetyValidatorClient function definition.....	140
7.6.7	SafetyValidatorServer function definition	148
7.7	Safety message and protocol data specifications	161
7.7.1	Mode octet.....	161
7.7.2	Time Stamp Section	162
7.7.3	Time Coordination Message	162
7.7.4	Time correction message	163
7.7.5	Safety data production	163
7.7.6	Producer dynamic variables	171
7.7.7	Producer per consumer dynamic variables.....	173
7.7.8	Consumer data variables.....	174
7.7.9	Consumer input static variables.....	176
7.7.10	Consumer dynamic variables.....	177
8	Safety communication layer management.....	179
8.1	Overview	179
8.2	Definition of the measures used during connection establishment	179
8.3	Originator-Target relationship validation	183
8.4	Detection of mis-routed connection requests.....	183
8.5	SafetyOpen processing	184
8.6	Ownership management.....	184
8.7	Bridging different physical layers	185
8.8	Safety connection establishment	187
8.8.1	Overview	187
8.8.2	Basic facts for connection establishment	187
8.8.3	Configuring safety connections.....	187
8.8.4	Network time expectation multiplier	189
8.8.5	Establishing connections.....	190
8.8.6	Recommendations for consumer number allocation.....	193
8.8.7	Recommendations for connection establishment.....	194
8.8.8	Ownership establishment	194
8.8.9	Ownership use cases	195
8.8.10	PID/CID usage and establishment	198
8.8.11	Proper PID/CID usage in multipoint and point-to-point connections	198
8.8.12	Network supported services	200
8.8.13	FSCP 2/1 safety device type	201
8.9	Safety configuration process	205
8.9.1	Introduction to safety configuration.....	205
8.9.2	Configuration goals	205

8.9.3	Configuration overview	206
8.9.4	User configuration guidelines	207
8.9.5	Configuration process SIL3 justification	208
8.9.6	Device functions for tool configuration	209
8.9.7	Password security	209
8.9.8	SNCT interface services	209
8.9.9	Configuration lock	209
8.9.10	Effect of configuration lock on device behavior	210
8.9.11	Configuration ownership	211
8.9.12	Configuration mode	211
8.9.13	Measures used to ensure integrity of configuration process	211
8.9.14	Download process	213
8.9.15	Verification process	216
8.9.16	Verification process	218
8.9.17	Configuration error analysis	219
8.10	Electronic Data Sheets extensions for safety	223
8.10.1	General rules for EDS based safety devices	223
8.10.2	EDS extensions for safety	224
8.11	Requirements for CP 2/2	229
8.11.1	EPI rules for safety messages that travel over CP 2/2	229
8.11.2	Default safety I/O service	229
8.11.3	Duplicate IP detection	229
8.11.4	Priority for safety connections	229
8.12	Requirements for CP 2/3	230
8.12.1	Allocation of CP 2/3 identifiers	230
8.12.2	Additional requirements	232
8.13	CP 16/3 requirements	232
8.13.1	General architecture for CPF 2 on CP 16/3	232
8.13.2	Baseline FSCP 2/1 on CP 16/3 device	233
8.13.3	Supported objects and services in CP 16/3 devices	234
8.13.4	Transport layer requirements	234
8.13.5	FSCP 2/1 and the CP 16/3 device model	237
8.13.6	UNID assignment on CP 16/3	238
9	System requirements	241
9.1	Indicators and switches	241
9.1.1	General indicator requirements	241
9.1.2	LED indications for setting the device UNID	241
9.1.3	Module Status LED	241
9.1.4	Indicator warning	242
9.1.5	Network Status LED	242
9.1.6	Switches	243
9.2	Installation guidelines	245
9.3	Safety function response time	246
9.3.1	Overview	246
9.3.2	Network time expectation	246
9.3.3	Equations for calculating network reaction times	247
9.4	Duration of demands	249
9.5	Constraints for calculation of system characteristics	249
9.5.1	Number of nodes	249

9.5.2	Network PFH	249
9.5.3	Bit Error Rate (BER)	252
9.6	Maintenance	253
9.7	Safety manual	253
10	Assessment	253
Annex A (informative) Additional information for functional safety communication profiles of CPF 2		254
A.1	Hash function example code	254
A.2		268
Annex B (informative) Information for assessment of the functional safety communication profiles of CPF 2		269
Bibliography		270

Figure 1 – Relationships of IEC 61784-3 with other standards (machinery)	14
Figure 2 – Relationships of IEC 61784-3 with other standards (process)	15
Figure 3 – Relationship of Safety Validators	27
Figure 4 – Communication layers	30
Figure 5 – ForwardOpen with safety network segment	34
Figure 6 – Safety network target format	36
Figure 7 – Target Processing SafetyOpen with no configuration data (Form 2 SafetyOpen)	39
Figure 8 – Target Processing for SafetyOpen with configuration data (Form 1 SafetyOpen)	40
Figure 9 – Originator logic to determine which format to use	41
Figure 10 – Applying device configuration	68
Figure 11 – Configure and Validate processing flowcharts	69
Figure 12 – UNID handling during “Waiting for TUNID”	75
Figure 13 – Safety Supervisor state diagram	76
Figure 14 – Configuration, testing and locked relationships	80
Figure 15 – Safety connection types	86
Figure 16 – Safety Validator state transition diagram	90
Figure 17 – Logic for Auto-detecting format type	104
Figure 18 – Connection Configuration Object state diagram	107
Figure 19 – Connection Configuration Object data flow	108
Figure 20 – Format of the mode octet	109
Figure 21 – 1 or 2 octet data section, Base Format	110
Figure 22 – 1 or 2 octet data section, Extended Format	111
Figure 23 – 3 to 250 octet data section format, Base Format	111
Figure 24 – 3 to 250 octet data section format, Extended Format	112
Figure 25 – Time Stamp section format, Base Format	113
Figure 26 – BF Time Coordination message encoding	114
Figure 27 – EF Time Coordination message encoding	114
Figure 28 – BF Time Correction message encoding	115
Figure 29 – EF Time Correction message encoding	115

Figure 30 – 1 or 2 octet point-to-point PDU encoding	117
Figure 31 – 1 or 2 Octet multipoint PDU encoding	117
Figure 32 – 1 or 2 Octet, multipoint, Format 2 safety connection format	118
Figure 33 – 3 to 250 Octet Point-to-point PDU encoding	118
Figure 34 – 3 to 248 Octet Multipoint PDU encoding	119
Figure 35 – 3 to 248 Octet, Multipoint, safety connection format	119
Figure 36 – CRC Calculation order for Extended Format messages	120
Figure 37 – Time stamp sequence.....	122
Figure 38 – Sequence diagram of a normal producer/consumer safety sequence	123
Figure 39 – Sequence diagram of a normal producer/consumer safety sequence (production repeated).....	124
Figure 40 – Sequence diagram of a corrupted producer to consumer message.....	125
Figure 41 – Sequence diagram of a lost producer to consumer message.....	126
Figure 42 – Sequence diagram of a delayed message	127
Figure 43 – Sequence diagram of a corrupted producer to consumer message with production repeated	128
Figure 44 – Sequence diagram of a connection terminated due to delays	129
Figure 45 – Sequence diagram of a failure of safety CRC check	129
Figure 46 – Sequence diagram of a point-to-point ping – normal response	130
Figure 47 – Sequence diagram of a successful multipoint ping, CP 2/3 safety	131
Figure 48 – Sequence diagram of a successful multipoint ping, CP 2/2 safety	132
Figure 49 – Sequence diagram of a multipoint ping retry.....	133
Figure 50 – Sequence diagram of a multipoint ping timeout	133
Figure 51 – Safety device reference model entity relation diagram	134
Figure 52 – Two devices interchanging safety data via a SafetyValidatorClient and a SafetyValidatorServer	135
Figure 53 – Point-to-point, originating consumer. target producer.....	137
Figure 54 – Point-to-point, originator producer, target consumer	138
Figure 55 – Multi-point, originator consumer, target producer.....	139
Figure 56 – Safety production data flow.....	140
Figure 57 – Consumer safety data monitoring.....	149
Figure 58 – SafetyValidatorServer – application triggered	150
Figure 59 – Target ownership.....	183
Figure 60 – SafetyOpen forms.....	184
Figure 61 – Connection ownership state chart	185
Figure 62 – SafetyOpen UNID mapping	185
Figure 63 – Common CPF 2 application layer	186
Figure 64 – End-to-End routing example	186
Figure 65 – Sources for safety related connection parameters	189
Figure 66 – Parameter mapping between originator and target.....	190
Figure 67 – CP 2/3 Safety connection establishment in targets for Form 2a SafetyOpen.....	192
Figure 68 – General sequence to detect configuration is required	193
Figure 69 – PID/CID exchanges for two originator scenarios	198
Figure 70 – Seed generation for multipoint connections	199

Figure 71 – PID/CID runtime handling	200
Figure 72 – Connection categories and supported services.....	203
Figure 73 – Recommended connection types.....	204
Figure 74 – Logic-to-logic supported services.....	204
Figure 75 – Recommended connection types for logic to logic	205
Figure 76 – Configuration data transfers.....	206
Figure 77 – Protection measures in safety devices	208
Figure 78 – Configuration, testing and locked relationships.....	210
Figure 79 – Originator's configuration data	212
Figure 80 – SNCT to device download process.....	214
Figure 81 – SNCT Downloads to originators that perform Form 1 configuration	215
Figure 82 – Protection from locking and ownership	217
Figure 83 – Example of read back and comparison of original and printout.....	217
Figure 84 – Diverse display without full data read back.....	218
Figure 85 – Verification process including all alternatives	219
Figure 86 – Baseline FSCP 2/1 on CP 16/3 device	233
Figure 87 – FSCP 2/1 Adaptation Layer and SMP interaction.....	236
Figure 88 – FSCP 2/1 Adaptation	237
Figure 89 – CP 16/3 device model.....	238
Figure 90 – Adding a standard module to a modular device	240
Figure 91 – Safety device NodeID processing logic	245
Figure 92 – Safety function response time	246
Figure 93 – Safety function response time components	248
Figure 94 – Network protocol reliability block diagram (RBD)	249
Figure 95 – Network PFH summary	251
Figure 96 – Extended Format PFH summary	252
 Table 1 – Communications errors and detection measures matrix	 29
Table 2 – New class attributes	31
Table 3 – Service extensions	32
Table 4 – SafetyOpen and SafetyClose response format.....	32
Table 5 – Safety network segment identifier	35
Table 6 – Safety network segment definition.....	35
Table 7 – Safety network segment router format.....	37
Table 8 – Safety Network Segment Extended Format	37
Table 9 – Multipoint producer parameter evaluation rules	42
Table 10 – ForwardOpen setting options for safety connections	44
Table 11 – Network connection parameters for safety connections.....	46
Table 12 – CP 2/3 Safety target application reply (size: 10 octets)	46
Table 13 – EF CP 2/3 Safety target application reply (size: 14 octets).....	47
Table 14 – SafetyOpen target application reply (size: 18 octets)	47
Table 15 – EF SafetyOpen target application reply (size: 22 octets).....	48
Table 16 – New and extended error codes for safety	48

Table 17 – SafetyOpen error event guidance table	49
Table 18 – Identity object common service changes	51
Table 19 – Identity object extensions for CP 16/3 devices	51
Table 20 – New DeviceNet object instance attribute	51
Table 21 – New TCP/IP Interface object instance attribute	52
Table 22 – SERCOS III Link object class attributes	52
Table 23 – SERCOS III Link object instance attributes	53
Table 24 – SERCOS III Link Object Common Services	53
Table 25 – Safety Supervisor class attributes	54
Table 26 – Safety Supervisor instance attributes	55
Table 27 – Device status attribute state values	59
Table 28 – Exception status attribute format	59
Table 29 – Common exception detail attribute values	60
Table 30 – Exception detail format summary	61
Table 31 – Summary of device behavior for various CFUNID values	63
Table 32 – Safety Supervisor common services	65
Table 33 – Safety Supervisor object specific services	65
Table 34 – Configure_Request message structure	67
Table 35 – Validate_Configuration message structure	67
Table 36 – Validate_Configuration success message structure	67
Table 37 – Validate_Configuration error code	68
Table 38 – Validate_Configuration extended codes	68
Table 39 – Set_Password message structure	70
Table 40 – Reset_Password message structure	70
Table 41 – Configuration_Lock/Unlock message structure	71
Table 42 – Mode_Change message structure	71
Table 43 – Safety_Reset message structure	72
Table 44 – Safety Supervisor safety reset types	72
Table 45 – Attribute bit map parameter	72
Table 46 – Reset processing rules for reset types	73
Table 47 – Propose_TUNID service	73
Table 48 – Apply_TUNID service	74
Table 49 – Safety Supervisor events	76
Table 50 – State event matrix for Safety Supervisor	77
Table 51 – Configuration owner control vs. device state	80
Table 52 – State mapping of Safety Supervisor to Identity object	81
Table 53 – Safety Supervisor object event mapping	81
Table 54 – Identity object event mapping	82
Table 55 – Safety Validator class attributes	83
Table 56 – Safety Validator instance attributes	83
Table 57 – Safety Validator state assignments	85
Table 58 – Safety Validator type, bit field assignments	86
Table 59 – Multipoint producer SafetyOpen parameter evaluation rules	87

Table 60 – Safety Validator class services.....	88
Table 61 – Safety Validator instance services.....	89
Table 62 – Safety Validator Get_Attributes_All service data.....	89
Table 63 – Safety Validator state event matrix.....	91
Table 64 – State mapping between Safety Supervisor and Safety Validator objects.....	92
Table 65 – Connection configuration object class attribute extensions.....	92
Table 66 – Connection Configuration Object instance attribute additions/extensions.....	92
Table 67 – Connection flag bit definitions	95
Table 68 – O-to-T connection parameters.....	96
Table 69 – T-to-O connection parameters.....	97
Table 70 – Data map formats	98
Table 71 – Data map format 0	99
Table 72 – Data map format 1	99
Table 73 – Target device’s SCCRC values	101
Table 74 – Target device’s SCTS values	101
Table 75 – Time correction connection parameters for multipoint connection.....	102
Table 76 – Format Type attribute meaning	103
Table 77 – Format Status attribute meaning	104
Table 78 – Connection Configuration Object-specific services.....	105
Table 79 – Get_Attributes_All Response service data (added attributes)	105
Table 80 – Get_Attributes_All Response service data (added parameters)	106
Table 81 – Set_Attributes_All Request service data (added attributes).....	106
Table 82 – Set_Attributes_All Response service data (added parameters)	106
Table 83 – State Mapping between Safety Supervisor and the CCO objects.....	107
Table 84 – Connection sections and PDU formats	109
Table 85 – Mode octet variables.....	110
Table 86 – Time Stamp variables	113
Table 87 – Time Coordination message variables	114
Table 88 – Time Correction Message variables	116
Table 89 – CRC polynomials used.....	120
Table 90 – Connection sections and message formats.....	121
Table 91 – Data reception – Link triggered	151
Table 92 – Time_Correction reception – Link triggered	151
Table 93 – Data reception – Application triggered.....	151
Table 94 – Time_Correction reception – Application triggered.....	152
Table 95 – Consuming application – Safety data monitoring.....	152
Table 96 – Producer connection status determination	164
Table 97 – Consuming safety connection status	175
Table 98 – Connection establishment errors and measures to detect errors	179
Table 99 – SNN Date/Time allocations	180
Table 100 – SNN legal range of time values	180
Table 101 – Safety connection parameters	188
Table 102 – SafetyOpen summary.....	191

Table 103 – Originator/Target service mapping.....	202
Table 104 – Unsupported originator/target service types.....	202
Table 105 – Configuration goals.....	206
Table 106 – Configuration owner control vs. device state.....	211
Table 107 – Errors and detection measures.....	220
Table 108 – Object Class section keywords.....	224
Table 109 – Safety Classx entry format	225
Table 110 – Parameter class keywords	225
Table 111 – New Connection Manager section keywords for safety.....	226
Table 112 – Connection Manager field usage for safety	227
Table 113 – Connection parameter field settings for safety	228
Table 114 – CP 2/3 ID assignment rules.....	230
Table 115 – LED indications for setting UNID	241
Table 116 – Module Status LED	242
Table 117 – Network status LED states	242
Table 118 – Connection reaction time type – producing/consuming applications.....	247

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**INDUSTRIAL COMMUNICATION NETWORKS –
PROFILES –****Part 3-2: Functional safety fieldbuses –
Additional specifications for CPF 2****FOREWORD**

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

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

This third edition cancels and replaces the second edition published in 2010. This edition constitutes a technical revision. The main changes with respect to the previous edition are listed below (and highlighted in yellow in this document).

- Added detailed requirements for use of FSCP 2/1 in conjunction with CP 16/3 (see 4.1, 6.4.3, 6.5.3, 8.2, 8.13, and miscellaneous references when referencing CPF 2 networks);
- Defined object class section keywords for safety to EDS file definition in 8.10.2.1;
- New sections on safety CRC overview in 7.1.2.1 and Rollover counts for EF format in 7.4;
- Corrections to PFH calculations in 9.5.2;

- Change from MACID to NodeID as general reference to network identifier;
- Miscellaneous minor corrections made since the last publication.

The text of this standard is based on the following documents:

FDIS	Report on voting
65C/851/FDIS	65C/854/RVD

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

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

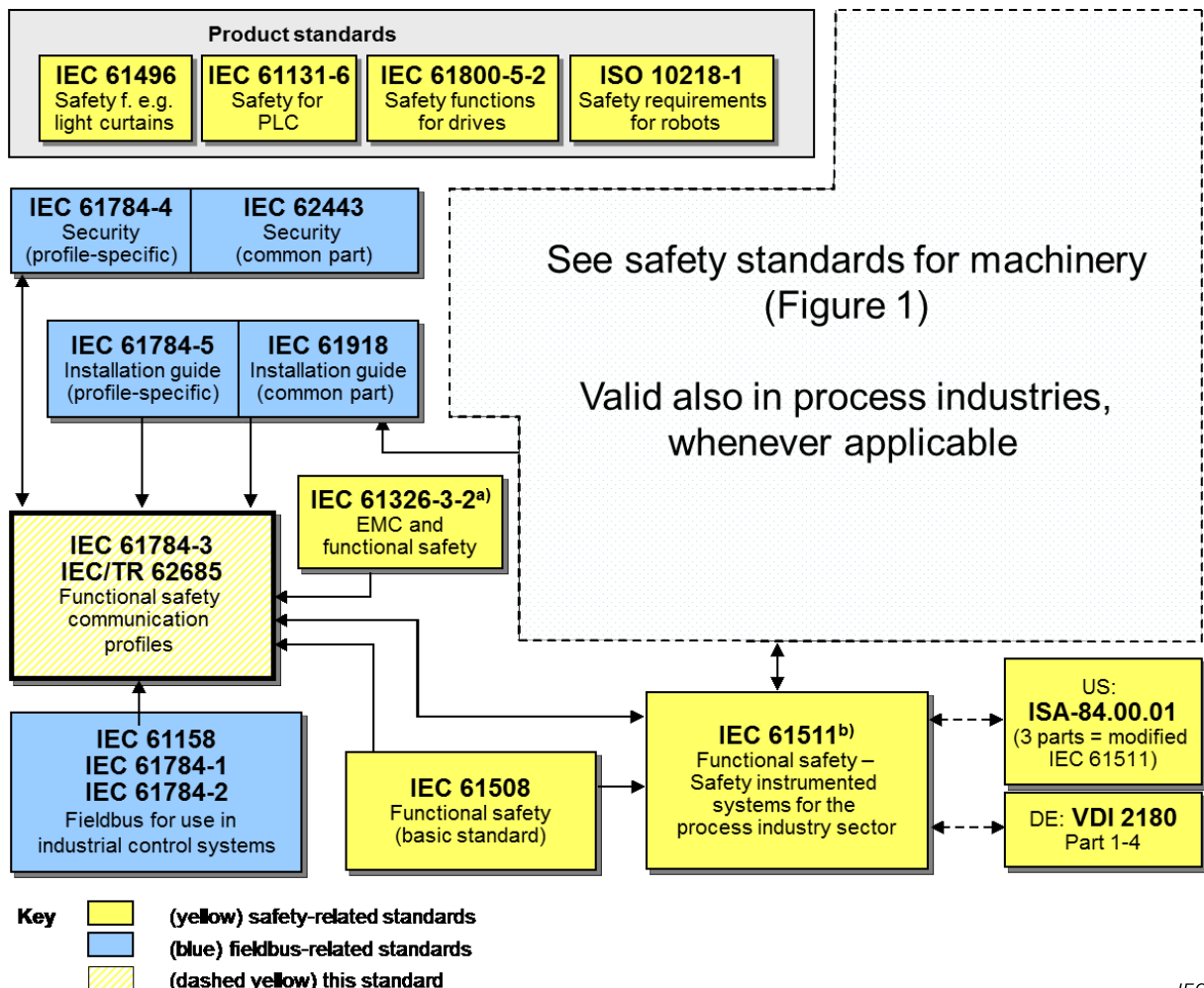
A list of all parts of the IEC 61784-3 series, published under the general title *Industrial communication networks – Profiles – Functional safety fieldbuses*, can be found on the IEC website.

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

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

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

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



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

^b EN ratified.

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

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

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

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

This standard describes:

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

0.2 Patent declaration

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

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

IEC takes no position concerning the evidence, validity and scope of these patent rights.

The holder of these patent rights has assured the IEC that he/she is willing to negotiate licences either free of charge or under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statement of the holder of these patent rights is registered with IEC.

Information may be obtained from:

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

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

ISO (www.iso.org/patents) and IEC (<http://patents.iec.ch>) maintain on-line data bases of patents relevant to their standards. Users are encouraged to consult the data bases for the most up to date information concerning patents.

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES –

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

1 Scope

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

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

This part¹ defines mechanisms for the transmission of safety-relevant messages among participants within a distributed network using fieldbus technology in accordance with the requirements of IEC 61508 series² for functional safety. These mechanisms may be used in various industrial applications such as process control, manufacturing automation and machinery.

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

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

2 Normative references

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

ISO 13849-1:2006, *Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design*

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

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

³ To be published.

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

3 Terms, definitions, symbols, abbreviated terms and conventions

3.1 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

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

3.1.1 Common terms and definitions

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

3.1.1.1

availability

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

3.1.1.2

bit error probability

P_e

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

3.1.1.3

black channel

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

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

3.1.1.4

bridge

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

3.1.1.5

closed communication system

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

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

3.1.1.6

communication channel

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

3.1.1.7

communication system

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

3.1.1.8

connection

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

3.1.1.9

Cyclic Redundancy Check

CRC

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

<method> procedure used to calculate the redundant data

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

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

3.1.1.10

defined communication system

defined channel

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

3.1.1.11

error

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

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

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

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

3.1.1.12

failure

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

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

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

3.1.1.13

fault

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

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

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

3.1.1.14

fieldbus

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

⁴ Figures in square brackets refer to the bibliography.

3.1.1.15**DLPDU**

DEPRECATED: frame

Data Link Protocol Data Unit

3.1.1.16**hash function**

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

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

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

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

3.1.1.17**hazard**

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

3.1.1.18**master**

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

3.1.1.19**message**

ordered series of octets intended to convey information

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

3.1.1.20**nuisance trip**

spurious trip with no harmful effect

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

3.1.1.21**performance level**

PL

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

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

3.1.1.22**redundancy**

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

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

3.1.1.23**reliability**

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

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

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

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

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

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

3.1.1.24

residual error rate

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

3.1.1.25

risk

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

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

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

3.1.1.26

safety communication channel

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

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

3.1.1.27

safety communication layer

SCL

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

3.1.1.28

safety connection

connection that utilizes the safety protocol for communications transactions

3.1.1.29

safety data

data transmitted across a safety network using a safety protocol

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

3.1.1.30

safety device

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

3.1.1.31

safety function

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

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

3.1.1.32

safety function response time

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

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

3.1.1.33

safety integrity level

SIL

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

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

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

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

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

3.1.1.34

safety measure

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

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

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

3.1.1.35

safety PDU

SPDU

PDU transferred through the *safety communication channel*

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

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

3.1.1.36

safety-related application

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

3.1.1.37

safety-related system

system performing *safety functions* according to IEC 61508

3.1.1.38

slave

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

3.1.1.39

spurious trip

trip caused by the safety system without a process demand

3.1.1.40

time stamp

time information included in a *message*

3.1.2 CPF 2: Additional terms and definitions

3.1.2.1

base format

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

3.1.2.2

extended format

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

3.1.2.3

ping

request for the consumer to acknowledge the reception of a message

3.1.2.4

ping response

response to a ping

3.1.2.5

signature

method of uniquely identifying a set of data

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

3.2 Symbols and abbreviated terms

3.2.1 Common symbols and abbreviated terms

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

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

3.2.2 CPF 2: Additional symbols and abbreviated terms

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

⁵ For trade name declaration, see Clause 4.

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

3.3 Conventions

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

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

4 Overview of FSCP 2/1 (CIP Safety™)

4.1 General

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

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

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

4.2 FSCP 2/1

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

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

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

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

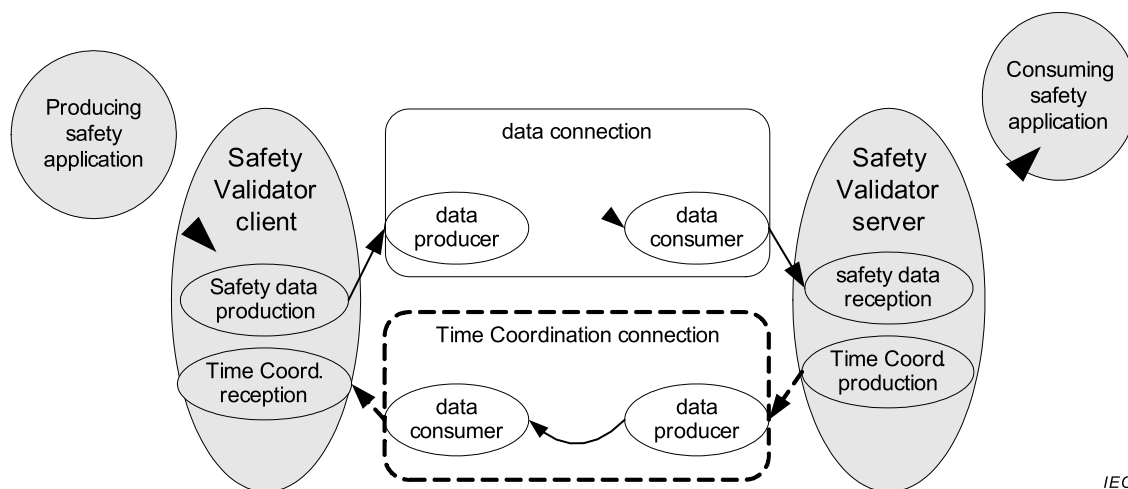


Figure 3 – Relationship of Safety Validators

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

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

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

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

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

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

5 General

5.1 External documents providing specifications for the profile

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

- GS-ET-26 [30]

5.2 Safety functional requirements

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

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

5.3 Safety measures

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

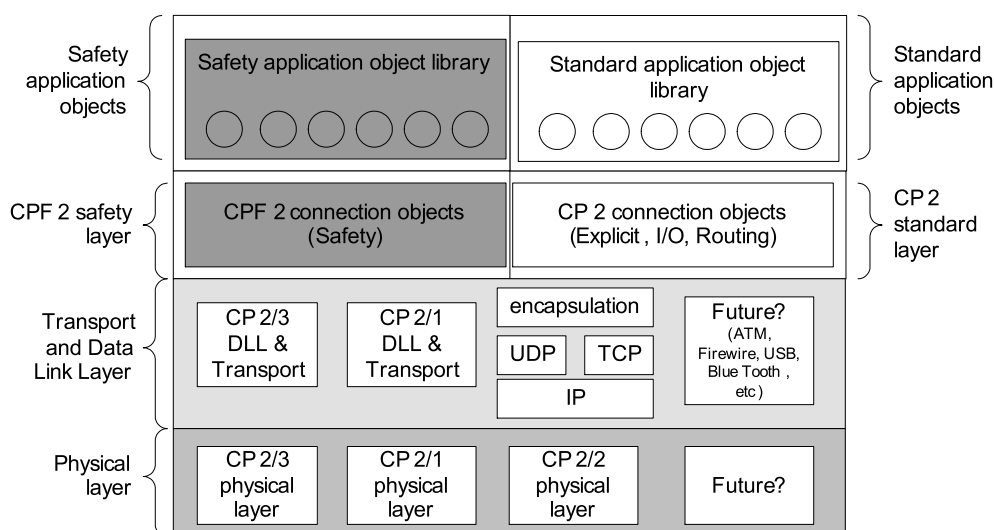
Table 1 – Communications errors and detection measures matrix

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

5.4 Safety communication layer structure

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

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



IEC

Figure 4 – Communication layers

5.5 Relationships with FAL (and DLL, PhL)

5.5.1 General

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

5.5.2 Data types

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

6 Safety communication layer services

6.1 Introduction

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

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

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

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

6.2 Connection object

6.2.1 General

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

6.2.2 Class attribute extensions

Table 2 defines the class attributes used by safety devices.

Table 2 – New class attributes

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

^a

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

^b

Included in class attribute 8.

6.2.3 Service extensions

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

Table 3 – Service extensions

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

6.2.4 Explicit message response format for SafetyOpen and SafetyClose

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

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

Table 4 – SafetyOpen and SafetyClose response format

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

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

6.3 Connection Manager object

6.3.1 General

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

6.3.2 ForwardOpen for safety

6.3.2.1 ForwardOpen for safety contents

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

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

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

Key

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

Figure 5 – ForwardOpen with safety network segment

6.3.2.2 ForwardOpen for safety for Extended Format

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

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

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

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

6.3.3 Safety network segment

6.3.3.1 Common format

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

Table 5 – Safety network segment identifier

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

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

Table 6 – Safety network segment definition

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

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

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

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

Key

 = Safety Segment fields covered by Connection Parameters CRC

Figure 6 – Safety network target format

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

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

Table 7 – Safety network segment router format

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

6.3.3.4 Safety network segment: Extended Format (0x02)

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

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

Table 8 – Safety Network Segment Extended Format

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

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

6.3.4 Originator rules for calculating the connection parameter CRC

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

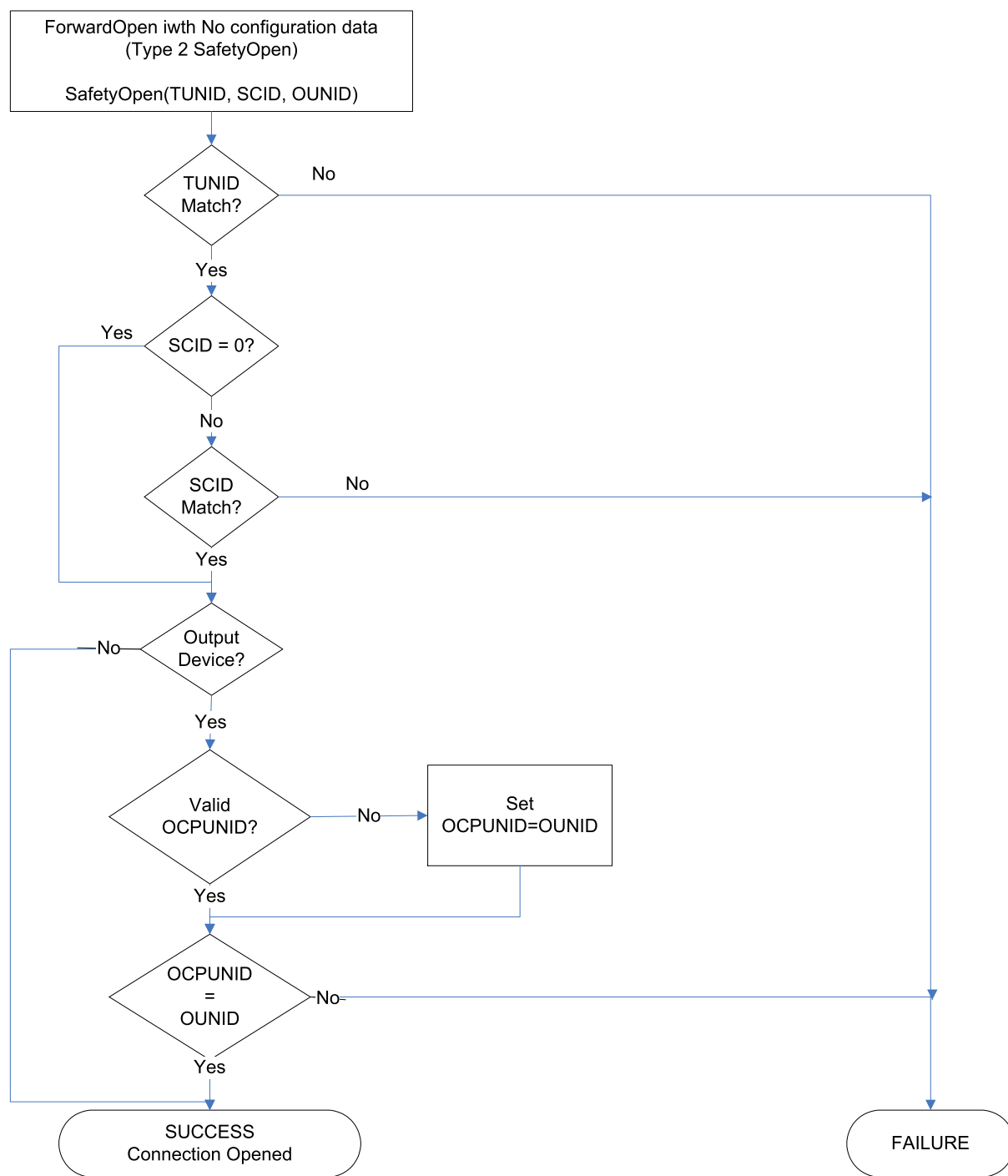
The connection path size in the SafetyOpen changes value depending on whether an originator is sending configuration data or not. Since this field is included in the CPCRC calculation, originators need to calculate and maintain two values when they support the SafetyOpen configuration function. One value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

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

6.3.5 SafetyOpen processing flowcharts

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

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



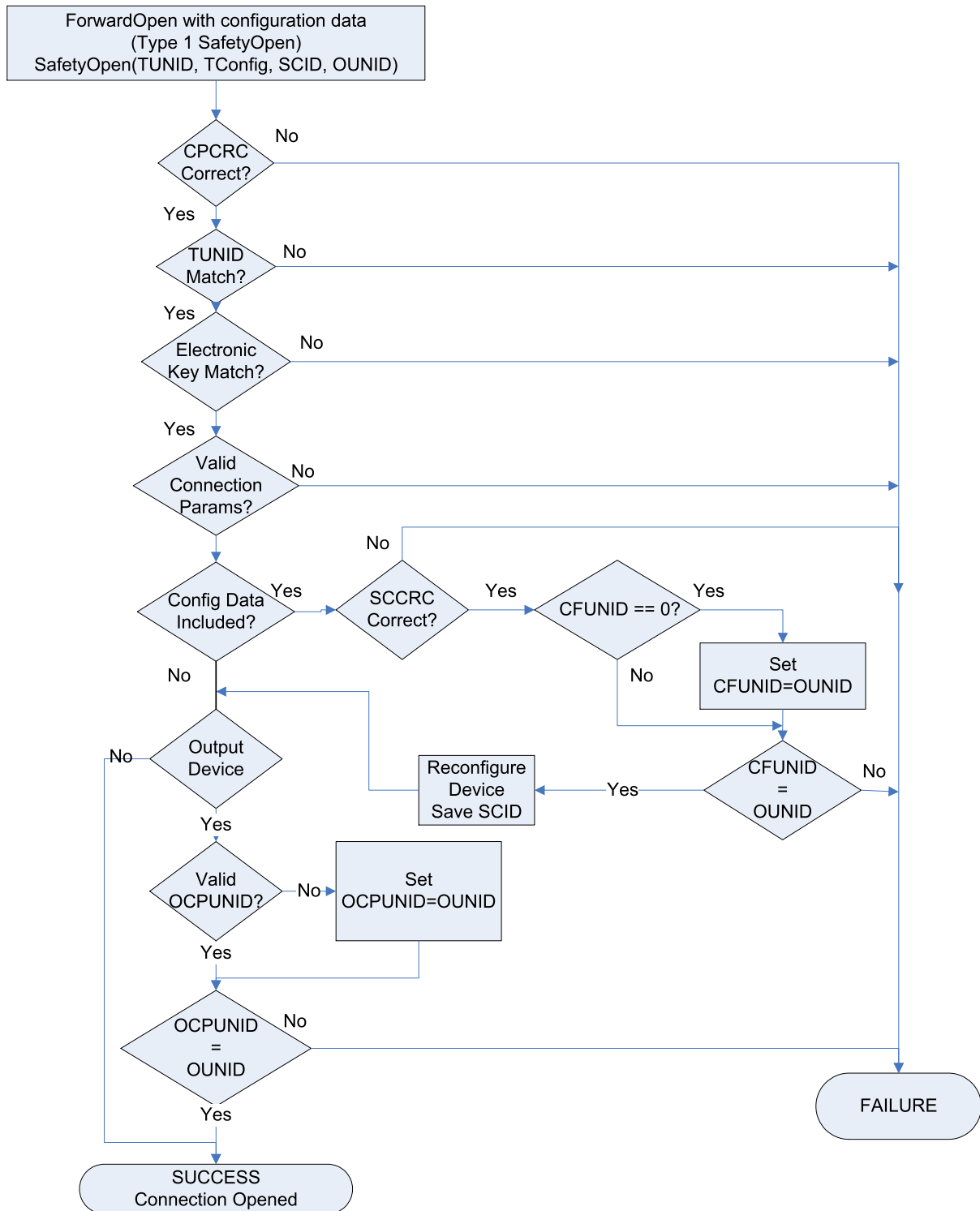
Key:

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

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

IEC

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



Key:

UNID = Unique Network Identifier
CPCRC = Connection Parameter CRC
SCCRC = CRC portion of the SCID
OCPUNID = Output Connection Owning UNID

TUNID = Target's Unique Network Identifier
SCID = Target's Safety Configuration ID
OUNID = Originator's Unique Network Identifier
CFUNID = Configuration Owning UNID

IEC

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

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

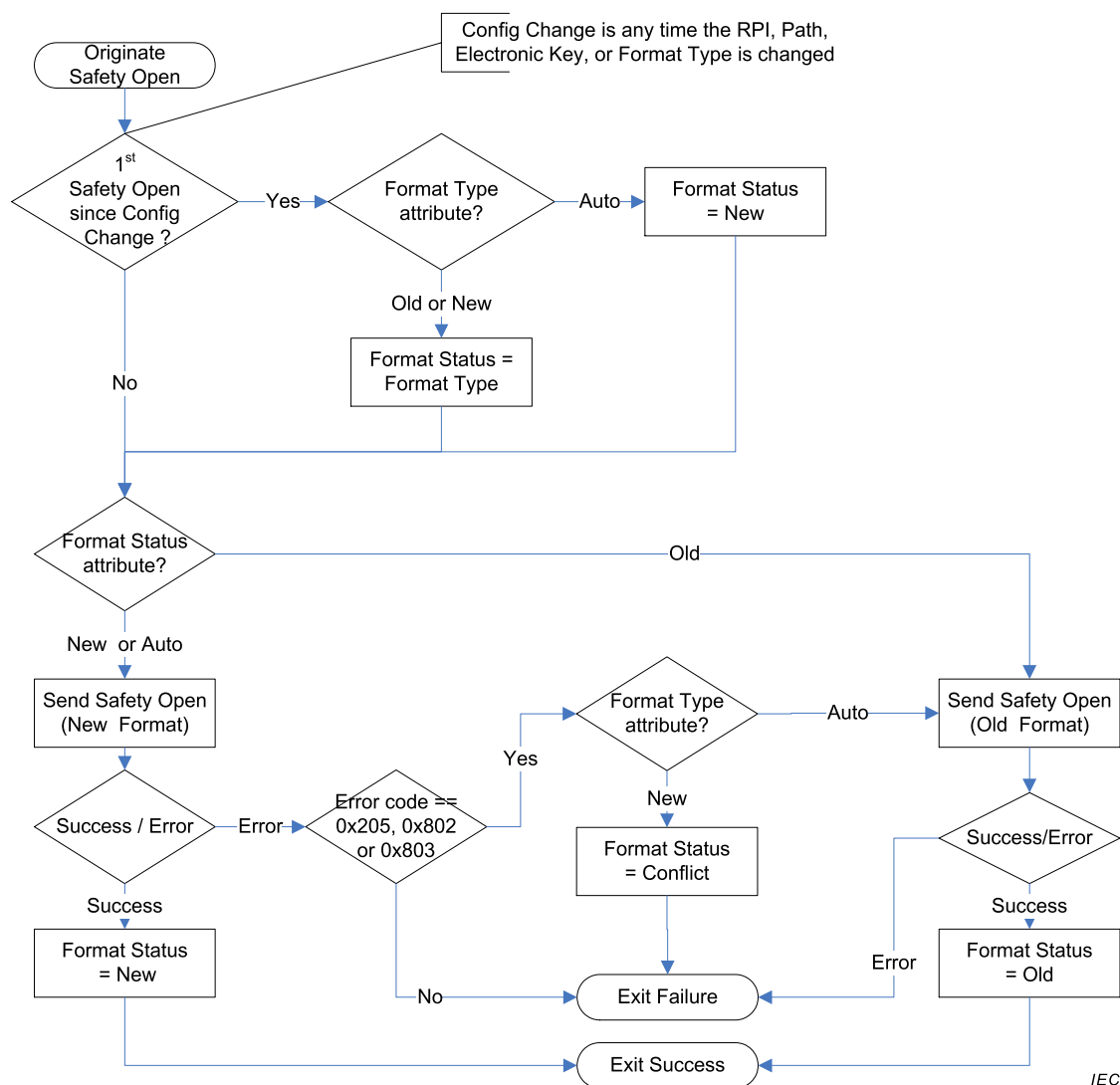


Figure 9 – Originator logic to determine which format to use

6.3.6 Checks required by Multipoint producers with existing connections

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

Table 9 – Multipoint producer parameter evaluation rules

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

6.3.7 Electronic key usage for safety

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

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

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

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

6.3.8 RPI vs. API in safety connections

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

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

6.3.9 Application path construction for safety

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

The possible path types are identified as follows:

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

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

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

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

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

The following rules apply to SafetyOpen path construction:

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

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

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

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

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

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

6.3.10 Safety Validator connection types

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

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

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

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

Table 10 – ForwardOpen setting options for safety connections

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

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

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

Table 11 – 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 12.

The target of a SafetyOpen shall return the data defined in Table 12 through Table 15 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 12 – CP 2/3 Safety target application reply (size: 10 octets)

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

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 13.

Table 13 – EF CP 2/3 Safety target application reply (size: 14 octets)

Parameter Name ^a	Data Type	Description
Consumer_Number	UINT	
PID/CID	STRUCT of:	Target Identifier used to generate a PID or CID seed value
Target Vendor Id	UINT	Target's Vendor Id
Target Device Serial Number	UDINT	Target's Device Serial Number
Target Connection Serial Number	UINT	Connection Serial Number Target assigned to the connection. The Safety Validator instance Id should be used
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 These fields are always present in the Application Reply field. When a CP 2/3 Safety target receives a SafetyOpen that is not multipoint (thus no Time Correction connection is established) the Time_Correction_Connection_ID parameter shall be set to FFFF _{hex} . If the target is not a multipoint producer, the consumer number is set to FFFF _{hex} .		
^b Consuming targets should echo back the values received in the SafetyOpen		

Table 14 – SafetyOpen target application reply (size: 18 octets)

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

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 15.

Table 15 – EF SafetyOpen target application reply (size: 22 octets)

Parameter Name ^a	Data Type	Description
Consumer_Number	UINT	
PID/CID	STRUCT of:	Target Identifier used to generate a PID or CID seed value
Target Vendor Id	UINT	Target's Vendor Id
Target Device Serial Number	UDINT	Target's Device Serial Number
Target Connection Serial Number	UINT	Connection Serial Number Target assigned to the connection. The Safety Validator instance Id should be used
Time_Correction_Connection_ID	UDINT	Connection ID selected by the Target for the Time Correction connection. If chosen by the originator, then the value is echoed back
Time_Correction_API	UDINT	Returns same value received in the Request packet
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 These fields are always present in the Application Reply field. When a CP 2/3 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 0xFFFF. If the target is not a multipoint producer, the consumer number is set to 0xFFFF. ^b Consuming targets should echo back the values received in the SafetyOpen.		

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

Table 16 – New and extended error codes for safety

General status	Extended status	Explanation
01 _{hex}	0105 _{hex}	Ownership conflict or OUNID mismatch. The configuration is already owned by another originator
01 _{hex}	0106 _{hex}	Ownership conflict or OUNID mismatch. The output connection was already owned by another originator
01 _{hex}	0205 _{hex}	Parameter Error in Unconnected Send service or Parameter Error in SafetyOpen or SafetyClose
01 _{hex}	801 _{hex}	Incompatible Multipoint RPI. An existing connection has been established at a different RPI
01 _{hex}	802 _{hex}	Invalid Safety Connection size
01 _{hex}	803 _{hex}	Invalid Safety Connection format
01 _{hex}	804 _{hex}	Invalid Time Correction Connection Parameters
01 _{hex}	805 _{hex}	Invalid Ping Interval EPI Multiplier
01 _{hex}	806 _{hex}	Time Coordination Msg Min Multiplier
01 _{hex}	807 _{hex}	Network Time Expectation Multiplier
01 _{hex}	808 _{hex}	Timeout Multiplier
01 _{hex}	809 _{hex}	Invalid Max Consumer Number

General status	Extended status	Explanation
01 _{hex}	80A _{hex}	Invalid CPCRC
01 _{hex}	80B _{hex}	Time Correction Connection Id invalid
01 _{hex}	80C _{hex}	SCID Mismatch. The SCID was non-zero and did not match the value in the target
01 _{hex}	80D _{hex}	TUNID not set. Device is out-of-box and TUNID has not been set, so connections are not allowed
01 _{hex}	80E _{hex}	TUNID Mismatch. The TUNID provided does not match. The message was likely routed to this node in error
01 _{hex}	80F _{hex}	Configuration operation not allowed

Event/Error Matrix Table 17 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 17 – SafetyOpen error event guidance table

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

Event	Error type	General status	Extended status
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: 01hex

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.

6.4.2 Changes to common services

Table 18 defines the services of the Identity object that require updates.

Table 18 – Identity object common service changes

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

6.4.3 Extensions for CP 16/3 devices

Extensions of the Identity object for CP 16/3 devices are specified in Table 19.

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 19 – 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				

6.5 Link objects

6.5.1 DeviceNet object changes

6.5.1.1 Additional attribute for safety

Class Code: 03hex

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 20.

Table 20 – 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 21.

Table 21 – 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 22.

Table 22 – 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 23.

Table 23 – 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	DINT	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	INT	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	INT		
			Error counter Port2	INT		
6	Optional	Get	SERCOS [®] Address	INT	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 24.

Table 24 – 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 to 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 25.

Table 25 – 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 Safety Supervisor are defined in Table 26.

Table 26 – Safety Supervisor instance attributes

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

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

Attr ID	Need in implementation	Access rule	NV	Name	Date type	Description of attribute
22	Conditional – Required if Calibration Expiration is supported	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 only by “Configuration Lock/Unlock” Service Gettable	NV	Configuration Lock	BOOL	Marks the device configuration contained within as Verified and locked, or alternatively as unverified, unlocked, and changeable
25	Conditional ^c	Get	NV	Configuration UNID	10 octets	CFUNID – Identifies the owner of a Device Configuration: All FF _{hex} = Tool-only configuration. 0 = un-owned, accept any owner
26	Required	Get	NV	Safety Configuration Identifier	10 octets	The SCID is comprised of the Safety Configuration CRC + Safety Configuration Time Stamp. This is the signature for the Configuration
27	Required	Get	NV	Target UNID	10 octets	The current UNID of the device
28	Conditional ^d	Get	NV	Output Connection Point Owners		
				Number of Array Entries	UINT	Number of OCPUNID STRUCT entries
				Output Owners	ARRAY of STRUCT	
				OCPUNID	10 octets	The owner UNID for the output resource. 0 = un-owned, accept any owner (default)
				ePath Size	USINT	Path size, number of octets
				Application Resource	Packed ePath	The path to owned resource (i.e. 20 04 24 01 – Assembly class, instance 1)
29	Conditional ^c	Get	V	Proposed TUNID	10 octets	The UNID value that an originator is attempting to set in the device
97-98	Reserved by FSCP 2/1 for Future Use					

Attr ID	Need in implementation	Access rule	NV	Name	Date type	Description of attribute
99	Conditional ^b	Get	NV	Subclass	UINT	Identifies a subset of additional instance attributes, services, and behaviors
^a The nonvolatile behavior of the Time attribute is conditional on the value of the Clock Power Cycle Behavior attribute. ^b If the value of Subclass is 00 which identifies "no subclass", then this attribute should be in implementation, otherwise, this attribute shall be in implementation. ^c Safety devices which support the SNCT interface (i.e. not configured by the SafetyOpen or some vendor specific means) shall support this attribute. ^d Conditional – the Output Connection Owner attribute shall be supported for all safety output assemblies.						

6.6.5 Semantics

6.6.5.1 Manufacturer name

The Manufacturer Name attribute identifies the manufacturer of the device.

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

6.6.5.2 Software revision level

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

6.6.5.3 Hardware revision level

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

6.6.5.4 Manufacturer's serial number

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

6.6.5.5 Device status

This attribute represents the current state of the device. Its value changes as the state of the device changes. The Device status attribute state values are defined in Table 27.

Table 27 – 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
51-99	Device specific
100-255	Vendor specific

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 28. 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 28 – 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 29. The SIZE for this revision is two (2). The criteria details for each exception condition are outside the scope of this part.

6.6.5.9 Common exception detail attribute values

Table 29 – 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.	

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 30), 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 30 – 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-process or	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 definition.								

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 Form 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}.

When the Configuration UNID attribute is set to “No owner, accept any”, FSCP 2/1 safety devices shall capture the first configuration source (Form 1 and/or Configure_Request) as the owner (see Table 31).

The CFUNID value is used in conjunction with the OUNID value provided in either the Configure_Request or a Form 1 SafetyOpen. See Table 31 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 31 – 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
Form 1 SafetyOpen	Fail	Accept Set CFUNID = OUNID	Accept only if CFUNID = OUNID Fail otherwise

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.

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.

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

The UNID 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 setting operation.

A device in Manufacturers default state shall have an invalid UNID value in its NV (for example FF_{hex}, FF_{hex}, FF_{hex}, FF_{hex}, FF_{hex}, FF_{hex}).

The UNID 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 (OUNID)

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

While a device is going through the “ProposeTUNID/ApplyTUNID” 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.

6.6.6 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} 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 32. The Safety Supervisor object specific services are defined in Table 33.

Table 32 – Safety Supervisor common services

Service code	Need in implementation		Service name	Description of service
	Class	Instance		
0E _{hex}	Conditional	Required	Get_Attributes_Single	Returns the contents of the specified attribute
010 _{hex}	n/a	Required	Set_Attributes_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 33 – 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
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 Required, 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

Service code	Need in implementation		Service name	Description of service
	Class	Instance		
57 _{hex}	n/a	Conditional ^d	Apply_TUNID	Used to complete the TUNID setting 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 for FSCP 2/1 safety devices which support the SNCT interface but highly recommended for devices which are configurable by Form 1 SafetyOpen but don't support the SNCT interface.				

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_Diagnostics 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 part.

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 34.

Table 34 – 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 35.

Table 35 – 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 36.

Table 36 – 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

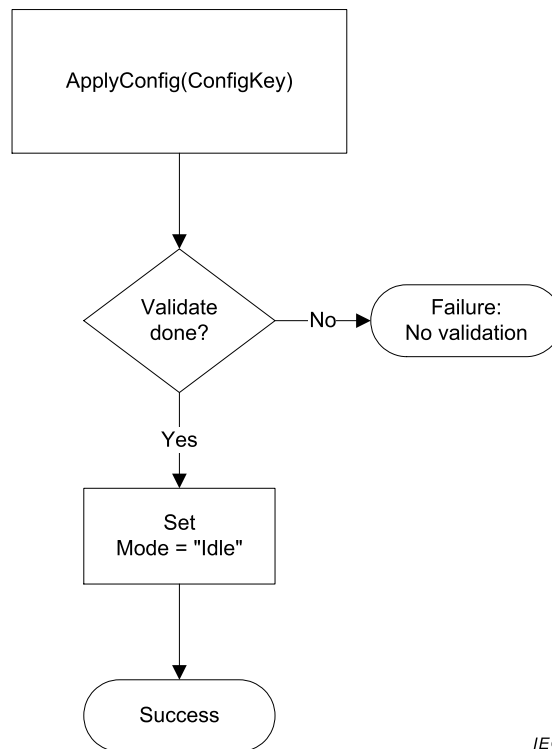
If the Safety Supervisor Validate_Configuration command does not succeed, the error response shall send a class defined “Validation Error” (D0_{hex}). The following error code defined in Table 37 is defined as a Validation Error in the Safety Supervisor, additional error codes are defined in Table 38.

Table 37 – Validate_Configuration error code

General error code	Additional error code	Error name	Description
D0 _{hex}	see Table 38	Validation Error	This error is a class specific error for the Safety Supervisor and is returned in response to a Validate_Configuration error

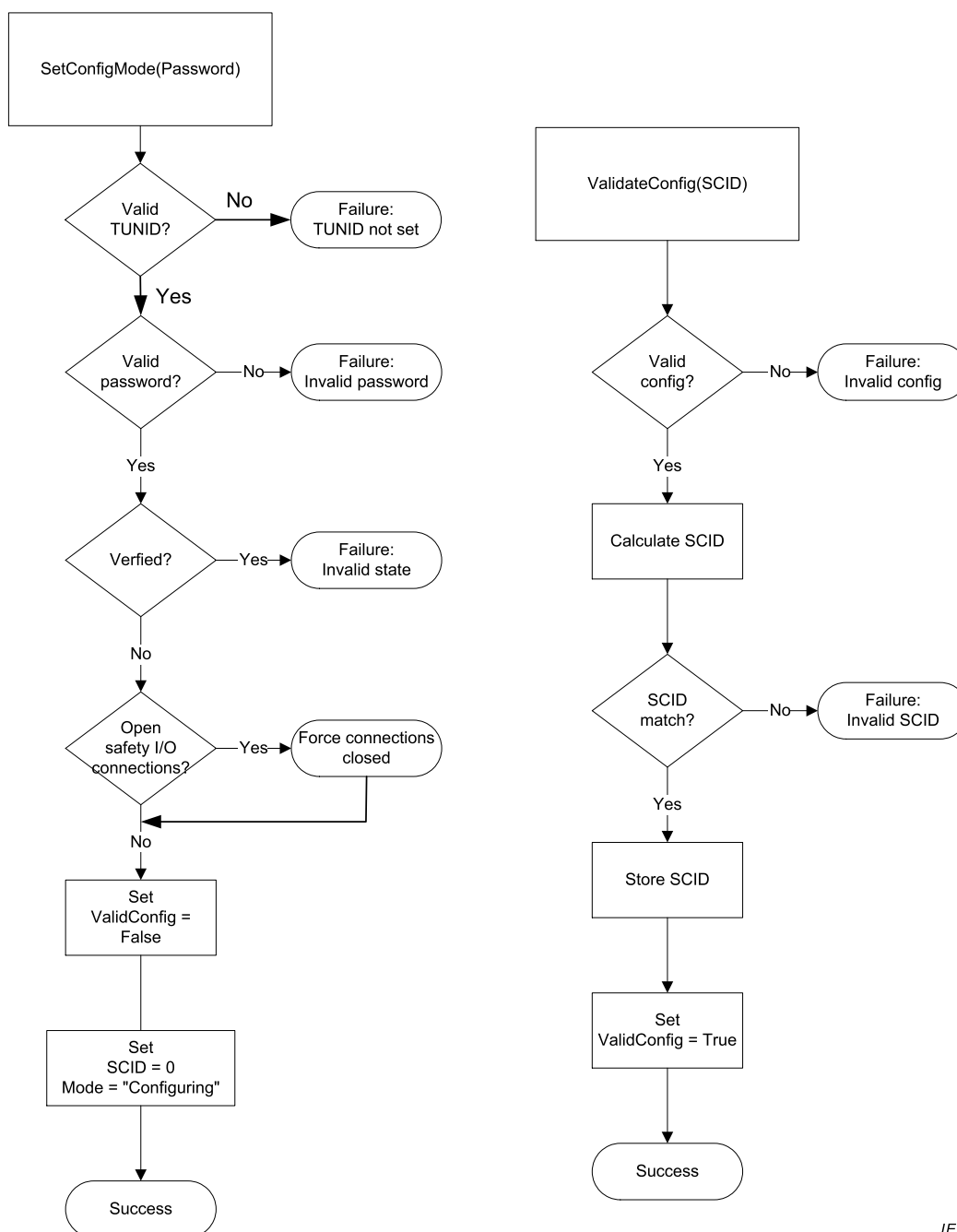
Table 38 – Validate_Configuration extended codes

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



IEC

Figure 10 – Applying device configuration



IEC

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 39.

Table 39 – 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 40.

Table 40 – 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 41.

Table 41 – 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 42.

Table 42 – 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 43.

Table 43 – Safety_Reset message structure

Name	Data type	Description
Service Code	USINT	54 _{hex}
Reset type	USINT	see Table 44
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 45

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 44 – 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 45 – 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 46 shows how a safety device shall process the various reset types based on the Lock/Unlock condition and safety connection status.

Table 46 – 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 47.

Table 47 – 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 behavior 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
        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 48 and a processing flow chart is defined in Figure 12.

Table 48 – Apply_TUNID service

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

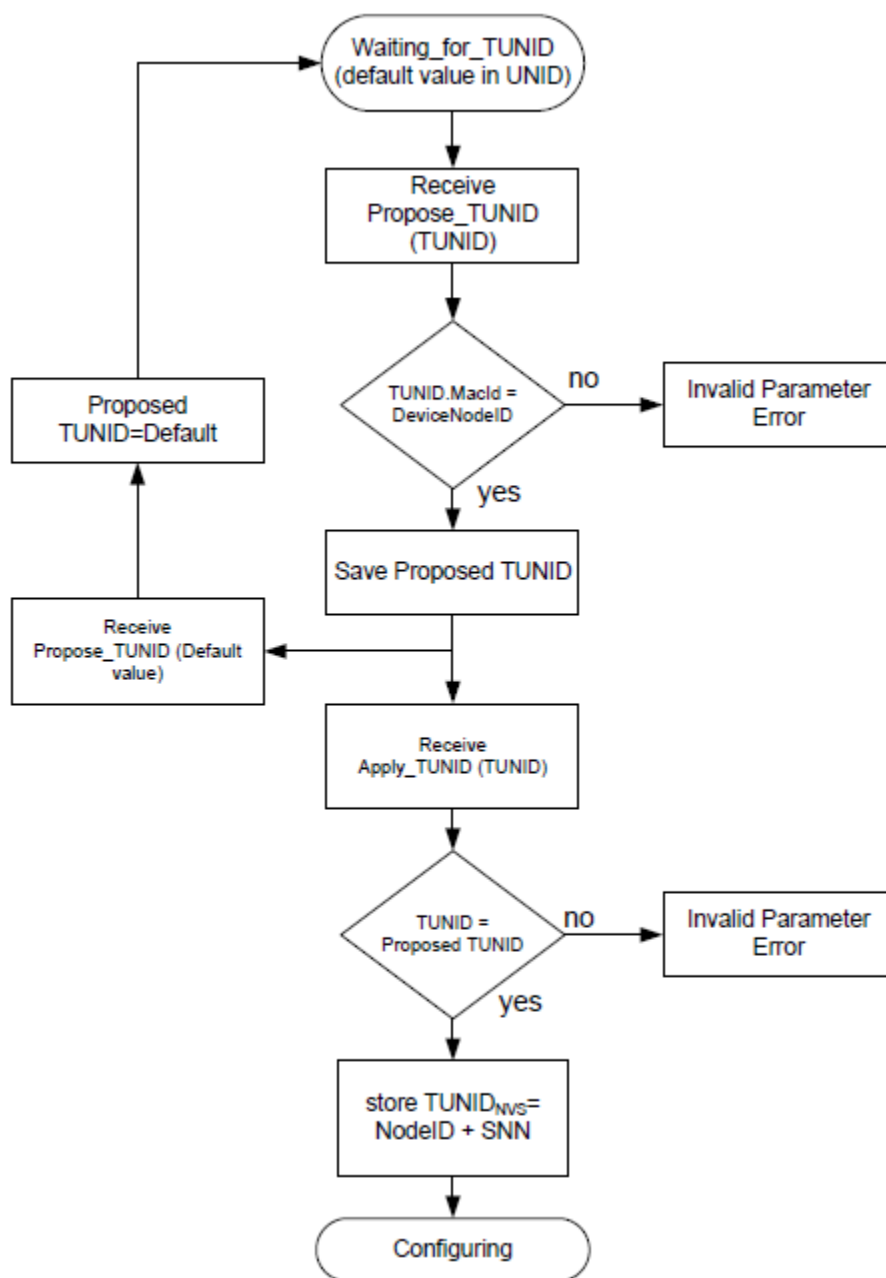
The Apply_TUNID service shall validate the TUNID against the proposed value, stops the LED flashing, saves the TUNID to nonvolatile storage, updates the TUNID attribute in the Supervisor, and sets the proposed_TUNID attribute to all FF_{hex}. The Supervisor shall then transition to Configuring.

The following pseudo code defines the behavior 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
    }
}

```

IEC

Figure 12 – UNID handling during “Waiting for TUNID”

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 49.

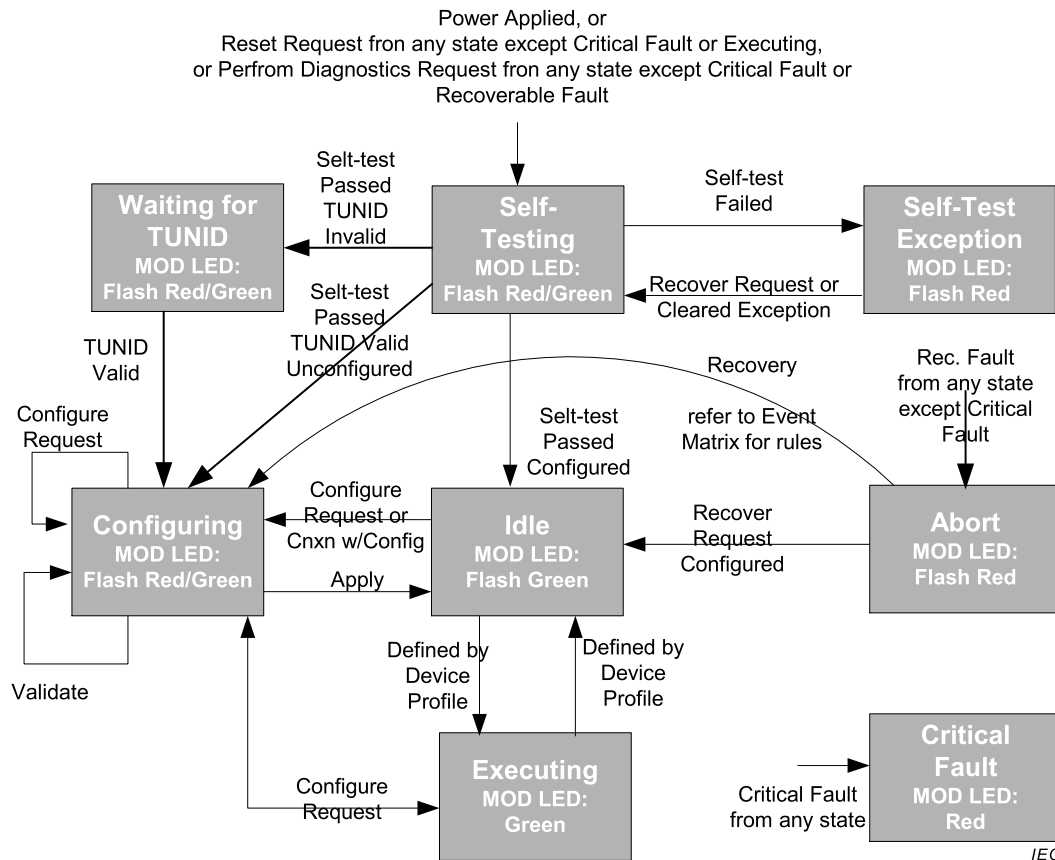


Figure 13 – Safety Supervisor state diagram

Table 49 – 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. Object services cannot be processed. The conditions required for exit from a critical fault is outside the scope of this part

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 part.

6.6.8.2 Safety Supervisor state event matrix

Table 50 defines the states and events for the Safety Supervisor.

Table 50 – 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 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 Configuring	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
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

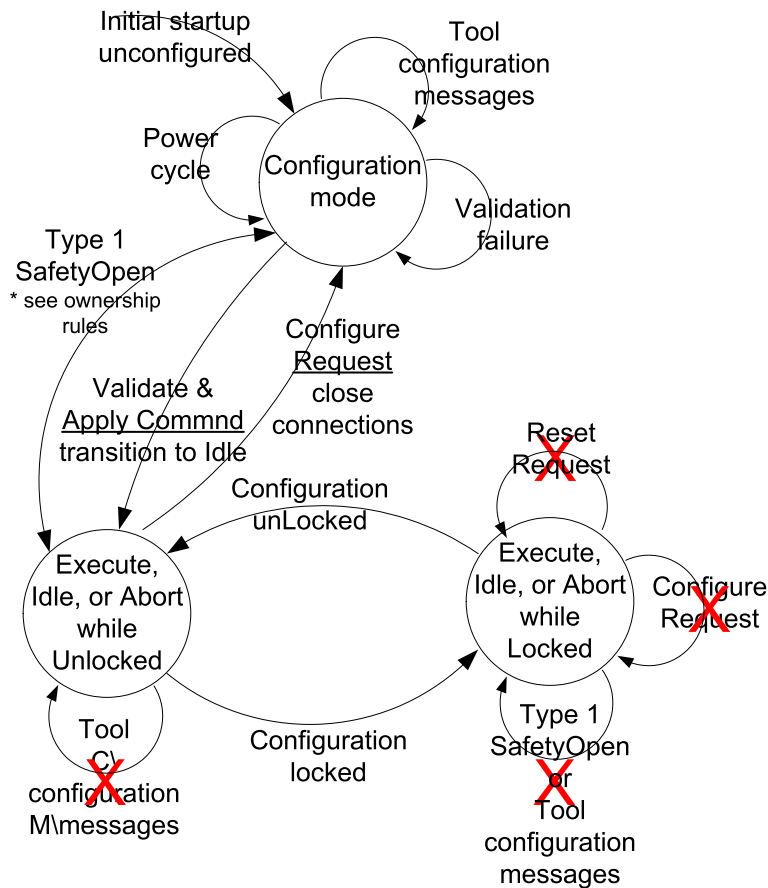
Event	State							
	Waiting for TUNID	Configuring (Safety State)	Idle (Safety State)	Self-Test (Safety State)	Self-Test Exception (Safety State)	Executing	Abort (Safety State)	Critical Fault (Safety State)
Configure Request	Error TNS ^c	Stay in state Validate and accept	If not Locked, Transition to Configuring	Error OSC ^b	Error OSC ^b	If not Locked, Drop Connections Apply Safety State Go to Configuring	If Configured: Transition to IDLE --- Unconfigured: 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
Form 1 SafetyOperation	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 Connections, Transition to Configuring, Proceed to IDLE EXECUTING dependent on Profile	Error OSC ^c	Error OSC ^b
Reset Request	Process type Transition to SELF TEST	Process type Transition to SELF TEST	If not Locked, Process type Transition to SELF TEST	Process type Transition to SELF TEST	Process type Transition to SELF TEST	If not Locked, Process type Transition to SELF TEST	If not Locked, Process type Transition to SELF TEST	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

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 Configured: Transition to IDLE --- Unconfigured: Transition to Configuring --- If Switch/TUNID mismatch Error OSC ^b	Error OSC ^b
Perform Diagnostic 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	Error OSC ^b
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.

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.



IEC

Figure 14 – Configuration, testing and locked relationships

Table 51 defines the effect that ownership has on a device’s ability to be configured. It shows that owned devices can only be Form 1 configured by the originator that has the owner UNID. A locked device can never be configured regardless of its ownership.

Table 51 – Configuration owner control vs. device state

Ownership rules	Configure mode	Execute/Idle Mode Unlocked	Execute/Idle Mode Locked
Config Owned (Config. OUNID = Owner UNID)	Form1 accepted by owner only	Form1 accepted by owner only	All Form 1 rejected
Config Un-owned (Config. OUNID = 0)	Form1 accepted from anyone	Form1 accepted from anyone	All Form 1 rejected
SW Tool Owned (Config. OUNID = all FF _{hex})	No Form 1 accepted	No Form 1 accepted	All Form 1 rejected

6.6.8.4 State mapping of Safety Supervisor object to Identity object

Table 52 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 52 – 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 53 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 53 – 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
Form 1 SafetyOpen	No equivalent event
Reset Request	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

6.6.8.6 Identity object event to Safety Supervisor event mapping

Table 54 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 54 – 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

6.7 Safety Validator object

6.7.1 General

Class Code: 3Ahex

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 55.

Table 55 – 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 56.

Table 56 – 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 μ s increments it could take for a Time Coordination Message to traverse from the consumer to the producer	0 – 7 813
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	

Attr ID	Need in Implementation	Access rule	NV	Name	Data type	Description of attribute	Semantics of value
				Network Time Expectation Multiplier	Array of: UINT	Maximum number of 128 μ s 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
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 μ s increments. Attribute only used for Safety Consumers	

Attr ID	Need in Implementation	Access rule	NV	Name	Data type	Description of attribute	Semantics of value
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.							

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 57. This attribute can be used to determine the condition of established safety connections.

Table 57 – 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 58. Targets shall derive this value from the Safety Connection parameters in the SafetyOpen.

Table 58 – 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.

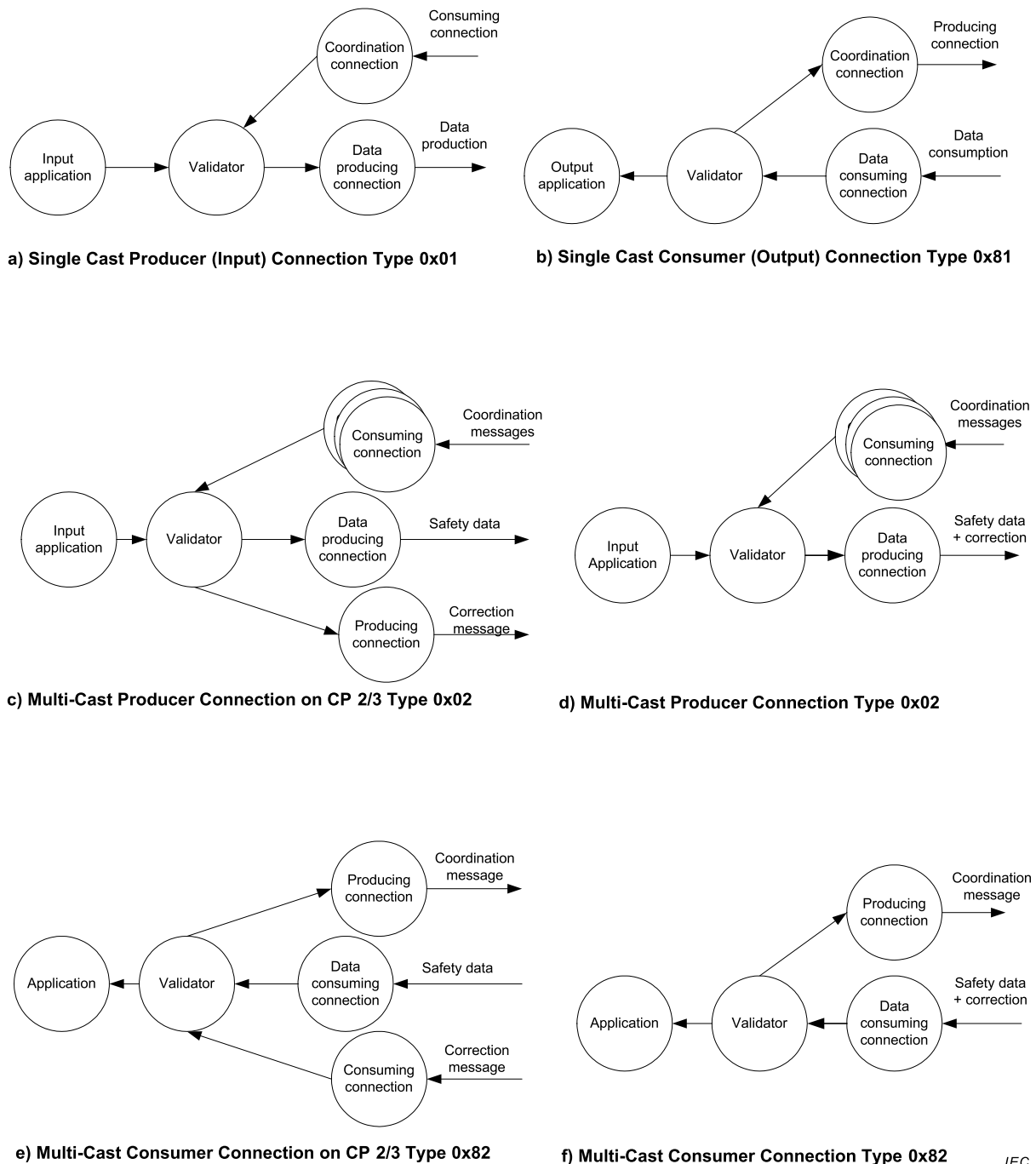


Figure 15 – Safety connection types

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 59.

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 59.

Table 59 – 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 59.

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 59.

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 59.

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.

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 μ s 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 60.

Table 60 – 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 61.

Table 61 – 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 62.

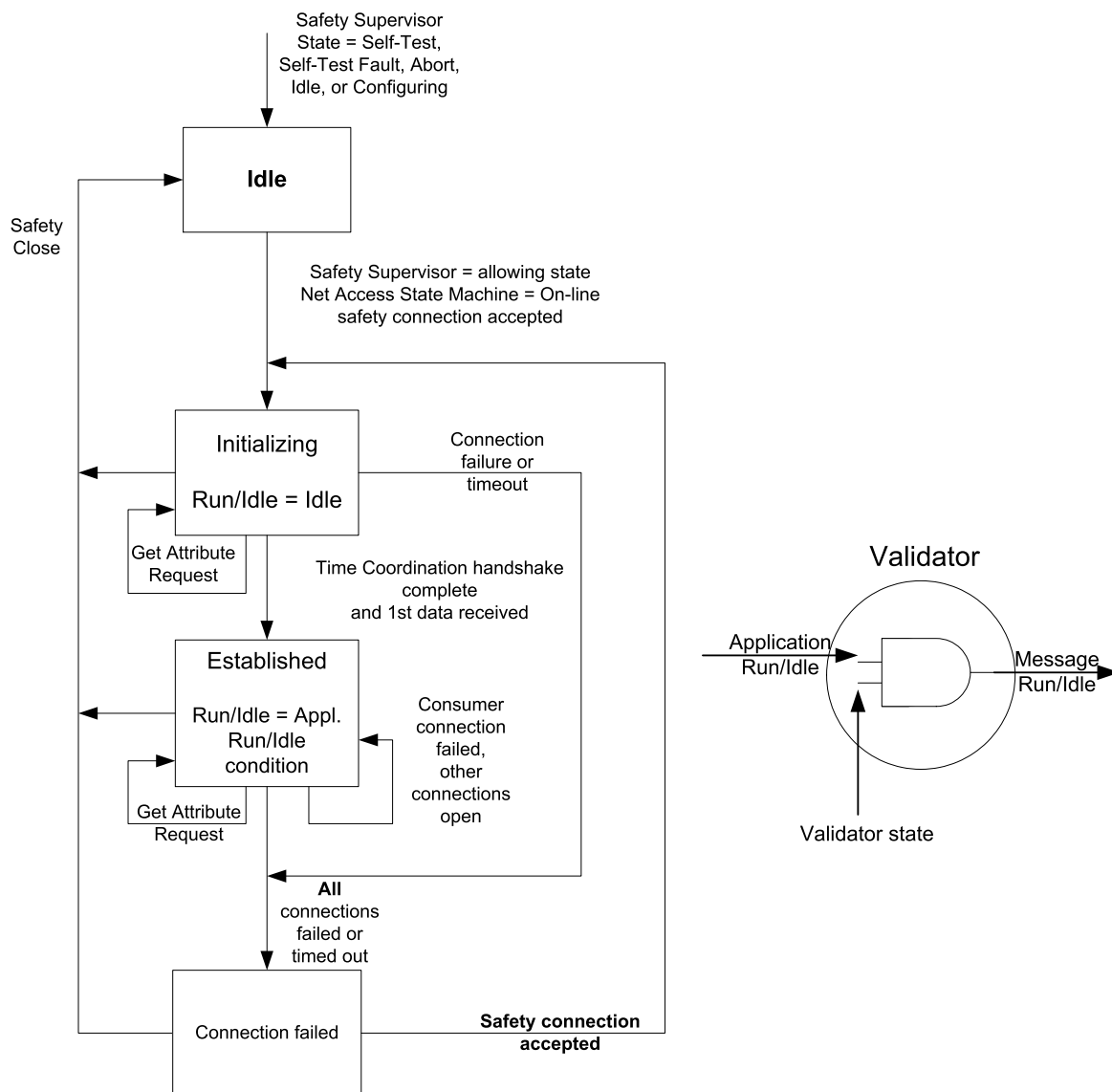
Table 62 – Safety Validator Get_Attributes_All service data

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 63.



IEC

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 63 is the state event matrix that defines the Safety Validator behavior. Table 64 maps the Safety Validator states to the Safety Supervisor states.

Table 63 – 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

Table 64 – 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 65.

Table 65 – 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 66 defines the instance attributes and changes for use by FSCP 2/1 devices.

Table 66 – 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	

Attr ID	Need in implem.	Access rule	NV	Name	Data type	Description of attribute	Semantics of value
				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
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 and 10 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		

Attr ID	Need in implem.	Access rule	NV	Name	Data type	Description of attribute	Semantics of value
				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
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	Used by both producers and consumers to determine how many erroneous packets can be dropped before a connection shall be closed	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 67.

Table 67 – 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 should timeout.

The timeout value for the connection is defined as:

$$\text{Connection RPI} \times (\text{CTM} + 1) \times 4$$

Range: 0 to 7

where

$$0 = (0 \times 4);$$

$$1 = (0 \times 8);$$

$$2 = (0 \times 12);$$

$$3 = (0 \times 16);$$

$$4 = (0 \times 20);$$

$$5 = (0 \times 24);$$

$$6 = (0 \times 28);$$

$$7 = (0 \times 32).$$

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 68.

Table 68 – 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 is 1 (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 69.

Table 69 – 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).

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 70 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 70 – Data map formats

Format number	Format name	Data Map data S\size (in octets)	Data Map data	Comment
0	Open scanner format	4 octets	See Table 71	Simple format which maps data in word granularity to input and output image tables
1	Octet-Index Scanner format	4 octets	See Table 72	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 71.

Table 71 – 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 72.

Table 72 – 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

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 μ s 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_Multiplier 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 μ s 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.

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 73.

Table 73 – 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 74.

Table 74 – 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 shown in Table 75.

Table 75 – 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.

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 be used in limited application scenarios where connection repeatability can be guaranteed.

6.8.5.14 Format Type

Table 76 defines the meaning of the Format Type attribute.

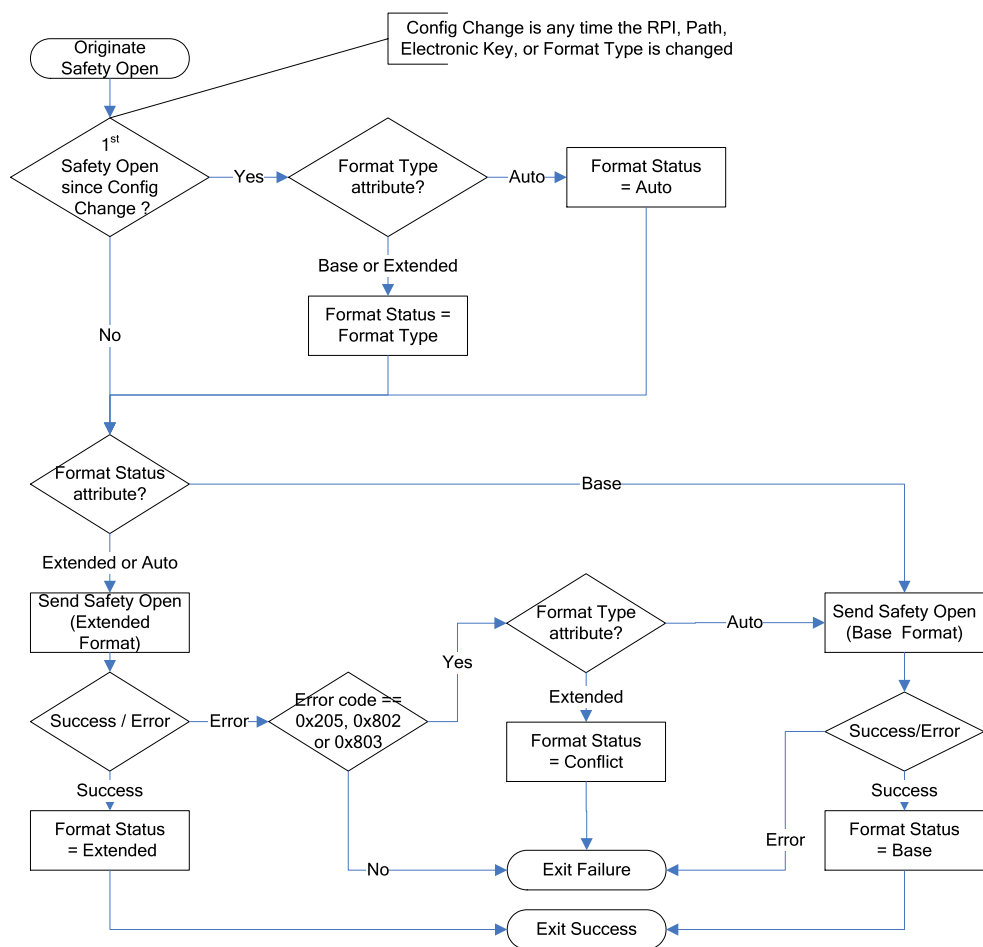
Table 76 – Format Type attribute meaning

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:



IEC

Figure 17 – Logic for Auto-detecting format type

6.8.5.15 Format Status

Table 77 defines the meaning of the Format Status attribute.

Table 77 – 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

6.8.6 Object-specific services

The Connection Configuration Object provides the following Object Specific Services, defined in Table 78.

Table 78 – 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 79 and Table 80. 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 79 – 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
Connection Parameter CRC	UDINT	CRC-32 over the connection parameters used in a SafetyOpen

Name	Data type	Description
Configuration Instance	UINT	
ID Allocation Flag	BOOL	
Target Connection Serial Number	UINT	Safety Validator Instance returned from Target during connection establishment

Table 80 – 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 81 and Table 82. 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 81 – 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	

Table 82 – 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 83, Figure 18, and Figure 19.

Table 83 – 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

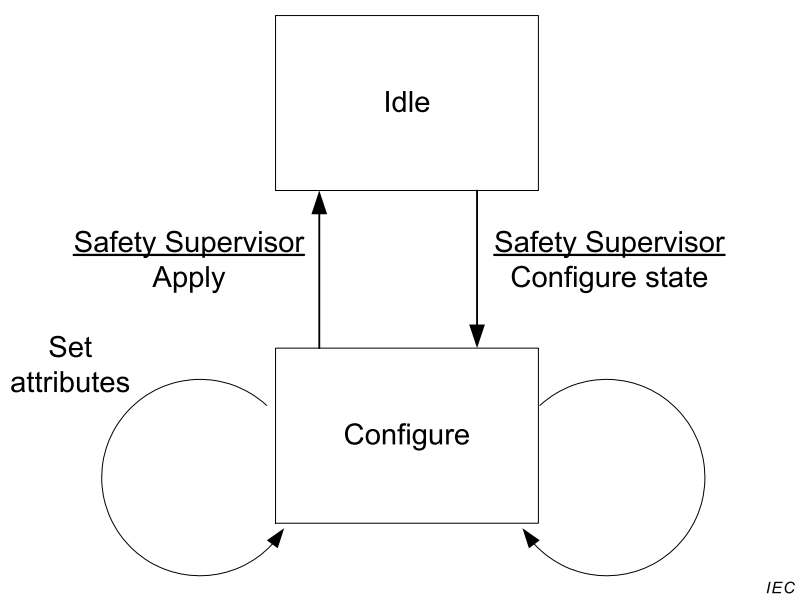
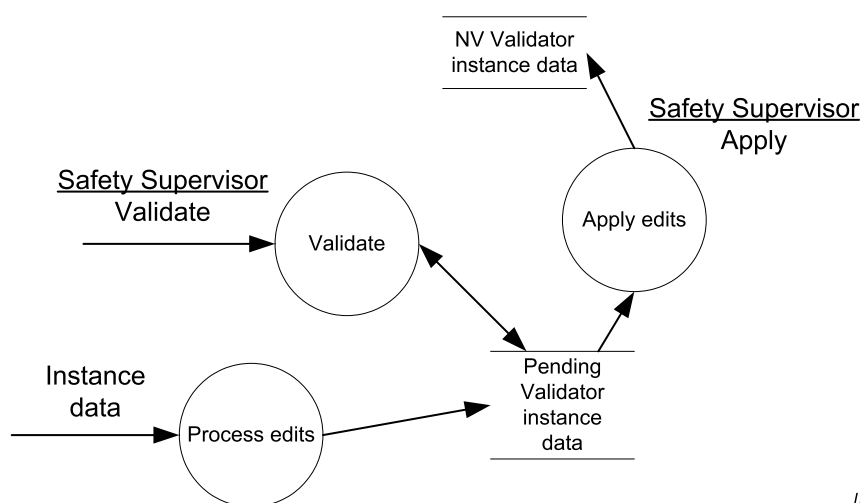


Figure 18 – Connection Configuration Object state diagram

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



IEC

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

Table 84 – 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.

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 85.

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 85 – 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

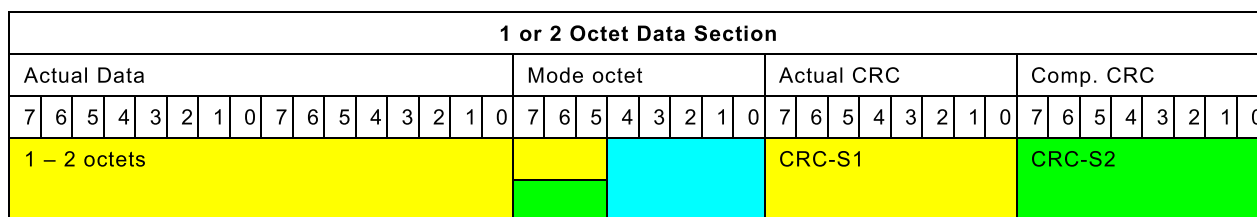
7.1.1.3 Mode octet CRC processing for Base Format

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.



Key

- = Covered by actual data CRC
- = Covered by the complemented data CRC
- = Covered by the Time Stamp Section CRC

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).

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 octet 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
2 octets	1 octet		2 octets		2 octets
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 octet 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 complemented 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

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).

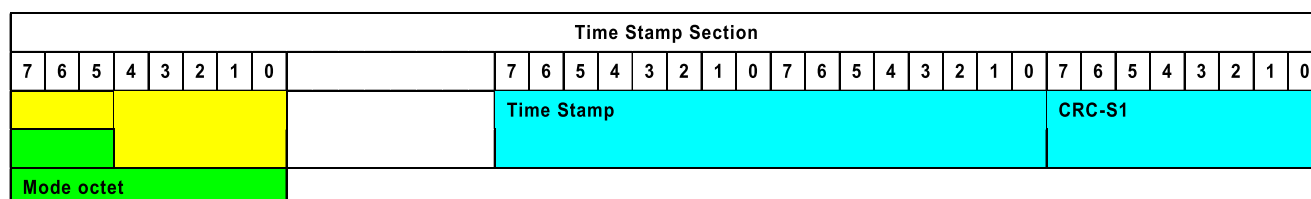
The EF 3-to250 Octet Complement Data CRC calculation shall include:

- 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 86.

**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 86 – 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:

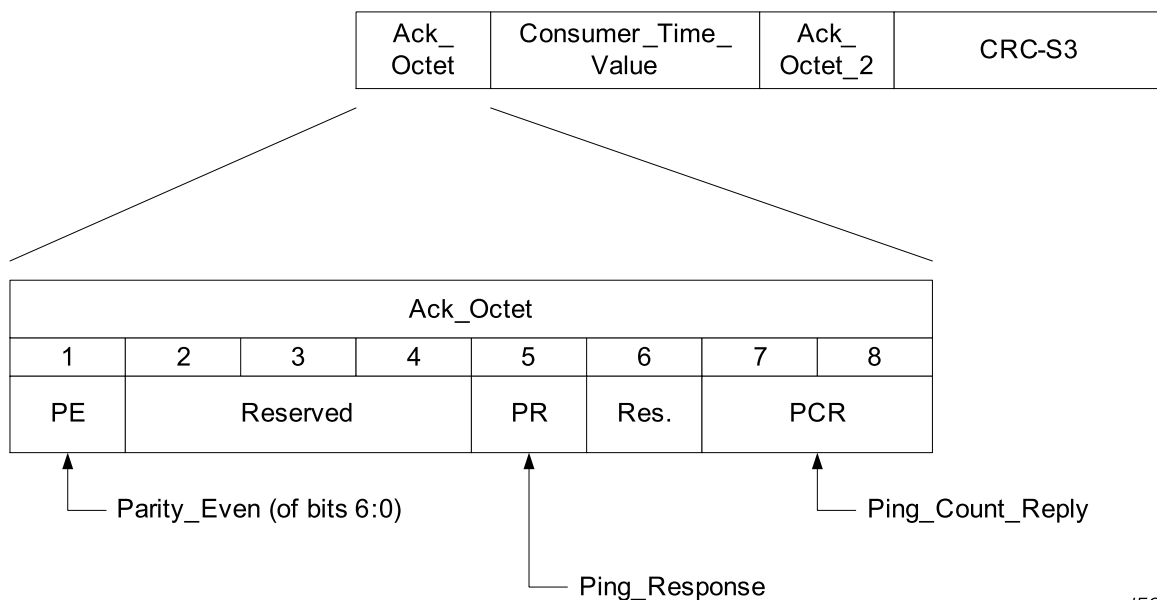
- Producer Identifier octet (PID) (by CRC-S1);
- The (Mode Octet) AND (1F_{hex}) (by CRC-S1);
- Time Stamp octet(s) (by CRC-S1).

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 87.



IEC

Figure 26 – BF Time Coordination message encoding



Figure 27 – EF Time Coordination message encoding

Table 87 – 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.

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

$$\text{Ack\_Octet\_2} = ((\text{Ack\_Octet} \text{ XOR } \text{FF}_{\text{hex}}) \text{ AND } 55_{\text{hex}}) \text{ OR } (\text{Ack\_Octet} \text{ AND } \text{AA}_{\text{hex}}).$$

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 than the produced data. The Time Correction message sends consumer specific information to the consumer at a slower rate than the produced data. The encoding for the BF time correction message is 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 88.

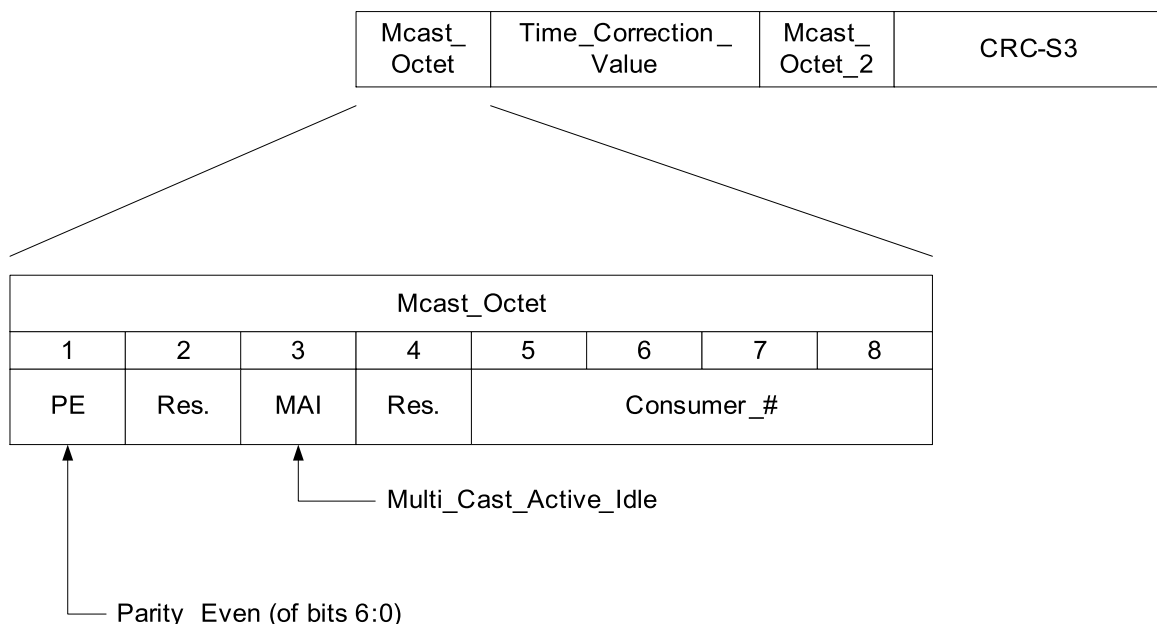


Figure 28 – BF Time Correction message encoding



Figure 29 – EF Time Correction message encoding

Table 88 – 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:

$$\text{Mcast\_Octet\_2} = ((\text{Mcast\_Octet} \text{ XOR } \text{FF}_{\text{hex}}) \text{ AND } \text{55}_{\text{hex}}) \text{ OR } (\text{Mcast\_Octet} \text{ AND } \text{AA}_{\text{hex}}).$$

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.

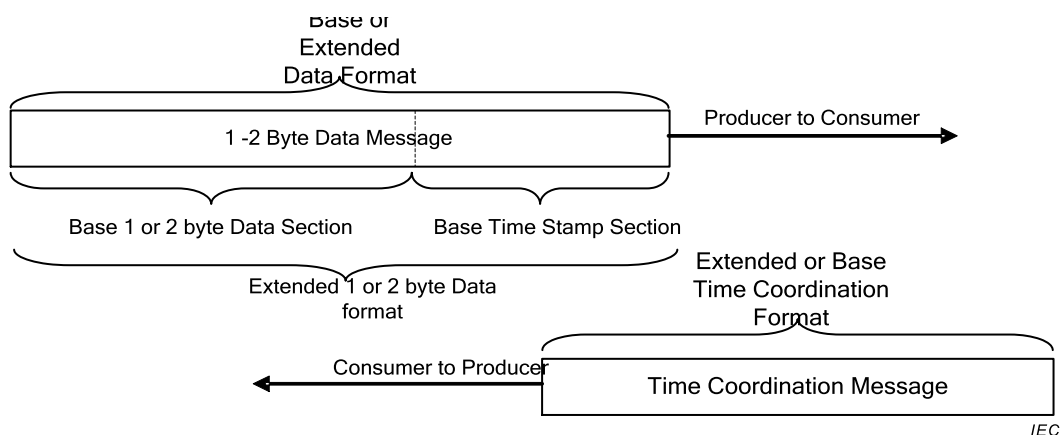


Figure 30 – 1 or 2 octet point-to-point PDU encoding

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.

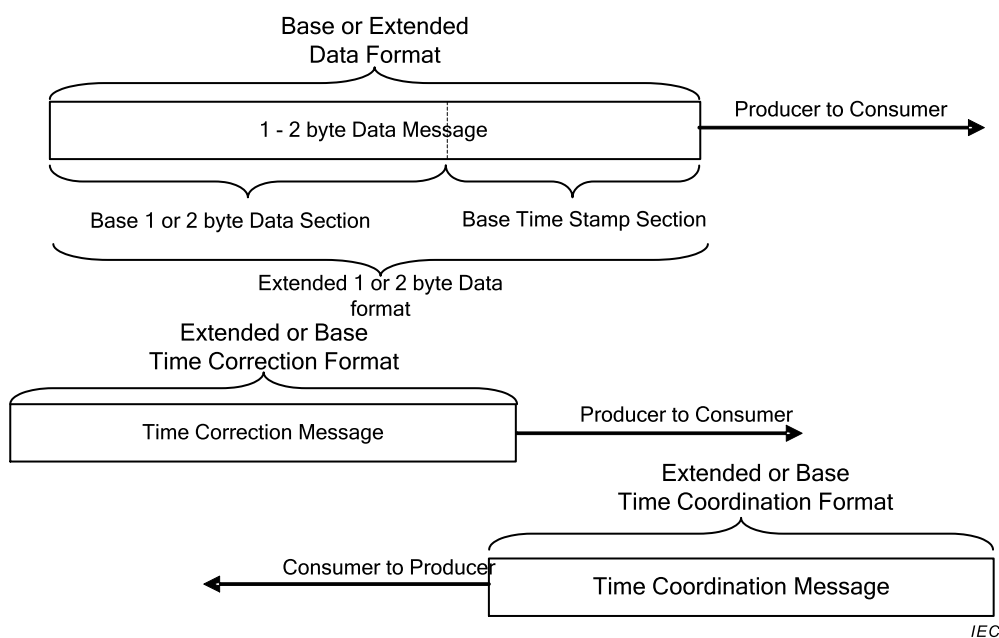


Figure 31 – 1 or 2 Octet multipoint PDU encoding

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.

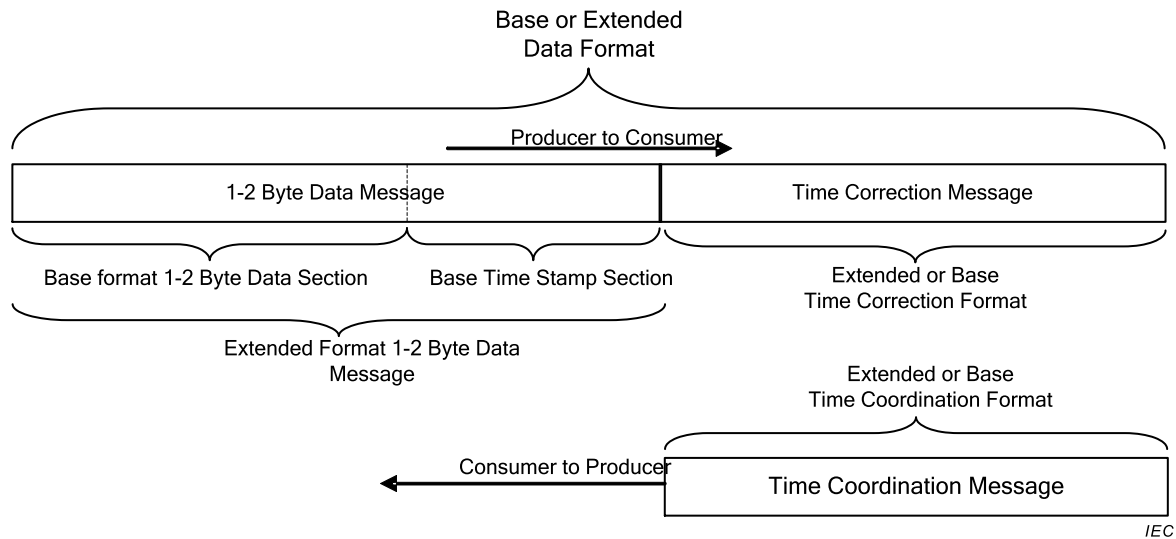


Figure 32 – 1 or 2 Octet, multipoint, Format 2 safety connection format

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.

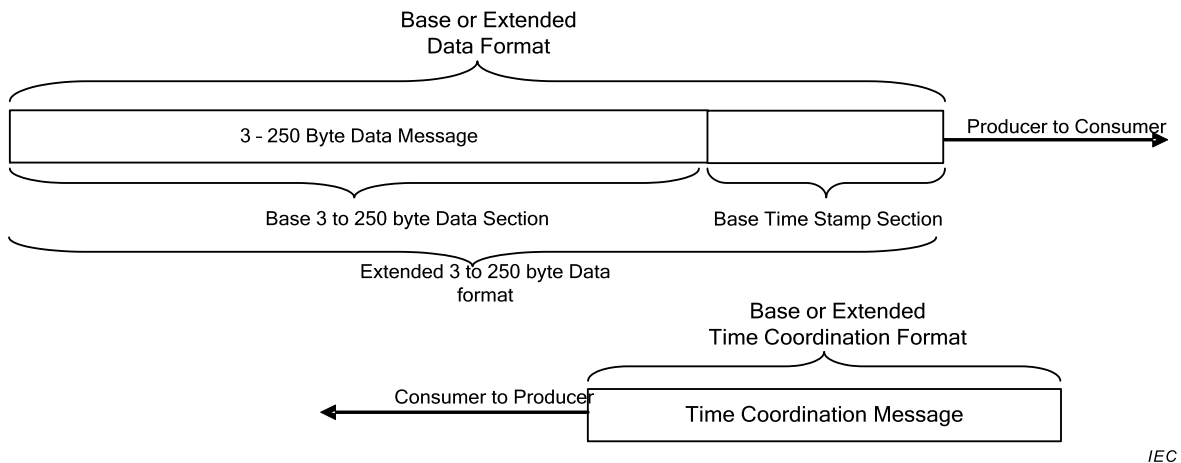


Figure 33 – 3 to 250 Octet Point-to-point PDU encoding

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.

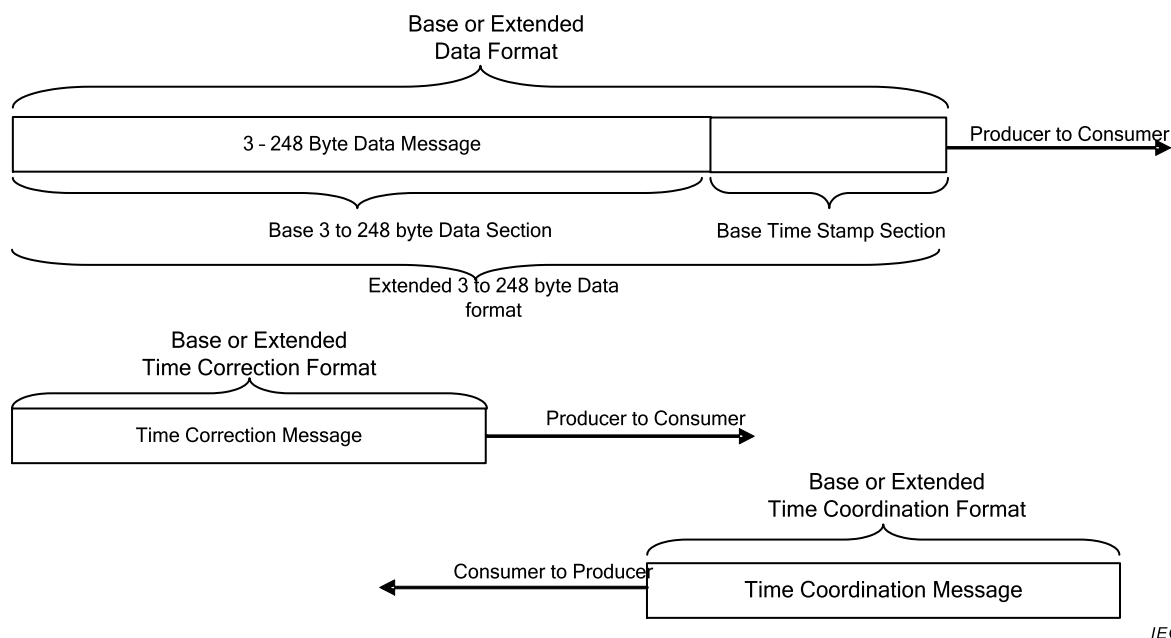


Figure 34 – 3 to 248 Octet Multipoint PDU encoding

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.

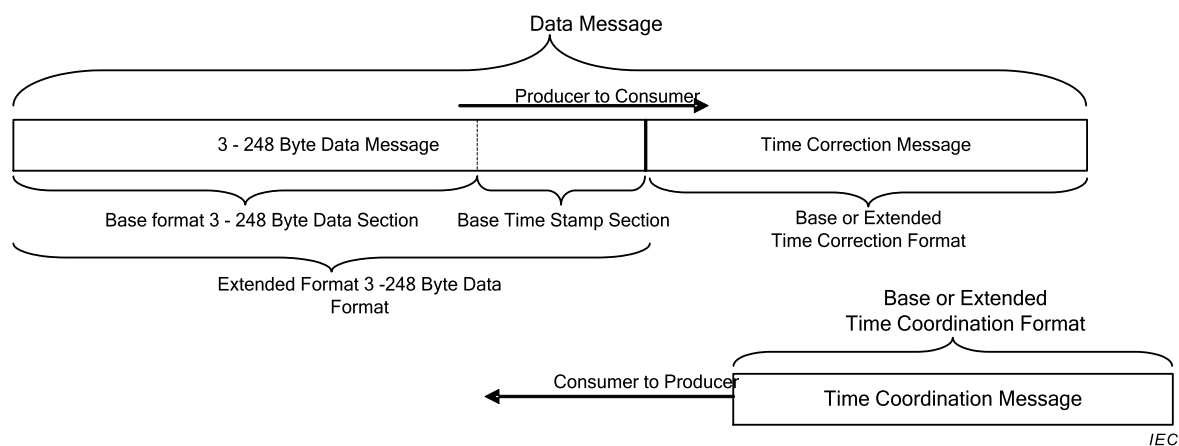
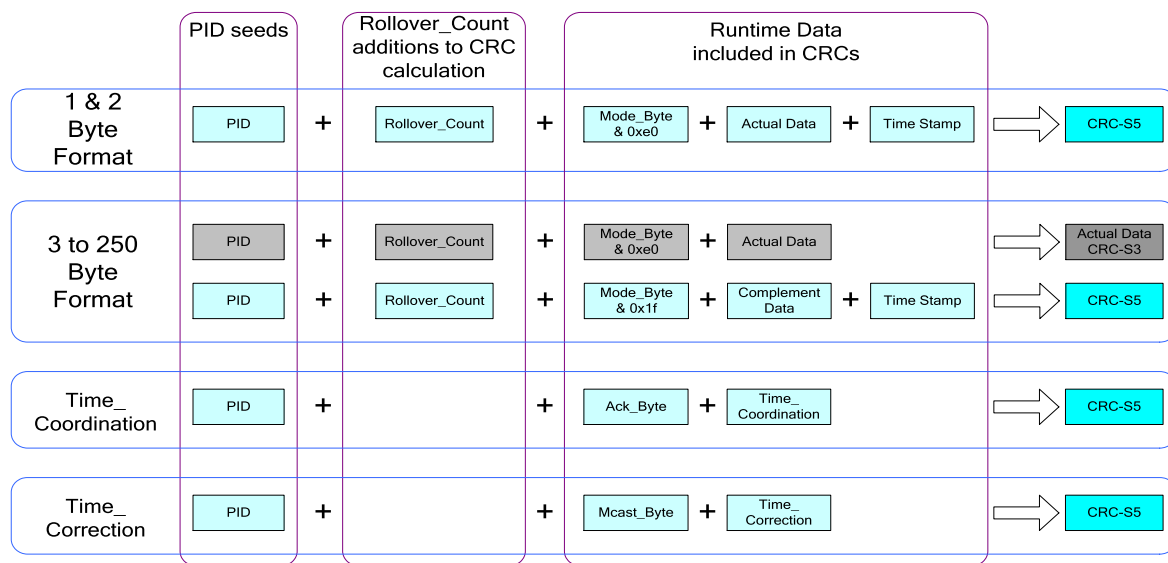


Figure 35 – 3 to 248 Octet, Multipoint, safety connection format

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.



IEC

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.

7.1.2.2 CRC polynomials

Table 89 defines the polynomials used in FSCP 2/1.

Table 89 – 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}

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 90 defines which algorithm is used and the starting seed value for each use.

Table 90 – Connection sections and message formats

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.

- Ping count check;
- Evaluate Time stamp section CRC;
- Evaluated Time Stamps;
- Evaluate Actual Data CRC;
- Evaluate Complement Data CRC;
- 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.

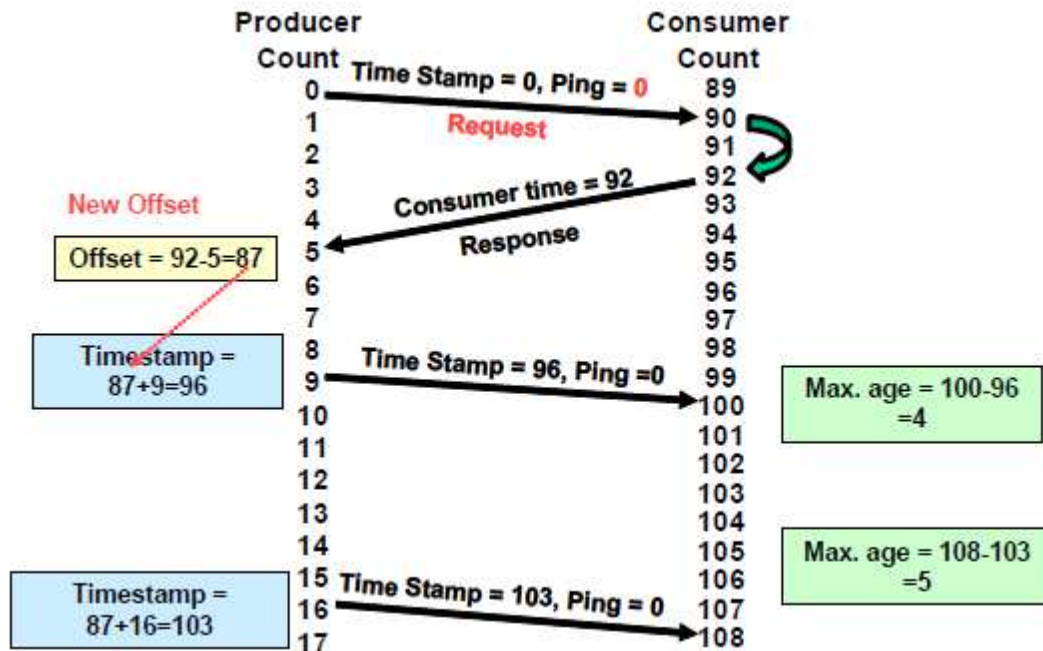
- The safety layer detects an error requiring termination.
- The safety layer notifies the application program by setting the connection status to indicate a safety communications fault.
- The safety-related application shall transition data and I/O (for example set outputs to the safety state) associated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



IEC

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 too old to use and the connection is terminated.

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 bold 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.

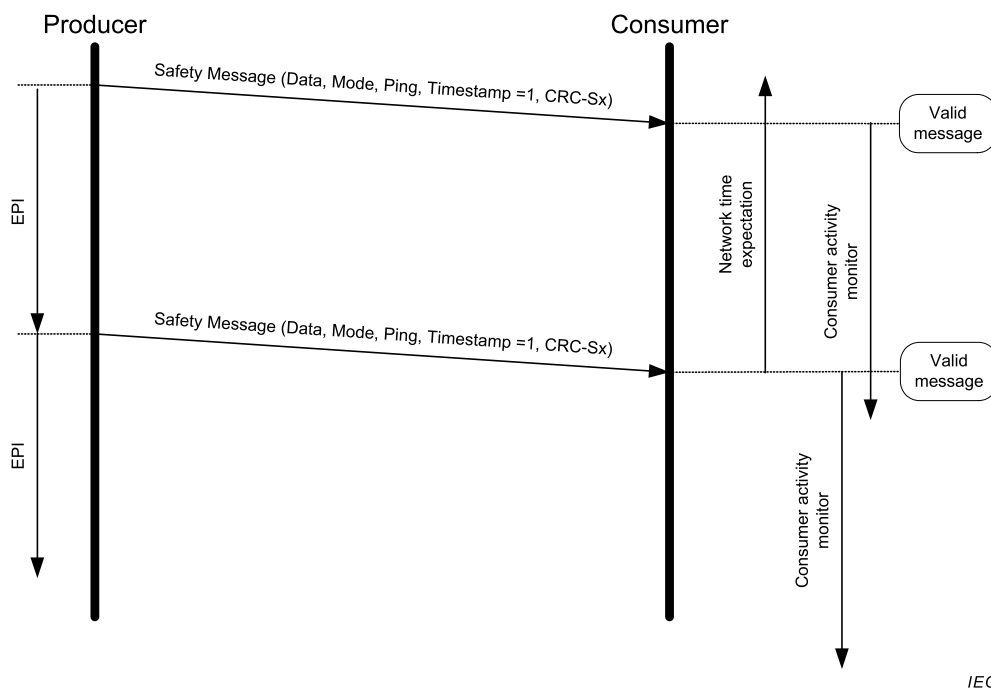


Figure 38 – Sequence diagram of a normal producer/consumer safety sequence

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

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.

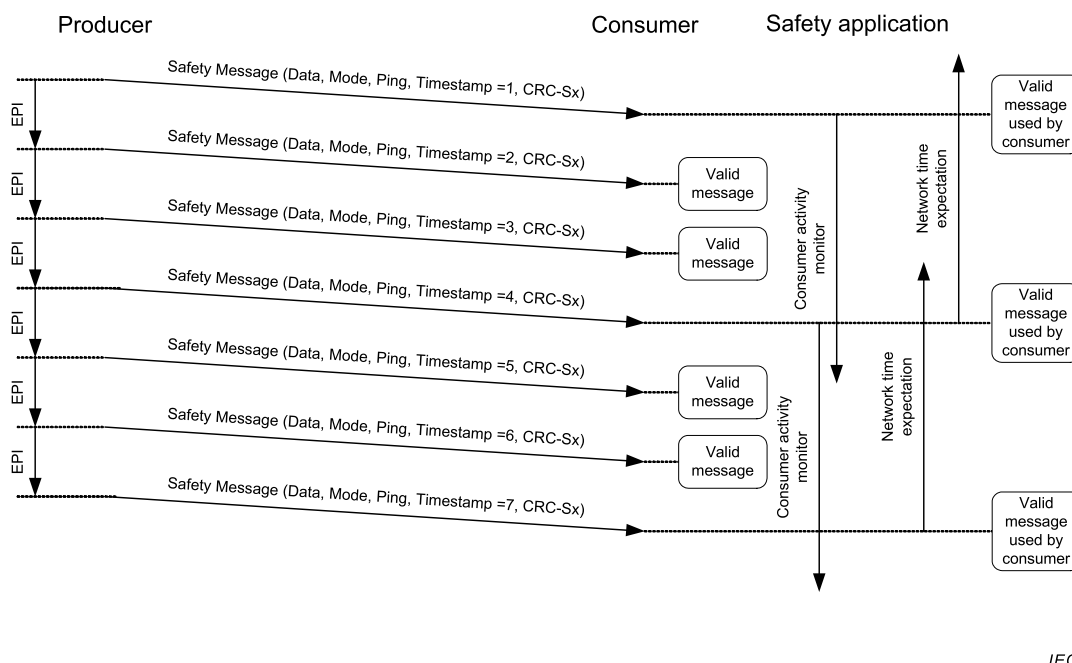


Figure 39 – Sequence diagram of a normal producer/consumer safety sequence (production repeated)

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.

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 $\geq$ Max_Fault_Number) (see 7.2.2).

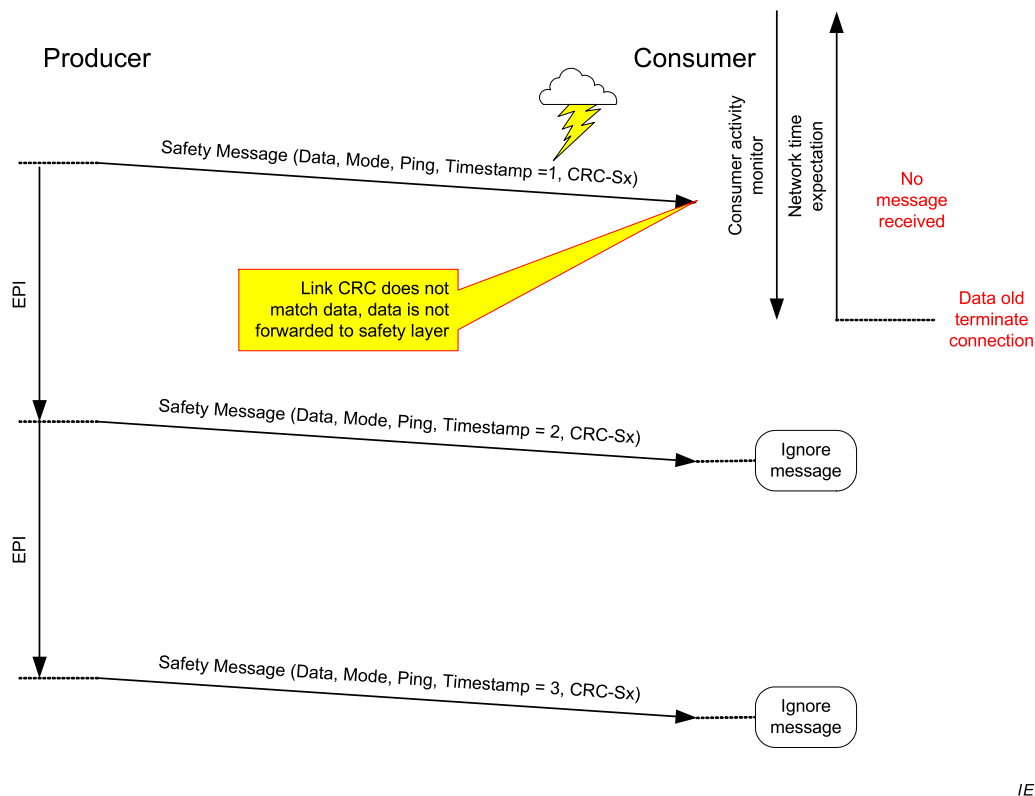
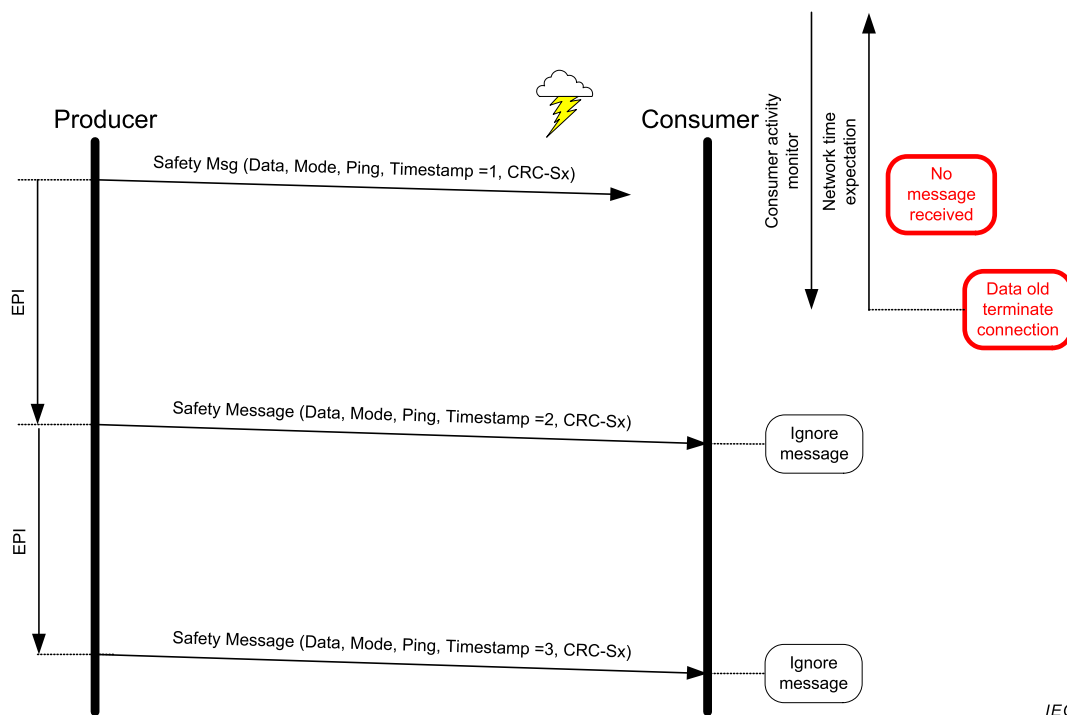


Figure 40 – Sequence diagram of a corrupted producer to consumer message

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.



IEC

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.

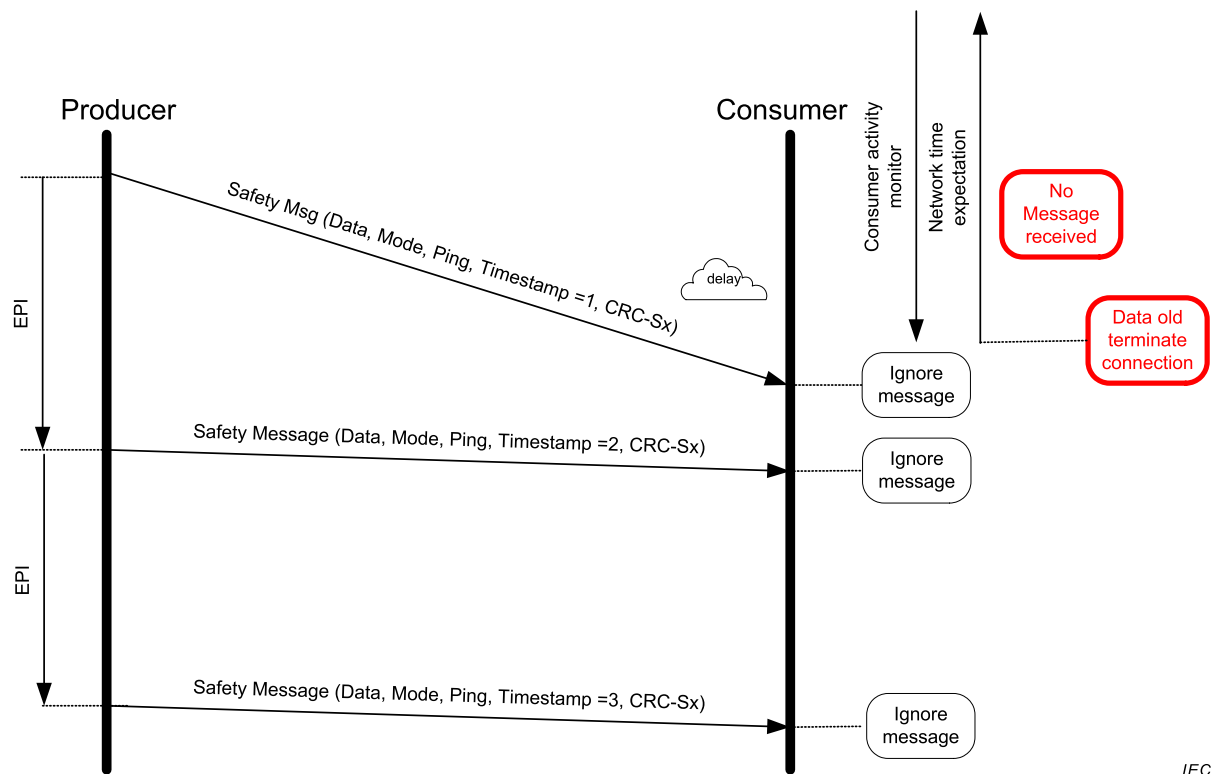


Figure 42 – Sequence diagram of a delayed message

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 nuisance trips and increase the availability of the overall system, production may be repeated.

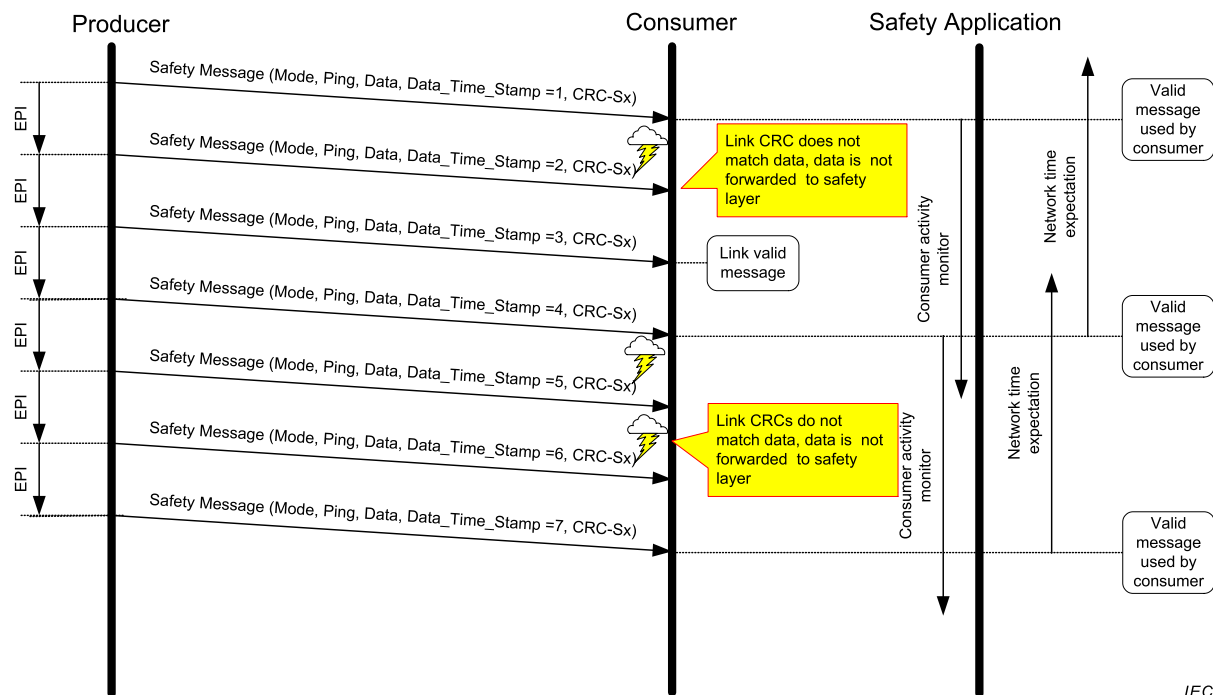


Figure 43 – Sequence diagram of a corrupted producer to consumer message with production repeated

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).

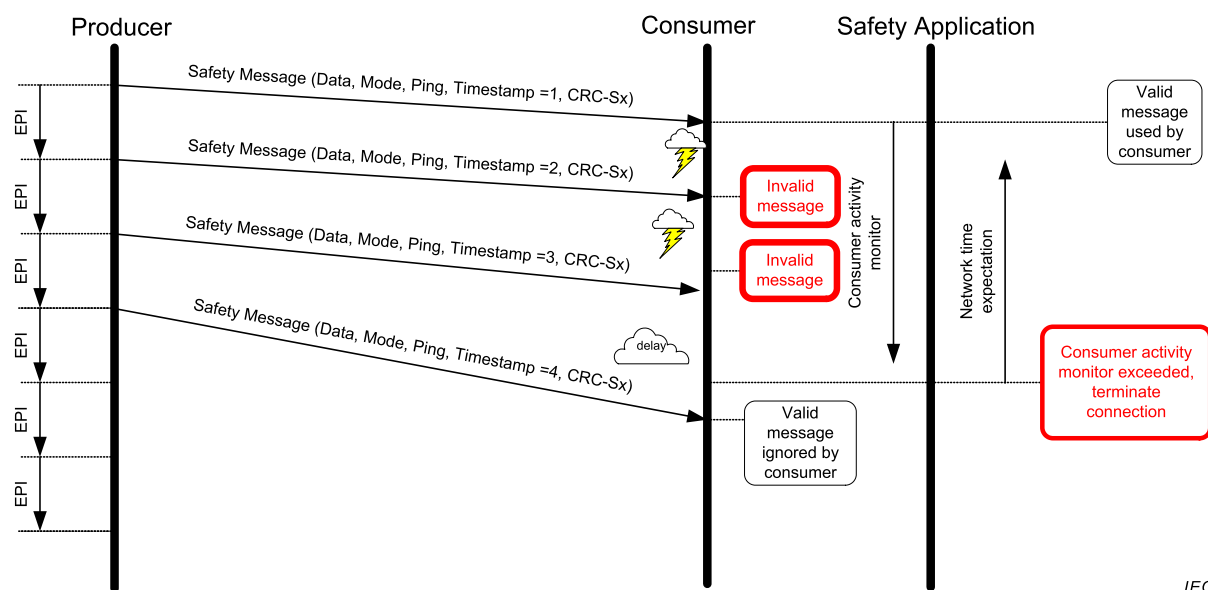


Figure 44 – Sequence diagram of a connection terminated due to delays

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.

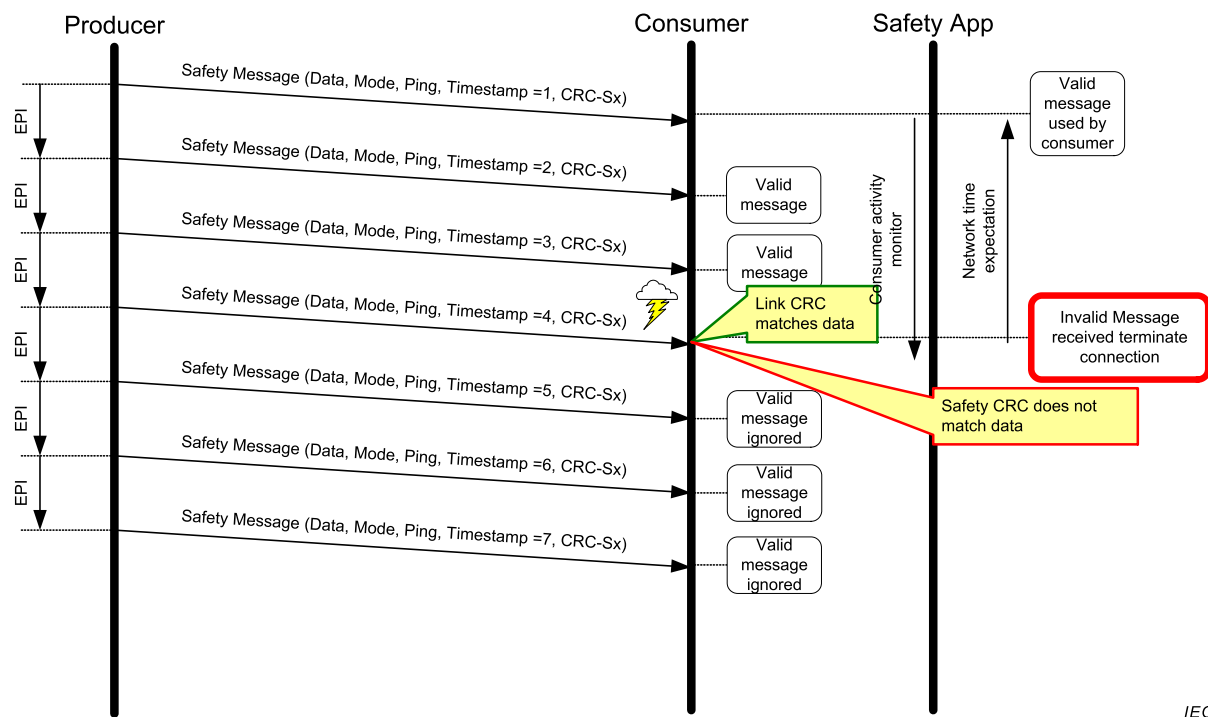


Figure 45 – Sequence diagram of a failure of safety CRC check

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.



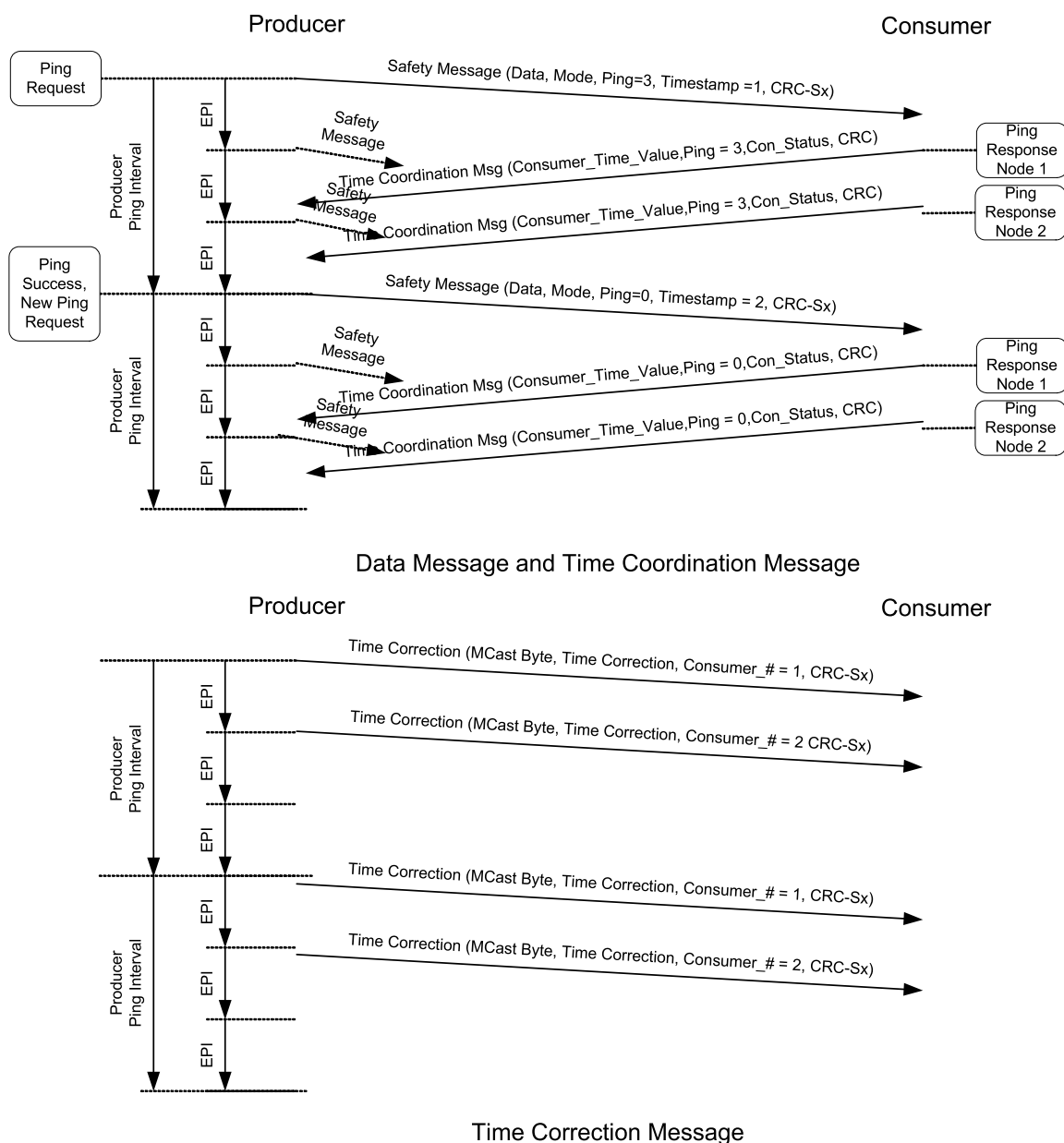
At each point-to-point producer ping interval, the ping count shall be incremented in the next available safety message header.

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

7.5.6 Multipoint ping on CP 2/3 Safety

For CP 2/3 Safety Multipoint connections, a separate message shall be used to communicate time correction information from 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.



IEC

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.

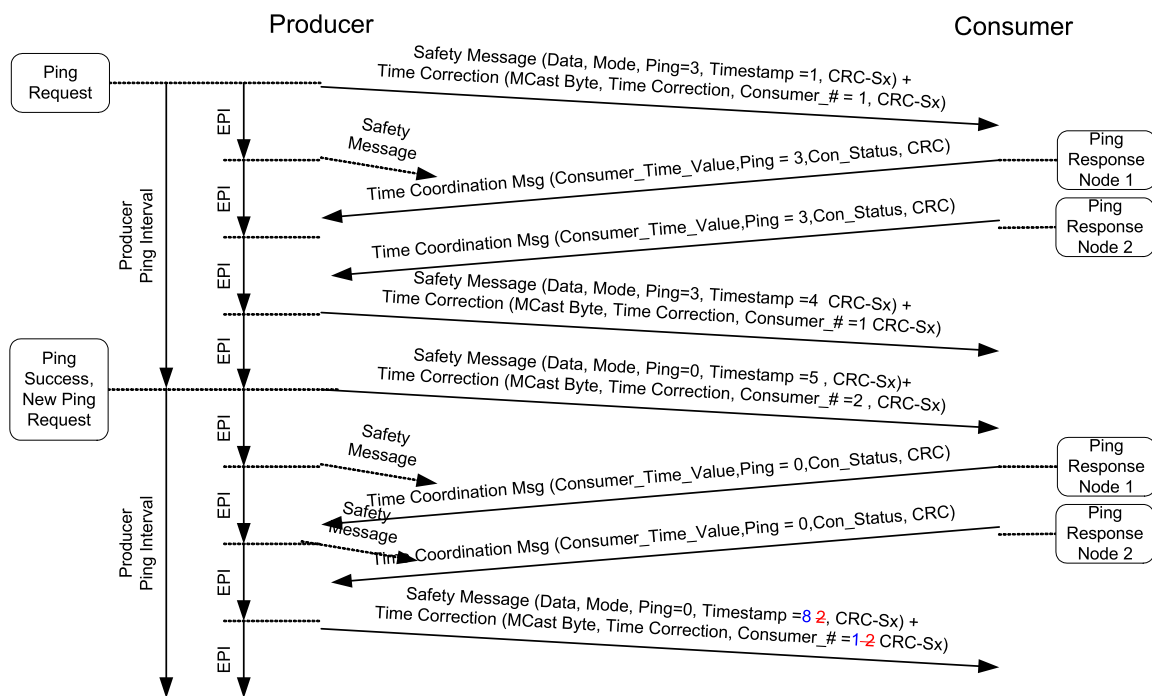
All of the multipoint consumers shall respond within the ping interval of the request or the next one.

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.



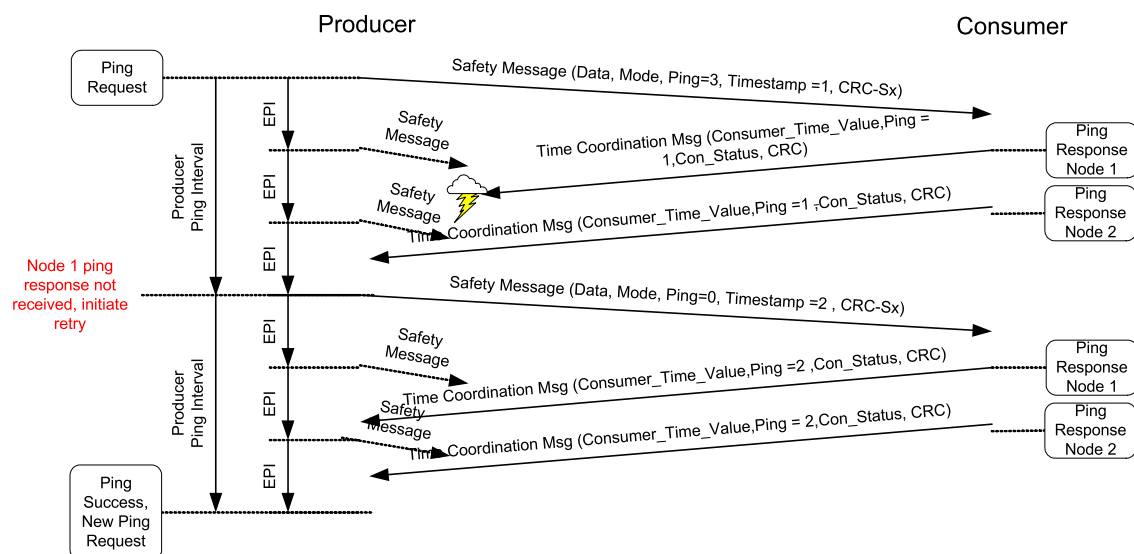
IEC

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.



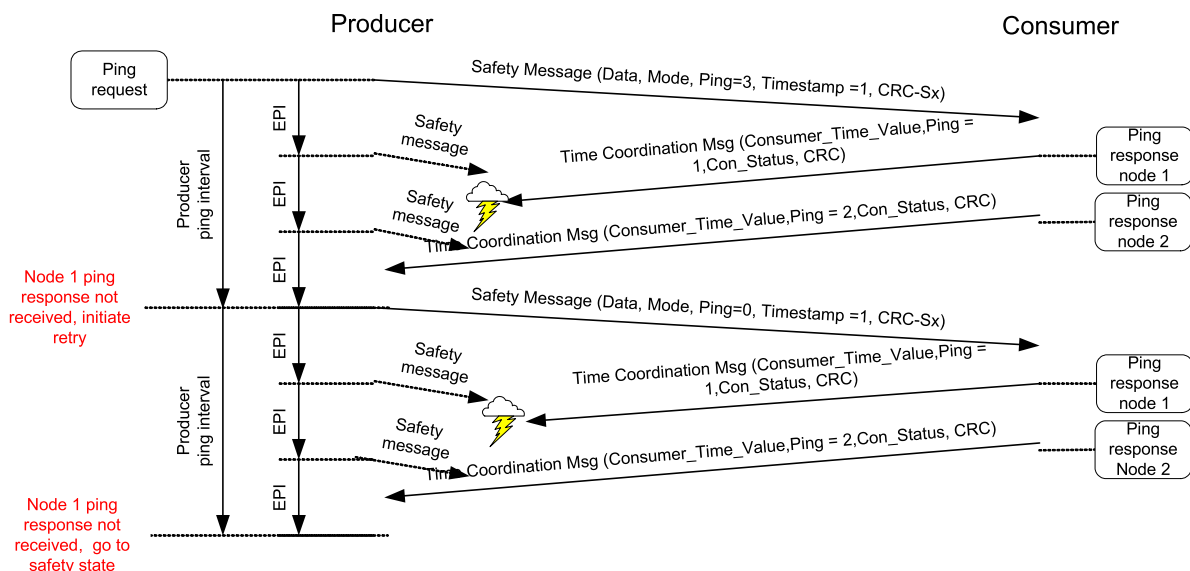
IEC

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.



IEC

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.

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 51. 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 data in a SIL 3 application. This behavior is implemented as the Safety Validator object as described in 6.7.

NOTE 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 reference model of a 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 SIL 3 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 model assumes a 1oo2 Safety Topology in which two independent CPUs participate in the safety protocol.

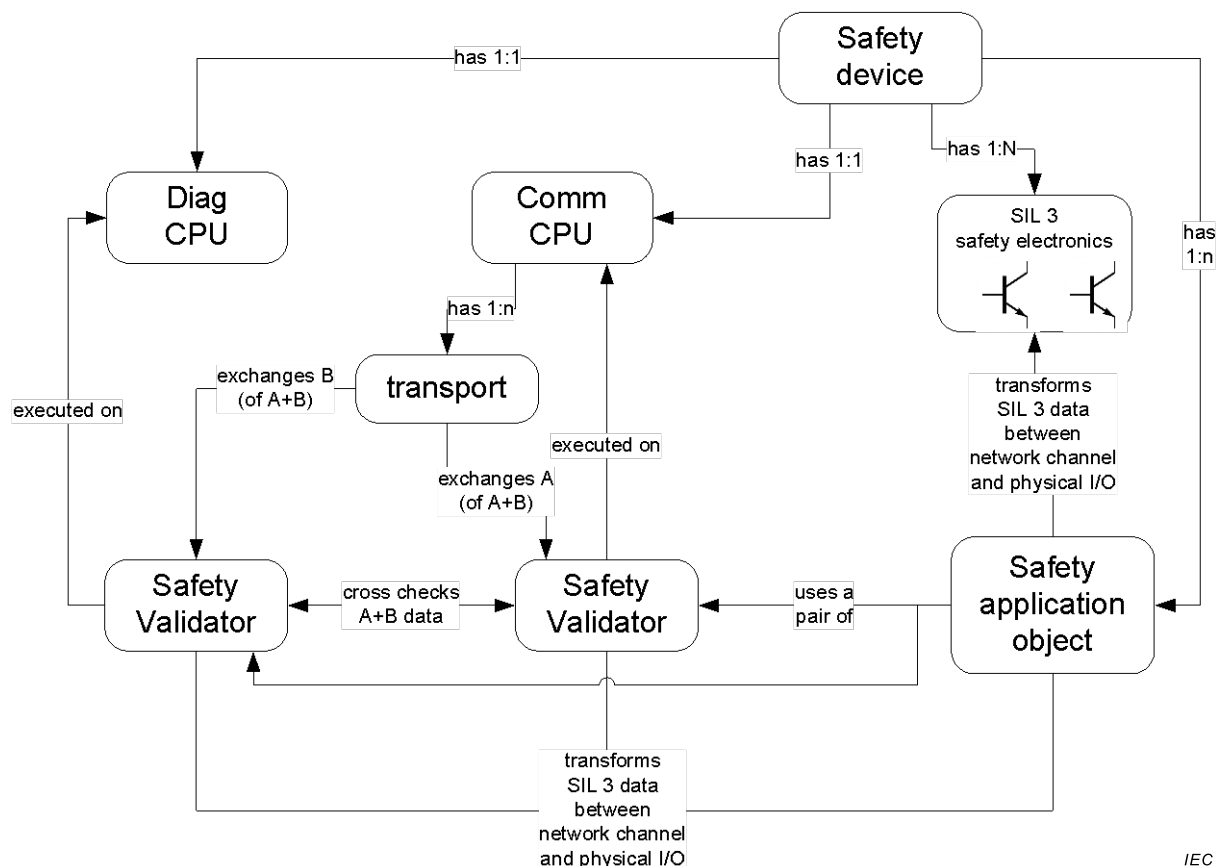


Figure 51 – Safety device reference model entity relation diagram

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 52 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.

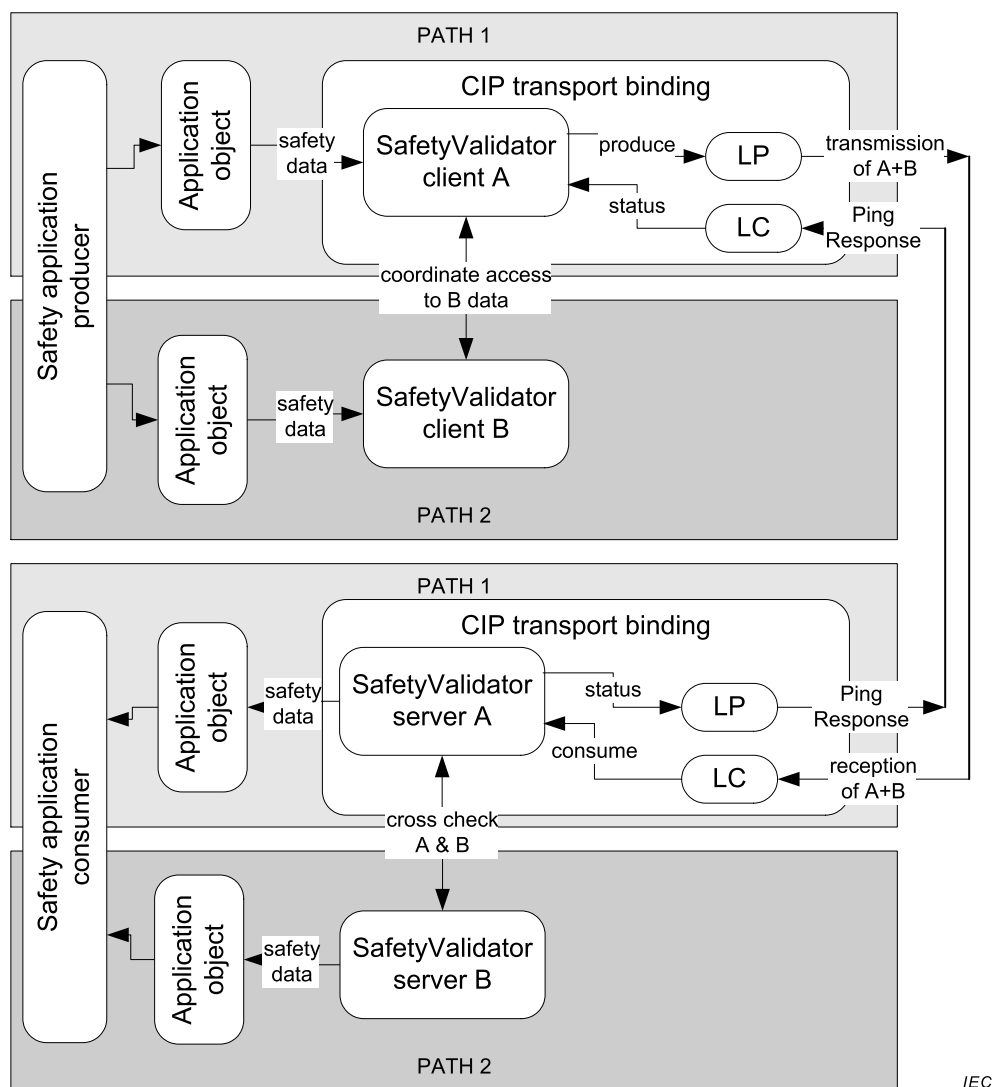


Figure 52 – Two devices interchanging safety data via a SafetyValidatorClient and a SafetyValidatorServer

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

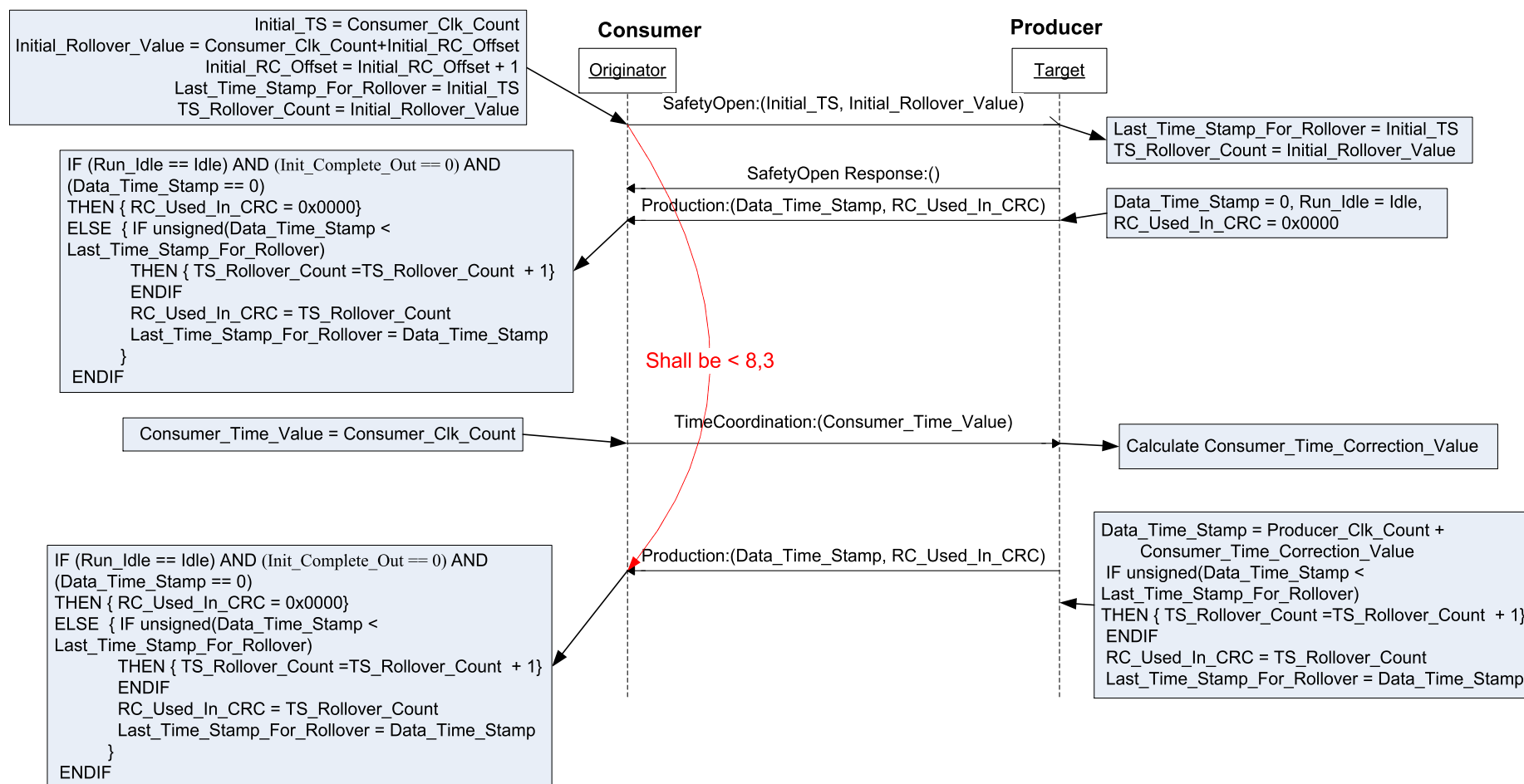
operations for each unique case. The example code shows these operations in their proper place in the code as well.

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 53.



IEC

Figure 53 – 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 54.

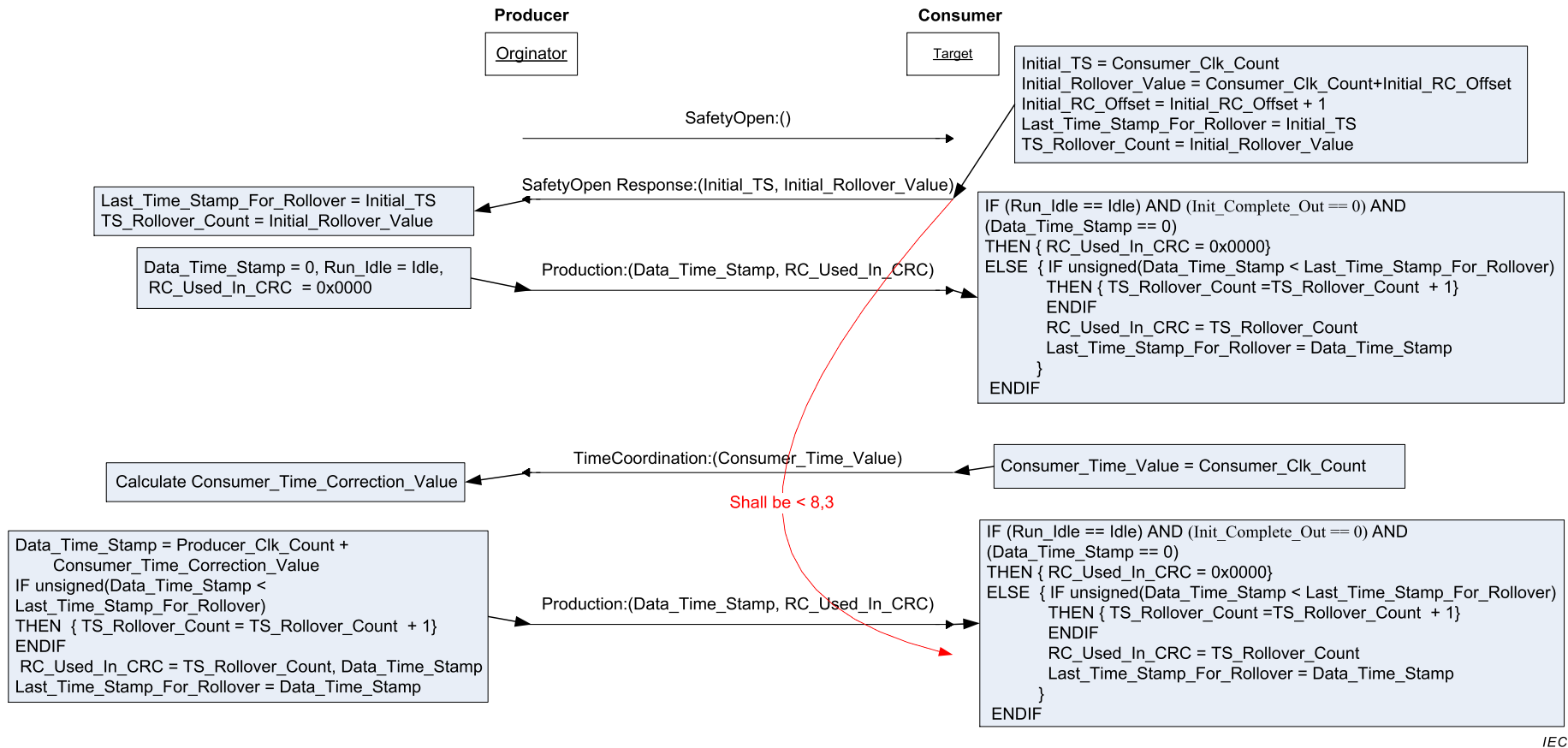


Figure 54 – Point-to-point, originator producer, target consumer

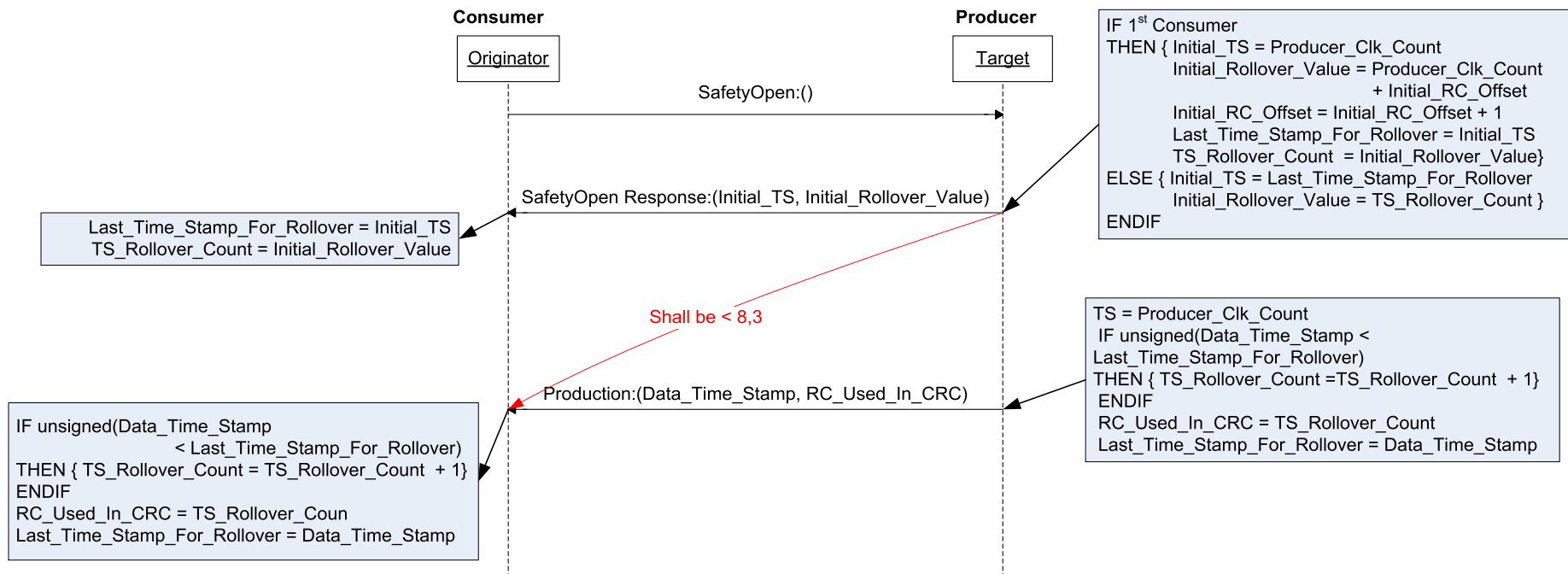
The time between the generation of the Safety Open Response and the Consumers processing of the first packet produced after the producers reception of the Time_Coordination message shall be less than 8,3 s.

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 55.



IEC

Figure 55 – Multi-point, originator consumer, target producer

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.

7.6.6 SafetyValidatorClient function definition

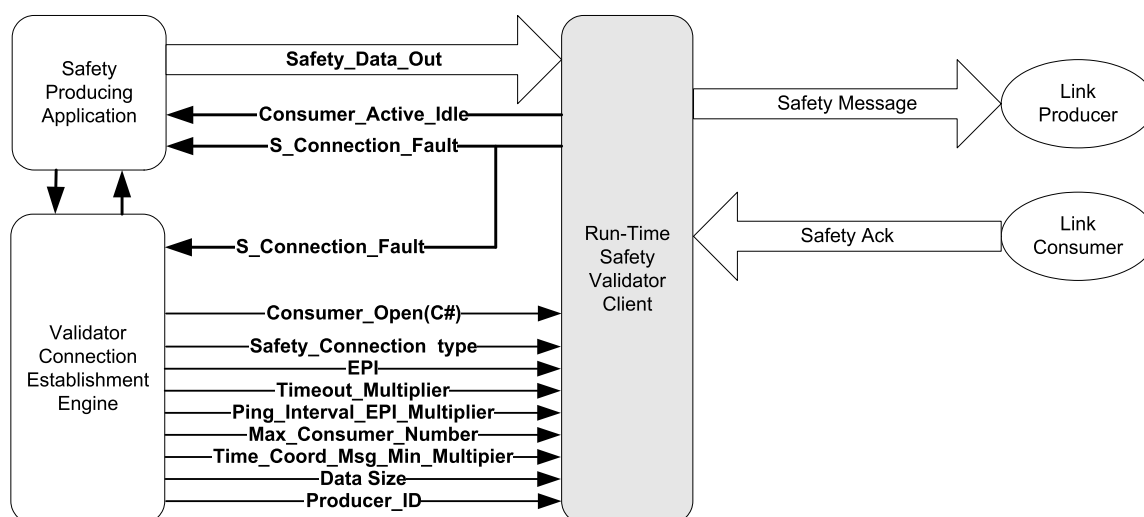
7.6.6.1 General

The SafetyValidatorClient is the embodiment of the safety layer that augments a standard connection on CP 2/3 or CP 2/2 to transmit SIL3 safety data. It coordinates the production of application data with a peer instance of the SafetyValidatorClient.

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 and this can be accomplished in many ways and is ultimately a vendor design decision.

Figure 56 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.



IEC

Figure 56 – 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.

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_Rcvd_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
}
}

```

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_Rcvd_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,
      }
    }
  ENENDIF
}

```

```

    }
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
{

```

```

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

```

```

// 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

```

//

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_Rcvd_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

{

 //check 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 approximately 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)
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_Rcvd_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 asynchronous
// clocks. This value will not be used until the second
// Time_Coordination message is received.

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 SIL3 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.

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:

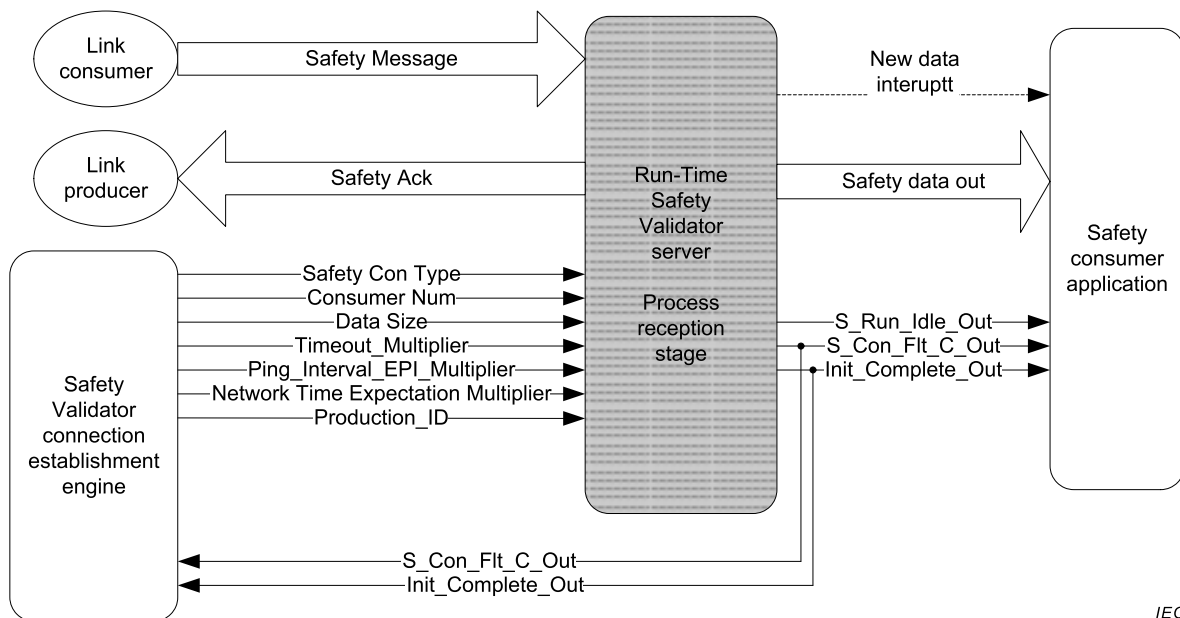
- **SafetyValidatorServer – Link Triggered.**
This is appropriate for consuming applications that are synchronized to the reception of the data, or consuming applications that present a continuous delay from the reception of data.
- **SafetyValidatorServer – Application Triggered.**
This is appropriate 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 57 shows the data flows for the SafetyValidatorServer in the link triggered mode.



IEC

Figure 57 – Consumer safety data monitoring

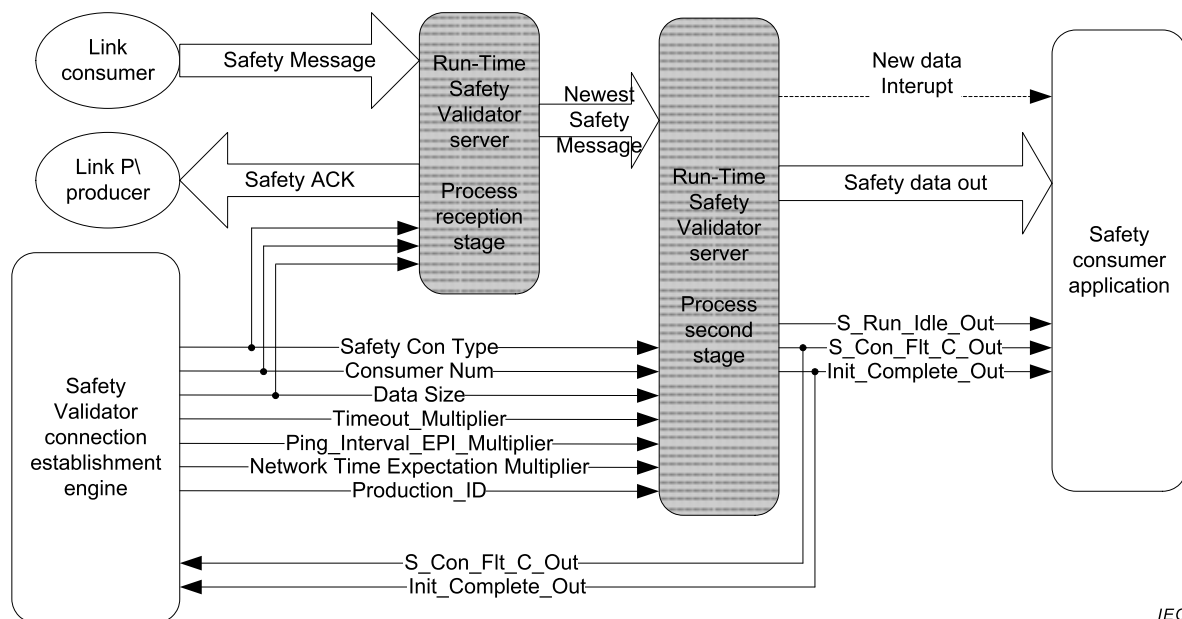
The Link Triggered SafetyValidatorServer shall perform all aspects of the safety protocol on each message received.

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.

The Link Triggered SafetyValidatorServer shall set the new data flag each time data is ready for consumption.

7.6.7.4 SafetyValidatorServer – application triggered



IEC

Figure 58 – 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 58 for the safety data messages that are used. This is particularly useful for the case where the network EPIs are at a faster rate than 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;

- 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 91 defines the safety data processing steps that are performed by the Link Triggered SafetyValidatorServer.

Table 91 – 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 92 defines the safety data processing steps that shall be performed by the Link Triggered SafetyValidatorServer for the reception of each Time Correction section.

Table 92 – 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 93 defines the safety data processing steps that are performed on each message reception by the application triggered SafetyValidatorServer.

Table 93 – 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 94 defines the safety data processing steps that shall be performed on each Time_Correction section reception by the application triggered SafetyValidatorServers.

Table 94 – 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 95 defines the safety data processing steps that are performed by the application triggered SafetyValidatorServer when safety data is requested.

Table 95 – 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

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_Rcvd_Multi_Cast_Active_Idle = Idle,
Last_Rcvd_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.

```

////////////////////
// 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,
}
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.
}
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,
    }

    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
    (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_Rcvd_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_Rcvd_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()

// 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 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_Rcvd_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_Rcvd_Time_Correction_Value =
Time_Correction_Section.Time_Correction_Value,

  // Save the Multi_Cast_Active_Idle bit.
  Last_Rcvd_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 92 and Table 95.

The protocol processing steps defined in Table 95 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.

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 should 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 μ s 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 should 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.

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 96 for definition).

Table 96 – 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 $(\text{Timeout\_Multiplier.PI} + 2) \times \text{Ping Interval}$ 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 $(\text{Timeout\_Multiplier.PI} + 2) \times \text{Ping Interval}$ 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 should 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.

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 exist 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 μ s to 1 000 000 μ s.

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 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 $\text{Max\_Consumer\_Number} \times \text{Timeout\_Multiplier.PI} + 15$, 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.

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_Rcvd_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 should trigger the sending of the Time Coordination message until the message should be sent.
- Time_Coord_Rcvd_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_Rcvd_TO_Time_Coord_Sent_Multiplier should be less than 3 times the EPI.

Time_Coord_Rcvd_TO_Time_Coord_Processed_Multiplier should be less than 3 times the EPI.

The equation to determine the minimum Ping_Interval_EPI_Multiplier is:

$$\begin{aligned}
 & [\{ \text{the maximum Timeout\_Multiplier.PI (C\#) for all consumers} \} \times \text{Max\_Consumer\_Num}] \\
 & \quad + \text{C\_TO\_S\_Delay\_Multiplier} \\
 & \quad + \text{S\_TO\_C\_Delay\_Multiplier} \\
 & \quad + \text{Ping\_Rcvd\_TO\_Time\_Coord\_Sent\_Multiplier} \\
 & \quad + \text{Time\_Coord\_Rcvd\_TO\_Time\_Coord\_Processed\_Multiplier} + 1
 \end{aligned} \tag{1}$$

where

$$\text{C\#} = \text{Consumer\_Number}$$

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_Rcvd_TO_Time_Coord_Sent_Multiplier and Time_Coord_Rcvd_TO_Time_Coord_Processed_Multiplier:

The Ping_Interval_EPI_Multiplier shall be greater than or equal to:

$$[\{ \text{the Max Timeout\_Multiplier.PI (C\#) for all consumers} \} \times \text{Max\_Consumer\_Num}] + 15 \tag{2}$$

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_Rcvd_TO_Time_Coord_Sent_Multiplier and Time_Coord_Rcvd_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_Rcvd_TO_Time_Coord_Sent_Multiplier, 1 to 3;
- Time_Coord_Rcvd_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 μ s 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 μ s 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_Rcvd_Time_Value upon reception of the Time Coordination Message

For any producer, each consumer may have a different Time_Coord_Msg_Min_Multiplier.

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 μ s 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 $0,000\ 2 \times 2$ 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 μ s).

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 μ s.

$$\begin{aligned} \text{Time\_Drift\_Per\_Ping\_Interval (C\#)} = \\ \text{Roundup [EPI} \times \text{Ping\_Interval\_EPI\_Multiplier / 320 000]} \\ \text{OR 1 whichever is greater} \end{aligned} \quad (3)$$

where

C# = Consumer_Number

EXAMPLE If EPI = 8 000 μ s and Ping_Interval_EPI_Multiplier = 100, then Time_Drift_Per_Ping_Interval(C#) = 3 (384 μ s)

7.7.5.15 Connection_Correction_Constant [per consumer]

Connection_Correction_Constant is a value in 128 μ s 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.

$$\begin{aligned} \text{Connection\_Correction\_Constant [C\#]} = \\ \text{Time\_Drift\_Constant} + 1 - \text{Time\_Coord\_Msg\_Min\_Multiplier [C\#]} \end{aligned} \quad (4)$$

where

C# = Consumer_Number

The Time_Drift_Constant (which is part of the Connection_Correction_Constant calculation) is a value in 128 μ s 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 $0,000\ 2 \times 2$ 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.

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.

$$\begin{aligned} \text{Time\_Drift\_Constant (in 128 } \mu\text{s counts)} = \\ \text{Roundup } [(\text{Timeout\_Multiplier.PI} \\ (\text{C\#}) + 1) \times \text{EPI\_in\_}\mu\text{s} \times \text{Ping\_Interval\_EPI\_Multiplier} / 320\,000] \\ \text{OR 1 whichever is greater.} \end{aligned} \quad (5)$$

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:

$$\{5 + [\text{Time\_Coord\_Msg\_Min\_Multiplier} \times 0,000\,128] + [\text{EPI} \times (\text{Consumer\_Num} - 1)]\} \text{ in seconds.} \quad (6)$$

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 $[\text{Time\_Coord\_Msg\_Min\_Multiplier}/0,000\,128]$ 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.

$$\begin{aligned} \text{Time\_Coord\_Response\_EPI\_Limit [C\#]} = \\ \text{Roundup } \{ \{5\,000\,000 + [\text{Time\_Coord\_Msg\_Min\_Multiplier}[C\#] \times 128] \\ + [\text{EPI} \times (\text{C\#} - 1)] \} / \text{EPI} \} \\ \text{OR 1\,000 whichever is lower.} \end{aligned} \quad (7)$$

where

C# = Consumer_Number

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 $\pm 0,02$ %.

`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 $\text{Max\_Consumer\_Number}$), on the 9th to $n+9$ productions of the Ping Interval.

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 $\text{Ping\_Interval\_EPI\_Multiplier}$.

At connection establishment, the $\text{Ping\_Interval\_EPI\_Count}$ variable should be set to 0000_{hex} .

7.7.6.5 RR_Con_Num_Index_Pntr

$\text{RR\_Con\_Num\_Index\_Pntr}$ 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 $\text{Max\_Consumer\_Number}$, 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 $(\text{Max\_Consumer\_Number} - 1)$ indicates which Time Coordination timeouts will be checked ($\text{Consumer\_Number} = \text{RR\_Con\_Num\_Index\_Pntr} + 1$) on this EPI and which Time Correction message ($\text{Consumer\_Number} = \text{RR\_Con\_Num\_Index\_Pntr} + 1$) may be sent based on this EPI production.

7.7.6.6 Time_Drift_Since_Last_Time_Coord [per consumer]

$\text{Time\_Drift\_Since\_Last\_Time\_Coord}$ 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 $\text{Ping\_Int\_Since\_Last\_Time\_Coord\_Msg\_Count}$ times $\text{Time\_Drift\_Per\_Ping\_Interval}$. The $\text{Ping\_Int\_Since\_Last\_Time\_Coord\_Msg\_Count}$ is the number of Ping Intervals since the last Time Coordination message.

The $\text{Time\_Drift\_Since\_Last\_Time\_Coord}$ 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 $\text{Consumer\_Time\_Correction\_Value}$ 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 $\text{Consumer\_Time\_Correction\_Value}$ may cause the Time_Stamp of the next EPI production to actually be less than 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 $\text{Last\_Time\_Correction\_Value}$ minus the $\text{Time\_Drift\_Since\_Last\_Time\_Coord}$ value, or the $\text{New\_Time\_Correction\_Value}$ 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`.

The legal range of values is from 0 to 3 910.

7.7.6.7 Worst_Case_Consumer_Time_Correction_Value

This is 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_Rcvd_Time_Value[per consumer]

`Producer_Rcvd_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_Rcvd_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_Rcvd_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`.

$$\begin{aligned} \text{Consumer\_Time\_Correction\_Value [Consumer\_Number]} = \\ \text{Consumer\_Time\_Value [Consumer\_Number]} \\ - \text{Producer\_Rcvd\_Time\_Value [Consumer\_Number]} \\ - \text{Connection\_Correction\_Constant [Consumer\_Number]} \end{aligned} \quad (10)$$

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.

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 97 summarizes the logic that the consuming application can use to drive the safety data and status.

Table 97 – 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 97.

7.7.8.3 S_Con_Flt_C_Out

S_Con_Flt_C_Out indicates to the consuming application if it should 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 should 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.

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 indicate 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 indicate 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 μ s increments that a consumer should allow the age of the safety data to reach.

If consumed safety data becomes older than `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 ($\text{FFFF}_{\text{hex}} \times 0,000\,128$) 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.

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 μ s.

Consumer_Clk_Count will have tolerances and stability within $\pm 0,02$ % 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 should 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.

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_Rcvd_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_Rcvd_Multi_Cast_Active_Idle

This value is the saved copy of the received `Multi_Cast_Active_Idle`.

The `Last_Rcvd_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_Rcvd_Multi_Cast_Active_Idle` shall be initialized to 0.

7.7.10.7 Last_Rcvd_Time_Correction_Value

This value is the saved copy of the received `Time_Correction_Value`.

The `Last_Rcvd_Time_Correction_Value` shall be used to correct the Time Stamp for each multipoint consumer.

When a connection is first established, the `Last_Rcvd_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 μ s increment.

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.

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 98 defines the errors and the measures to detect these errors.

Table 98 – 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	X ¹	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 99 for details.

Table 99 – 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 100.

Table 100 – 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

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.

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 Form 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.

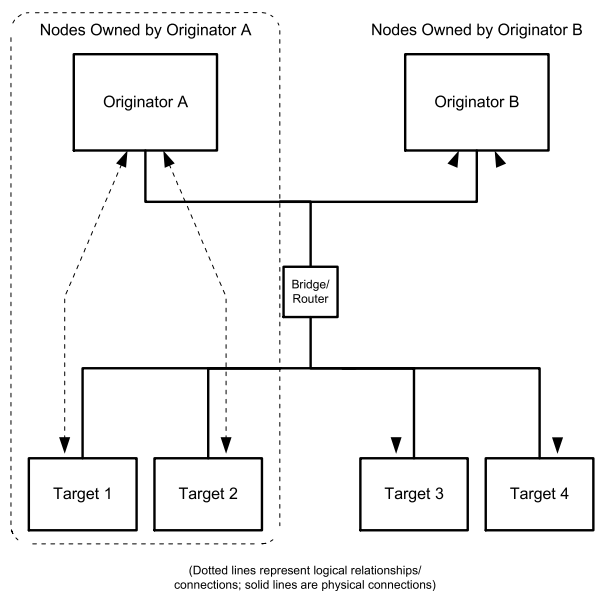
Initial Time Stamp – When the Extended Format safety message format is being used, the Extended Format safety segment and Extended Format SafetyOpen Response is used during connection establishment. Depending on the type of connection (see 7.6.5), the Initial Time Stamp is either sent in SafetyOpen or 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 59. For the purposes of illustration, assume that all targets are the exact same.



IEC

Figure 59 – 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.

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 60):

- Destination, Ownership, Configuration data processing and SCID checking;
- Destination, Ownership and SCID Checking (Optional).

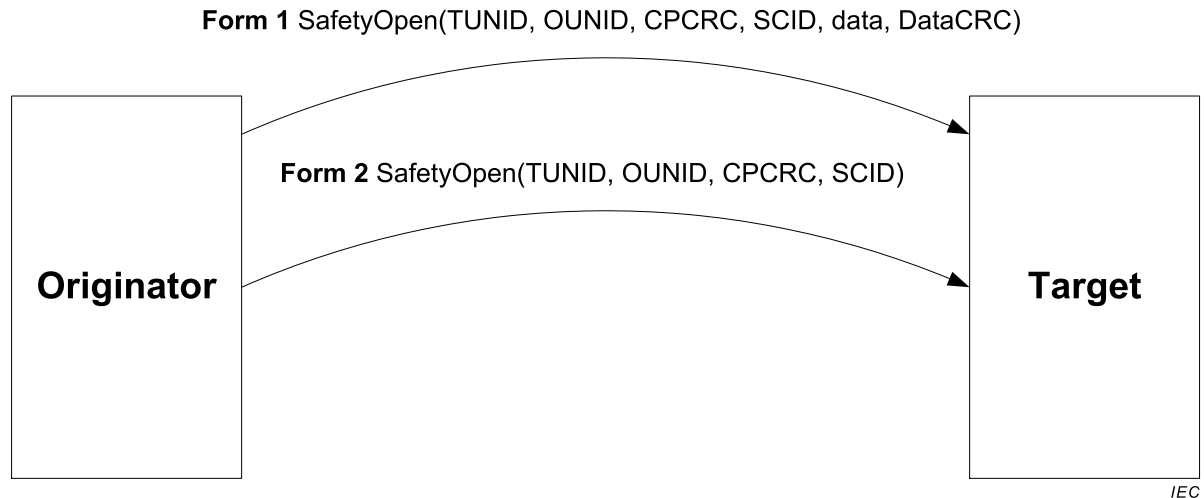


Figure 60 – SafetyOpen forms

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 61 defines the ownership states the methods of transitioning from ownership state to another ownership state.

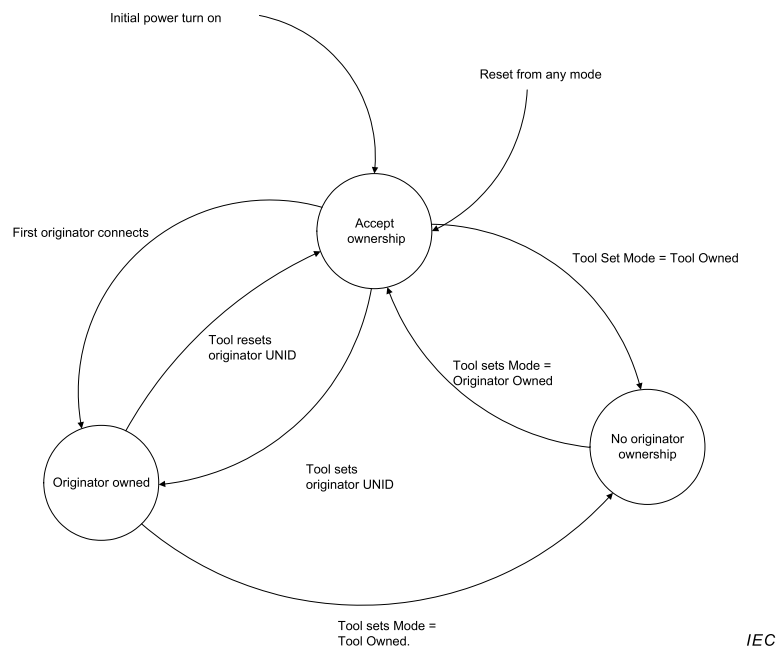


Figure 61 – Connection ownership state chart

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 62 defines the mapping of the SafetyOpen UNIDs to the target device originator ownership locations.

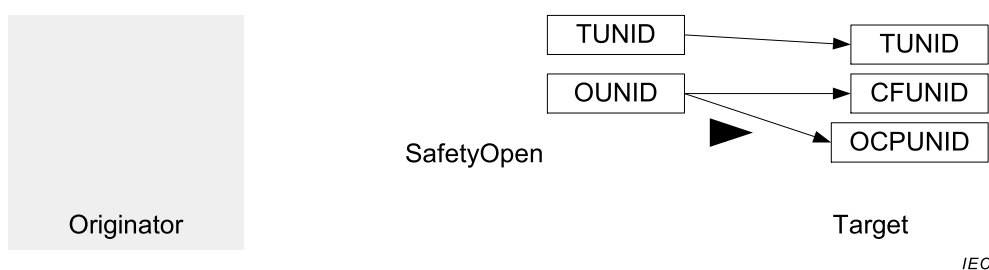
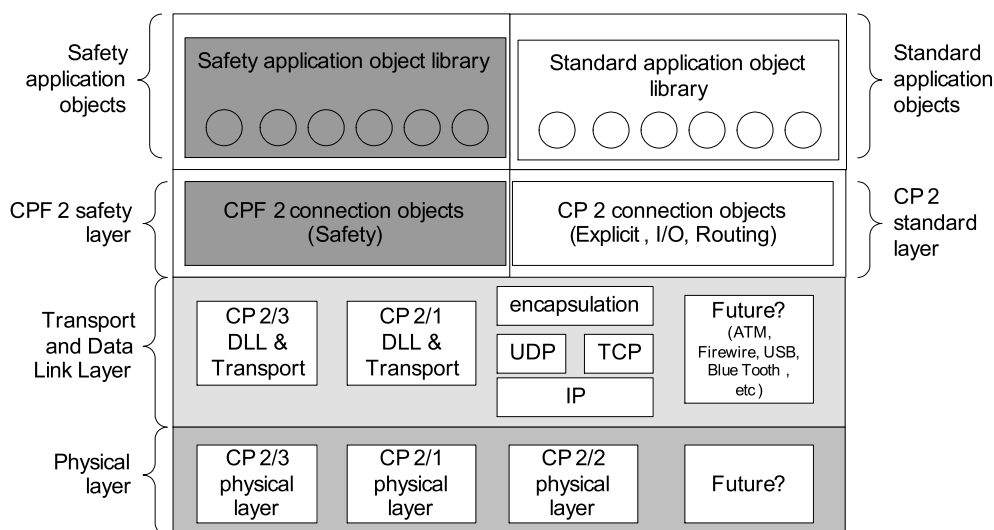


Figure 62 – SafetyOpen UNID mapping

8.7 Bridging different physical layers

CPF 2 nodes share a common application and user layer as defined in Figure 63.



IEC

Figure 63 – 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 SIL 3 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; where as 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. Figure 64 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 SIL 3 data.

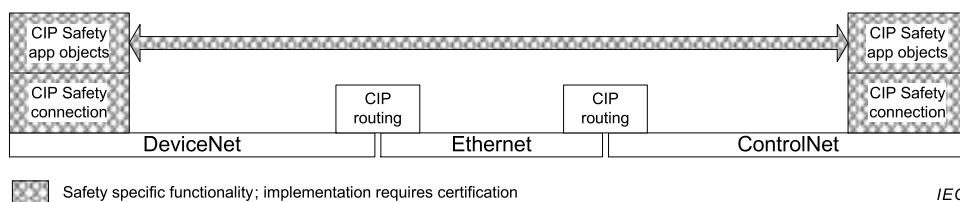


Figure 64 – End-to-End routing example

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.

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.
- 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 (refer to ISO 15745-4:2003, Annex C).
- The application path for the Time Coordination connection shall always be a null path.
- Form 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).

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 range of values for Max_Fault_Number shall be restricted to the range 0 to 255. Table 101 summarizes how these parameters and others will be obtained.

Table 101 – 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)	Default value	5

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:

$$\text{Network\_Time\_Expectation\_Multiplier} > \frac{[\text{EPI\_in\_sec} \times \text{Timeout\_Multiplier} + \text{Safety\_Message\_Time(max)} + \text{Time\_Coord\_Message\_Time(max)}] / 128 \mu\text{s} + \text{Connection\_Correction\_Constant}}{1} \quad (11)$$

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:

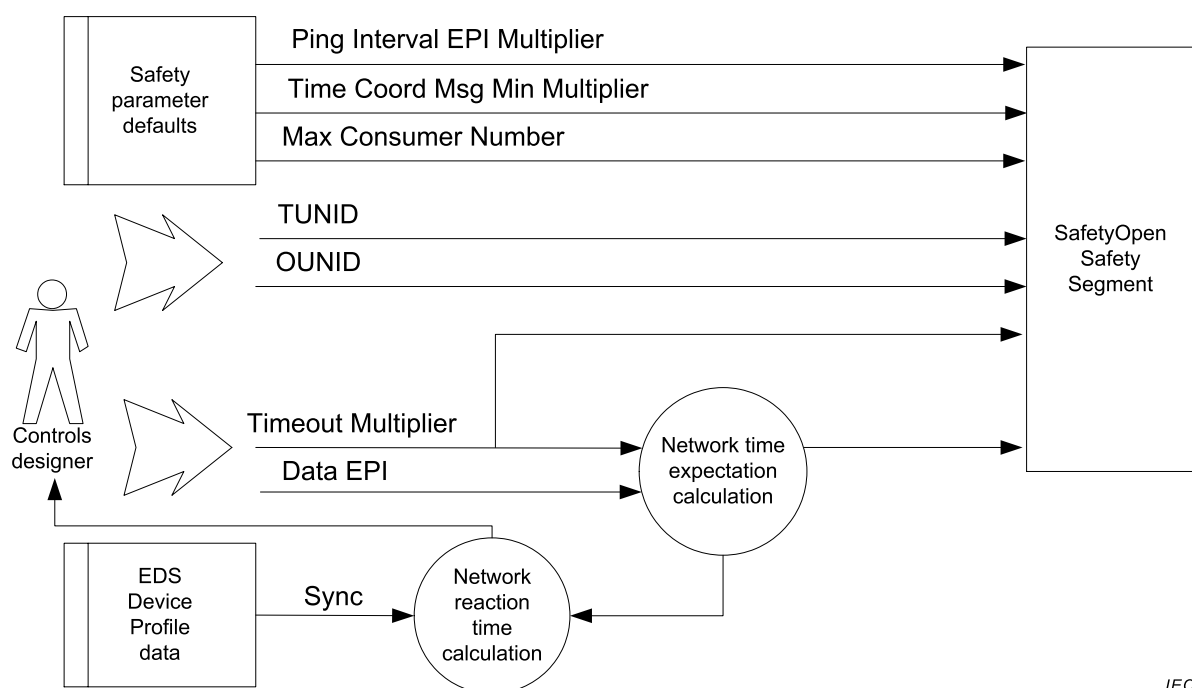
$$\text{Network Time Expectation Multiplier} = [\text{EPI\_in\_sec} \times (\text{Timeout\_Multiplier} + 2)] / 128 \mu\text{s} \quad (12)$$

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 65 shows where the various parameters defined in Table 101 are obtained. It also shows how these parameters are used by the software to construct the safety segment of a SafetyOpen.



IEC

Figure 65 – Sources for safety related connection parameters

Figure 66 defines how the SafetyOpen parameters are mapped in Originators and Targets of a safety connection.

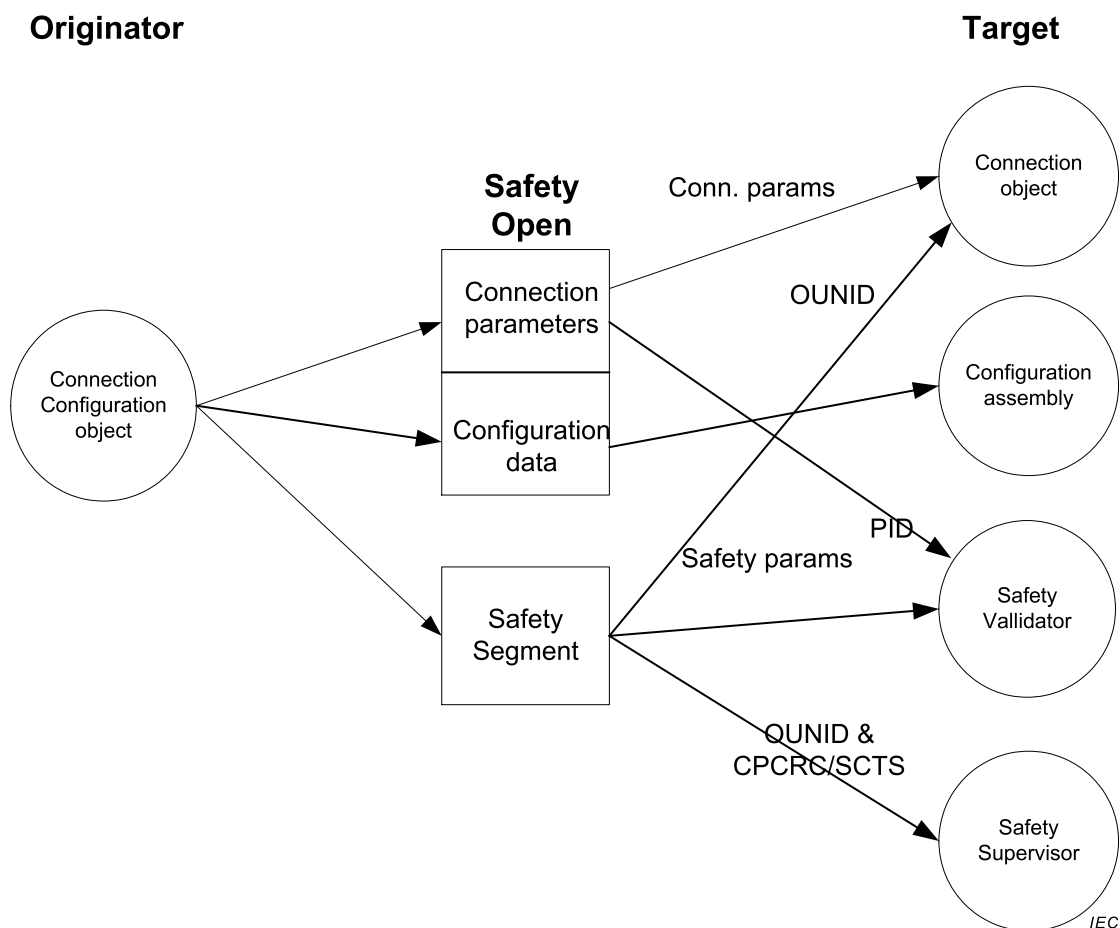


Figure 66 – Parameter mapping between originator and target

8.8.5 Establishing connections

When configuration data is transmitted within the SafetyOpen this is defined as a Form 1 SafetyOpen. When no configuration data is transmitted within the SafetyOpen this is defined as a Form 2 SafetyOpen. This is defined in Figure 67.

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 Form 2 SafetyOpen, and only followed with a Form 1 SafetyOpen if the target responds with Device Not Configured error.

When a device receives a Form 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 68.

Targets shall respond to a Form 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 Form 1 connection request the first time it connects. The SCID returned shall be validated against the value held.

There are two kinds of Form 2 SafetyOpens: with and without the SCID.

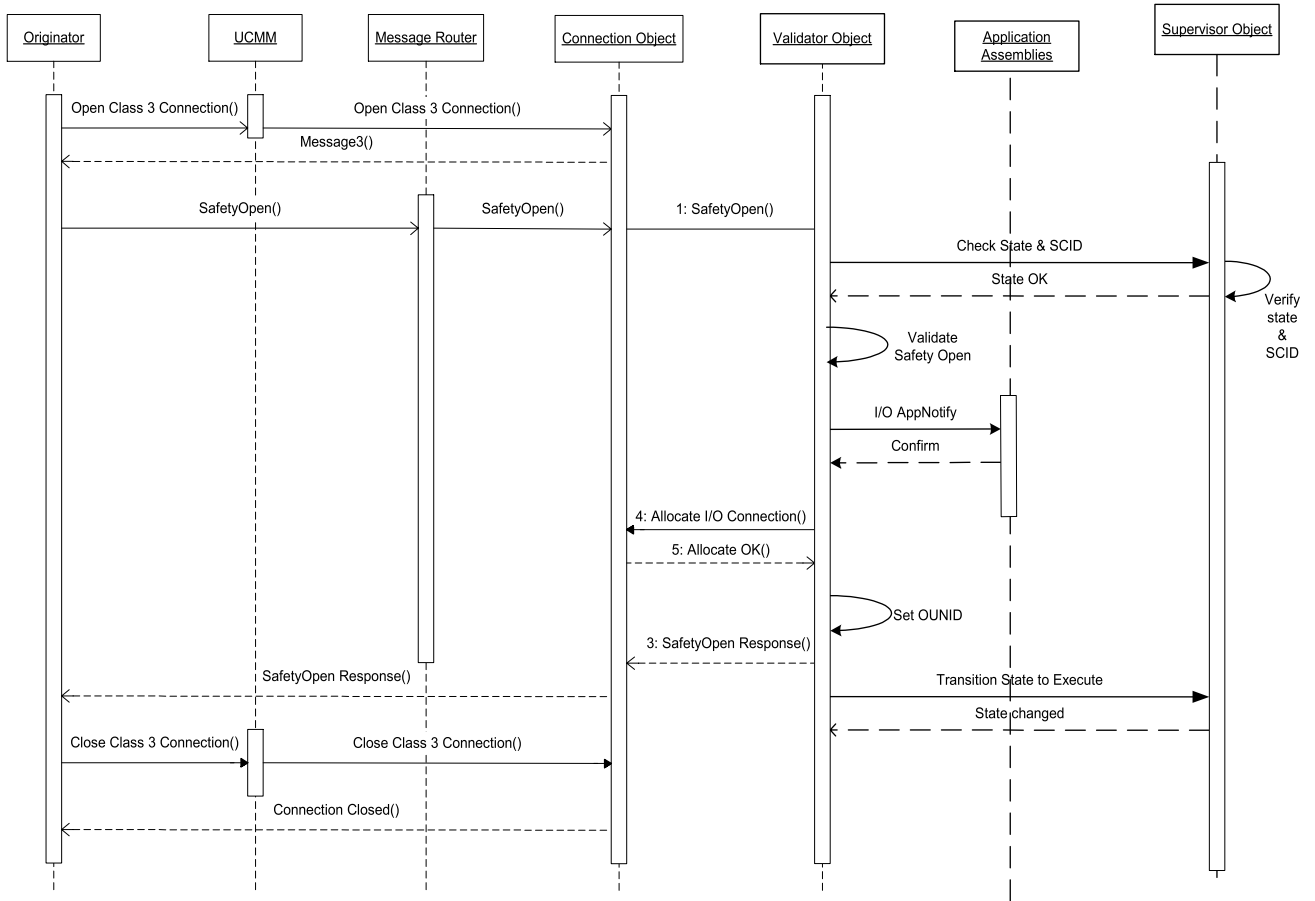
- Form 2a: When a target receives a Form 2 SafetyOpen (no configuration data) accompanied by a non-zero Safety Configuration ID (SCID = SCCRC + SCTS), it shall compare it against the SCID of the configuration and only accept the connection if they match.
- Form 2b: When a target receives a Form 2 SafetyOpen (no configuration data) accompanied by a zero value SCID, it skips the check.

Table 102 provides a summary of the Forms of SafetyOpens.

Table 102 – SafetyOpen summary

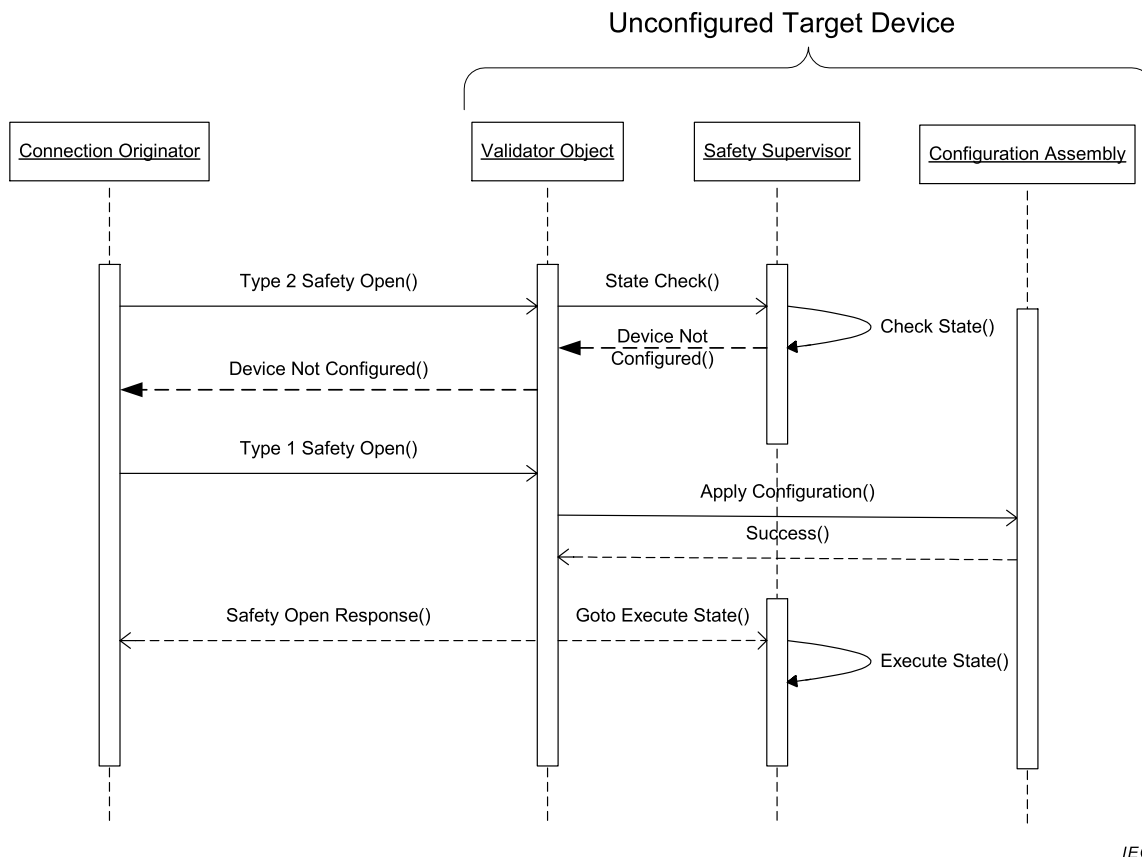
	Form 1SafetyOpen with data	Form 2aSafetyOpen with SCID check	Form 2bSafetyOpen without SCID check
TUNID	X	X	X
OUNID	X	X	X
UPID ^a	X	X	X
CPCRC	X	X	X
SCID	X	X	= 0
Config. Data in SafetyOpen	Yes	No	No
^a UPID is derived from components in the SafetyOpen or from application data returned in the SafetyOpen response. See 6.3.12.			

The processing of SafetyOpens in Targets will differ depending on the Form of SafetyOpen message that is received. Figure 68 defines the message and event sequence for the Form 1 SafetyOpen and the objects that are responsible for the various processing steps. Figure 68 defines that the primary difference between processing Form 1 and Form 2 is the step where configuration data is passed to a configuration assembly and an owner assigned to that configuration.



IEC

Figure 67 – CP 2/3 Safety connection establishment in targets for Form 2a SafetyOpen



IEC

Figure 68 – General sequence to detect configuration is required

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 $\text{Timeout\_Multiplier.PI} + 1$ 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 $\text{Timeout\_Multiplier.PI} + 2$ 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 $\text{Timeout\_Multiplier.PI} + 2$ 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.

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 should 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 Form 1 SafetyOpen that configures a previously unconfigured and unowned input device shall become the owner of the configuration.

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 Form 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 Form 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 may or may not be the same as what exists in the device and the SCID may or may not match the existing SCID. Regardless, as long as the following process is followed, it should 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 Form 1 SafetyOpen is received:

- verify that the TUNID in the SafetyOpen matches the device TUNID;
- if configuration data is included (Form 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;
- 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 may or may not be the same as what exists in the device and the SCID may or may not match the existing SCID. Regardless, as long as the following process is followed, it should 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 Form 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 is included (Form 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 should 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., Form 1) without a matching OUNID will be rejected with an error response, “OUNID Mismatch”.

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., Form 2a, or Form 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 Form 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;

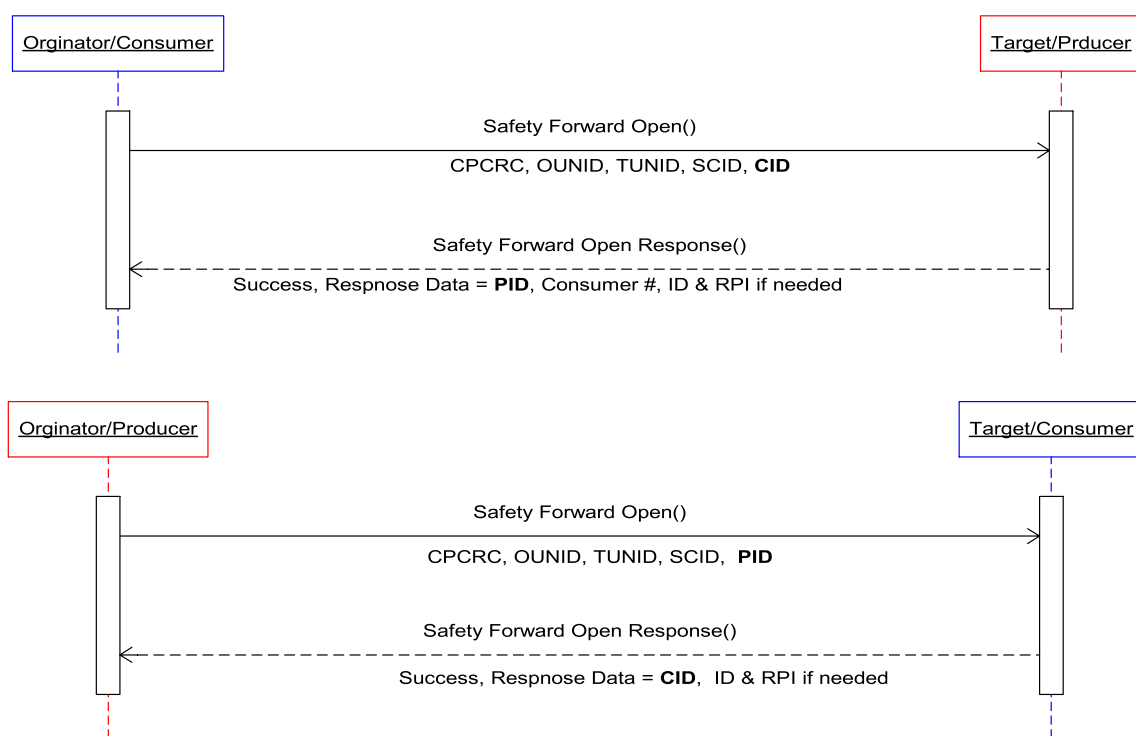
- transition the connection to the established state.

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 69.

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.

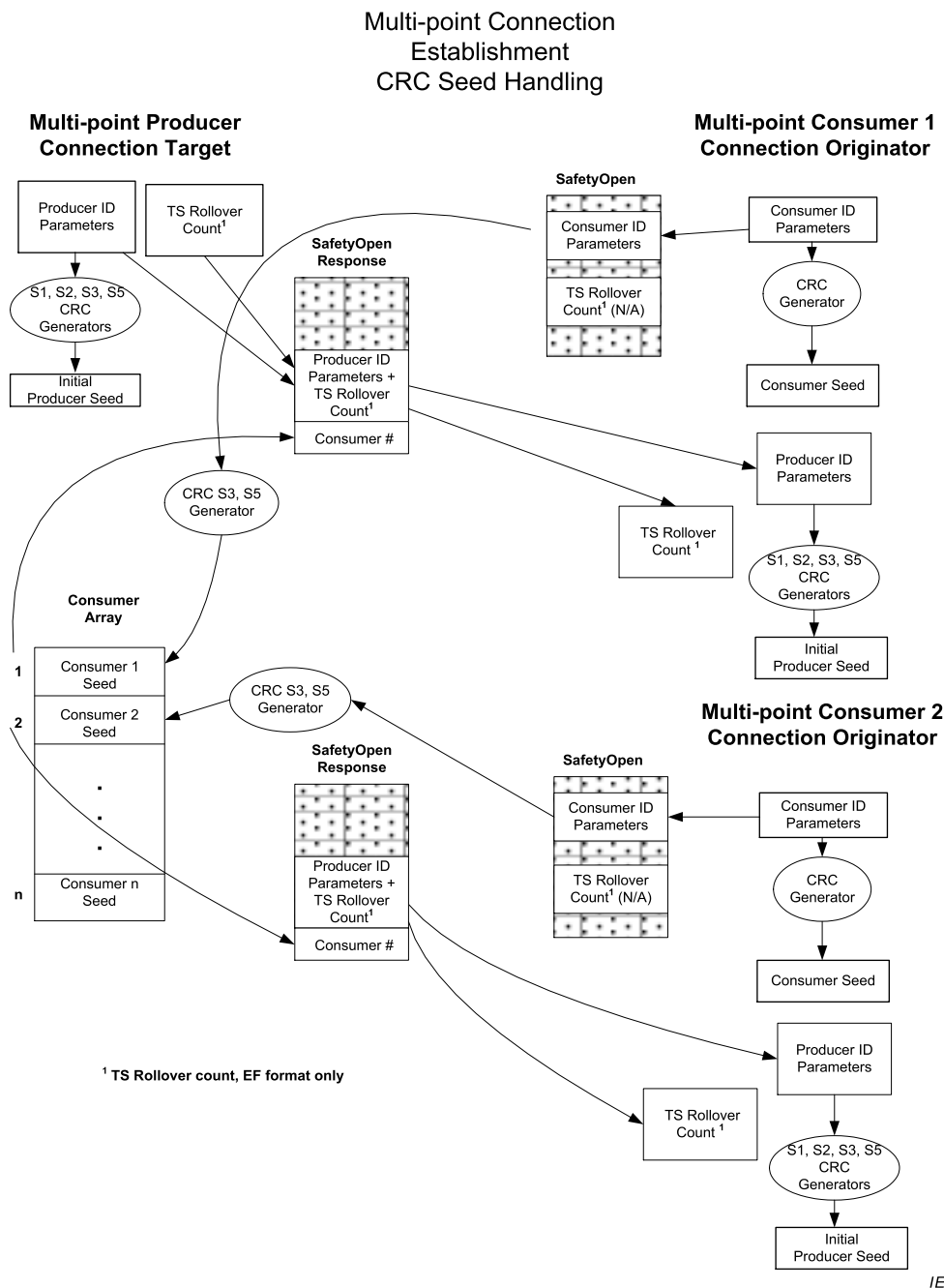


IEC

Figure 69 – PID/CID exchanges for two originator scenarios

8.8.11 Proper PID/CID usage in multipoint and point-to-point connections

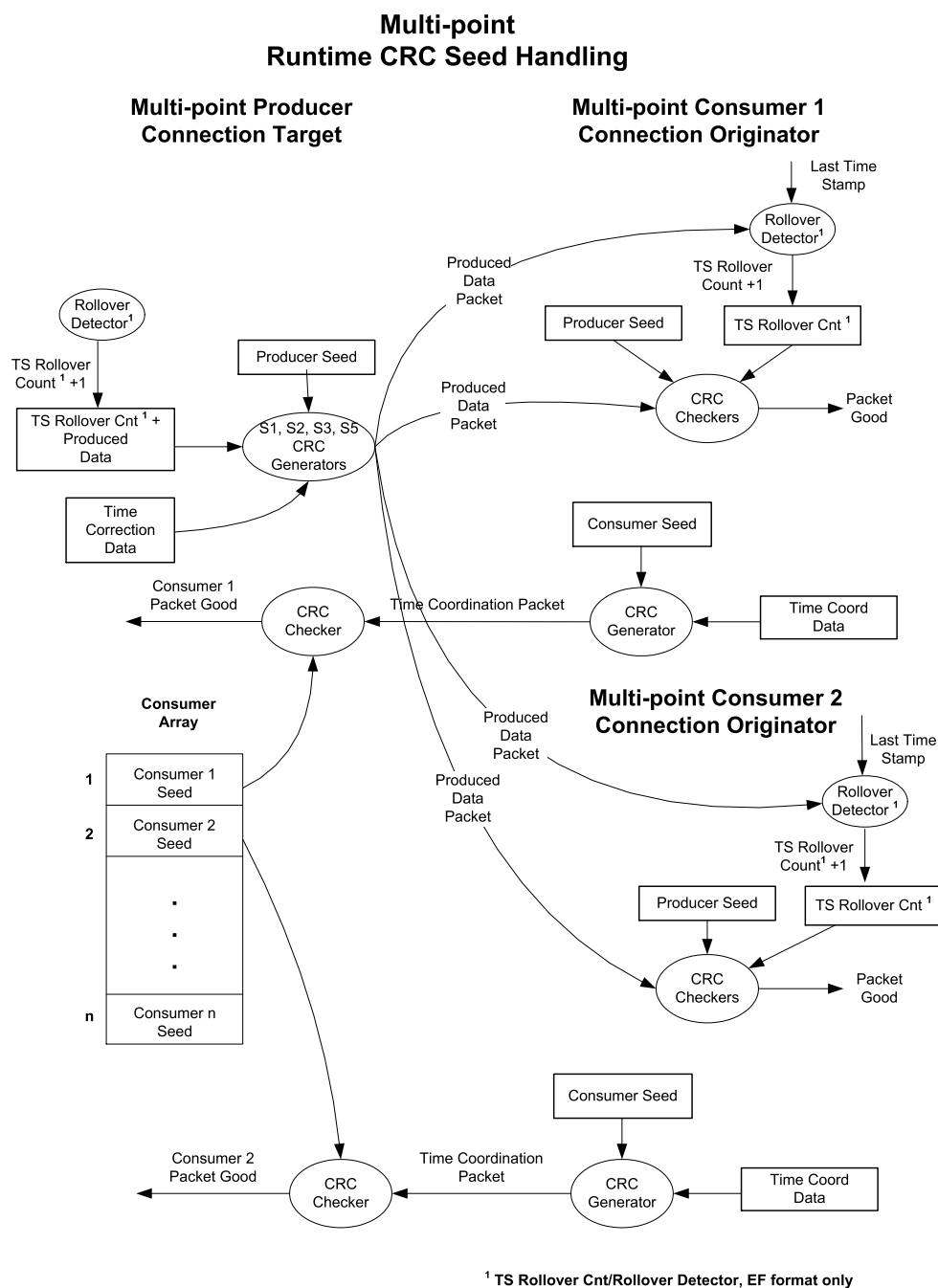
The diagram shown in Figure 70 illustrates how the Producer and Consumer ID parameters are to be used to generate the CRC seed values for both the Base and Extended Format. This diagram defines the multipoint case, but it also applies to Point-to-point connections as well (this is done simply for consistency). 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.

**Figure 70 – 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 71 illustrates how the seed values, set up during connection establishment, get used in the run-time data production.



IEC

Figure 71 – 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 should 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 should support all the recommended services of that category.

8.8.13.3 Safety connection services

Table 103 defines all the defined Safety Validator Services that Connection Targets or Connection Originators can support.

Table 103 – 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 104 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 104 – 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 72 and Figure 74 list the preferred Safety Connection Services for various Connection Categories (see Figure 73 and Figure 75 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.

					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 72 – Connection categories and supported services

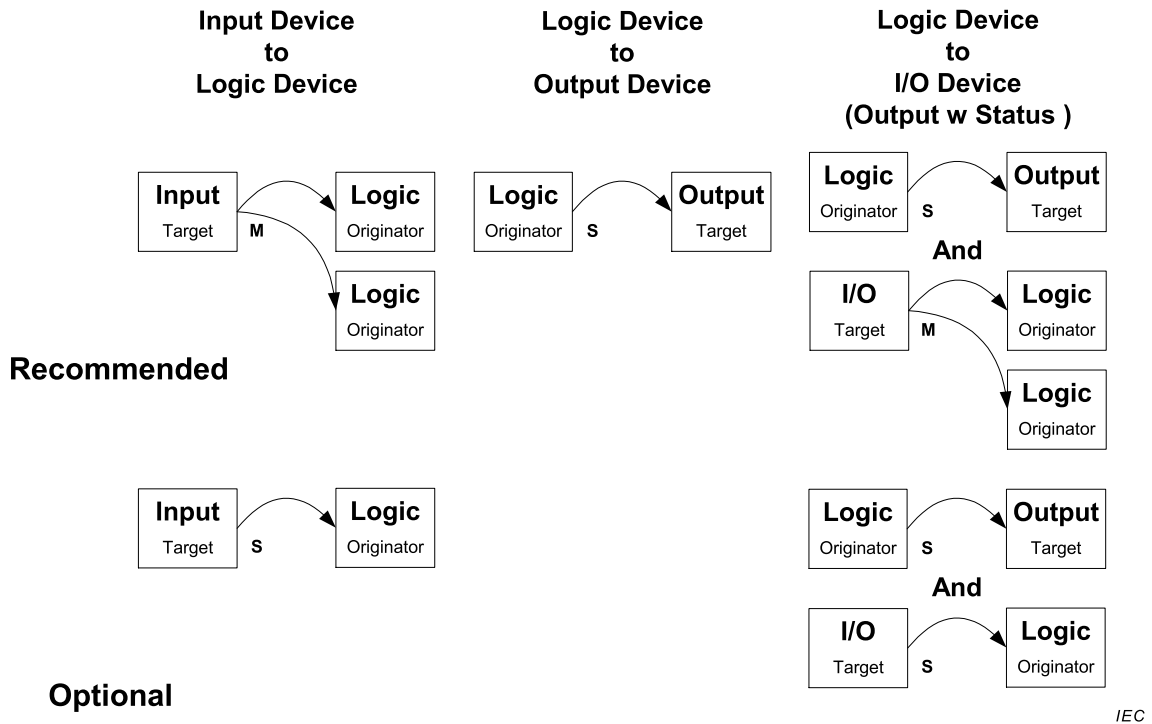


Figure 73 – Recommended connection types

Safety connection service				Safety connection Category 4			
	Originator or Target	Safety Validator type		Logic device to logic device			
				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 74 – Logic-to-logic supported services

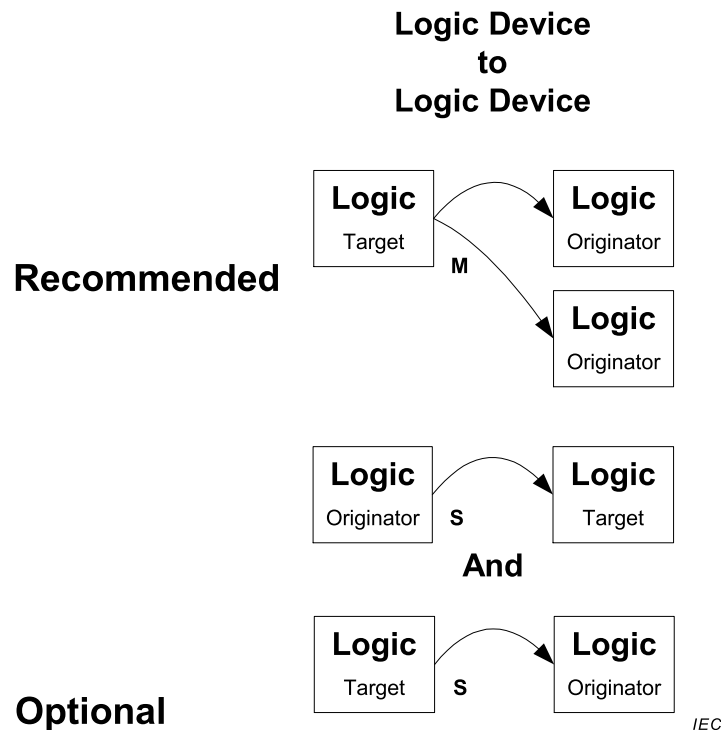


Figure 75 – Recommended connection types for logic to logic

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 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 SIL3 environment.

8.9.2 Configuration goals

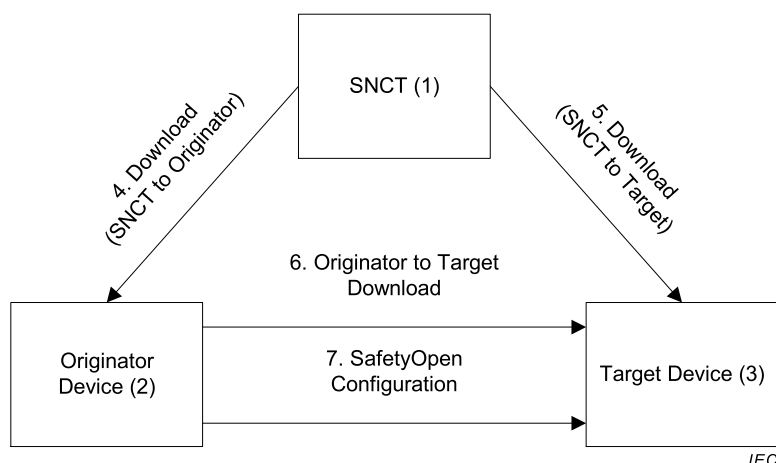
The safety related goals for the configuration process for FSCP 2/1 safety devices are shown in Table 105.

Table 105 – 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 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 76 shows the possible configuration data transfers into safety devices. The numbers in the figure are references to the discussion numbering below.

**Figure 76 – Configuration data transfers**

The devices involved in the configuration process are shown in Figure 76. 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 part 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 76). 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 77.

- 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 Form 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.

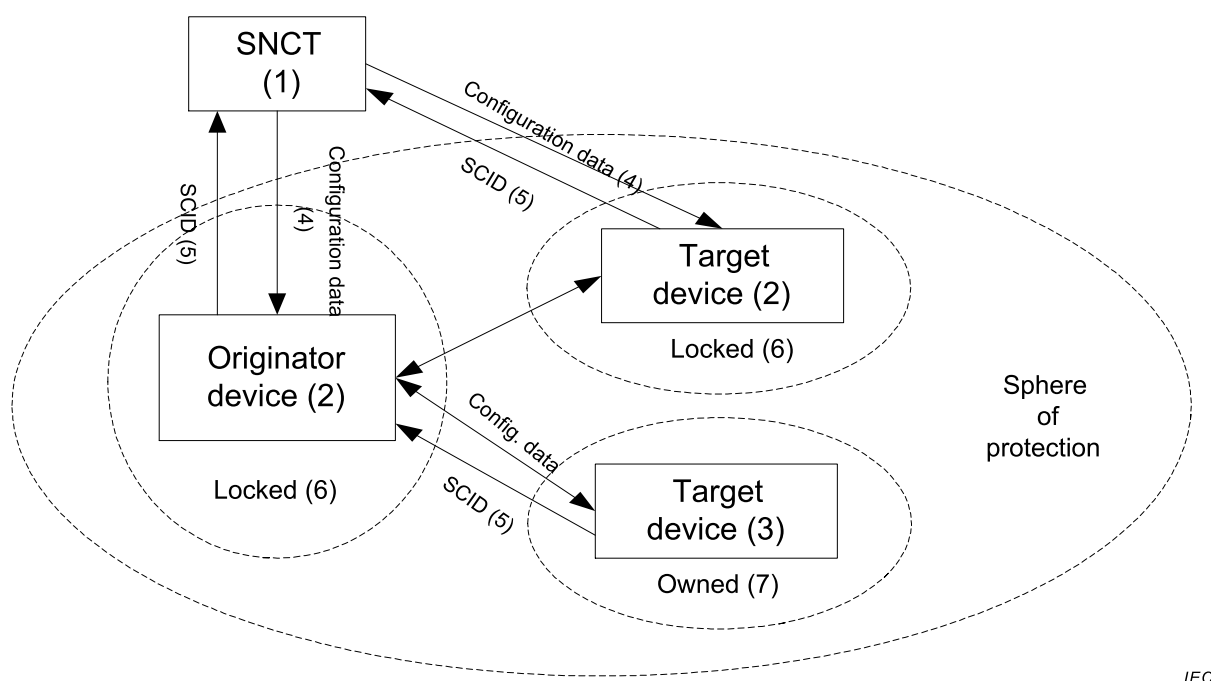


Figure 77 – Protection measures in safety devices

8.9.5 Configuration process SIL3 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 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 SIL3 device shall calculate a SCCRC with SIL3 integrity and compare it to the SCCRC within the SCID;
- For Form 1 configured or tool configured devices, configuration validation of the downloaded safety-relevant data from the software (or originator) shall be performed with SIL3 integrity;
- When a SIL3 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;
- SIL3 devices shall store/restore its configuration data with SIL3 integrity;
- SIL3 devices shall handle all device state transitions with SIL3 integrity;
- Sub-systems that are required to be examined and assessed to SIL3;
- Target device configuration processing;
- Target device configuration storage;
- Target device configuration validation;
- Target device modes.

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.
- 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

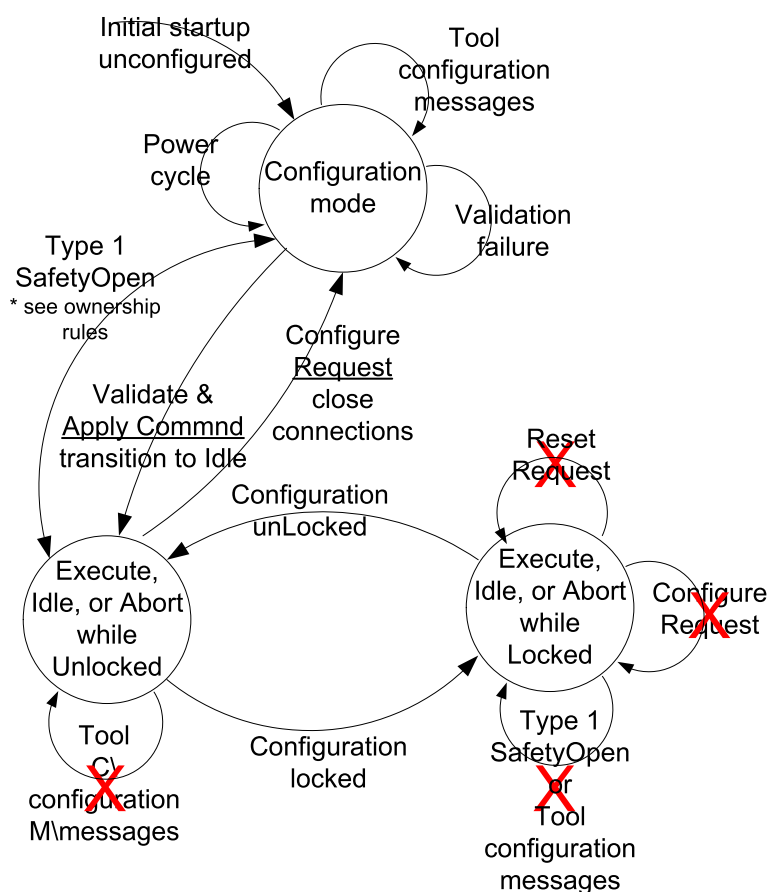
The SNCT interface defines the following functions for Configuration Lock. Its intent is to provide a way for the user to flag that a tool-generated configuration has been tested and verified as valid. From that point, the signature (SCID) reflects a verified configuration. The configuration lock has 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 Form 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 80.

8.9.10 Effect of configuration lock on device behavior

Figure 78 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.



IEC

Figure 78 – Configuration, testing and locked relationships

Table 106 defines the effect that ownership has on a device's ability to be configured. It shows that owned devices can only be Form 1 configured by the originator that has the owner UNID. A locked device can never be configured regardless.

Table 106 – Configuration owner control vs. device state

Ownership rules	Configure mode	Execute/Idle Mode Unlocked	Execute/Idle Mode Locked
Configuration Un-owned	Tool configuration or Form 1 acceptance by anyone	Tool configuration or Form 1 acceptance by anyone	No Tool configuration, No Form 1 accepted
Originator Owned	Tool configuration or Form1 by owner only	No Tool configuration (shall reset first) or Form1 by owner only	No Tool configuration, No Form 1 accepted
Software Tool Owned	Tool configuration only No Form 1 accepted	Tool configuration only No Form 1 accepted	No Tool configuration, No Form 1 accepted

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 79 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.

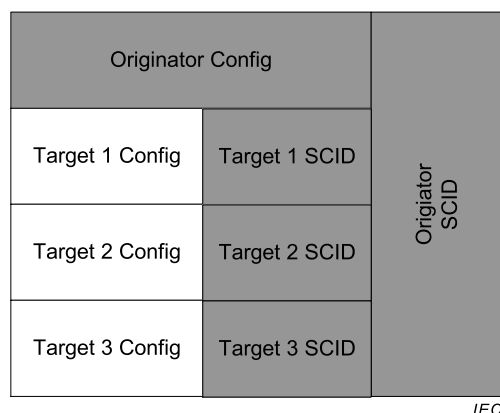


Figure 79 – Originator's configuration data

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.

Other uses of UNID:

- TUNID = Target's Unique Network Identifier. The safety function of the TUNID is to identify 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 Owing 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 Owing 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 function 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

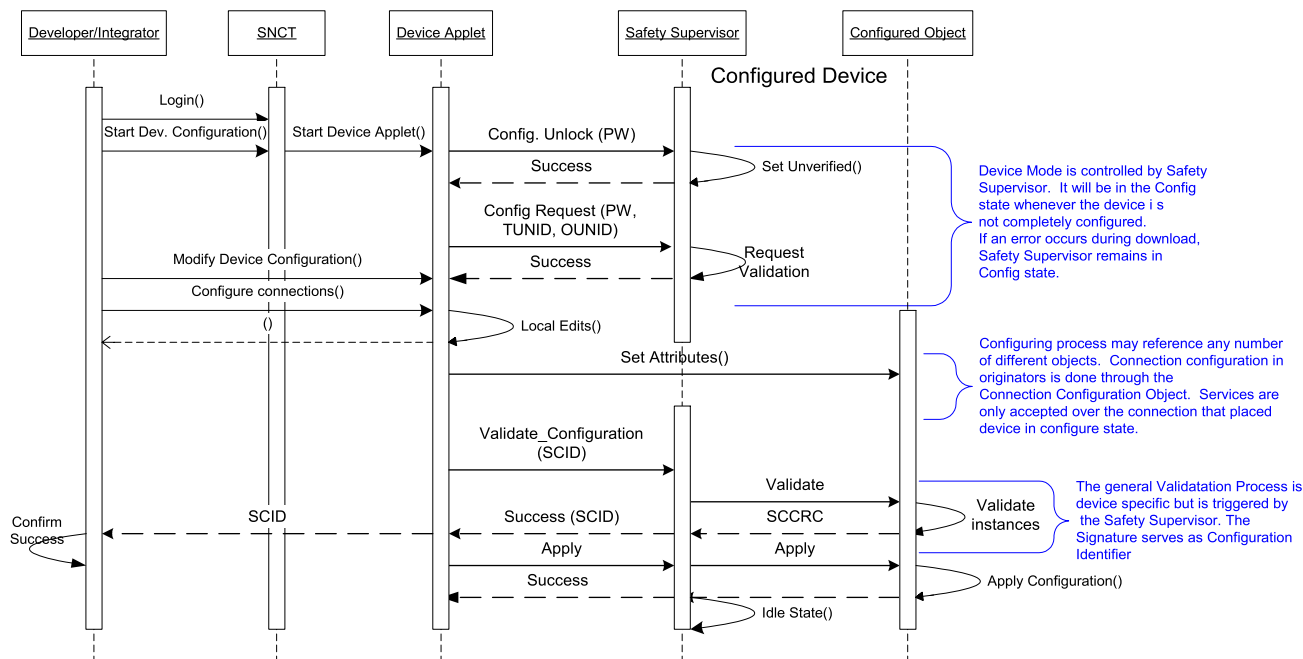
The safety download process ensures that the configuration data is transferred with high integrity from the SNCT or the Originator to the device being configured. At the successful completion of the download process the configuration is considered valid. There are two download processes used with safety devices:

- SNCT downloads to originators and targets;
- Originator downloads to targets using a Form 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 80 show 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.



IEC

Figure 80 – 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 80.

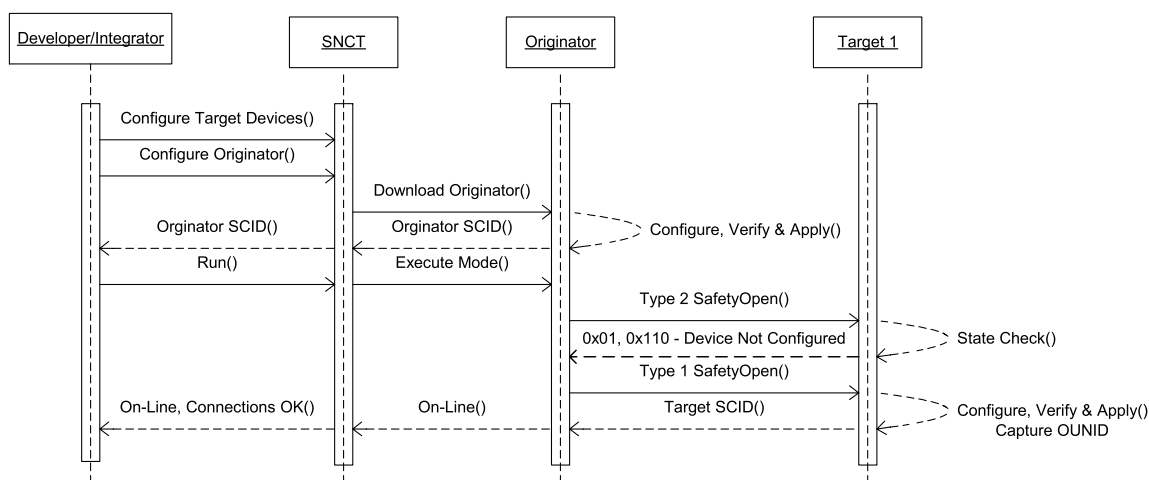
- a) Clear Configuration Lock Attribute
 - i) Device: Configuration Lock Attribute cleared
- b) Enter configuration state with password, TUNID, OUNID
 - i) Device: No safety I/O connections can be active.
 - ii) Device: Device saves Config mode to NV storage
 - A) Until “Validate” and “Apply”, power cycles go back to config mode
- c) Transfer of configuration data
 - i) Tool: Calculate “proposed SCCRC” for data (SCCRC part of SCID)
 - ii) Device: Any explicit messages are allowed to set configuration in device, but device shall only accept safety-related explicit messages over the connection that put it into the configuration mode
- 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.

8.9.14.4 SNCT downloads to originators which do Form 1 target configuration

Figure 81 show the process by which Originators are initially configured and how the Form 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.



IEC

Figure 81 – SNCT Downloads to originators that perform Form 1 configuration

8.9.14.5 SNCT downloads to originators that perform Form 1 configuration

The following are the process steps for SNCT Downloads to originators that perform Form 1 configuration as shown in Figure 81.

- 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)
 - ii) Tool: Any explicit messages are allowed to set configuration in device, but device shall only accept safety-related explicit messages over the connection that put it into the configuration mode.
- 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.
- f) Set Mode to Run
 - i) Originator: Sends Form 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 Form 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 SIL 3 operation. 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 82, 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 82 is that Targets can also be tool-configured as well. In this case, these targets are also “locked” after verification and testing.

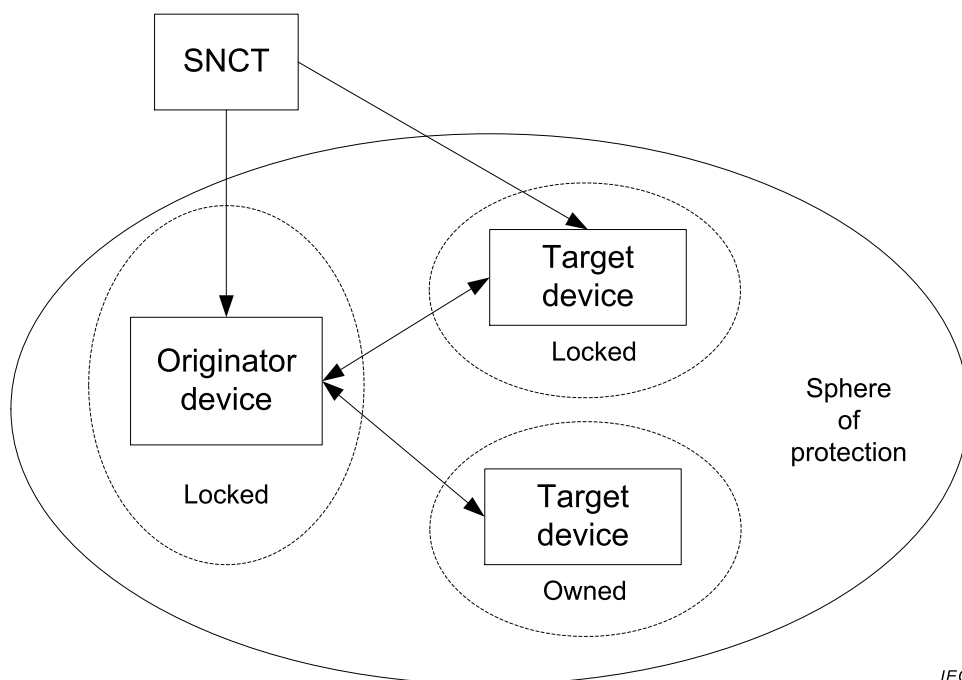


Figure 82 – Protection from locking and ownership

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 four 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.

One or a combination of the following options can be used to fulfill the user verification requirement: user comparison of the original software display, and results of the read back that have been displayed by a diverse means.

8.9.15.2.2 Alternative 1 – immediate read back and diverse comparison

The device configuration data is read back by the work station and presented to the user utilizing a diverse execution path in the workstation, this is shown in Figure 83.

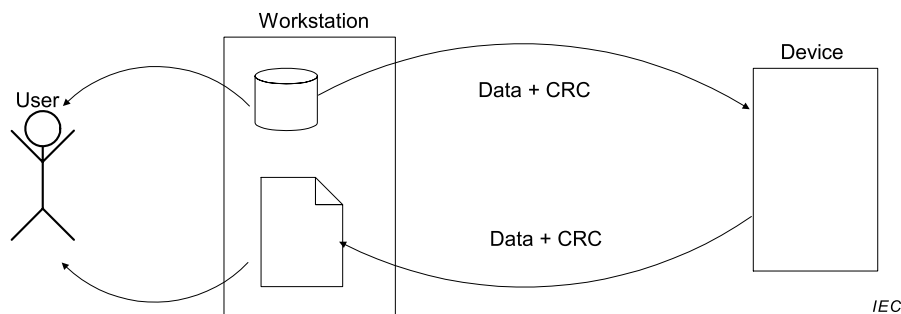


Figure 83 – Example of read back and comparison of original and printout

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.

The user shall examine and compare the printout to the original data to satisfy the integrity requirements. Any automated comparison by the software tools is a diagnostic and shall not be relied upon in and of itself to ensure integrity.

The read back and display using a diverse means reduces the possibility of a systemic error in the workstation causing the same data corruption on data entry and user checking, which could cause an undetected error. If, for instance, a corruption occurred prior to the generation of the CRC the data would be interpreted as correct by the device and the same data and CRC would be sent back to the workstation. Automated checks of the original and read back data would not indicate an error, because the data matches the CRC. If the data was displayed using the same mechanism as the original display mechanism the error could still be masked and would be undetected. The diverse display paths should reduce this common cause of error.

8.9.15.2.3 Alternative 2 – local diverse display

It is possible to achieve the same level of integrity as 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 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. The device then verifies the correct transfer by comparing the data and CRC. 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. At that point the workstation compares the device CRC to the stored CRC. At this time it can be assumed that the data in the workstation was correctly sent to the device. It is important that the CRC is only calculated once by the workstation and stored on the local drive. It is not recalculated for the purpose of transfers. This also ensures the integrity of the data on the local drive. At this point it can be assumed that the data in the workstation was correctly sent to the device.

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. Figure 84 graphically depicts this process.

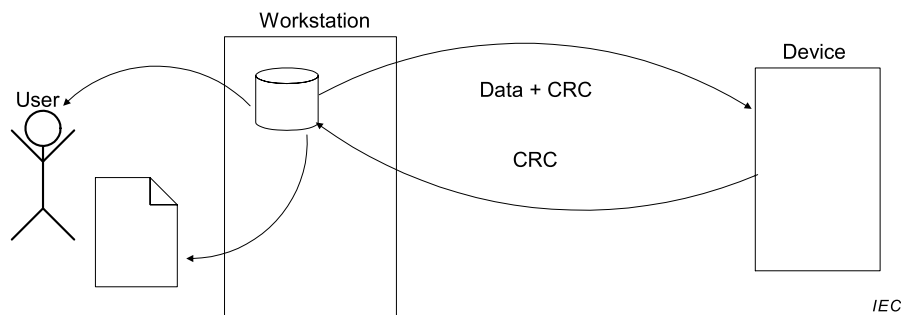
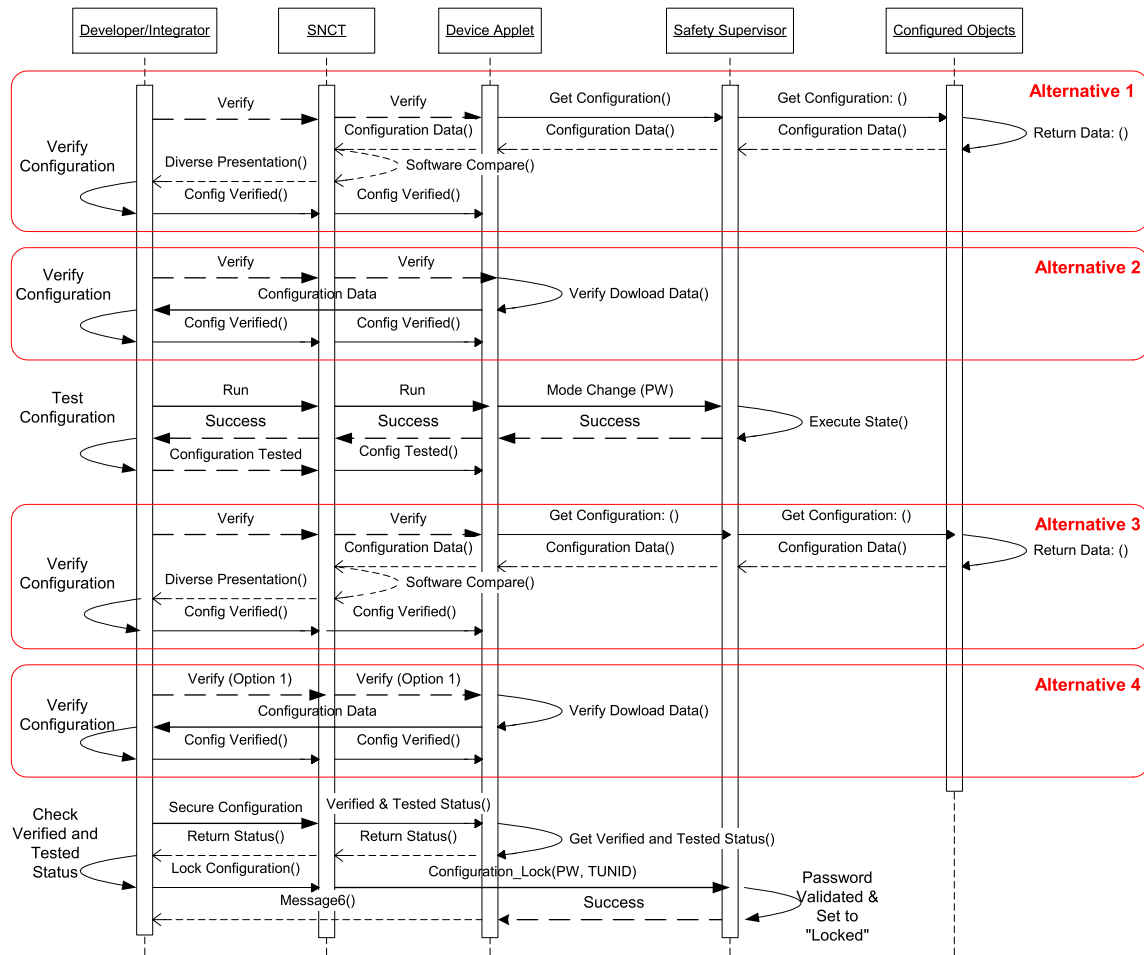


Figure 84 – Diverse display without full data read back

8.9.16 Verification process

Figure 85 defines the complete process for verifying the configuration of safety devices. It is assumed that the data has been 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 SIL 3 operation.



IEC

Figure 85 – Verification process including all alternatives

8.9.17 Configuration error analysis

8.9.17.1 Configuration errors and detection measures relationships

Table 107 defines the errors and detection measures that are considered for the download and configuration process defined by the SNCT interface.

Table 107 – Errors and detection measures

Errors	Detection measures							
	User Authentication	Identification	Identification	SCID validation	Configuration protection	Configuration	Configuration	User Functionality
User misdirected configuration	X					X		X
System misrouted configuration	X		X			X		X
Lost Configuration Message				X				X
Corrupted configuration				X				X
Configuration at inappropriate time							X	
User loads wrong configuration		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.								

8.9.17.2 Configuration errors

8.9.17.2.1 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.

8.9.17.2.2 System misroutes configuration

There are two different cases for a system to misroute a configuration: configuration performed during connection establishment by a Form 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.

8.9.17.2.3 Lost configuration message

The detections for a lost message are the same as those for a misrouted message.

8.9.17.2.4 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.

8.9.17.2.5 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.

8.9.17.2.6 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.

8.9.17.2.7 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.

8.9.17.3 Detection measures

8.9.17.3.1 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.

8.9.17.3.2 Identification of configuration file

All safety configuration files are uniquely identified by the SCID.

8.9.17.3.3 Identification of target to be configured

The configuration mode message and the verify message both use the TUNID for identification of the target.

8.9.17.3.4 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.

8.9.17.3.5 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.

8.9.17.3.6 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 than 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.

8.9.17.3.7 User functional testing

The user is required to functionally test new and replacement devices prior to utilizing the system in a SIL3 environment.

8.9.17.3.8 Configuration protection

After configuration, testing, and user verification has been completed by one of the procedures defined in 8.9.16, 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 82, the combination of locked tool-configured originators and owned targets provides a secure environment to protect the verified system from unauthorized changes.

8.9.17.3.9 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 SIL3 or be assessed. 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.

8.9.17.4 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 part 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.

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 Form1 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 108 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 108 – 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

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:

- Open file as a binary file. Load the entire file into memory;
- Remove the entire line including the carriage return that has the EDSFileCRC= entry;
- Calculate the CRC over the remaining contents of the file;
- 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 109.

Table 109 – 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 SafetyCfgAssembly Keyword shall be used in the safety devices to identify the configuration assembly object instance. The keyword is defined in Table 110.

Table 110 – 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 “SafetyCfgAssembly=” 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.

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 111.

Table 111 – 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
Extended Format Support	ExtendedFormat	1	USINT	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.

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 112 lists the fields currently defined for the Connection Manager section.

Table 112 – 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: always high 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
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 Form 1 SafetyOpen

Field name	Field number	Data type	Usage for safety
config #2 format	12	Param or Assem	This field can indicate which assembly will hold the Form 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
Data Path	15	Eds_Char Array	Complete path comprising of Config, Consumed, and Produced path. Null paths are inserted where no path exists (see possible formats below)
ASYN1	16	USINT	This is a FSCP 2/1 exclusive field Only applies to producing connections. Field should 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 113 provides the only valid values for Safety devices.

Table 113 – Connection parameter field settings for safety

Connection Tltype	Connection parameter setting
Producing (client) input connection	22645505 _{hex} or 22445505 _{hex} (no multipoint)
Consuming (server) output connection	22445505 _{hex}

8.10.2.5.5.4 Data Path field

IEC 61158-6-2 defines a method to construct an application path in a Forward Open for 3 references: one for configuration, one for consumed data, and one for produced data. With the introduction of NULL paths for safety, there are some additional requirements for safety.

8.10.2.5.5.5 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 ASYNC value for those connections, and devices which produce on output connections (i.e. logic devices or scanners) shall define a ASYNC value for these connections. Any value provided on consuming (server) connections will be ignored by the software. If an 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:

- ASYNC = 0 = synchronous;
- 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 EtherNet/IP has a number of system complications when Multicast 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 should 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.

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 114.

Table 114 – CP 2/3 ID assignment rules

Connection Type	Intermediate (First) Hop	Last (Only) Hop 1 st attempt	Last (Only) Hop 2 nd attempt	Last (Only) Hop 3 rd 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.

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.

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 should work reputably. 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 $2 \times$ 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 multi-cast 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 $(\text{connection\_EPI} \times \text{Ping\_Interval\_Multiplier}) \times (\text{Timeout\_Multiplier.PI} + 2)$. 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.

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 standard,
- the same CRC polynomials, seed values and algorithms are used, and

- all FSCP 2/1 objects and services are implemented according to this standard.

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.

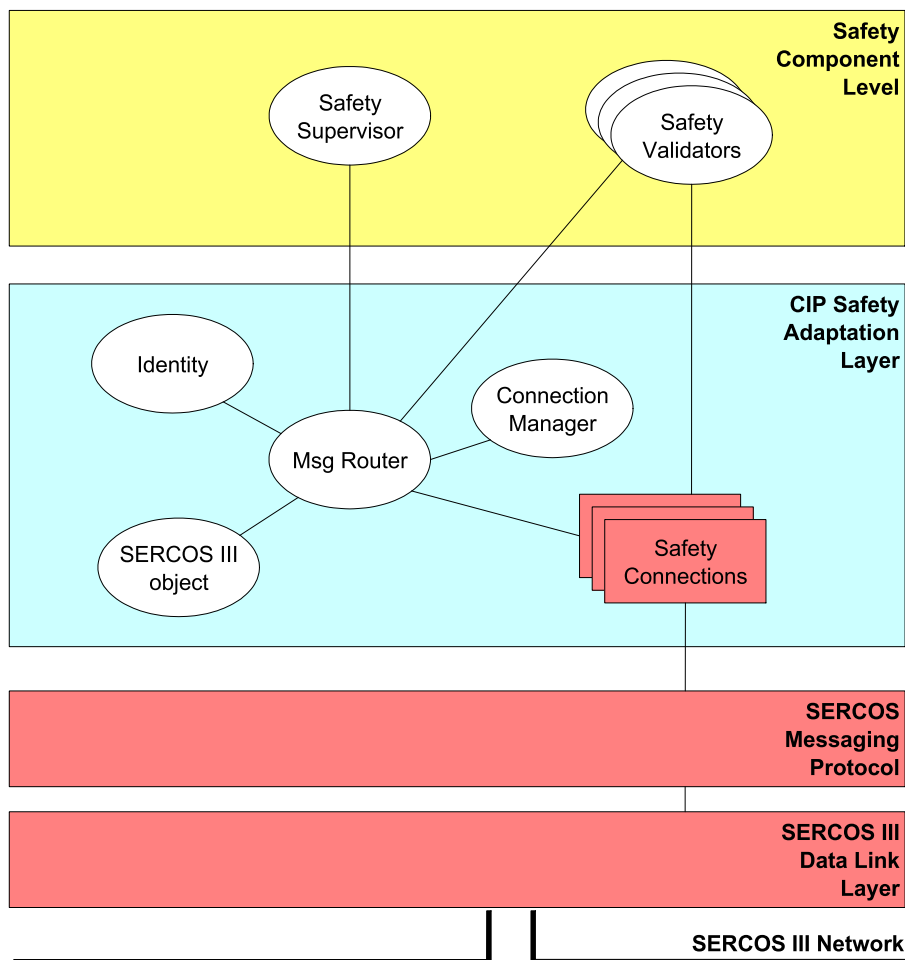
FSCP 2/1 relies on a basic set of standard CIP objects and services to establish transport connections and exchange cyclic data. As CP 16/3 does not provide an implementation of the CIP application layer, an adaptation layer is needed to fill the gap between the CP 16/3 transport layer and FSCP 2/1.

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 86 shows how the FSCP 2/1 Adaptation Layer provides CIP functionality similar to the Baseline Safety Device defined in 6.6.



IEC

Figure 86 – 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 88. 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.

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.

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 87 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.

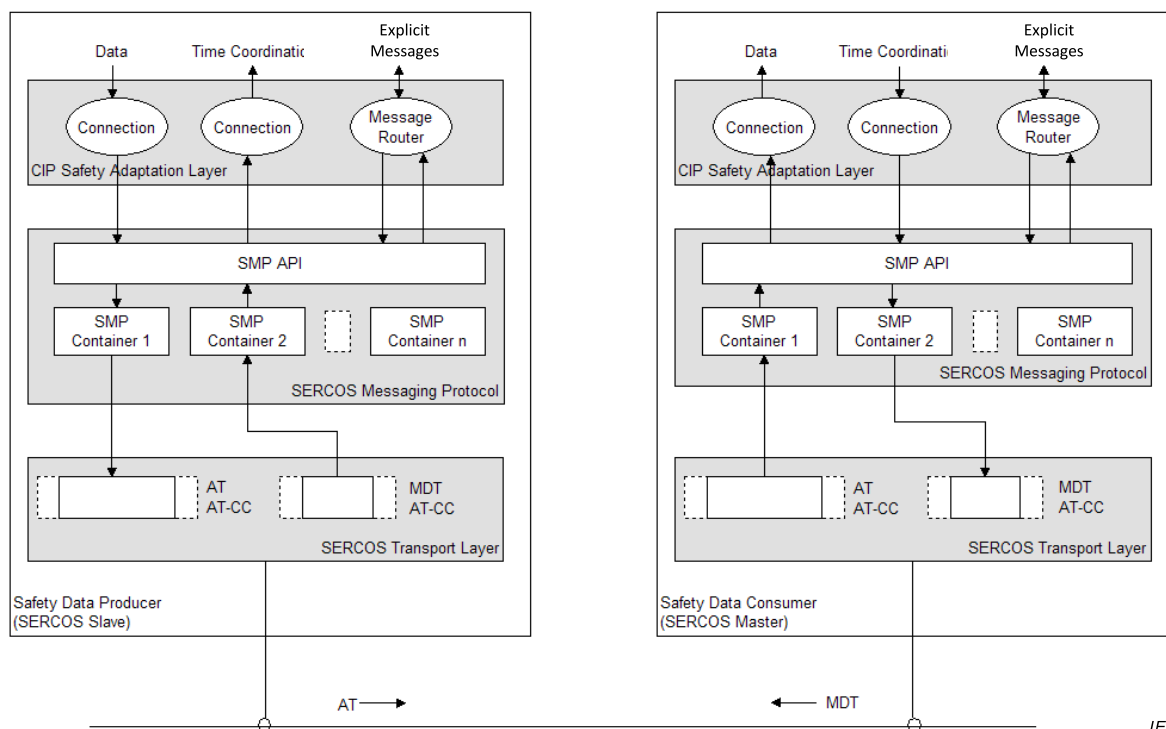


Figure 87 – FSCP 2/1 Adaptation Layer and SMP interaction

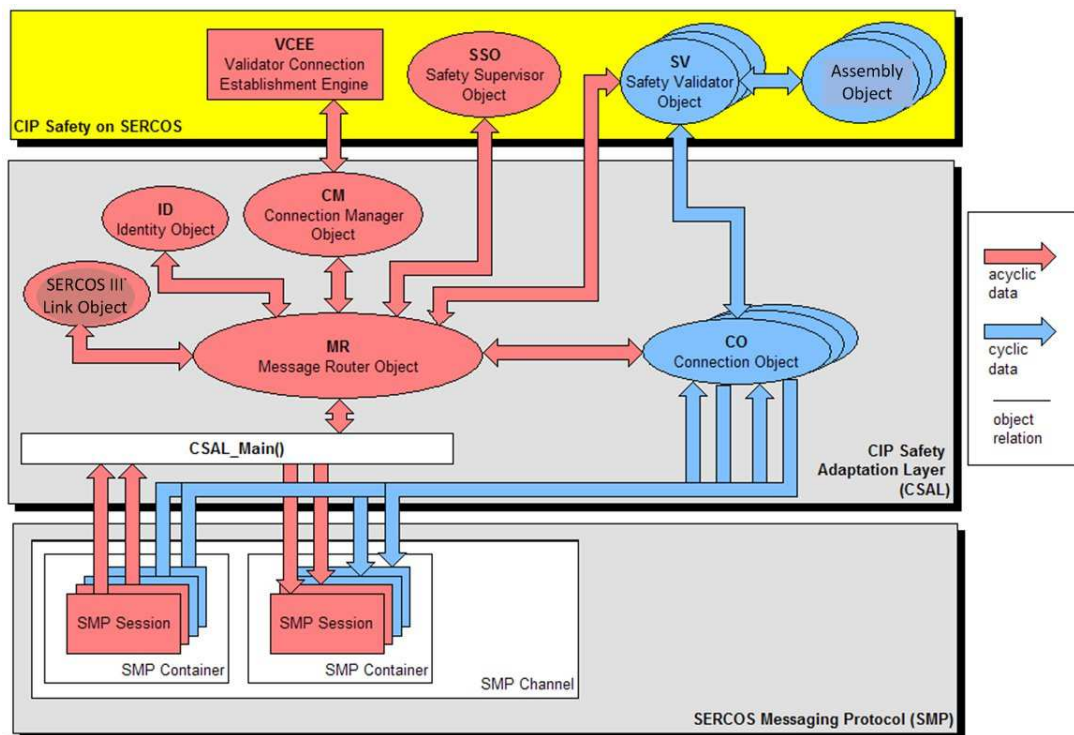
8.13.4.3 Multicast connections

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 88 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.



IEC

Figure 88 – FSCP 2/1 Adaptation

8.13.5 FSCP 2/1 and the CP 16/3 device model

Figure 89 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.

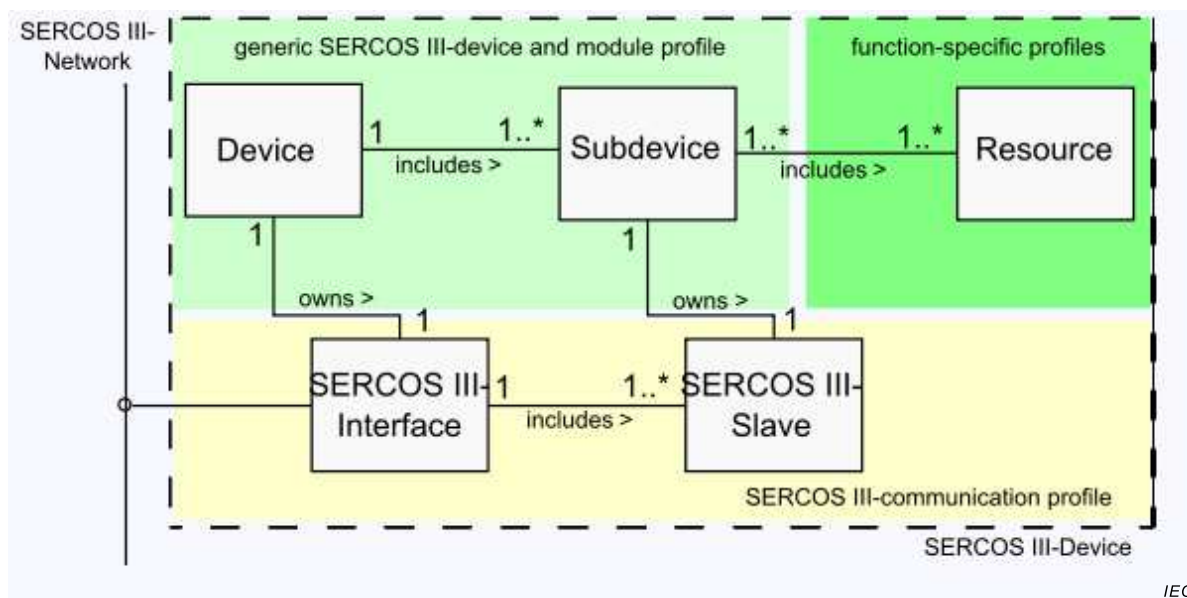


Figure 89 – CP 16/3 device model

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 controllers 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 part. 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 MACID/IPNodeID address portion of the UNID shall be replaced by a 4 octet CP 16/3 Safety Device ID (SDID). Both the SDID and the SNN shall be stored as attributes of the CP 16/3 object.

```
struct UNID
{
    S_SNNDate_AND_Time    SNN;
    UDINT                 SDID;
}
```

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. 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.

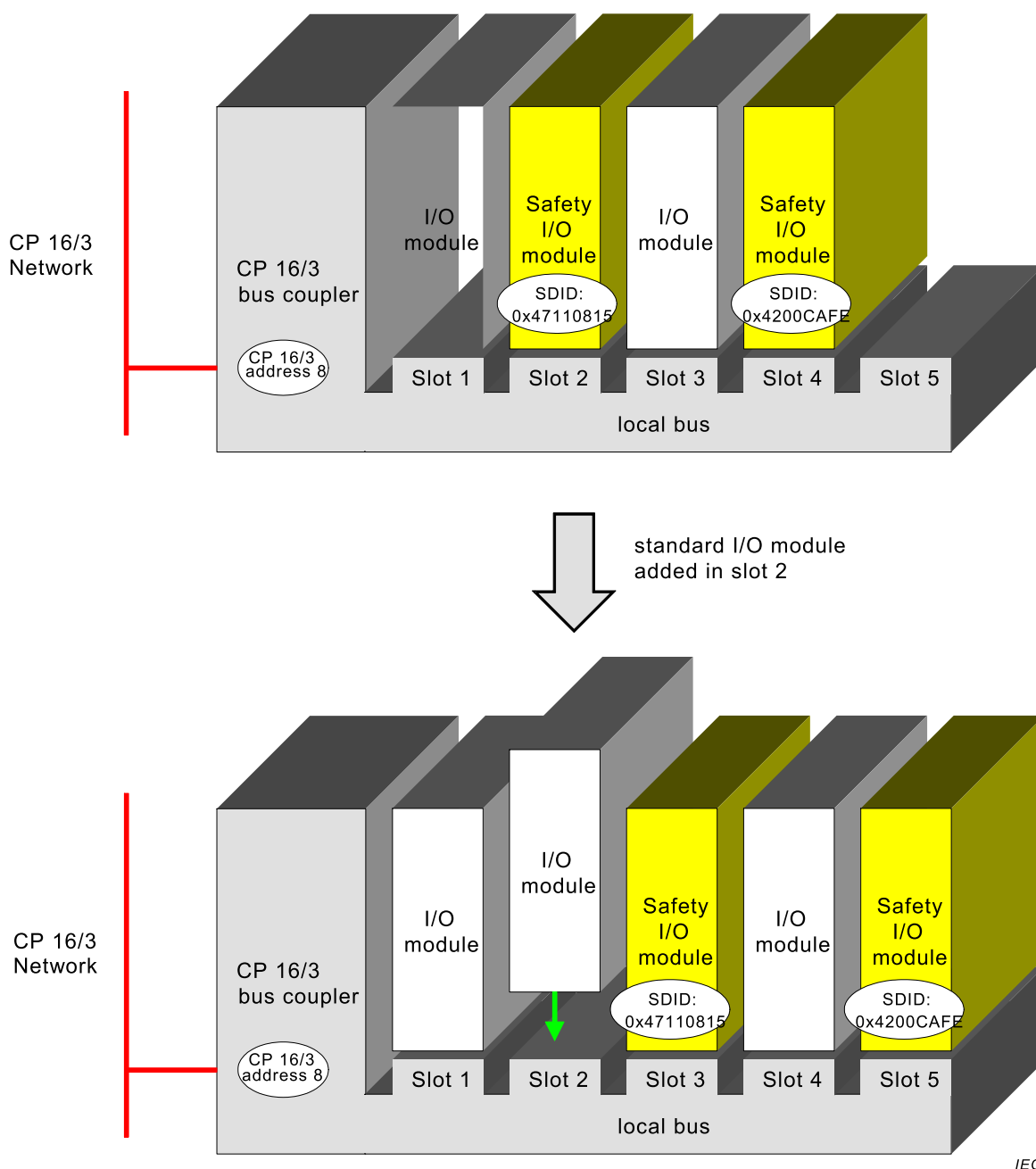


Figure 90 – Adding a standard module to a modular device

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.

Important: FSCP 2/1 safety devices shall provide a separate Module Status LED and a Network Status LED. 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 should be turned on Red.

9.1.2 LED indications for setting the device UNID

Table 115 defines the way the LED indications are used for setting the UNID.

Table 115 – 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 UNID Rcvd	Flash Red/Green	Flash Red/Green 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

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 116 defines the Module Status LED states. Table 116 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 116 – 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 ²	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 117.

Table 117 – Network status LED states

For Safety Supervisor state:	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 may not be powered, look at Module Status LED
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

For Safety Supervisor state:	LED is:	To indicate:
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 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. Safety devices use this indication to allow maintenance personnel to commission the UNID in a safety device
^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.		

9.1.6 Switches

9.1.6.1 NodeID switches

The following algorithm can also be applied to the handling of the Baud Rate switch if implemented. When hardware switches are used for setting NodeID and/or Baud Rate there are some differences in how these values are processed in safety devices. This subclause 9.1.6 will outline the algorithm.

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:

- 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 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). For FSCP 2/1 on CP 16/3 the SDID in the SERCOS III Link object has to be set to default values.
- If the device is out-of-box it shall use the current NodeID switch settings if these are valid values.

Safety devices shall monitor and detect changes in the NodeID and Baud Rate (if applicable) switch settings. Developers are free to determine an appropriate sample period for this detection.

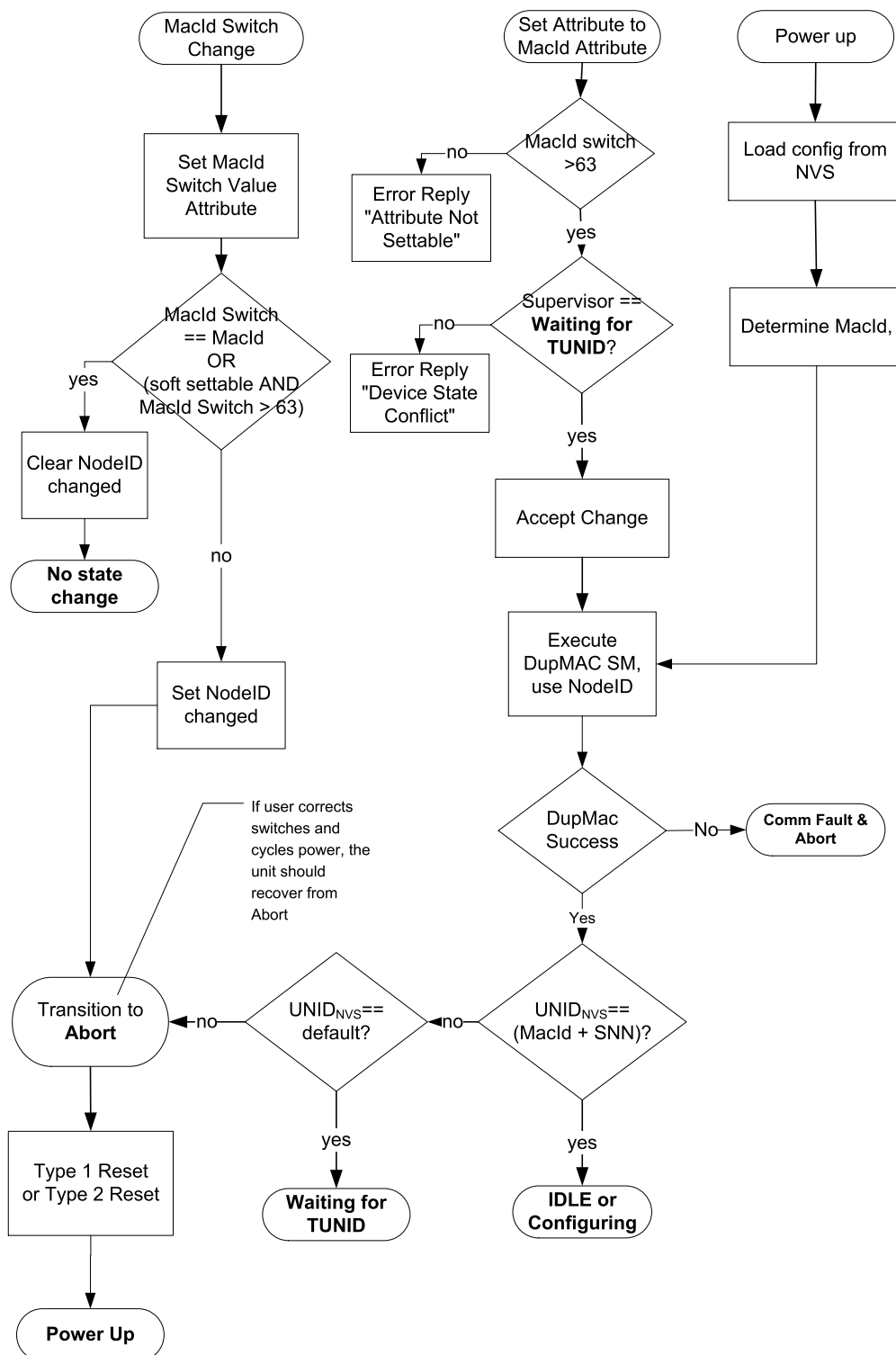
When a NodeID switch setting change is detected, the device shall update the MACID_Switch_Value attribute. If the NodeID switch equals the NodeID in use or the NodeID Switches are greater than 63 and software settable clear the NodeID changed attribute and make no change in the state of the device, otherwise set the NodeID changed attribute and transition to the ABORT state (see flow chart in Figure 91).

When an IP switch setting change is detected it shall determine if the change creates a mismatch condition. If the IP switch differs from the IP Address attribute, it shall transition to the ABORT state.

When a Baud Rate switch setting change is detected, the device shall update the Baud_Rate_Switch_Changed attribute and the Baud_Rate_Switch_Value attribute, then transition to ABORT.

If a FSCP 2/1 safety device supports the Set_Attribute service to the NodeID attribute, and the NodeID switches are set to enable the set service, safety devices shall only accept the Set_Attribute while in the “Waiting for TUNID” state. Otherwise, it shall reply with a “Device State Conflict”.

If a FSCP 2/1 safety 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”.



IEC

Figure 91 – 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).

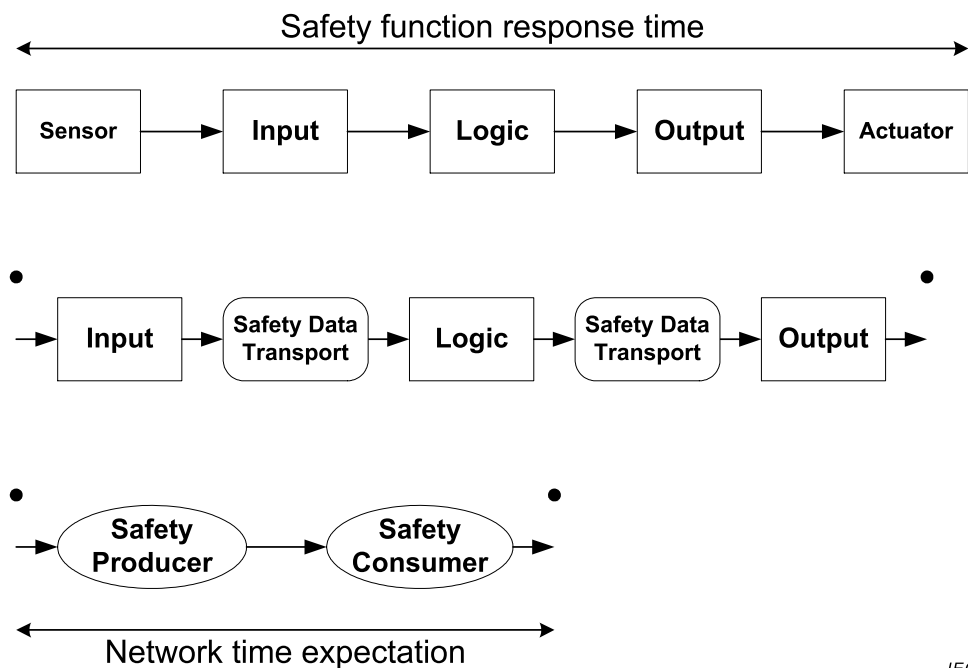
9.2 Installation guidelines

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 92.



IEC

Figure 92 – 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 92, the safety function response time would be:

$$\begin{aligned}
 \text{Safety function response time} = & \text{Sensor reaction time} \\
 & + \text{Input reaction time} \\
 & + \text{Network reaction time} \\
 & + \text{Controller reaction time} \\
 & + \text{Network reaction time} \\
 & + \text{Output reaction time} \\
 & + \text{Actuator reaction time}
 \end{aligned}
 \tag{13}$$

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 part, 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.

The `Network_Time_Expectation_Multiplier` value necessary to ensure a timeout error is not detected is:

$$\begin{aligned} \text{Network\_Time\_Expectation\_Multiplier} > & \text{EPI} \times \text{Timeout\_Multiplier} \\ & + \text{Safety\_Message\_Time}(\text{max}) \\ & + \text{Time\_Coord\_Message\_Time}(\text{max})) / 128 \mu\text{s} \\ & + \text{Connection\_Correction\_Constant} \end{aligned} \quad (14)$$

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_Rcvd_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 118 defines the producing application and consuming application for the Network reaction time cases above.

Table 118 – 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 93 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.

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.

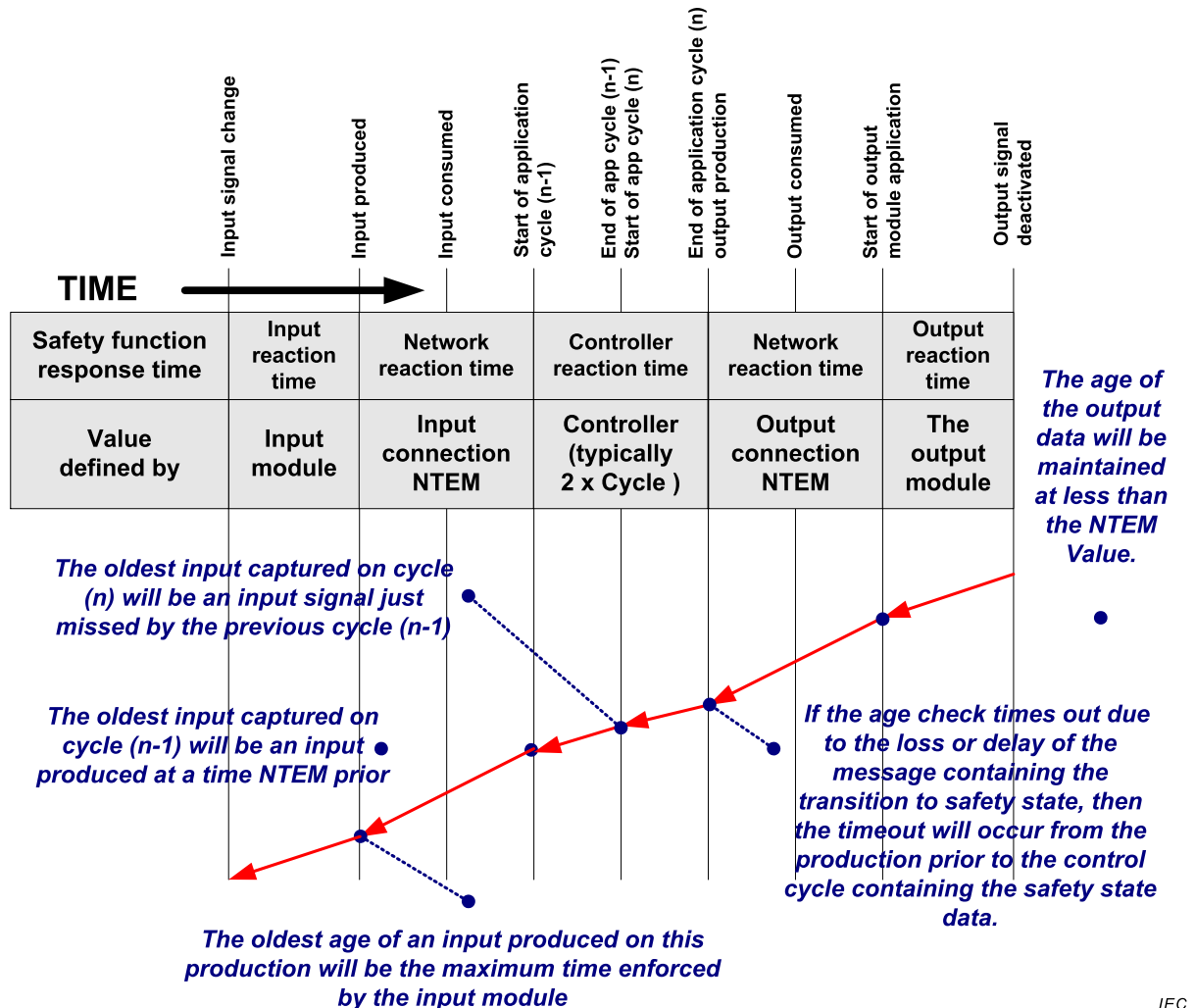


Figure 93 – Safety function response time components

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:

$$\text{Network reaction time} = \text{Network\_Time\_Expectation\_Multiplier} \times 128 \mu\text{S} \quad (16)$$

If the Output Production is Synchronous to the Controller Cycle:

$$\text{Network reaction time} = \text{Network\_Time\_Expectation\_Multiplier} \times 128 \mu\text{S} - \text{EPI\_in\_Sec} \quad (17)$$

IEC

The Output Connection cases can be simplified to:

$$\text{Network reaction time} = \text{Network Time Expectation Multiplier} \times 128 \mu\text{S} + (\text{EPI\_in\_Sec} \times (\text{ASync} - 1)) \quad (18)$$

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

This subclause 9.5.2 will describe the calculations used for the determination of the network PFH. The network is targeted at SIL 3 systems therefore the PFH shall be $<10^{-9}$ (or $<10^{-7}$ if a 1 % factor is included in the calculations).

The safety 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.

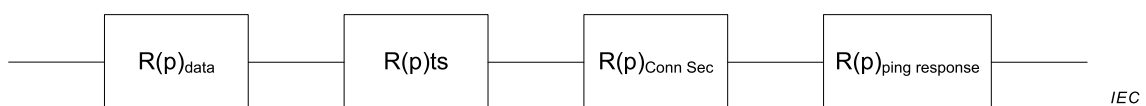


Figure 94 – Network protocol reliability block diagram (RBD)

From the RBD in Figure 94, the equation for the overall network residual error rate is:

$$R(p)T = R(p) \text{ data} + R(p)ts + R(p)\text{time coord} + R(p) \text{ time\_corr} \quad (19)$$

When applying the residual error rates in the calculation of the PFH, it is important to consider that the time coordination and the multipoint time correction information are transmitted at rates other than the rate of the time stamp and data. Using the different transmission rates and the information from the RBD, for the overall PFH equation for point-to-point connection is:

$$\Lambda = 3\,600 \times (((R(p)ts + R(p) \text{ data}) \times v_{\text{msg}}) + (R(p)t_{\text{coord}} \times v_{\text{ping}})) \times (\text{NoProd} - 1) \times 100 \quad (20)$$

where

v_{msg} is the transmission rate in messages/second;
 v_{ping} is the transmission rate in messages/second;
 NoP is the number of Producers;
 $3\,600$ is the conversion of hours to seconds;
 100 is the 1 % factor.

The PFH equation for multipoint PFH is:

$$\Lambda = 3\,600 \times (((R(p)t_s + R(p)t_{data}) \times v_{msg} \times NoP) + ((R(p)t_{coord} + R(p)t_{corr}) \times v_{ping} \times NoC/P)) \times 100 \quad (21)$$

where

v_{msg} is the transmission rate in messages/second;
 v_{ping} is the transmission rate in messages/second;
 NoC/P is the number of Consumers per Producer;
 NoP is the number of Producers;
 $3\,600$ is the conversion of hours to seconds;
 100 is the 1 % factor.

Figure 95 and Figure 96 summarizes the worst-case result. The numbers are obtained from detailed calculations and the equations above.

Inputs			
Expected Packet Interval (EPI)		0,010	Seconds
Ping Interval		1,000	Seconds
Number of Nodes (m)		63	
Multipoint Consumers		15	
Bit Error Probability		0,001	
Results			
		Point-to-point	Multipoint
R(p)data ≤ 2 octets	R(p) data section – 2 octets of data	$7,02 \times 10^{-20}$	$7,02 \times 10^{-20}$
R(p)data ≥ 3 octets	R(p) data section – 250 octets of data	$8,54 \times 10^{-19}$	$8,54 \times 10^{-19}$
R(p)data	R(p) data section	$8,54 \times 10^{-19}$	$8,54 \times 10^{-19}$
R(p)ts	R(p)time stamp section	$3,18 \times 10^{-18}$	$3,18 \times 10^{-18}$
R(p)multi	R(p) Time correction message		$2,68 \times 10^{-18}$
R(p)reply	R(p) Time coordination message	$2,68 \times 10^{-18}$	$2,68 \times 10^{-18}$
Msg_per_sec	Messages per second = 1 / EPI	100	100
Rpl_per_sec	Replies per second = 1 / Ping_Interval	1,00	1,00
	λ	$9,07 \times 10^{-9}$	$1,08 \times 10^{-8}$
	% of 1,00E-07 goal, up to 100 % is OK	9,07 %	10,80 %
	PFH = λ / 100	$9,07 \times 10^{-11}$	$1,08 \times 10^{-10}$
	% of SIL 3 (1,00E-07) PFD limit, up to 1 % is OK	0,090 7 %	0,108 0 %

Figure 95 – Network PFH summary

Inputs			
Expected Packet Interval (EPI)		0,010	Seconds
Ping Interval		0,524	Seconds
Number of Nodes (m)		63	
Multipoint Consumers		15	
Bit Error Probability		0,001	
Results			
		Point-to-point	Multipoint
R(p)data <= 2 octets	R(p) data section – 2 octets of data	$5,05 \times 10^{-22}$	$5,05 \times 10^{-22}$
R(p)data >= 3 octets	R(p) data section – 250 octets of data	$4,34 \times 10^{-25}$	$4,34 \times 10^{-25}$
R(p)data	R(p) data section	$5,05 \times 10^{-22}$	$5,05 \times 10^{-22}$
R(p)ts	R(p)time stamp section	$1,26 \times 10^{-22}$	$1,26 \times 10^{-22}$
R(p)multi	R(p) Time correction message		$1,31 \times 10^{-18}$
R(p)reply	R(p) Time coordination message	$1,13 \times 10^{-18}$	$1,31 \times 10^{-18}$
Msg_per_sec	Messages per second = 1 / EPI	100	100
Rpl_per_sec	Replies per second = 1 / Ping_Interval	1,00	1,00
	λ	$2,66 \times 10^{-11}$	$8,18 \times 10^{-10}$
	% of 1,00E-07 goal, up to 100 % is OK	0,022 6 %	0,818 %
	PFH = λ / 100	$2,66 \times 10^{-13}$	$8,18 \times 10^{-12}$
	% of SIL 3 (1,00E-07) PFD limit, up to 1 % is OK	0,000 3 %	0,008 2 %

Figure 96 – Extended Format PFH summary

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.

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 be 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 part 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.

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, 0xBF06116,
0x21B4F4B5, 0x56B3C423, 0xCFBA9599, 0xB8BDA50F,
0x2802B89E, 0x5F058808, 0xC60CD9B2, 0xB10BE924,
0x2F6F7C87, 0x58684C11, 0xC1611DAB, 0xB6662D3D,
0x76DC4190, 0x01DB7106, 0x98D220BC, 0xEF5102A,
0x71B18589, 0x06B6B51F, 0x9FBE4A5, 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,
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, 0x4FDDF252,
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, 0xCA7, 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,
0xEEDB, 0xE6D4, 0xFEC5, 0xF6CA, 0xC EE7, 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,
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,
};

```

```

// polynomial 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, 0x000cd6643, 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,
0x00f6cba0, 0x00aba66b, 0x004c1036, 0x00117dfd,
0x006eebcc, 0x00338607, 0x00d4305a, 0x00895d91,
0x0046312b, 0x001b5ce0, 0x00fceaabd, 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, 0x0022fbfa, 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)
```

```
{
    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
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

/xx 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

/** 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.
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

/xx 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:
x/
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++)
{
    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()
{
    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;

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++)
    {
        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;

//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();

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

Annex B

(informative)

Information for assessment of the functional safety communication profiles of CPF 2

According to IEC rules, this standard 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 standard 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.

Bibliography

- [1] IEC 60050 (all parts), *International Electrotechnical Vocabulary* (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 60204-1, *Safety of machinery – Electrical equipment of machines – Part 1: General requirements*
- [3] IEC TS 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 61131-6, *Programmable controllers – Part 6: Functional safety*
- [6] IEC 61158 (all parts), *Industrial communication networks – Fieldbus specifications*
- [7] IEC 61496 (all parts), *Safety of machinery – Electro-sensitive protective equipment*
- [8] IEC 61508-1:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements*
- [9] IEC 61508-4:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations*
- [10] 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*
- [11] IEC 61511 (all parts), *Functional safety – Safety instrumented systems for the process industry sector*
- [12] IEC 61784-4¹¹, *Industrial communication networks – Profiles – Part 4: Secure communications for fieldbuses*
- [13] IEC 61784-5 (all parts), *Industrial communication networks – Profiles – Part 5: Installation of fieldbuses – Installation profiles for CPF x*
- [14] IEC 61800-5-2, *Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional*
- [15] IEC TR 62059-11:2002, *Electricity metering equipment – Dependability – Part 11: General concepts*
- [16] IEC 62061, *Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems*

¹¹ Proposed new work item under consideration.

- [17] IEC TR 62210:2003, *Power system control and associated communications – Data and communication security*
- [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] IEC TR 62685, *Industrial communication networks – Profiles – Assessment guideline for safety devices using IEC 61784-3 functional safety communication profiles (FSCPs)*
- [21] ISO/IEC Guide 51:2014, *Safety aspects – Guidelines for their inclusion in standards*
- [22] ISO/IEC 2382-14, *Information technology – Vocabulary – Part 14: Reliability, maintainability and availability*
- [23] ISO/IEC 2382-16:1996, *Information technology – Vocabulary – Part 16: Information theory*
- [24] ISO/IEC 7498-1, *Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model*
- [25] ISO/IEC 19501:2005, *Information technology – Open Distributed Processing – Unified Modeling Language (UML) Version 1.4.2*
- [26] ISO 10218-1, *Robots and robotic devices – Safety requirements for industrial robots – Part 1: Robots*
- [27] ISO 12100, *Safety of machinery – General principles for design – Risk assessment and risk reduction*
- [28] ISO 13849 (all parts), *Safety of machinery – Safety-related parts of control systems*
- [29] ANSI/ISA-84.00.01-2004 (all parts), *Functional Safety: Safety Instrumented Systems for the Process Industry Sector*
- [30] GS-ET-26¹², *Grundsatz für die Prüfung und Zertifizierung von Bussystemen für die Übertragung sicherheitsrelevanter Nachrichten*, May 2002. HVBG, Gustav-Heinemann-Ufer 130, D-50968 Köln ("*Principles for Test and Certification of Bus Systems for Safety relevant Communication*") (available in German only)
- [31] VDI/VDE 2180 (all parts), *Safeguarding of industrial process plants by means of process control engineering*
- [32] ANDREW S. TANENBAUM, DAVID J. WETHERALL, *Computer Networks*, 5th Edition, Prentice Hall, N.J., ISBN-10: 0132126958, ISBN-13: 978-0132126953
- [33] W. WESLEY PETERSON, EDWARD J. WELDON, *Error-Correcting Codes*, 2nd Edition 1972, MIT-Press, ISBN 0-262-16-039-0
- [34] NFPA79 (2012), *Electrical Standard for Industrial Machinery*

¹² This document has been one of the starting points for this part. It is currently undergoing a major revision.

- [35] GUY E. CASTAGNOLI, *On the Minimum Distance of Long Cyclic Codes and Cyclic Redundancy-Check Codes*, 1989, Dissertation No. 8979 of ETH Zurich, Switzerland
 - [36] 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
 - [37] The CIP Networks Library Volume 5: *CIP Safety Specification*, Edition 2.6, November 2012, available at <<http://www.odva.org>>
 - [38] The CIP Networks Library Volume 1: *CIP Common*, Edition 3.18, April 2015, available at <<http://www.odva.org>>
 - [39] IEC 62026-3, *Low-voltage switchgear and controlgear – Controller-device interfaces (CDIs) – Part 3: DeviceNet*
-

SOMMAIRE

AVANT-PROPOS	284
0 Introduction	286
0.1 Généralités	286
0.2 Déclaration de droits de propriété	289
1 Domaine d'application.....	291
2 Références normatives	291
3 Termes, définitions, symboles, abréviations et conventions	293
3.1 Termes et définitions	293
3.1.1 Termes et définitions communs	293
3.1.2 CPF 2: Termes et définitions supplémentaires	298
3.2 Symboles et abréviations	299
3.2.1 Symboles et abréviations communs	299
3.2.2 CPF 2: Symboles et abréviations supplémentaires	299
3.3 Conventions.....	300
4 Présentation générale du FSCP 2/1 (CIP Safety™)	301
4.1 Généralités	301
4.2 FSCP 2/1	301
5 Généralités.....	303
5.1 Documents externes de spécifications applicables au profil.....	303
5.2 Exigences fonctionnelles de sécurité	303
5.3 Mesures de sécurité	303
5.4 Structure de la couche de communication de sécurité	304
5.5 Relations avec la FAL (et DLL, PhL)	306
5.5.1 Généralités	306
5.5.2 Types de données.....	306
6 Services de la couche de communication de sécurité	306
6.1 Introduction.....	306
6.2 Objet connexion	306
6.2.1 Généralités	306
6.2.2 Extensions des attributs de classe.....	306
6.2.3 Extensions de services.....	307
6.2.4 Format de réponse de messages explicites pour SafetyOpen et SafetyClose	308
6.3 Objet Gestionnaire de connexion	308
6.3.1 Généralités	308
6.3.2 ForwardOpen pour la sécurité	309
6.3.3 Segment de réseau de sécurité	311
6.3.4 Règles du point d'origine pour le calcul du CRC de paramètre de connexion	315
6.3.5 Organigrammes de traitement de SafetyOpen.....	316
6.3.6 Contrôles exigés par les producteurs multipoints avec les connexions existantes	322
6.3.7 Utilisation de la clé électronique de sécurité	322
6.3.8 RPI en fonction d'API dans les connexions de sécurité	323
6.3.9 Élaboration du chemin d'application de sécurité.....	323
6.3.10 Types de connexion de l'objet de validation de sécurité	324

6.3.11	Données de réponse d'application dans une réponse SafetyOpen satisfaisante	326
6.3.12	Réponse SafetyOpen non satisfaisante	328
6.3.13	Service ForwardClose de sécurité	330
6.4	Objet Identité	330
6.4.1	Généralités	330
6.4.2	Modifications apportées aux services communs	331
6.4.3	Extensions pour les appareils CP 16/3.....	331
6.5	Objets de liaison	331
6.5.1	Modifications apportées à l'objet DeviceNet.....	331
6.5.2	Modifications apportées à l'objet Interface TCP/IP	332
6.5.3	Objet Liaison SERCOS III	332
6.6	Objet Programme de contrôle de sécurité	334
6.6.1	Généralités	334
6.6.2	Attributs de classe de programme de contrôle de sécurité.....	335
6.6.3	Sous-classes	335
6.6.4	Attributs instance de programme de contrôle de sécurité	335
6.6.5	Sémantique	339
6.6.6	Sous-classes	346
6.6.7	Services communs du programme de contrôle de sécurité	346
6.6.8	Comportement du Programme de contrôle de sécurité	358
6.7	Objet de validation de sécurité	366
6.7.1	Généralités	366
6.7.2	Attributs de classe	366
6.7.3	Attributs instance	366
6.7.4	Services de classes	374
6.7.5	Services instance.....	374
6.7.6	Comportement d'objet.....	375
6.8	Objet de configuration de connexion.....	379
6.8.1	Généralités	379
6.8.2	Extensions d'attributs de classe	379
6.8.3	Attributs, ajouts et extensions instances	379
6.8.4	Extensions ou restrictions de sémantique des attributs instance pour des raisons de sécurité	382
6.8.5	Paramètres spéciaux relatifs à la sécurité – (Attribut 13).....	387
6.8.6	Services spécifiques à l'objet	393
6.8.7	Extensions des services communs pour la sécurité	394
6.8.8	Comportement d'objet.....	396
7	Protocole de couche de communication de sécurité.....	397
7.1	Format PDU de sécurité	397
7.1.1	Codage PDU de sécurité	397
7.1.2	CRC de sécurité.....	411
7.2	Comportement du protocole de communication	412
7.2.1	Séquence des contrôles de sécurité	412
7.2.2	Terminaison de connexion.....	412
7.2.3	Erreur de contre-vérification	413
7.3	Opération de datation.....	413
7.4	Comptages de remplacement dans l'EF	414
7.5	Diagrammes séquentiels de protocoles.....	414

7.5.1	Généralités	414
7.5.2	Transmission de sécurité normale	415
7.5.3	Transmission de messages perdus, corrompus et retardés	417
7.5.4	Transmission de messages perdus, corrompus ou retardés avec production répétée	419
7.5.5	Demande Ping point à point	422
7.5.6	Demande Ping multipoints avec sécurité CP 2/3	423
7.5.7	Demande Ping multipoints sur les réseaux de sécurité CP 2/2	425
7.5.8	Demande Ping multipoints – Retransmission aboutie	426
7.5.9	Demande Ping multipoints – Retransmission avec temporisation	427
7.6	Définition du protocole de sécurité	428
7.6.1	Généralités	428
7.6.2	Vue de haut niveau d'un appareil de sécurité	428
7.6.3	Objet de validation de sécurité	429
7.6.4	Relation entre SafetyValidatorServer et SafetyValidatorClient	429
7.6.5	Gestion du remplacement de la datation de format étendu	431
7.6.6	Définition de la fonction SafetyValidatorClient	437
7.6.7	Définition de la fonction SafetyValidatorServer	446
7.7	Spécifications des messages de sécurité et des données de protocole	459
7.7.1	Octet de mode	459
7.7.2	Section de datation	460
7.7.3	Message de coordination temporelle	460
7.7.4	Message de correction de temps	461
7.7.5	Production des données de sécurité	462
7.7.6	Variables dynamiques du producteur	469
7.7.7	Variables dynamiques de producteur par consommateur	472
7.7.8	Variables de données du consommateur	473
7.7.9	Variables statiques d'entrée du consommateur	475
7.7.10	Variables dynamiques du consommateur	476
8	Gestion de la couche de communication de sécurité	478
8.1	Présentation générale	478
8.2	Définition des mesures utilisées lors de l'établissement d'une connexion	479
8.3	Validation de la relation point d'origine-cible	483
8.4	Détection des demandes de connexion mal acheminées	484
8.5	Traitement de SafetyOpen	484
8.6	Gestion de propriété	484
8.7	Pontage de différentes couches physiques	486
8.8	Établissement de connexion de sécurité	487
8.8.1	Présentation générale	487
8.8.2	Faits de base pour l'établissement d'une connexion	488
8.8.3	Configuration des connexions de sécurité	488
8.8.4	Multiplicateur de délai de réseau	490
8.8.5	Établissement de connexions	492
8.8.6	Recommandations pour l'attribution d'un nombre de consommateurs	495
8.8.7	Recommandations pour l'établissement d'une connexion	496
8.8.8	Établissement de propriété	497
8.8.9	Cas d'utilisation de la propriété	497
8.8.10	Utilisation et établissement de la relation PID/CID	500

8.8.11	Utilisation PID/CID correcte dans les connexions multipoints et point à point	501
8.8.12	Services pris en charge par le réseau	504
8.8.13	Type d'appareil de sécurité FSCP 2/1	504
8.9	Processus de configuration de sécurité	509
8.9.1	Introduction à la configuration de sécurité	509
8.9.2	Objectifs de configuration	509
8.9.3	Présentation générale de la configuration	510
8.9.4	Lignes directrices pour la configuration de l'utilisateur	511
8.9.5	Justification de niveau SIL3 du processus de configuration	512
8.9.6	Fonctions d'appareils pour configuration par outil	513
8.9.7	Sécurité par mot de passe	513
8.9.8	Services d'interface SNCT	513
8.9.9	Verrouillage de configuration	514
8.9.10	Influence du verrouillage de configuration sur le comportement des appareils	514
8.9.11	Propriété de configuration	516
8.9.12	Mode de configuration	516
8.9.13	Mesures d'assurance de l'intégrité du processus de configuration	516
8.9.14	Processus de téléchargement aval	519
8.9.15	Processus de vérification	523
8.9.16	Processus de vérification	526
8.9.17	Analyse des erreurs de configuration	528
8.10	Extensions de fiches techniques électroniques à des fins de sécurité	532
8.10.1	Règles générales applicables aux appareils de sécurité EDS	532
8.10.2	Extensions EDS à des fins de sécurité	532
8.11	Exigences pour le profil CP 2/2	538
8.11.1	Règles EPI applicables aux messages de sécurité acheminés via CP 2/2	538
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 profil CP 2/3	539
8.12.1	Attribution des identifiants CP 2/3	539
8.12.2	Exigences supplémentaires	542
8.13	Exigences pour le profil CP 16/3	542
8.13.1	Architecture générale de la CPF 2 sur CP 16/3	542
8.13.2	FSCP 2/1 de référence pour 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	548
8.13.6	Attribution de l'UNID sur CP 16/3	549
9	Exigences système	551
9.1	Voyants et commutateurs	551
9.1.1	Exigences générales concernant les voyants	551
9.1.2	Indications LED pour le paramétrage de l'UNID des appareils	551
9.1.3	LED État du module	551
9.1.4	Avertissement lié aux voyants	552
9.1.5	LED État de réseau	552

9.1.6	Commutateurs	553
9.2	Lignes directrices d'installation	556
9.3	Temps de réponse de la fonction de sécurité	556
9.3.1	Présentation générale	556
9.3.2	Délai du réseau	558
9.3.3	Équation de calcul des temps de réaction du réseau	558
9.4	Durée des demandes (ou sollicitations)	561
9.5	Contraintes liées au calcul des caractéristiques du système	561
9.5.1	Nombre de nœuds	561
9.5.2	PFH de réseau	561
9.5.3	Taux d'erreurs sur les bits (BER)	564
9.6	Maintenance	565
9.7	Manuel de sécurité	565
10	Évaluation	565
Annexe A (informative) Informations supplémentaires pour les profils de communication de sécurité fonctionnelle de la CPF 2		566
A.1	Exemple de code de fonction de hachage	566
A.2		580
Annexe B (informative) Information pour l'évaluation des profils de communication de sécurité fonctionnelle de la CPF 2		581
Bibliographie		582
Figure 1 – Relation entre l'IEC 61784–3 et d'autres normes (machines)		287
Figure 2 – Relations entre l'IEC 61784–3 et d'autres normes (transformation)		289
Figure 3 – Relation des objets de validation de sécurité		302
Figure 4 – Couches de communication		305
Figure 5 – ForwardOpen avec segment de réseau de sécurité		311
Figure 6 – Format cible de réseau de sécurité		313
Figure 7 – Service SafetyOpen de traitement de cible sans données de configuration (SafetyOpen de forme 2)		318
Figure 8 – Service SafetyOpen de traitement de cible avec données de configuration (SafetyOpen de forme 1)		320
Figure 9 – Logique du point d'origine permettant de déterminer le format à utiliser		322
Figure 10 – Application de configuration d'appareil		350
Figure 11 – Organigrammes de traitement de Configuration et Validation		352
Figure 12 – Traitement UNID pendant l'état "Waiting for TUNID"		358
Figure 13 – Diagramme d'états du Programme de contrôle de sécurité		359
Figure 14 – Relations entre configuration, essais et verrouillage		364
Figure 15 – Types de connexion de sécurité		372
Figure 16 – Diagramme de transitions d'état de l'Objet de validation de sécurité		377
Figure 17 – Logique pour le type de format «Autodétection»		393
Figure 18 – Diagramme d'états de l'objet Configuration de connexion		396
Figure 19 – Flux de données de l'objet Configuration de connexion		397
Figure 20 – Format de l'octet Mode		399
Figure 21 – Section de données à 1 ou 2 octets, format de base		399
Figure 22 – Section de données à 1 ou 2 octets, format Etendu		400

Figure 23 – Format de section de données de 3 à 250 octets, format de base	401
Figure 24 – Format de section de données de 3 à 250 octets, format Etendu	401
Figure 25 – Format de section de datation, Format de base	402
Figure 26 – Codage du message de coordination temporelle BF	403
Figure 27 – Codage du message de coordination temporelle EF	403
Figure 28 – Codage du message de correction de temps BF	405
Figure 29 – Codage du message de correction de temps EF	405
Figure 30 – Codage PDU point à point à 1 ou 2 octets	406
Figure 31 – Codage PDU multipoints à 1 ou 2 octets	407
Figure 32 – Format de connexion de sécurité de format 2 multipoints à 1 ou 2 octets	408
Figure 33 – Codage PDU point à point de 3 à 250 octets	409
Figure 34 – Codage PDU multipoints de 3 à 248 octets	409
Figure 35 – Format de connexion de sécurité multipoints de 3 à 248 octets	410
Figure 36 – Ordre de calcul du CRC pour les messages de format étendu	411
Figure 37 – Séquence de datation	414
Figure 38 – Diagramme d'une séquence de sécurité producteur/consommateur normale	415
Figure 39 – Diagramme d'une séquence de sécurité producteur/ consommateur normale (production répétée)	416
Figure 40 – Diagramme séquentiel d'un message producteur vers consommateur corrompu	417
Figure 41 – Diagramme séquentiel d'un message producteur vers consommateur perdu	418
Figure 42 – Diagramme séquentiel d'un message retardé	419
Figure 43 – Diagramme séquentiel d'un message producteur vers consommateur corrompu avec production répétée	420
Figure 44 – Diagramme séquentiel d'une terminaison de connexion occasionnée par des retards	421
Figure 45 – Diagramme séquentiel d'un contrôle CRC de sécurité non satisfait	422
Figure 46 – Diagramme séquentiel d'une demande Ping point à point – réponse normale	423
Figure 47 – Diagramme séquentiel d'une demande Ping multipoints satisfaisante, sécurité CP 2/3	425
Figure 48 – Diagramme séquentiel d'une demande Ping multipoints satisfaisante, sécurité CP 2/2	426
Figure 49 – Diagramme séquentiel d'une retransmission de demande Ping multipoints	427
Figure 50 – Diagramme séquentiel d'une temporisation de demande Ping multipoints	427
Figure 51 – Diagramme de relations des entités de modèle de référence d'un appareil de sécurité	429
Figure 52 – Deux appareils échangeant des données de sécurité via un SafetyValidatorClient et un SafetyValidatorServer	430
Figure 53 – Consommateur d'origine et producteur cible point à point	433
Figure 54 – Producteur d'origine et consommateur cible point à point	434
Figure 55 – Consommateur d'origine et producteur cible multipoints	436
Figure 56 – Flux de données de production de sécurité	437
Figure 57 – Contrôle des données de sécurité de consommation	447

Figure 58 – SafetyValidatorServer – déclenché par l'application	448
Figure 59 – Propriété cible	483
Figure 60 – Formes de SafetyOpen	484
Figure 61 – Diagramme d'états de la propriété de connexion	485
Figure 62 – Mapping de l'UNID de service SafetyOpen	486
Figure 63 – Couche application CPF 2 commune	486
Figure 64 – Exemple d'acheminement de bout en bout	487
Figure 65 – Sources des paramètres de connexion relative à la sécurité	491
Figure 66 – Mapping des paramètres entre le point d'origine et la cible	492
Figure 67 – Établissement d'une connexion de sécurité CP 2/3 dans les cibles pour un service SafetyOpen de forme 2a	494
Figure 68 – Séquence générale de détection de la nécessité d'une configuration	495
Figure 69 – Échanges PID/CID pour deux scénarios de point d'origine	501
Figure 70 – Génération des valeurs de départ pour les connexions multipoints	502
Figure 71 – Traitement d'exécution PID/CID	504
Figure 72 – Catégories de connexion et services pris en charge	506
Figure 73 – Types de connexion recommandés	507
Figure 74 – Services pris en charge logique à logique	508
Figure 75 – Types de connexion recommandés pour les services logique à logique	509
Figure 76 – Transferts de données de configuration	510
Figure 77 – Mesures de protection des appareils de sécurité	512
Figure 78 – Relations entre configuration, essais et verrouillage	515
Figure 79 – Données de configuration du point d'origine	517
Figure 80 – Processus de téléchargement aval du SNCT à l'appareil	520
Figure 81 – Téléchargements aval du SNCT vers les points d'origine qui réalisent la configuration de forme 1	522
Figure 82 – Protection contre le verrouillage et propriété	524
Figure 83 – Exemple de relecture et de comparaison du point d'origine et de l'exemplaire	525
Figure 84 – Affichage divers sans relecture complète des données	526
Figure 85 – Processus de vérification comprenant toutes les méthodes alternatives	528
Figure 86 – FSCP 2/1 de référence des appareils CP 16/3	543
Figure 87 – Interaction entre Couche d'adaptation FSCP 2/1 et SMP	546
Figure 88 – Couche d'adaptation FSCP 2/1	547
Figure 89 – Modèle d'appareil CP 16/3	548
Figure 90 – Ajout d'un module normalisé à un appareil modulaire	550
Figure 91 – Logique de traitement du NodeID des appareils de sécurité	556
Figure 92 – Temps de réponse de la fonction de sécurité	557
Figure 93 – Composantes du temps de réponse de la fonction de sécurité	560
Figure 94 – Schéma de principe de fiabilité de protocole de réseau (RBD)	561
Figure 95 – Synthèse de la PFH de réseau	563
Figure 96 – Synthèse de la PFH de format étendu	564
Tableau 1 – Erreurs de communication et matrice de mesures de détection	304

Tableau 2 – Nouveaux attributs de classe	307
Tableau 3 – Extensions de service	308
Tableau 4 – Format de réponse SafetyOpen et SafetyClose	308
Tableau 5 – Identifiant de segment de réseau de sécurité.....	311
Tableau 6 – Définition du segment de réseau de sécurité	312
Tableau 7 – Format de routage de segment de réseau de sécurité.....	314
Tableau 8 – Format étendu de segment de réseau de sécurité.....	314
Tableau 9 – Règles d'évaluation des paramètres de production multipoints.....	322
Tableau 10 – Options de paramétrage du service ForwardOpen pour les connexions de sécurité	325
Tableau 11 – Paramètres de connexion de réseau pour les connexions de sécurité	326
Tableau 12 – Réponse d'application de cible de sécurité CP 2/3 (taille: 10 octets)	326
Tableau 13 – Réponse d'application de cible de sécurité CP 2/3 EF (taille: 14 octets)	327
Tableau 14 – Réponse d'application de cible SafetyOpen (taille: 18 octets).....	327
Tableau 15 – Réponse d'application de cible SafetyOpen EF (taille: 22 octets)	328
Tableau 16 – Nouveaux codes d'erreurs étendus de sécurité.....	328
Tableau 17 – Tableau de lignes directrices concernant les événements d'erreur SafetyOpen	329
Tableau 18 – Modifications apportées aux services communs de l'objet Identité.....	331
Tableau 19 – Extensions de l'objet Identité pour les appareils CP 16/3	331
Tableau 20 – Nouvel attribut instance de l'objet DeviceNet	332
Tableau 21 – Nouvel attribut instance de l'objet Interface TCP/IP	332
Tableau 22 – Attributs de classe de l'objet Liaison SERCOS III.....	333
Tableau 23 – Attributs instance de l'objet Liaison SERCOS III	333
Tableau 24 – Services communs de l'objet Liaison SERCOS III	334
Tableau 25 – Attributs de classe de programme de contrôle de sécurité.....	335
Tableau 26 – Attributs instance de programme de contrôle de sécurité	335
Tableau 27 – Valeurs d'indication de l'attribut État de l'appareil	340
Tableau 28 – Format de l'attribut État d'exception	340
Tableau 29 – Valeurs communes de l'attribut Détail d'exception	341
Tableau 30 – Synthèse du format de détail d'exception.....	342
Tableau 31 – Synthèse du comportement des appareils pour diverses valeurs CFUNID	344
Tableau 32 – Services communs du programme de contrôle de sécurité	346
Tableau 33 – Services spécifiques de l'objet Programme de contrôle de sécurité	346
Tableau 34 – Structure de message Configure_Request.....	348
Tableau 35 – Structure de message Validate_Configuration	349
Tableau 36 – Structure de message de réussite Validate_Configuration.....	349
Tableau 37 – Code d'erreur Validate_Configuration	349
Tableau 38 – Codes étendus Validate_Configuration	350
Tableau 39 – Structure de message Set_Password	352
Tableau 40 – Structure de message Reset_Password.....	353
Tableau 41 – Configuration_Lock/Unlock message structure.....	353
Tableau 42 – Structure de message Mode_Change	354
Tableau 43 – Structure de message Safety_Reset.....	354

Tableau 44 – Types de réinitialisation de sécurité du Programme de contrôle de sécurité	354
Tableau 45 – Paramètre d'attribut Mode point	355
Tableau 46 – Règles de traitement applicables aux types de réinitialisation	355
Tableau 47 – Service Propose_TUNID	356
Tableau 48 – Service Apply_TUNID	356
Tableau 49 – Événements liés au Programme de contrôle de sécurité	359
Tableau 50 – Matrice d'événements d'état du Programme de contrôle de sécurité.....	360
Tableau 51 – Contrôle du propriétaire de configuration par rapport à l'état de l'appareil	364
Tableau 52 – Mapping des états du Programme de contrôle de sécurité et de l'objet Identité	364
Tableau 53 – Mapping des événements de l'objet Programme de contrôle de sécurité	365
Tableau 54 – Mapping des événements d'objet Identité	365
Tableau 55 – Attributs de classe de l'Objet de validation de sécurité.....	366
Tableau 56 – Attributs instance de l'Objet de validation de sécurité	367
Tableau 57 – Attributions d'états de l'Objet de validation de sécurité	369
Tableau 58 – Type d'Objet de validation de sécurité, attributions de champs de bits	370
Tableau 59 – Règles d'évaluation du paramètre SafetyOpen des producteurs multipoints.....	372
Tableau 60 – Services de classes de l'Objet de validation de sécurité.....	374
Tableau 61 – Services instance de l'Objet de validation de sécurité	374
Tableau 62 – Données du service Get_Attributes_All de l'objet de Validation de sécurité	375
Tableau 63 – Matrice d'événements d'état de l'Objet de validation de sécurité	378
Tableau 64 – Mapping des états des objets Programme de contrôle de sécurité et Validation de sécurité	378
Tableau 65 – Extensions d'attributs de classe d'objet de configuration de connexion.....	379
Tableau 66 – Ajouts/extensions d'attributs instance d'Objet de configuration de connexion.....	379
Tableau 67 – Définitions des bits de drapeaux de connexion	383
Tableau 68 – Paramètres de connexion O-à-T	384
Tableau 69 – Paramètres de connexion T-à-O.....	385
Tableau 70 – Formats de mise en correspondance des données.....	386
Tableau 71 – Format 0 de mise en correspondance des données	387
Tableau 72 – Format 1 de mise en correspondance des données	387
Tableau 73 – Valeurs SCCRC de l'appareil cible	390
Tableau 74 – Valeurs SCTS de l'appareil cible	390
Tableau 75 – Paramètres de connexion de correction de temps pour une connexion multipoints.....	390
Tableau 76 – Signification de l'attribut Type de format.....	391
Tableau 77 – Signification de l'attribut État du format	393
Tableau 78 – Services spécifiques à l'objet Configuration de connexion.....	394
Tableau 79 – Données du service de réponse Get_Attributes_All (attributs ajoutés)	394
Tableau 80 – Données du service de réponse Get_Attributes_All (paramètres ajoutés)	395
Tableau 81 – Données du service de Demande Set_Attributes_All (attributs ajoutés)	395

Tableau 82 – Données du service Réponse Set_Attributes_All (paramètres ajoutés)	395
Tableau 83 – Mapping des états des objets Programme de contrôle de sécurité et CCO	396
Tableau 84 – Sections de connexion et formats PDU	398
Tableau 85 – Variables de l'octet Mode	399
Tableau 86 – Variables de datation	402
Tableau 87 – Variables du message de coordination temporelle	403
Tableau 88 – Variables du message de correction de temps	405
Tableau 89 – Polynômes de CRC utilisés	412
Tableau 90 – Sections de connexion et formats de messages	412
Tableau 91 – Réception des données – Déclenchée par la liaison	449
Tableau 92 – Réception Time_Correction – Déclenchée par la liaison	449
Tableau 93 – Réception des données – Déclenchée par l'application	450
Tableau 94 – Réception de Time_Correction – Déclenchée par l'application	450
Tableau 95 – Application de consommation – Contrôle des données de sécurité	450
Tableau 96 – Détermination de l'état de la connexion du producteur	462
Tableau 97 – État de la connexion de sécurité de consommation	474
Tableau 98 – Erreurs d'établissement de connexion et mesures de détection des erreurs	479
Tableau 99 – Attributions de Date/Heure SNN	480
Tableau 100 – Plage légale SNN des valeurs temporelles	480
Tableau 101 – Paramètres de connexion de sécurité	489
Tableau 102 – Récapitulatif SafetyOpen	493
Tableau 103 – Mapping des services point d'origine/cible	505
Tableau 104 – Types de service point d'origine/cible non pris en charge	506
Tableau 105 – Objectifs de configuration	509
Tableau 106 – Contrôle du propriétaire de configuration par rapport à l'état de l'appareil	516
Tableau 107 – Erreurs et mesures de détection	528
Tableau 108 – Mots clés des sections de classe d'objet	533
Tableau 109- Format d'entrée de Classex de sécurité	534
Tableau 110 – Mots clés de classes de paramètres	534
Tableau 111 – Nouveaux mots clés de la section Gestionnaire de connexion à des fins de sécurité	535
Tableau 112 – Utilisation du champ Gestionnaire de connexion à des fins de sécurité	536
Tableau 113 – Paramétrages du champ de paramètres de connexion à des fins de sécurité	537
Tableau 114 – Règles d'attribution d'ID CP 2/3	539
Tableau 115 – Indications LED pour le paramétrage de l'UNID	551
Tableau 116 – LED État du module	552
Tableau 117 – États de la LED État de réseau	553
Tableau 118 – Type de temps de réaction de connexion – applications de production/consommation	559

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 Électrotechnique 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.

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 et de ne pas avoir signalé leur existence.

La Norme internationale 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.

Cette troisième édition annule et remplace la deuxième édition parue en 2010. Cette édition constitue une révision technique. Les modifications majeures par rapport à l'édition précédente sont énumérées ci-dessous (et surlignées en jaune dans le présent document).

- Ajout d'exigences détaillées pour l'utilisation de FSCP 2/1 en liaison avec CP 16/3 (voir 4.1, 6.4.3, 6.5.3, 8.2, 8.13, et diverses références lors du référencement des réseaux CPF 2);

- Définition des mots-clés de la section de classe d'objet pour la sécurité donnée dans la définition du fichier EDS en 8.10.2.1;
- De nouvelles sections sur la présentation générale du CRC de sécurité en 7.1.2.1 et les comptages de remplacement pour le format EF en 7.4;
- Corrections apportées aux calculs de la PFH en 9.5.2;
- Changement de MACID en NodeID à titre de référence générale à l'identifiant de réseau;
- Diverses corrections mineures apportées depuis la dernière publication.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
65C/851/FDIS	65C/854/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à l'approbation de cette norme.

Cette publication a été rédigée selon les Directives ISO/IEC, Partie 2.

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 de cette publication ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous "<http://webstore.iec.ch>" dans les données relatives à la publication recherchée. À cette date, la publication sera

- reconduite,
- supprimée,
- remplacée par une édition révisée, ou
- amendée.

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.

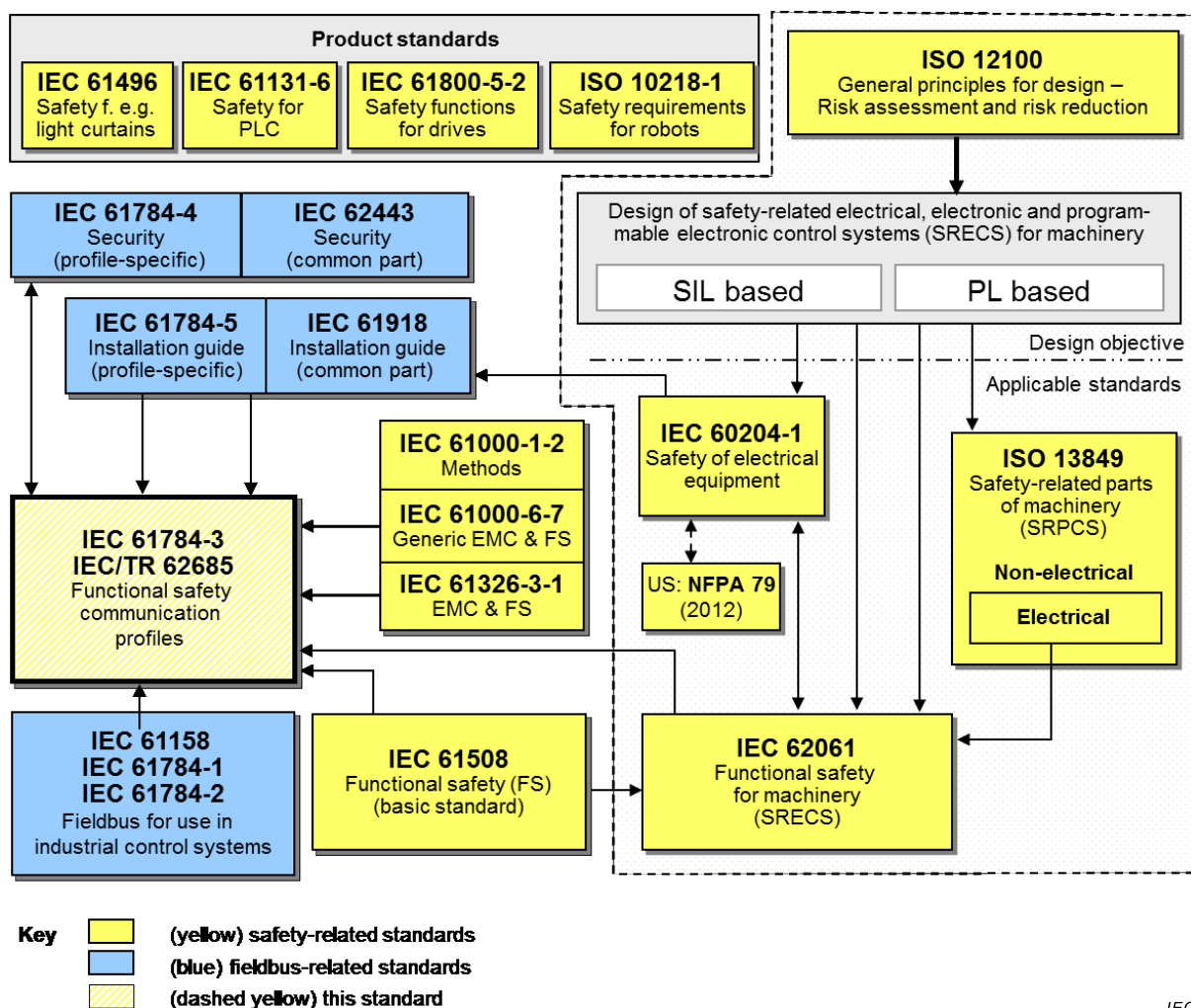
0 Introduction

0.1 Généralités

La norme IEC 61158 relative aux bus de terrain, ainsi que ses normes associées IEC 61784-1 et IEC 61784-2, définit un ensemble de protocoles de communication qui assurent la commande répartie d'applications automatisées. La technologie de bus terrain est désormais reconnue et bien éprouvée. Ainsi, les améliorations des bus de terrain continuent à se développer, traitant des applications pour des domaines tels que les applications en temps réel relatives à la sécurité et à la sûreté.

La présente norme définit les principes pertinents applicables aux communications en termes de sécurité fonctionnelle en référence à la série IEC 61508, et spécifie plusieurs couches de communication de sécurité (profils et protocoles correspondants) basées sur les profils de communication et les couches de protocoles de l'IEC 61784-1, l'IEC 61784-2 et la série IEC 61158. Elle ne couvre pas les aspects relatifs à la sécurité électrique et à la sécurité intrinsèque.

La Figure 1 représente les relations entre la présente norme et les normes pertinentes relatives à la sécurité et au bus de terrain dans un environnement machines.



IEC

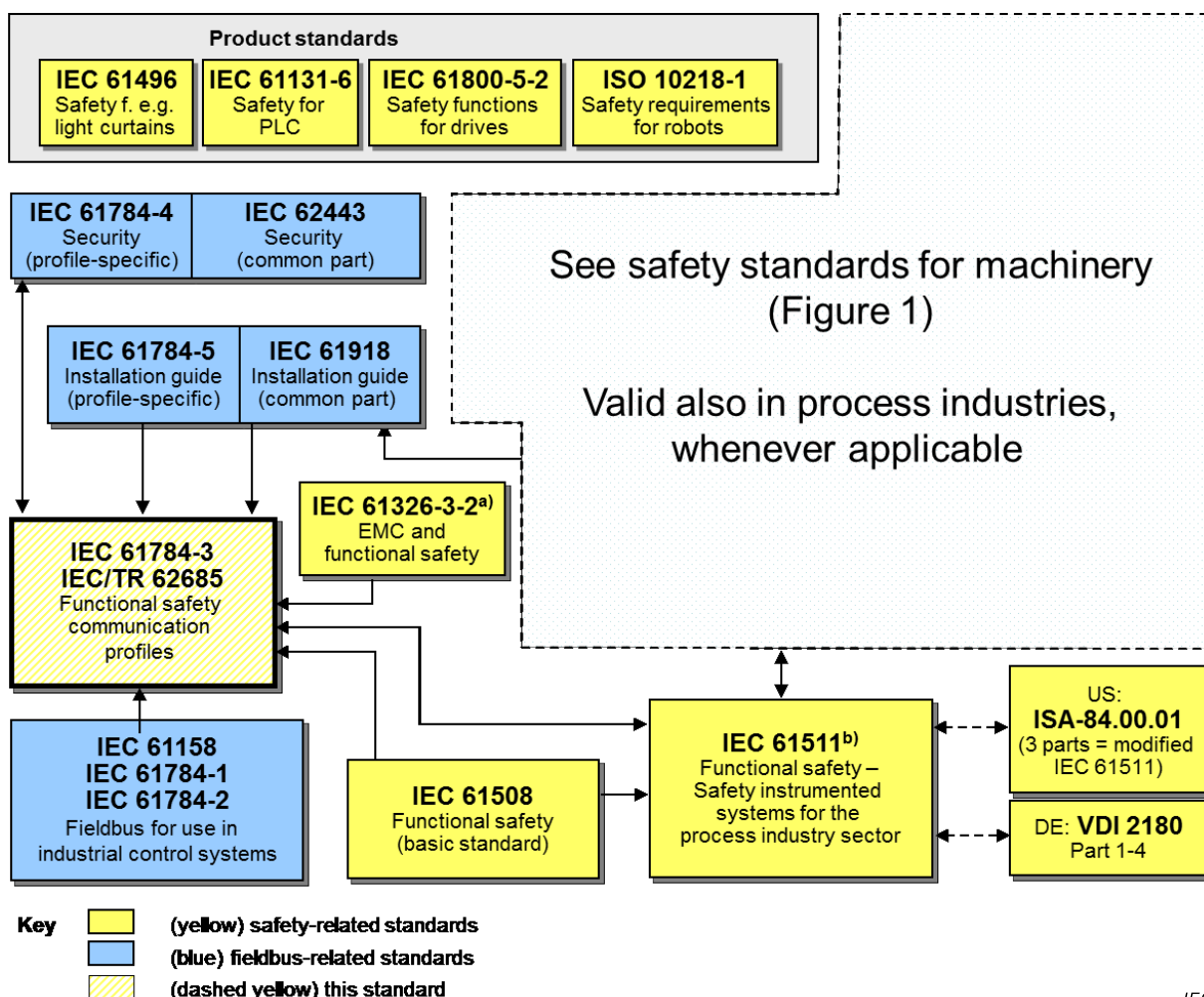
Anglais	Français
Product standards	Normes de produits
Safety function, e.g. light curtains	Fonction de sécurité, par exemple rideaux de lumière

Anglais	Français
Safety for PLC	Sécurité relative aux automates programmables
Safety functions for drives	Fonctions de sécurité applicables aux entraînements
Safety requirements for robots	Exigences de sécurité applicables aux robots
General principles for design – Risk assessment and risk reduction	Principes généraux de conception – Appréciation du risque et réduction du risque
Security (profile-specific)	Sûreté (spécifique au profil)
Security (common part)	Sûreté (partie commune)
Design of safety-related electrical, electronic and programmable electronic control systems (SRECS) for machinery	Conception des systèmes de commande électriques, électroniques et électroniques programmables relatifs à la sécurité pour les machines
SIL based	Basé sur SIL
PL based	Basé sur PL
Installation guide (profile-specific)	Guide d'installation (spécifique au profil)
Installation guide (common part)	Guide d'installation (partie commune)
Design objective	Objectif de conception
Applicable standards	Normes applicables
Methods	Méthodes
Generic EMC & FS	CEM & FS génériques
EMC & FS	CEM & FS
Safety of electrical equipment	Sécurité des équipements électriques
Safety-related parts of machinery (SRPCS)	Sécurité des machines – Parties des systèmes de commande relatives à la sécurité (SRPCS)
Non-electrical	Non électrique
Electrical	Électrique
Functional safety communication profiles	Profils de communication de sécurité fonctionnelle
Fieldbus for use in industrial control systems	Bus de terrain pour utilisation dans des systèmes de commande industriels
Functional safety (FS) (basic standard)	Sécurité fonctionnelle (FS) (norme de base)
Functional safety for machinery (SRECS)	Sécurité fonctionnelle des machines (SRECS)
Key	Légende
(yellow) safety-related standards	(jaune) normes relatives à la sécurité
(blue) fieldbus-related standards	(bleu) normes relatives au bus de terrain
(dashed yellow) this standard	(jaune pointillé) la présente norme

NOTE Les paragraphes 6.7.6.4 (haute complexité) et 6.7.8.1.6 (faible complexité) de l'IEC 62061 spécifient la relation entre PL (catégorie) et SIL.

Figure 1 – Relation entre l'IEC 61784–3 et d'autres normes (machines)

La Figure 2 représente les relations entre la présente norme et les normes pertinentes relatives à la sécurité et au bus de terrain dans un environnement de transformation.



IEC

Anglais	Français
Product standards	Normes de produits
Safety function, e.g. light curtains	Fonction de sécurité, par exemple rideaux de lumière
Safety for PLC	Sécurité relative aux automates programmables
Safety functions for drives	Fonctions de sécurité applicables aux entraînements
Safety requirements for robots	Exigences de sécurité applicables aux robots
Security (profile-specific)	Sûreté (spécifique au profil)
Security (common part)	Sûreté (partie commune)
Installation guide (profile-specific)	Guide d'installation (spécifique au profil)
Installation guide (common part)	Guide d'installation (partie commune)
See safety standards for machinery (Figure 1)	Voir normes de sécurité pour les machines (Figure 1)
Valid also in process industries, whenever applicable	Valable également dans les industries de transformation, le cas échéant
Functional safety communication profiles	Profils de communication de sécurité fonctionnelle
EMC and functional safety	CEM et sécurité fonctionnelle
Fieldbus for use in industrial control systems	Bus de terrain pour utilisation dans des systèmes de commande industriels
Functional safety (basic standard)	Sécurité fonctionnelle (norme de base)
Functional safety–safety instrumented systems for the process industry sector	Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur des industries de transformation
3 parts = modified IEC 61511	3 parties = IEC 61511 modifiée

Anglais	Français
Part 1 –4	Parties 1 à 4
Key	Légende
(yellow) safety-related standards	(jaune) normes relatives à la sécurité
(blue) fieldbus-related standards	(bleu) normes relatives au bus de terrain
(dashed yellow) this standard	(jaune pointillé) la présente norme

^a Pour des environnements électromagnétiques spécifiés, sinon IEC 61326-3-1 ou IEC 61000-6-7

^b EN ratifiée.

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 la série IEC 61508, assurent la confiance nécessaire à accorder à la transmission de messages (information) entre deux participants ou plus 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 la présente norme permettent de garantir cette assurance en utilisant un bus de terrain dans des applications nécessitant 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.

La présente norme décrit:

- les principes de base de mise en œuvre des exigences de la série IEC 61508 pour les communications de données relatives à la sécurité, y compris les défauts de transmission potentiels, les mesures correctives et les considérations concernant l'intégrité des données;
- les profils de communication de sécurité fonctionnelle pour plusieurs familles de profils de communication dans les IEC 61784-1 et IEC 61784-2, y compris les extensions de la couche de sécurité aux sections relatives au service et aux protocoles de communication de la série IEC 61158.

0.2 Déclaration de droits de propriété

La commission électrotechnique internationale (IEC) attire l'attention sur le fait qu'il est déclaré que la conformité aux dispositions du présent document peut impliquer l'utilisation de brevets intéressant les profils de communication de sécurité fonctionnelle pour la famille 2, où la notation [xx] désigne le détenteur des droits de propriété.

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

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, gratuitement ou à des termes et conditions raisonnables et non discriminatoires. À ce propos, la déclaration du détenteur des droits de propriété est enregistrée à l'IEC.

Des informations peuvent être demandées à:

[RA] Rockwell Automation, Inc.
 1201 S. Second Street
 Milwaukee, WI 53204
 USA
 Contact: Département de la propriété intellectuelle.

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 intellectuelle autres que ceux identifiés ci-dessus. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et de ne pas avoir signalé leur existence.

L'ISO (www.iso.org/patents) et l'IEC (<http://patents.iec.ch>) maintiennent à disposition des bases de données en ligne des brevets relatifs à leurs normes. Les utilisateurs sont invités à les consulter pour obtenir les dernières informations relatives à ces brevets.

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 la série IEC 61784-3 spécifie une couche de communication relative à la sécurité (services et protocole) fondée sur la CPF 2 de l'IEC 61784-1, l'IEC 61784-2 et le Type 2 de l'IEC 61158. Elle identifie les principes applicables aux communications de sécurité fonctionnelle définies dans l'IEC 61784-3, et appropriés 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.

La présente partie¹ 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 61508² concernant la sécurité fonctionnelle. Ces mécanismes peuvent être utilisés dans diverses applications industrielles, telles que la commande de processus, l'usinage automatique et les machines.

La présente partie fournit des lignes directrices tant pour les développeurs que pour les évaluateurs d'appareils et 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 du profil de communication de sécurité fonctionnelle, conforme à la présente partie, dans un appareil normal ne suffit pas à le qualifier d'appareil de sécurité.

2 Références normatives

Les documents suivants sont cités en référence de manière normative, en intégralité ou en partie, dans le présent document et sont indispensables pour son application. 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, *Automates programmables – Partie 2: Exigences et essais des équipements*

IEC 61131-3, *Automates programmables – Partie 3: Langages de programmation*

IEC 61158-2, *Réseaux de communication 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 – Éléments de type 2*

¹ Dans les pages suivantes de la présente norme, "la présente partie" se substitue à "cette partie de la série IEC 61784-3".

² Dans les pages suivantes de la présente norme, "IEC 61508" se substitue à "série IEC 61508".

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 – Éléments de type 19*

IEC 61158-4-2, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 4-2: Spécification du protocole de la couche liaison de données – Éléments 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 liaison de données – Éléments 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 – Éléments 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 – Éléments de type 19*

IEC 61158-6-2, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 6-2: Spécification du protocole de la couche application – Éléments de type 2*

IEC 61158-6-19, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 6-19: Spécification du protocole de la couche application – Éléments 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 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 basés sur l'ISO/CEI 8802-3*

IEC 61784-3: —³, *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 les locaux industriels*

ISO 13849-1:2006, *Sécurité des machines – Parties des systèmes de commande relatives à la sécurité – Partie 1: Principes généraux de conception*

³ A publier.

ISO 15745-2:2003, *Systèmes d'automatisation industrielle et intégration – Cadres d'intégration d'application pour les systèmes ouverts – Partie 2: Description de référence pour les systèmes de contrôle fondés sur l'ISO 11898* (disponible en anglais seulement)

ISO 15745-3:2003, *Systèmes d'automatisation industrielle et intégration – Cadres d'intégration d'application pour systèmes ouverts – Partie 3: Description de référence pour les systèmes de contrôle fondés sur la CEI 61158* (disponible en anglais seulement)

ISO 15745-4:2003, *Systèmes d'automatisation industrielle et intégration – Cadres d'intégration d'application pour les systèmes ouverts – Partie 4: Description de référence pour les systèmes de contrôle fondés sur Ethernet* (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 suivants s'appliquent.

NOTE Les définitions des termes eux-mêmes définis au 3.1 sont marquées en italique.

3.1.1 Termes et définitions communs

NOTE Ces termes et définitions communs proviennent de l'IEC 61784-3:—.

3.1.1.1

disponibilité

probabilité, pour un système automatisé, qu'il ne se produise pas de conditions opérationnelles non satisfaisantes, telles que la perte de production, pendant une période donnée

3.1.1.2

probabilité d'erreurs sur les éléments binaires

P_e

probabilité de réception d'un bit donné avec la valeur incorrecte

3.1.1.3

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.

3.1.1.4

pont

appareil abstrait qui relie des segments de réseau multiples le long de la couche de liaison de données

3.1.1.5

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"]

3.1.1.6

canal de communication

connexion logique entre deux points limites d'un *système de communication*

3.1.1.7**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

3.1.1.8**connexion**

liaison logique entre deux objets d'application d'appareils identiques ou différents

3.1.1.9**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», et les étiquettes telles que CRC1, CRC2, peuvent également être utilisés dans la présente norme pour se référer aux données redondantes.

Note 2 à l'article: Voir également [32], [33]⁴.

3.1.1.10**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 tolérable conformément au modèle de cycle de vie de l'IEC 62443, en utilisant par exemple des zones et des conduits

3.1.1.11**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]

3.1.1.12**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]

3.1.1.13**anomalie**

condition anormale qui peut entraîner une réduction de capacité ou la perte de capacité d'une unité fonctionnelle à accomplir une fonction requise

⁴ Les chiffres entre crochets se réfèrent à la bibliographie.

Note 1 à l'article: L'IEC 60050-191:1990, 191-05-01, définit le terme "fault" (en français "panne") comme un état d'incapacité à accomplir une fonction requise, en excluant l'incapacité 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]

3.1.1.14

bus de terrain

système de communication basé sur le transfert de données en série et utilisé dans des applications d'automatisation industrielle ou de commande de processus

3.1.1.15

DLPDU

DÉCONSEILLÉ: trame

Data Link Protocol Data Unit (Unité de données de protocole de liaison de données)

3.1.1.16

fonction de hachage

fonction (mathématique) de mise en correspondance 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 courantes incluent la parité, la somme de contrôle ou le CRC.

[SOURCE: IEC TR 62210:2003, 4.1.12, modifié – ajout de " habituellement " et de notes]

3.1.1.17

danger

état ou ensemble de conditions d'un système qui, avec d'autres conditions associées, entraîne inévitablement un préjudice pour les personnes, les biens ou l'environnement

3.1.1.18

maître

entité de communication active capable d'initier et de programmer des activités de communication effectuées par d'autres stations qui peuvent être des maîtres ou des esclaves

3.1.1.19

message

série ordonnée d'octets destinée à communiquer des informations

[SOURCE: ISO/IEC 2382-16:1996, 16.02.01, modifié – caractère remplacé par octet]

3.1.1.20

déclenchement de nuisance

déclenchement parasite sans effet préjudiciable

Note 1 à l'article: Les erreurs anormales internes peuvent être générées dans des systèmes de communication tels que des systèmes de transmission par ondes radioélectriques, par exemple, du fait d'un trop grand nombre de nouvelles tentatives en présence de perturbations.

3.1.1.21

niveau de performance

PL

niveau discret utilisé pour spécifier la capacité des parties relatives à la sécurité des systèmes de commande à accomplir 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 13849-1:2006, 3.1.23]

3.1.1.22

redondance

existence de plusieurs moyens pour accomplir une fonction exigée ou pour représenter des informations

[SOURCE: IEC 61508-4:2010, 3.4.6, modifié – exemple et notes supprimés]

3.1.1.23

fiabilité

probabilité qu'un système automatisé puisse accomplir une fonction exigée, dans des conditions données, pendant un intervalle de temps donné (t_1 , t_2)

Note 1 à l'article: Il est considéré en général que le système automatisé est en état d'accomplir la fonction exigée au début de l'intervalle de temps donné.

Note 2 à l'article: Le terme "fiabilité" est aussi employé pour désigner l'aptitude caractérisée par cette probabilité.

Note 3 à l'article: Au cours de la période MTBF ou MTTF, la probabilité qu'un système automatisé exécute une fonction exigée dans les conditions données décroît.

Note 4 à l'article: La fiabilité est différente de la disponibilité.

[SOURCE: IEC TR 62059-11:2002, 3.17, modifié – utilisation des mots "un système automatisé" à la place de "une entité" et ajout de deux notes]

3.1.1.24

taux d'erreurs résiduelles

taux statistique de défaut de détection d'erreurs par les mesures de sécurité SCL

3.1.1.25

risque

combinaison de la probabilité d'occurrence d'un dommage ou préjudice et de la gravité de ce dernier

Note 1 à l'article: Pour plus d'informations sur ce concept, se reporter à l'Annexe A de l'IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6], [SOURCE: Guide ISO/IEC 51:2014, définition 3.9, modifiée – note différente]

3.1.1.26

canal de communication de sécurité

canal de communication qui débute 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 ou un système de communication défini, ou un canal défini.

3.1.1.27

couche de communication de sécurité

SCL

couche de communication située au-dessus de la FAL qui comprend toutes mesures complémentaires nécessaires permettant d'assurer la transmission de données en toute sécurité conformément aux exigences de l'IEC 61508

3.1.1.28

connexion de sécurité

connexion qui utilise le protocole de sécurité pour des transactions de communications

3.1.1.29

données de sécurité

données transmises par un réseau de sécurité utilisant un protocole de sécurité

Note 1 à l'article: La *couche de communication de sécurité* ne garantit pas la sécurité des données proprement dites, mais uniquement la transmission en toute sécurité de ces dernières.

3.1.1.30

appareil de sécurité

appareil conçu conformément à l'IEC 61508 et qui met en œuvre le profil de communication de sécurité fonctionnelle

3.1.1.31

fonction de sécurité

fonction qu'un système E/E/PE relatif à la sécurité ou d'autres mesures de réduction du risque doivent mettre en œuvre, et qui est destinée à atteindre ou à maintenir un état de sécurité de l'équipement commandé, compte tenu d'un événement dangereux spécifique

[SOURCE: IEC 61508-4:2010, 3.5.1, modifiée – références et exemple supprimés]

3.1.1.32

temps de réponse de la fonction de sécurité

temps écoulé dans le cas le plus défavorable après l'activation d'un capteur de sécurité relié à un bus de terrain, avant que ne soit atteint l'état de sécurité correspondant de son (ses) actionneur(s) 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:—, 5.2.4, est traité par les profils de communication de sécurité fonctionnelle définis dans la présente partie.

3.1.1.33

niveau d'intégrité de sécurité

SIL

niveau discret (un sur quatre niveaux possibles), correspondant à une plage de valeurs d'intégrité de sécurité, où le niveau d'intégrité de sécurité 4 est le niveau le plus élevé et le niveau d'intégrité de sécurité 1 est le niveau le plus faible

Note 1 à l'article: Les mesures de défaillance cible (voir l'IEC 61508-4:2010, 3.5.17) applicables aux quatre niveaux d'intégrité de sécurité sont spécifiées 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 d'intégrité de sécurité des fonctions équivalentes à attribuer aux systèmes E/E/PE relatifs à la sécurité.

Note 3 à l'article: Le niveau d'intégrité de sécurité (SIL) n'est pas une propriété d'un système, sous-système, élément ou composant. L'interprétation correcte de l'expression «système relatif à la sécurité avec SILn» (où n est égal à 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]

3.1.1.34

mesure de sécurité

mesure permettant 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 détaillées dans l'IEC 61784-3:—, 5.3 et 5.4.

3.1.1.35

PDU de sécurité

SPDU

PDU transféré via le canal de communication de sécurité

Note 1 à l'article: Le SPDU peut comporter deux exemplaires ou plus des données de sécurité utilisant des structures de codage et des fonctions de hachage différentes, associées à des parties explicites de protections supplémentaires telles qu'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 à l'article: L'abréviation «SPDU» est dérivée du terme anglais développé correspondant "safety PDU".

3.1.1.36

application relative à la sécurité

programmes conçus conformément à l'IEC 61508 pour satisfaire aux exigences SIL de l'application

3.1.1.37

système relatif à la sécurité

système qui exécute les *fonctions de sécurité* conformément à l'IEC 61508

3.1.1.38

esclave

entité de communication passive capable de recevoir des messages et de les envoyer en réponse à une autre entité de communication qui peut être maître ou esclave

3.1.1.39

déclenchement parasite

déclenchement provoqué par le système de sécurité sans injonction du processus

3.1.1.40

horodatage

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 sont admises

3.1.2.2

format étendu

utilisé pour les RPI de connexion d'une durée supérieure à 100 ms ou pour des applications dans lesquelles des connexions interrompues sont à éviter

3.1.2.3

demande ping (demande d'acquittement)

demande d'acquittement de la réception d'un message par le consommateur

3.1.2.4

réponse à demande ping

réponse à une demande ping

3.1.2.5

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 convenue entre les appareils d'origine et cibles.

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	Cyclic Redundancy Check (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 (Équipement commandé)	[IEC 61508-4:2010]
E/E/PE	Electrical/Electronic/Programmable Electronic (Électrique/électronique/électronique programmable)	[IEC 61508-4:2010]
FAL	Fieldbus Application Layer (Couche application de bus de terrain)	[IEC 61158-5]
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)	
SCL	Safety Communication Layer (Couche de communication de sécurité)	
SIL	Safety Integrity Level (Niveau d'intégrité de sécurité)	[IEC 61508-4:2010]

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™ 5	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	Device physical address (CP 2/3) (Adresse physique d'appareil (CP 2/3))

⁵ Pour la déclaration des marques, voir l'Article 4.

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-Volatile (Non volatil)
NVS	Non-Volatile Storage (Mémoire non volatile)
OCPUNID	Output Connection Owner UNID (Propriétaire de connexion de sortie UNID)
OSC	Object State Conflict (Conflit d'état d'objet)
O-à-T	Originator to Target (Point d'origine vers Cible)
OUNID	Originator UNID (Point d'origine UNID)
PID	Producer Identifier (Identifiant de producteur)
PS	Power Supply (Alimentation)
Res.	Reserved (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)
SNCT	Safety Network Configuration Tool (Outil de configuration de réseau de sécurité)
SNN	Safety Network Number (Numéro de réseau de sécurité)
T-à-O	Target to Originator (Cible vers Point d'origine)
TBD	To Be Defined (À 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 les IEC 61158-3-2, IEC 61158-4-2, IEC 61158-5-2 et IEC 61158-6-2.

Le cas échéant, la présente partie 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™⁶) définit des profils de communication sur la base du type 2 de l'IEC 61158-2, de 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®⁷) définit un profil de communication CP 16/3 sur la base des normes IEC 61158-3-19, IEC 61158-4-19, IEC 61158-5-19 et 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™⁶) est fondé 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 les spécifications de la couche de communication de sécurité définies dans la présente partie.

4.2 FSCP 2/1

Le FSCP 2/1 est basé sur le modèle producteur/consommateur de CPF 2. L'association des producteurs et des consommateurs constitue un élément important de la relation qui garantit la haute intégrité nécessaire aux applications relatives à la sécurité.

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, tel que représenté à la Figure 3. L'objet de validation de sécurité garantit l'intégrité des transferts de données de sécurité.

⁶ CIP™ (Common Industrial Protocol) et CIP Safety™ désignent les appellations commerciales de l'organisme sans but 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 quelconque de ses produits. La conformité à la présente norme n'exige pas l'emploi des appellations CIP™ ou CIP Safety™. L'emploi des appellations CIP™ ou CIP Safety™ exige l'autorisation de ODVA et la conformité aux conditions d'utilisation (essais et validation).

⁷ SERCOS® est une appellation commerciale de SERCOS International e.V. 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 quelconque de ses produits. La conformité à la présente norme 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).

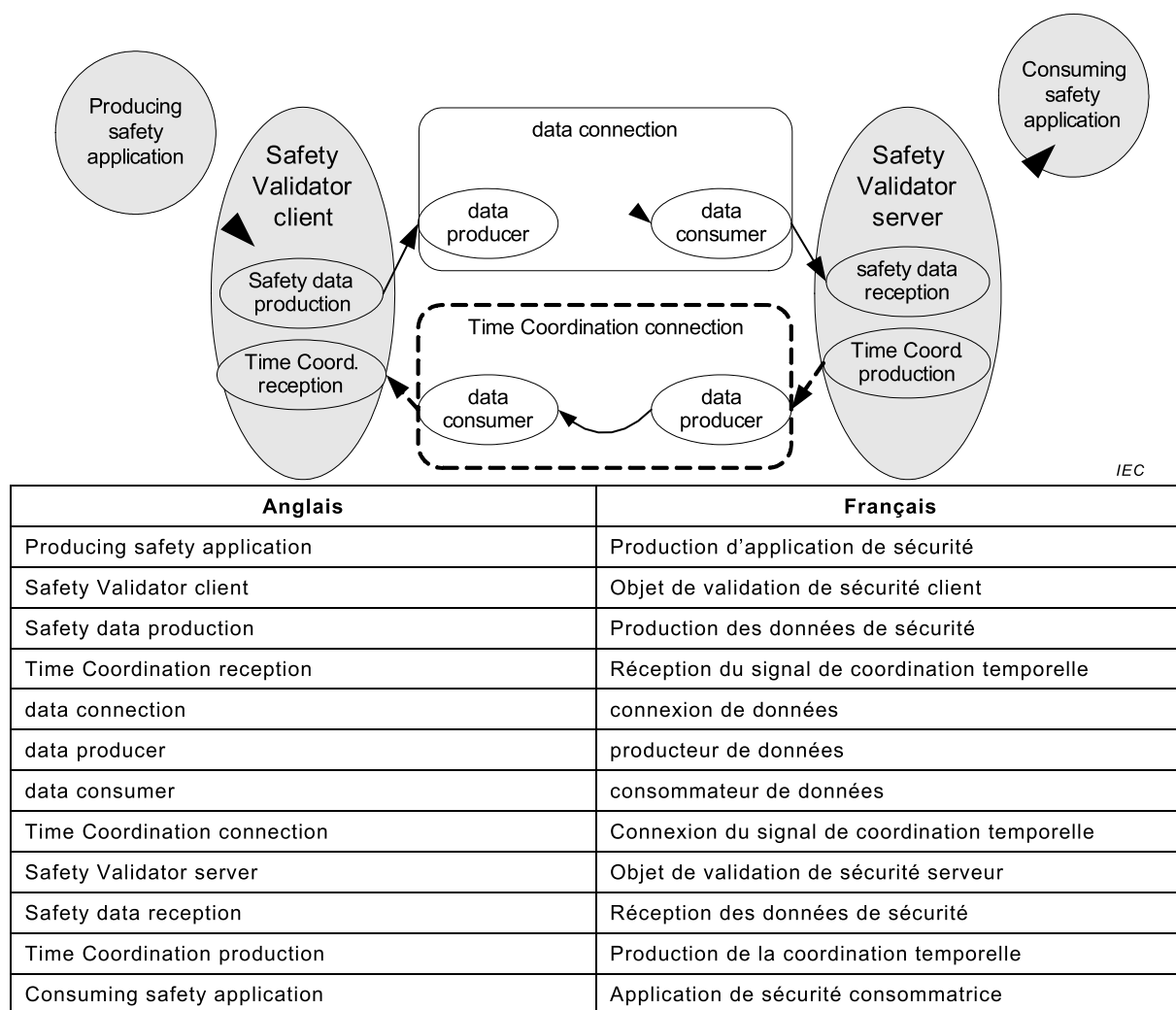


Figure 3 – Relation des objets de validation de sécurité

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.

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. Diverses mesures de production de messages relatifs à la sécurité permettent de s'assurer que les messages CPF 2 standard ne sont pas interprétés comme des messages de sécurité.

5 Généralités

5.1 Documents externes de spécifications applicables au profil

Le document suivant est particulièrement utile pour bien comprendre la conception des protocoles FSCP 2/1:

- GS-ET-26 [30]

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 (SIL 3) (voir IEC 61508), et le PLe/catégorie 4 (voir 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 fondamentales relatives 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 satisfaire à l'IEC 61508.
- Les conditions environnementales doivent être conformes à l'IEC 61131-2 pour les niveaux de base et aux IEC 61326-3-1 et 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 la présente partie, les exigences relatives au 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.

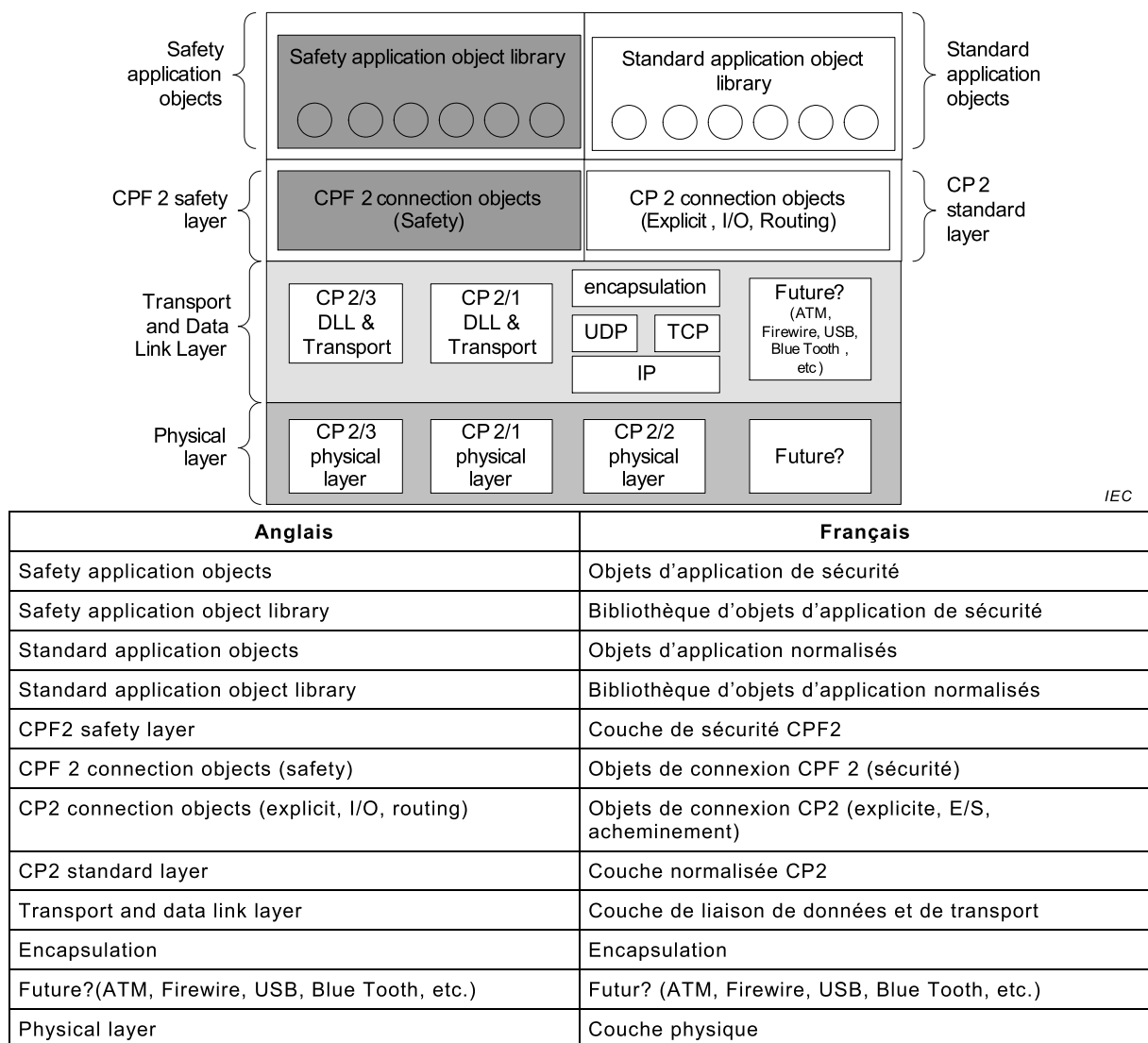
Tableau 1 – Erreurs de communication et matrice de mesures de détection

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.								

5.4 Structure de la couche de communication de sécurité

Le protocole de sécurité est structuré en couches au haut du protocole de réseau standard (la pile de protocoles standard 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 provenant 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. Une fois le message de sécurité 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 doit être utilisée uniquement avec les profils de communication CPF 2 (CP 2/3 (DeviceNet™⁸), CP 2/2 (EtherNet/IP™⁹) et CP 16/3 (SERCOS III™¹⁰)). Il n'existe aucune exigence concernant les profils de communication CPF 2 autres que celles définies dans la présente partie.

5.5.2 Types de données

Les profils définis dans la présente partie 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 Introduction

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 standard sont utilisées pour l'établissement des connexions E/S de sécurité.

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.

⁸ DeviceNet™ désigne l'appellation commerciale de l'organisme sans but 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 quelconque de ses produits. La conformité à la présente norme n'exige pas l'emploi de l'appellation commerciale DeviceNet™. L'emploi de l'appellation commerciale DeviceNet™ exige l'autorisation de ODVA.

⁹ EtherNet/IP™ désigne l'appellation commerciale de 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 quelconque de ses produits. La conformité à la présente norme n'exige pas l'emploi de l'appellation commerciale EtherNet/IP™. L'emploi de l'appellation commerciale EtherNet/IP™ exige l'autorisation de ODVA.

¹⁰ SERCOS® et l'interface SERCOS® désignent les appellations commerciales de SERCOS International e.V. 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 quelconque 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.

Tableau 2 – Nouveaux attributs de classe

ID d'attribut	Mise en œuvre nécessaire	Règles 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	Compteur des connexions de sécurité	STRUCT de:	Compteurs d'états
				Comptage de demandes SafetyOpen abouties	UINT	Comptage de demandes SafetyOpen abouties émises de ce nœud vers une autre cible
				Comptage de demandes SafetyOpen non abouties	UINT	Comptage de demandes SafetyOpen non abouties émises de ce nœud vers une autre cible
				Comptage de demandes SafetyClose abouties	UINT	Comptage de demandes SafetyClose abouties émises de ce nœud vers une autre cible
				Comptage de demandes SafetyClose non abouties ^b	UINT	Comptage de demandes SafetyClose non abouties émises de ce nœud vers une autre cible
				Comptage des indications SafetyOpen abouties	UINT	Comptage de demandes SafetyOpen abouties émises d'un point d'origine externe vers ce nœud
				Comptage des indications SafetyOpen non abouties ^b	UINT	Comptage de demandes SafetyOpen non abouties émises d'un point d'origine externe vers ce nœud
				Comptage des indications SafetyClose abouties	UINT	Comptage de demandes SafetyClose abouties émises d'un point d'origine externe vers ce nœud
				Comptage des indications SafetyClose non abouties ^b	UINT	Comptage de demandes SafetyClose non abouties émises d'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. Une fois que 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.

6.2.3 Extensions de services

Le Tableau 3 définit les services pouvant être 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 ce même profil. 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 service

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 portant 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
État 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 le tableau d'états supplémentaires
État supplémentaire	MATRICE de UINT	État 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.

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 paragraphe 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 présenté à la Figure 5 ci-dessous. Les réglages appropriés des divers 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-à-T		UDINT	Instance de connexion de consommation:: ID de connexion consommée CIP
ID de connexion de réseau T-à-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
Multiplicateur de temporisation de connexion		USINT	Instance de connexion de production et de consommation: Multiplicateur de temporisation
Réservé		3 OCTETS	
RPI O-à-T		UDINT	Instance de connexion de consommation: EPR
Paramètres de connexion de réseau O-à-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: Priorité élevée; 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 Mode Octet, Actual (Réel), Complement (Complémentaire) et Time stamp (Datation); Destinataire: Instance de connexion de consommation: Attribut de taille de connexion consommée
RPI T-à-O		UDINT	Instance de connexion de production: EPR
Paramètres de connexion de réseau T-à-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
	Priorité		Valeur: Priorité élevée; Destinataire: Gestionnaire de connexion
	Fixe/Variable		Valeur: Fixe; Destinataire: Gestionnaire de connexion

Nom de paramètre		Type de données / Taille	Destination cible et sémantique
	Taille de connexion (en octets)		Valeur: Taille du PDU de sécurité, y compris les sections Mode Octet, Actual (Réel), Complement (Complémentaire) et Time stamp (Datation). Destinataire: Instance de connexion de production; Taille de connexion produite
Type de transport/Déclencheur		SWORD	Valeur: Valeur de sécurité simple ou multipoints. 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 La valeur incluse dans le calcul du CRC ne comprend pas les mots employés pour les segments Réseau/Port.
Connection_Path (EPATH complété)	Chemin		Variable
			Consommé par le(s) gestionnaire(s) de connexion en pont intermédiaire(s). Chaque segment Format de routage-Réseau de sécurité suit immédiatement le pont (CPF 2 – vers – CPF 2) pour lequel il est destiné
	Segment logique: Clé électronique	ID du fournisseur	UINT
		Type de prod.	UINT
		Code de prod.	UINT
		Compatible/ Rev. principale	SWORD
		Rev. secondaire	USINT
	Chemin d'application 1	Segment logique: Classe	Variable; 1 mot généralement
		Segment logique: Instance	Variable; 1 mot généralement
	Chemin d'application 2	Segment logique: Point de connexion	Variable; 1 mot généralement
	>Chemin d'application 3	Segment logique: Point de connexion	Variable; 1 mot généralement
	Données de configuration	Segment de données: Données simples	Variable
	Segment de réseau:	Nom de segment de sécurité	50 _{hex}
		Taille de segment	USINT
		Format de segment	USINT
		Données de sécurité de réseau	TABLEAU D' OCTETS

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**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 tel que 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} (produisant 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 de 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 de segment de réseau de sécurité, définies par le format de segment

6.3.3.2 Segment de réseau de sécurité: Format cible (00_{hex})

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.

Nom de champ	Type de données	Description
Réservé	SWORD	Remplissage
CRC de configuration (SCCRC)	UDINT	CRC-54 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	Datation 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, multipoints
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 valide 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(Multipoints)
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**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 Safety ForwardOpen. 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 duquel la demande de connexion a été émise. Les segments de réseau de sécurité du format de routage apparaissent uniquement dans la partie du chemin du Connection_Path d'un service Safety

ForwardOpen. 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 dans l'objet Gestionnaire de connexion. Non utilisé: 0 (Nul). Utilisé: Fixe, priorité élevée, multipoints

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	Datation 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 dans l'objet Gestionnaire de connexion. Non utilisé: 0 (Nul). Utilisé: Fixe, priorité élevée, multipoints
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)

Nom de champ	Type de données	Description
Ping_Interval_EPI_Multiplier	UINT	Nombre qui définit le Ping_Count_Interval pour la connexion. La plage de valeurs valide 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 HiAvailabilityFormat
Max_Consumer_Number	USINT	Valeur: 1 (point à point), 2-15(multipoints)
Max_Fault_Number	UINT	Utilisé par les producteurs et les consommateurs afin de déterminer le nombre de paquets erronés pouvant être omis avant qu'une connexion ne doive être fermée. Plage valide comprise entre 0 et 255 ^b Valeur par défaut = 5. Une valeur de 0 indique que les connexions doivent être fermées dès qu'une erreur est détectée
CRC des paramètres de connexion (CPCRC)	UDINT	CRC-S32 des paramètres de connexion cible dans cette demande
ID ^a de connexion de correction de temps	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.		
^b Voir 8.8.3 pour les règles et restrictions en matière de configuration du point d'origine.		

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.

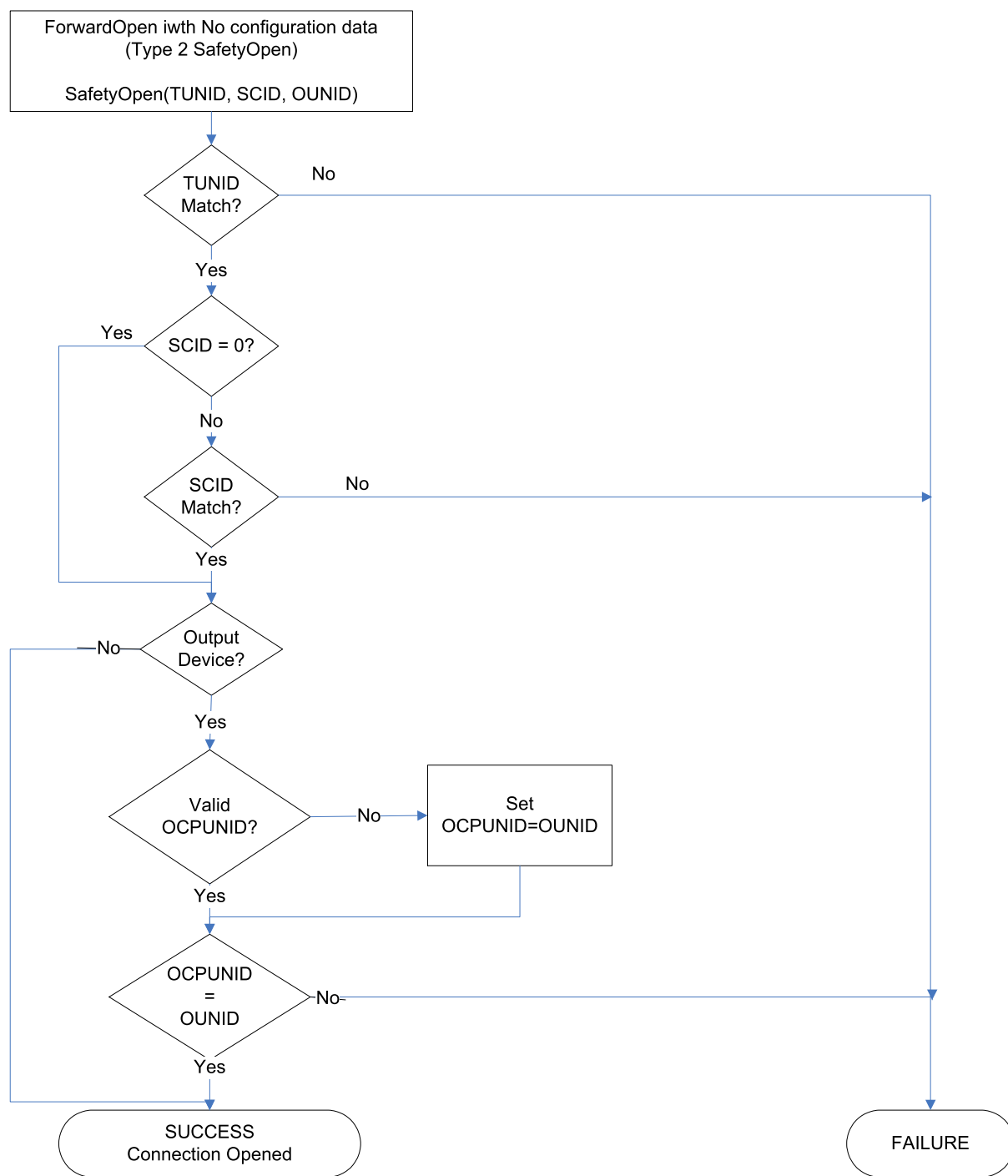
La taille du chemin de connexion dans le service SafetyOpen change de valeur selon qu'un point d'origine envoie ou non des données de configuration. Dans la mesure où ce champ est inclus dans le calcul du CPCRC, il est nécessaire que les points d'origine calculent et conservent deux valeurs lorsqu'ils 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 Safety ForwardOpen 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 l'adaptation 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.



Key:

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

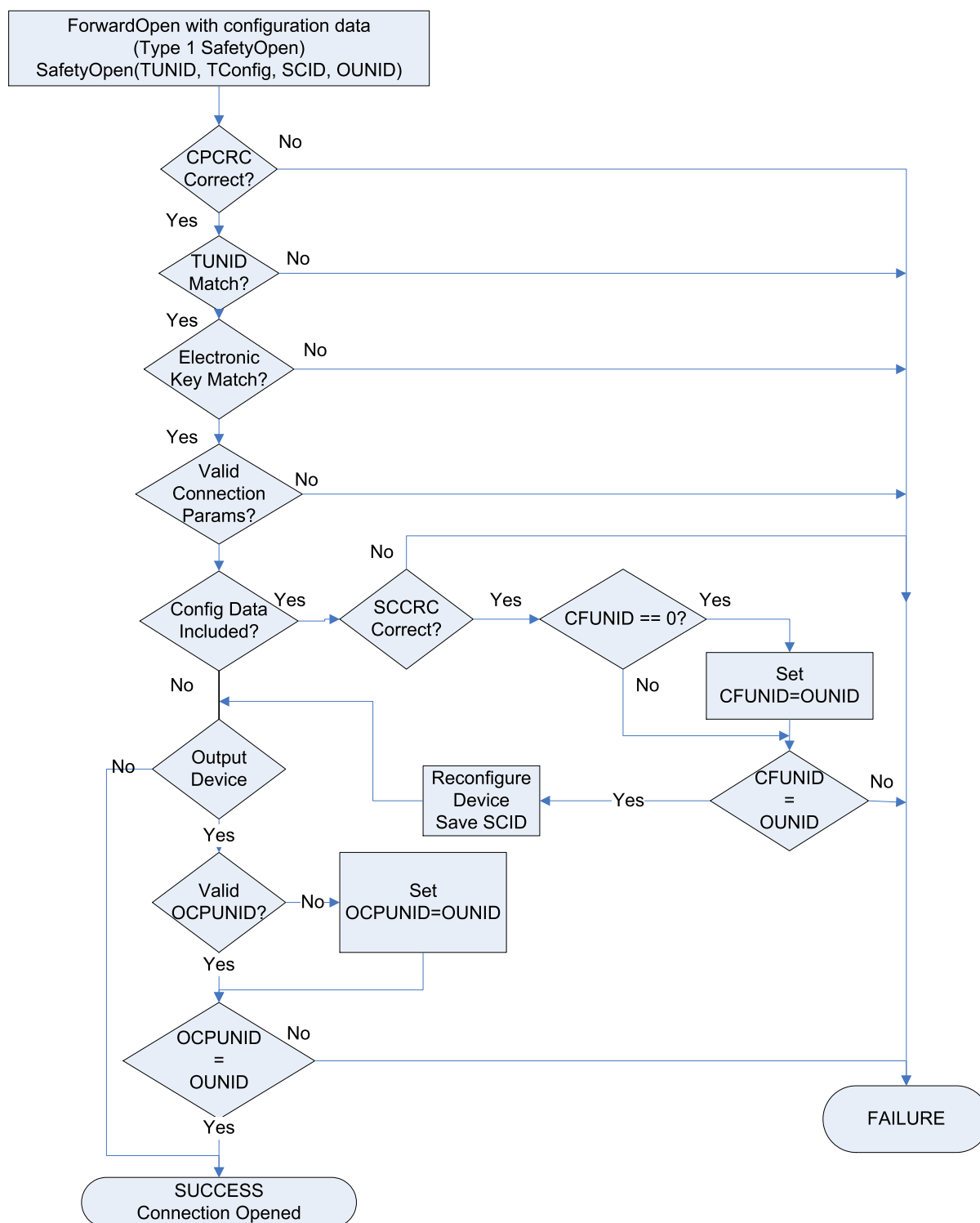
TUNID = Target's Unique Network Identifier
 OUNID = Originator's Unique Network Identifier
 OCPUNID = Output Connection Owing UNID

IEC

Anglais	Français
ForwardOpen with no configuration data	ForwardOpen sans données de configuration
TUNID match?	TUNID adapté?
No	Non
Yes	Oui
SCID match?	SCID adapté?

Anglais	Français
Output device	Appareil de sortie
Valid OCPUND?	OCPUNID valide?
Set	Régler
SUCCESS Connection Opened	RÉUSSITE Connexion Ouverte
FAILURE	ÉCHEC
Key	Légende
UNID unique network identifier	identifiant de réseau unique
SCID target's safety configuration ID	ID de configuration de sécurité de la cible
OCP output connection point	point de connexion de sortie
CFUNID configuration owning UNID	UNID de propriétaire de la configuration
TUNID target's unique network identifier	identifiant de réseau unique de la cible
OUNID originator's unique network identifier	identifiant de réseau unique du point d'origine
OCPUNID output connection owning UNID	UNID de propriétaire de la connexion de sortie

Figure 7 – Service SafetyOpen de traitement de cible sans données de configuration (SafetyOpen de forme 2)



Key:

UNID = Unique Network Identifier
 CPCRC = Connection Parameter CRC
 SCCRC = CRC portion of the SCID
 OCPUNID = Output Connection Owning UNID

TUNID = Target's Unique Network Identifier
 SCID = Target's Safety Configuration ID
 OUNID = Originator's Unique Network Identifier
 CFUNID = Configuration Owning UNID

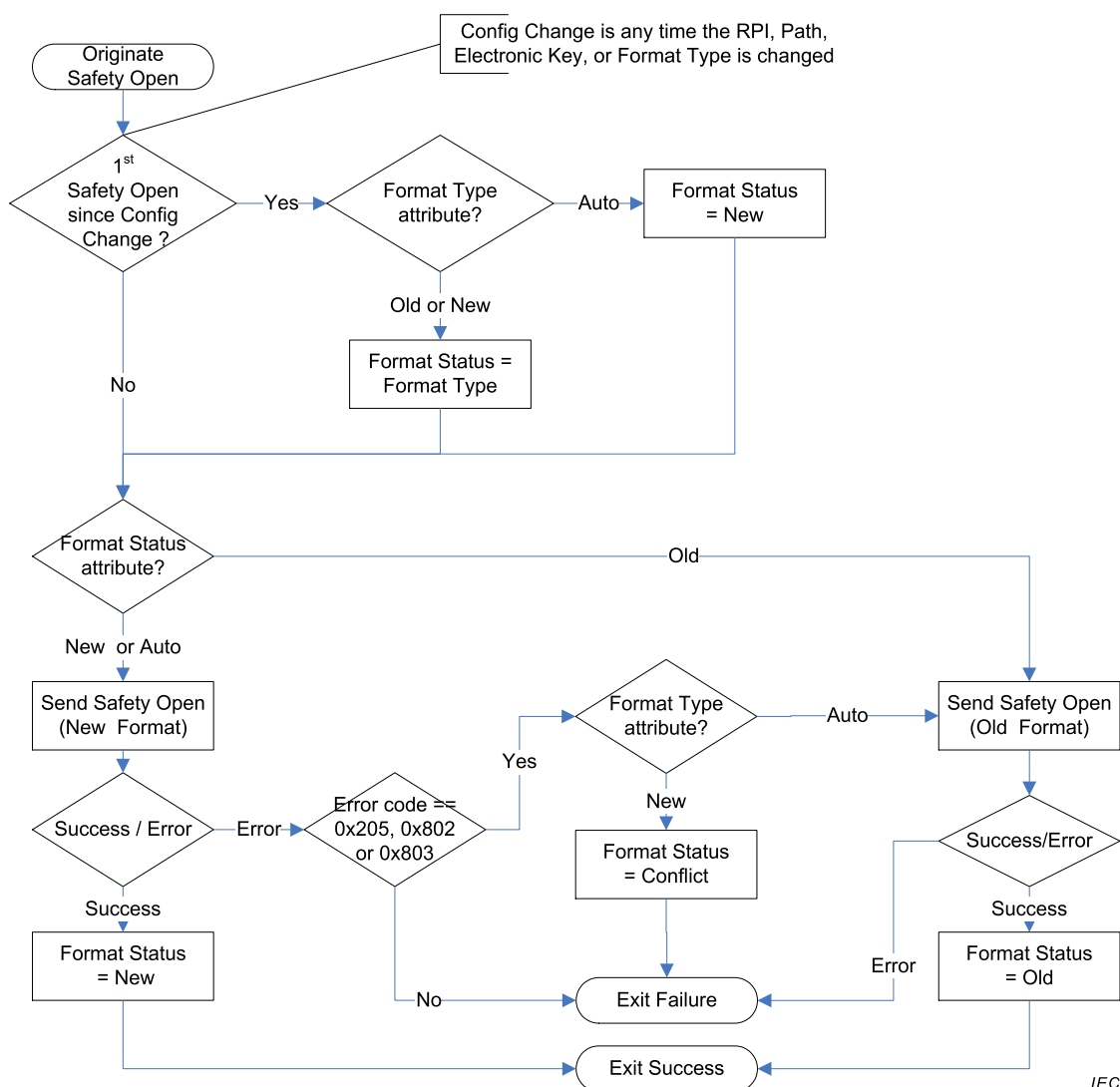
IEC

Anglais	Français
ForwardOpen with configuration data	ForwardOpen avec données de configuration
CPCRC Correct?	CPCRC correct?

Anglais	Français
TUNID Match?	TUNID adapté?
No	Non
Yes	Oui
Electronic key match?	Clé électronique adaptée?
Valid connection params?	Paramètres de connexion valides
Config data included?	Données de config incluses?
SCCRC Correct?	SCCRC correct?
Set	Régler
Output device	Appareil de sortie
Reconfigure device save SCID	Reconfigurer SCID de sécurité d'appareil
Valid OCPUNID?	OCPUNID valide?
SUCCESS connection opened	RÉUSSITE connexion ouverte
FAILURE	ÉCHEC
Key	Légende
UNID unique network identifier	identifiant de réseau unique
SCID target's safety configuration ID	ID de configuration de sécurité de la cible
CPCRC connection parameter CRC	CRC de paramètre de connexion
CFUNID configuration owning UNID	UNID de propriétaire de la configuration
TUNID target's unique network identifier	identifiant de réseau unique de la cible
OCPUNID output connection owning UNID	UNID de propriétaire de la connexion de sortie
SCCRC CRC portion of the SCID	partie CRC de SCID
OUNID originator's unique network identifier	identifiant de réseau unique du point d'origine

Figure 8 – Service SafetyOpen de traitement de cible avec données de configuration (SafetyOpen de forme 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.



Anglais	Français
Originate SafetyOpen	SafetyOpen de point d'origine
Config change is any time the RPI, Path, Electronic Key, or Format Type is changed	Modification de configuration à chaque modification de RPI, de chemin, de clé électronique ou de type de format
1 st SafetyOpen since ConfigChange?	1er SafetyOpen en fonction de la modification de configuration?
Yes	Oui
Format Type attribute	Attribut de type de format
Auto	Auto
Format status	État de format
New	Nouveau
Old or new	Ancien ou nouveau
Format type	Type de format
No	Non
Format status attribute?	Attribut d'état de format?
Old	Ancien
New or auto	Nouveau ou auto
Send SafetyOpen (new format)	Envoi de SafetyOpen (nouveau format)

Anglais	Français
(Old format)	(Ancien format)
Success	Réussite
Error	Erreur
Error code or	Code d'erreur ou
Conflict	Conflit
Exit failure	Échec en sortie
Exit success	Réussite en sortie

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 divers 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 multipoints, 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 multipoints.

Tableau 9 – Règles d'évaluation des paramètres de production multipoints

Paramètre de sécurité	Règle d'évaluation de production si la connexion existe	Réponse d'erreur ^a (le cas échéant)	
		Générale	Étendue
Ping_Interval EPI Multiplier	Doit correspondre au P.I.E.M. existant	01 _{hex} 00 _{hex}	0801 _{hex} 0012 _{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 s'adapter au Max_Consumer_Number existant	00 _{hex} 01 _{hex}	0801 _{hex} 002A _{hex}
RPI T-à-O, RPI O-à-T et RPI de correction de temps	Doit s'adapter aux RPI de connexion existants	01 _{hex}	0111 _{hex}
Type de segment de réseau	Doit s'adapter au format de connexion existant ^b	0x01	0x803
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.			
^b Les demandes de connexion ultérieures formulées sur une connexion multipoints existante doivent toutes avoir le même format que la connexion existante			

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 SafetyForwardOpen.

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, tel que défini. Les caractères de remplacement (champs réglés 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 $\pm 128 \mu\text{s}$.

Les intervalles API T-à-O, O-à-T et de correction de temps dans une réponse satisfaisante doivent toujours avoir la même valeur que le service SafetyOpen reçoit.

6.3.9 Élaboration du chemin d'application de sécurité

L'IEC 61158-6-2 définit une méthode d'élaboration d'un chemin d'application dans un service SafetyOpen pour les 3 références suivantes: une méthode pour configuration, une méthode pour les données consommées et une méthode pour les données produites.

Les types de chemin possibles sont identifiés comme suit:

- A. - [Classe] [Ensemble] [Instance] [Configuration-instance]
- B. - [Classe] [Ensemble] [Instance] [Producteur-instance]
- C. - [Classe] [Ensemble] [Instance] [Consommateur-instance]
- 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).

[Class] [Class #] [Instance] [# Instance] [CNP] [CNP Consommateur] [CNP] [CNP Producteur]

Dans la mesure où la classe de référence des trois chemins doit être identique, une valeur 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;

- les points d'origine doivent toujours transmettre un chemin de configuration valide sur toutes les connexions qui peuvent accepter un service SafetyOpen de forme 1, et ce, même en l'absence de toute donnée de configuration (c'est-à-dire forme 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 formes 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;
- [À, 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 formes 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.

6.3.10 Types de connexion 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 2 et 3 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 paragraphe 6.3.10 indique de quelle manière sont déterminés les types de connexion, 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 divers 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 divers 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. Les instances d'objet de connexion peuvent ne pas être disponibles en raison de la capacité ou des limites de l'identifiant de cible; il peut par ailleurs n'y avoir aucun identifiant de connexion qui ne soit pas attribué. L'appareil peut également ne pas avoir la capacité nécessaire au traitement de la connexion supplémentaire; etc. Les objets Connexion de sécurité exigent des ressources similaires aux connexions E/S standard.

**Tableau 10 – Options de paramétrage du service ForwardOpen
pour les connexions de sécurité**

Type de connexion O-à-T	Type de connexion T-à-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	Multipoints	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 multipoints CP 2/3	2 – Multipoints + 1 point à point + Client	Connexion de production: Données de sécurité Connexion de production: Correction Connexion de consommation: coordination
Point à point	Multipoints	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 multipoints CP 2/2	1 – Multipoints + 1 point à point + Client	Connexion de production: Données de sécurité + correction Connexion de consommation: coordination
Multipoints	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 multipoints CP 2/3	2 – Multipoints + 1 point à point + Serveur	Connexion de consommation: Données de sécurité Connexion de consommation: Correction Connexion de production: coordination
Multipoints	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 multipoints CP 2/2	1 – Multipoints + 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 via EDS doivent définir un chemin Nul d'application dans le fichier EDS.

Le Tableau 11 définit les paramètres de connexion de réseau à utiliser pour l'ensemble des trois connexions associées à chaque type de connexion de sécurité.

Tableau 11 – 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-à-T	4406 _{hex}	Priorité élevée point à point, fixe
	T-à-O	4408 _{hex}	Priorité élevée point à point, fixe
	Correction de temps	0000 _{hex}	Non utilisé
Producteur point à point	O-à-T	4408 _{hex}	Priorité élevée point à point, fixe
	T-à-O	4406 _{hex}	Priorité élevée point à point, fixe
	Correction de temps	0000 _{hex}	Non utilisé
Producteur multipoints	O-à-T	4406 _{hex}	Priorité élevée point à point, fixe
	T-à-O	240E _{hex}	Priorité élevée, multipoints, fixe
	Correction de temps	2406 _{hex}	Priorité élevée multipoints, 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 12.

La cible d'une fonction SafetyOpen doit renvoyer les données, définies du Tableau 12 au Tableau 15 dans le champ Réponse d'application de la réponse SafetyOpen. Le nombre de consommateurs et les données de réponse PID sont importants uniquement lorsque le point d'origine est le consommateur.

Tableau 12 – Réponse d'application de cible de sécurité CP 2/3 (taille: 10 octets)

Nom de paramètre	Type de données	Description
Consumer_Number	UINT	
PID/CID	STRUCT de:	Identifiant de cible permettant de générer une valeur de départ PID ou CID
Id du fournisseur de cible	UINT	Id du fournisseur de cible
Numéro de série de l'appareil de cible	UDINT	Numéro de série de l'appareil de cible
Numéro de série de connexion de cible	UINT	Numéro de série de connexion de cible attribué à la connexion. L'identifiant 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 13.

Tableau 13 – Réponse d'application de cible de sécurité CP 2/3 EF (taille: 14 octets)

Nom de paramètre ^a	Type de données	Description
Consumer_Number	UINT	
PID/CID	STRUCT de:	Identifiant de cible permettant de générer une valeur de départ PID ou CID
Id du fournisseur de cible	UINT	Id du fournisseur de cible
Numéro de série de l'appareil de cible	UDINT	Numéro de série de l'appareil de cible
Numéro de série de la connexion de cible	UINT	Numéro de série de la connexion de cible attribué à la connexion. Il convient d'utiliser l'identifiant instance de l'Objet de validation de sécurité
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 Ces champs sont toujours présents dans le champ Réponse d'application. Lorsqu'une cible de sécurité CP 2/3 reçoit une fonction SafetyOpen qui n'est pas multipoints (aucune connexion de correction de temps n'étant ainsi établie), le paramètre Time_Correction_Connection_ID doit être réglé sur FFFF _{hex} . Si la cible n'est pas un producteur multipoints, le nombre de consommateurs est réglé sur FFFF _{hex} . ^b Il convient que les cibles de consommation renvoient les valeurs reçues dans la fonction SafetyOpen		

Tableau 14 – Réponse d'application de cible SafetyOpen (taille: 18 octets)

Nom de paramètre ^a	Type de données	Description
Consumer_Number	UINT	
PID/CID	STRUCT de:	Identifiant de cible permettant de générer une valeur de départ PID ou CID
Id du fournisseur de cible	UINT	Id du fournisseur de cible
Numéro de série de l'appareil de cible	UDINT	Numéro de série de l'appareil de cible
Numéro de série de la connexion de cible	UINT	Numéro de série de la connexion de cible attribué à la connexion. L'identifiant instance de l'Objet de validation de sécurité doit être utilisé
Time_Correction_Connection_ID	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 Ces champs sont toujours présents dans le champ Réponse d'application. Lorsqu'une cible de sécurité CP 2/3 reçoit une fonction SafetyOpen qui n'est pas multipoints (aucune connexion de correction de temps n'est ainsi établie), le paramètre Time_Correction_Connection_ID doit être réglé sur FFFF _{hex} . Si la cible n'est pas un producteur multipoints, le nombre de consommateurs est réglé 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 15.

Tableau 15 – Réponse d'application de cible SafetyOpen EF (taille: 22 octets)

Nom de paramètre ^a	Type de données	Description
Consumer_Number	UINT	
PID/CID	STRUCT de:	Identifiant de cible utilisé pour générer une valeur de départ PID ou CID
Id du fournisseur de cible	UINT	Id du fournisseur de cible
Numéro de série de l'appareil de cible	UDINT	Numéro de série de l'appareil de cible
Numéro de série de la connexion de cible	UINT	Numéro de série de la connexion de cible attribué à la connexion. Il convient d'utiliser l'identifiant instance de l'Objet de validation de sécurité
Time_Correction_Connection_ID	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 Ces champs sont toujours présents dans le champ Réponse d'application. Lorsqu'une cible CP 2/3 reçoit une fonction SafetyOpen qui n'est pas multipoints (aucune connexion de correction de temps n'est ainsi établie), le paramètre Time_Correction_Connection_ID doit être réglé sur FFFF _{hex} . Si la cible n'est pas un producteur mutlipoints, le nombre de consommateurs est réglé sur 0xFFFF.		
^b Il convient que les cibles de consommation renvoient les valeurs reçues dans la fonction SafetyOpen.		

6.3.12 Réponse SafetyOpen non satisfaisante

La fonction SafetyOpen comporte certains cas d'erreurs spéciaux qui ne sont pas mis en correspondance avec l'ensemble existant de codes d'erreurs, et étend la définition des codes d'erreurs existants.

Le Tableau 16 définit de nouveaux codes d'erreurs étendus de sécurité et présente la définition étendue des codes d'erreurs existants.

Tableau 16 – Nouveaux codes d'erreurs étendus de sécurité

État général	État étendu	Explication
01 _{hex}	0105 _{hex}	Conflit de propriété ou défaut d'adaptation OUNID. La configuration est déjà propriété d'un autre point d'origine
01 _{hex}	0106 _{hex}	Conflit de propriété ou défaut d'adaptation 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}	801 _{hex}	RPI multipoints incompatible. Une connexion existante a été établie à un RPI différent.
01 _{hex}	802 _{hex}	Taille de connexion de sécurité invalide
01 _{hex}	803 _{hex}	Format de connexion de sécurité invalide
01 _{hex}	804 _{hex}	Paramètres de connexion de correction de temps invalides
01 _{hex}	805 _{hex}	Multiplicateur EPI d'intervalles Ping invalide
01 _{hex}	806 _{hex}	Multiplicateur minimal de messages de coordination temporelle
01 _{hex}	807 _{hex}	Multiplicateur de délai du réseau

État général	État étendu	Explication
01 _{hex}	808 _{hex}	Multiplicateur de temporisation
01 _{hex}	809 _{hex}	Nombre maximal de consommateurs invalide
01 _{hex}	80A _{hex}	CPRC invalide
01 _{hex}	80B _{hex}	ID de connexion de correction de temps invalide
01 _{hex}	80C _{hex}	Défaut d'adaptation SCID. La valeur de SCID était non nulle et ne correspondait pas à la valeur de la cible
01 _{hex}	80D _{hex}	TUNID non défini. L'appareil est out-of-box (hors connexion) et TUNID n'a pas été défini, les connexions ne sont donc pas admises
01 _{hex}	80E _{hex}	Défaut d'adaptation TUNID. Le TUNID fourni n'est pas adapté. Le message a été vraisemblablement acheminé vers ce nœud par erreur
01 _{hex}	80F _{hex}	Opération de configuration non admise

Le Tableau 17 de matrice d'événements/erreurs fournit des lignes directrices concernant les codes d'erreurs à appliquer pour les erreurs potentielles détectées lors du traitement d'un service SafetyOpen. Ces lignes directrices ne sont pas censées constituer une liste exhaustive.

Tableau 17 – Tableau de lignes directrices concernant les événements d'erreur SafetyOpen

Événement	Type d'erreur	État général	État étendu
L'appareil cible a reçu une demande SafetyOpen dans des états de l'objet Programme de contrôle de sécurité autres que l'état de repos et l'état d'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}
Multiplicateur Min. 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 multipoints	Erreur de paramètre de sécurité – Nombre maximal de consommateurs invalide	01 _{hex}	0809 _{hex}

Événement	Type d'erreur	État général	État étendu
Valeur CPCRC dans SafetyOpen et valeur CPCRC calculée	Erreur de paramètre de sécurité – CPCRC 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 multipoints incompatible	01 _{hex}	801 _{hex}
RPI O-à-T, RPI T-à-O, ou RPI de correction de temps non pris en charge	RPI non pris en charge	01 _{hex}	0111 _{hex}
Toutes les instances Objet de validation de sécurité sont utilisées	Le Gestionnaire de connexion ou l'objet de connexion ne peut plus prendre en charge 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 dont 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 sont adaptés. Les informations supplémentaires fournies par ce service (c'est-à-dire le chemin de connexion) doivent être ignorées par la cible.

Une réponse satisfaisante SafetyClose doit être transmise après suppression de la connexion au niveau de la cible.

À réception d'une réponse satisfaisante SafetyClose, 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 sélectionnée par le fournisseur.

6.4 Objet Identité

6.4.1 Généralités

Code de classe: 01hex

Le présent paragraphe 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 18 définit les services de l'objet Identité qui exigent des actualisations.

Tableau 18 – Modifications apportées aux services communs de l'objet Identité

Code de service	Mise en œuvre nécessaire		Nom de service	Description du service
	Classe	Instance		
05 _{hex}	Facultatif	Conditionnel ^a	Réinitialisation	Appelle le service Réinitialisation pour l'appareil
^a Conditionnel – Le service Réinitialisation de l'objet Identité ne doit pas être pris en charge dans les appareils de sécurité (réponse aux demandes avec erreur «Service non pris en charge»). Le service doit être remplacé par le service Réinitialisation défini par le programme de contrôle de sécurité.				

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 19.

Certains des attributs des extensions de l'objet pour CP 16/3 renvoient à des IDN (Numéros d'identification) de CP 16/3 utilisant la nomenclature de CP 16/3, par exemple S-0-1300. Ces IDN de CP 16/3 sont spécifiés en détail dans l'IEC 61158-4-19.

Tableau 19 – 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 IEC 61158-5-2		
2	Exigé	Obtenir	Type d'appareil	Voir IEC 61158-5-2		
3	Exigé	Obtenir	Code produit	Voir IEC 61158-5-2		
4	Exigé	Obtenir	Révision	Voir IEC 61158-5-2		
5	Exigé	Obtenir	État	Voir IEC 61158-5-2		
6	Exigé	Obtenir	Numéro de série	Voir IEC 61158-5-2		
7	Exigé	Obtenir	Nom du produit	Voir IEC 61158-5-2		Les 32 premiers caractères de CP 16/3 S-0-1300.x.4
8-18	Facultatif	Voir 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: 03hex

Le présent paragraphe 6.5.1 définit les modifications et ajouts nécessaires 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 20.

Tableau 20 – Nouvel attribut instance de l'objet DeviceNet

ID de l'attribut	Mise en œuvre nécessaire	Règle d'accès	Nom	Type de données	Description de l'attribut	Sémantique de la valeur
11	Exigé	Obtenir	Numéro de réseau de sécurité	6 OCTETS	Numéro unique pour 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 ultérieure 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 caractéristique Quick Connect (Connexion rapide). L'attribut Connexion Rapide ne doit pas être pris en charge et doit répondre à tout service d'attribut Get/Set (Obtenir/Définir) avec le code d'erreur «Attribut non pris en charge».

6.5.2 Modifications apportées à l'objet Interface TCP/IP

Code de classe: F5_{hex}

Le présent paragraphe 6.5.2 définit les modifications et ajouts nécessaires 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 21.

Tableau 21 – Nouvel attribut instance de l'objet Interface TCP/IP

ID de l'attribut	Mise en œuvre nécessaire	Règle d'accès	Nom	Type de données	Description de l'attribut	Sémantique de la valeur
7	Exigé	Obtenir	Numéro de réseau de sécurité	6 OCTETS	Numéro unique pour 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 ultérieure 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 paragraphe 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 FSCP 2/1 sur 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 22.

Tableau 22 – Attributs de classe de l'objet Liaison SERCOS III

ID de l'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	Obtenir	Instance maximale	UINT	Nombre maximal d'instances d'un objet actuellement créé à ce niveau 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 des liaisons d'interface CP 16/3 multiples, cet attribut doit être pris en charge.						

6.5.3.3 Attributs Instance

Les attributs instance de l'objet Liaison SERCOS III sont définis dans le Tableau 23.

Tableau 23 – Attributs instance de l'objet Liaison SERCOS III

ID de l'attribut	Mise en œuvre nécessaire	Règle d'accès	Nom	Type de données	Description de l'attribut	Sémantique de la valeur
1	Exigé	Obtenir	Numéro de réseau de sécurité	6 OCTETS	Numéro unique pour 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 ultérieure de cet attribut
2	Facultatif	Obtenir	Durée du cycle de communication	DINT	CP 16/3 S-0-1002	
3	Facultatif	Obtenir	État interface	WORD	CP 16/3 S-0-1014	
4	Facultatif	Obtenir	Compteur d'erreurs MST-P/S	INT	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	INT		
			Compteur d'erreurs Port2	INT		
6	Facultatif	Obtenir	Adresse SERCOS®	INT	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 24.

Tableau 24 – Services communs de l'objet Liaison SERCOS III

Code de service	Mise en œuvre nécessaire		Nom de 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 n'importe quel 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:

- 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 portant 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 considérés 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'objets d'application et les informations d'état associées, les indications d'état d'exception (alarmes et avertissements), et définit un modèle de comportement supposé 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 de ses 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 semi-conducteurs.

6.6.2 Attributs de classe de programme de contrôle de sécurité

Les attributs de classe utilisés par le programme de contrôle de sécurité sont définis dans le Tableau 25.

Tableau 25 – Attributs de classe de 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», alors il convient d'appliquer cet attribut. Dans le cas contraire, cet attribut doit être appliqué.					

6.6.3 Sous-classes

Chaque sous-classe de niveau de classe donne une signification unique pour un intervalle de recouvrement d'identifiants d'attributs de classe et/ou de services de classe. L'intervalle 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 de programme de contrôle de sécurité

Les attributs instance utilisés par le programme de contrôle de sécurité sont définis dans le Tableau 26.

Tableau 26 – Attributs instance de 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

ID d'attribut	Mise en œuvre nécessaire	Règle d'accès	NV	Nom	Type de données	Description de l'attribut
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	État de l'appareil	USINT	Voir 6.6.5.5
12	Exigé	Obtenir	V	État d'exception	SWORD	Voir 6.6.5.6
13	Conditionnel, basé sur le bit 7 d'état d'exception	Obtenir	V	Alarme de détail d'exception	STRUCT. de:	Structure de 3 éléments contenant 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
				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
				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, basé sur le bit 7 d'état d'exception	Obtenir	V	Avertissement de détail d'exception	STRUCT. de:	Structure de 3 éléments contenant une représentation en mode point du détail d'avertissement
				Détail d'exception commun	STRUCT. de:	
				Taille	USINT	Nombre d'octets de détail commun
				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
				Détail	MATRICE de:	Spécifié par le fabricant
				Détail n	SWORD	Spécifié par le fabricant

ID d'attribut	Mise en œuvre nécessaire	Règle d'accès	NV	Nom	Type de données	Description de l'attribut
				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	Exigé	Définir	NV	Activation alarme	BOOL	Voir 6.6.5.12
16	Exigé	Définir	NV	Activation avertissement	BOOL	Voir 6.6.5.12
17	Facultatif	Définir	A	Temps	DATE_ AND_ TIME	Valeur de l'horloge temps réel interne de l'appareil
18	Facultatif	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 «Time») 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 fonctionnant 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 – Exigé si l'expiration d'étalonnage est prise en charge	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

ID d'attribut	Mise en œuvre nécessaire	Règle d'accès	NV	Nom	Type de données	Description de l'attribut
24	Conditionnel ^c	Défini uniquement par le service «Verrouillage/Déverrouillage de configuration» Obtention possible	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 FF _{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	Exigé	Obtenir	NV	UNID Cible (Target UNID)	10 octets	UNID courante de l'appareil
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 du e-chemin (ePath)	USINT	Taille du chemin, nombre d'octets
				Ressource d'application	e-chemin compact	Chemin vers la ressource «avec propriétaire» (c'est-à-dire 20 04 24 01 – classe d'ensemble, instance 1)
29	Conditionnel ^c	Obtenir	V	Proposition de TUNID	10 octets	Valeur UNID qu'un point d'origine tente de définir dans l'appareil
97-98	Réservé par le FSCP 2/1 pour une utilisation future					

ID d'attribut	Mise en œuvre nécessaire	Règle d'accès	NV	Nom	Type de données	Description de l'attribut
99	Conditionnel ^b	Obtenir	NV	Sous-classe	UINT	Identifie un sous-ensemble d'attributs d'instance, de services et de comportements supplémentaires
^a Le comportement non volatil de l'attribut Time dépend de la valeur de l'attribut Comportement de l'horloge pendant un cycle d'alimentation. ^b Si la valeur de sous-classe est 00, qui identifie «aucune sous-classe», alors 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.						

6.6.5 Sémantique

6.6.5.1 Nom du fabricant

L'attribut Nom du fabricant, identifie le fabricant de l'appareil.

Cet attribut n'est pas garanti, par spécification, d'être unique. Il ne constitue par conséquent 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 textes à 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 textes à 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 soit adapté 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 État 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 État de l'appareil sont définies dans le Tableau 27.

Tableau 27 – Valeurs d'indication de l'attribut État de l'appareil

Valeur d'attribut	État
0	Non défini
1	Autovérification
2	Repos
3	Exception d'autovérification
4	Exécution
5	Abandon
6	Anomalie critique
7	Configuration
8	Attente de TUNID
9-50	Réservé par FSCP 2/1
51-99	Spécifique à l'appareil
100-255	Spécifique au fournisseur

6.6.5.6 État 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 sept de l'attribut État d'exception est réglé sur zéro; la communication de cet attribut permet de consigner de manière exclusive toutes ces exceptions. Le format des bits zéro à six 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 sept de l'attribut État d'exception est réglé sur un; la communication de cet attribut permet de consigner ces exceptions, le format étant spécifié dans le Tableau 28. De plus, les attributs Détail d'exception sont pris en charge. Les bits de l'attribut État d'exception sont déterminés par un élément logique «OR» des bits associés de l'attribut Détail d'exception, tel qu'indiqué.

Tableau 28 – Format de l'attribut État d'exception

Bit	Mode point de l'état d'exception, bit 7 réglé sur 0 fonction	Mode point de l'état d'exception, bit 7 réglé sur 1 fonction
0	Définition spécifique à l'appareil (voir Profil de l'appareil)	ALARME/commune à l'appareil ^a
1		ALARME/spécifique à l'appareil
2		ALARME/spécifique au fabricant
3		Réservé – réglé sur 0
4		AVERTISSEMENT/commun à l'appareil ^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 détaillé des alarmes ou des avertissements sont associés à l'appareil. Chaque attribut est une structure contenant trois membres, chacun de ces membres étant relatif respectivement à l'état détaillé 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 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 SIZE (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 contenant une liste ordonnée (c'est-à-dire une matrice) d'OCTETS de longueur SIZE (TAILLE), et un entier non signé dont la valeur est SIZE (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 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 établi. 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 «nulle».

L'existence d'une structure variable du détail d'exception dépend de la valeur de l'attribut État d'exception. L'existence d'une structure variable du détail d'exception est exigée uniquement si le bit sept de l'attribut État d'exception est réglé sur 1 (indiquant la consignation de la méthode étendue), le bit (parmi les bits zéro à six) dudit attribut correspondant au type d'exception particulier étant également réglé 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 SIZE qui constitue la valeur de l'élément de structure Size. Pour chaque octet du champ Détail, tous les bits non identifiés sont réservés pour une normalisation future.

Le premier octet de cet attribut est CommonExceptionDetail[0]. Les détails d'exception supplémentaires, s'ils sont fournis, sont appelés CommonExceptionDetail[1] et CommonExceptionDetail[SIZE]. L'exception spécifique associée à chacun des modes point est donnée dans le Tableau 29. La SIZE pour cette révision est de deux (2). Les détails des critères propres à chaque condition d'exception ne relèvent pas du domaine d'application de la présente partie.

6.6.5.9 Valeurs communes de l'attribut Détail d'exception

Tableau 29 – Valeurs communes de l'attribut Détail d'exception

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 établi.

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 SIZE qui constitue la valeur de l'élément de structure Size. 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 30), 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 SIZE qui constitue la valeur de l'élément de structure Size. Pour une description détaillée de cet attribut, consulter la documentation du fabricant d'appareils spécifiques appropriée.

Tableau 30 – 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	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.								

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 d'établissement des bits correspondants, cette désactivation

contribuant à la suppression de ces bits s'ils avaient été établis. Les états d'alarme et d'avertissement ne sont également pas conservés; lorsqu'ils sont activés, les bits doivent être réglés uniquement si la condition correspondante est vraie.

L'état par défaut de ces attributs Activer est activé (1).

6.6.5.13 Time (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 Time est zéro (0), ce qui correspond à 00:00:00, 1970-01-01.

6.6.5.14 Temporisateur d'expiration de maintenance programmée

Cet attribut, comportant une résolution d'une heure, permet d'engendrer un avertissement signifiant que l'appareil doit faire l'objet d'un étalonnage. 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 Activer Avertissement de l'expiration de maintenance programmée est réglé 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 Activer Avertissement de l'expiration de maintenance programmée. Ce même temporisateur, toujours lorsqu'il est mis en œuvre, doit être maintenu 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 d'établissement du bit correspondant, cette désactivation contribuant à la suppression de ce bit s'il avait été établi. Lorsqu'il est activé, le bit doit être réglé uniquement si la condition correspondante est vraie.

L'état par défaut de cet attribut Activer 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 règle 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 préalablement au déverrouillage et à la modification de 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 (Safety Reset) de types 1 et 2 et de toute fonction SafetyOpen de forme 1 valide.

6.6.5.17 Configuration UNID (CFUNID)

L'attribut Configuration UNID doit être mis en œuvre comme partie intégrante de l'interface SNCT. La configuration UNID identifie le propriétaire de la configuration dans cet appareil de sécurité. L'attribut Configuration UNID peut être réglé par différents moyens. Les significations spéciales suivantes doivent être attribuées à l'attribut Configuration UNID:

- Tous les octets réglés sur 00_{hex} = Pas de propriétaire, accepte tout propriétaire,
- Tous les octets réglés sur FF_{hex} = l'outil logiciel est le propriétaire attribué.

La valeur par défaut de la configuration UNID doit correspondre au réglage de tous les octets sur 00_{hex}.

Lorsque l'attribut Configuration UNID est réglé sur «Pas de propriétaire, accepte tout propriétaire», les appareils de sécurité FSCP 2/1 doivent saisir la première source de configuration (Forme 1 et/ou Configure_Request) comme étant le propriétaire. (voir Tableau 31).

La valeur CFUNID est utilisée conjointement à la valeur OUNID qui accompagne la Configure_Request ou une fonction SafetyOpen de forme 1. Voir le Tableau 31 pour la définition de la méthode utilisée par les appareils pour répondre aux divers services basés sur 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 réglé sur toutes les valeurs FF_{hex}, l'attribut OUNID de Configure_Request doit être égal à cette valeur pour traiter la commande.

Tableau 31 – Synthèse du comportement des appareils pour diverses valeurs CFUNID

Service	Valeur de CFUNID		
	FF _{hex}	00 _{hex}	OUNID
Configure_Request (FF _{hex}) de SNCT	Acceptation	Acceptation Définir CFUNID = FF _{hex}	Échec
Configure_Request (OUNID)	Échec	Acceptation Définir CFUNID = OUNID	Accepter uniquement si CFUNID = OUNID Échec à défaut
SafetyOpen de forme 1	Échec	Acceptation Définir CFUNID = OUNID	Accepter uniquement si CFUNID = OUNID Échec à défaut

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 la configuration de sécurité (SCCRC) + la datation de la configuration de sécurité (SCTS). Ces valeurs sont obtenues à partir 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 réglé sur 0 et maintenu à cette valeur (par l'intermédiaire de cycles d'alimentation) jusqu'à exécution satisfaisante de Validate (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.

L'attribut UNID Cible du programme de contrôle de sécurité doit toujours refléter soit l'UNID cible par défaut ou courante que le processus de paramétrage UNID a sauvegardée.

L'UNID d'un appareil doit être archivé dans la mémoire non volatile NV comme partie intégrante de la procédure de paramétrage UNID.

L'UNID d'un appareil doit être archivé 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 UNID.

La mémoire non volatile d'un appareil présentant un état par défaut du fabricant doit comporter une valeur UNID non valide (par exemple FF_{hex}, FF_{hex}, FF_{hex}, FF_{hex}, FF_{hex}, FF_{hex}).

L'UNID d'un appareil doit être lu à partir de la mémoire non volatile lors de la mise sous tension, puis téléchargé sur un attribut de l'objet Programme de contrôle de sécurité et 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 l'état "out-of-box"), ce nombre doit être comparé au NodeID. En cas d'adaptation, la procédure de démarrage de l'appareil se poursuit. En cas de défaut d'adaptation, l'appareil passe à l'état Abandon (Abort).

Lorsque la défaillance d'un appareil a pour origine le défaut d'adaptation du paramétrage Commutation mémoire non volatile (Switch-NV), cet appareil doit permettre soit une réinitialisation sur l'état out-of-box, soit la transmission d'une demande Récupération (Recover) au programme de contrôle de sécurité afin de supprimer la fonction Abandon. Dans les deux cas, l'appareil doit passer à l'état «Attente de 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 (NV) doit s'effectuer avec une intégrité de sécurité.

6.6.5.20 Proposition de TUNID (OUNID)

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". Une fois l'application achevée, cet attribut doit être réglé de nouveau sur la valeur par défaut out-of-box 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 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 de chaque ressource, cet attribut prend la forme d'une structure permettant le maintien séparé de chaque ressource. La ressource est identifiée par une adresse de Segment logique.

La valeur par défaut pour tous les OCPUNID doit être 0 (accepte tout propriétaire), chaque ePath étant dirigé vers la ressource respective.

6.6.6 Sous-classes

Chaque sous-classe de niveau d'instance donne une signification unique pour un intervalle de recouvrement d'identifiants d'attributs instance et/ou de services instance. L'intervalle 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 32. Les services spécifiques de l'objet Programme de contrôle de sécurité sont définis dans le Tableau 33.

Tableau 32 – Services communs du programme de contrôle de sécurité

Code de service	Mise en œuvre nécessaire		Nom de service	Description du service
	Classe	Instance		
0E _{hex}	Conditionnel	Exigé	Get_Attributes_Single	Renvoie le contenu de l'attribut spécifié
010 _{hex}	n/a	Exigé	Set_Attributes_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, tel que spécifié par le fabricant.

Tableau 33 – Services spécifiques de l'objet Programme de contrôle de sécurité

Code de service	Mise en œuvre nécessaire		Nom de 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

Code de service	Mise en œuvre nécessaire		Nom de service	Description du service
	Classe	Instance		
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 exigé, Types 1 et 2 Conditionnel ^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 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 l'état out-of-box
57 _{hex}	n/a	Conditionnel ^d	Apply_TUNID	Permet d'effectuer pleinement le paramétrage TUNID
^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 Doit être mis en œuvre pour les appareils de sécurité FSCP 2/1 qui prennent en charge l'interface SNCT, mais vivement recommandé pour les appareils configurables par la fonction SafetyOpen de forme 1, mais qui ne prennent pas en charge l'interface SNCT.				

L'appareil peut solliciter l'existence d'un service instance de Programme de contrôle de sécurité en interne, tel que 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 d'appareils 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_Diagnostics 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 dépendant de l'appareil ne relèvent pas du domaine d'application de la présente partie.

6.6.7.4 Service Configure_Request

Le service Configure_Request permet de faire passer les objets d'application d'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 retournée 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 d'appareil cible et l'UNID du point d'origine. Ces valeurs sont adaptées aux mots de passe, TUNID et 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 doit accepter uniquement les messages de configuration destinés aux objets relatifs à la sécurité sur «cette seule connexion». Les tentatives d'écriture d'autres messages destinés aux objets relatifs à la sécurité 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 34.

Tableau 34 – 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 d'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'UNID de l'appareil

Un code d'erreur «Paramètre invalide» (20_{hex}) doit être retourné en cas d'erreur de défaut d'adaptation TUNID ou 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 retourné en cas de défaut d'adaptation de 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 retournée. Dans le cas contraire, une réponse «réussite» est retournée. Voir la Figure 10 et la 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 archive le SCID final dans l'attribut 26 du Programme de contrôle de sécurité.

La structure du message Validate_Configuration est définie dans le Tableau 35.

Tableau 35 – 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 tel que calculé par le logiciel. Cette proposition est validée par l'appareil
SCTS	6 OCTETS	Datation de 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 aboutie (Success Validate Reply) est définie dans le Tableau 36.

Tableau 36 – 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 tel que calculé par l'appareil
SCTS	6 OCTETS	Datation de configuration de sécurité. Cette valeur reflète les données transmises dans la demande Validation

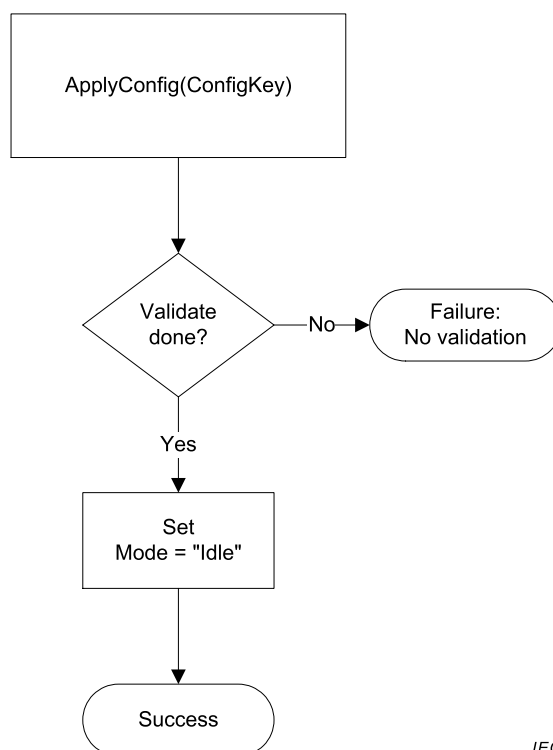
En cas d'échec de la commande Validate_Configuration du Programme de contrôle de sécurité, la réponse d'erreur doit transmettre une "erreur de validation" définie par la classe (D0_{hex}). Le code d'erreur suivant présenté dans le Tableau 37 est défini comme une erreur de validation dans le Programme de contrôle de sécurité, les codes d'erreur supplémentaires sont définis dans le Tableau 38.

Tableau 37 – Code d'erreur Validate_Configuration

Code d'erreur général	Code d'erreur supplémentaire	Nom d'erreur	Description
D0 _{hex}	Voir Tableau 38	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 38 – Codes étendus Validate_Configuration

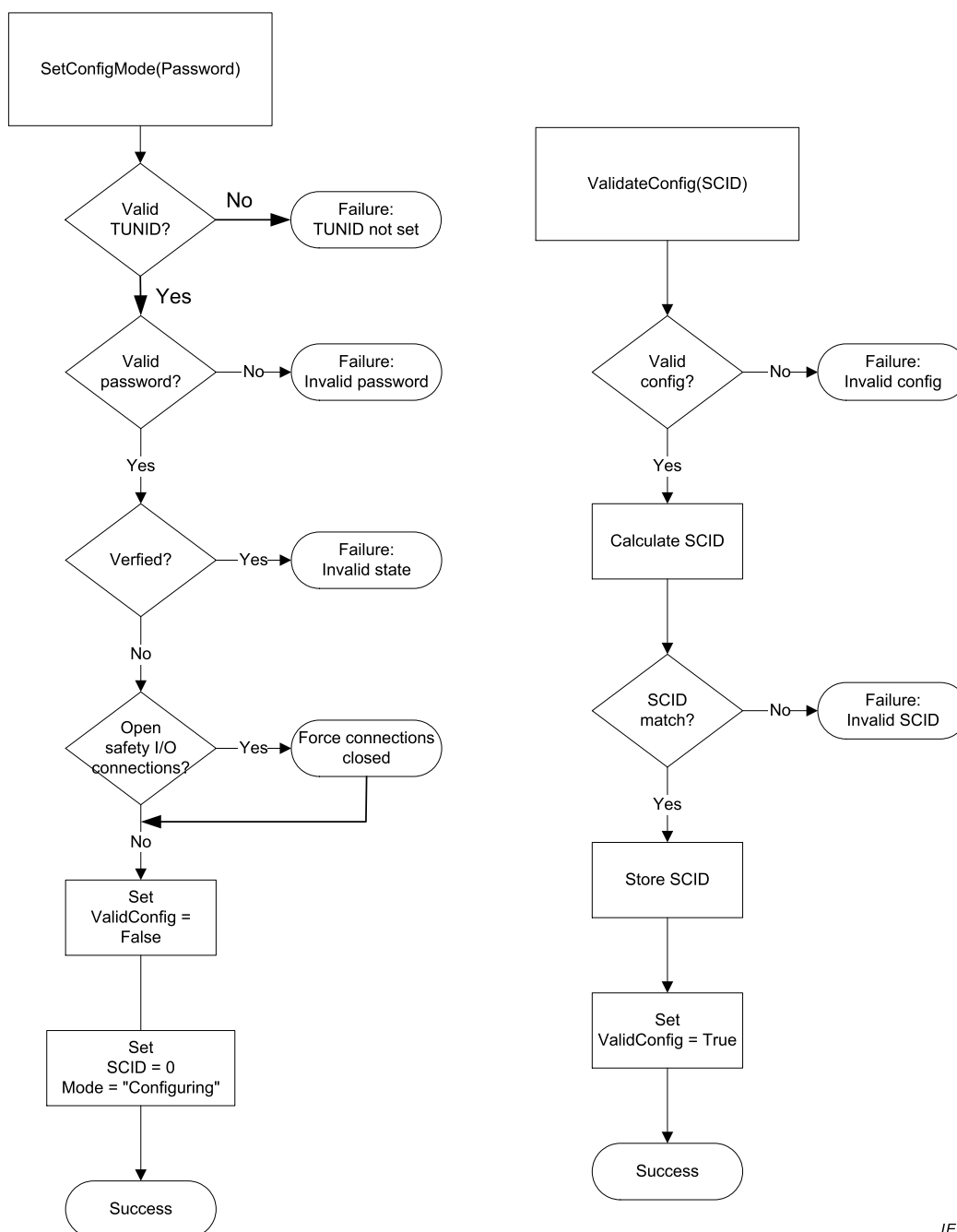
Codes d'erreur supplémentaires	Code de raison	Description
1	Défaut d'adaptation CRC	Il s'agit du code supplémentaire non spécifique par défaut, en l'absence de toute autre information supplémentaire et lorsque le CRC de configuration ne correspond pas à la valeur transmise
2	Paramètre de configuration 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 Ceci peut se produire même en cas de mise en correspondance des CRC.
3	TUNID non défini	Ce code peut être utilisé pour indiquer que l'appareil est en attente de l'état TUNID et que son TUNID doit être défini



IEC

Anglais	Français
ApplyConfig (ConfigKey)	Application de la configuration (clé de configuration)
Validate done?	Validation réalisée?
No	Non
Failure: no validation	Échec: pas de validation
Yes	Oui
Set Mode = "idle"	Définir Mode = "Repos"
Success	Réussite

Figure 10 – Application de configuration d'appareil



IEC

Anglais	Français
SetConfigMode (Password)	Définition du mode de configuration (Mot de passé)
Valid TUNID?	TUNID valide?
No	non
failure: TUNID not set	échec: TUNID non défini
yes	oui
valid password?	mot de passe valide?
failure: invalide password	échec: mot de passe invalide
vaid config?	config valide?
failure: invalid config	échec: config invalide
verified?	vérifié?
failure: invalid state	échec: état invalide

Anglais	Français
SetConfigMode (Password)	Définition du mode de configuration (Mot de passé)
calculate SCID	calculer SCID
openSafety I/O connections?	connexions E/S SafetyOpen
force connections closed	forcer les connexions fermées
SCID match?	SCID adapté?
failure: invalid SCID	échec: SCID invalide
set	définir ...
store SCID	archiver SCID
success	réussite

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 mot de passe 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 de mot de passe Current (courant) est réglé sur la valeur par défaut Out-of-box (zéro).

La structure de Set_Password est définie dans le Tableau 39.

Tableau 39 – 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 retourné en cas de défaut d'adaptation 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 de caractères réduits par rapport au 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 dans un appareil. Le contenu exact et l'usage sont spécifiques au fournisseur afin de protéger l'intégrité des mots de passe. Ce service requiert l'utilisation de 1 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. Le contenu des données du fournisseur est supposé être unique 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 40.

Tableau 40 – 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 contenant d'autres données nécessaires à la réinitialisation du mot de passe

En cas d'erreur «Taille de données» au niveau de 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 retourné.

Un code d'erreur «Violation de privilège» (0F_{hex}) doit être retourné en cas de défaut d'adaptation des données du fournisseur lors du traitement d'une commande Reset_Password du Programme de contrôle de sécurité.

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 requiert 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 d'adaptation du mot de passe. Une erreur «Défaut d'adaptation de mot de passe» est retournée en cas de défaut d'adaptation du mot de passe.

La structure de Configuration_Lock/Unlock est définie dans le Tableau 41.

Tableau 41 – Configuration_Lock/Unlock message structure

Nom	Type de données	Description
Code de service	USINT	52 _{hex}
Valeur	BOOL	0 = non verrouillé, 1 = verrouillé
Mot de passe	16 OCTETS	
TUNID	10 OCTETS	UNID d'appareil cible. Permet de détecter les demandes mal acheminées

En cas de défaut d'adaptation de TUNID de la commande Configuration_Lock/Unlock du Programme de contrôle de sécurité, le code d'erreur (020_{hex}) "Paramètre invalide" doit être retourné.

Un code d'erreur «Violation de privilège» (0F_{hex}) doit être retourné en cas de défaut d'adaptation du mot de passe lors du traitement de la commande Configuration_Lock/Unlock du Programme de contrôle de sécurité.

6.6.7.9 Service de changement de mode

Le service Changement de mode est utilisé par les appareils devant 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 42.

Tableau 42 – 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 retourné en cas de défaut d'adaptation du mot de passe de la commande «Changement de mode» du Programme de contrôle de sécurité.

6.6.7.10 Service Safety_Reset

Ce service 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 retournée si l'attribut Configuration_Lock est défini.

La structure de Safety_Reset est définie dans le Tableau 43.

Tableau 43 – Structure de message Safety_Reset

Nom	Type de données	Description
Code de service	USINT	54 _{hex}
Type de réinitialisation	USINT	Voir Tableau 44
Mot de passe	16 OCTETS	
TUNID	10 OCTETS	UNID d'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 est inclus uniquement lorsque le type de réinitialisation est 2. Voir Tableau 45.

En cas de défaut d'adaptation de TUNID lors de la transmission de la commande Réinitialisation de sécurité du Programme de contrôle de sécurité, le code d'erreur (20_{hex}) «Paramètre invalide» doit être retourné.

Un code d'erreur «Violation de privilège» (0F_{hex}) doit être retourné en cas de défaut d'adaptation du mot de passe lors du traitement d'une commande «Réinitialisation de sécurité» du Programme de contrôle de sécurité.

Tableau 44 – Types de réinitialisation de sécurité du Programme de contrôle de sécurité

Valeur:	Type de réinitialisation
0	Émule 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 out-of-box, sauf pour protéger les paramètres indiqués par l'attribut Mode point, puis émule le mieux possible la puissance d'itération (des cycles)

Tableau 45 – Paramètre d'attribut Mode point

Bit	Affectations de l'attribut Mode point
0	Lorsque défini, protège le MACID défini par le logiciel
1	Lorsque défini, protège le débit en bauds défini par le logiciel
2	Lorsque défini, protège le TUNID
3	Lorsque défini, protège le mot de passe
4	Lorsque défini, protège le CFUNID
5	Lorsque défini, protège le OCPUNID
6	Réservé, toujours 0
7	Utilise la mise en correspondance étendue (à définir ultérieurement)

Le Tableau 46 indique de quelle manière un appareil de sécurité doit traiter les différents types de réinitialisation basés sur la condition Verrouillage/Déverrouillage et sur l'état de connexion de sécurité.

Tableau 46 – Règles de traitement applicables aux types de réinitialisation

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/état	Réponse d'erreur de mode/état	Traitement et réponse	Traitement et réponse
Type 1	Réponse d'erreur de mode/état	Réponse d'erreur de mode/état	Réponse d'erreur de mode/état	Traitement et réponse
Type 2	Réponse d'erreur de mode/état	Réponse d'erreur de mode/état	Réponse d'erreur de mode/état	Traitement et réponse

6.6.7.11 Service Propose_TUNID

Le service Propose_TUNID établit une proposition de paramétrage 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 doit être accepté uniquement lorsque l'appareil cible est dans l'état "Waiting_for_TUNID".

Une fois que le TUNID est défini avec succès, il peut passer à l'état Configuration.

Le NodeID du TUNID doit être adapté au 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 47.

Tableau 47 – Service Propose_TUNID

Nom	Type de données	Description
Code de service	USINT	56 _{hex}
TUNID	10 OCTETS	Proposition de valeur UNID d'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 48 et un organigramme de traitement est défini à la Figure 12.

Tableau 48 – Service Apply_TUNID

Nom	Type de données	Description
Code de service	USINT	57 _{hex}
TUNID	10 OCTETS	Proposition de valeur UNID d'appareil cible

Le service Apply_TUNID doit valider le TUNID par rapport à la valeur proposée. Il interrompt également le clignotement LED, sauvegarde le TUNID dans la mémoire non volatile, actualise l'attribut TUNID dans le Programme de contrôle, et règle l'attribut proposed_TUNID sur toutes les valeurs FF_{hex}. Le Programme de contrôle doit alors passer à l'état Configuration.

Le pseudo-code suivant définit le comportement du service Apply_TUNID:

```

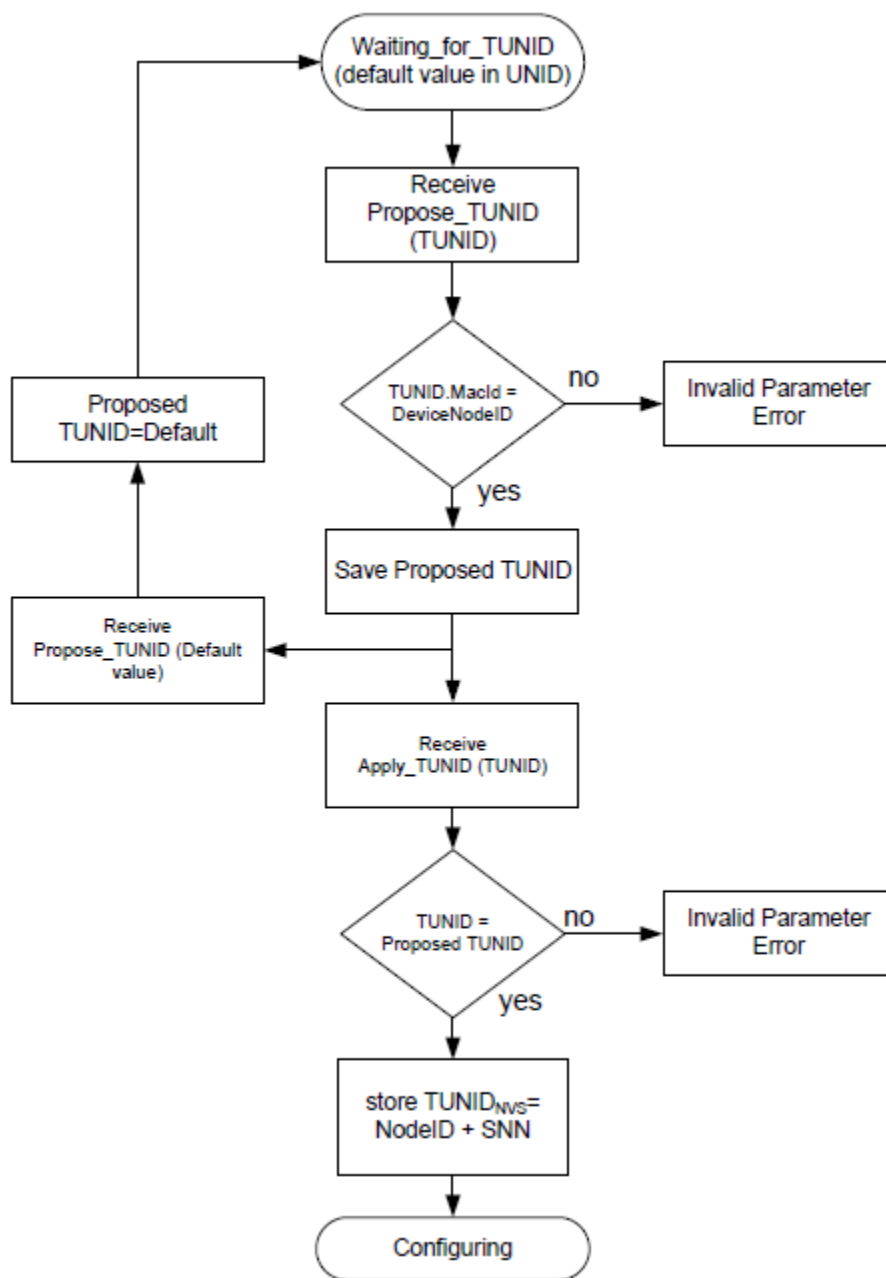
Apply_TUNIDHandler()
{
  IF (Device_State=Waiting_for_TUNID)
    THEN IF {(Apply_TUNID[TUNID] != all FFhex)
      AND (TUNIDProposedAttr == Apply_TUNID[TUNID])
        THEN
          Stop Flash Sequence
          Target_UNID = TUNIDProposedVar[TUNID]
          //NV Memory operation

```

```

// 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
}

```



IEC

Anglais	Français
Waiting_for_TUNID (default value in UNID.)	Waiting_for_TUNID (valeur par défaut dans UNID)
receive ...	réception ...

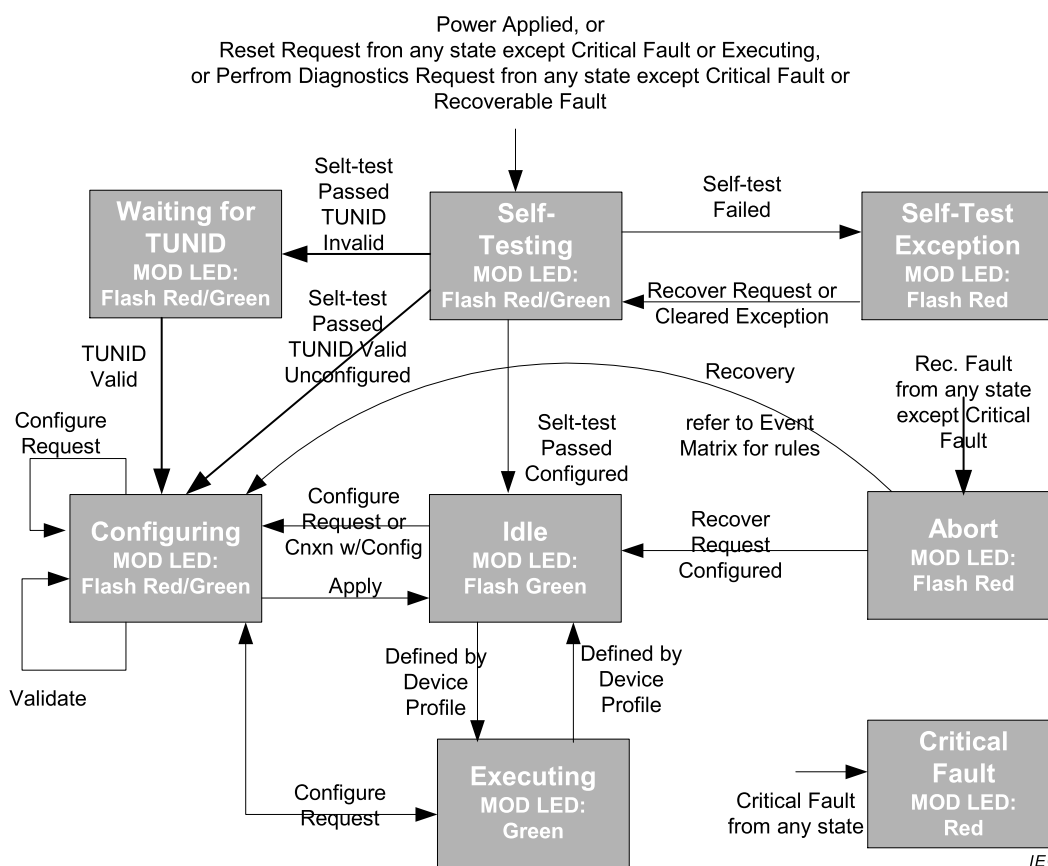
Anglais	Français
default	par défaut
no	Non
yes	Oui
invalid parameter error	erreur de paramètre invalide
save	sauvegarde ...
store	archive ...
configuring	configuration

Figure 12 – Traitement UNID pendant l'état "Waiting for TUNID"

6.6.8 Comportement du Programme de contrôle de sécurité

6.6.8.1 États de l'objet Programme de contrôle de sécurité

La Figure 13 indique 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 49.



Anglais	Français
power applied, or Reset Request from any state except Critical Fault or Executing, or Perform Diagnostic Request from any state except Critical Fault or Recoverable Fault	alimentation appliquée ou demande de réinitialisation de tout état, sauf Anomalie critique ou Exécution, ou exécution demande de diagnostic de tout état, sauf Anomalie critique ou Anomalie récupérable
self-test passed	autovérification réussie
invalid	invalide
waiting for	attente de
flash red/green	rouge/vert clignotant

Anglais	Français
self-testing	autovérification
self-test failed	échec de l'autovérification
recover request or cleared exception	demande de récupération ou exception supprimée
flash red	rouge clignotant
valid	valide
unconfigured	non configuré
configured	configuré
or	ou
recovery	récupération
refer to event matrix for rules	se reporter à la matrice d'événements pour les règles
rec. fault from any state except critical fault	anomalie récupérable de tout état, sauf anomalie critique
configuring	configuration
apply	application
idle	repos
abort	abandon
validate	validation
defined by device profil	défini par le profil d'appareil
executing	exécution
critical fault from any state	anomalie critique de tout état
critical fault	anomalie critique
red	rouge
green	vert

Figure 13 – Diagramme d'états du Programme de contrôle de sécurité**Tableau 49 – Événements liés au Programme de contrôle de sécurité**

État	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, doit être spécifié 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'État 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 protégés par des cycles d'alimentation
Abandon	L'instance objet est dans l'état Abandon; l'adoption de cet état est possible uniquement par 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 de TUNID	L'appareil quitte l'état d'autovérification et détermine que le TUNID archivé dans la mémoire non volatile a une valeur par défaut out-of-box. Il reste dans cet état jusqu'à l'achèvement satisfaisant de la séquence de paramétrage TUNID (c'est-à-dire opération de proposition/application dans l'interface SNCT). L'appareil peut alors être configuré

État	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 prudents protégés par des cycles d'alimentation
Anomalie critique	L'objet (et l'appareil) sont dans un état d'anomalie à partir duquel aucune récupération ne se produit. Les services d'objet ne peuvent pas être traités. Les conditions nécessaires à la sortie d'un état d'anomalie critique ne relèvent pas du domaine d'application de la présente partie

La valeur de l'attribut État 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 de la présente partie.

6.6.8.2 Matrice d'événements d'état du Programme de contrôle de sécurité

Le Tableau 50 définit les états et événements applicables au Programme de contrôle de sécurité

Tableau 50 – Matrice d'événements d'état du Programme de contrôle de sécurité

Événement	État							
	Attente de TUNID	Configuration (État de sécurité)	Repos (État de sécurité)	Autovérification (État de sécurité)	Exception d'autovérification (État de sécurité)	Exécution	Abandon (État de sécurité)	Anomalie critique (État de sécurité)
Alimentation appliquée			--	Le point d'entrée par défaut effectue son processus d'application d'autovérification	--	--	--	Transition vers l'AUTOVERIFICATION
Autovérification réussie			Non applicable	Transition vers le dernier état sauvegardé s'il ne s'agit pas de l'état out-of-box À défaut, Attente de TUNID	Non applicable	Non applicable	Non applicable	Non applicable
Échec de l'autovérification			Non applicable	Définition des bits d'état d'exception appropriés et transition vers l'état EXCEPTION DE L'AUTO-VERIFICATION	Non applicable	Non applicable	Non applicable	Non applicable
Proposition de TUNID	Validation des paramètres et du diagramme LED FlashNet	Erreur OSC ^b	Erreur OSC ^b	Erreur OSC ^b	Erreur OSC ^b	Erreur OSC ^b	Erreur OSC ^b	Erreur OSC ^b

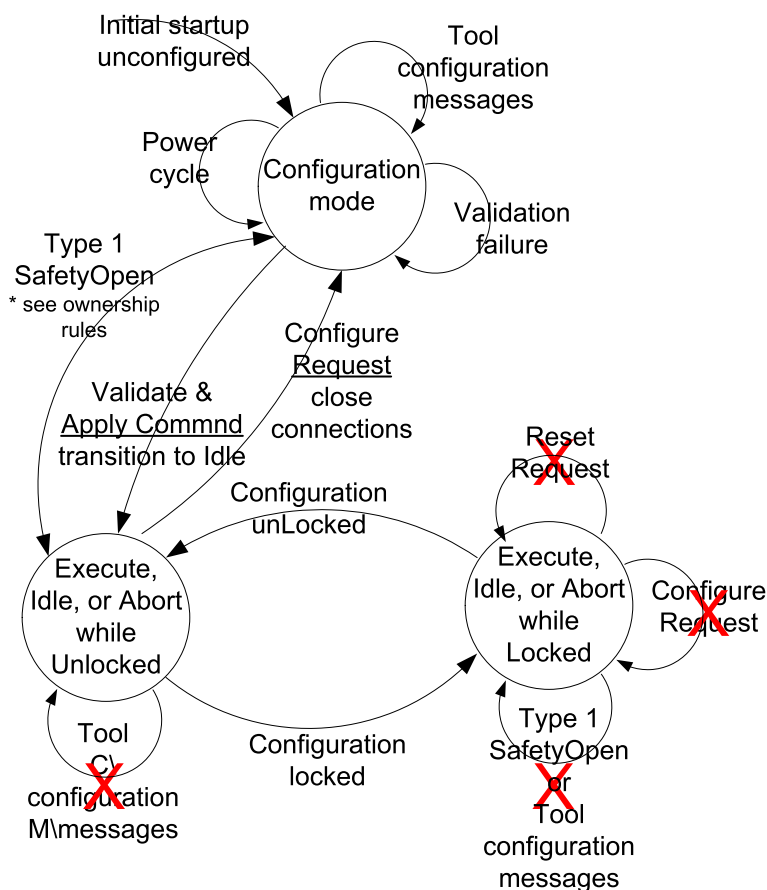
Événement	État							
	Attente de TUNID	Configuration (État de sécurité)	Repos (État de sécurité)	Autovérification (État de sécurité)	Exception d'autovérification (État de sécurité)	Exécution	Abandon (État de sécurité)	Anomalie critique (État de sécurité)
Application de TUNID	Sauvegarde de TUNID dans 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 AUTO-VERIFICATION	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	Transition vers l'état Configuration , Si non verrouillé	Erreur OSC ^b	Erreur OSC ^b	Retrait des connexions, Si non verrouillé 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 défaut d'adaptation Commutateur/TUNID Erreur OSC ^b	Erreur OSC ^b
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 forme 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 fonction du profil	Erreur OSC ^b	Erreur OSC ^b	Retrait des connexions, transition vers l'état Configuration, adoption de l'état REPOS/EXÉCUTION fonction du profil	Erreur OSC ^c	Erreur OSC ^b
Demande de réinitialisation	Traitement de type Transition vers l'AUTO-VERIFICATION	Traitement de type Transition vers l'AUTO-VERIFICATION	Traitement de type si non verrouillé Transition vers l'AUTO-VERIFICATION	Traitement de type Transition vers l'AUTO-VERIFICATION	Traitement de type Transition vers l'AUTO-VERIFICATION	Traitement de type Si non verrouillé, Transition vers l'AUTO-VERIFICATION	Traitement de type Si non verrouillé Transition vers l'AUTO-VERIFICATION	Traitement de type Transition vers l'AUTO-VERIFICATION

Événement	État							
	Attente de TUNID	Configuration (État de sécurité)	Repos (État de sécurité)	Autovérification (État de sécurité)	Exception d'autovérification (État de sécurité)	Exécution	Abandon (État de sécurité)	Anomalie critique (État de sécurité)
Demande 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 Récupération	Erreur OSC ^b	Erreur OSC ^b	Erreur OSC ^b	Nouvelle AUTO-VERIFICATION	Transition vers l'AUTO-VERIFICATION	Erreur OSC ^b	Si configuré: Transition vers l'état REPOS --- Non configuré: Transition vers l'état Configuration --- Si défaut d'adaptation Commutateur//TUNID Erreur OSC ^b	Erreur OSC ^b
Exécution de la demande Diagnostic	Erreur OSC ^b	Erreur OSC ^b	Transition vers l'AUTO-VERIFICATION	Nouvelle AUTO-VERIFICATION	Transition vers l'AUTO-VERIFICATION	Erreur OSC ^b	Exécution de tous les essais de diagnostic	Erreur OSC ^b
Échec 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	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	Erreur OSC ^b
Définitions des LED applicables aux états								
LED 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 0C _{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.								

L'appareil peut solliciter l'existence d'un service instance de Programme de contrôle de sécurité en interne, tel que 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 rejeteront toutes les tentatives de modification des données de configuration qui affectent le SCID.



IEC

Anglais	Français
initial startup unconfigured	démarrage initial non configuré
tool configuration messages	messages de configuration par outil
power cycle	cycle d'alimentation
configuration mode	mode configuration
validation failure	échec de la validation
type 1 SafetyOpen	SafetyOpen type 1
see ownership rules	voir règles de propriété
configure request	demande de configuration
close connections	fermer les connexions
validate & apply command	commande Validation & Application
transition to Idle	transition vers Repos
configuration unLocked	configuration non verrouillée
reset request	demande Réinitialisation
execute, idle, or abort while	exécution, repos ou abandon lorsque
unlocked	non verrouillé
locked	verrouillé

Anglais	Français
configure request	demande de Configuration
tool C	C outil
configuration M\messages	M\messages de configuration
configuration locked	configuration verrouillée
or tool configuration messages	ou messages de configuration par outil

Figure 14 – Relations entre configuration, essais et verrouillage

Le Tableau 51 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 forme 1, ladite configuration étant effectuée par le point d'origine ayant l'UNID du propriétaire. Un appareil verrouillé ne peut jamais être configuré sans tenir compte de son propriétaire.

Tableau 51 – Contrôle du propriétaire de configuration par rapport à l'état de l'appareil

Règles de propriété	Mode de configuration	Mode Exécution/Repos non verrouillé	Mode Exécution/Repos verrouillé
Configuration avec propriétaire (Config. OUNID = UNID du propriétaire)	Forme 1 acceptée par le seul propriétaire	Forme 1 acceptée par le seul propriétaire	Toutes les formes 1 refusées
Configuration sans propriétaire (Config. OUNID = 0)	Forme 1 acceptée par quiconque	Forme 1 acceptée par quiconque	Toutes les formes 1 refusées
Outil SW détenu (Config. OUNID = toutes les valeurs FF _{hex})	Aucune forme 1 acceptée	Aucune forme 1 acceptée	Toutes les formes 1 refusées

6.6.8.4 Mapping des états de l'objet Programme de contrôle de sécurité et de l'objet Identité

Le Tableau 52 définit le mapping entre les états du Programme de contrôle de sécurité et 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 52 – Mapping des états du Programme de contrôle de sécurité et de 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 de TUNID	En attente
Exécution	Opérationnel
Abandon	Principalement récupérable
Anomalie critique	Principalement non récupérable

6.6.8.5 Mapping des événements des objets Programme de contrôle de sécurité et Identité

Le Tableau 53 décrit le mapping des événements du Programme de contrôle de sécurité définis et 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 53 – Mapping des événements de l'objet Programme de contrôle de sécurité

Mapping des événements d'état du Programme de contrôle de sécurité avec ->	Événement d'identité équivalent
Alimentation appliquée	Alimentation appliquée
Échec de l'autovérification	Essais non satisfaits
Autovérification satisfaite	Essais satisfaits
Proposition de TUNID	Aucun événement équivalent
Application de 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 forme 1	Aucun événement équivalent
Demande Réinitialisation	Réinitialisation
Abandon (Interne)	Anomalie principale récupérable
Demande Récupération	Anomalie corrigée
Exécution de la demande Diagnostic	Aucun événement équivalent
Échec de la connexion de sécurité	Désactivé
Connexion de sécurité établie	Activé
Connexion de sécurité supprimée	Aucun événement équivalent
Changement de mode	Aucun événement équivalent
Restauration	Aucun événement équivalent
Verrouillage/Déverrouillage	Aucun événement équivalent

6.6.8.6 Mapping des événements des objets Identité et Programme de contrôle de sécurité

Le Tableau 54 décrit le mapping des conditions d'événements définies des objets Identité avec les événements équivalents définis pour l'objet Programme de contrôle de sécurité. Ce mapping des événements définit les événements équivalents entre ces objets. Ce mapping est fourni uniquement 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 54 – Mapping des événements d'objet Identité

Mapping des événements d'identité avec ->	Événements de Programme de contrôle de sécurité
Alimentation appliquée	Alimentation appliquée
Essais non satisfaits	Échec de l'autovérification
Essais satisfaits	Autovérification satisfaite
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

6.7 Objet de validation de sécurité

6.7.1 Généralités

Code de classe: 3Ahex

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 Validation de sécurité est d'agir comme gestionnaire de transport de sécurité des multiples connexions CPF 2 de faible niveau qui ensemble constituent une connexion de sécurité complète.

L'appareil contenant l'Objet de validation de sécurité peut créer plusieurs instances de l'Objet de validation de sécurité 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: Point à point et multipoints. 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 55.

Tableau 55 – 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 IEC 61158-5-2 et 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: l'attribut Comptage des anomalies de connexion de sécurité de l'Objet de validation de sécurité doit représenter le cumul (avec auto-remplacement) des fréquences d'occurrence d'une anomalie des 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 incorporées au programme ou obtenues à partir du processus d'établissement des connexions dynamiques. La seule valeur d'attribut définissable est le diagnostic de l'âge maximal des données (Max Data Age). Une liste complète des attributs instance est définie dans le Tableau 56.

Tableau 56 – 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		État de l'Objet de validation de sécurité	USINT	État 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'intervalle Ping	UINT	Nombre qui définit le Ping_Count_Interval pour une connexion particulière	16 à 1 000
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 max. de consommateurs pour les producteurs multipoints, et à 1 pour le consommateur point à point et multipoints	
				Multiplicateur minimal de messages de coordination temporelle	MATRIC E de: UINT	Nombre minimum d'incrément de 128 µs susceptible d'être utilisé pour un message de coordination temporelle pour le passage du consommateur au producteur	0 – 7 813
5	Facultatif	Obtenir		Multiplicateur de délai du réseau	STRUCT . de:		
				Taille de matrice de multiplicateurs de délai du réseau	USINT	La taille de la matrice est égale au nombre max. de consommateurs pour les producteurs multipoints, et à 1 pour le consommateur point à point et multipoints	
				Multiplicateur de délai du réseau	MATRIC E de: UINT	Nombre maximum d'incrément de 128 µs qu'un consommateur doit permettre à l'âge des données de sécurité d'atteindre	0 – 45 313
6	Facultatif	Obtenir		Multiplicateur de temporisation	STRUCT . de:		
				Taille de matrice de multiplicateurs de temporisation	USINT	La taille de la matrice est égale au nombre max. de consommateurs pour les producteurs multipoints, et à 1 pour le consommateur point à point et multipoints	

ID d'attribut	Mise en œuvre nécessaire	Règle d'accès	NV	Nom	Type de données	Description de l'attribut	Sémantique de la valeur
				Multiplicateur de temporisation	MATRIC E de: USINT	Détermine le nombre de messages susceptibles d'être perdus préalablement à toute déclaration d'erreur de connexion	Format de base: 1-4 Format étendu: 1-255
7	Facultatif	Obtenir		Nombre maximal de consommateurs	USINT	Nombre de consommateurs maximum admis pour la connexion	1 (Point à point) 2-15 (Multipoints)
8	Facultatif ^a	Obtenir		Instance de connexion de données	UINT	ID d'instance de connexion de la connexion de données de sécurité	
9	Facultatif ^a	Obtenir		Instance de connexion de coordination	STRUCT . de:	ID d'instance de connexion de la connexion de coordination de sécurité	1-nombre max. de connexions de l'appareil
				Taille de matrice d'instances de connexion de coordination	USINT	La taille de la matrice est égale au nombre max. de consommateurs pour les producteurs multipoints, et à 1 pour le consommateur point à point et multipoints	
				Instance de connexion de coordination	MATRIC E de: UINT		
10	Facultatif ^a	Obtenir		Instance de connexion de correction	UINT	ID d'instance de connexion de la connexion de correction de temps	0 (Lorsque non utilisé) 1-nombre max. de connexions de l'appareil
11	Facultatif ^a	Obtenir		Rattachement 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 rattachement)
12	Exigé	Définir		Âge max. des données	UINT	Diagnostic qui détient l'âge des données le plus élevé détecté dans des incréments de 128 µs. Attribut utilisé uniquement pour les consommateurs de sécurité	
13	Exigé	Obtenir		Chemin de données d'application	EPATH mis en paquets	Points de liaison avec les données d'application associées à cette connexion 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
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/Consommateur	STRUCT . de:		
				Taille de matrice de compteurs Producteur/Consommateur	USINT	La taille de la matrice est égale au nombre max. de consommateurs pour les producteurs multipoints, et à 1 pour le consommateur point à point et multipoints	
				Compteur des anomalies Producteur/Consommateur	MATRIC E de: USINT	Nombre d'anomalies détectées par ce compteur	Voir 6.7.3.14

^a Ces paramètres peuvent éventuellement être publiés. 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.

6.7.3.2 État de l'Objet de validation de sécurité

Cet attribut définit l'état courant de l'instance d'Objet de validation de sécurité. Les transitions propres à cet attribut d'état reflètent l'état courant de l'objet; les définitions sont fournies dans le Tableau 57. Cet attribut peut être utilisé pour déterminer la condition des connexions de sécurité établies

Tableau 57 – 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	Établi	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	Connexion_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 multipoints doivent avoir échoué. Le producteur reste dans l'état Etabli tant qu'un consommateur est toujours actif.
4-255	Réservé	

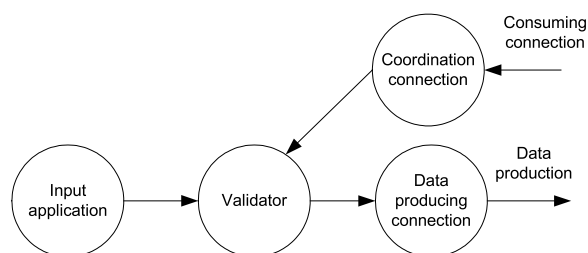
6.7.3.3 Type d'Objet de validation de sécurité

Cet attribut définit le type de transport utilisé par l'objet de validation de sécurité, dont la définition est donnée dans le Tableau 58. Les cibles doivent déduire cette valeur des paramètres de connexion de sécurité de la fonction SafetyOpen.

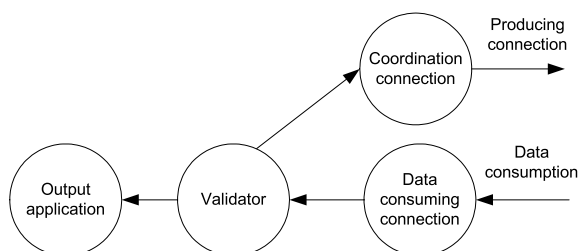
Tableau 58 – Type d'Objet de validation de sécurité, attributions de champs de bits

Bit 7	Bits 0 – 6
Producteur (client) = 0/ Consommateur (serveur) = 1	Type de connexion de sécurité: 0 = non attribué 1 = point à point 2 = Multipoints 3-127 = Réserve

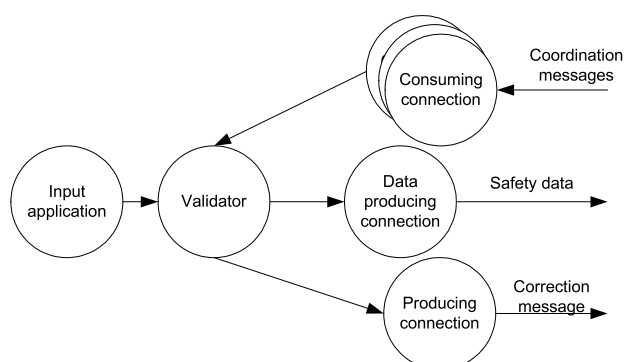
Les transports propres à chaque type d'Objet de validation de sécurité sont représentés à la Figure 15. Cet attribut peut être utilisé pour demander à un appareil de déterminer le type de connexion qui a été établie.



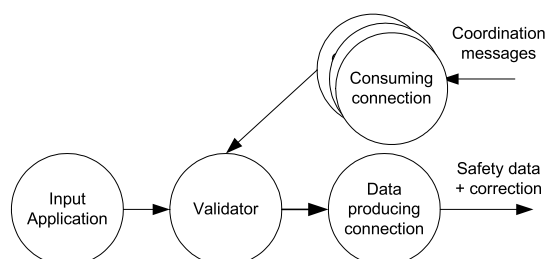
a) Single Cast Producer (Input) Connection Type 0x01



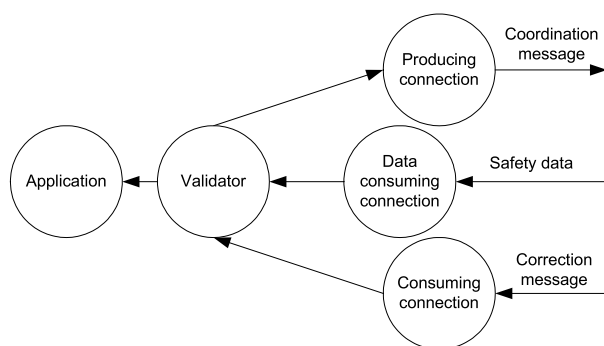
b) Single Cast Consumer (Output) Connection Type 0x81



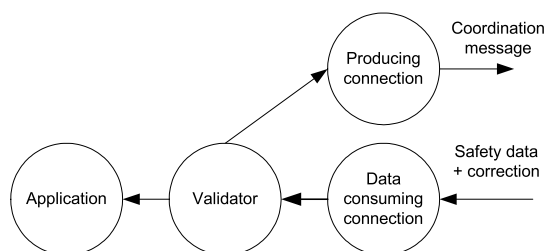
c) Multi-Cast Producer Connection on CP 2/3 Type 0x02



d) Multi-Cast Producer Connection Type 0x02



e) Multi-Cast Consumer Connection on CP 2/3 Type 0x82



f) Multi-Cast Consumer Connection Type 0x82

IEC

Anglais	Français
consuming connection	connexion de consommation
coordination connection	connexion de coordination
producing connection	connexion de production
input application	application d'entrée
validator	objet de validation
data producing connection	connexion de production de données
data production	production de données
output application	application de sortie
data consuming connection	connexion de consommation de données
data consumption	consommation de données

Anglais	Français
a)single cast producer (input) connection Type 0x01	connexion (entrée) de producteur monodiffusion de type 0x01
b)single cast consumer (output) connection Type 0x81	connexion (sortie) de consommateur monodiffusion de type 0x81
coordination messages	messages de coordination
safety data	données de sécurité
correction message	message de correction
c)multi-cast producer connection on CP 2/3 Type 0x02	connexion de producteur multidestinataires sur CP 2/3 type 0x02
d)multi-cast producer connection Type 0x02	connexion de producteur multidestinataires de type 0x02
e)multi-cast consumer connection on CP 2/3 Type 0x82	connexion de consommateur multidestinataires sur CP 2/3 type 0x82
f)multi-cast consumer connection Type 0x82	connexion de consommateur multidestinataires de type 0x82

Figure 15 – Types de connexion de sécurité

6.7.3.4 Multiplicateur EPI d'intervalle Ping

Cet attribut est utilisé comme partie intégrante de la fonction 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 59.

6.7.3.5 Multiplicateur minimal de messages de coordination temporelle

Cet attribut est utilisé comme partie intégrante de la fonction 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 59.

Tableau 59 – 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'intervalle 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 59.

6.7.3.7 Multiplicateur de temporisation

Cet attribut définit la tolérance de 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 provenant de consommateurs multiples sont définies dans le Tableau 59.

6.7.3.8 Nombre maximal de consommateurs

Cet attribut définit le nombre maximal de consommateurs autorisés à se connecter à un producteur multipoints (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 provenant de consommateurs multiples sont définies dans le Tableau 59.

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 attribué 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 Coordination temporelle. Cet attribut est attribué comme partie intégrante du processus d'établissement de la connexion.

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 attribué 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 est utilisé uniquement avec les points d'origine de connexion. Cet attribut peut être attribué comme partie intégrante du processus d'établissement de connexion ou incorporé au programme au moment de la conception.

6.7.3.13 Âge maximal des données

L'âge des données de paquets reçues est défini comme la différence entre l'horloge de 128 μ s du consommateur et la datation reçue au moment de la réception du paquet. L'attribut Âge 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 consommateur internes, dans le cas des connexions qui utilisent le format étendu.

Lorsque la connexion est une connexion de consommation EF, l'attribut Compteur d'anomalies de 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 60.

Tableau 60 – 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

6.7.5 Services instance

6.7.5.1 Présentation générale des services instance

Les services instance pris en charge par le l'objet de Validation de sécurité sont définis dans le Tableau 61.

Tableau 61 – 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 réinitialiser l'attribut Age maximum des données
4B _{hex}	Facultatif	Réinitialisation du code d'erreur	Utilisé pour réinitialiser l'attribut instance 14

6.7.5.2 Get_Attributes_All Response

Les données de réponse pour le service Get_Attributes_All sont définies dans le Tableau 62.

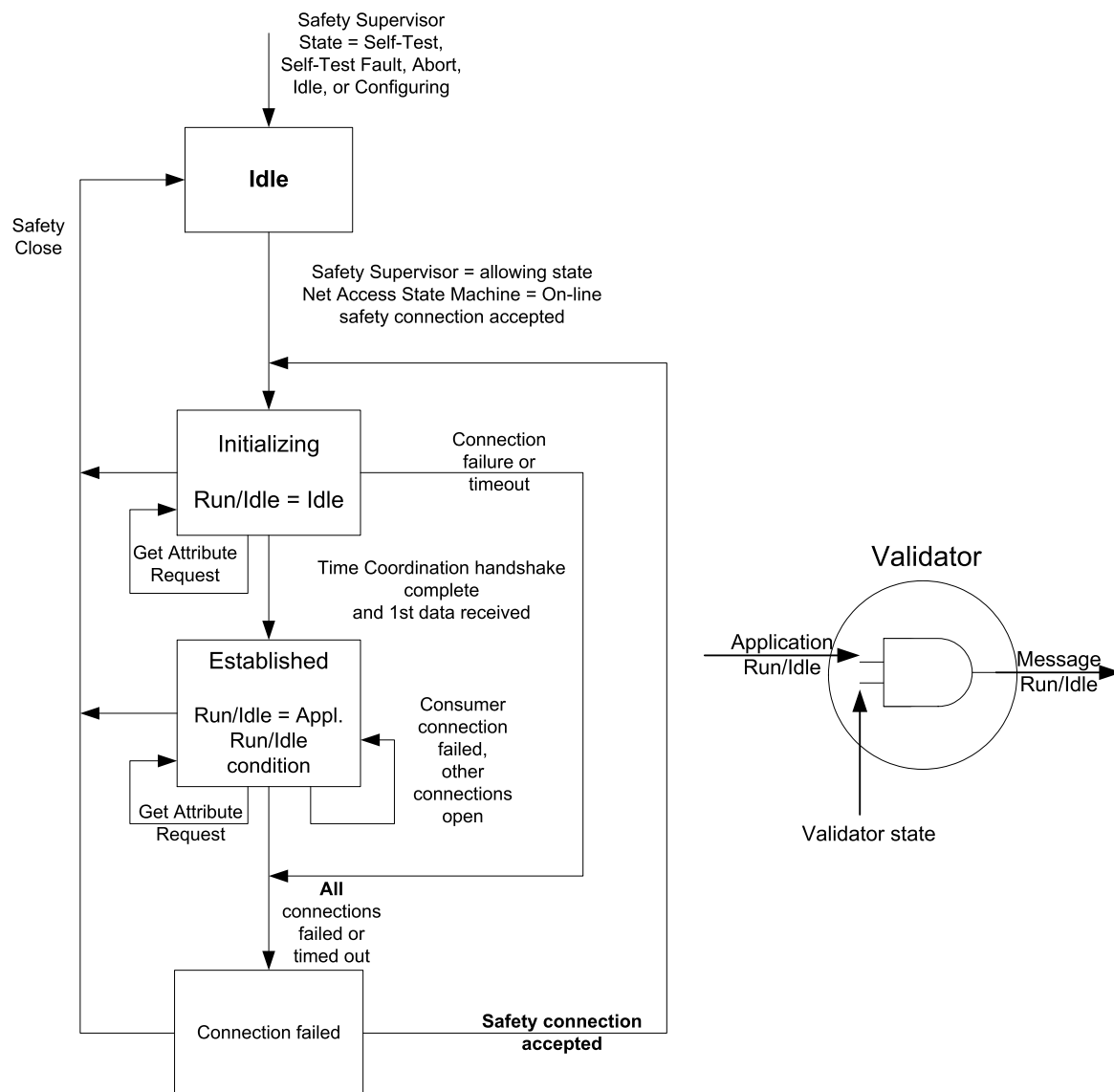
Tableau 62 – Données du service Get_Attributes_All de l'objet de Validation de sécurité

ID d'attribut	Nombre d'octets	Nom	Type de données
1	0	État de l'Objet de validation de sécurité	USINT
2	1	Type d'Objet de validation de sécurité	USINT
3	2,3	Multiplicateur EPI d'intervalle 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	Âge maximal des données	UINT
13	variable	Chemin d'application	EPATH
14		Code d'erreur	UINT

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 au Tableau 63.



IEC

Anglais	Français
safety supervisor State = Self-Test, Self-Test Fault, Abort, Idle, or Configuring	état du programme de contrôle de sécurité = autovérification, anomalie de l'autovérification, Abandon, Repos ou Configuration
safety close	fermeture de la sécurité
idle	repos
safety supervisor = allowing state Net Access State Machine = On-line safety connection accepted	programme de contrôle de sécurité = état d'autorisation diagramme d'états d'accès au réseau = connexion de sécurité en ligne acceptée
initialising	initialisation
run/idle = idle	Exécution/repos = repos
connection failure or timeout	échec de connexion ou temporisation
get attribute request	obtenir demande d'attribut
time coordination handshake complete and 1 st data received	transfert de coordination temporelle complet et premières données reçues
validator	objet de Validation
established	établi
run/idle = appl.	exécution/repos = appl.

Anglais	Français
application run/idle	exécution/repos d'application
message run/idle	exécution/repos des messages
run/idle condition	condition exécution/repos
consumer connection failed, other connections open	échec de connexion du consommateur, autres connexions ouvertes
validator state	état de l'objet de validation
all connections failed or timed out	échec de toutes les connexions ou temporisation
connection failed	échec de connexion
safety connection accepted	connexion de sécurité acceptée

Figure 16 – Diagramme de transitions d'état de l'Objet de validation de sécurité

6.7.6.2 REPOS (IDLE)

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 Établi

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 d'adaptation (c'est-à-dire que OUNID et le chemin d'application correspondent à une ressource de connexion).

6.7.6.6 Matrice d'événements d'état

Le Tableau 63 présente la matrice d'événements d'état qui définit le comportement de l'Objet de validation de sécurité. Le Tableau 64 met en correspondance les états de l'Objet de validation de sécurité et du Programme de contrôle de sécurité.

Tableau 63 – Matrice d'événements d'état de l'Objet de validation de sécurité

Événement	État			
	Repos	Initialisation	Exécution	Échec connexion
Alimentation appliquée et autovérification effectuée	État 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 multipoints, Initialisation de la connexion de sécurité	Si producteur multipoints, initialisation de la connexion de sécurité	Adaptation de OUNID et du chemin d'application, Si adaptation, transition vers l'état Initialisation
Transfert de coordination temporelle achevé	--	Transition vers l'état Exécution	Si producteur multipoints, Nouveau consommateur en ligne	--
Échec du consommateur dans un producteur multipoints tandis que d'autres consommateurs sont toujours en ligne	--	LED de l'état Net rouge clignotant	LED de l'état Net rouge clignotant	--
Échec de toutes les connexions	--	Échec de la transition vers l'état Connexion	Échec de la transition vers l'état Connexion	LED de l'état Net rouge clignotant
Adaptation de la demande de connexion du consommateur (c'est-à-dire que 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

Tableau 64 – Mapping des états des objets Programme de contrôle de sécurité et Validation de sécurité

Programme de contrôle de sécurité	Objet de validation de sécurité
Autovérification	Repos
Exception d'autovérification	Repos
Attente de TUNID	Repos
Repos	Repos ^a , Initialisation, Exécution, ou Connection_Failed
Configuration	Repos
Exécution	Repos ^a , état Initialisation ou Exécution, ou Connection_Failed
Abandon	Repos
Anomalie critique	Repos
^a Un Objet de validation de sécurité doit accepter des connexions uniquement lorsque l'état du Programme de contrôle de sécurité peut accepter les connexions dépendant de l'appareil (c'est-à-dire état Exécution uniquement, ou état Exécution/Repos). Un Objet de validation de sécurité peut être au repos tandis qu'un autre est toujours actif.	

6.8 Objet de configuration de connexion

6.8.1 Généralités

Ce paragraphe définit les extensions de l'Objet de configuration de connexion, de classe F3_{hex} pour FSCP 2/1. Voir l'IEC 61158-4-2 pour une définition complète.

Code de classe: F3hex

6.8.2 Extensions d'attributs de classe

Les attributs de classe destinés à être utilisés par les appareils FSCP 2/1 sont définis dans le Tableau 65.

Tableau 65 – Extensions d'attributs de classe d'objet de 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	Émission de signature	UDINT	Créé et utilisé par le logiciel de configuration pour détecter les modifications apportées aux valeurs d'attributs instance
a Cet attribut est exigé avec les seuls appareils qui n'utilisent pas l'interface SNCT de sécurité.					

6.8.3 Attributs, ajouts et extensions instances

Le Tableau 66 définit les attributs et modifications instances destinés à être utilisés par les appareils FSCP 2/1.

Tableau 66 – Ajouts/extensions d'attributs instance d'Objet de configuration de connexion

ID d'attribut	Mise en œuvre nécessaire	Règle d'accès	Mémoire non volatile	Nom	Type de données	Description de l'attribut	Sémantique de la valeur
9	Exigé	Définir	Mémoire non volatile	Mise en correspondance de données	STRUCT. de:		
				format_number	UINT	Ce numéro détermine le format de mise en correspondance utilisé	2 – 99 Réserve 100 – 199 Spécifiques au fournisseur. Toutes les autres valeurs sont Réservées
				Data_Map data_size	UINT	Taille, en octets, des informations de mise en correspondance	
				Data_Map_data	Matrice d'octets	Données de format de mise en correspondance de données basées sur le numéro de format	

ID d'attribut	Mise en œuvre nécessaire	Règle d'accès	Mémoire non volatile	Nom	Type de données	Description de l'attribut	Sémantique de la valeur
10	Facultatif	Définir	Mémoire non volatile	Config #2 Data2	STRUCT. de:		
				config_data_size	UINT	Longueur de config_data en octets	
				config_data	Matrice d'octets	Config #2 data	
11	Facultatif	Définir	Mémoire non volatile	ID d'appareil de remplacement	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	Mémoire non volatile	Désactivation de connexion	BOOL		0 – connexion activée. 1 – connexion désactivée. En cas de réception d'un service Ouverture, cette valeur doit être réglée sur 0. En cas de réception d'un service Fermeture ou Arrêt, cette valeur doit être réglée sur 1
13	Conditionnel ^a	Définir	Mémoire non volatile	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 portant 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		

ID d'attribut	Mise en œuvre nécessaire	Règle d'accès	Mémoire non volatile	Nom	Type de données	Description de l'attribut	Sémantique de la valeur
				EPI de correction de temps	UDINT		
				Paramètres de connexion de correction de temps	WORD		
				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 Exp. de temps réseau	UINT		
				Multiplicateur de temporisation	USINT		
				Nombre maximal de consommateurs	USINT		
14	Conditionnel ^a	Obtenir	Mémoire non volatile	CRC de paramètre de connexion	UDINT	CRC-S4 portant 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
15	Conditionnel ^a	Définir	Mémoire non volatile	Instance de configuration	UINT	Objet configuré pour ce nœud	= 0, lorsqu'aucun objet n'est attribué
16	Conditionnel ^a	Définir	Mémoire non volatile	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

ID d'attribut	Mise en œuvre nécessaire	Règle d'accès	Mémoire non volatile	Nom	Type de données	Description de l'attribut	Sémantique de la valeur
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 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	Mémoire non volatile	Type de format	USINT	Définit le format à utiliser pour la connexion avec une cible	0 = Auto (par défaut) 1 = «Base» 2 = «Étendu»
21	Conditionnel ^b	Obtenir	Mémoire non volatile	État du format	USINT	Indique le format actuellement utilisé lorsque le type de format est Auto (ou en l'absence d'accord possible sur un format donné)	0 = Auto 1 = «Base» 2 = «Étendu» 0xFF = "détection de conflit"
22	Conditionnel ^b	Définir	Mémoire non volatile	Nombre d'anomalies maximal	UINT	Utilisé par les producteurs et les consommateurs afin de déterminer le nombre de paquets erronés pouvant être éliminés avant qu'une connexion ne doive être fermée	Valeur par défaut = 5 Une valeur de 0 indique que les connexions doivent être fermées dès qu'une erreur est détectée
^a Cet attribut est nécessaire pour un appareil qui prend en charge les connexions de sécurité; cet attribut est facultatif dans les autres cas. ^b Cet attribut est nécessaire pour un appareil qui prend en charge le format étendu; cet attribut 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)

Ces drapeaux sont définis dans le Tableau 67.

Tableau 67 – Définitions 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-à-T Toujours 101 = Format de sécurité
Bits 4-6:	Format de transfert en temps réel T-à-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 convient de temporiser la connexion.

La valeur de temporisation de la connexion est définie comme suit:

$$\text{RPI de connexion} \times (\text{CTM} + 1) \times 4$$

Intervalle: 0 à 7

où

$$0 = (0 \times 4);$$

$$1 = (0 \times 8);$$

$$2 = (0 \times 12);$$

$$3 = (0 \times 16);$$

$$4 = (0 \times 20);$$

$$5 = (0 \times 24);$$

$$6 = (0 \times 28);$$

$$7 = (0 \times 32).$$

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-à-T (partie de l'attribut 5)

Si la direction est 0 (Client / T-à-O), il s'agit du RPI de la coordination temporelle et le RPI T-à-O est le RPI de production des données.

Si la direction est 1 (Serveur / O-à-T), il s'agit du RPI de production des données et le RPI T-à-O est le RPI de coordination temporelle.

Le RPI de coordination temporelle est défini comme suit:

Intervalle: 100 μ s à 100 000 000 μ s

Multiplicateur EPI d'intervalles Ping $\times$ RPI de production de données

RPI de production de données

Intervalle: 100 μ s à 1 000 000 μ s

6.8.4.6 Paramètres de connexion O-à-T – (partie de l'attribut 5)

Les paramètres de connexion O-à-T sont définis dans le Tableau 68.

Tableau 68 – Paramètres de connexion O-à-T

Bits	Paramètre	Valeur
0-8	Taille de connexion (en octets)	Si la direction est 1 (Serveur / O-à-T), il s'agit de la taille du message de sécurité: Si la taille des données est de 1-2 octets: Taille des données d'application + 6 Si la taille des données est de 3-250 octets: (Taille des données d'application $\times$ 2) + 8 Si la direction est 0 (Client / T-à-O), il s'agit de la taille du message de coordination temporelle (6 octets) Intervalle: 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-à-O – (partie de l'attribut 5)

Si la direction est 0 (Client / T-à-O), il s'agit du RPI de la production de données et le RPI O-à-T est le RPI de coordination temporelle.

Si la direction est 1 (Serveur / O-à-T), il s'agit du RPI de coordination temporelle et le RPI O-à-T est le RPI de production de données.

Valeur: voir RPI O-à-T.

6.8.4.8 Paramètres de connexion T-à-O – (partie de l'attribut 5)

Les paramètres de connexion T-à-O sont définis dans le Tableau 69.

Tableau 69 – Paramètres de connexion T-à-O

Bits	Paramètre	Valeur
0-8	Taille de connexion (en octets)	Si la direction est 0 (Client / T-à-O), il s'agit de la taille du message de sécurité. Pour une connexion point à point, voir les paramètres de connexion O-à-T. Pour les connexions multipoints avec une taille de données de 1-2 octets: Taille des données d'application + 12 Pour les connexions multipoints avec une taille de données de 3-248 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-à-T), il s'agit de la taille du message de coordination temporelle (6 octets). Intervalle: 7-508
9	Fixe/Variable	Toujours 0 (Fixe)
10-11	Priorité	Toujours 01 (Elevée)
12	Réservé	Toujours 0
13-14	Type de connexion	01 (Multipoints) 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 après que le (les) pont(s) aura (auront) retiré ses (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).

6.8.4.9.5 Chemin de consommation cible

Le chemin est valide s'il s'agit de la direction 1 (Serveur / O-à-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-à-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 # 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 # 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 Config#2.

6.8.4.12 Taille des données de configuration # 2 (partie de l'attribut 10)

Nombre d'octets stockés dans les données Config #2 (ci-dessous).

Intervalle: 1 à < Taille de configuration maximale admissible>

6.8.4.13 Données de configuration # 2 (partie de l'attribut 10)

Utilisées pour stocker les données de configuration de l'appareil cible.

6.8.4.14 Mise en correspondance des données (Attribut 9)

6.8.4.14.1 Attribution de format de mise en correspondance

Le Tableau 70 définit un ensemble de formats de mise en correspondance actuellement définis dans l'intervalle normalisé. L'intervalle spécifique au fournisseur peut toujours être utilisé pour des formats de mise en correspondance spéciaux.

Tableau 70 – Formats de mise en correspondance des données

Numéro de format	Nom de format	Taille S des données de mise en correspondance de données (en octets)	Données de mise en correspondance de données	Commentaire
0	Format de scrutation ouvert	4 octets	Voir Tableau 71	Format simple qui met en correspondance 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 72	Format simple qui met en correspondance 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			

6.8.4.14.2 Utilisation du format 0 pour les scrutateurs de sécurité

Le format 0 de mise en correspondance de données contient la structure des données de mise en correspondance qui utilise le format décrit dans le type de format de mise en correspondance, défini dans le Tableau 71.

Tableau 71 – Format 0 de mise en correspondance 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-à-O): Toujours 0. Si la direction est 1 (Serveur / O-à-T): Décalage de mots dans le tableau des données de sortie de sécurité
Décalage des images de données de la cible à l'origine	UINT	Décalage, en unités de 16 bits, dans le tableau d'images de la cible à l'origine	Si la direction est 0 (Client / T-à-O): Décalage de mots dans le tableau des données d'entrée de sécurité Si la direction est 1 (Serveur / O-à-T): Toujours 0

6.8.4.14.3 Utilisation du format 1 pour les scrutateurs de sécurité

Le format 1 de mise en correspondance de données contient la structure des données de mise en correspondance qui utilise le format décrit dans le type de format de mise en correspondance, défini dans le Tableau 72.

Tableau 72 – Format 1 de mise en correspondance 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-à-O): Toujours 0. Si la direction est 1 (Serveur / O-à-T): Décalage d'octets dans le tableau des données de sortie de sécurité
Décalage des images de données de la cible à l'origine	UINT	Décalage, en unités de 8 bits, dans le tableau d'images de la cible à l'origine	Si la direction est 0 (Client / T-à-O): Décalage d'octets dans le tableau des données d'entrée de sécurité. Si la direction est 1 (Serveur / O-à-T): Toujours 0

6.8.4.15 ID d'appareil de remplacement

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 dans les cycles d'alimentation. Lorsque l'attribut Désactivation de connexion dans l'objet CCO est FALSE, la connexion doit rester activée dans les 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 intervalles portant 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:

Intervalle: $[\text{Max\_Consumer\_Number} \times \text{Timeout\_Multiplier.PI} + 15]$ à 1 000.

Valeur par défaut:

Si la direction est 0 (Client / T-à-O): 100

Si la direction est 1 (Serveur / O-à-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. Time_Coord_Msg_Min_Multiplier est le nombre minimum d'incrément de 128 μs susceptible d'être utilisé pour un message de coordination temporelle pour le passage 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 intervalles portant sur le Time_Coord_Msg_Min_Multiplier au cours d'une demande Validate_Configuration.

L'emploi du multiplicateur minimal de messages de coordination temporelle est défini comme suit:

Intervalle: 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 maximum d'incrément 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 intervalles portant 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:

Intervalle 0 à 45 313, ce qui équivaut à 1 s à 5,8 s.

Équation 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.

Les appareils qui mettent en œuvre les extensions de sécurité de l'objet CCO doivent effectuer un contrôle des intervalles portant sur le Timeout_Multiplier au cours d'une demande Validate_Configuration.

L'emploi du multiplicateur de temporisation est défini comme suit:

Format de base d'intervalle	1 à 4
Format étendu d'intervalle	1 à 255
Valeur par défaut	2

6.8.5.5 Nombre maximal de consommateurs

Cet attribut définit le nombre maximal de consommateurs autorisés à se connecter à un producteur multipoints (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 intervalles portant sur le Nombre maximal de consommateurs au cours d'une demande Validate_Configuration.

L'emploi du nombre maximal de consommateurs est défini comme suit:

Intervalle:	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 permettant de confirmer que cette valeur est correcte.

Le format UNID cible avec le CP 2/3 est défini comme suit:

OCTET 0-5:	Numéro de réseau de sécurité
OCTET 6:	CP 2/3 MACID
OCTET 7-9:	Toujours 0 pour 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 application de la demande au Programme de contrôle de sécurité).

Le manuel de sécurité doit indiquer à l'utilisateur de soumettre à 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 73.

Tableau 73 – Valeurs SCCRC de l'appareil cible

Type de connexion de sécurité	Valeur SCCRC
Type 1	SCCRC identifiant les données de configuration dans les données Config #2
Type 2a	SCCRC identifiant 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 74.

Tableau 74 – Valeurs SCTS de l'appareil cible

Type de connexion de sécurité	Valeur SCTS
Type 1	SCTS identifiant les données de configuration dans les données Config #1
Type 2a	SCTS identifiant 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 multipoints.

La valeur d'une connexion multipoints est la suivante:

Multiplicateur EPI d'intervalles Ping × RPI de production de données;

Dans les autres cas, cette valeur est nulle.

6.8.5.10 Paramètres de connexion de correction de temps

Définit les paramètres de connexion utilisés dans le message de correction de temps utilisé dans une connexion multipoints.

La valeur est 0000_{hex} pour une connexion non multipoints ou 2406_{hex} pour une connexion multipoints, tel que défini dans le Tableau 75.

Tableau 75 – Paramètres de connexion de correction de temps pour une connexion multipoints

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 (Multipoints)
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 SCCRC doit être archivé dans la mémoire non volatile avec les autres attributs NV à chaque application d'une configuration (c'est-à-dire application de la demande au Programme de contrôle de sécurité).

Il convient d'exiger de l'utilisateur qu'il soumette à essai cette connexion, après qu'elle soit appliquée, afin de confirmer la configuration de connexion. À partir de là, le SCCRC 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 pour les 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 pour 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 garantie.

6.8.5.14 Type de format

Le Tableau 76 définit la signification de l'attribut Type de format.

Tableau 76 – Signification de l'attribut Type de format

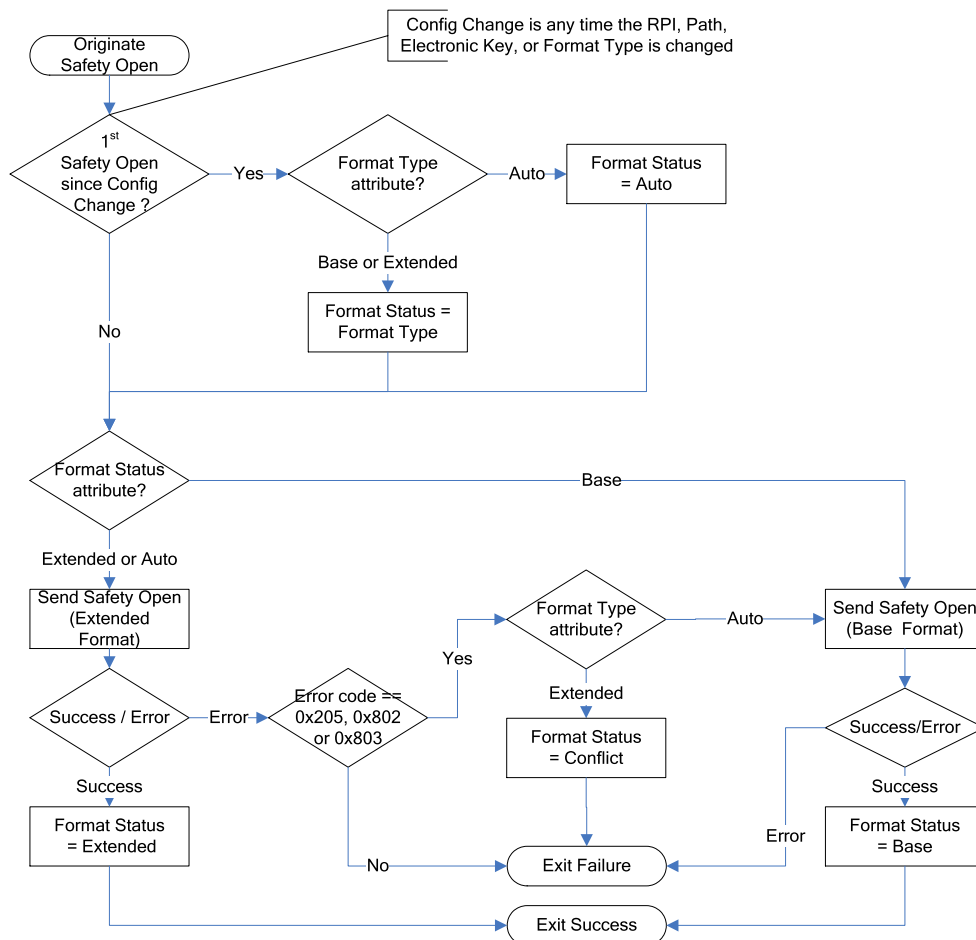
Nom de valeur du type de format	Signification
Auto	Le point d'origine détermine le format à utiliser pour l'établissement de la première connexion
de Base	Le point d'origine utilise le format existant pour l'établissement de la connexion suivante
Étendu	Le point d'origine utilise le format étendu pour 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 «Étendu» est la valeur de configuration facultative de l'attribut Type de format, le point d'origine utilise uniquement le format «Étendu».

L'attribut État du format doit être réglé sur la valeur 0xFF (Détection de conflit) si le type de format est «de Base» ou «Étendu» 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 présentée à la Figure 17 doit être utilisée:



IEC

Anglais	Français
Config change is any time the RPI, Path, Electronic Key, or Format Type is changed	modification de configuration à chaque modification de RPI, Chemin, clé électronique ou type de format
originate SafetyOpen	SafetyOpen de point d'origine
1 st SafetyOpen Config change	1er SafetyOpen du fait de la modification de config.?
yes	oui
format type attribute?	attribut Type de format?
format status	état du format
base or extended	de base ou étendu
no	non
format type	type de format
format status attribute?	attribut État du format?
extended or auto	étendu ou auto

Anglais	Français
send safety open	envoi de SafetyOpen
(extended format)	(format étendu)
(base format)	(format de base)
success /error	réussite / erreur
error	erreur
error code	code d'erreur
extended	étendu
conflict	conflit
success	réussite
exit failure	échec de sortie
exit success	réussite de sortie

Figure 17 – Logique pour le type de format «Autodétection»

6.8.5.15 État du format

Le Tableau 77 définit la signification de l'attribut État du format.

Tableau 77 – Signification de l'attribut État 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 requiert 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 «Étendu» Il convient que cette condition ne se produise jamais	La cible utilise le format «de Base»
«Étendu»	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 «Étendu» Le point d'origine se connecte uniquement avec le nouveau format	La cible utilise le format «Étendu»
“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 78.

Tableau 78 – Services spécifiques à l'objet Configuration de connexion

Service	Mise en œuvre nécessaire		Nom de service	Description du service
	Classe	Instance		
4B _{hex}	Conditionnel ^a	N/A	Kick-Timer (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	Obtenir 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 doivent être acceptés uniquement en cas de déverrouillage de l'appareil. Si l'appareil est verrouillé, il doit répondre par une erreur «Conflit d'état de l'appareil».				

6.8.7 Extensions des services communs pour la sécurité

6.8.7.1 Obtenir Tous Attributs (Code de service 01_{hex})

Les attributs ajoutés à la fin de la réponse Get_Attribute_All sont définis dans le Tableau 79 et le Tableau 80. Tous les autres paramètres de ce service sont tels que définis dans l'objet CCO normalisé dans les IEC 61158-5-2 et IEC 61158-6-2.

Tableau 79 – Données du service de réponse Get_Attributes_All (attributs ajoutés)

Nom	Type de données	Description
Paramètres de sécurité	STRUCT. de:	
	USINT	Remplissage, réglé sur zéro
	USINT	Remplissage, réglé 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	UNID Cible
	10:octets	Remplissage, réglé sur zéro
	UINT	Multiplicateur EPI d'intervalles Ping
	UINT	Multiplicateur minimal de messages de coordination temporelle
	UINT	Multiplicateur Exp. de temps réseau
	USINT	Multiplicateur de temporisation
	USINT	Nombre maximal de consommateurs
CRC de paramètre de connexion	UDINT	CRC-32 portant sur les paramètres de connexion utilisés dans un service SafetyOpen
Instance de configuration	UINT	

Nom	Type de données	Description
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 80 – 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	
État du format	USINT	
Nombre d'anomalies maximal	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 défini dans le Tableau 81 et le Tableau 82. Tous les autres paramètres de ce service sont tels que définis dans l'objet CCO normalisé dans les IEC 61158-5-2 et IEC 61158-6-2.

Tableau 81 – Données du service de Demande Set_Attributes_All (attributs ajoutés)

Nom	Type de données	Description
Paramètres de sécurité	STRUCT. de:	
	USINT	Remplissage, réglé sur zéro
	USINT	Remplissage, réglé sur zéro
	UDINT	CRC de configuration (SCCRC) (valeur réglée = 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
	10octets	UNID Cible
	10octets	Remplissage, réglé sur zéro
	UINT	Multiplicateur EPI d'intervalles Ping
	UINT	Multiplicateur minimal de messages de coordination temporelle
	UINT	Multiplicateur Exp. de temps réseau
	USINT	Multiplicateur de temporisation
	USINT	Nombre maximal de consommateurs
Instance de configuration	UINT	
Drapeau d'attribution d'ID	BOOL	

Tableau 82 – Données du service 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 d'anomalies maximal	UINT	

6.8.7.3 Restauration (Code de service 15_{hex})

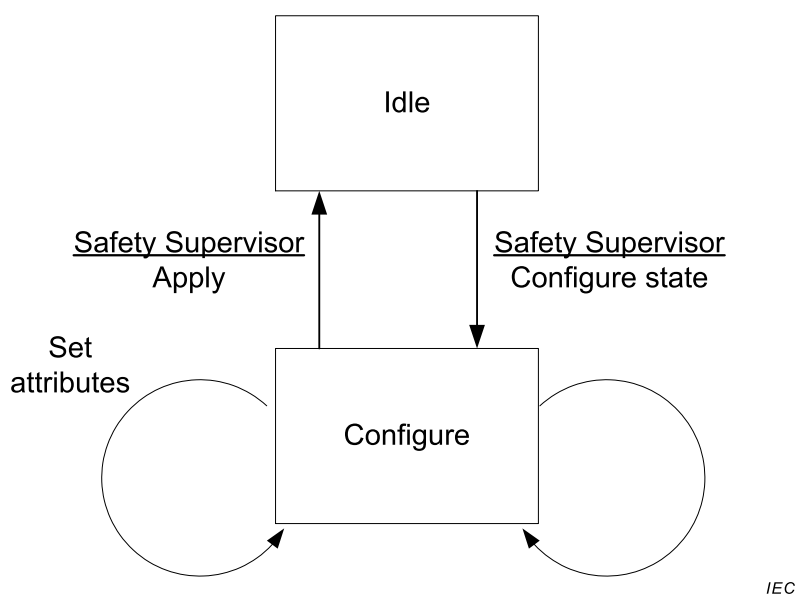
Les appareils de sécurité ne doivent pas mettre en œuvre le service Restauration au niveau de la classe ou de l'instance, dans la mesure où l'outil de configuration coordonne la configuration par l'intermédiaire du Programme de contrôle de sécurité.

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 83, la Figure 18 et la Figure 19.

Tableau 83 – Mapping des états des objets Programme de contrôle de sécurité et CCO

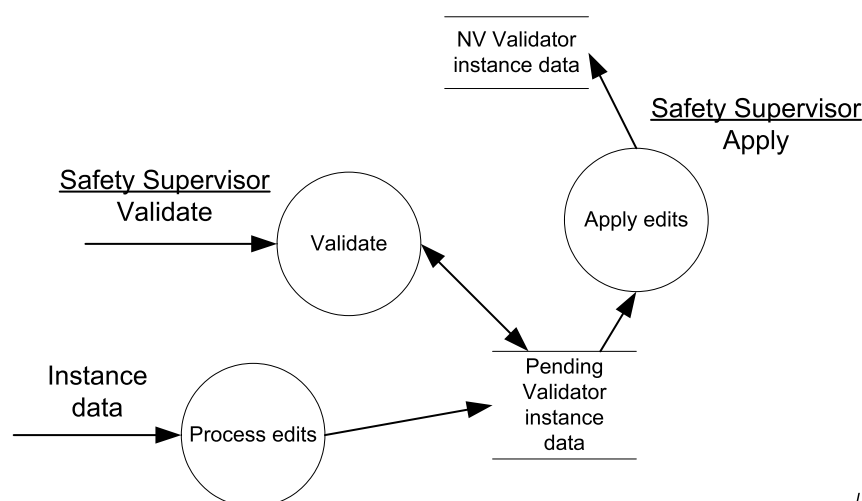
Programme de contrôle de sécurité	Configuration de connexion
Autovérification	Éditions non admises
Exception d'autovérification	Éditions non admises
Repos	Éditions non admises
Configuration	Éditions admises
Exécution	Éditions non admises
Abandon	Éditions non admises
Anomalie critique	Éditions non admises



Anglais	Français
idle	repos
safety supervisor	programme de contrôle de sécurité
apply	application
configure state	état de configuration
set attributes	définir les attributs
configure	configuration

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 de configuration est défini à la Figure 19.



IEC

Anglais	Français
NV validator instance data	données d'instance de l'objet de validation NV
safety supervisor	programme de contrôle de sécurité
apply	application
validate	validation
apply edits	application des éditions
instance data	données d'instance
process edits	traitement des éditions
pending validator instance data	données d'instance de l'objet de validation en attente

Figure 19 – Flux de données de l'objet Configuration de connexion

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 message. Les six types de formats de connexion sont les suivants:

- point à point à 1 ou 2 octets (voir 7.1.1.13),
- multipoints à 1 ou 2 octets format 1 (voir 7.1.1.14),
- multipoints à 1 ou 2 octets format 2 (voir 7.1.1.15),
- multipoints de 3 à 248 octets format 1 (voir 7.1.1.16),
- multipoints de 3 à 248 octets format 1 (voir 7.1.1.17),
- multipoints de 3 à 248 octets format 2 (voir 7.1.1.18),

Le Tableau 84 définit les sections utilisées dans les divers types de messages pour les six types de format de connexion différents:

Tableau 84 – 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	
	multipoints	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	
	Multipoints	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 Etendu.

^b Le message peut utiliser soit le format de base, soit le format Etendu.

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 divers 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 Etendu à paquets courts, les bits 5 à 7 font partie intégrante du CRC des données. Dans le format Etendu 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 visant à compléter les descriptions sont données dans le Tableau 85.

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 85 – Variables de l'octet Mode**

Nom	Description	Référence
Run_Idle	Run_Idle doit être utilisée 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 réglé 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 comptage 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 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 le 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.

Section de données à 1 ou 2 octets																																							
Données réelles																Octet Mode								CRC réel								CRC compl.							
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 ($E0_{\text{hex}}$) (par CRC-S1);
- Le 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);
- L' (Octet Mode XOR FF_{hex}) AND ($E0_{\text{hex}}$) (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 Etendu doit comprendre le ou les octets des données réelles, l'octet Mode, la datation et le CRC-S5 calculé sur l'ensemble du paquet. Le format Etendu de la section de données à 1 ou 2 octets est représenté à la Figure 22.

Format Etendu de la section de données à 1 ou 2 octets					
Données réelles	Octet Mode ^a		CRC S5		Datation
2 octets	1 octet		2 octets		2 octets
1 – 2 Octets			CRC-S5_0	CRC-S5_1	Datation
					CRC-S5_2

^a Les Bits 0-4 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 Etendu

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 ($E0_{\text{hex}}$);
- le 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 à 3 ou 250 octets est définie à la Figure 23.

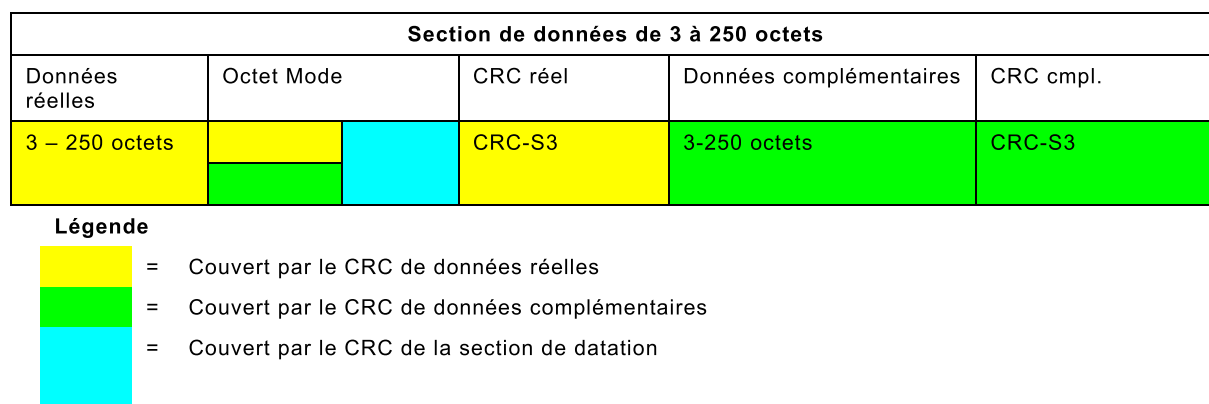


Figure 23 – Format de section de données de 3 à 250 octets, format de base

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);
- Le 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);
- L' (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 Etendu

La section de données EF de 3 à 250 octets doit comporter 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.

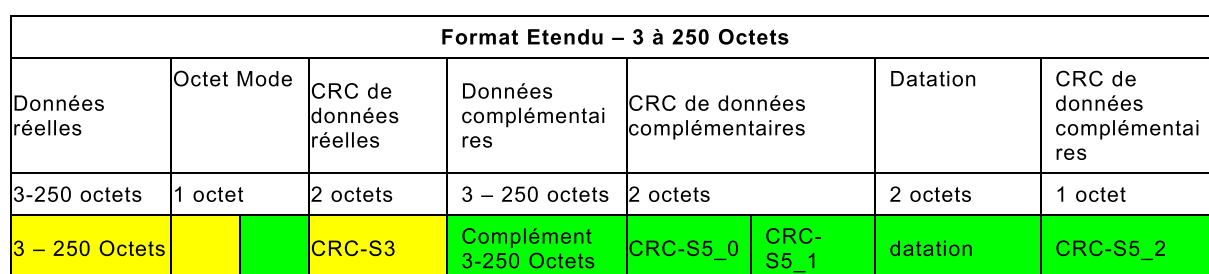


Figure 24 – Format de section de données de 3 à 250 octets, format Etendu

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);
- L' (Octet Mode) **AND** ($0xE0$) (par CRC-S3);
- le ou les octets des données réelles (par CRC-S3).

Le calcul du CRC des données complémentaires EF de 3 à 250 octets doit inclure:

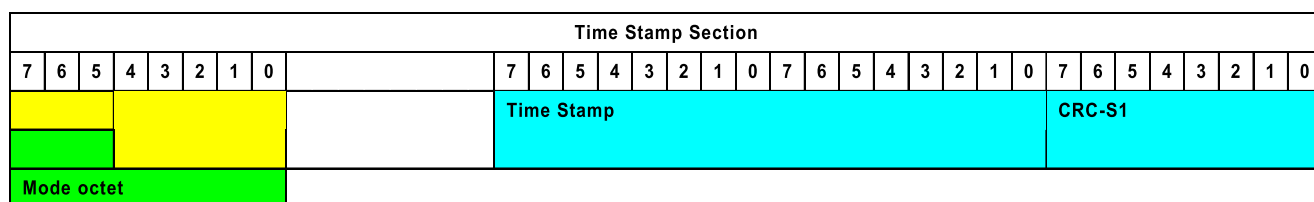
- L'identifiant du producteur (PID) (par CRC-S5);
- Le comptage de remplacement (par CRC-S5);

- 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 Datation se compose de l'octet Mode, de Time_Stamp et du CRC de datation. La disposition de la section Datation est définie à la Figure 25.

Les descriptions des variables de la section Datation sont définies dans le Tableau 86.



Légende

- = Couvert par le CRC de données réelles
- = Couvert par le CRC de données complémentaires
- = Couvert par le CRC de la section Datation

Anglais	Français
time stamp section	section Datation
time stamp	datation
octet	octet

Figure 25 – Format de section de datation, Format de base

Tableau 86 – Variables de datation

Nom	Description	Référence
Data_Time_Stamp	Point à point -- Data_Time_Stamp représente la datation du prélèvement des données pour production, par rapport à l'horloge du consommateur. Multipoints -- Data_Time_Stamp représente la datation du prélèvement des données pour production, par rapport à l'horloge du producteur.	7.7.2

Le calcul du CRC de datation BF doit inclure:

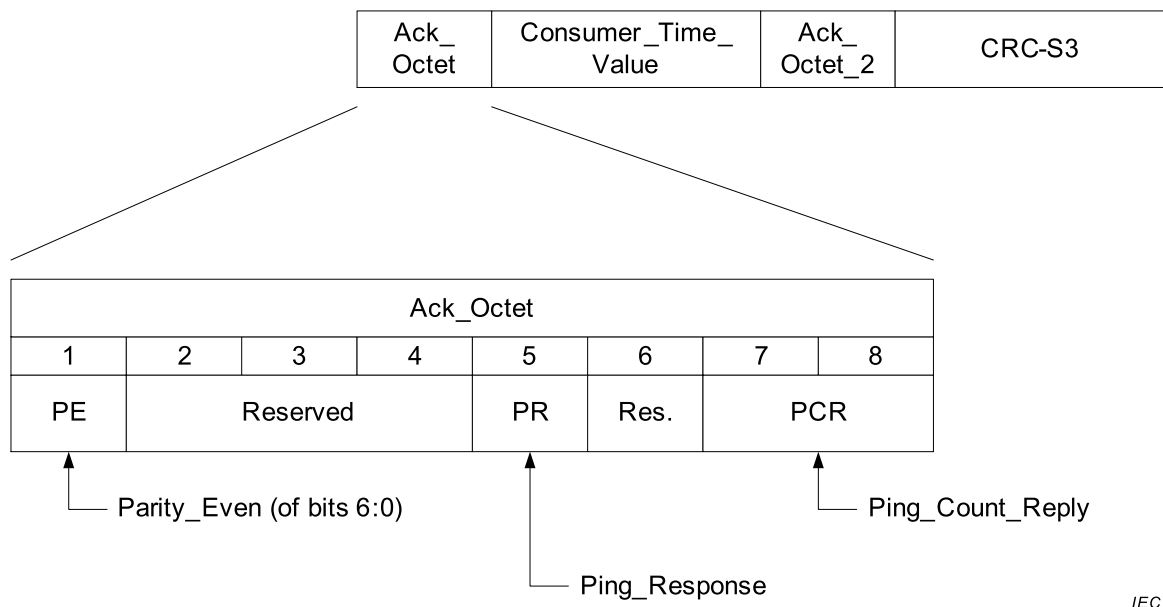
- L'octet Identifiant du producteur (PID) (par CRC-S1);
- L' (Octet Mode) AND (1F_{hex}) (par CRC-S1);
- Le ou les octets de datation (par CRC-S1).

7.1.1.9 Section de coordination temporelle

La section de coordination temporelle doit être transmise au producteur par le consommateur en réponse à un changement dans le comptage de demandes Ping.

La section de coordination temporelle est utilisée comme Message de coordination temporelle pour toutes les demandes de coordination temporelle point à point et multipoints. 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 visant à compléter les descriptions sont données dans le Tableau 87.



Anglais	Français
reserved	réservé
of bits	des bits

Figure 26 – Codage du message de coordination temporelle BF



Figure 27 – Codage du message de coordination temporelle EF

Tableau 87 – 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 de Ping à laquelle répond le consommateur	7.7.3.3
Réservé	Réservé, réglé sur zéro	
CRC-S3	CRC couvrant les données contenues dans le message de coordination temporelle BF	
CRC-S5	CRC couvrant les données contenues dans le message de coordination temporelle EF	

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 paramétrage des bits dans le Ack_Octet_2 du message de Coordination temporelle:

$\text{Ack\_Octet\_2} = ((\text{Ack\_Octet} \text{ XOR } \text{FF}_{\text{hex}}) \text{ AND } 55_{\text{hex}}) \text{ OR } (\text{Ack\_Octet} \text{ ET } \text{AA}_{\text{hex}}).$

Le format de Coordination temporelle EF doit être utilisé lors de l'établissement d'une connexion avec le format Etendu. Dans les autres cas, le format de Coordination temporelle BF doit être utilisé.

7.1.1.10 Calcul du CRC de coordination temporelle

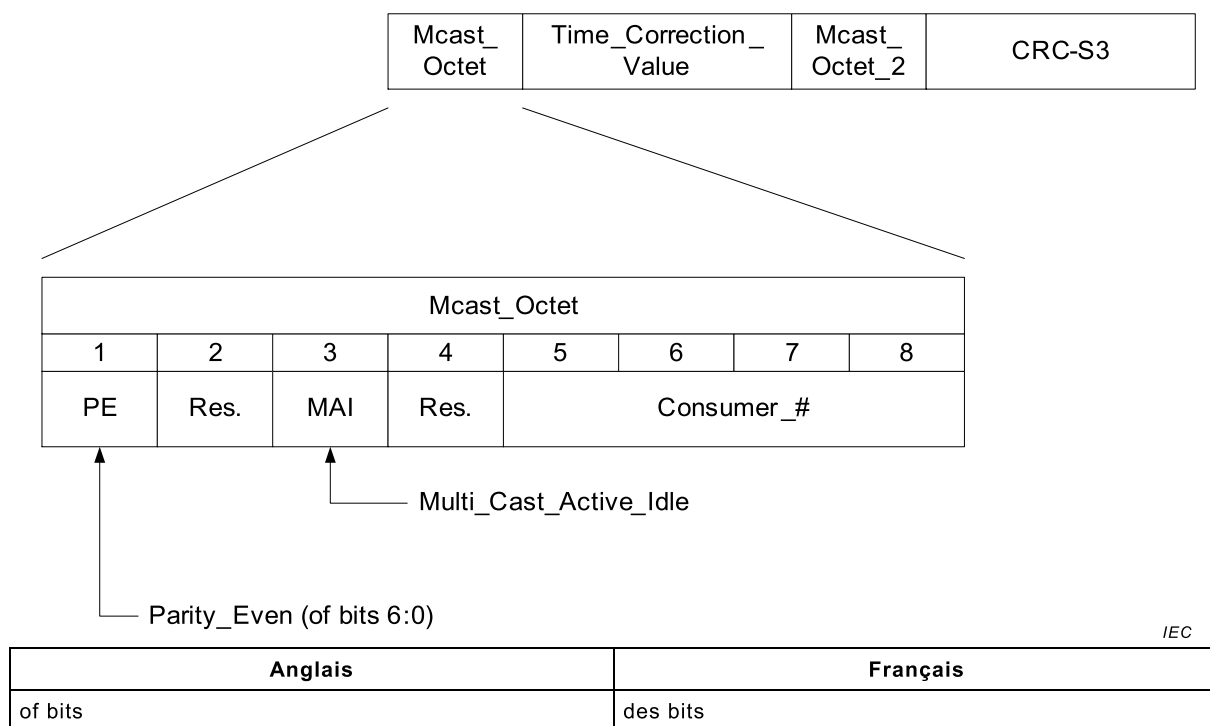
Le calcul du CRC de coordination temporelle doit inclure:

- L'identifiant de consommateur (CID) (par CRC-S3 ou CRC-S5);
- L'octet Ack (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 multipoints à chaque consommateur multipoints, 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 88.

**Figure 28 – Codage du message de correction de temps BF****Figure 29 – Codage du message de correction de temps EF****Tableau 88 – 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_#	Le 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, réglé sur zéro	7.7.4.4
CRC-S3	CRC couvrant les données contenues dans le message de correction de temps BF	
CRC-S5	CRC couvrant les données contenues dans le message de correction de temps EF	

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 paramétrage des bits dans le Mcast_Octet_2 du message de correction de temps:

$$\text{MCast\_Octet\_2} = ((\text{MCast\_Octet} \text{ XOR } \text{FF}_{\text{hex}}) \text{ AND } \text{55}_{\text{hex}}) \text{ OR } (\text{MCast\_Octet} \text{ AND } \text{AA}_{\text{hex}}).$$

Le format de correction de temps EF doit être utilisé lors de l'établissement d'une connexion avec le format Etendu. 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.

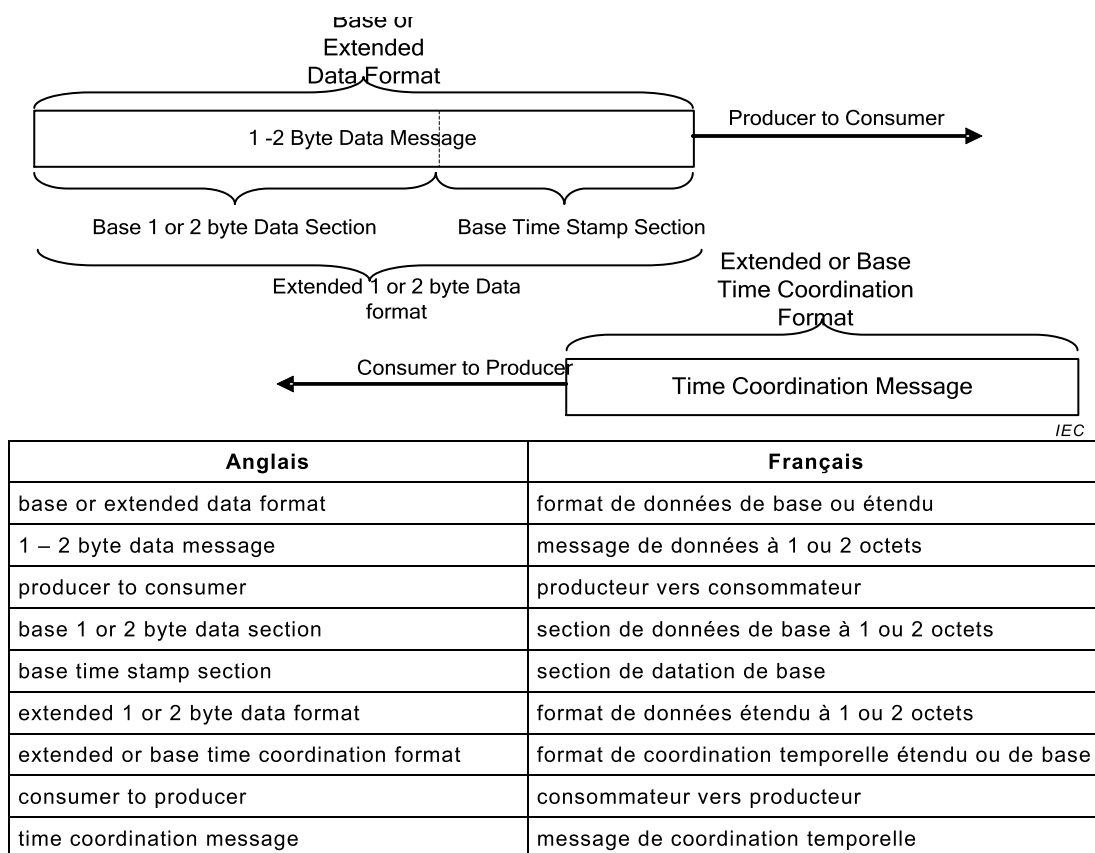


Figure 30 – Codage PDU point à point à 1 ou 2 octets

7.1.1.14 Format de connexion de format 1 multipoints à 1 ou 2 octets

La Figure 31 définit l'organisation de la section pour le format de connexion multipoints de format 1 à 1 ou 2 octets.

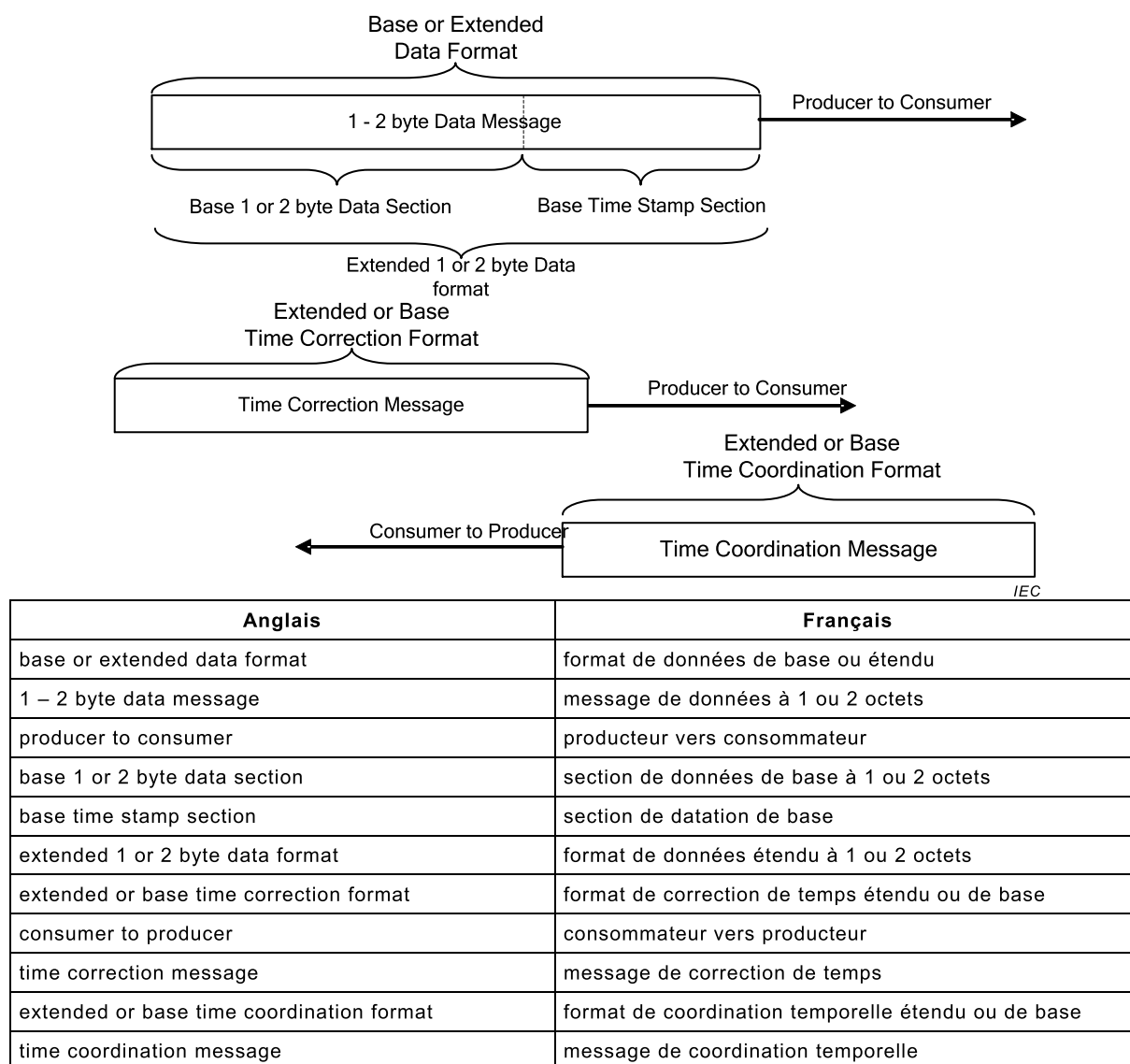


Figure 31 – Codage PDU multipoints à 1 ou 2 octets

7.1.1.15 Format de connexion de sécurité de format 2 multipoints à 1 ou 2 octets

La Figure 32 définit l'organisation de la section pour le format de connexion de sécurité de format 2 multipoints à 1 ou 2 octets.

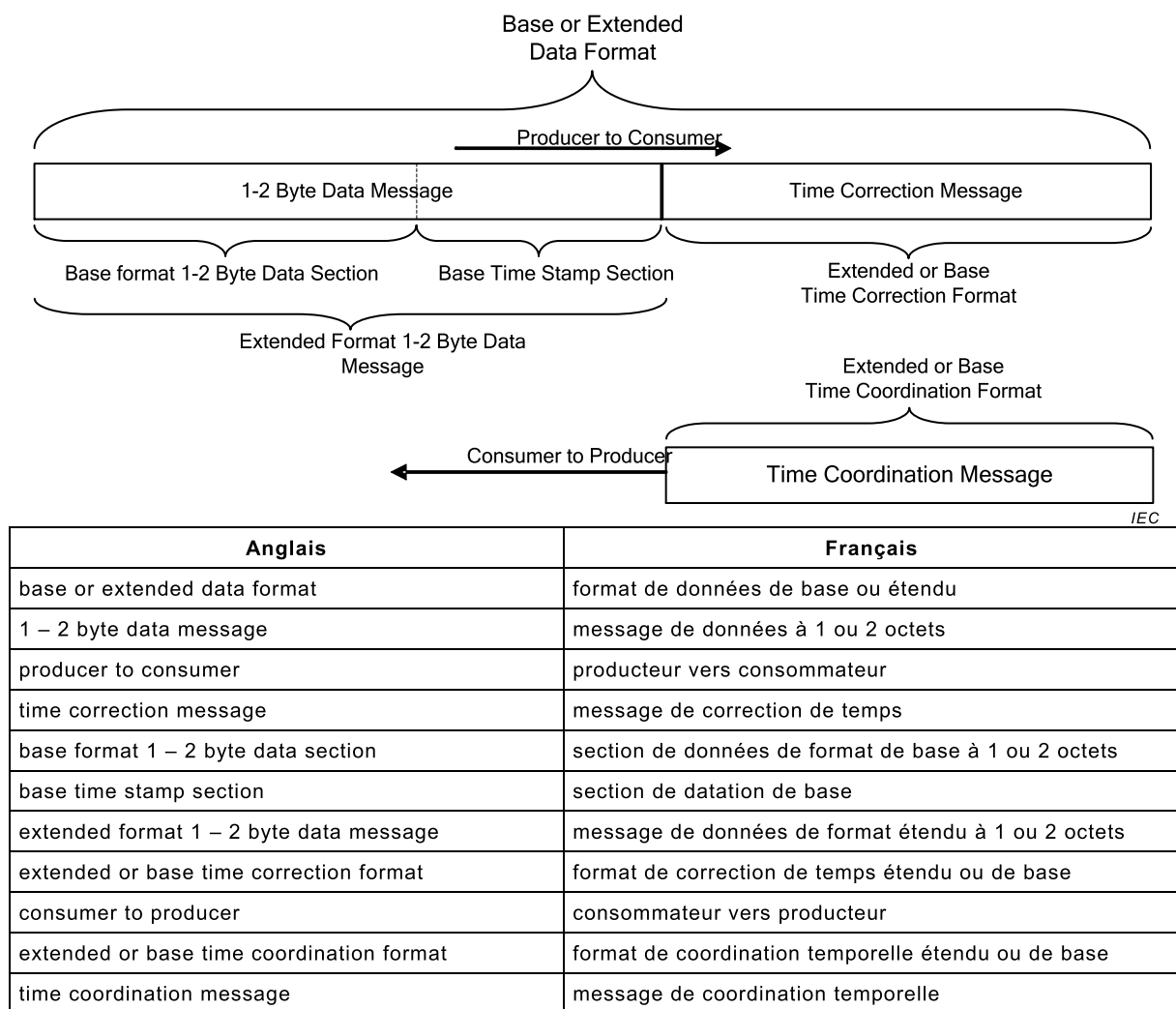
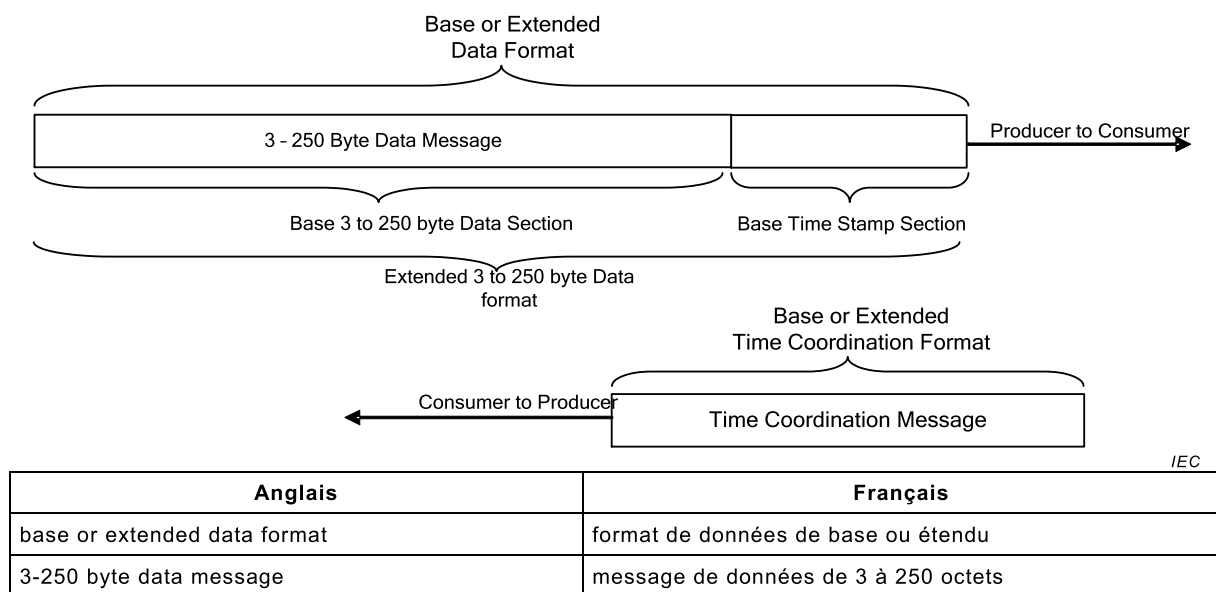


Figure 32 – Format de connexion de sécurité de format 2 multipoints à 1 ou 2 octets

7.1.1.16 Format de connexion de sécurité point à point de 3 à 250 octets

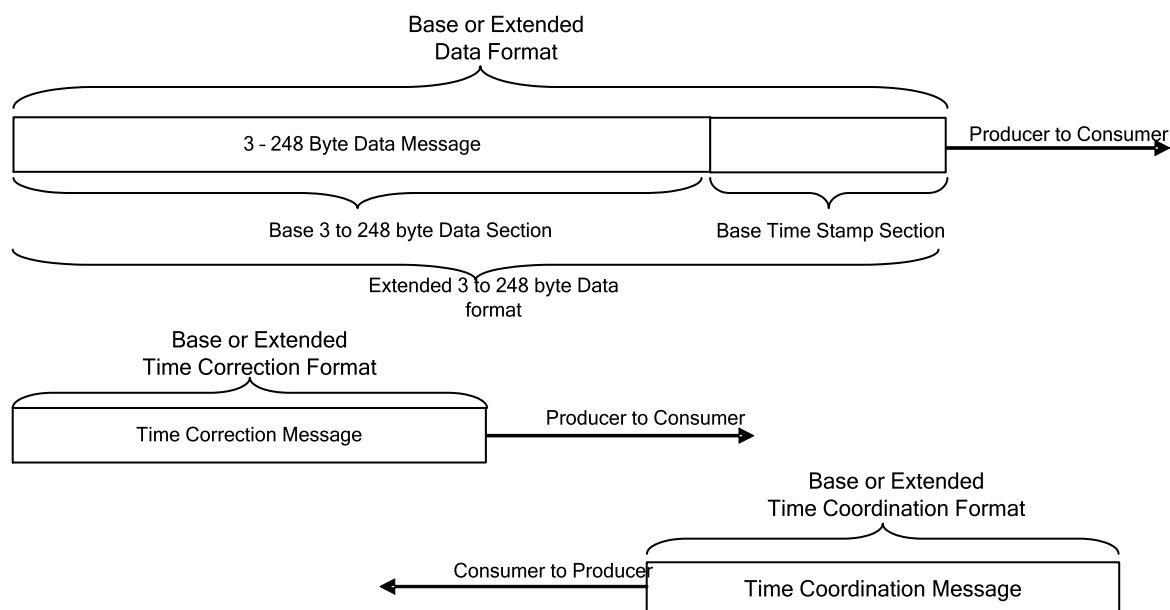
La Figure 33 définit l'organisation de la section pour le format de connexion de sécurité point à point de 3 à 250 octets.



Anglais	Français
producer to consumer	producteur vers consommateur
base 3 to 250 byte data section	section de données de base de 3 à 250 octets
base time stamp section	section de datation de base
extended 3 to 250 byte data format	format de données de format étendu de 3 à 250 octets
consumer to producer	consommateur vers producteur
base or extended time coordination format	format de coordination temporelle de base ou étendu
time coordination message	message de coordination temporelle

Figure 33 – Codage PDU point à point de 3 à 250 octets**7.1.1.17 Format PDU de sécurité de format 1 multipoints de 3 à 248 octets**

La Figure 34 définit l'organisation de la section pour le format de connexion de sécurité multipoints de 3 à 248 octets.



IEC

Anglais	Français
base or extended data format	format de données de base ou étendu
3-248 byte data message	message de données de 3 à 248 octets
producer to consumer	producteur vers consommateur
base 3 to 248 byte data section	section de données de base de 3 à 248 octets
base time stamp section	section de datation de base
extended 3 to 248 byte data format	format de données de format étendu de 3 à 248 octets
consumer to producer	consommateur vers producteur
base or extended time correction format	format de correction de temps de base ou étendu
time correction message	message de correction de temps
base or extended time coordination format	format de coordination temporelle de base ou étendu
time coordination message	message de coordination temporelle

Figure 34 – Codage PDU multipoints de 3 à 248 octets

7.1.1.18 Format PDU de sécurité de format 2 multipoints de 3 à 248 octets

La Figure 35 définit l'organisation de la section pour le format de connexion de sécurité multipoints de 3 à 248 octets.

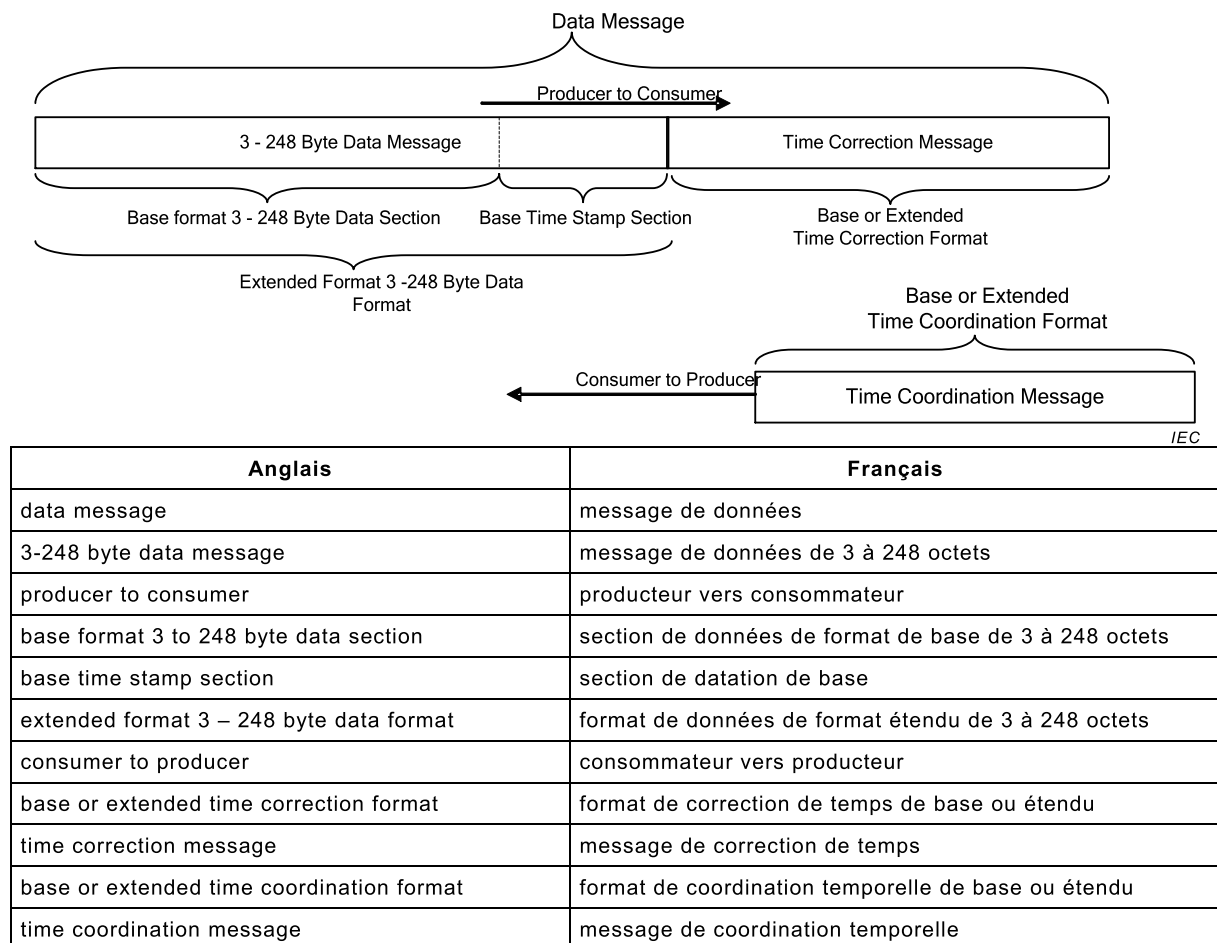
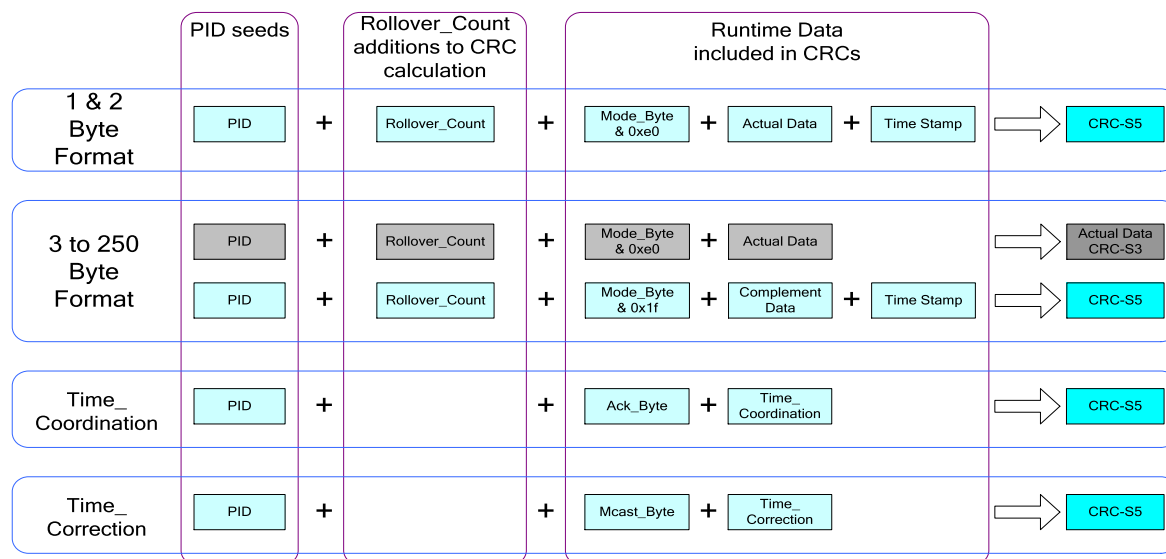


Figure 35 – Format de connexion de sécurité multipoints de 3 à 248 octets

7.1.1.19 Ordre des calculs du CRC pour le format Etendu

La Figure 36 représente le point d'ajustement du comptage de remplacement aux calculs du CRC pour les messages de format étendu.

NOTE La base de calcul 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.



IEC

Anglais	Français
PID seeds	marquages du PID
Rollover_Count additions to CRC calculations	ajouts de Rollover_Count aux calculs de CRC
Runtime data included in CRCs	données Runtime incluses dans les CRC
1 & 2 byte format	format à 1 & 2 octets
actual data	données réelles
time stamp	datation
3 to 250 byte format	format de 3 à 250 octets
complement data	données complémentaires

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 diverses sections de 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 contenant jusqu'à deux octets de données de sécurité, ainsi que 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 en BF.
- Un CRC de 24 bits (CRC-S5) est utilisé pour le format de données EF 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 en 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.

7.1.2.2 Polynômes de CRC

Le Tableau 89 définit les polynômes utilisés dans le FSCP 2/1.

Tableau 89 – 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 90 définit le type d'algorithme utilisé et la valeur de départ pour chaque utilisation.

Tableau 90 – Sections de connexion et formats de messages

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.

- Contrôle des comptages de demandes Ping;
- Évaluation du CRC de section de datation;
- Évaluation des datations;
- Évaluation du CRC des données réelles;
- Évaluation du CRC des données complémentaires;
- Réalisation d'une contre-vérification.

7.2.2 Terminaison de connexion

Lorsqu'un producteur détecte une erreur qui exige une terminaison de connexion (c'est-à-dire une réponse aux demandes Ping hors de l'intervalle Ping du producteur), il doit terminer 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 terminer la connexion de consommation associée à cette erreur.

Lorsque la couche de sécurité détecte une erreur qui exige la terminaison d'une connexion, la séquence suivante doit être suivie pour effectuer ladite terminaison.

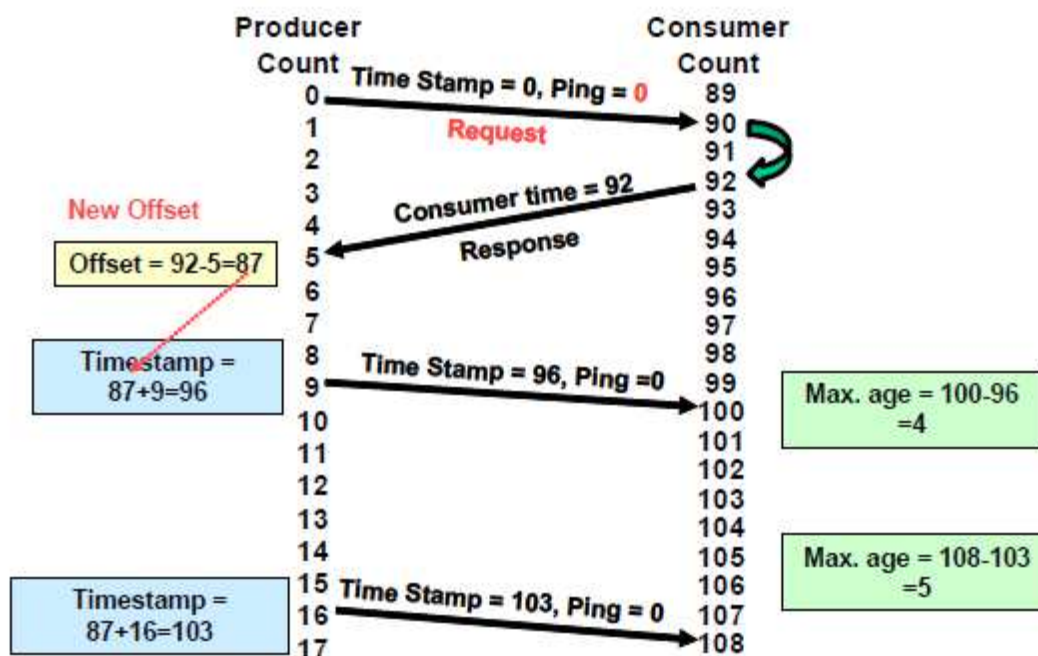
- La couche de sécurité détecte une erreur qui exige une terminaison de connexion.
- La couche de sécurité notifie le programme d'application par le paramétrage de l'état de connexion, afin d'indiquer une anomalie de communication de sécurité.
- L'application relative à la sécurité doit transférer les données et les E/S (par exemple, réglage des sorties sur l'état de sécurité) associées à la connexion vers un état de sécurité
- La couche de sécurité doit notifier le système de communications sous-jacent d'une erreur et solliciter la terminaison de la connexion par le paramétrage de son état de manière à indiquer une erreur de communication de sécurité.
- 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 terminer 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 termine 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 des opérations de datation pour une paire producteur/consommateur point à point simple.



IEC

Anglais	Français
producer count	comptage du producteur
consumer count	comptage du consommateur
Request	demande
consumer time	temps de consommation

Anglais	Français
new offset	nouveau décalage
Offset	décalage
time stamp	datation
max. age	âge max.

Figure 37 – Séquence de datation

À 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 contenant 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 qu'il a reçue du producteur pour calculer l'âge des données, et ce, par soustraction de la datation du producteur de son comptage d'horloge courant. Si le delta calculé est inférieur au delta maximum 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 considérées comme trop anciennes pour être utilisées, ce qui entraîne la terminaison 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.

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 pas toutefois 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.

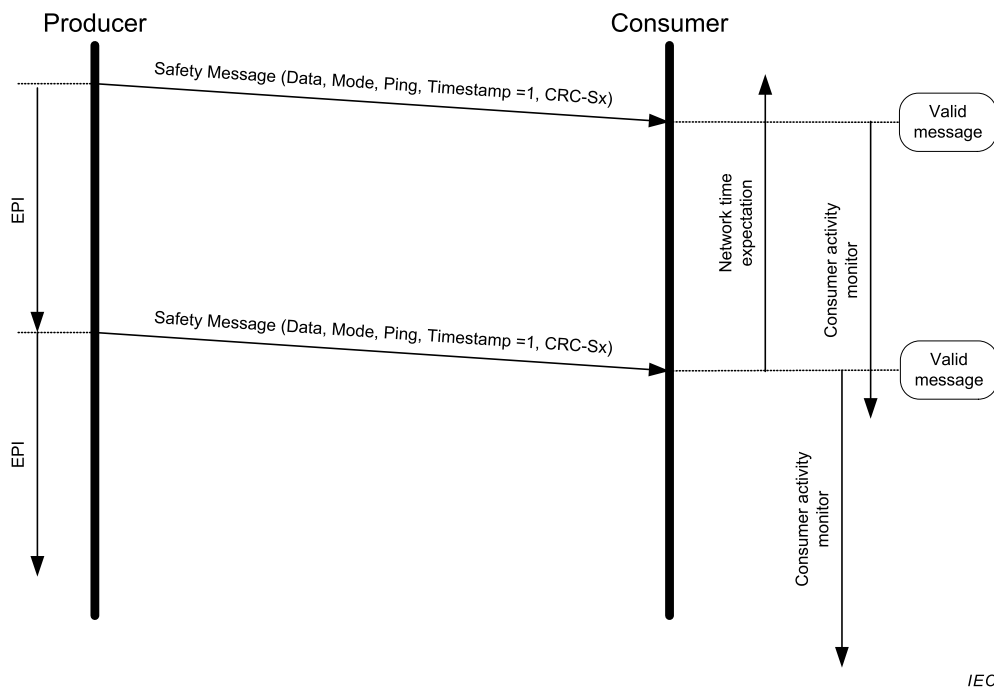
7.5 Diagrammes séquentiels de protocoles

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 tel que défini à la Figure 38.



Anglais	Français
producer	producteur
consumer	consommateur
safety message	message de sécurité
valid message	message valide
network time expectation	délai du réseau
consumer activity monitor	contrôleur d'activité du consommateur

Figure 38 – Diagramme d'une séquence de sécurité producteur/consommateur normale

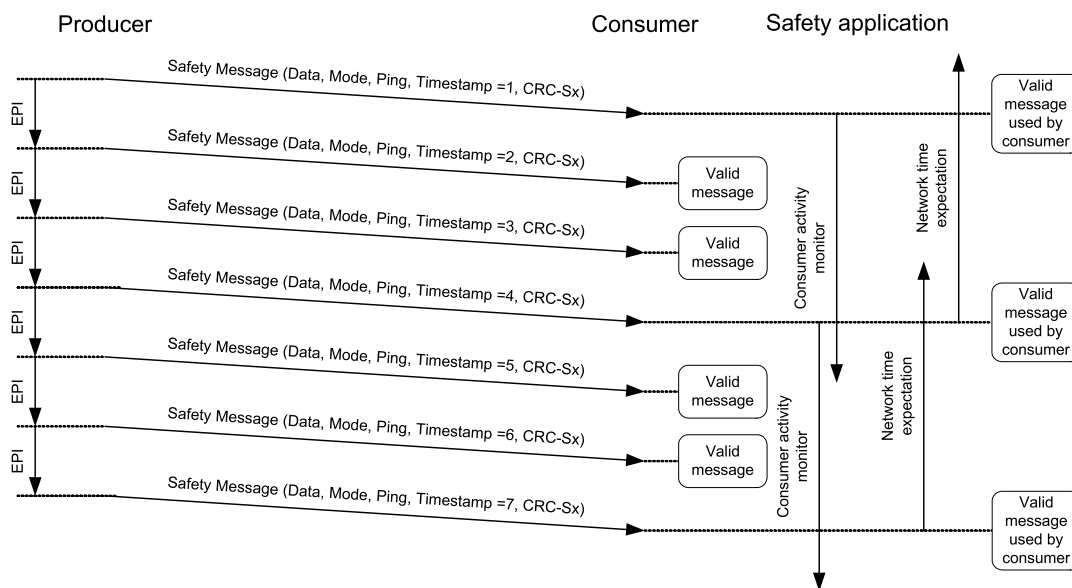
Le producteur de sécurité génère des données à une fréquence fixe appelée Intervalle de paquets attendu (EPI).

Les consommateurs déclenchés par la liaison doivent maintenir un temporisateur d'activité réinitialisé après réception d'un message attendu valide.

Si un message valide n'a pas été reçu avant expiration du temporisateur d'activité, le consommateur déclenché par la liaison doit terminer 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 terminer la connexion (voir 7.2.2) et passer à l'état de sécurité défini.



IEC

Anglais	Français
producer	producteur
consumer	consommateur
safety application	application de sécurité
safety message	message de sécurité
valid message used by consumer	message valide utilisé par le consommateur
valid message	message valide
network time expectation	délai du réseau
consumer activity monitor	contrôleur d'activité du consommateur

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, tel que représenté à la Figure 39.

Les consommateurs qui utilisent les connexions de format de base doivent constater l'augmentation de datation pour chaque période successive; à défaut, la connexion doit être terminée (voir 7.2.2).

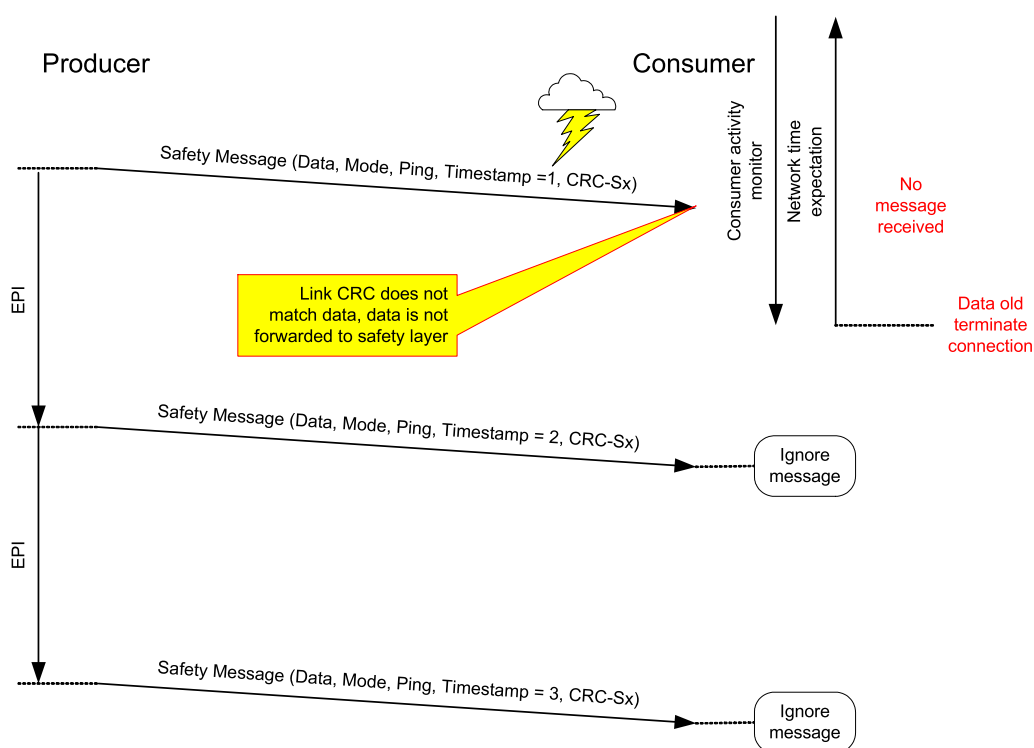
Les consommateurs qui utilisent les connexions de format étendu doivent constater l'augmentation de datation pour chaque période successive. Si le consommateur reçoit un paquet avec une datation hors séquence, il doit rejeter ce dernier à moins que le compteur d'anomalies du consommateur n'ait atteint le nombre d'anomalies maximal; auquel cas, la connexion doit être terminée.

L'envoi d'un message avec une production répétée offre l'avantage supplémentaire d'utiliser les données les plus récentes.

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 soit corrompu, tel que 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. L'âge des données dépasse également le délai du réseau et le consommateur termine 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 Etendu AND ((Consumer_Fault_Count < Max_Fault_Number)), ou terminer la connexion et passer à l'état de sécurité défini (format de base OR format Etendu) AND ((Consumer_Fault_Count ≥ Max_Fault_Number) (voir 7.2.2).

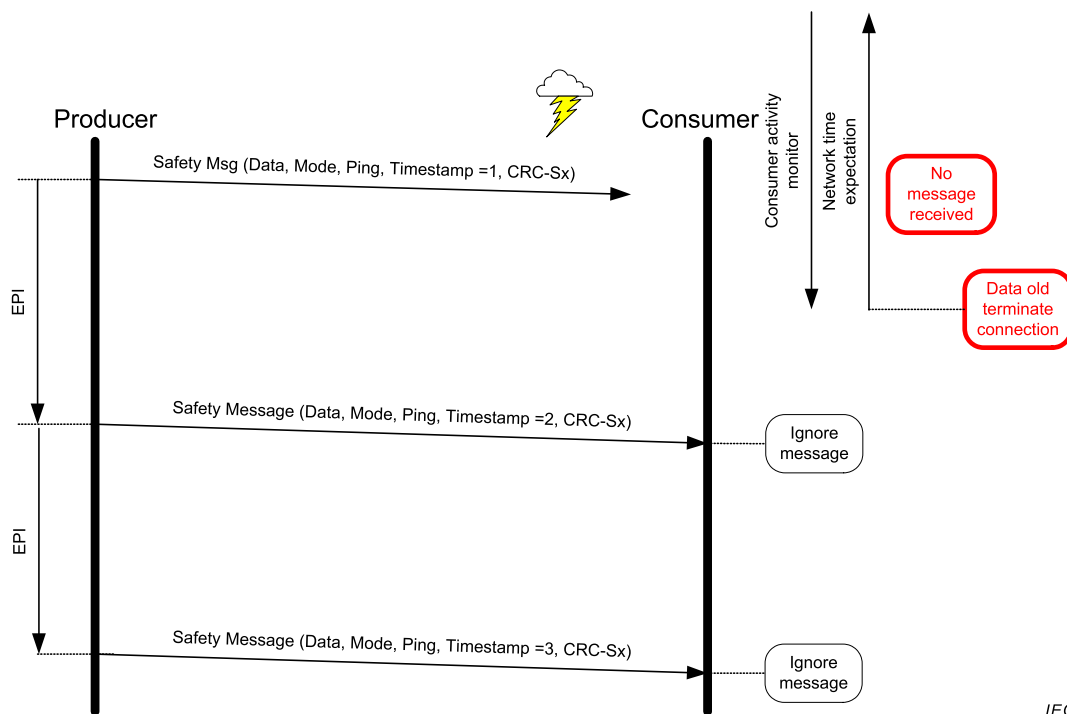


IEC

Anglais	Français
producer	producteur
consumer	consommateur
safety message	message de sécurité
no message received	aucun message reçu
network time expectation	délai du réseau
consumer activity monitor	contrôleur d'activité du consommateur
Link CRC does not match data, data is not forwarded to safety layer	Le CRC de liaison ne correspond pas aux données, les données ne sont pas transmises à la couche de sécurité
data old terminate connection	les anciennes données terminent la connexion
ignore message	ignorer message

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 soit perdu, tel que défini à la Figure 41. Ceci entraîne une expiration du contrôleur d'activité du consommateur. L'âge des données dépasse également le délai du réseau et le consommateur termine la connexion (voir 7.2.2) et passe à l'état de sécurité défini.



IEC

Anglais	Français
producer	producteur
consumer	consommateur
safety message	message de sécurité
no message received	aucun message reçu
network time expectation	délai du réseau
consumer activity monitor	contrôleur d'activité du consommateur
data old terminate connection	les anciennes données terminent la connexion
ignore message	ignorer message

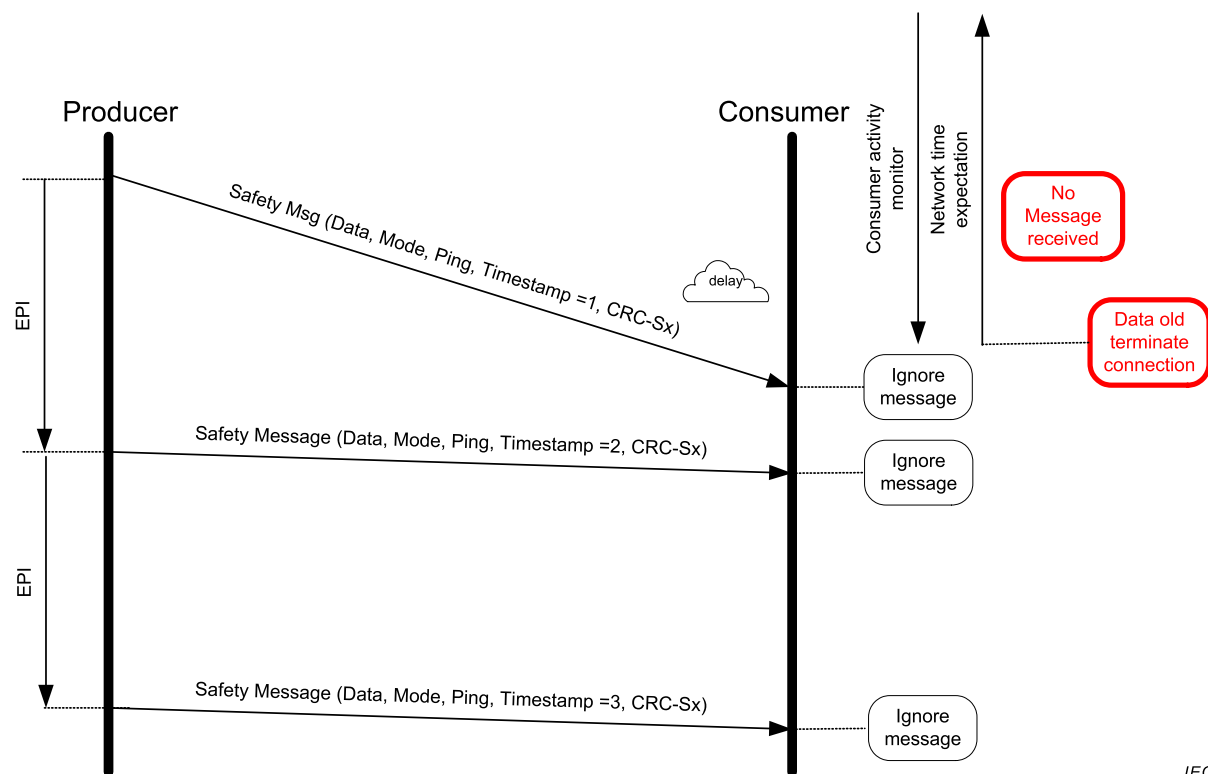
Figure 41 – Diagramme séquentiel d'un message producteur vers consommateur perdu

La transmission des messages peut être retardée. Si un message est retardé de sorte

- qu'il est reçu au-delà du 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 la connexion doit être terminée.

Dans les deux cas, le consommateur termine la connexion (voir 7.2.2) et passe à l'état de sécurité défini. Ce comportement est défini à la Figure 42.



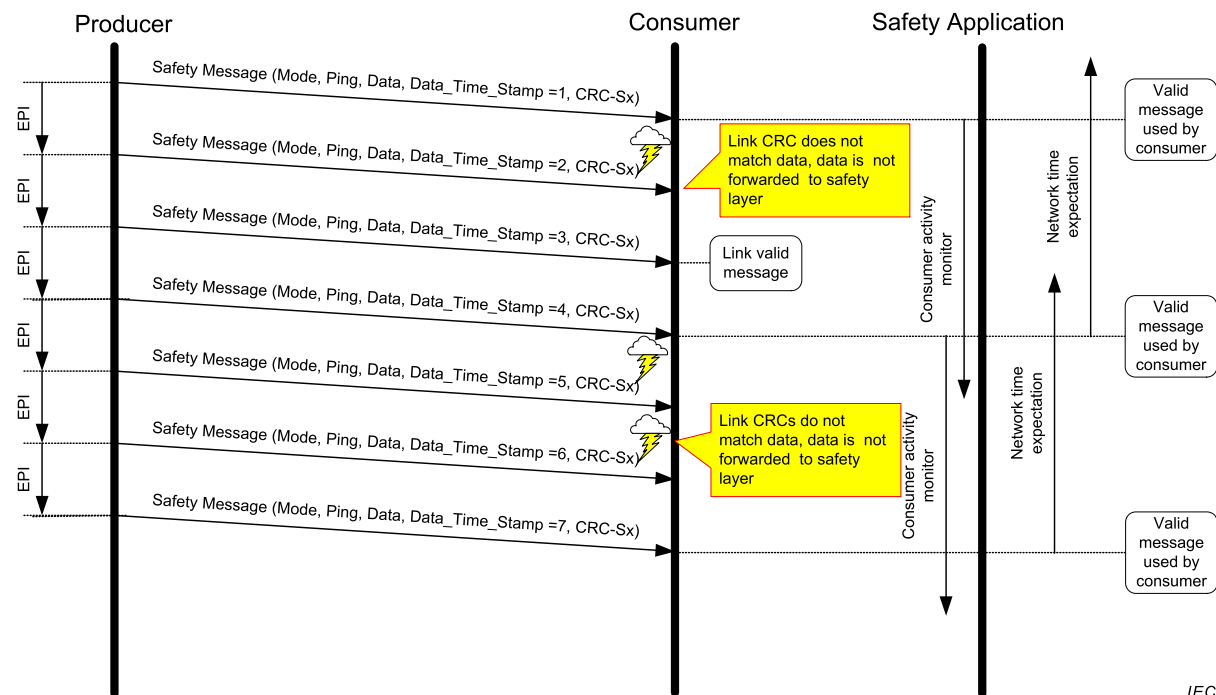
IEC

Anglais	Français
producer	producteur
consumer	consommateur
safety message	message de sécurité
no message received	aucun message reçu
network time expectation	délai du réseau
consumer activity monitor	contrôleur d'activité du consommateur
data old terminate connection	les anciennes données terminent la connexion
ignore message	ignorer message
delay	retard

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 soit corrompu, tel que défini à la Figure 43. La production peut être répétée afin de minimiser les déclenchements de nuisance et accroître la disponibilité du système entier.



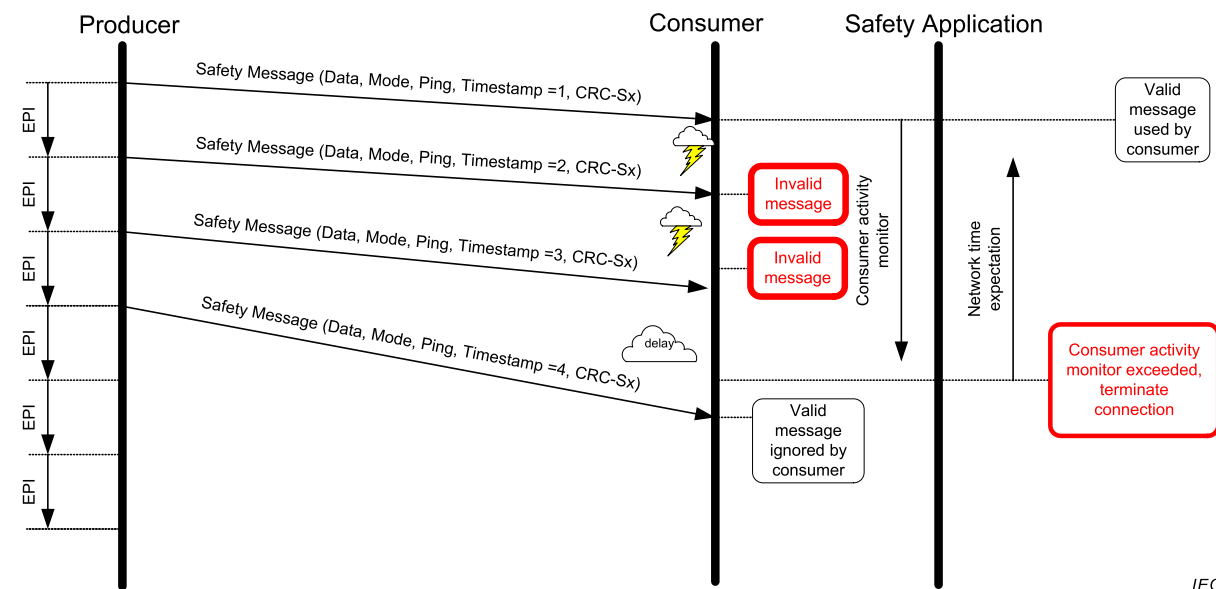
Anglais	Français
producer	producteur
consumer	consommateur
safety application	application de sécurité
safety message	message de sécurité
valid message used by consumer	message valide reçu par le consommateur
network time expectation	délai du réseau
consumer activity monitor	contrôleur d'activité du consommateur
Link CRC does not match data, data is not forwarded to safety layer	Le CRC de liaison ne correspond pas aux données, les données ne sont pas transmises à la couche de sécurité
link valid message	message de liaison valide

Figure 43 – Diagramme séquentiel d'un message producteur vers consommateur corrompu avec production répétée

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.

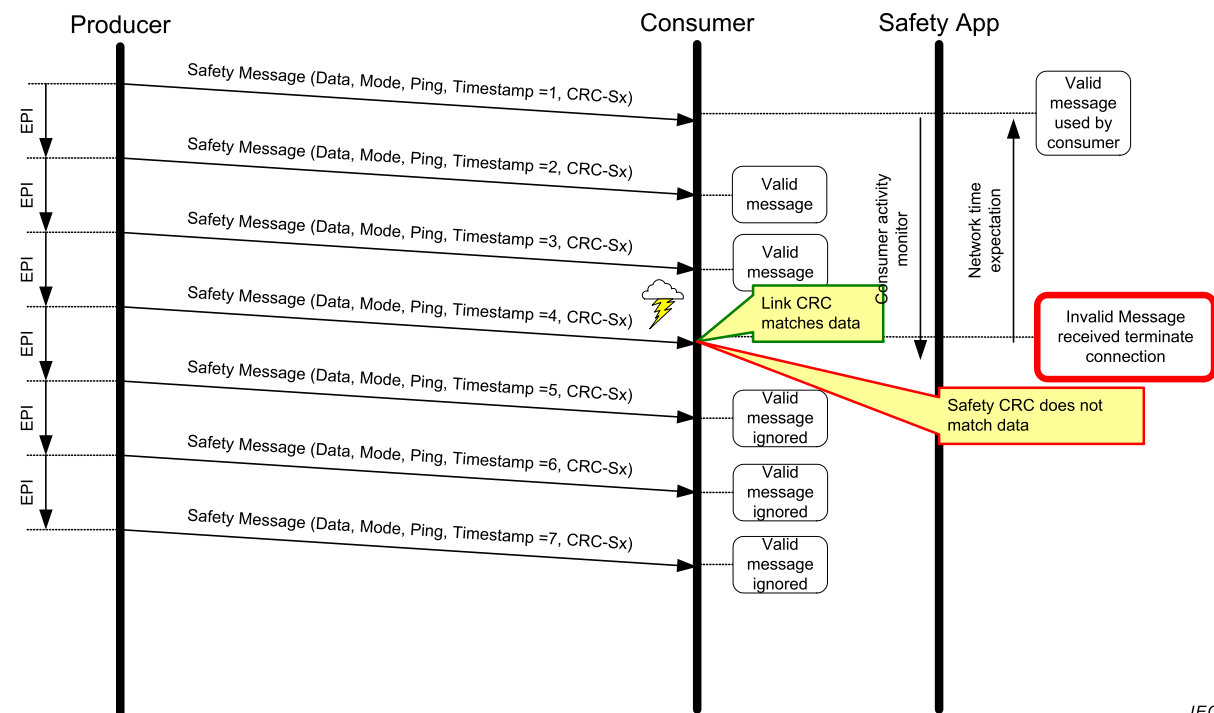
Il peut être possible, en raison de perturbations extérieures, qu'une série de messages soit retardée, entraînant la perte de la connexion. Cette séquence est définie à la Figure 44. La connexion est terminée si aucun message valide n'est reçu avant expiration du temporisateur périodique du consommateur



Anglais	Français
producer	producteur
consumer	consommateur
safety application	application de sécurité
safety message	message de sécurité
valid message used by consumer	message valide reçu par le consommateur
network time expectation	délai du réseau
consumer activity monitor	contrôleur d'activité du consommateur
invalid message	message invalide
Delay	retard
consumer activity monitor exceeded, terminate connection	délai du contrôleur d'activité du consommateur dépassé, terminaison de la connexion
valid message ignored by consumer	message valide ignoré par le consommateur

Figure 44 – Diagramme séquentiel d'une terminaison de connexion occasionnée par des retards

Un message de liaison valide qui ne satisfait pas au contrôle CRC de sécurité conduira le consommateur à supposer que la liaison sous-jacente n'est pas fiable et, selon le format utilisé et/ou le nombre d'occurrences, peut provoquer la terminaison de la connexion. Cette séquence est définie à la Figure 45.



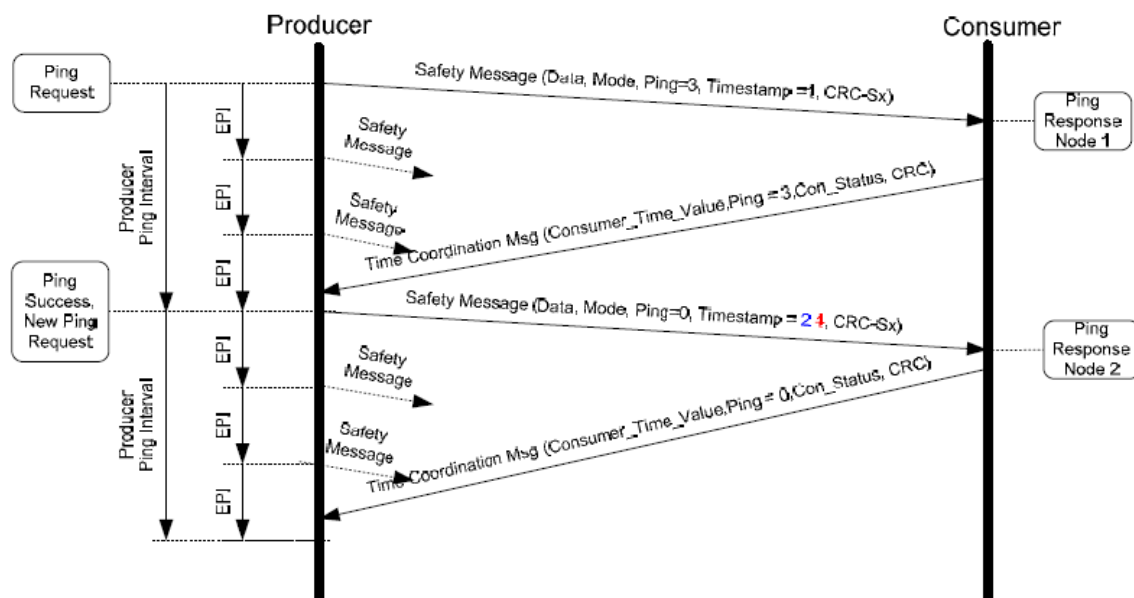
IEC

Anglais	Français
Producer	producteur
Consumer	consommateur
safety application	application de sécurité
safety message	message de sécurité
valid message used by consumer	message valide reçu par le consommateur
network time expectation	délai du réseau
consumer activity monitor	contrôleur d'activité du consommateur
valid message	message valide
link CRC matches data	le CRC de liaison correspond aux données
invalid message received terminate connection	message invalide reçu, terminaison de la connexion
valid message ignored	message valide ignoré
safety CRC does not match data	le CRC de sécurité ne correspond pas aux données

Figure 45 – Diagramme séquentiel d'un contrôle CRC de sécurité non satisfait

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.



IEC

Anglais	Français
Producer	producteur
Consumer	consommateur
safety message	message de sécurité
ping request	demande Ping
producer ping interval	intervalle Ping du producteur
ping response	réponse à demande Ping
Node	nœud
ping success, new ping request	demande ping satisfaisante, nouvelle demande Ping
time coordination msg	message de coordination temporelle

Figure 46 – Diagramme séquentiel d'une demande Ping point à point – réponse normale

À chaque intervalle Ping de producteur point à point, le comptage de demandes Ping doit être incrémenté dans l'en-tête de message de sécurité disponible suivant.

L'intervalle Ping de producteur point à point doit être un multiple de l'EPI; les demandes Ping doivent être formulées à une fréquence basée sur le Ping_Interval_EPI_Multplier.

Lorsqu'un consommateur point à point constate une modification dans le comptage de demandes Ping, il génère un message de coordination temporelle.

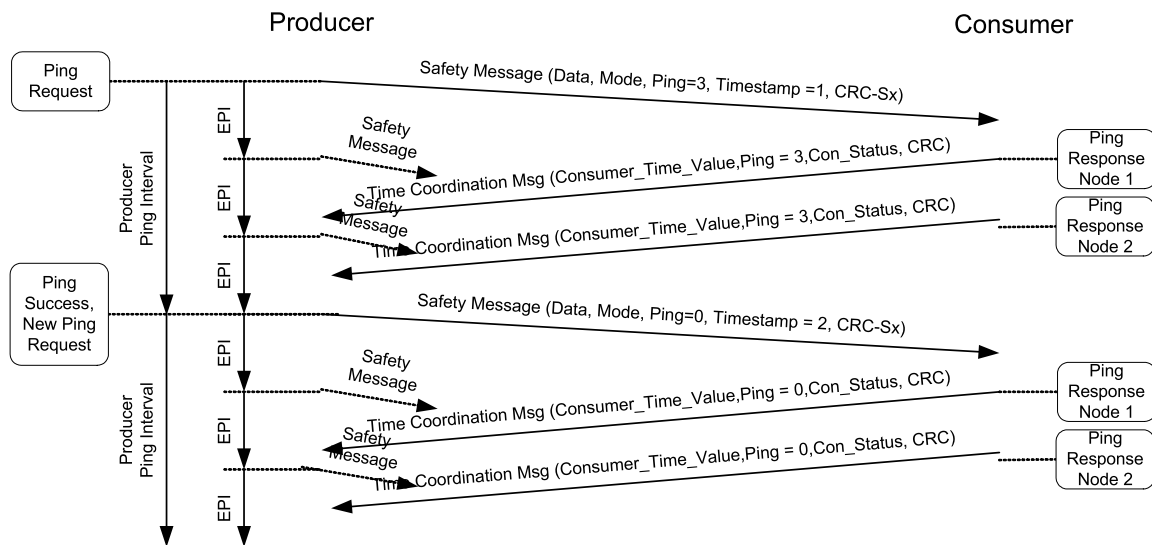
Le message de coordination temporelle (voir 7.5.2) doit être reçu par le producteur dans un délai prescrit. Si le message de coordination temporelle n'est pas reçu dans ce délai, le producteur doit terminer la connexion (voir 7.2.2).

7.5.6 Demande Ping multipoints avec sécurité CP 2/3

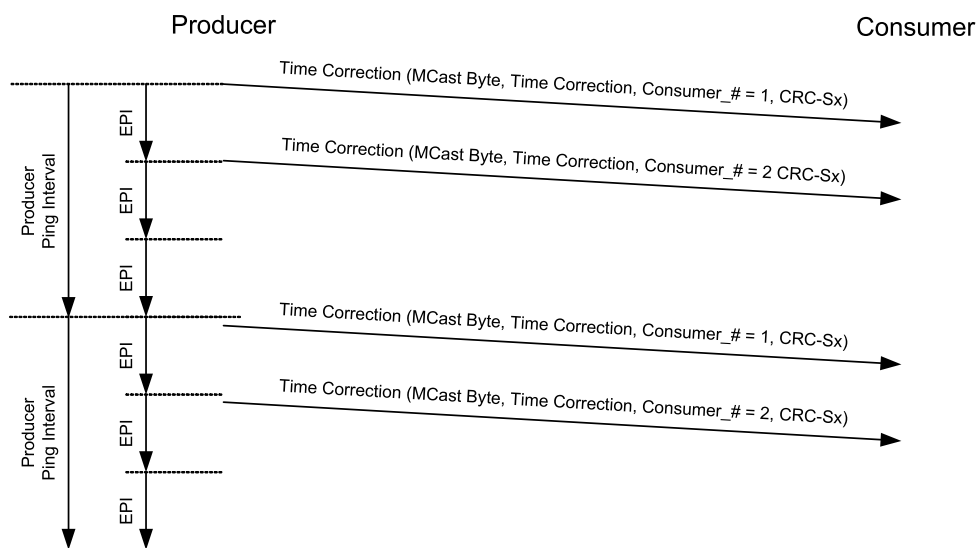
Une séquence de transaction de messages de demande et de réponse Ping permet de maintenir une temporisation cohérente entre producteurs et consommateurs.

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 multipoints.

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 multipoints est définie à la Figure 47. Le message de correction de temps est défini sur un diagramme séparé pour des raisons de clarté.



Data Message and Time Coordination Message



Time Correction Message

IEC

Anglais	Français
Producer	producteur
Consumer	consommateur
safety message	message de sécurité
ping request	demande Ping
producer ping interval	intervalle Ping du producteur
ping response	réponse à demande Ping
Node	Nœud
ping success, new ping request	demande ping satisfaisante, nouvelle demande Ping
time coordination msg	message de coordination temporelle
data message and time coordination message	message de données et message de coordination temporelle

Anglais	Français
time correction	correction de temps
time correction message	message de correction de temps

Figure 47 – Diagramme séquentiel d'une demande Ping multipoints satisfaisante, sécurité CP 2/3

Pendant chaque intervalle Ping de producteur multipoints, une demande Ping est transmise par les producteurs multipoints aux consommateurs multipoints sollicitant une réponse.

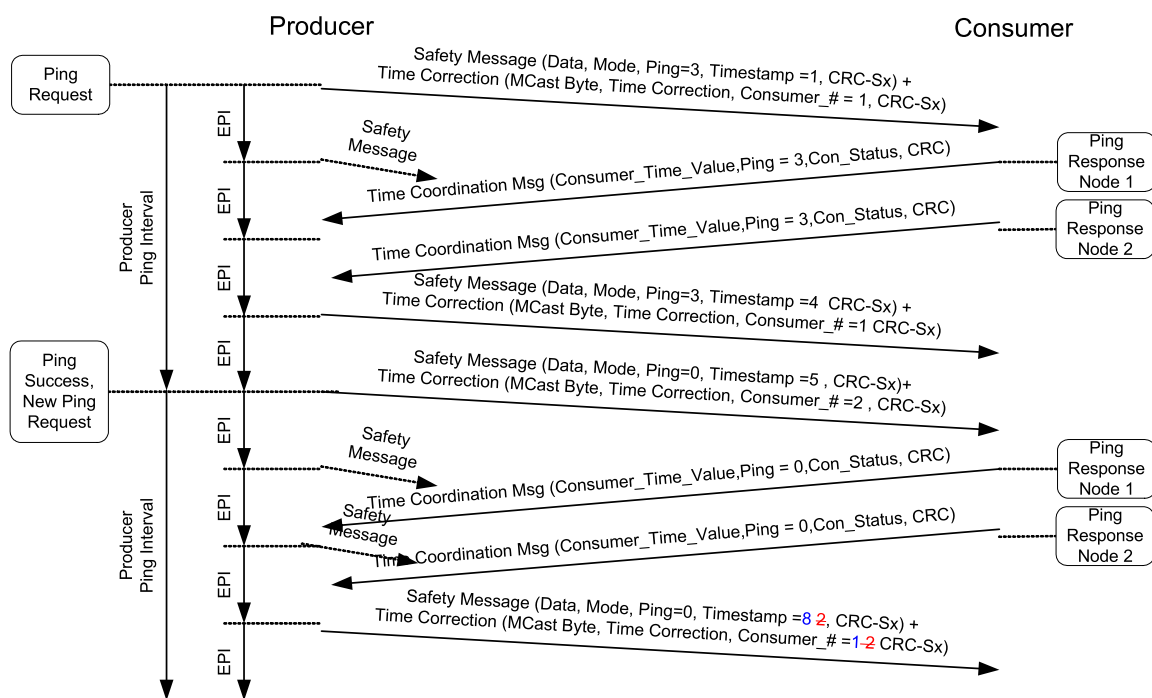
Tous les consommateurs multipoints doivent répondre à une modification de la valeur de demande Ping, et les consommateurs autres que le consommateur 1 doivent attendre $\text{Consumer\_Number} - 1 \times \text{l'EPI}$ pour répondre.

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 multipoints sur les réseaux de sécurité CP 2/2

Une demande et une réponse à 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 multipoints est définie à la Figure 48.



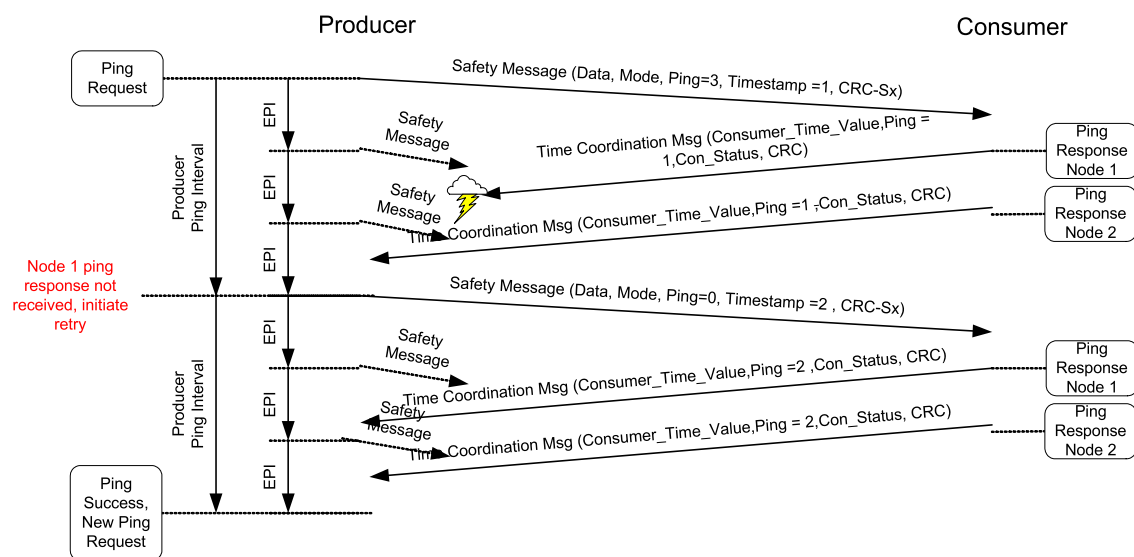
Anglais	Français
Producer	producteur
Consumer	consommateur
safety message	message de sécurité
ping request	demande Ping
producer ping interval	intervalle Ping du producteur
ping response	réponse à demande Ping
Node	nœud
ping success, new ping request	demande ping satisfaisante, nouvelle demande Ping
time coordination msg	message de coordination temporelle
data message and time coordination message	message de données et message de coordination temporelle
time correction	correction de temps
time correction message	message de correction de temps

Figure 48 – Diagramme séquentiel d'une demande Ping multipoints satisfaisante, sécurité CP 2/2

Pendant chaque intervalle Ping de producteur, une demande Ping est transmise par les producteurs multipoints aux consommateurs multipoints sollicitant une réponse.

7.5.8 Demande Ping multipoints – Retransmission aboutie

Cette séquence de messages pour une demande Ping multipoints avec retransmissions est définie à la Figure 49. La connexion de correction de temps n'est pas définie pour des raisons de clarté.



IEC

Anglais	Français
Producer	producteur
Consumer	consommateur
safety message	message de sécurité
ping request	demande Ping
producer ping interval	intervalle Ping du producteur
ping response	réponse à demande Ping
Node	nœud

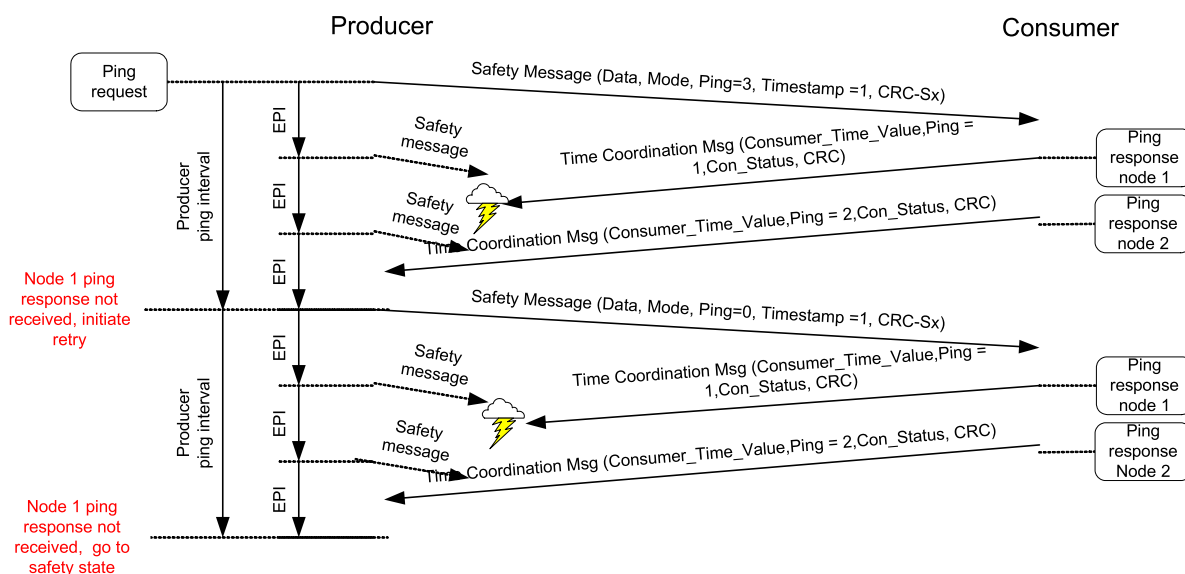
Anglais	Français
ping success, new ping request	demande ping satisfaisante, nouvelle demande Ping
time coordination msg	message de coordination temporelle
node 1 ping response not received, initiate retry	réponse à demande Ping de nœud 1 non reçue, lancer retransmission

Figure 49 – Diagramme séquentiel d'une retransmission de demande Ping multipoints

La perte ou le retard d'un message de coordination temporelle multipoints après les intervalles Ping ($\text{Timeout\_Multiplier.PI} + 2$) doit entraîner la génération d'une erreur et la fermeture de la connexion.

7.5.9 Demande Ping multipoints – Retransmission avec temporisation

Cette séquence de messages pour une demande Ping multipoints 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.



IEC

Anglais	Français
Producer	producteur
Consumer	consommateur
safety message	message de sécurité
ping request	demande Ping
producer ping interval	intervalle Ping du producteur
ping response	réponse à demande Ping
Node	nœud
time coordination msg	message de coordination temporelle
node 1 ping response not received, initiate retry	réponse à demande Ping de nœud 1 non reçue, lancer retransmission
node 1 ping response not received, go to safety state	réponse à demande Ping de nœud 1 non reçue, passer à l'état de sécurité

Figure 50 – Diagramme séquentiel d'une temporisation de demande Ping multipoints

Si la réponse à 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 sera déjà passé à un état de sécurité.

7.6 Définition du protocole de sécurité

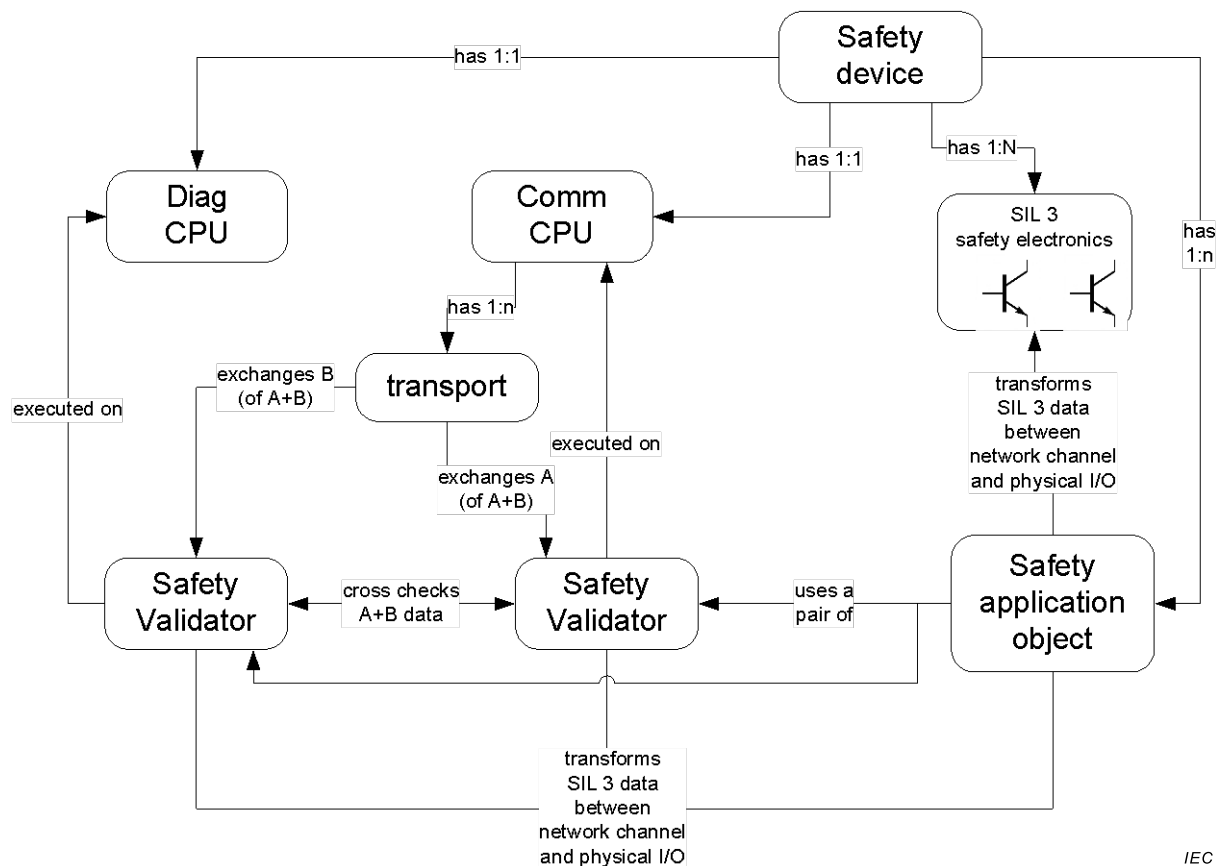
7.6.1 Généralités

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, tel que défini à la Figure 51. 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 dans une application SIL 3. Ce comportement est mis en œuvre en tant qu'objet de validation de sécurité tel que décrit en 6.7.

NOTE Plusieurs méthodes peuvent permettre de réaliser ce comportement souhaité. Les objets indiqués dans ce paragraphe sont à considérer comme modèle de référence. Des produits et des applications individuels peuvent choisir de mettre en œuvre ce comportement, s'ils le considèrent 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 modèle de référence d'un appareil de sécurité contenant 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 SIL 3 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 SIL 3. 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. Ce modèle suppose une topologie de sécurité 1oo2 dans laquelle deux CPU indépendants participent au protocole de sécurité.



IEC

Anglais	Français
safety device	appareil de sécurité

Anglais	Français
diag CPU	CPU diag
comm CPU	CPU comm
SIL 3 safety electronics	circuits électroniques de sécurité SIL 3
has ...	a ...
executed on	exécuté sur
exchanges ...	échange ...
(of A+B)	(de A+B)
transforms SIL 3 data between network channel and physical I/O	transforme les données SIL 3 entre le canal du réseau et les E/S physiques
safety validator	objet de validation de sécurité
cross checks A+B data	contre-vérification des données A+B
uses a pair of	utilise une paire de
safety application object	objet d'application de sécurité

Figure 51 – Diagramme de relations des entités de modèle de référence d'un appareil de sécurité

7.6.3 Objet de validation de sécurité

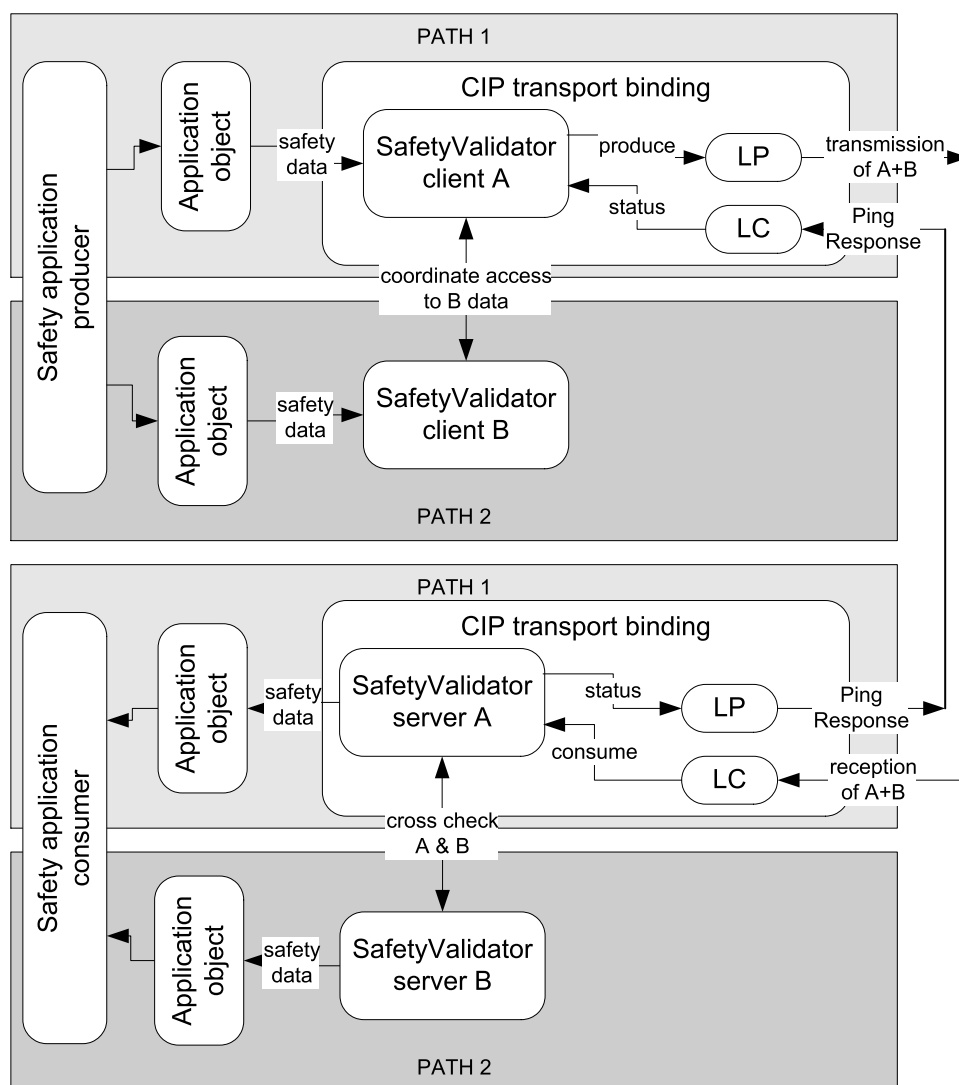
Le paragraphe 6.7 définit un Objet de validation de sécurité duquel les fonctions SafetyValidatorServer et SafetyValidatorClient sont mises en œuvre.

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 52 représente une vue de haut niveau de deux appareils qui échangent des données via un SafetyValidatorClient et un SafetyValidatorServer. Une application de production de sécurité utilise un SafetyValidatorClient pour transmettre des données de sécurité à une application de consommation de sécurité qui utilise un 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.



IEC

Anglais	Français
PATH	CHEMIN
safety application producer	producteur d'application de sécurité
application object	objet d'application
CIP transport binding	rattachement de transport CIP
safety data	données de sécurité
produce	produit
transmission of	transmission de
status	état
ping response	réponse à demande Ping
coordinate access to B data	coordonne l'accès aux données B
safety application consumer	consommateur d'application de sécurité
consume	consomme
reception of	réception de
cross check	contre-vérification

Figure 52 – Deux appareils échangeant des données de sécurité via un SafetyValidatorClient et un SafetyValidatorServer

7.6.5 Gestion du remplacement de la datation de format étendu

7.6.5.1 Généralités

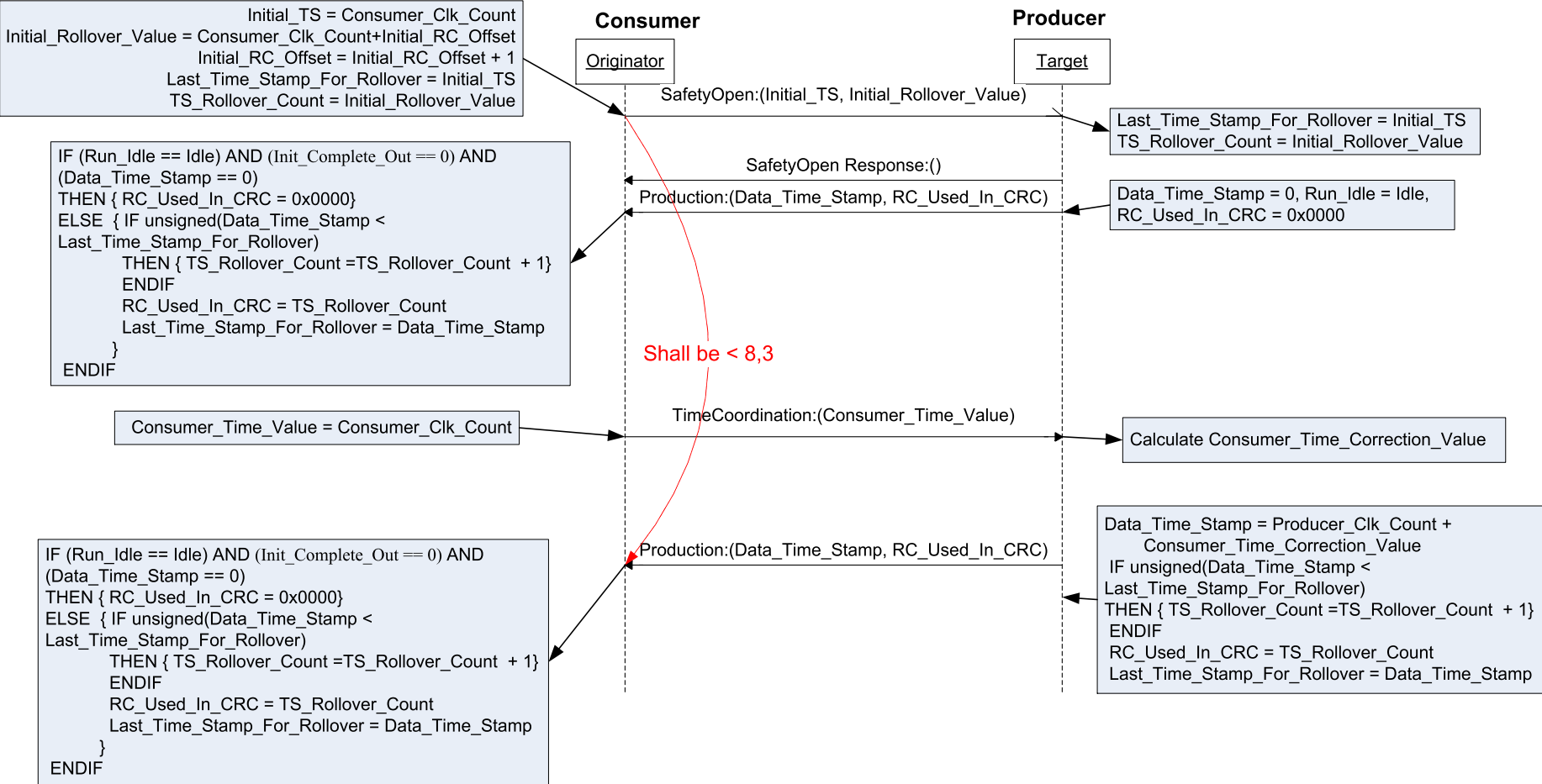
Le Format étendu requiert une synchronisation coordonnée entre les producteurs et les consommateurs lors de l'établissement d'une connexion associée à des opérations de maintenance, afin de détecter et gérer les événements de remplacement de datation. Les paragraphes suivants 7.6.5.2 à 7.6.5.4 présentent de manière graphique ces opérations pour chaque cas unique. 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.

Le processus complet est représenté à la Figure 53.



IEC

Anglais	Français
consumer	consommateur
producer	producteur
originator	point d'origine

Anglais	Français
target	cible
shall be	doit être
calculate ...	calculer

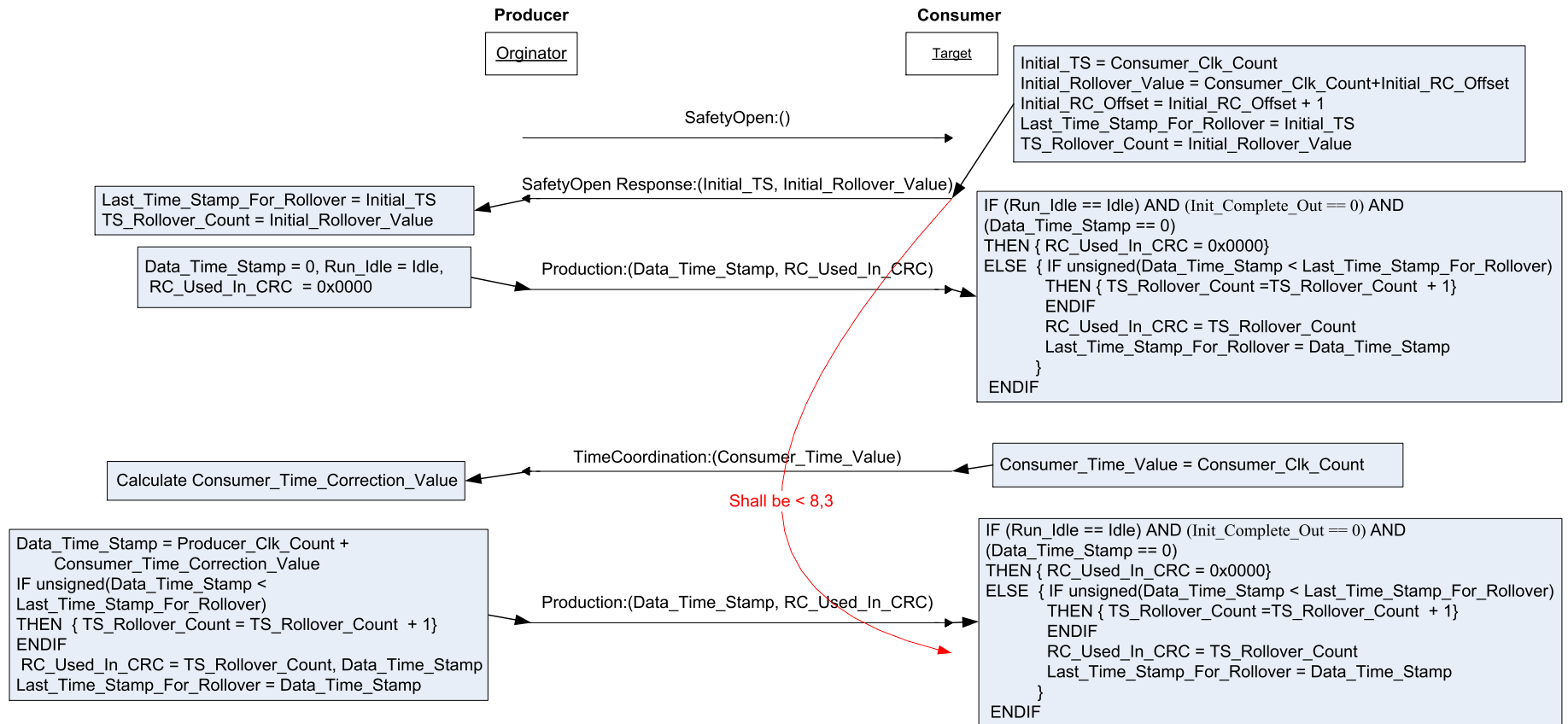
Figure 53 – Consommateur d’origine et producteur cible point à point

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 secondes.

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 54.



Anglais	Français
consumer	consommateur
producer	producteur
originator	point d'origine
target	cible
shall be	doit être
calculate ...	calculer

Figure 54 – Producteur d'origine et consommateur cible point à point

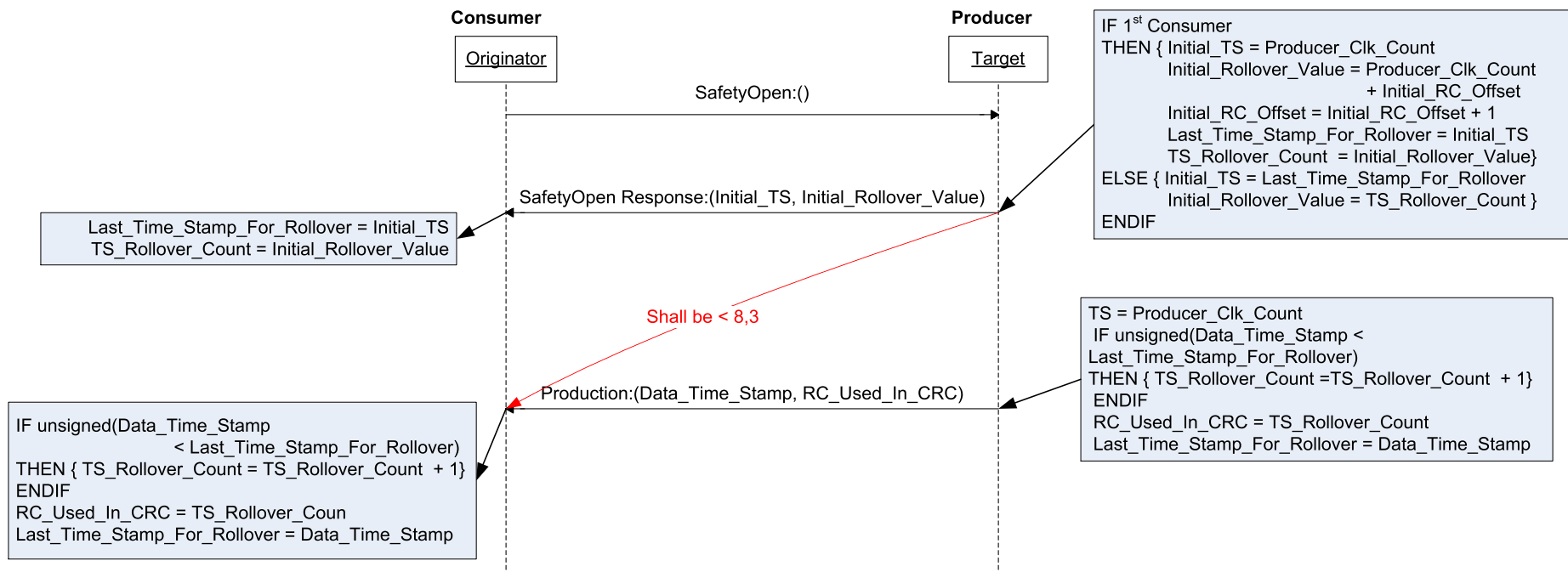
Le temps qui s'écoule entre la génération de la réponse SafetyOpen et le traitement par les consommateurs du premier paquet produit après la réception par les producteurs du message Time_Coordination doit être inférieur à 8,3 secondes.

7.6.5.4 Consommateur d'origine et producteur cible multipoints

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.

Le marquage actif du CRC par le comptage de remplacement dans les messages multipoints de Format Etendu doit commencer immédiatement à la première production.

Le processus complet est représenté à la Figure 55.



Anglais	Français
consumer	consommateur
producer	producteur
originator	point d'origine
target	cible
shall be	doit être

Figure 55 – Consommateur d’origine et producteur cible multipoints

Le temps qui s’écoule entre la génération de la réponse Safety Open et le traitement par les consommateurs du premier paquet doit être inférieur à 8,3 secondes.

7.6.6 Définition de la fonction SafetyValidatorClient

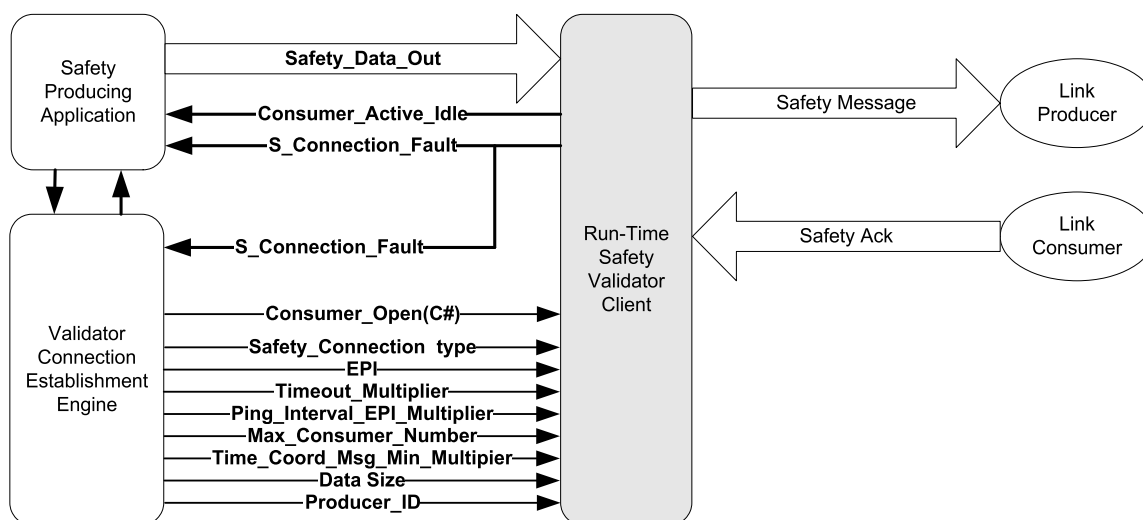
7.6.6.1 Généralités

Le 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 SIL 3. Il coordonne la production des données d'application avec une instance homologue du SafetyValidatorClient.

7.6.6.2 Production de sécurité

Le présent paragraphe 7.6.6 décrit la production des données et les interfaces entre l'application, le SafetyValidatorClient et la couche de liaison sous-jacente. Le comportement d'exécution de SafetyValidatorClient et ses interfaces constituent l'objet du présent paragraphe. L'application proprement dite doit présenter une intégrité élevée, ce qui peut être accompli de nombreuses manières et constitue une décision de conception finale du fournisseur.

La Figure 56 représente graphiquement le flux de données entre le 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). Le SafetyValidatorClient doit échantillonner, saisir et dater les données à transmettre à chaque période EPI.



IEC

Anglais	Français
safety producing application	application de production de sécurité
safety message	message de sécurité
link producer	producteur de liaison
link consumer	consommateur de liaison
safety Ack	Acq. de sécurité
run-time safety validator client	Safety validator client d'exécution
validator connection establishment engine	unité d'établissement de connexion d'objet de validation

Figure 56 – Flux de données de production de sécurité

7.6.6.3 Interface d'application de production

L'application de production fournit le Safety_Data_Out au SafetyValidatorClient. Le SafetyValidatorClient doit élaborer les Mode_Octet, Actual_Data et Complement_Data, ainsi que la section de datation.

Le 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

Les paragraphes 7.6.6.4 à 7.6.6.8 décrivent la logique que tous les producteurs de données de sécurité doivent suivre. La mise en œuvre réelle de la logique peut varier, mais des résultats équivalents doivent être obtenus. La logique définie dans le présent document suppose une application de production asynchrone qui met les données de sécurité à disposition du SafetyValidatorClient.

Les définitions relatives aux variables utilisées dans la logique de production de données de sécurité sont données 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_Rcvd_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
}
ENDFOR

```

```

////////////////////////////////////
// end, Cold start after connection establishment processing
////////////////////////////////////

```

7.6.6.6 Exemple de logique de réamorçage d'un consommateur multipoints pour la production de données de sécurité

Cette logique permet l'arrêt et le réamorçage de chaque consommateur multipoints, tandis que la production multipoints destinée à d'autres consommateurs se poursuit.

Le présent paragraphe 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 Multipoints production to individual consumers
////////////////////////////////////
// This Logic should be executed after a multipoints consumer performs
// a successful open to a multipoints 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_Rcvd_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
}
ENDIF
}
```

7.6.6.7 Exemple de production de données combinée

La logique exigée commune du 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 == multipoints),
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 Multipoints, 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
////////////////////////////////////////////////////////////////

////////////////////////////////////////////////////////////////
// Start of multipoints 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

// 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 multipoints processing
////////////////////

```

7.6.6.8 Exemple de logique de réception des messages de coordination temporelle

Le 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 multipoints
////////////////////
// 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_Rcvd_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
{
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
// multipoints 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)
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_Rcvd_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 asynchronous
// clocks. This value will not be used until the second
// Time_Coordination message is received.

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 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 SIL 3. Elle coordonne la réception des données de sécurité avec une instance homologue de la classe du SafetyValidatorClient et fournit ces données à l'application relative à la sécurité de consommation.

7.6.7.2 Consommation de sécurité

Le présent paragraphe 7.6.7 décrit la consommation des données et les interfaces entre l'application, le SafetyValidatorServer et la couche de liaison sous-jacente.

Il existe deux versions de contrôle des consommateurs de données de sécurité. Il s'agit des:

- SafetyValidatorServer – Déclenché 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 – Déclenché par l'application.
Ceci convient aux applications de consommation à caractère périodique et non synchronisées sur la réception des données.

Dans les deux versions, le 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 – déclenché par la liaison

La Figure 57 représente les flux de données applicables au SafetyValidatorServer dans le mode déclenché par la liaison.

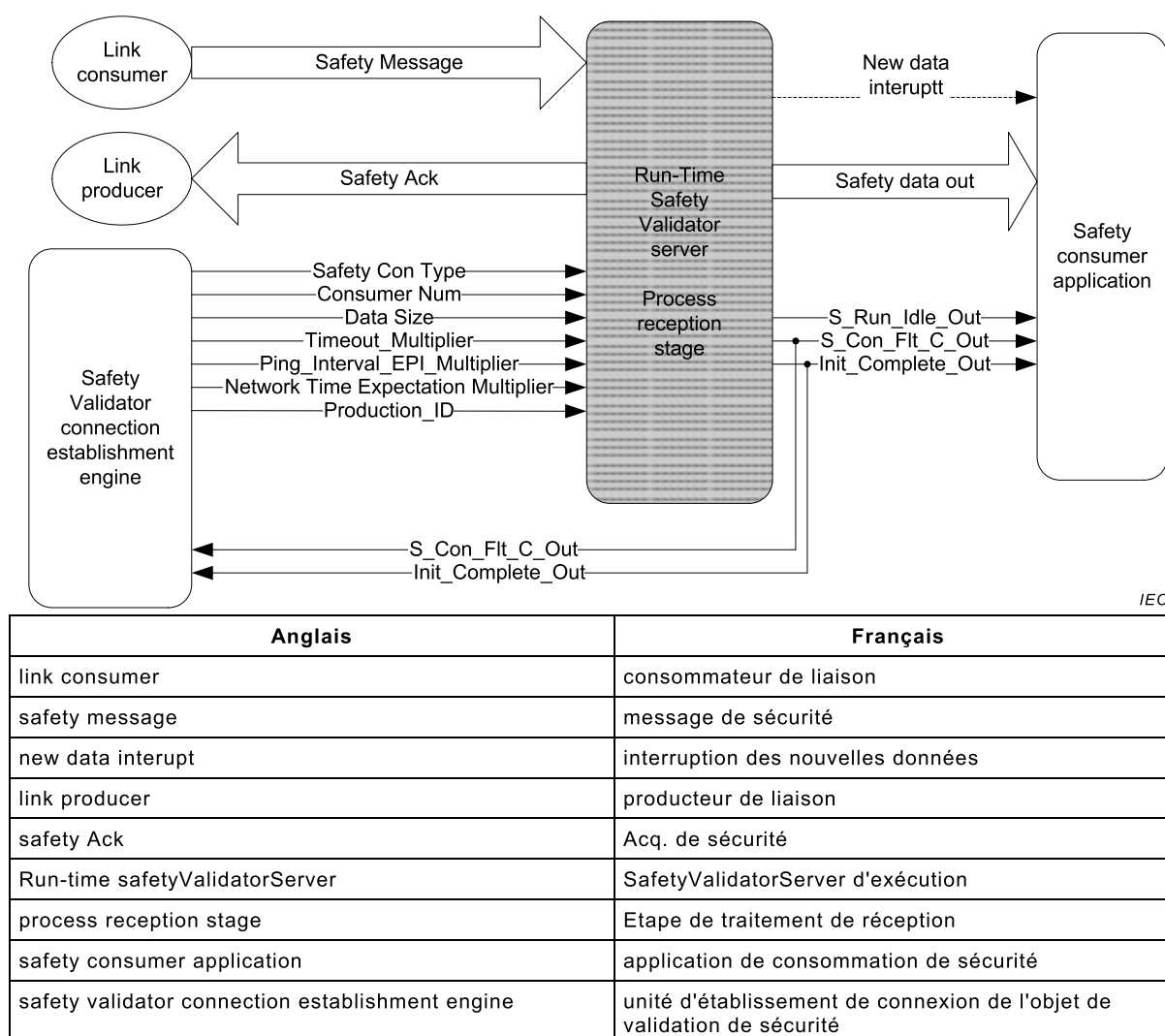


Figure 57 – Contrôle des données de sécurité de consommation

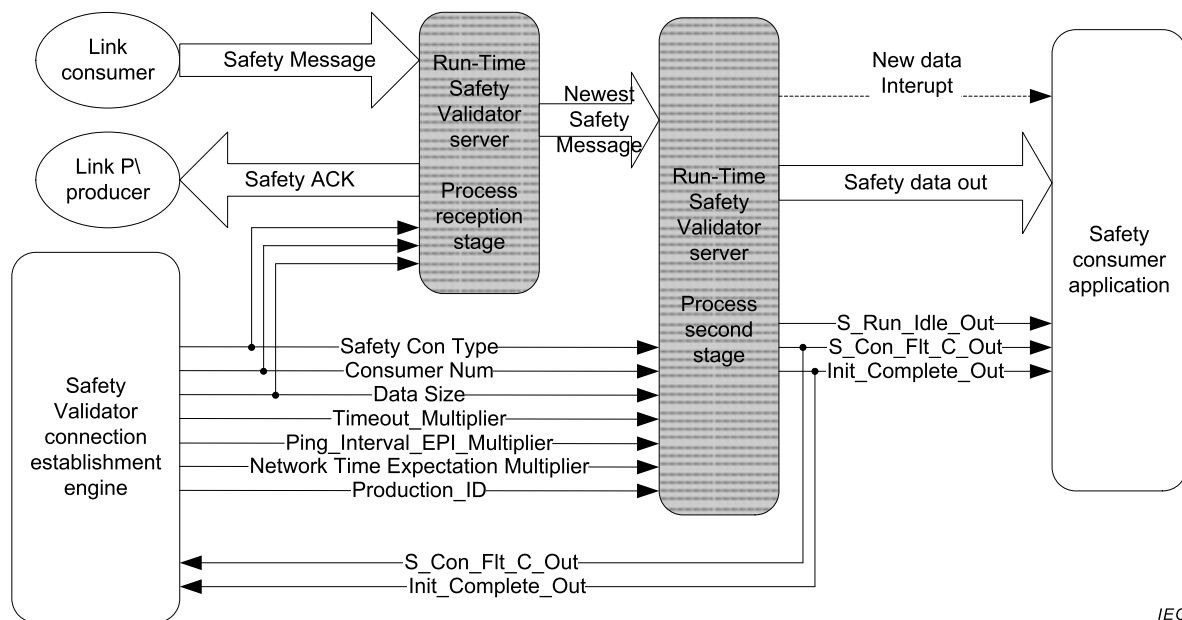
Le SafetyValidatorServer déclenché par la liaison doit exécuter tous les aspects du protocole de sécurité de chaque message reçu.

Pour les connexions multipoints, le SafetyValidatorServer déclenché par la liaison doit exécuter également tous les aspects du protocole de sécurité de chaque section Time_Correction reçue.

Le 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.

Le SafetyValidatorServer déclenché par la liaison doit régler le nouveau drapeau de données à chaque fois que les données sont prêtes à être utilisées.

7.6.7.4 SafetyValidatorServer – déclenché par l'application



Anglais	Français
link consumer	consommateur de liaison
safety message	message de sécurité
new data interrupt	interruption des nouvelles données
safety Ack	Acq. de sécurité
Run-time safetyValidatorServer	SafetyValidatorServer d'exécution
safety consumer application	application de consommation de sécurité
safety validator connection establishment engine	unité d'établissement de connexion de l'objet de validation de sécurité
newest safety message	nouveau message de sécurité
link P producer	liaison P-producteur
process reception stage	étape de réception de traitement
safety data out	sortie des données de sécurité
process second stage	deuxième étape de traitement

Figure 58 – SafetyValidatorServer – déclenché par l'application

Le SafetyValidatorServer déclenché par l'application ne traite pas entièrement chaque message.

L'étape de réception de traitement du SafetyValidatorServer déclenché par l'application doit vérifier le comptage de demandes Ping pour tous les messages de données entrants.

Pour la consommation multipoints des SafetyValidatorServers déclenchés 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 du 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 58 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;
- un contrôle 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 sont données en 7.7.7.6.

Le Tableau 91 définit les étapes de traitement des données de sécurité exécutées par le SafetyValidatorServer déclenché par la liaison.

Tableau 91 – Réception des données – Déclenchée par la liaison

	Point à point	Multipoints
Contrôle de Ping_Response	Non	Non
Contrôle de Ping_Count	Oui	Oui
Contrôle du CRC de 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 92 définit les étapes de traitement des données de sécurité qui doivent être exécutées par le SafetyValidatorServer déclenché par la liaison pour la réception de chaque section de correction de temps.

Tableau 92 – Réception Time_Correction – Déclenchée par la liaison

Multipoints	Multipoints
Contrôle MCast_Octet et MCast_Octet_	Oui, si adaptation de consumer_#
Contrôle du CRC de Time_Correction	Oui, si adaptation de consumer_#
Obtention de Time_Correction_Value	Oui, si adaptation de consumer_#
Contrôle de Multi_Cast_Active_Idle	Oui, si adaptation de consumer_#

Le Tableau 93 définit les étapes de traitement des données de sécurité exécutées à la réception de chaque message par le SafetyValidatorServer déclenché par l'application.

Tableau 93 – Réception des données – Déclenchée par l'application

	Point à point	Multipoints
Contrôle de Ping_Response	Non	Non
Contrôle de Ping_Count	Oui	Oui
Contrôle du CRC de 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 94 définit les étapes de traitement des données de sécurité qui doivent être exécutées à réception de chaque section Time_Correction par les SafetyValidatorServers déclenchés par l'application.

Tableau 94 – Réception de Time_Correction – Déclenchée par l'application

	Multipoints
Contrôle de MCast_Octet et MCast_Octet_2	Transmission du message si adaptation de consumer_#
Contrôle du CRC de Time_Correction	Non
Obtention de Time_Correction_Value	Non
Contrôle de Multi_Cast_Active_Idle	Non

Le Tableau 95 définit les étapes de traitement des données de sécurité exécutées par le SafetyValidatorServer déclenché par l'application, en cas de sollicitation des données de sécurité.

Tableau 95 – Application de consommation – Contrôle des données de sécurité

	Point à point	Multipoints
Contrôle de Ping_Response	NA	NA
Contrôle de Ping_Count	NA	NA
Contrôle du CRC de section de datation	Oui	Oui
Contrôle de MCast_Octet et MCast_Octet_2	NA	Oui (à partir de la dernière correction)
Contrôle du CRC de Time_Correction	NA	Oui (à partir de la dernière correction)
Obtention de Time_Correction_Value	NA	Oui (à partir de la dernière correction)
Contrôle de Multi_Cast_Active_Idle	NA	Oui (à partir de la dernière correction)
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

7.6.7.6 Contrôle des comptages de demandes Ping

Le 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 un 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 petite 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 de 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 paragraphes 7.6.7.10 et 7.6.7.11 décrivent la logique de réception des données de sécurité du consommateur pour le SafetyValidatorServer – option déclenchée par la liaison. L'expression «Déclenché par la liaison» signifie que la logique dans son ensemble est exécutée à chaque réception.

Le paragraphe 7.6.7.10 décrit la logique combinée associée à la réception des paquets de données de sécurité pour les types de connexion de sécurité point à point et multipoints.

Le paragraphe 7.6.7.11 décrit la logique associée à la réception des messages de correction de temps pour le type de connexion de sécurité multipoints.

Cette logique doit être exécutée uniquement 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 multipoints, pour le SafetyValidatorServer – Logique déclenchée par la liaison.

Les connexions multipoints doivent transmettre un message de coordination temporelle (Consumer_Num – 1) après variation du comptage 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)),
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

// 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 == Multipoints),
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 multipoints
connection
    // or if this is a point to point connection that is out of the
initialization
    // phase.
    IF ((Connection_Type == Multipoints) 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,
}
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 multipoints, 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

END single_cast_consumer_function()
////////////////////////////////////
// end of point to point processing
////////////////////////////////////

////////////////////////////////////
// Start of multipoints consumer function
////////////////////////////////////
multi_cast_consumer_function()
// If multipoints, 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 multipoints, add correction value to time stamp
Corrected_Data_Time_Stamp = Time_Stamp_Section.Data_Time_Stamp +
    Last_Rcvd_Time_Correction_Value
// Determine the Init_Complete_Out state to be passed on to the
// consuming application.
// For multipoints, 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
multipoints
    (Last_Rcvd_Multi_Cast_Active_Idle==Idle))//used only on
multipoints
THEN
{
    S_Run_Idle_Out_Temp = Idle,
}
ELSE
{
    S_Run_Idle_Out_Temp = Run,
}
ENDIF
end multi_cast_consumer_function()
////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////
// end of multipoints processing
////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////

////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////////
// Start of ping count check function
////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////////
ping_count_check_in_consumer_function()

// Check if its time to send a Time Coordination Message
// Multipoints 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 multipoints-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 multipoints, pour le consommateur – déclenché 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.
    THEN
    {
        IF (Time_Coordination_message_CRC_incorrect)
        OR (MCast_Octet_parity_incorrect)
        OR {MCast_Octet_2 != ((MCast_Octet XOR 0xFF) AND 0x55)
            OR (MCast_Octet AND 0xAA))
            OR {(MCast_Octet.Multi_Cast_Active_Idle == Idle)
        AND (Last_Rcvd_Multi_Cast_Active_Idle == Active)},
        // only one transition from connection idle to active will
        // be allowed, to prevent an erroneous idle indication,
        // a transition 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_Rcvd_Time_Correction_Value =
    Time_Correction_Section.Time_Correction_Value,

    // Save the Multi_Cast_Active_Idle bit.
    Last_Rcvd_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 le SafetyValidatorServer – déclenché par l'application, la même logique décrite ci-dessus doit être appliquée par la combinaison du SafetyValidatorServer, mais uniquement lorsque sollicité 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 typique. Les fonctions peuvent être réparties tel que défini dans le Tableau 92 et le Tableau 95.

Les étapes de traitement de protocoles définies dans le Tableau 95 nécessitent d'être exécutées uniquement avec les messages utilisés par l'application de consommation.

7.6.7.13 Exemple de logique de production des messages de coordination temporelle

Le 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 décrite également 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,

    // 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 de mode

7.7.1.1 Mode_Octet.Run_Idle

La valeur nulle du bit Run_Idle doit indiquer l'état Repos (Idle), et la valeur 1 du bit Run_Idle doit indiquer l'état Exécution (Run).

Pour les connexions point à point, le bit Run_Idle doit être réglé 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 à recevoir au début de la production des données.

Si ces informations ont été reçues, le bit Run_Idle doit être réglé sur l'état Run_idle indiqué par l'application de production.

Pour les connexions multipoints, le bit Run_Idle doit être réglé 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 compléter le bit Run_Idle

7.7.1.3 Mode_Octet.TBD_2_Bit

Le Mode_Octet Reserved TBD_2_bit doit être réglé 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.

7.7.1.5 Mode_Octet.Ping_Count

Le consommateur utilise le Ping_Count pour déterminer le moment où il convient d'envoyer un message de coordination temporelle.

7.7.1.6 Mode_Octet.TBD_Bit

Le TBD_bit Réserve Mode_Octet doit être réglé 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.

7.7.1.7 Mode_Octet.N_TBD_Bit

Le bit complémentaire N_TBD_Bit doit toujours compléter le TBD_Bit.

7.7.2 Section de datation

Time_Stamp.Section.Data_Time_Stamp: la Data_Time_Stamp correspond à l'heure de prélèvement des données pour cette production.

Pour les connexions point à point, la Data_Time_Stamp est définie par rapport au temporisateur placé sur le consommateur. Pour les connexions multipoints, la Data_Time_Stamp est définie par rapport au temporisateur placé sur le producteur.

La Data_Time_Stamp est toujours exprimée en incréments de 128 μ s.

7.7.3 Message de coordination temporelle

7.7.3.1 Bit Ack_Octet.Ping_Response

Le bit Ping_Response doit indiquer qu'une réponse à demande Ping est transmise par le consommateur des données de sécurité sur ce nœud, à la production des données.

Si le bit Ping_Response est égal à 1, il doit indiquer que les Consumer_Time_Value et Ping_Count_Reply sont valides pour cette production des données.

Si le bit Ping_Response bit est égal à 0, il doit indiquer que les Consumer_Time_Value et Ping_Count_Reply ne sont pas valides pour cette production des données, et qu'il convient de les ignorer.

7.7.3.2 Ack_Octet.Consumer_Time_Value

La Consumer_Time_Value doit être la valeur d'horloge du consommateur des données de sécurité au moment de la transmission du message.

La Consumer_Time_Value permet de déduire la Data_Time_Stamp pour la production de données dans les autres directions.

7.7.3.3 Ack_Octet.Ping_Count_Reply

La Ping_Count_Reply est utilisée par chaque consommateur pour indiquer la demande Ping à laquelle il est répondu.

La Ping_Count_Reply est égale à la valeur du Ping_Count auquel il est répondu.

7.7.3.4 Bits réservés de coordination temporelle Ack_Octet.

Le consommateur doit régler les bits réservés de coordination temporelle sur la valeur 0.

Le producteur doit ignorer les bits réservés sauf pour le contrôle du CRC et de Ack_Octet_2.

7.7.4 Message de correction de temps

7.7.4.1 Mcast_Octet.Consumer_#

Pour les données à production multipoints, les bits Multi_Cast_Active_Idle et Consumer_Time_Correction_Value doivent être dirigés vers le consommateur indiqué par le champ Consumer_# du message.

Le Consumer_# est dirigé vers un consommateur spécifique (1 à 15).

Les bits Multi_Cast_Active_Idle et Consumer_Time_Correction_Value doivent être appliqués par le consommateur indiqué par le Consumer_#.

Un Consumer_# égal à 0 doit être utilisé pour indiquer l'absence de transfert des bits Multi_Cast_Active_Idle et Consumer_Time_Correction_Value si nécessaire.

7.7.4.2 Time_Correction_Section.Consumer_Time_Correction_Value

Le consommateur multipoints utilise Consumer_Time_Correction_Value pour corriger Producer_Time_Stamp, la datation résultante étant ainsi définie par rapport à l'horloge du consommateur.

7.7.4.3 Mcast_Octet.Multi_Cast_Active_Idle

La valeur 0 du bit Multi_Cast_Active_Idle doit indiquer l'état Repos, et la valeur 1 du bit Multi_Cast_Active_Idle doit indiquer l'état Actif.

Une fois le bit Multi_Cast_Active_Idle réglé sur "Actif" après la première production de données, ce bit ne doit plus être réglé sur repos jusqu'à la réinitialisation de la connexion de sécurité.

Si le consommateur constate la transition du bit Multipoints_Active_Idle de l'état Actif à l'état Repos, il doit fermer la connexion en cas d'utilisation du format de Base. Si le format Etendu

est utilisé et si le Max_Fault_Count n'a pas été atteint, le paquet est supprimé. À défaut, la connexion est fermée.

Pour les connexions multipoints, le bit Run_Idle de Mode_Octet doit être réglé sur l'état Run_Idle indiqué par l'application de production.

Il est nécessaire que le consommateur observe les deux bits Run_Idle et Multi_Cast_Active_Idle.

7.7.4.4 Bits réservés de correction de temps Mcast_octet

Le producteur doit régler les bits réservés de correction de temps sur 0.

Le consommateur doit ignorer les bits réservés sauf pour le contrôle du CRC et de MC_Octet_2.

7.7.5 Production des données de sécurité

7.7.5.1 État de la connexion de production

L'état de la connexion du producteur doit être déterminé par la combinaison des drapeaux S_Connection_Fault et Consumer_Active_Idle (voir Tableau 96 pour une définition).

Tableau 96 – Détermination de l'état de la connexion du producteur

S_Connection_Fault	Consumer_Active_Idle	État de la connexion du producteur	Commentaire
Anomalie	Négliger	État = Défectueux (anomalie)	Réamorçage exigé
OK	Repos	État = Repos	La connexion de sécurité n'a pas été activée
OK	Actif	État = Actif	La connexion de sécurité est active

7.7.5.2 Consumer_Open

Pour les producteurs de données de sécurité, la ressource Consumer_Open utilisée entre l'unité d'établissement de connexion de l'objet de validation et l'Objet de validation d'exécution doit permettre d'indiquer si un consommateur particulier des données produites a ou non une connexion ouverte active.

Si le producteur est multipoints, une ressource Consumer_Open doit exister pour chaque consommateur multipoints, de 1 à Max_Consumer_Number (index de 0 à Max_Consumer_Number – 1).

Les valeurs Consumer_Open sont Ouvertes ou Fermées.

L'indication Consumer_Open doit agir comme une activation de l'Objet de validation d'exécution, sur une base connexion par connexion. Après l'établissement satisfaisant de la connexion, les drapeaux Consumer_Open doivent passer de l'état Fermé à l'état Ouvert.

L'unité d'établissement de connexion de l'objet de validation doit fournir une matrice de ressources d'état de la connexion du consommateur pour les producteurs multipoints qui doivent être attribués lorsqu'un consommateur établit une connexion.

Le nombre de consommateurs attribué à un Objet de validation d'exécution doit être le nombre transmis au consommateur dans la réponse d'établissement de connexion.

Le nombre de connexions du consommateur peut être traité comme un groupe d'attribution pouvant être réutilisé et réattribué si nécessaire.

L'unité d'établissement de connexion de l'objet de validation doit s'assurer que la ressource `Consumer_Open` pour tout nombre de consommateurs attribué est réglée sur l'état Fermé pendant une durée minimale de $(\text{Timeout\_Multiplier.PI} + 2) \times \text{Intervalle Ping}$ préalablement à toute réattribution de ce nombre de consommateurs à une autre connexion. Cette opération est destinée à s'assurer de la temporisation des connexions établies précédemment, et ce, préalablement à toute attribution de ce nombre à une nouvelle connexion.

En d'autres termes, si l'unité d'établissement de connexion de l'objet de validation constate le réglage de `S_Connection_Fault`, elle doit régler la ressource `Consumer_Open` sur Fermé pendant une durée minimale de $(\text{Timeout\_Multiplier} + 2) \times \text{Intervalle Ping}$, ou éventuellement jusqu'à ce que le même consommateur tente de rétablir la même connexion.

7.7.5.3 Application_Run_Idle

Si l'application de production contrôle de manière active les données, l'indication `Run_Idle` doit mentionner l'état Exécution. Si l'application de production ne contrôle pas de manière active les données, et s'il convient que ces données adoptent un état de sécurité, l'indication `Run_Idle` doit mentionner l'état Repos.

7.7.5.4 Consumer_Active_Idle [par consommateur]

`Consumer_Active_Idle` est un drapeau d'exécution qui indique si des informations valides concernant le message de coordination temporelle ont été reçues pour ce consommateur.

Si un producteur de données de sécurité génère des données et si des informations valides concernant la coordination temporelle ont été reçues sans aucune erreur, l'état du drapeau `Consumer_Active_Idle` doit être égal à Actif, ou à Repos dans le cas contraire.

Pour les producteurs multipoints, un drapeau `Consumer_Active_Idle` doit exister pour chaque consommateur multipoints, numéroté de 1 à `Max_Consumer_Number`.

Les valeurs `Consumer_Active_Idle` sont Repos et Actif.

À l'établissement d'une connexion, tous les drapeaux `Consumer_Active_Idle` doivent être initialisés sur l'état Repos.

7.7.5.5 S_Connection_Fault [par consommateur]

Drapeau d'exécution qui indique si la connexion de sécurité avec le client est OK ou Défectueuse.

L'indication `S_Connection_Fault` d'une anomalie doit signaler que le producteur a décelé un problème au niveau de la connexion de sécurité avec ce consommateur ou que le consommateur a signalé en retour une erreur au producteur.

Si le producteur de données de sécurité a reçu une information invalide concernant la coordination temporelle, ou une temporisation de ladite information, l'état du drapeau `S_Connection_Fault` doit être égal à «Anomalie», ledit état étant OK dans les autres cas.

Pour les producteurs multipoints, il doit y avoir un drapeau `S_Connection_Fault` pour chaque consommateur multipoints, numéroté de 1 à `Max_Consumer_Number`.

Les valeurs de `S_Connection_Fault` sont OK et Défectueux.

À l'établissement d'une connexion, toutes les variables `S_Connection_Fault` doivent être initialisées sur OK.

7.7.5.6 Variables statiques d'entrée du producteur

Il s'agit des paramètres de temps de configuration qui définissent l'opération du producteur de protocoles de sécurité.

7.7.5.7 EPI

Le terme EPI désigne l'intervalle de paquets attendu. La fréquence de production des données de sécurité ne doit pas dépasser l'EPI. L'EPI est exprimé comme une valeur entière en microsecondes. La plage légale des valeurs est comprise entre 100 µs et 1 000 000 µs.

Pour toutes les connexions de sécurité, le producteur et tous les consommateurs doivent avoir le même EPI.

7.7.5.8 Timeout_Multiplier [par consommateur]

Le `Timeout_Multiplier` indique le nombre de nouvelles tentatives de production de données à utiliser dans les équations de détection d'une défaillance de connexion.

Le Format de base a limité le paramètre `Timeout_Multiplier` à des valeurs comprises entre 1 et 4. Pour ce format, la valeur `Timeout_Multiplier` a été utilisée pour un double objectif. À savoir:

- a) Pour calculer le délai du réseau;
- b) Pour déterminer le nombre d'intervalles Ping à attendre sans `Time_Coordination` ou la correction de temps avant de déclarer une anomalie de connexion.

Le format Etendu permet d'utiliser une plus grande valeur du paramètre `Timeout_Multiplier` pour le calcul du délai du réseau, la valeur utilisée pour déterminer le nombre d'intervalles Ping à attendre sans `Time_Coordination` ou la correction de temps avant de déclarer une anomalie de connexion restant par ailleurs limitée à une valeur maximale de 4. Le format Etendu permet d'utiliser une valeur du paramètre `Timeout_Multiplier` comprise entre 1 et 255.

Dans l'ensemble du présent document, le terme "`Timeout_Multiplier`" fait référence à la valeur du paramètre `Timeout_Multiplier`. "`Timeout_Multiplier.PI`" fait référence à la valeur déduite de "`Timeout_Multiplier`" afin de déterminer le nombre d'intervalles Ping à attendre sans `Time_Coordination` ou la correction de temps avant de déclarer une anomalie de connexion.

Pour le format de Base, `Timeout_Multiplier.PI` doit être égal à `Timeout_Multiplier`. Pour le format Etendu, `Timeout_Multiplier.PI` doit être égal à la plus petite valeur de `Timeout_Multiplier` ou à 4, selon la plus faible des deux valeurs.

Le `Timeout_Multiplier` doit être utilisé pour déterminer le nombre d'intervalles Ping (`Timeout_Multiplier.PI + 2`) qu'un producteur attend avant de rejeter un consommateur qui a omis d'envoyer une réponse de coordination temporelle après une demande Ping.

La plage légale des valeurs `Timeout_Multiplier` du format de Base doit correspondre aux valeurs 1, 2, 3 ou 4. La plage légale des valeurs `Timeout_Multiplier` du format Etendu doit être comprise entre 1 et 255 tant que la valeur de délai du réseau ne dépasse pas 5,8 s.

Pour tout producteur, chaque consommateur peut avoir un `Timeout_Multiplier` différent.

7.7.5.9 Connection_Type

Il spécifie si la connexion est point à point ou multipoints.

Pour tout producteur, chaque connexion de producteur et la (les) connexion(s) de consommateur correspondante(s) doivent avoir le même Type de connexion.

7.7.5.10 Ping_Interval_EPI_Multiplier

Il s'agit du nombre qui définit le Ping_Count_Interval pour une connexion particulière.

Le Ping_Count_Interval doit être égal à l'EPI fois le Ping_Interval_EPI_Multiplier.

Ce même intervalle doit définir la fréquence de demande et de transmission des messages de coordination temporelle.

Il doit par ailleurs définir la fréquence de transmission des sections de Correction de temps à chaque consommateur.

Un Ping_Interval_EPI_Multiplier légal doit comporter une valeur minimale déterminée à partir de l'équation $\text{Max\_Consumer\_Number} \times \text{Timeout\_Multiplier.PI} + 15$, et une valeur maximale inférieure à 1 000. Les valeurs par défaut doivent être 100 pour les connexions multipoints et 19 pour les connexions point à point.

Il convient de définir le Ping_Interval_EPI_Multiplier suffisamment grand pour permettre à la demande Ping d'être reconnue par le(s) serveur(s), au(x) serveur(s) de transmettre la (les) section(s) de coordination temporelle, et à toutes les sections Time_Coordination d'arriver et d'être traitées par le client. Toutes ces étapes doivent se dérouler avant expiration du délai du Ping_Interval.

Le client doit transmettre toutes les sections Time_Correction dans le Ping_Interval.

Le Ping_Interval_EPI_Multiplier doit être défini suffisamment petit pour garantir que le Ping_Count_Interval est inférieur ou égal à 100 s

Un intervalle de comptage de demandes Ping supérieur à 100 s peut contribuer, selon un écart de plus de 0,5 s, à la dérive de l'horloge, selon le Timeout_Multiplier.PI pour cette connexion. Une durée de 0,5 s a été définie comme la valeur maximale pouvant être attribuée à la dérive de l'horloge, et ce, afin d'éviter toute remise à zéro de l'horloge.

Les variables suivantes permettent de calculer le Ping_Interval_EPI_Multiplier.

- C_TO_S_Delay_Multiplier est égal à la durée, en tant que multiplicateur du temps EPI, équivalant à la durée d'initiation d'un message, au délai de transport et au délai de traitement de réception du Message de données, ou au message Time_Correction transmis par le client au serveur.
- S_TO_C_Delay_Multiplier est égal à la durée, en tant que multiplicateur du temps EPI, équivalant à la durée d'initiation d'un message, au délai de transport et au délai de traitement de réception du Message Time_Coordination transmis par le serveur au client.
- Ping_Rcved_TO_Time_Coord_Sent_Multiplier est égal à la durée, en tant que multiplicateur du temps EPI, admise entre le temps de réception EPI, dont il convient qu'elle déclenche l'envoi du message de coordination temporelle, et le moment où il convient que ce message soit transmis.
- Time_Coord_Rcved_TO_Time_Coord_Processed_Multiplier est égal à la durée, en tant que multiplicateur du temps EPI, admise entre le temps de réception du message de coordination temporelle et le traitement effectif dudit message.

Pour un réseau simple, il est raisonnable de prévoir que les C_TO_S_Delay_Multiplier et S_TO_C_Delay_Multiplier seront inférieurs à 2 fois la valeur de l'EPI.

Pour un réseau shunté qui dépend du nombre de sauts, il est raisonnable de prévoir que les C_TO_S_Delay_Multiplier et S_TO_C_Delay_Multiplier seront inférieurs à 4 fois la valeur de l'EPI. 4 sera utilisé comme valeur minimale de C_TO_S_Delay_Multiplier et de S_TO_C_Delay_Multiplier pour le calcul de la valeur minimale de Ping_Interval_EPI_Multiplier.

Il convient que les multiplicateurs EPI C_TO_S_Delay_Multiplier et S_TO_C_Delay_Multiplier ne tiennent pas compte des messages perdus sur le réseau. Le Timeout_Multiplier tient compte des messages perdus.

Il convient que la valeur de Ping_Rcvd_TO_Time_Coord_Sent_Multiplier soit inférieure à 3 fois la valeur de l'EPI.

Il convient que la valeur de Time_Coord_Rcvd_TO_Time_Coord_Processed_Multiplier soit inférieure à 3 fois la valeur de l'EPI.

L'équation qui permet de déterminer le Ping_Interval_EPI_Multiplier minimum est la suivante:

$$\begin{aligned} & [\{ \text{Timeout\_Multiplier.PI (C\#) max pour tous les consommateurs} \} \times \text{Max\_Consumer\_Num}] \\ & + \text{C\_TO\_S\_Delay\_Multiplier} \\ & + \text{S\_TO\_C\_Delay\_Multiplier} \\ & + \text{Ping\_Rcvd\_TO\_Time\_Coord\_Sent\_Multiplier} \\ & + \text{Time\_Coord\_Rcvd\_TO\_Time\_Coord\_Processed\_Multiplier} + 1 \end{aligned} \quad (1)$$

où

C# = Consumer_Number

4 étant la constante utilisée pour C_TO_S_Delay_Multiplier et S_TO_C_Delay_Multiplier et 3 étant la constante utilisée pour Ping_Rcvd_TO_Time_Coord_Sent_Multiplier et Time_Coord_Rcvd_TO_Time_Coord_Processed_Multiplier.

Le Ping_Interval_EPI_Multiplier doit être supérieur ou égal à:

$$[\{ \text{Timeout\_Multiplier.PI (C\#) max pour tous les consommateurs} \} \times \text{Max\_Consumer\_Num}] + 15 \quad (2)$$

Le producteur se fonde sur cette relation lors de la transmission des messages Correction de temps. Il convient d'augmenter en conséquence le Ping_Interval_EPI_Multiplier pour les valeurs de C_TO_S_Delay_Multiplier et S_TO_C_Delay_Multiplier supérieures à 4, et les valeurs de Ping_Rcvd_TO_Time_Coord_Sent_Multiplier et Time_Coord_Rcvd_TO_Time_Coord_Processed_Multiplier supérieures à 3.

Le Ping_Interval_EPI_Multiplier doit être inférieur à: 100 s / EPI.

La plage du Ping_Interval_EPI_Multiplier comprise entre 75 et 100 satisfait aux restrictions définies ci-dessus pour toutes les valeurs légales définies ci-dessous:

- EPI, 0,000 1 s à 1 1;
- Timeout_Multiplier.PI, 1 à 4;
- Max_Consumer_Num, 1 à 15;
- C_TO_S_Delay_Multiplier et S_TO_C_Delay_Multiplier, 1 à 4;
- Ping_Rcvd_TO_Time_Coord_Sent_Multiplier, 1 à 3;
- Time_Coord_Rcvd_TO_Time_Coord_Processed_Multiplier, 1 à 3.

Le producteur, quel qu'il soit, et tous les consommateurs doivent avoir le même Ping_Interval_EPI_Multiplier.

7.7.5.11 Max_Consumer_Number

Nombre maximum de consommateurs pouvant être configurés.

Si le type de connexion est point à point, le Max_Consumer_Number doit être égal à 1.

Pour les connexions multipoints, la plage légale des valeurs de Max_Consumer_Number doit être comprise entre 1 et 15.

Le producteur, quel qu'il soit, et tous les consommateurs doivent avoir le même Max_Consumer_Number.

7.7.5.12 Time_Coord_Msg_Min_Multiplier [par consommateur]

Time_Coord_Msg_Min_Multiplier est le nombre minimum d'incréments de 128 μ s susceptible d'être utilisé pour un message de coordination temporelle pour le passage du consommateur au producteur. Une valeur de cette variable autre que 0 permet une meilleure précision de la datation. La valeur par défaut du Time_Coord_Msg_Min_Multiplier doit être 0, et la plage légale des valeurs doit être comprise entre 0 et 7 813, ce qui équivaut de 0 s à 1 s.

Nombre minimal d'incréments de 128 μ s susceptibles d'être pris en charge:

Du:

Consommateur saisissant la Consumer_Time_Value à partir du Consumer_Clk_Count pour le message de coordination temporelle,

Au:

Producteur saisissant la Producer_Rcvd_Time_Value à réception du message de coordination temporelle

Pour tout producteur, chaque consommateur peut avoir un Time_Coord_Msg_Min_Multiplier différent.

7.7.5.13 Variables statiques déduites de la connexion du producteur

Ces variables statiques sont déduites des variables statiques d'entrée. Elles sont déduites au moment de la configuration et sont utilisées lors du traitement du producteur.

7.7.5.14 Time_Drift_Per_Ping_Interval [par consommateur]

Valeur exprimée en incréments de 128 μ s qui représente la dérive temporelle la plus défavorable due à une imprécision du quartz au cours d'un intervalle Ping.

La précision des horloges des appareils de sécurité doit être de 0,02 % (0,000 2). Compte tenu de la dérive positive et négative, la précision respective des horloges sera de 0,000 2 $\times$ 2 ou 0,004 (0,04 %).

La plage légale des valeurs est comprise entre 1 et 313, dans la mesure où l'intervalle Ping est limité à 100 s (100 000 000 μ s).

Le calcul de Time_Drift_Per_Ping_Interval est effectué avec des références temporelles exprimées en microsecondes (EPI désigne l'EPI en microsecondes). Le calcul de Time_Drift_Per_Ping_Interval est effectué avec un entier de 32 bits, le résultat obtenu étant un entier de 16 bits. La division par un facteur de 320 000 effectuée dans le calcul de

Time_Drift_Per_Ping_Interval équivaut à une multiplication par la dérive d'horloge la plus défavorable égale à 0,000 4 et à une division par 128 μ s.

$$\begin{aligned} \text{Time\_Drift\_Per\_Ping\_Interval (C\#)} = \\ \text{Arrondi [EPI} \times \text{Ping\_Interval\_EPI\_Multiplier / 320 000]} \\ \text{OR 1, selon la plus grande des deux valeurs} \end{aligned} \quad (3)$$

où

C# = Consumer_Number

EXEMPLE Si EPI = 8 000 μ s et Ping_Interval_EPI_Multiplier = 100, Time_Drift_Per_Ping_Interval(C#) = 3 (384 μ s)

7.7.5.15 Connection_Correction_Constant [par consommateur]

Valeur exprimée en incréments de 128 μ s qui est soustraite de la datation afin de représenter l'erreur la plus défavorable due à:

- la dérive temporelle;
- la nature asynchrone des horloges des producteur et consommateur;
- la durée minimale nécessaire au message de coordination temporelle pour passer du consommateur au producteur.

$$\begin{aligned} \text{Connection\_Correction\_Constant [C\#]} = \\ \text{Time\_Drift\_Constant} + 1 - \text{Time\_Coord\_Msg\_Min\_Multiplier [C\#]} \end{aligned} \quad (4)$$

où

C# = Consumer_Number

La Time_Drift_Constant (qui fait partie intégrante du calcul de Connection_Correction_Constant) est une valeur exprimée en incréments de 128 μ s qui est soustraite de la datation afin de représenter la dérive temporelle la plus défavorable due à une imprécision du cristal. La précision des horloges des producteur et consommateur doit être de 0,02 % (0,000 2). Compte tenu de la dérive positive et négative, la précision respective des horloges sera de 0,000 2 $\times$ 2 ou 0,004 (0,04 %).

La plage légale des valeurs applicables à la Time_Drift_Constant est comprise entre 1 et 1 563.

Le calcul de la Time_Drift_Constant est effectué avec des références temporelles exprimées en microsecondes (EPI désigne l'EPI en microsecondes).

Le calcul de la Time_Drift_Constant doit être effectué en utilisant au moins un entier de 32 bits, le résultat obtenu étant un entier de 16 bits.

Le facteur de 1/320 000 dans le calcul de la Time_Drift_Constant équivaut à une multiplication par la dérive d'horloge la plus défavorable égale à 0,000 4 et à une division par 128.

$$\begin{aligned} \text{Time\_Drift\_Constant (comptages par incréments de 128 } \mu\text{s)} = \\ \text{Arrondi [(Timeout\_Multiplier.PI} \\ \text{(C\#) + 1) } \times \text{EPI\_in\_}\mu\text{s} \times \text{Ping\_Interval\_EPI\_Multiplier / 320 000]} \\ \text{OR 1, selon la plus grande des deux valeurs.} \end{aligned} \quad (5)$$

EXEMPLE Timeout_Multiplier.PI = 2, EPI(en microsecondes) = 8 000, Ping_Interval_EPI_Multiplier = 100, Time_Drift_Constant = 8, Time_Coord_Msg_Min_Multiplier = 2, alors Connection_Correction_Constant = 7.

7.7.5.16 Time_Coord_Response_EPI_Limit [par consommateur]

La Time_Coord_Response_EPI_Limit permet de s'assurer qu'un message de coordination temporelle transmis au producteur qui le demande, parvient dans un délai suffisant pour prévenir toute possibilité de remplacement mathématique d'une datation de 16 bits. D'autres contrôles permettent de s'assurer de la transmission du message Time_Coordination dans l'intervalle Ping, et de la suppression d'un nombre de messages de coordination temporelle limité.

Time_Coord_Response_EPI_Limit (valeur exprimée en incréments d'EPI) permet de déterminer si la durée comprise entre l'incrément du comptage de demandes Ping et la réponse de coordination temporelle est inférieure à une valeur temporelle égale à:

$$\{5 + [\text{Time\_Coord\_Msg\_Min\_Multiplier} \times 0,000\ 128] + [\text{EPI} \times (\text{Consumer\_Num} - 1)]\} \text{ en secondes.} \quad (6)$$

Pour maintenir un temps de réaction inférieur à 5,8 s, le temps de transport du message de sécurité plus le temps de transport du message de coordination temporelle moins la durée minimale du message de coordination temporelle $[\text{Time\_Coord\_Msg\_Min\_Multiplier}/0,000\ 128]$ doivent être inférieurs à 5,0 s si la dérive la plus défavorable de 0,5 s est prise en compte. Cette procédure permet de maintenir la Connection_Correction_Constant dans la plage définie afin d'éviter tout remplacement lors du contrôle de l'âge.

La plage légale des valeurs applicables à Time_Coord_Response_EPI_Limit est comprise entre 5 et 1 000.

Si Consumer_Active_Idle[Consumer_Num-1] == Actif, les producteurs doivent vérifier que les messages de coordination temporelle sont reçus dans la Time_Coord_Response_EPI_Limit et annulent la connexion s'ils ne le sont pas.

Le calcul de la Time_Coord_Response_EPI_Limit s'effectue avec des références temporelles exprimées en microsecondes (EPI désigne l'EPI en microsecondes).

Le calcul de la Time_Coord_Response_EPI_Limit doit être effectué avec un entier de 32 bits, le résultat obtenu étant un entier de 16 bits.

$$\begin{aligned} \text{Time\_Coord\_Response\_EPI\_Limit [C\#]} = \\ \text{Arrondi } (\{5\ 000\ 000 + [\text{Time\_Coord\_Msg\_Min\_Multiplier}[C\#] \times 128] \\ + [\text{EPI} \times (\text{C\#} - 1)]\} / \text{EPI}) \\ \text{OR } 1\ 000 \text{ selon la plus faible des deux valeurs.} \end{aligned} \quad (7)$$

où

$$\text{C\#} = \text{Consumer\_Number}$$

EXEMPLE Si Time_Coord_Msg_Min_Multiplier = 2 (256 µs), EPI = 8 000 µs et Consumer_Number = 1, Time_Coord_Response_EPI_Limit = 626.

7.7.6 Variables dynamiques du producteur

7.7.6.1 Producer_Clk_Count

Chaque produit qui génère ou consomme des données de sécurité doit déduire un temporisateur périodique qui incrémente un compteur (Producer_Clk_Count ou Consumer_Clk_Count) toutes les 128 µs.

Les tolérances et la stabilité de Producer_Clk_Count doivent être de ± 0,02 %.

Producer_Clk_Count (et Consumer_Clk_Count) doivent avoir une longueur de 16 bits.

7.7.6.2 Producer_Safe_Data_TS

Producer_Safe_Data_TS est une variable qui doit être définie égale à Producer_Clk_Count au moment du prélèvement et de la saisie à partir de l'application de production des Safety_Data pour une production de données EPI particulière.

Le point de prélèvement est le point qui marque la fin des responsabilités de contrôle temporel des applications de production et le début des responsabilités de contrôle temporel des protocoles de sécurité. Cette valeur sert de datation des données relatives à l'horloge du producteur. La plage légale des valeurs est comprise entre 0 et 65 535.

7.7.6.3 Data_Time_Stamp

Moment de prélèvement des données de sécurité, par rapport à l'horloge du consommateur.

La valeur Data_Time_Stamp est déduite par le producteur pour une production point à point.

La valeur Data_Time_Stamp est déduite par le consommateur dans les connexions multipoints.

La plage légale des valeurs est comprise entre 0 et 65 535.

Pour les connexions point à point:

$$\text{Data\_Time\_Stamp} = \text{Producer\_Safe\_Data\_TS} + \text{Consumer\_Time\_Correction\_Value} \quad (8)$$

Pour les connexions multipoints:

$$\text{Data\_Time\_Stamp} = \text{Producer\_Safe\_Data\_TS} \quad (9)$$

7.7.6.4 Ping_Interval_EPI_Count

Comptage du nombre de périodes EPI entre l'incrémementation du Ping_Count.

Ping_Interval_EPI_Count permet de contrôler les intervalles Ping et la transmission des messages de correction de temps pour les producteurs multipoints.

Son incrémementation s'effectue à chaque production de données. Lorsque Ping_Interval_EPI_Count atteint le Ping_Interval_EPI_Multiplier, il est réinitialisé sur 0, et le comptage de demandes Ping est incrémenté.

Pour les producteurs multipoints, les messages de correction de temps doivent être transmis aux n consommateurs (où n = 1 à Max_Consumer_Number), pour les 9^e à n+9 productions de l'intervalle Ping.

Le message de correction de temps du consommateur 1 doit être transmis en premier, suivi de 2,3, ..., n.

L'objectif de cette logique est de répartir les messages de correction de temps à un point donné dans l'intervalle Ping, lorsqu'il convient que lesdits messages soient déjà parvenus et qu'ils aient été traités pour ce même intervalle.

La plage légale des valeurs est comprise entre 0 et le Ping_Interval_EPI_Multiplier.

Il convient de régler la variable Ping_Interval_EPI_Count sur 0000_{hex} lors de l'établissement d'une connexion.

7.7.6.5 RR_Con_Num_Index_Pntr

Variable utilisée par le producteur multipoints pour contrôler la vérification de la temporisation à la réception des messages de coordination temporelle, et pour contrôler également la transmission des messages de correction de temps.

Une valeur supérieure ou égale à Max_Consumer_Number indique l'absence de vérification des temporisations de coordination temporelle sur cet EPI, et l'absence de transmission de corrections de temps, sur la base de cet EPI.

Une valeur de 0 à (Max_Consumer_Number - 1) indique quelles temporisations de coordination temporelle font l'objet d'un contrôle (Consumer_Number = RR_Con_Num_Index_Pntr + 1) sur cet EPI et quel message de correction de temps (Consumer_Number = RR_Con_Num_Index_Pntr + 1) peut être transmis sur la base de cette production EPI.

7.7.6.6 Time_Drift_Since_Last_Time_Coord [par consommateur]

Variable contenant la dérive temporelle maximale qui aurait pu se produire entre le producteur et le consommateur depuis la dernière réception d'un message de coordination temporelle. Cette valeur est égale à Ping_Int_Since_Last_Time_Coord_Msg_Count fois le Time_Drift_Per_Ping_Interval. Le Ping_Int_Since_Last_Time_Coord_Msg_Count est le nombre d'intervalles Ping depuis le dernier message de coordination temporelle.

La Time_Drift_Since_Last_Time_Coord doit permettre de déterminer de manière indirecte si le délai de réception du message de coordination temporelle est bien plus important que le délai du message de coordination temporelle précédent.

Le délai du message de coordination temporelle a une influence sur la Consumer_Time_Correction_Value utilisée. Des délais plus importants du message de coordination temporelle occasionnent la compensation de Time_Stamp dans une direction négative, provoquant le vieillissement des données.

Si la différence entre les délais de deux messages Time_Coordination consécutifs est supérieure à la durée de l'EPI, la Consumer_Time_Correction_Value ultérieure peut donner lieu à une Time_Stamp de la production EPI suivante effectivement inférieure à la Time_Stamp de la production EPI précédente. Ceci entraînerait une erreur de séquençement du consommateur de Time_Stamp.

Dans la mesure où la dérive temporelle maximale est contrôlée, soit la dernière Time_Correction_Value moins la valeur Time_Drift_Since_Last_Time_Coord, ou la nouvelle valeur Time_Correction_Value, doit être transmise au consommateur, selon la meilleure des deux valeurs.

Ceci empêche les longs délais de remise des messages de correction de temps de provoquer des erreurs de séquençement dans les contrôles de la datation.

Pour les producteurs multipoints, une Time_Drift_Since_Last_Time_Coord doit exister pour chaque consommateur multipoints, 1 à Max_Consumer_Number.

La plage légale des valeurs est comprise entre 0 et 3 910.

7.7.6.7 Worst_Case_Consumer_Time_Correction_Value

Valeur provisoire utilisée pour déterminer la Consumer_Time_Correction_Value.

7.7.7 Variables dynamiques de producteur par consommateur

7.7.7.1 Généralités

Les variables dynamiques suivantes sont des variables de producteur qui existent pour chaque consommateur. Il n'y a qu'une seule variable pour chaque consommateur dans le cas des connexions point à point. Pour les connexions multipoints, il existe un Max_Consumer_Number de variables, chaque nombre représentant un consommateur individuel.

7.7.7.2 Consumer_Time_Value[par consommateur]

Valeur temporelle transmise par le consommateur au producteur d'une datation ou dans un message de coordination temporelle. Une Consumer_Time_Value est reçue pour chaque consommateur multipoints, 1 à Max_Consumer_Number.

La plage légale des valeurs est comprise entre 0 et 65 535.

Toutes les variables Consumer_Time_Value doivent être réglées sur 0000_{hex} lors de l'établissement d'une connexion.

Lors de la réception d'un message de coordination temporelle, le producteur doit vérifier que la Time_Coordination_Section.Consumer_Time_Value est différente de la dernière Consumer_Time_Value reçue. Si tel est le cas, le message de coordination temporelle ne doit pas être traité.

Ce contrôle empêche tout traitement par un producteur des messages de coordination temporelle dupliqués générés par le réseau.

7.7.7.3 Producer_Rcved_Time_Value[par consommateur]

Producer_Rcved_Time_Value doit être définie égale au Producer_Clk_Count au moment de la réception des informations concernant les messages de coordination temporelle, en provenance du consommateur de datation.

Une Producer_Rcved_Time_Value doit exister pour chaque consommateur multipoints, 1 à Max_Consumer_Number.

La plage légale des valeurs est comprise entre 0 et 65 535.

Toutes les variables Producer_Rcved_Time_Value doivent être réglées sur 0000_{hex} lors de l'établissement d'une connexion.

7.7.7.4 Consumer_Time_Correction_Value[par consommateur]

La Consumer_Time_Correction_Value existe uniquement pour les connexions de sécurité multipoints.

La Consumer_Time_Correction_Value est ajoutée à la datation des données du producteur pour permettre au résultat d'indiquer le moment de prélèvement le plus tôt et le plus défavorable des données par rapport à la valeur d'horloge du consommateur.

Une Consumer_Time_Correction_Value existe pour chaque consommateur multipoints, 1 à Max_Consumer_Number.

$$\begin{aligned} \text{Consumer\_Time\_Correction\_Value} [\text{Consumer\_Number}] = \\ \text{Consumer\_Time\_Value} [\text{Consumer\_Number}] \\ - \text{Producer\_Rcvd\_Time\_Value} [\text{Consumer\_Number}] \\ - \text{Connection\_Correction\_Constant} [\text{Consumer\_Number}] \end{aligned} \quad (10)$$

La plage légale des valeurs est comprise entre 0 et 65 535.

Toutes les variables `Consumer_Time_Correction_Value` doivent être réglées sur 0000_{hex} lors de l'établissement d'une connexion.

7.7.7.5 Ping_Int_Since_Last_Time_Coord_Msg_Count [par consommateur]

`Ping_Int_Since_Last_Time_Coord_Msg_Count` est le comptage d'exécution du nombre d'intervalles Ping entre les messages de coordination temporelle pour un consommateur particulier.

Pour les connexions point à point, le `Ping_Int_Since_Last_Time_Coord_Msg_Count` doit être incrémenté à la 8^e production EPI de l'intervalle Ping.

Pour les connexions multipoints, `Ping_Int_Since_Last_Time_Coord_Msg_Count` doit être incrémenté toutes les (8+n)^{èmes} productions EPI de l'intervalle Ping, où n est égal au nombre de consommateurs – 1.

Le `Ping_Int_Since_Last_Time_Coord_Msg_Count` pour tout consommateur particulier doit être réinitialisé à la réception d'un message de coordination temporelle valide provenant de ce consommateur.

Si le `Ping_Int_Since_Last_Time_Coord_Msg_Count` venait à dépasser le `Timeout_Multiplier.PI` plus 2 pour une connexion donnée, le consommateur considéré doit être réglé sur l'état défectueux.

Si le producteur est multipoints, `Ping_Int_Since_Last_Time_Coord_Msg_Count` existe pour chaque consommateur multipoints, 1 à `Max_Consumer_Number`.

La valeur légale des valeurs est comprise entre 0 et 5.

Toutes les variables `Ping_Int_Since_Last_Time_Coord_Msg_Count` doivent être réglées sur 0000_{hex} lors de l'établissement d'une connexion.

7.7.7.6 Producer_Fault_Counter

Dans le cas du format Etendu, il s'agit d'une valeur provisoire utilisée pour la traçabilité du nombre d'erreurs d'intégrité des données détectées par le producteur à la réception des messages de coordination temporelle. Cette valeur est incrémentée à chaque détection d'un message de coordination temporelle comportant une erreur d'intégrité des données. Cette valeur est remise à 0 toutes les heures. Si cette valeur atteint le `Max_Fault_Number` pour le consommateur concerné (paramètre `SafetyOpen`), la connexion est fermée.

7.7.8 Variables de données du consommateur

7.7.8.1 Généralités

Le présent paragraphe 7.7.8 décrit les variables de données utilisées par un consommateur de sécurité pour la réception des données de sécurité. Les variables internes sont définies dans une tentative de définition du comportement du consommateur de données de sécurité à la réception de ces dernières.

7.7.8.2 État de la connexion de consommation

Il est possible de déduire l'état des données et des connexions de sécurité à partir des drapeaux S_Con_Flt_C_Out, S_Run_Idle_Out et Init_Complete_Out. Le Tableau 97 récapitule la logique que l'application de consommation peut employer pour déduire les données et l'état de sécurité.

Tableau 97 – État de la connexion de sécurité de consommation

S_Con_Flt_C_Out	S_Run_Idle_Out	Init_Complete_Out	État de la connexion	Description
Anomalie	Ignorer	Ignorer	Défectueux	La connexion de sécurité est défectueuse. Un réamorçage est nécessaire. Mettre les données en état de sécurité.
OK	Repos	0	Repos	La connexion de sécurité n'a pas été activée. Mettre les données en état de sécurité..
OK	Repos	1	Repos	La connexion de sécurité a été activée et l'application de production est en mode Repos. Mettre les données en état de sécurité.
OK	Actif	0	N/A	Illégal – ne peut pas se produire
OK	Actif	1	Exécuter	La connexion de sécurité est active et l'application de production est en mode Exécution. Utiliser les données

L'état de connexion des connexions de sécurité de consommation doit être indiqué tel que défini dans le Tableau 97.

7.7.8.3 S_Con_Flt_C_Out

S_Con_Flt_C_Out indique à l'application de consommation s'il convient que les données de sécurité qu'elle utilise soient dans un état de sécurité, étant donné que les objets de validation de sécurité ont détecté une anomalie de connexion de sécurité. S_Con_Flt_C_Out_Temp sert d'emplacement provisoire à cette variable.

Les valeurs de S_Con_Flt_C_Out sont OK et Défectueux.

Tous les drapeaux S_Con_Flt_C_Out doivent être réglés sur OK lors de l'établissement d'une connexion.

7.7.8.4 S_Run_Idle_Out

S_Run_Idle_Out doit être utilisé par une application de consommation pour déterminer s'il convient que les données de sécurité qu'elle utilise soient dans un état de sécurité.

Le S_Run_Idle_Out doit indiquer l'état Repos lorsque l'application de production est au repos ou les Objets de validation de sécurité ne sont pas actifs. S_Run_Idle_Out_Temp sert d'emplacement provisoire à cette variable.

Les valeurs de S_Run_Idle_Out sont IDLE (REPOS) ou RUN (EXÉCUTION).

Tous les drapeaux S_Run_Idle_Out doivent être réglés sur Repos lors de l'établissement d'une connexion.

7.7.8.5 Init_Complete_Out

Init_Complete_Out indique si l'initialisation de la datation est achevée ou non.

S_Run_Idle_Out doit être en mode Repos jusqu'à ce que Init_Complete_Out soit réglé sur 1.

Après le premier établissement de la connexion, l'application consommatrice doit fermer les connexions de format de base si l'initialisation n'a pas lieu dans un délai de 10 s. L'application consommatrice doit fermer les connexions étendues si l'initialisation n'a pas lieu dans un délai de 8,3 s.

S_Run_Idle_Out indique l'état Repos, indépendamment de cette temporisation. En cas d'intégration de la temporisation, l'erreur doit être verrouillée jusqu'à la fermeture de la connexion de sécurité, et une tentative de réouverture.

Pour les connexions point à point, le drapeau Init_Complete_Out doit indiquer que le producteur a effectivement reçu le premier message de coordination temporelle, et que le producteur génère des données avec une datation par rapport à l'horloge du consommateur.

Pour les connexions multipoints, le drapeau Init_Complete_Out doit indiquer que le producteur a effectivement reçu le premier message de coordination temporelle pour ce consommateur, et que ce dernier a reçu le premier message de correction de temps sur la base des informations concernant la coordination temporelle.

Pour les connexions point à point, la valeur Data_Time_Stamp doit être réglée sur 0 par le producteur jusqu'à réception de la première section de coordination temporelle.

Si le consommateur reçoit la Data_Time_Stamp sous forme de valeur non nulle, la vérification de la datation doit être activée.

Pour les connexions multipoints, la valeur Data_Time_Stamp doit toujours être réglée égale à l'horloge du producteur.

Le consommateur multipoints doit activer la vérification de la datation à la réception de la première section de correction de temps.

Pour toutes les connexions de sécurité consommées, la vérification de la datation doit être activée si le mode des données indique Exécution.

Init_Complete_Out_Temp sert d'emplacement provisoire à cette variable.

7.7.9 Variables statiques d'entrée du consommateur

7.7.9.1 Connection_Type

Spécifie si la connexion est point à point ou multipoints. Le producteur, quel qu'il soit, et tous les consommateurs doivent avoir le même Connection_Type.

7.7.9.2 Consumer_Num

Numéro d'attribution d'un consommateur multipoints (1 à 15).

7.7.9.3 Network_Time_Expectation_Multiplier

Nombre maximum d'incréments de 128 μ s dont il convient qu'un consommateur permette à l'âge des données de sécurité d'atteindre.

Les données de sécurité doivent adopter un état de sécurité si les données de sécurité consommées sont plus anciennes que le Network_Time_Expectation_Multiplier.

La plage légale des valeurs est comprise entre 0 et 45 313, ce qui équivaut à une durée de 0 s à 5,8 s. La limite de 5,8 s, l'exigence imposant la vérification de Network_Time_Expectation

au moins une fois toutes les 2 s, et la variation de valeur Time_Correction maximale (ou la dérive d'horloge maximale) pour un intervalle Ping de 0,5 s, permettent de s'assurer que la valeur de base de l'horloge de 8,388 s ($FFFF_{\text{hex}} \times 0,000\,128$) ne revient pas à zéro entre les contrôles.

Le temps de réaction réel du réseau peut être cette valeur temporelle plus 1 EPI si l'application de production est asynchrone par rapport à la production des données, dans la mesure où, dans ce cas, l'âge des données peut correspondre à un EPI au moment où la datation s'appliquait aux données produites.

7.7.9.4 Timeout_Multiplier

Nombre de nouvelles tentatives de production de données à utiliser dans les équations de détection d'une anomalie de réseau. Il s'agit de la même valeur utilisée par le producteur.

7.7.9.5 Ping_Interval_EPI_Multiplier

Nombre qui définit le Ping_Count_Interval pour une connexion particulière. Le Ping_Count_Interval est égal à l'EPI fois le Ping_Interval_EPI_Multiplier.

Il s'agit de la même valeur utilisée par le producteur.

7.7.9.6 Variables statiques déduites de la connexion du consommateur

Ces variables statiques sont déduites des variables statiques d'entrée. Ces variables statiques sont déduites au moment de la configuration et sont utilisées lors du traitement du producteur.

7.7.10 Variables dynamiques du consommateur

7.7.10.1 Consumer_Clk_Count

Chaque produit qui consomme des données de sécurité déduit un temporisateur périodique qui incrémente un compteur (Consumer_Clk_Count) toutes les 128 μs .

Les tolérances et la stabilité de Consumer_Clk_Count sont de $\pm 0,02\%$ étant donné que les appareils de sécurité doivent comporter des horloges ayant cette tolérance.

Consumer_Clk_Count doit avoir une longueur de 16 bits.

Si la différence entre le Consumer_Clk_Count au moment où les données sont transmises à l'application de consommation pour utilisation et la Data_Time_Stamp transmise avec les données est supérieure au Network_Time_Expectation_Multiplier, le drapeau S_Con_Flt_C_Out doit être réglé sur "Défectueux" pour indiquer que le temps de réaction du réseau n'a pas été satisfait.

7.7.10.2 Last_Ping_Count

Un consommateur de données de sécurité doit être capable de détecter le moment où le Ping_Count a été modifié. Cette variable à 2 bits permet de maintenir le Ping_Count pour comparaison lors de la réception suivante.

Dans la mesure où il convient que la production initiale des données de sécurité comporte un Ping_Count de 00, le Last_Ping_Count doit être initialisé sur 11.

7.7.10.3 Time_Coordination_Count_Down

Doit être réglé égal à Consumer_Number à réception d'une demande de messages Ping multipoint.

Le consommateur doit décrémenter la valeur `Time_Coordination_Count_Down` lors de la réception ultérieure des données consommées, jusqu'à ce que la valeur soit égale à 0.

Si la valeur est égale à 1 lors de la réception des données consommées, la réponse à demande Ping pour ce consommateur doit être transmise.

L'objectif de cette logique est de répartir les réponses à demande Ping multipoints.

Lors du premier établissement d'une connexion, le `Time_Coordination_Count_Down` doit être initialisé à 0.

7.7.10.4 Corrected_Data_Time_Stamp

Cette valeur est l'exemplaire consommateur de la `Data_Time_Stamp` reçue.

Pour les connexions multipoints, la `Corrected_Data_Time_Stamp` doit être la somme de la datation reçue et de la `Last_Rcvd_Time_Correction_Value`.

7.7.10.5 Last_Data_Time_Stamp

Cette valeur est l'exemplaire sauvegardé de la `Data_Time_Stamp` reçue.

La `Last_Data_Time_Stamp` doit être utilisée pour détecter les messages hors séquence.

Lors du premier établissement d'une connexion, la `Last_Data_Time_Stamp` doit être initialisée à 0.

7.7.10.6 Last_Rcvd_Multi_Cast_Active_Idle

Cette valeur est l'exemplaire sauvegardé du `Multi_Cast_Active_Idle` reçu.

Le dernier `Last_Rcvd_Multi_Cast_Active_Idle` doit être utilisé pour détecter un changement de l'état actif à l'état repos, qui serait considéré comme une anomalie.

Lors du premier établissement d'une connexion, le `Last_Rcvd_Multi_Cast_Active_Idle` doit être initialisé à 0.

7.7.10.7 Last_Rcvd_Time_Correction_Value

Cette valeur est l'exemplaire sauvegardé de la `Time_Correction_Value` reçue.

La `Last_Rcvd_Time_Correction_Value` doit être utilisée pour corriger la datation pour chaque consommateur multipoints.

Lors du premier établissement d'une connexion, la `Last_Rcvd_Time_Correction_Value` doit être initialisée à 0.

7.7.10.8 Time_Correction_Ping_Interval_Count

Cette valeur indique le nombre d'intervalles Ping effectifs depuis la dernière réception d'un message de correction de temps.

Si le `Time_Correction_Ping_Interval_Count` est supérieur à `Timeout_Multiplier.PI + 1`, la connexion doit être défectueuse.

7.7.10.9 Time_Correction_Received_Flag

Cette valeur indique qu'un message de correction de temps a été reçu pour ce consommateur multipoints. Cette valeur indique qu'un message de correction de temps a été reçu et que la datation peut être corrigée et vérifiée.

Lorsque le Time_Correction_Received_Flag est réglé, le consommateur doit initier le processus de correction et de vérification de la datation.

7.7.10.10 Data_Age

Cette valeur indique l'âge le plus défavorable des données avec un incrément de 128 μ s.

L'âge des données est déterminé au point de prélèvement de ces dernières par une application de consommation. Avec les consommateurs déclenchés par l'application, ce prélèvement est asynchrone par rapport à la réception des données. Avec les consommateurs déclenchés par la liaison, ce prélèvement est effectué à la réception des données.

L'âge des données est défini comme la différence entre le Consumer_Clk_Count au point de prélèvement et la datation des données lors de la dernière saisie de ces dernières.

7.7.10.11 Max_Data_Age

Cette valeur indique la valeur maximale de Data_Age depuis sa dernière réinitialisation.

7.7.10.12 Consumer_Fault_Counter

Pour le format Etendu, il s'agit d'une valeur provisoire utilisée pour la traçabilité du nombre d'erreurs d'intégrité des données que le consommateur détecte à la réception des messages de correction des données et de temps. Cette valeur est incrémentée à chaque détection d'un message de correction des données et de temps, avec une erreur d'intégrité des données. Cette valeur est réinitialisée sur 0 toutes les heures. Si cette valeur atteint le Max_Fault_Number (paramètre SafetyOpen), la connexion est fermée.

8 Gestion de la couche de communication de sécurité

8.1 Présentation générale

Les paragraphes 8.1 à 8.7 ne cherchent pas à fournir un tutoriel sur chaque aspect de la CPF 2, mais en revanche une présentation générale de haut niveau de la méthode d'établissement des connexions CPF 2 sur chaque réseau et pour les différents types de réseau, en soulignant les caractéristiques utilisées et les extensions exigées pour prendre en charge les connexions de sécurité.

Toutes les connexions FSCP 2/1 doivent être établies en utilisant un service Forward Open avec un segment de réseau de sécurité (CP 2/2) ou un service SafetyOpen (CP 2/3). Il existe des mesures de détection des erreurs système et utilisateur définies. Le Tableau 98 définit les erreurs et les mesures de détection de ces erreurs.

Tableau 98 – Erreurs d'établissement de connexion et mesures de détection des erreurs

Erreurs d'établissement de connexion	Mesures de détection des erreurs d'établissement de connexion				
	Essais utilisateur	Vérification OUNID	Vérification TUNID	CPCRC CRC	ID de configuration (SCID)
Mauvais acheminement de la demande de connexion par l'utilisateur	X	X ¹	X		
Mauvais acheminement de la demande de connexion par le système			X		
SafetyOpen corrompu				X	X
Configuration d'application corrompue ou modifiée					X
Reconfiguration à partir d'un point d'origine erroné		X ^a			
^a S'applique uniquement si la propriété a été établie.					

8.2 Définition des mesures utilisées lors de l'établissement d'une connexion

«Numéro de réseau de sécurité» (SNN) unique global – Identifie de manière unique un réseau sur tous les réseaux du système de sécurité. Le manuel de sécurité de l'utilisateur doit contenir une recommandation qui stipule «Il convient que l'utilisateur attribue des numéros SNN pour chaque réseau ou sous-réseau de sécurité, qui sont des numéros globaux uniques», ou un libellé à cet effet.

Le numéro de réseau de sécurité fait partie intégrante de l'UNID. Cette valeur est une valeur de 6 octets qui utilise le format CPF 2 DATE_AND_TIME.

Les valeurs DATE comprises entre les décimales 1 et 11 687 (1972-01-01 à 2002-12-31) sont des valeurs anciennes réservées aux valeurs de paramétrage manuel du SNN.

Le SNN peut être un des deux types suivants:

- Paramétrage manuel, ou
- Généré par outil logiciel.

Le type de SNN peut être déterminé à partir de la section DATE, voir le Tableau 99 pour des détails.

Tableau 99 – Attributions de Date/Heure SNN

De DATE (décimale)	A DATE (décimale)	De DATE (Jour)	A DATE (Jour)	Type SNN
0	0	1972-01-01	1972-01-01	SNN nul (valeur illégale)
1	1	1972-01-02	1972-01-02	Paramétrage manuel – fond de panier
2	2	1972-01-03	1972-01-03	Paramétrage manuel – CP 2/1
3	3	1972-01-04	1972-01-04	Réservé pour une utilisation future
4	4	1972-01-05	1972-01-05	Paramétrage manuel – CP 2/2
5	5	1972-01-06	1972-01-06	Paramétrage manuel – CP 2/3
6	6	1972-01-07	1972-01-07	Paramétrage manuel – CP 16/3
7	1 460	1972-01-07	1975-12-31	Réservé pour une utilisation future
1 461	11 687	1976-01-01	2003-12-31	Plage spécifique au fournisseur
11 688	65 534	2004-01-01	2151-06-05	Généré par outil logiciel
65 535	65 535	2151-06-06	2151-06-06	Indication de la cible signifiant qu'aucun SNN n'a été défini

Si un outil logiciel déchiffre un type SNN réservé, il doit l'afficher comme une valeur Hex.

La plage légale des valeurs TIME pour le type de SNN est énumérée au Tableau 100.

Tableau 100 – Plage légale SNN des valeurs temporelles

Type SNN	De valeur hex temporelle	À valeur hex temporelle	De date j/h/min/s	A date j/h/min/s
SNN nul	00000000	00000000	00d00h00min00,000s	00d00h00min00,000s
Paramétrage manuel (DATE = 1 à 5)	00000001	0000270F (9 999 décimale)	00d00h00min00,001s	00d00h00min09,999s
Réservé pour une utilisation future	-	-	-	-
Généré par outil logiciel	00000000	05265BFF	00d00h00min00,000s	00d23h59min59,999s
Indication de la cible signifiant qu'aucun SNN n'a été défini	FFFFFFFF	FFFFFFFF	-24d20h31min23,648s	-24d20h31min23,648s

«Identifiant de nœud unique» (UNID) global – Identifie de manière unique un nœud sur tous les réseaux du système de sécurité. Cette valeur est constituée du numéro de réseau de sécurité (SNN) et de l'adresse de nœud de l'appareil. Elle constitue ainsi une structure composée du SNN de 6 octets et d'une adresse de nœud à 4 octets. L'adresse de nœud à 4 octets est dimensionnée de façon à s'adapter à toutes les formes d'adresses de réseau CPF 2.

```
struct UNID
{
DATE_AND_TIME    SNN;
UDINT            NodeID;
};
```

Les NodeID inférieurs à 4 octets (c'est-à-dire CP 2/3) doivent être alignés sur l'octet de poids faible dans l'ordre petit-boutiste. Les octets non utilisés doivent être remplis de zéros.

Fonction de sécurité – L'UNID permet d'identifier de manière unique les points d'origine et/ou cibles au cours du processus d'établissement de connexion.

Autres utilisations de l'UNID:

TUNID = Identifiant de réseau unique de la cible

Fonction de sécurité – Identifie la cible dans le service SafetyOpen.

OUNID = Identifiant de réseau unique du point d'origine

Fonction de sécurité – Identifie le point d'origine dans le service SafetyOpen.

OCPUNID = UNID de propriété de connexion de sortie

Fonction de sécurité – Identifie le propriétaire de la connexion de sortie dans la cible; ceci doit être équivalent à l'OUNID en fonctionnement normal.

CFUNID = UNID de propriété de configuration

Fonction de sécurité – Identifie le propriétaire de la configuration de sécurité dans la cible; ceci doit être équivalent à l'OUNID en fonctionnement normal.

Identifiant du producteur (PID) = Identifie le producteur des données d'exécution et des données de correction de temps.

L'identifiant du producteur (PID) doit être utilisé comme valeur initiale dans les CRC du protocole d'exécution.

Le consommateur doit obtenir l'identifiant du producteur à partir de SafetyOpen ou de la réponse SafetyOpen (selon le point d'origine) et utiliser la valeur comme valeur initiale de vérification d'exécution des CRC de sécurité.

La valeur du PID est la suivante: ID du fournisseur + Numéro de série de l'appareil + Numéro de série de connexion CIP.

Fonction de sécurité – Le PID permet d'assurer le bon acheminement des données de connexion produites/de sécurité et des données de correction de temps.

Identifiant du consommateur (CID) – Identifie le producteur du message de coordination temporelle.

L'identifiant du consommateur (CID) doit être utilisé comme valeur initiale du CRC du message de coordination temporelle.

Le producteur doit obtenir l'identifiant du consommateur à partir du SafetyOpen ou de la réponse SafetyOpen (selon le point d'origine) et utiliser la valeur comme valeur initiale de vérification d'exécution des CRC de sécurité.

La valeur du CID est la suivante: ID du fournisseur + Numéro de série de l'appareil + Numéro de série de connexion CIP.

Fonction de sécurité – Le CID permet d'assurer le bon acheminement des données de coordination temporelle.

CRC des paramètres de connexion (CPCRC) – Il s'agit d'un CRC relatif à la sécurité couvrant les données d'établissement de connexion CPF 2 dans le service SafetyOpen. Ce CRC couvre également les paramètres supplémentaires exigés par le protocole de sécurité. Le CRC utilisé pour le CPCRC est CRC-S4, défini en 7.1.2.

Fonction de sécurité – Le CPCRC permet d'assurer l'intégrité des données de connexion contenues dans le service SafetyOpen.

CRC de configuration de sécurité (SCCRC) – Il s'agit d'un CRC couvrant les données de configuration de l'appareil contenues dans le service SafetyOpen. Les paramètres couverts par le CPCRC ne sont pas couverts par le SCCRC. Le CRC utilisé pour le SCCRC est CRC-S4 défini en 7.1.2.

Le CRC des données de configuration de sécurité (SCCRC) doit être calculé sur toute la section de données d'application transmise à l'appareil dont la configuration est effectuée par outil logiciel.

Le SCCRC proprement dit doit être inclus dans le calcul du CPCRC.

Fonction de sécurité – Le SCCRC permet d'assurer l'intégrité des données de configuration lors de leur transmission ainsi que lors de leur archivage.

Datation de configuration de sécurité (SCTS) – Signature relative à la sécurité qui identifie la révision de la configuration d'appareil contenue dans un service SafetyOpen ou dans un appareil de sécurité.

La SCTS doit constituer un marquage de la datation (Heure/Date) de la création ou de la modification de configuration.

Le paramètre SCTS dans le service SafetyOpen doit être inclus dans le calcul du CPCRC.

Le logiciel de configuration doit suivre le format de datation défini CPF 2 (voir IEC 61131-3) pour le paramétrage de la signature.

Fonction de sécurité – La SCTS permet de s'assurer de l'identité des données d'application relatives à la sécurité.

Identifiant de configuration de sécurité (SCID) – combinaison du SCCRC et de la SCTS. La SCTS et le SCCRC permettent tous deux d'identifier de manière unique une configuration de l'utilisateur et du point d'origine.

Le SCID = 0 dans un service SafetyOpen de forme 2b doit comporter une signification particulière qui permet d'indiquer que le SCID ne doit pas être vérifié par une cible avant l'acceptation de la connexion.

Cette valeur SCID spéciale permet aux points d'origine qui ne se préoccupent pas de la configuration d'un appareil d'établir des connexions sans connaître la valeur SCID.

Le manuel de sécurité doit contenir des instructions de l'utilisateur qui stipulent «S'il est choisi de configurer des connexions de sécurité avec un SCID = 0, il faut s'assurer que les points d'origine et les cibles ont les configurations appropriées», ou un libellé équivalent similaire.

Datation initiale – Lorsque le format de message de sécurité étendu est utilisé, le segment de sécurité et la réponse SafetyOpen de format Etendu sont utilisés lors de l'établissement d'une connexion. Selon le type de connexion (voir 7.6.5), la datation initiale est transmise dans le service SafetyOpen ou dans la réponse SafetyOpen. La valeur de datation initiale permet de définir un paramètre de datation initiale utilisé pour détecter les remplacements de datation.

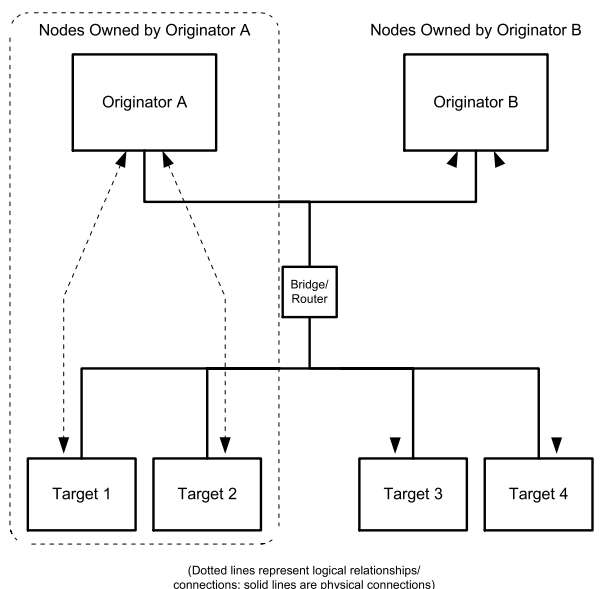
Valeur de remplacement initiale – Lorsque le format de message de sécurité étendu est utilisé, le segment de sécurité et la réponse SafetyOpen de format Etendu sont utilisés lors de l'établissement d'une connexion. Selon le type de connexion (voir 7.6.5), la datation initiale

est transmise dans le service SafetyOpen ou dans la réponse SafetyOpen. La valeur de remplacement initiale permet de définir le paramètre de comptage de remplacement initial au niveau du consommateur. Cette valeur est incluse dans le calcul CRC pour les paquets de données. Si le producteur et le consommateur n'utilisent pas la même valeur, les contrôles CRC du consommateur échouent. Cette caractéristique fournit une capacité de détection supplémentaire pour les messages insérés et les paquets hors séquence.

8.3 Validation de la relation point d'origine-cible

Dans la trame CPF 2, les nœuds sont soit des points d'origine (nœuds qui sollicitent des connexions) soit des cibles (nœuds qui reçoivent des demandes de connexion). Les contrôleurs sont généralement les points d'origine de connexion. Les modules E/S (ainsi que d'autres contrôleurs ou moniteurs) sont généralement les cibles. Les cibles peuvent prendre en charge deux points de connexion d'application ou plus.

Considérer le système représenté à la Figure 59. Supposer, pour les besoins de l'illustration, que toutes les cibles sont parfaitement identiques.



IEC

Anglais	Français
Nodes owned by originator ..	Nœuds détenus par le point d'origine ...
Originator	Point d'origine
Bridge/router	Pont/routeur
Target	Cible
(dotted lines represent logical relationship /connections; solid lines re physical connections)	(les lignes en pointillé représentent les relations logiques/connexions; les lignes continues représentent les connexions physiques)

Figure 59 – Propriété cible

L'utilisation de ponts/routeurs normalisés et de piles de protocoles à couches inférieures normalisées dans les nœuds d'extrémité favorise l'occurrence d'erreurs supplémentaires qui exigent des mesures de protection plus sévères que celles appliquées lors de l'établissement d'une connexion CPF 2. Par exemple, le pont/routeur est susceptible de mal acheminer (par exemple, corrompre le NodeID de destination) une demande de connexion du point d'origine A destinée à la cible 1 plutôt à la cible 2, 3 ou 4. La source de l'erreur peut également être une mauvaise configuration du point d'origine B par l'utilisateur en vue d'une connexion à la cible 1, tandis que le point d'origine A est en mode hors ligne et la cible 1 est sous tension. La connexion du point d'origine B à la cible 1 serait admise sans un second niveau de

comparaison au-dessus de la clé électronique identique, point auquel l'application du point d'origine B peut placer la cible 1 (en supposant qu'il s'agit d'un appareil de sortie) dans un état de fonctionnement incorrect eu égard à l'application mise en œuvre par le point d'origine A.

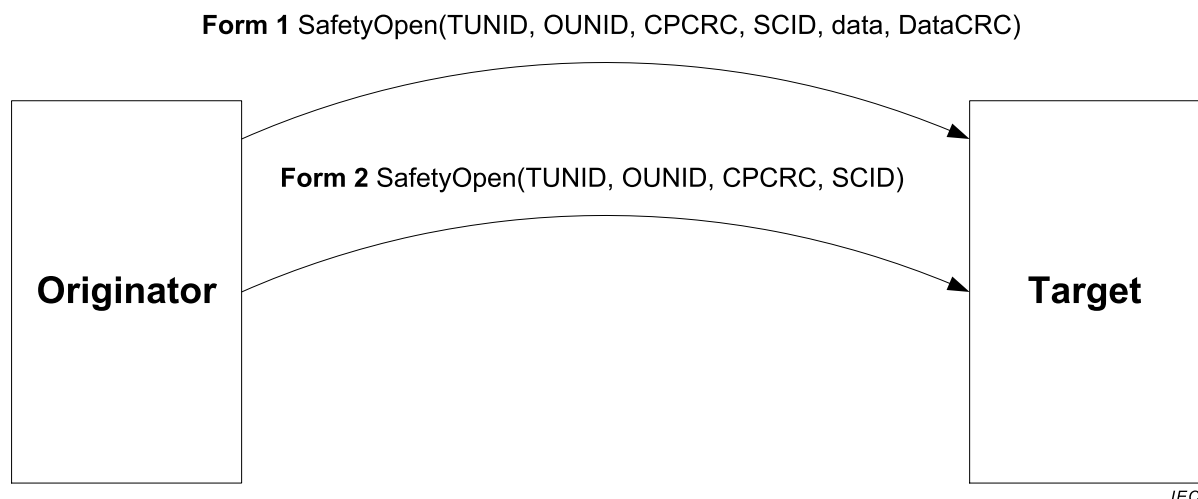
8.4 Détection des demandes de connexion mal acheminées

Toutes les demandes SafetyOpen contiennent l'UNID de l'appareil cible. À réception d'un service SafetyOpen, la cible doit comparer l'UNID de la cible SafetyOpen (TUNID) avec son propre UNID. Si la comparaison entre TUNID et UNID est satisfaisante, la destination de SafetyOpen est considérée correcte et le traitement doit se poursuivre.

8.5 Traitement de SafetyOpen

Il existe deux méthodes de traitement de SafetyOpen (voir Figure 60).

- Destination, propriété, traitement des données de configuration et vérification SCID;
- Destination, propriété et vérification SCID (facultatif).



Anglais	Français
Form	Forme
Data	Données
Originator	Point d'origine
Target	Cible

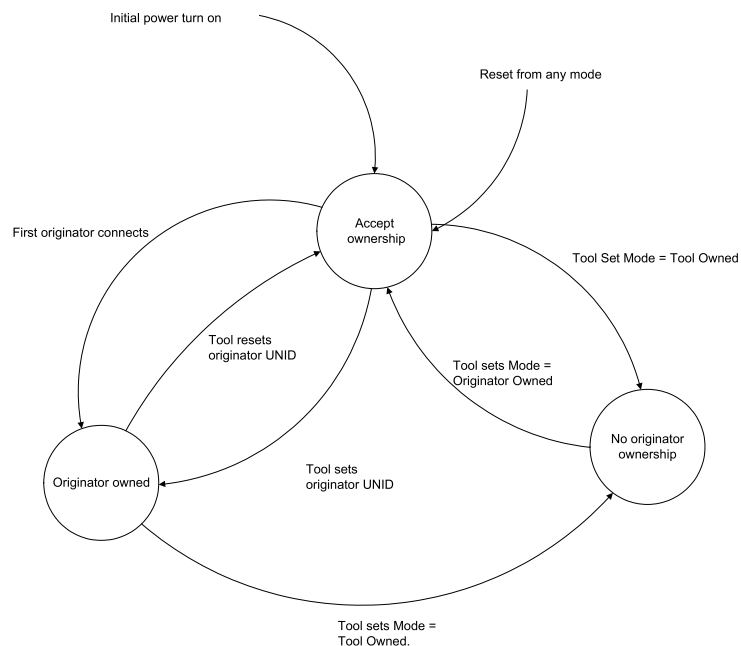
Figure 60 – Formes de SafetyOpen

8.6 Gestion de propriété

Il existe deux méthodes d'établissement de propriété de configuration et/ou connexion, à savoir par les outils de configuration ou par le service SafetyOpen. L'outil peut régler le mode de sorte que la configuration relève de lui seul ou du point d'origine.

Les tentatives de reconfiguration d'un appareil via le service SafetyOpen doivent être refusées si seul le mode de configuration par outil est sélectionné.

Si le mode configuré par le point d'origine est utilisé, l'OUNID du point d'origine sélectionné peut être défini par outil logiciel lors de la mise en service de l'appareil cible pour une sécurité supplémentaire. La Figure 61 définit les méthodes de transition d'un état de propriété à un autre.



IEC

Anglais	Français
Initial power turn on	Mise sous tension initiale
Reset from any mode	Réinitialisation depuis tout mode
First originator connects	Première connexion du point d'origine
Accept ownership	Acceptation de propriété
Tool set mode = tool owned	Mode de réglage par outil = outil avec propriétaire
Tool resets originator UNID	L'outil réinitialise l'UNID du point d'origine
Tool sets mode = originator owned	L'outil règle le mode = point d'origine avec propriétaire
originator owned	point d'origine avec propriétaire
Tool sets originator UNID	L'outil règle l'UNID du point d'origine
No originator ownership	Aucune propriété du point d'origine
Tool sets mode = tool owned	L'outil règle le mode = outil avec propriétaire

Figure 61 – Diagramme d'états de la propriété de connexion

Pour établir la propriété de la configuration (et de la connexion des sorties) des cibles, l'OUNID de l'appareil d'origine doit être transféré à la cible dans le service SafetyOpen.

L'OUNID de l'appareil d'origine doit être archivé dans la mémoire non volatile avec la configuration à laquelle elle est associée.

Les appareils de sortie doivent archiver l'OUNID associé aux sorties de sécurité afin d'éviter que d'autres points d'origine ne détournent les sorties de manière intempestive. Le maintien de l'OUNID du point d'origine associé à la configuration permet à plusieurs appareils de se connecter à un appareil d'entrée tout en maintenant la propriété de configuration. La Figure 62 définit le mapping des UNIDS de service SafetyOpen avec les emplacements de propriété de point d'origine de l'appareil cible.

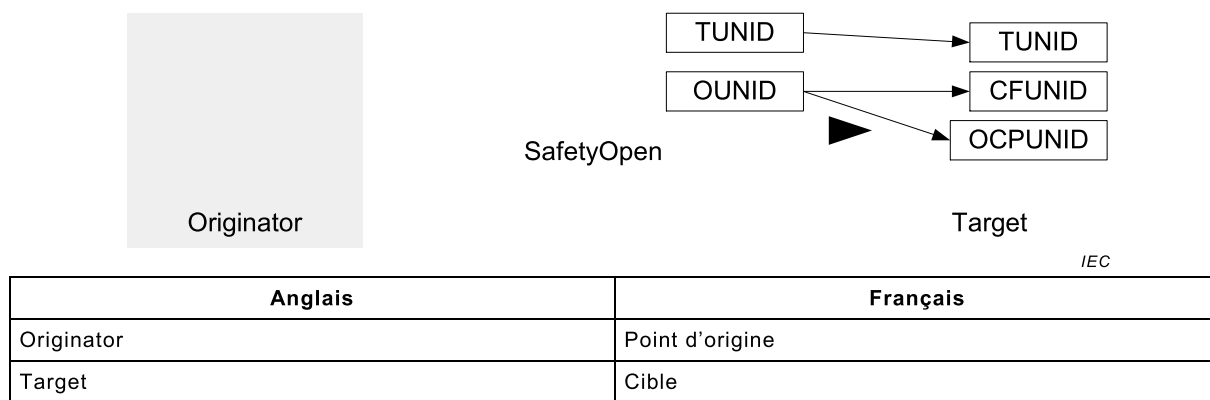
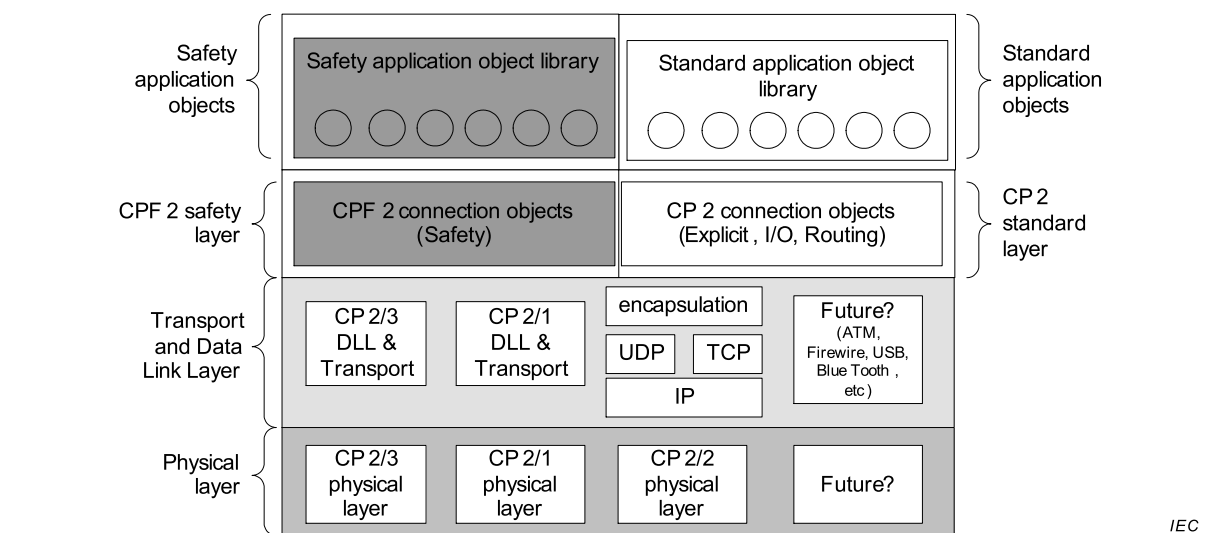


Figure 62 – Mapping de l'UNID de service SafetyOpen

8.7 Pontage de différentes couches physiques

Les nœuds CPF 2 partagent une application et une couche utilisateur communes tel que défini à la Figure 63.

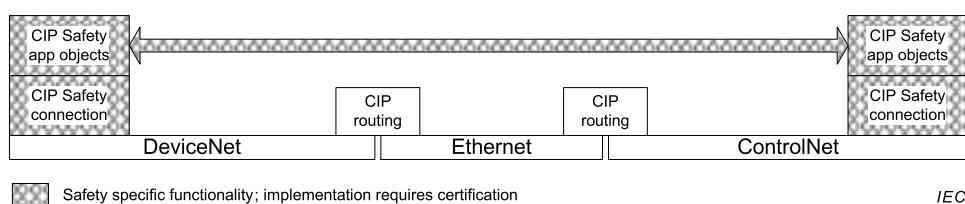


Anglais	Français
Safety application objects	Objets d'application de sécurité
Safety application object library	Bibliothèque d'objets d'application de sécurité
Standard application objects	Objets d'application normalisés
Standard application object library	Bibliothèque d'objets d'application normalisés
CPF 2 safety layer	Couche de sécurité CPF 2
CPF 2 connection objects (safety)	Objets de connexion CPF 2 (sécurité)
(explicit, I/O, routing)	(explicite , E/S, acheminement)
encapsulation	encapsulation
CP 2 standard layer	Couche normalisée CP 2
Transport and data link layer	Couche de liaison de transport et données
Future?	Futur?
Physical layer	Couche physique

Figure 63 – Couche application CPF 2 commune

Les objets de connexion CPF 2 sont les entités qui rapprochent les différences intrinsèques entre les capacités et les services fournis par les réseaux sous-jacents, avec échange des données SIL 3 avec les objets d'application ci-dessus. Par exemple, les trames de données de couche physique CP 2/3 (c'est-à-dire CAN) se limitent chacune à un nombre maximal de 8 octets. L'objet de connexion CPF 2 dans un nœud CP 2/3 transporte des paquets E/S de plus de 8 octets via le protocole de fragmentation E/S du CP 2/3, tandis que sur les réseaux de plus grande capacité tels que le CP 2/2, la taille de connexion maximale de 511 octets s'ajuste à une trame de données de couche physique. Une fois la connexion de sécurité établie, la couche application relative à la sécurité échange les données de sécurité avec les objets de connexion de sécurité.

Le protocole de sécurité a été conçu pour permettre le transport de bout en bout des données de sécurité sans exiger une connaissance spécifique du protocole de sécurité interne ou de l'évaluation SIL 3 d'appareils intermédiaires. La Figure 64 représente une connexion de bout en bout entre un nœud de sécurité sur le CP 2/3 et un nœud de sécurité sur le CP 2/1 acheminé sur un réseau CP 2/2. Les points d'extrémité de connexion de sécurité permettent aux homologues de niveau d'application de partager les données SIL 3.



IEC

Anglais	Français
CIP safety app. Objects	Objets d'app. de sécurité CIP
CIP safety connection	Connexion de sécurité CIP
CIP routing	Acheminement CIP
Safety specific functionality; implementation requires certification	Fonctionnalité spécifique à la sécurité; la mise en œuvre nécessite une certification

Figure 64 – Exemple d'acheminement de bout en bout

L'établissement d'une connexion de sécurité est dynamique sur chaque réseau. Les points d'origine CP 2/2 utilisent le service ForwardOpen de l'objet Gestionnaire de connexion. Le chemin de connexion des données d'un service ForwardOpen inclut un segment de réseau de sécurité pour le nœud d'extrémité. Ce segment de réseau de sécurité informe le destinataire qu'un objet de connexion capable de prendre en charge une connexion de sécurité doit pouvoir accepter la demande. Il inclut également les données utilisées pour spécifier les attributs d'objet de connexion associés à son comportement de sécurité (par exemple, temporisateurs de délai).

Pour la sécurité CP 2/3, le point d'origine doit établir une connexion de messagerie explicite avec le routeur ou le nœud d'extrémité afin de fournir les demandes de service ForwardOpen ou SafetyOpen. Les autres réseaux CPF 2 fournissent (généralement) le service ForwardOpen à l'UCMM sans connexion.

8.8 Établissement de connexion de sécurité

8.8.1 Présentation générale

L'établissement de connexions de sécurité constitue une fonction système essentielle. Deux éléments de sécurité sont à traiter: à savoir, l'établissement d'une relation de connexion avec un point d'origine et l'établissement d'une connexion d'exécution. Le présent paragraphe décrit les exigences système visant à exécuter ces deux opérations avec intégrité.

8.8.2 Faits de base pour l'établissement d'une connexion

Les faits de base pour l'établissement d'une connexion de sécurité sont définis ci-dessous.

- SafetyOpen est un service défini dans l'objet Connexion.
 - une connexion de messagerie explicite est exigée avec un chemin ayant pour cible l'objet Connexion.
- ForwardOpen est un service défini dans l'objet Gestionnaire de connexion.
 - Il s'agit d'un message non connecté comportant un chemin ayant pour cible l'objet Gestionnaire de connexion.
 - Lorsqu'elle provient d'un point d'origine de sécurité CP 2/3, une connexion de message explicite est exigée avec un chemin ayant pour cible l'objet Gestionnaire de connexion.
- Le service SafetyOpen exige un ensemble complémentaire de paramètres de connexion afin de définir le troisième point de connexion dans les nœuds de sécurité CP 2/3, lorsque le type de connexion est multipoints. Ces paramètres sont contenus dans le segment de sécurité.
- Un chemin d'application nul est défini pour indiquer qu'une connexion n'a pas de données d'application, ou que le service SafetyOpen ne comporte aucune donnée de configuration. Chaque fournisseur de module de sécurité doit définir un chemin nul approprié à son appareil. Un chemin nul doit toujours utiliser une référence de chemin complète (c'est-à-dire 20 04 24 [instance spécifique au fournisseur]). Pour les appareils avec EDS, l'instance nulle sélectionnée doit être diffusée avec une entrée dans la section de gestionnaire de connexion du fichier EDS (se reporter à l'ISO 15745-4:2003, Annexe C).
- Le chemin d'application de la connexion de Coordination temporelle doit toujours être nul.
- Le service SafetyOpen de forme 2 (aucune donnée de configuration) doit inclure un chemin d'application nul pour le chemin de configuration.
- La connexion de Correction de temps n'exige aucun chemin.
- Les paramètres supplémentaires du troisième point de connexion sont désignés et comportent les valeurs suivantes:
 - RPI de correction de temps;
 - ID de connexion de réseau de correction de temps;
 - Type de connexion = multipoints;
 - Priorité = Priorité élevée;
 - Fixe/Variable = Fixe;
 - Taille de connexion = 6 (taille de correction de temps fixe).
- L'ID de connexion de réseau de correction de temps ne fait pas partie intégrante du CPCRC.
- Les tailles de connexions normalisées O-à-T et T-à-O doivent toujours refléter la taille à 2 connexions pour chaque connexion. En d'autres termes, la taille de la connexion comportant les paquets de correction de données et de temps concaténés reflète cette combinaison. Le calcul des tailles de ressources de connexion appropriées pour la sécurité CP 2/3 relève de la responsabilité des ponts et des nœuds de sécurité CP 2/3 (cette opération est facilitée en ce sens que la taille du troisième point de connexion, que comporte le message SafetyOpen, peut être ajoutée ou soustraite).

8.8.3 Configuration des connexions de sécurité

Le présent paragraphe 8.8.3 définit les paramètres nécessaires pour exécuter le protocole de sécurité. Il définit également les paramètres du segment de sécurité nécessaires pour un transfert dans le service SafetyOpen, afin d'établir correctement une connexion de sécurité. Le présent paragraphe 8.8.3 décrit la méthode d'attribution de ces paramètres et propose des valeurs par défaut raisonnables pour un système de sécurité.

Les paramètres qu'il est nécessaire de configurer pour une connexion de sécurité sont les suivants:

- Timeout_Multiplier;
- Max Consumer Number;
- UNID Cible;
- UNID de point d'origine;
- EPI;
- Multiplicateur EPI d'intervalle Ping;
- Multiplicateur minimal de messages de coordination temporelle;
- Timeout_Multiplier;
- Nombre maximal de consommateurs;
- Multiplicateur de délai de réseau;
- ASYNC;
- Max_Fault_Number (Format étendu uniquement).

Presque tous les paramètres ASYNC sont inclus dans le service SafetyOpen. Le logiciel de configuration pour un point d'origine de connexion de sécurité doit prévoir un moyen de configuration des paramètres suivants, ou d'attribution de valeurs par défaut aux dits paramètres: Intervalle de paquets prévu, UNID cible, UNID de point d'origine, Timeout_Multiplier, Multiplicateur EPI d'intervalle Ping, Multiplicateur minimal de messages de coordination temporelle, nombre maximal de consommateurs, multiplicateur de délai de réseau, ASYNC et Max_Fault_Number (format Etendu uniquement). La plage de valeurs de Max_Fault_Number doit être limitée à la plage comprise entre 0 et 255. Le Tableau 101 récapitule les méthodes d'obtention de ces paramètres et d'autres paramètres.

Tableau 101 – Paramètres de connexion de sécurité

Paramètre	Méthode de configuration proposée	Valeur par défaut proposée
Intervalle de paquets prévu de données (EPI).	Estimation attribuée par l'utilisateur ou basée sur un outil	Aucune, l'utilisateur doit en fournir une
EPI de coordination temporelle	EPI de données × Multiplicateur EPI d'intervalle Ping	Calculée par logiciel
EPI de correction de temps	EPI de données × Multiplicateur EPI d'intervalle Ping	Calculée par logiciel
UNID Cible	Attribué par l'utilisateur ou obtenu par logiciel	Aucune, l'utilisateur doit en fournir une
UNID de point d'origine	Attribué par l'utilisateur	Aucune, l'utilisateur doit en fournir une
Timeout_Multiplier	Attribué par l'utilisateur	2
Multiplicateur EPI d'intervalle Ping	Valeur par défaut pour les entrées ou les sorties	100 pour les entrées 19 pour les sorties
Multiplicateur minimal de messages de coordination temporelle	Valeur par défaut du chemin	2 sans pont 3 avec pont
Nombre maximal de consommateurs	Valeur fixe	15
Multiplicateur de délai de réseau	Calcul	Calculée
ASYNC	Entrée de fichier EDS	1 (asynchrone)

Paramètre	Méthode de configuration proposée	Valeur par défaut proposée
Datation initiale (format Etendu uniquement)	Attribution dynamique	Aucune, le producteur doit attribuer une valeur basée sur le format et le type de connexion
Comptage de remplacement initial (format Etendu uniquement)	Attribution dynamique	Aucune, le producteur doit attribuer une valeur basée sur le format et le type de connexion
Max_Fault_Number (format Etendu uniquement)	Valeur par défaut	5

8.8.4 Multiplicateur de délai de réseau

Le calcul du Multiplicateur de délai de réseau constitue l'un des principaux calculs exigés d'un outil de configuration de sécurité ou d'un point d'origine de connexion. Le présent paragraphe 8.8.4 décrit une méthode de calcul simplifiée.

Le paragraphe 9.3.2 définit le multiplicateur de délai de réseau comme suit:

$$\text{Network\_Time\_Expectation\_Multiplier} > \frac{[\text{EPI\_in\_sec} \times \text{Timeout\_Multiplier} + \text{Safety\_Message\_Time(max)} + \text{Time\_Coord\_Message\_Time(max)}] / 128 \mu\text{s} + \text{Connection\_Correction\_Constant}}{1} \quad (11)$$

Certaines hypothèses de simplification peuvent être formulées comme suit:

- Temps de message de sécurité (max) = 1 EPI;
- Temps de message de coordination temporelle = Temps de message de sécurité (max);
- L'effet de Time_Drift_Constant est négligeable (la constante Correction de connexion peut être ignorée).

Ces hypothèses permettent de formuler l'équation généralisée suivante:

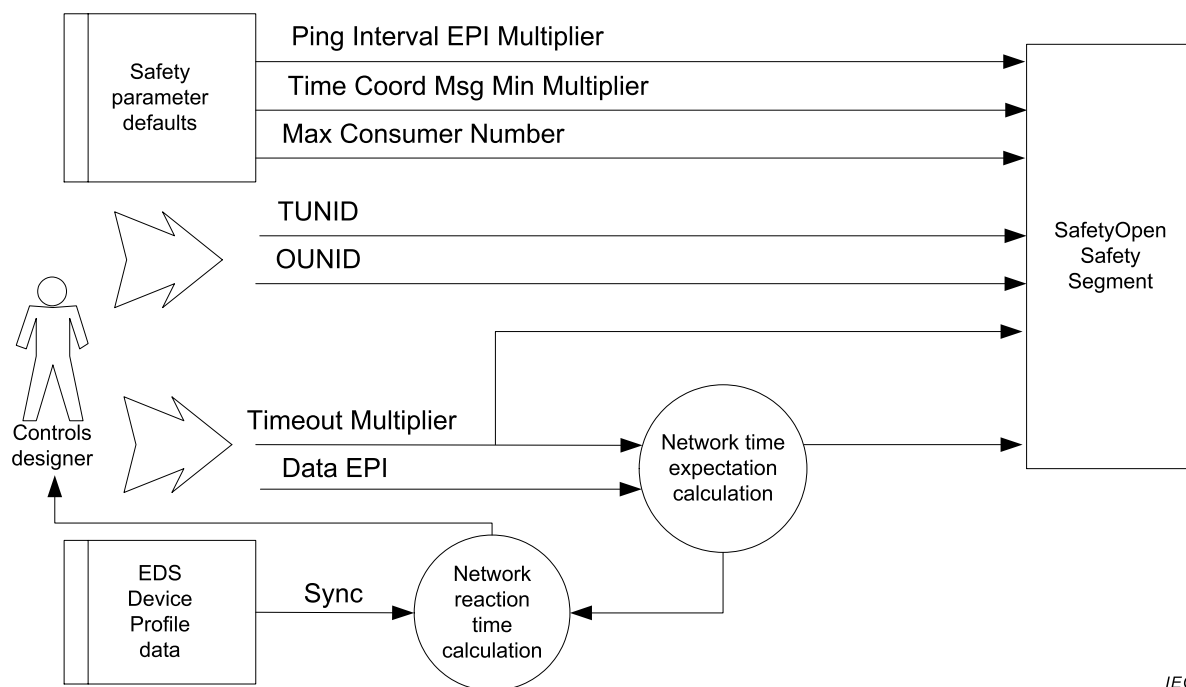
$$\text{Multiplicateur de délai de réseau} = [\text{EPI\_in\_sec} \times (\text{Timeout\_Multiplier} + 2)] / 128 \mu\text{s} \quad (12)$$

Où:

La valeur ne dépasse pas 5,8 s.

Le paramètre Multiplicateur de délai de réseau peut à présent être déterminé par un ensemble commun d'entrées utilisateur et un paramètre de fichier EDS.

La Figure 65 représente les points d'obtention des divers paramètres définis dans le Tableau 101. Elle représente également la méthode d'utilisation de ces paramètres par le logiciel afin de constituer le segment de sécurité d'un service SafetyOpen.



IEC

Anglais	Français
Safety parameter defaults	Valeurs par défaut des paramètres de sécurité
SafetyOpen safety segment	Segment de sécurité de SafetyOpen
Controls designer	Concepteur de commandes
Timeout multiplier	Multiplicateur de temporisation
Data EPI	EPI de données
Network time expectation calculation	Calcul du délai de réseau
EDS device profile data	Données de profil d'appareil EDS
Network reaction time calculation	Calcul du temps de réaction de réseau

Figure 65 – Sources des paramètres de connexion relative à la sécurité

La Figure 66 définit la méthode de mise en correspondance des paramètres SafetyOpen dans les points d'origine et les cibles d'une connexion de sécurité.

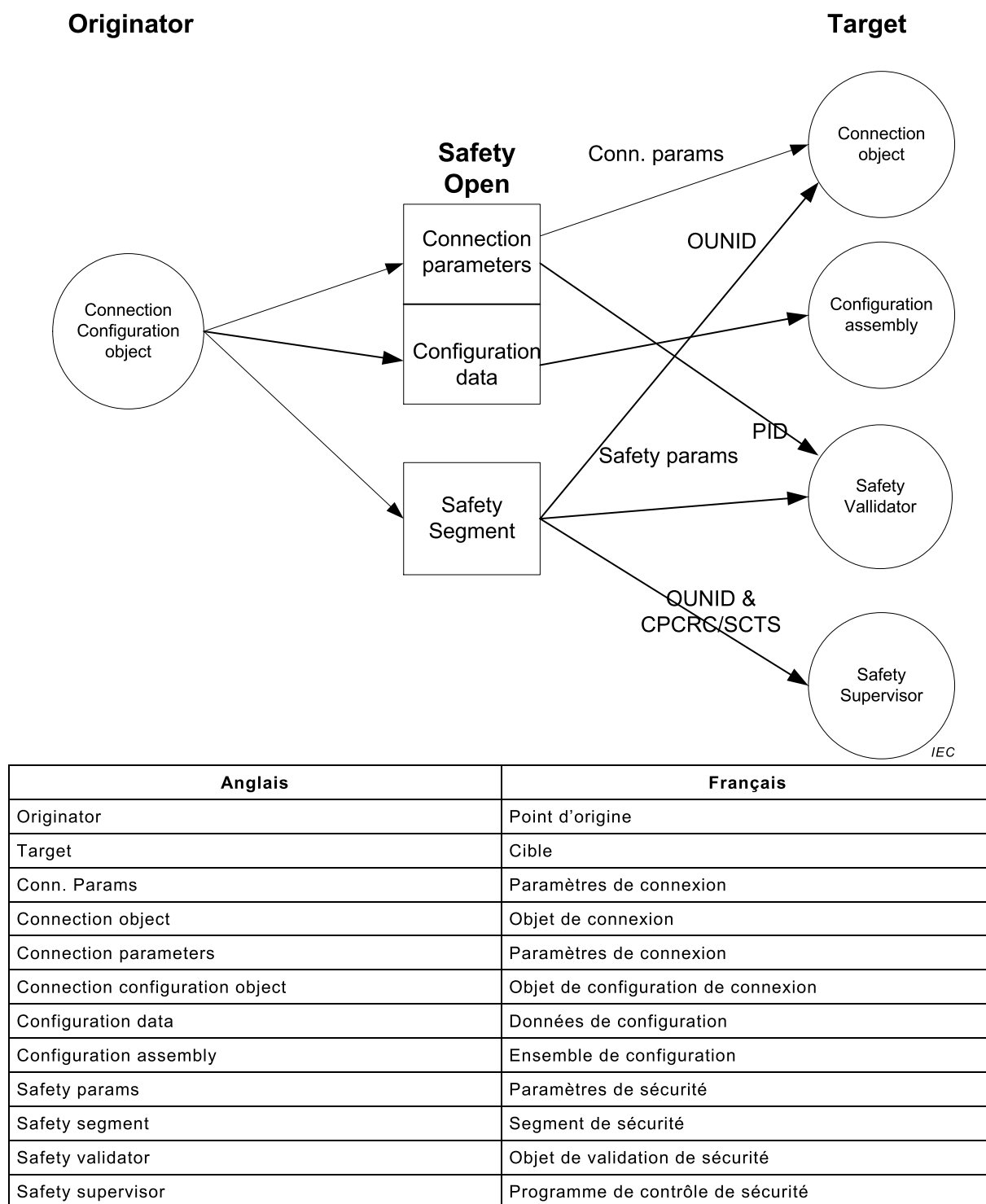


Figure 66 – Mapping des paramètres entre le point d'origine et la cible

8.8.5 Établissement de connexions

La transmission des données de configuration dans le service SafetyOpen est définie comme un service SafetyOpen de forme 1. L'absence de transmission des données de configuration dans le service SafetyOpen est définie comme un service SafetyOpen de forme 2. Cette séquence est définie à la Figure 67.

Si une connexion comporte des données de configuration, ces dernières doivent être transmises uniquement si nécessaire. Cette transmission doit être exécutée, sauf modification

de la configuration, par l'envoi d'un service SafetyOpen de forme 2, et uniquement suivie d'un service SafetyOpen de forme 1 si la cible renvoie une erreur «Appareil non configuré».

Lorsqu'un appareil reçoit un service SafetyOpen de forme 1 contenant des données de configuration et un SCID adapté à sa configuration existante, il doit réappliquer la configuration. Tous les contrôles de règles existantes (c'est-à-dire contrôles OUNID et TUNID) doivent toujours s'appliquer.

Dans la mesure où tous les nœuds de sécurité doivent comporter un archivage NV pour les données de configuration, cette transmission est probable uniquement lors du remplacement d'un appareil, d'un amorçage initial ou d'une modification de la configuration. Ce processus est représenté à la Figure 68.

Les cibles doivent répondre à un service SafetyOpen de forme 2 par un code d'erreur 01_{hex}, un code supplémentaire 0110_{hex} (appareil non configuré), lorsque l'appareil n'est pas configuré.

Lorsqu'un point d'origine détecte une modification des données de configuration conservées pour un appareil, il doit toujours émettre une demande de connexion de forme 1 à sa première connexion. Le SCID renvoyé doit être validé par rapport à la valeur conservée.

Il existe deux types de services SafetyOpen de forme 2: avec et sans le SCID.

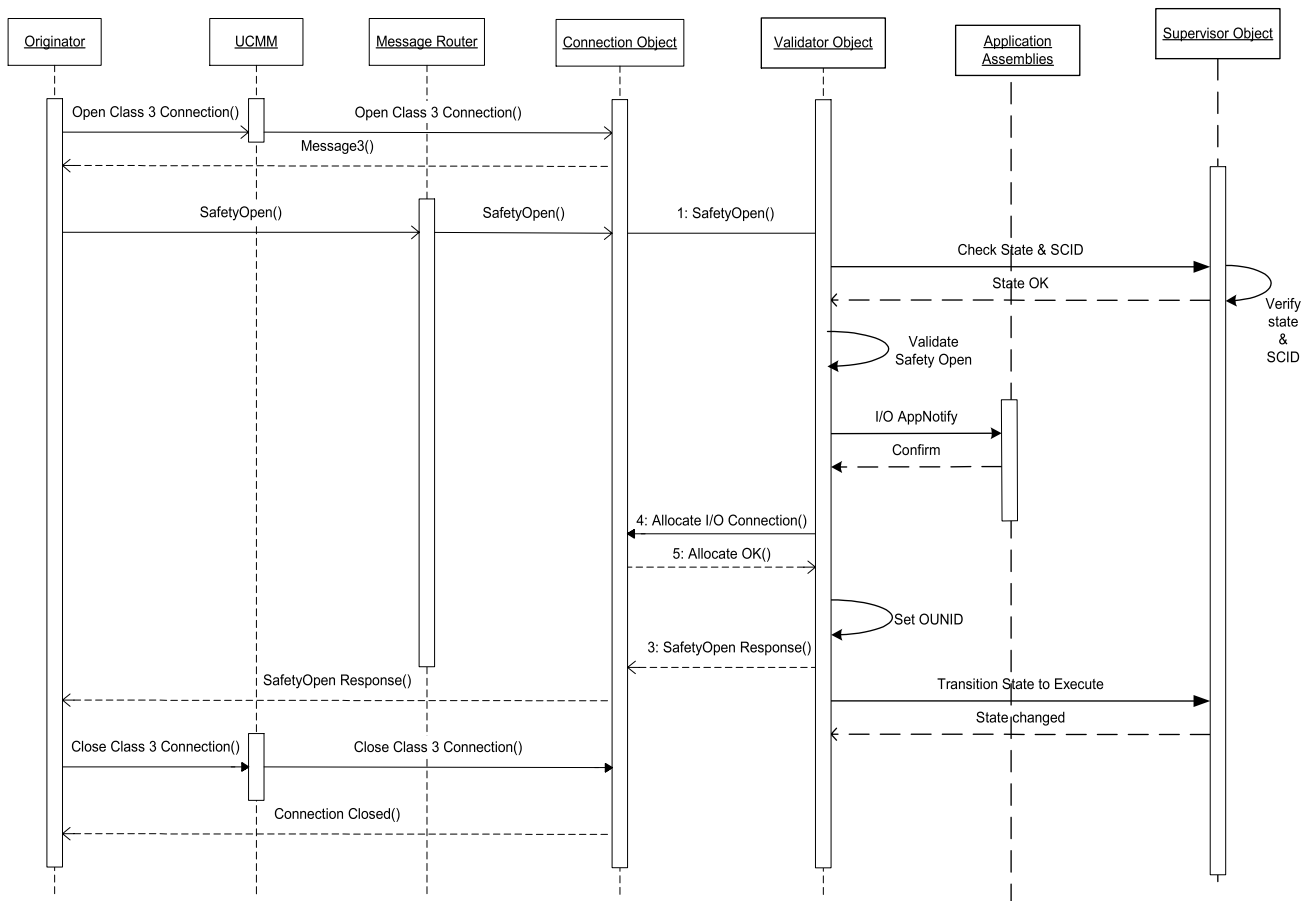
- Forme 2a: Lorsqu'une cible reçoit un service SafetyOpen de forme 2 (aucune donnée de configuration) accompagné d'un ID de configuration de sécurité non nul (SCID = SCCRC + SCTS), elle doit le comparer au SCID de la configuration et accepter uniquement la connexion si elles sont adaptées.
- Forme 2b: Lorsqu'une cible reçoit un service SafetyOpen de forme 2 (aucune donnée de configuration) accompagné d'un SCID de valeur nulle, elle omet le contrôle.

Le Tableau 102 récapitule les formes de services SafetyOpen.

Tableau 102 – Récapitulatif SafetyOpen

	SafetyOpen de forme 1 avec données	SafetyOpen de forme 2a avec contrôle SCID	SafetyOpen de forme 2b sans contrôle SCID
TUNID	X	X	X
OUNID	X	X	X
UPID ^a	X	X	X
CPCRC	X	X	X
SCID	X	X	= 0
Données de configuration dans le service SafetyOpen	Oui	Non	Non
^a L'UPID est déduit des composants du service SafetyOpen ou des données d'application contenues dans la réponse SafetyOpen. Voir 6.3.12.			

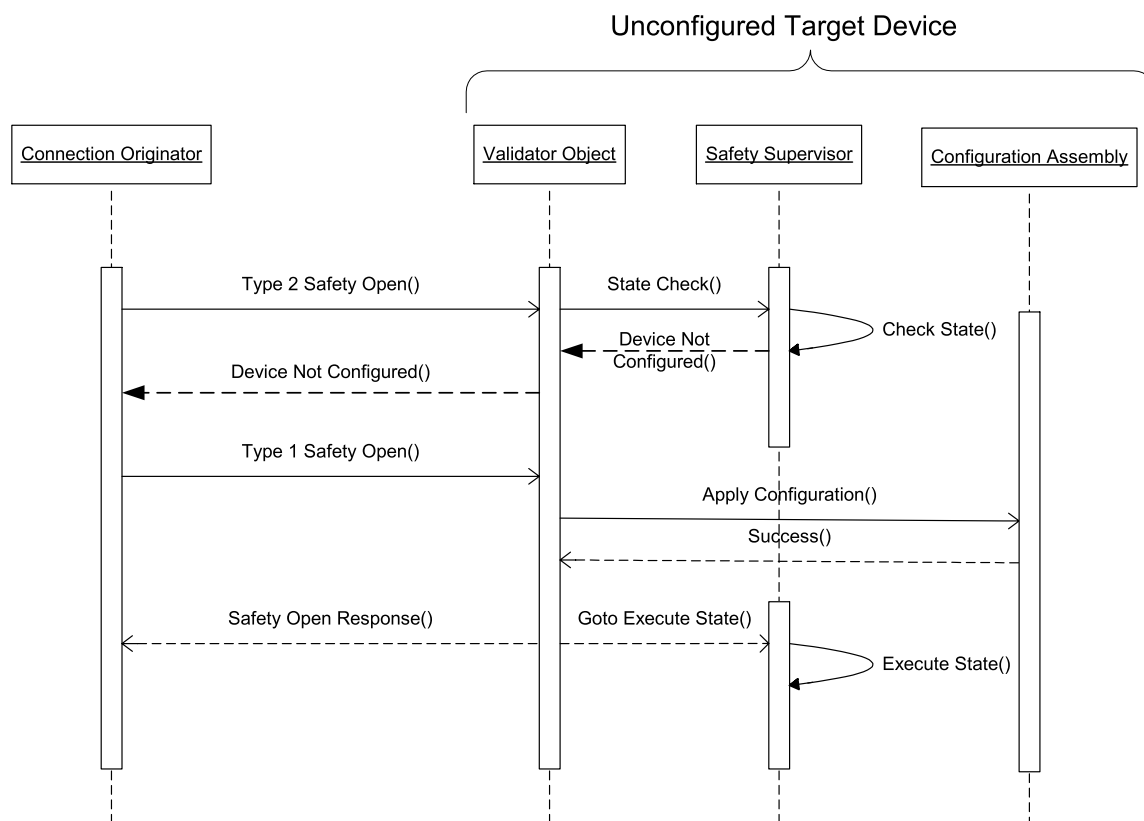
Le traitement des services SafetyOpen dans les cibles diffère selon la forme du message SafetyOpen reçu. La Figure 68 définit le message et la séquence d'événements pour le service SafetyOpen de forme 1, ainsi que les objets chargés des diverses étapes de traitement. Cette figure précise également que la différence principale entre les formes 1 et 2 de traitement constitue l'étape de transition des données de configuration vers un ensemble de configuration et d'attribution d'un propriétaire à cette configuration.



IEC

Anglais	Français
Originator	Point d'origine
Message router	Routeur de messages
Connection object	Objet de connexion
Validator object	Objet de validation
Application assemblies	Ensembles d'application
Supervisor object	Objet de programme de contrôle
Open class 3 connection	Connexion de classe 3 ouverte
Check state & SCID	Vérification de Etat & SCID
State OK	État OK
Validate SafetyOpen	Validation de SafetyOpen
Verify state & SCID	Vérification de Etat & SCID
Confirm	Confirmation
Allocate I/O connection	Attribution de connexion E/S
Allocate OK	Attribution OK
Set OUNID	Réglage de OUNID
SafetyOpen response	Réponse de SafetyOpen
Transition state to execute	Transition d'état vers Exécution
State changed	État modifié
Close class 3 connection	Connexion de classe 3 fermée
Connection closed	Connexion fermée

Figure 67 – Établissement d'une connexion de sécurité CP 2/3 dans les cibles pour un service SafetyOpen de forme 2a



IEC

Anglais	Français
Unconfigured target device	Appareil cible non configuré
Connection originator	Point d'origine de connexion
Validator object	Objet de validation
Safety supervisor	Programme de contrôle de sécurité
Configuration assembly	Ensemble de configuration
Type 2 safetyOpen	SafetyOpen de type 2
State check	Vérification d'état
Device not configured	Appareil non configuré
Type 1 SafetyOpen	SafetyOpen de type 1
Apply configuration	Application de la configuration
Success	Réussite
SafetyOpen response	Réponse de SafetyOpen
Goto execute state	Aller vers l'état Exécution
Execute state	État Exécution

Figure 68 – Séquence générale de détection de la nécessité d'une configuration

8.8.6 Recommandations pour l'attribution d'un nombre de consommateurs

Lors de l'établissement d'une connexion multipoints, le producteur de cette connexion doit attribuer au consommateur un nombre unique. La difficulté principale de ce processus ne réside pas dans l'attribution initiale, mais dans la gestion du cas où un producteur a fermé une connexion pour un motif donné et nécessite à présent de décider du moment où la réattribution de ce nombre de consommateurs est acceptable.

Dans la mesure où les producteurs multipoints continuent de produire des données même en cas de fermeture d'une connexion à un consommateur particulier (c'est-à-dire en supposant que d'autres connexions de consommateur sont toujours ouvertes), le seul mécanisme à disposition d'un consommateur multipoints pour détecter la perte de la connexion consiste à déterminer qu'un message de correction de temps ne lui a pas été attribué dans le cadre des intervalles $\text{Ping Timeout\_Multiplier.PI} + 1$. Au cours de cette période, le consommateur pense toujours que la connexion est ouverte, continue à traiter les données reçues et à transmettre les réponses de coordination temporelle (même si le producteur les ignore).

Si le producteur venait à recevoir une nouvelle demande de connexion d'un autre consommateur et à réattribuer ce nombre de consommateurs, deux consommateurs utiliseraient alors le même nombre au cours de cette période. Le producteur recommencerait à traiter les réponses de coordination temporelle et à transmettre des messages de correction de temps avec ce nombre de consommateurs. En d'autres termes, si la temporisation était simplement correcte, l'ancien consommateur pourrait ne jamais détecter que la connexion a échoué et il existerait deux consommateurs avec le même nombre qui transmettraient des informations d'horloge conflictuelles avec des valeurs de correction tout aussi conflictuelles. Bien que ce cas soit détecté finalement par le producteur par un marquage PID, un moyen doit être prévu pour en réduire l'occurrence.

Les producteurs multipoints doivent mettre en quarantaine les nombres de consommateurs qui ont été utilisés hors ligne pendant les intervalles $\text{Ping Timeout\_Multiplier.PI} + 2$, avant qu'ils ne puissent être réattribués à une autre connexion. La seule exception à cette opération est le moment où un consommateur émet un service `ForwardClose` pour signifier au producteur la fermeture de la connexion. Dans ce cas, il est possible de réutiliser immédiatement le nombre de consommateurs.

8.8.7 Recommandations pour l'établissement d'une connexion

Lorsqu'un consommateur multipoints décide de fermer une connexion de manière unilatérale, la seule façon pour un producteur de détecter cet événement (autrement que par la transmission d'un service `ForwardClose` par le consommateur) est le moment où il ne reçoit plus de réponse de coordination temporelle pendant les intervalles $\text{Ping Timeout\_Multiplier.PI} + 2$. Pendant cet intervalle de temps, le nombre de consommateurs est toujours attribué au consommateur concerné. Il est très probable que ce consommateur émette un nouveau service `SafetyOpen` tandis que cette connexion reste ouverte. Deux options s'offrent aux producteurs dans ce cas:

- Examiner les connexions existantes et déterminer si une connexion avec ce même consommateur est déjà établie et si tel est le cas, réémettre le nombre de consommateurs;
- Attribuer un nouveau consommateur et permettre la temporisation, puis la mise en quarantaine, de l'ancien nombre de consommateurs.

La première option est la plus difficile à coder, mais représente l'option recommandée dans la mesure où elle propose un programme de réattribution plus robuste pour des nombres de consommateurs. La seconde option présente l'avantage d'une mise en œuvre plus simple, tout en permettant aux nombres de consommateurs de rester en quarantaine plus longtemps que nécessaire. Cette seconde option peut également rendre problématique l'amorçage des connexions pour des applications avec lesquelles le nombre de consommateurs est > 8 .

Si la première option est retenue, il convient que le programme recommandé d'adaptation aux connexions soit également adapté:

- à l'OUNID, et
- au chemin de données d'application.

Si ces éléments sont adaptés aux paramètres d'une connexion existante, le nombre de consommateurs concerné de l'appareil peut être réémis.

8.8.8 Établissement de propriété

Le paragraphe 8.9 présente deux méthodes d'établissement de la propriété de connexion, par les outils logiciels ou à partir du service SafetyOpen. Ce paragraphe indique que des appareils sont nécessaires pour prendre en charge une installation qui permet une configuration «par outil uniquement» ou une configuration par point d'origine. Ce paragraphe implique enfin que les tentatives de reconfiguration d'un appareil via le service SafetyOpen sont refusées en cas de verrouillage de la configuration. Lorsque l'état «outil uniquement» n'est pas défini, l'outil logiciel peut également définir l'OUNID du point d'origine sélectionné lors de la mise en service de l'appareil cible pour une sécurité supplémentaire.

Le présent paragraphe 8.8.8 spécifie la méthode de définition de cette capacité dans les nouveaux objets Sécurité. Les appareils configurés par outil de configuration de réseau de sécurité (SNCT) doivent comporter les nouveaux objets Sécurité.

Pour établir la propriété de la configuration (et la connexion des sorties), l'OUNID de l'appareil d'origine est transmis à la cible dans le message SafetyOpen.

Les appareils de sécurité doivent archiver l'OUNID dans la mémoire non volatile pour la configuration de l'appareil. Ces appareils doivent également archiver dans la mémoire non volatile la signature de la configuration (SCID) dans l'appareil. Le SCID est déduit par concaténation du SCCRC et de la SCTS dans le service SafetyOpen.

Les appareils de sortie doivent archiver dans la mémoire non volatile l'OUNID associé à la connexion de sortie de sécurité.

Lorsque l'utilisateur a soumis à essai et vérifié la configuration générée par outil, il peut verrouiller la configuration contre tout changement et l'étiqueter comme «Verrouillée». Le drapeau «Verrouillage de configuration» est un attribut du Programme de contrôle de sécurité. Un mot de passe qui fournit une sécurité définie par l'utilisateur peut le modifier.

Les appareils configurés par le service SafetyOpen ne peuvent pas comporter un «Verrouillage de configuration». L'hypothèse formulée pose la définition de la condition de verrouillage et son contrôle au point d'origine de connexion.

8.8.9 Cas d'utilisation de la propriété

8.8.9.1 Généralités

Le présent paragraphe 8.8.9 présente une série de scénarios de connexion comportant également une tentative de configuration. Chaque scénario fournit une description succincte de la façon dont il convient que l'appareil traite chaque cas. La plupart de ces cas utilisent le service SafetyOpen pour configurer l'appareil. Ainsi, les caractéristiques de configuration par outil, telles que l'attribut «Verrouillage de configuration», ne doivent pas être utilisées.

8.8.9.2 Le propriétaire désigné par l'utilisateur connecte et configure un appareil d'entrée sans propriétaire et non configuré – (attribution de l'OUNID à la première connexion)

L'attribut Verrouillage de configuration dans la cible doit être «déverrouillé» et le Programme de contrôle de sécurité doit être en mode Configuration; l'appareil n'est pas configuré. L'appareil cible valide le service SafetyOpen comme correct et l'OUNID de point d'origine est archivé dans la cible et associé à la configuration. Une connexion point à point ou multipoints est établie. Le fonctionnement normal démarre.

Le point d'origine d'un service SafetyOpen de forme 1 qui configure un appareil d'entrée précédemment non configuré et sans propriétaire doit devenir le propriétaire de la configuration.

8.8.9.3 Le propriétaire désigné par l'utilisateur connecte et configure un appareil de sortie sans propriétaire et non configuré – (attribution de l'OUNID à la première connexion)

L'attribut «Verrouillage de configuration» de la cible doit être «déverrouillé» et le Programme de contrôle de sécurité doit être en mode Configuration; l'appareil n'est pas configuré. L'appareil cible valide le service SafetyOpen comme correct et l'OUNID est archivé dans la cible et associé à la configuration et à la connexion. Une connexion point à point est établie. Le fonctionnement normal démarre.

Un service SafetyOpen de forme 1 qui configure un appareil de sortie précédemment non configuré et sans propriétaire doit devenir le propriétaire de la connexion et de la configuration.

8.8.9.4 Le propriétaire connecte et configure un appareil d'entrée avec propriétaire et non configuré – (attribution de l'OUNID par outil)

L'attribut «Verrouillage de configuration» de la cible doit être «déverrouillé» et le Programme de contrôle de sécurité doit être en mode Configuration; l'appareil n'est pas configuré. L'appareil cible valide le service SafetyOpen comme correct et l'OUNID du service SafetyOpen correspond à l'OUNID archivé. Une connexion point à point ou multipoints est établie. Le fonctionnement normal démarre.

8.8.9.5 Le propriétaire connecte et configure un appareil de sortie avec propriétaire et non configuré – (attribution de l'OUNID par outil)

L'attribut «Verrouillage de configuration» de la cible doit être «déverrouillé» et le Programme de contrôle de sécurité doit être en mode Configuration; l'appareil n'est pas configuré. L'appareil cible valide le service SafetyOpen comme correct et l'OUNID du service SafetyOpen correspond à l'OUNID archivé pour la configuration et la connexion. La cible archive la configuration. Une connexion point à point est établie. Le fonctionnement normal démarre.

Un second appareil tente de se relier à une connexion de sortie pont à point avec propriétaire.

L'appareil cible évalue le service SafetyOpen si aucune connexion n'est ouverte. Lorsqu'un service SafetyOpen de forme 1 est transmis au point de différence entre l'OUNID de point d'origine et l'OUNID archivé avec la connexion, le service SafetyOpen doit être refusé et un message d'erreur, "O_UNID Mismatch", est renvoyé.

8.8.9.6 Le propriétaire connecte et tente de reconfigurer un appareil détenu par outil et configuré – (Verrouillage de configuration défini)

Si un point d'origine tente de configurer un appareil avec l'attribut Verrouillage de configuration défini, l'appareil doit rejeter le service SafetyOpen et renvoyer un message d'erreur «Configuration non admise».

8.8.9.7 Reconfiguration d'appareil – Appareil d'entrée

Le propriétaire d'un appareil transmet à l'appareil cible un service SafetyOpen avec des données de configuration et un SCID (SCCRC et SCTS). Les données peuvent ou non être identiques à celles que comporte l'appareil et le SCID peut ou non être adapté au SCID existant. Indépendamment de ce qui précède, il convient que le message transmis soit traité comme une reconfiguration, et ce, tant que le processus suivant est respecté.

Un appareil d'entrée cible qui comporte une configuration existante doit (au minimum) exécuter ce qui suit à la réception d'un service SafetyOpen de forme 1.

- vérifier que le TUNID du service SafetyOpen correspond au TUNID de l'appareil;

- si les données de configuration sont incluses (forme 1), vérifier que l'OUNID du service SafetyOpen correspond à l'OUNID archivé;
- vérifier que la clé électronique est adaptée à l'appareil;
- calculer le SCCRC avec les données reçues et confirmer que la même valeur est obtenue;
- vérifier que le CPCRC de la configuration est correct;
- initier son processus de reconfiguration (saisie État de configuration), fermer et neutraliser les connexions au cours de la reconfiguration (répondre aux demandes de connexion avec une réponse d'erreur, «Mode/État invalide»);
- actualiser la configuration et le SCID dans la mémoire non volatile;
- vérifier et valider les paramètres de connexion;
- valider le chemin d'application;
- confirmer la prise en charge de la connexion de sécurité demandée;
- les paramètres de sécurité figurent dans des plages valides;
- faire passer la connexion dans l'état établi, et l'appareil dans l'état d'exécution;
- les nouvelles connexions peuvent désormais être acceptées.

Une connexion du type sollicité est établie. Tandis que les nouvelles connexions peuvent une nouvelle fois être acceptées, ces autres appareils doivent à présent comporter le nouvel SCID ou se connecter avec un SCID = 0.

8.8.9.8 Reconfiguration d'appareil – Appareil de sortie

Le propriétaire d'un appareil transmet à l'appareil cible un service SafetyOpen avec une configuration et un SCID. Les données peuvent ou non être identiques à celles que comporte l'appareil et le SCID peut ou non être adapté au SCID existant. Indépendamment de ce qui précède, il convient que le message transmis soit traité comme une reconfiguration, et ce, tant que le processus suivant est respecté.

Un appareil de sortie cible qui comporte une configuration existante doit (au minimum) exécuter ce qui suit à la réception d'un service SafetyOpen de forme 1.

- si le chemin de connexion se dirige vers une ressource de sortie, vérifier que l'OUNID du service SafetyOpen correspond à l'OUNID pour la connexion.
- vérifier que le TUNID du service SafetyOpen correspond au TUNID de l'appareil;
- vérifier que la clé électronique est adaptée à l'appareil;
- si les données de configuration sont incluses (forme 1), vérifier que l'OUNID du service SafetyOpen correspond à l'OUNID archivé pour la configuration;
- calculer le SCCRC avec les données reçues et confirmer que la même valeur est obtenue;
- vérifier que le CPCRC de la configuration est correct;
- initier son processus de reconfiguration par la fermeture et la neutralisation des connexions au cours de la reconfiguration (répondre aux demandes de connexion avec une réponse d'erreur, «Mode/État invalide»);
- actualiser la configuration et le SCID dans la mémoire non volatile;
- vérifier et valider les paramètres de connexion;
- valider le chemin d'application;
- confirmer la prise en charge de la connexion de sécurité demandée;
- les paramètres de sécurité figurent dans des plages valides;
- faire passer la connexion dans l'état établi, et l'appareil dans l'état d'exécution.

Il convient d'établir à présent une connexion du type sollicité.

8.8.9.9 Établissement d'une connexion à un appareil avec propriétaire précédent (modification de l'OUNID)

Lors de sa tentative de configuration d'un appareil ayant un autre propriétaire, une demande de configuration SafetyOpen (c'est-à-dire de forme 1) sans OUNID correspondant sera refusée avec une réponse d'erreur, «Défaut d'adaptation OUNID».

Pour supprimer un OUNID existant, les cibles de sécurité doivent prendre en charge une «réinitialisation sur out-of-box» en appliquant une remise à zéro de l'appareil ou en utilisant la commande de réinitialisation spéciale définie dans le Programme de contrôle de sécurité.

Si l'appareil comporte une connexion E/S de sortie en cas de réception d'une commande de réinitialisation, cette commande doit être refusée et un message d'erreur doit être renvoyé, (Mode/État invalide). Aucune connexion E/S de sortie ne doit être établie pour qu'un appareil soit réinitialisé par commande.

Un second appareil tente de se relier à une connexion multipoints avec propriétaire.

Un second point d'origine transmet un service SafetyOpen (c'est-à-dire de forme 2a ou 2b) à un appareil comportant une connexion multipoints dont le propriétaire est un autre point d'origine. Si le SCID du service SafetyOpen est non nul, il est comparé au SCID sauvegardé. Si les signatures correspondent, la connexion est établie. Si ces signatures ne correspondent pas, la réponse d'erreur «Défaut d'adaptation SCID» est renvoyée. Il n'est pas nécessaire que le propriétaire soit actif au cours de ce processus.

Un appareil cible qui comporte une configuration existante doit (au minimum) exécuter ce qui suit à la réception d'un service SafetyOpen de forme 2a ou 2b:

- si le chemin de connexion se dirige vers une ressource de sortie, vérifier que l'OUNID du service SafetyOpen correspond à l'OUNID pour la connexion.
- Si le SCID est non nul, confirmer que celui-ci correspond au SCID de l'appareil;
- vérifier que le TUNID du service SafetyOpen correspond au TUNID de l'appareil;
- vérifier que la clé électronique est adaptée à l'appareil;
- vérifier que le CPCRC de la configuration est correct;
- vérifier et valider les paramètres de connexion;
- valider le chemin d'application;
- confirmer la prise en charge de la connexion de sécurité demandée;
- les paramètres de sécurité figurent dans des plages valides;
- faire passer la connexion vers l'état établi.

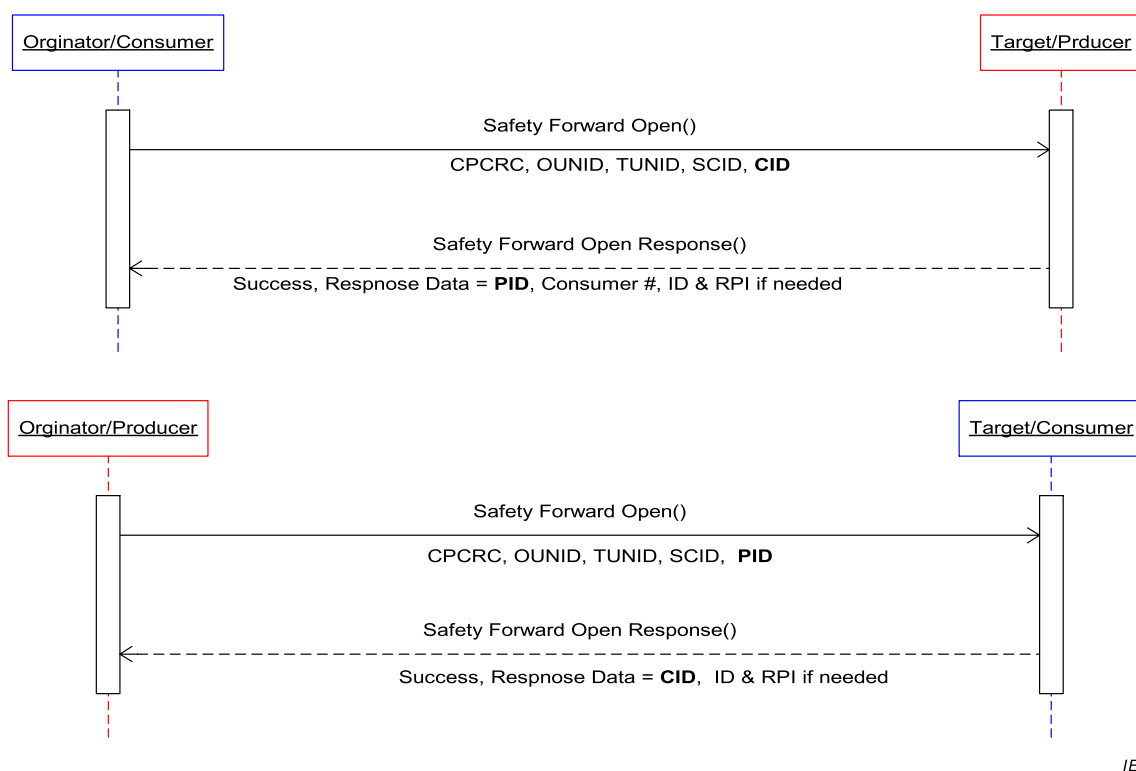
8.8.10 Utilisation et établissement de la relation PID/CID

Le mécanisme de marquage PID/CID a été défini pour détecter l'insertion de messages à partir d'une source non valide. Cette insertion peut être effectuée par un autre producteur qui transmet des données de sécurité, un autre producteur qui transmet des messages de correction de temps ou un consommateur invalide qui transmet des messages de coordination temporelle. Tous ces cas sont traités par le programme PID/CID dans le protocole de sécurité. L'échange des informations PID/CID au cours du processus d'établissement de connexion constitue l'élément clé de cette situation. Le producteur fournit son PID à tous ses consommateurs, et ces derniers doivent fournir leur CID respectif en retour au producteur. Cet échange a lieu quelle que soit l'origine de la connexion, ou quel que soit le type de connexion de sécurité établi.

Lors de l'établissement d'une connexion, les nœuds de production et de consommation doivent échanger leurs informations PID/CID respectives (ID du fournisseur + Numéro de série de l'appareil + Numéro de série de connexion). Le point d'origine transmet son ID dans

la demande SafetyOpen, et la cible renvoie son ID comme partie intégrante de la réponse satisfaisante SafetyOpen. Les deux cas sont définis à la Figure 69.

Le PID doit être utilisé pour le marquage des CRC de production de données et du CRC de correction de temps, et le CID doit être utilisé pour le marquage du CRC de coordination temporelle.



IEC

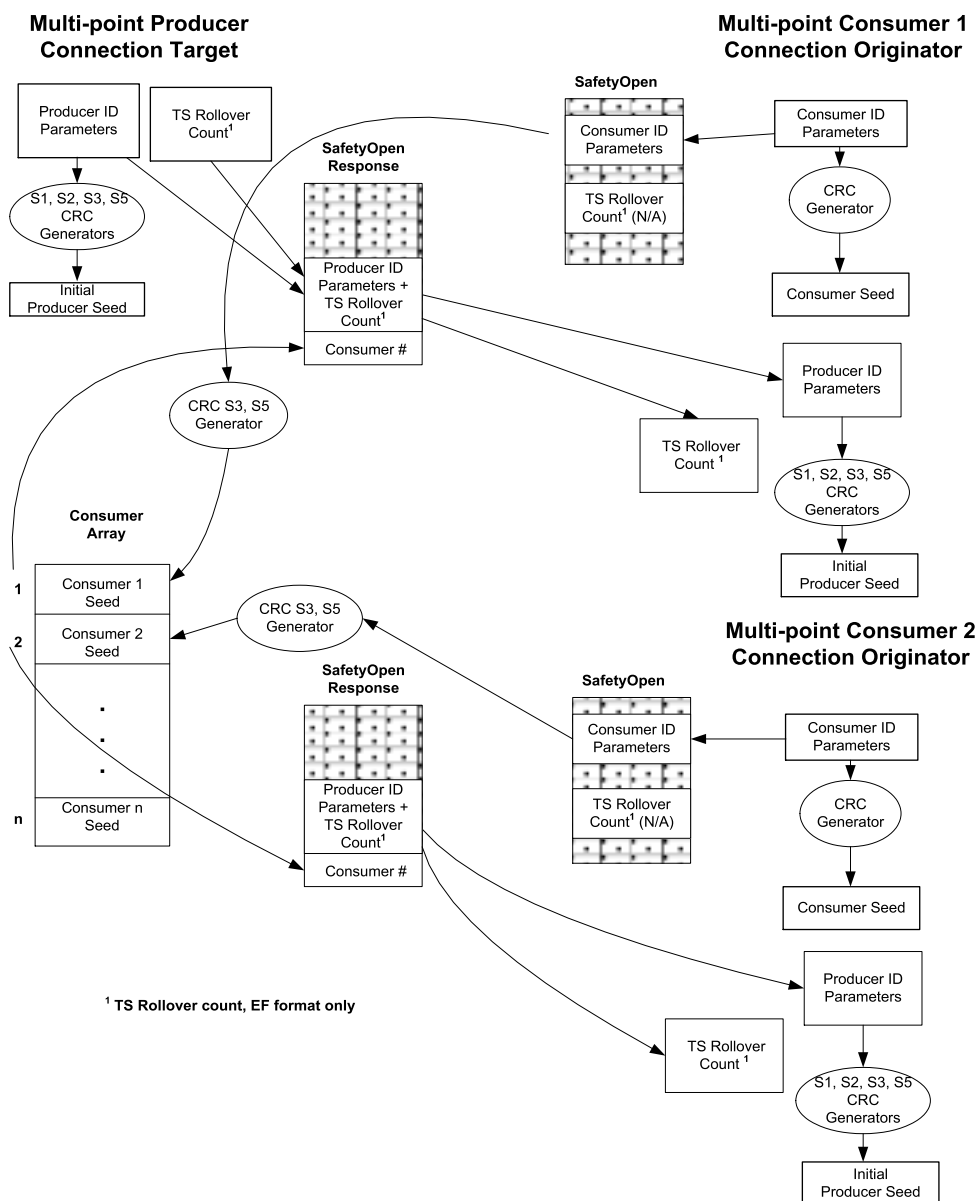
Anglais	Français
originator/consumer	point d'origine/consommateur
target/producer	cible/producteur
safety forward open	ForwardOpen de sécurité
safety forward open response	réponse de ForwarOpen de sécurité
success, response data =	données de réponse satisfaisantes
if needed	si nécessaire
originator/producer	point d'origine/producteur
target/consumer	cible/consommateur

Figure 69 – Échanges PID/CID pour deux scénarios de point d'origine

8.8.11 Utilisation PID/CID correcte dans les connexions multipoints et point à point

Le diagramme présenté à la Figure 70 représente la méthode d'utilisation des paramètres d'identifiant du producteur et du consommateur pour générer les valeurs de départ CRC pour les formats de Base et Etendu. Ce diagramme définit le cas de connexion multipoints, mais s'applique également aux connexions point à point (opération effectuée simplement à des fins de cohérence). Les références à TS _Rollover_Cnt et au détecteur de remplacement s'appliquent uniquement au format Etendu, et ne sont pas utilisées dans les formats de base. Les valeurs de départ du producteur sont générées uniquement au moyen des générateurs S1, S3 et S5 (c'est-à-dire même marquage utilisé pour les calculs des CRC S1 et S2), et le marquage CID est généré au moyen des générateurs S3 et S5.

Multi-point Connection
Establishment
CRC Seed Handling



IEC

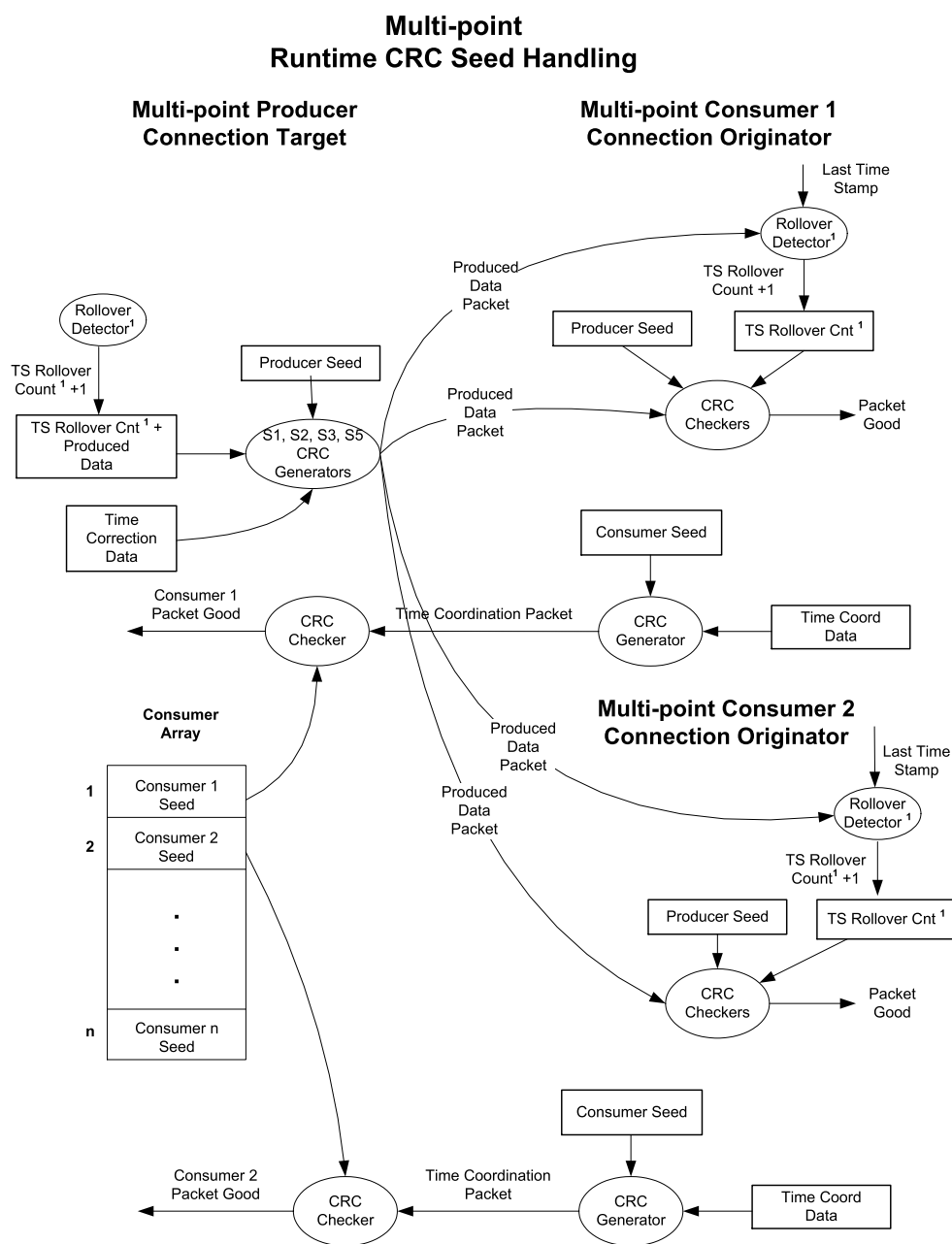
Anglais	Français
multi-point connection Establishment CRC seed handling	établissement de connexion multipoints – traitement de marquage CRC
multi-point producer connection target	cible de connexion du producteur multipoints
multi-point consumer 1 connection originator	point d'origine de connexion du consommateur 1 multipoints
producer ID parameters	paramètres d'ID de producteur
safetyopen response	réponse SafetyOpen
consumer ID parameters	paramètres d'ID de consommateur
S1, S2, S3, S5 CRC generators	générateurs CRC S1, S2, S3, S5
CRC generator	générateur CRC
initial producer seed	marquage de producteur initial
consumer seed	marquage de consommateur
consumer array	matrice de consommateur
multi-point consumer 2 connection originator	point d'origine de connexion du consommateur 2 multipoints

Figure 70 – Génération des valeurs de départ pour les connexions multipoints

Les paramètres PID doivent être utilisés pour le marquage des CRC des messages de données produites et des messages de correction de temps, et les paramètres CID doivent être utilisés pour le marquage du CRC des réponses de coordination temporelle.

Comme le représente la figure, il est nécessaire pour les producteurs multipoints de conserver une matrice de consommateurs afin de suivre l'évolution de la valeur de départ pour chaque nombre de consommateurs attribué. Le programme doit également s'appliquer aux connexions point à point, à l'exception du fait qu'il est nécessaire de conserver une seule valeur de départ de consommateur.

Le diagramme présenté à la Figure 71 représente la méthode d'application des valeurs de départ, établies lors de l'établissement de la connexion, dans la production des données d'exécution.



Anglais	Français
multi-point runtime CRC seed handling	traitement de marquage CRC d'exécution multipoints
multi-point producer connection target	cible de connexion du producteur multipoints
multi-point consumer 1 connection originator	point d'origine de connexion du consommateur 1 multipoints
last time stamp	dernière datation
rollover detector	détecteur de remplacement
producer seed	marquage de producteur
produced data	données produites
produced data packet	paquet de données produites
CRC checkers	vérificateurs CRC
packet good	paquet correct
S1, S2, S3, S5 CRC generators	générateurs CRC S1, S2, S3, S5
time correction data	données de correction de temps
consumer seed	marquage de consommateur
consumer 1 packet good	paquet de consommateur 1 correct
CRC checker	vérificateur CRC
CRC generator	générateur CRC
time coordination packet	paquet de coordination temporelle
time coord data	données de coordination temporelle
consumer array	matrice de consommateur
multi-point consumer 2 connection originator	point d'origine de connexion du consommateur 2 multipoints
consumer 1 seed	marquage de consommateur 1
consumer 2 seed	marquage de consommateur 2
consumer n seed	marquage de consommateur n

Figure 71 – Traitement d'exécution PID/CID

8.8.12 Services pris en charge par le réseau

Les paragraphes 8.8.12 et 8.8.13 ont pour objet de favoriser la compatibilité entre les appareils développés pour échanger des données de sécurité sur les réseaux de sécurité FSCP 2/1. Ils définissent par ailleurs des recommandations concernant les appareils de sécurité dont il convient que les différents types d'appareils de sécurité prennent en charge.

L'objectif est de permettre le développement des appareils d'entrée et de sortie qui incluent aussi bien des modules E/S discrets très simples que des modules E/S spécialisés de fonctionnalité élevée et intelligents. Lorsqu'un module d'entrée ou de sortie atteint un certain niveau d'exigences de fonctionnement, il peut se révéler nécessaire de le considérer comme intégrant un appareil logique de sécurité dans le module.

8.8.13 Type d'appareil de sécurité FSCP 2/1

8.8.13.1 Généralités

Pour une simplification de l'échange des informations et de la présentation des données de sécurité aux utilisateurs de systèmes multiples, les appareils qui participent au réseau de sécurité sont répartis en 4 types. Ces types sont les suivants:

- appareils d'entrée;
- appareils logiques;

- appareils de sortie;
- appareils E/S.

Les appareils d'entrée sont des appareils qui traduisent des signaux utilisateur en données de sécurité et transmettent ces données aux appareils logiques. Les appareils d'entrée ne reçoivent aucune autre donnée de sécurité que les données présentant un état de connexion de sécurité. Si un appareil comportant des informations d'entrée doit recevoir des données de sécurité de l'autre partie de la connexion de sécurité, il convient de le considérer comme un appareil E/S ou un appareil logique, et suivre les lignes directrices du type d'appareil E/S ou d'appareil de sécurité logique.

Les appareils logiques sont des appareils qui traitent les données d'entrée de sécurité et les données de sortie de production. La communication directe entre les appareils d'entrée et les appareils de sortie n'est pas prise en charge. Un appareil logique doit se situer entre un appareil d'entrée et un appareil de sortie, peu importe la simplicité impliquée.

Les appareils de sortie sont des appareils qui présentent un certain niveau de signal à l'environnement utilisateur sur la base des données de sécurité consommées par l'appareil concerné. L'état des appareils de sortie peut être «transmis» à l'appareil logique.

Les appareils E/S sont des appareils qui comportent des entrées et des sorties de sécurité.

8.8.13.2 Catégorie de connexions de sécurité

Toutes les connexions de sécurité peuvent être réparties dans l'une des quatre catégories ci-dessous:

- Input_Device_To_Logic_Device;
- Logic_Device_To_Output_Device;
- Logic_Device_To_I/O_Device (un appareil de sortie avec État est considéré comme un appareil E/S);
- Logic_Device_To_Logic_Device.

Les appareils logiques peuvent choisir de prendre en charge une ou l'ensemble des catégories de connexion de sécurité. Si un appareil prend effectivement en charge une catégorie de connexion de sécurité, il convient qu'il prenne en charge tous les services recommandés de cette catégorie.

8.8.13.3 Services de connexions de sécurité

Le Tableau 103 présente tous les services d'objet de validation de sécurité définis que les cibles ou les points d'origine de connexion peuvent prendre en charge.

Tableau 103 – Mapping des services point d'origine/cible

Point d'origine ou cible de connexion	Types de connexion de sécurité		Type d'objet de validation
	Type	Utilisation	
Cible	Point à point	Producteur	Type 1
Cible	Point à point	Consommateur	Type 2
Cible	Multipoints	Producteur	Type 3
Point d'origine	Point à point	Producteur	Type 1
Point d'origine	Point à point	Consommateur	Type 2
Point d'origine	Multipoints	Consommateur	Type 4

Le Tableau 104 présente les services d'objet de validation de sécurité dont il convient que les cibles ou points d'origine de connexion n'assurent pas la prise en charge. Il n'est pas nécessaire que les producteurs multipoints initient des connexions avec leurs consommateurs qui doivent se connecter; il convient que les consommateurs multipoints constituent le point d'origine de connexion, et que les producteurs multipoints constituent les cibles de connexion.

Tableau 104 – Types de service point d'origine/cible non pris en charge

Point d'origine ou cible de connexion	Types de connexion de sécurité		Type d'objet de validation
	Type	Utilisation	
Cible	Multipoints	Consommateur	N/A
Point d'origine	Multipoints	Producteur	N/A

8.8.13.4 Services pris en charge pour chaque catégorie

La Figure 72 et la Figure 74 répertorient les services de connexion de sécurité préférentiels pour les diverses catégories de connexion (voir la Figure 73 et la Figure 75 pour plus de clarification). Pour chaque catégorie de connexion de sécurité, les différentes colonnes représentent les méthodes préférentielles d'établissement de connexions de sécurité entre les deux appareils. Pour tout appareil particulier, une seule colonne serait prise en charge à la fois.

Catégorie de connexion de sécurité				Services pris en charge pour le type d'entrée ou de sortie						
				1		2	3			
				Appareil d'entrée à Appareil logique		Dispositif logique à Dispositif de sortie	Appareil logique à Appareil E/S (Sortie avec état)			
Service de connexion de sécurité				Op 1	Op 2		Op 1	Op 2	Op 3	
Point d'origine ou cible	Type de connexion de sécurité									
Appareils d'entrée et de sortie	Cible	Point à point	Producteur		O			O		
	Cible	Point à point	Consommateur			R	R	O		
	Cible	Multipoints	Producteur	R			R			
Appareils logiques	Point d'origine	Point à point	Producteur			R	R	O		
	Point d'origine	Point à point	Consommateur		O			O		
	Point d'origine	Multipoints	Consommateur	R			R			

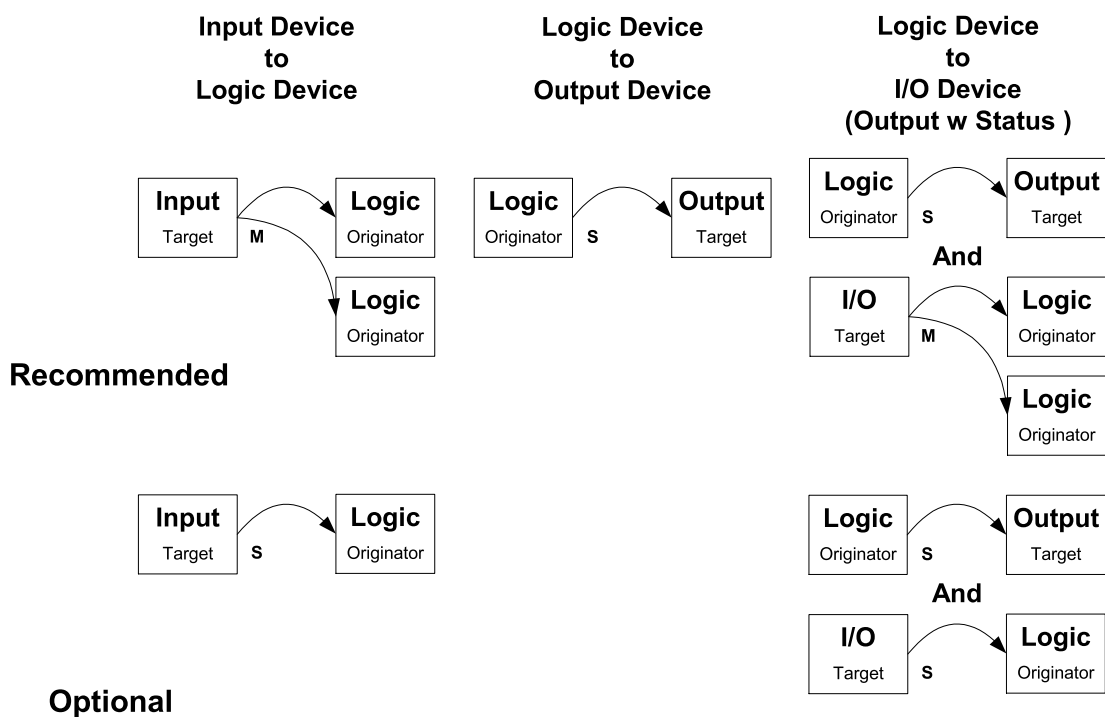
Légende

Op1, 2, 3 = Combinaisons facultatives

R = Services recommandés applicables à la compatibilité

O = Service facultatif

Figure 72 – Catégories de connexion et services pris en charge



IEC

Anglais	Français
input device to logic device	appareil d'entrée à appareil logique
logic device to output device	appareil logique à appareil de sortie
logic device to I/O device (output w status)	appareil logique à appareil E/S (sortie avec Etat)
input	entrée
target	cible
logic	logique
originator	point d'origine
output	sortie
I/O	E/S
and	et
recommended	recommandé
optional	facultatif

Figure 73 – Types de connexion recommandés

Service de connexion de sécurité				Catégorie de connexion de sécurité 4			
Point d'origine ou cible				Appareil logique à appareil logique			
Type d'objet de validation de sécurité				Combinaisons de services pris en charge			
				Op 1	Op 2	Op 3	Op 4
Cible d'appareil logique	Cible	Point à point	Producteur			O	
	Cible	Point à point	Consommateur		O		
	Cible	Multipoints	Producteur	R			
Point d'origine d'appareil logique	Point d'origine	Point à point	Producteur		O		
	Point d'origine	Point à point	Consommateur			O	
	Point d'origine	Multipoints	Consommateur	R			

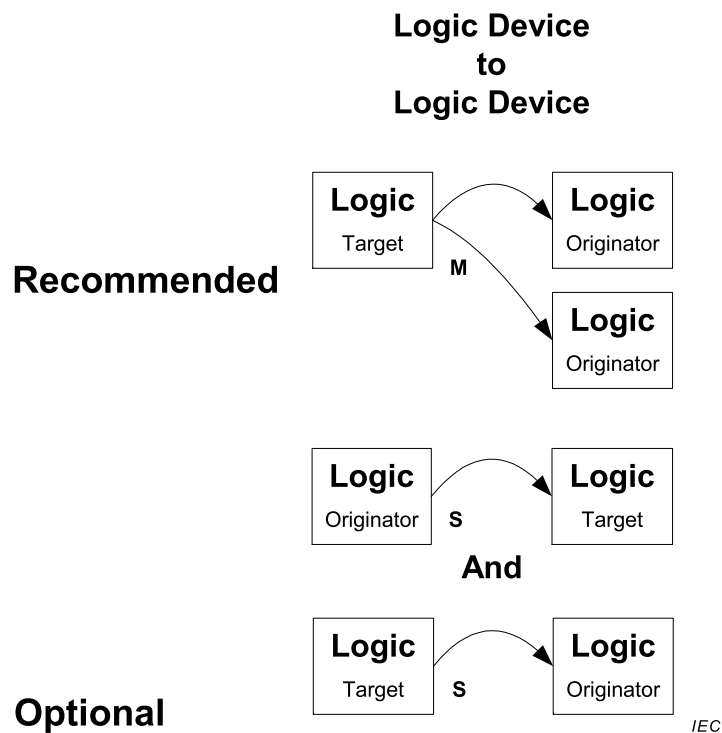
Légende

Op1, 2, 3 = Combinaisons facultatives

R = services recommandés applicables à la compatibilité

O = Service facultatif

Figure 74 – Services pris en charge logique à logique



Anglais	Français
logic device to logic device	appareil logique à appareil logique
target	cible
logic	logique

Anglais	Français
originator	point d'origine
and	et
recommended	recommandé
optional	facultatif

Figure 75 – Types de connexion recommandés pour les services logique à logique

8.9 Processus de configuration de sécurité

8.9.1 Introduction à la configuration de sécurité

Le présent paragraphe 8.9 a pour objet d'identifier le processus de configuration de réseau de sécurité et les flux de données de configuration dans le système de sécurité. Ce paragraphe 8.9 définit les exigences systèmes et logicielles de l'interface de configuration de réseau de sécurité, ainsi que la méthode de protection des données permettant de s'assurer que le système de sécurité satisfait au niveau SIL 3.

Le processus de configuration comprend deux parties: 1) téléchargement aval et 2) essais et vérification.

Processus de téléchargement aval:

Au cours du téléchargement aval du processus de configuration, les données de configuration proviennent de l'une des deux sources suivantes:

- de l'outil de configuration du réseau de sécurité (SNCT) à l'appareil configuré;
- du point d'origine à l'appareil cible.

Processus de vérification:

- l'utilisateur soumet l'appareil à un essai de fonctionnement dans le système pendant la phase de vérification, et vérifie de manière visuelle que les données de configuration appropriées ont été transmises à l'appareil configuré.
- les protections de ces deux parties permettent de s'assurer que la configuration des appareils est adaptée à une utilisation dans un environnement SIL 3.

8.9.2 Objectifs de configuration

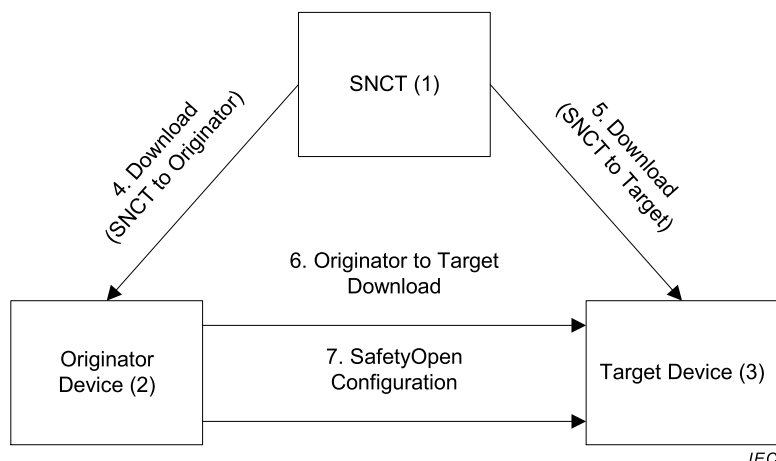
Les objectifs relatifs à la sécurité du processus de configuration applicable aux appareils de sécurité FSCP 2/1 sont présentés dans le Tableau 105.

Tableau 105 – Objectifs de configuration

Objectif	Description
Objectif 1	S'assurer avec une haute intégrité que la configuration prévue créée par l'utilisateur avec le logiciel a été correctement transmise et archivée dans l'appareil de sécurité
Objectif 2	Disposer d'un processus de téléchargement aval commun identique pour le transfert des données de configuration à tous les appareils de sécurité
Objectif 3	Disposer d'un processus de téléchargement aval commun identique pour le transfert des données de configuration à partir d'un outil logiciel ou d'un appareil d'origine pendant la configuration
Objectif 4	S'assurer avec une intégrité de niveau SIL 3 qu'un appareil cible présente la configuration prévue préalablement à l'ouverture d'une connexion de sécurité. Il convient de réappliquer les mesures utilisées au cours du téléchargement aval de configuration, dans le processus d'établissement de la connexion de sécurité
Objectif 5	S'assurer de l'identification unique de la configuration avec ou sans inclusion de données dans l'établissement d'une connexion

8.9.3 Présentation générale de la configuration

La configuration de sécurité débute avec le téléchargement aval des données de configuration dans un appareil de sécurité. La Figure 76 représente les transferts de données de configuration possibles vers les appareils de sécurité. Les nombres qui apparaissent sur la Figure constituent des références à la numérotation de travail ci-dessous.



Anglais	Français
download	téléchargement aval
SNCT to originator	SNCT à point d'origine
SNCT to target	SNCT à cible
originator to target download	téléchargement aval du point d'origine à la cible
originator device	appareil d'origine
safetyopen configuration	configuration SafetyOpen
target device	appareil cible

Figure 76 – Transferts de données de configuration

Les appareils impliqués dans le processus de configuration sont représentés à la Figure 76. Les fonctions des éléments 1, 2 et 3 sont décrites comme suit:

- l'outil de configuration de réseau de sécurité SNCT (1) et le processus décrit dans la présente partie permettent à cet outil de ne pas être critique pour la sécurité;
- Le point d'origine (2) est un appareil capable de configurer les appareils cibles de configuration (3) tout en initiant des connexions avec eux. Ces appareils sont associés à des procédures supplémentaires visant à achever le processus de configuration dans la mesure où ils peuvent conserver des données de configuration dédiées aux cibles (pour les cibles non configurées directement par le SNCT).
- L'appareil cible (3) est un appareil qui peut être configuré directement par le SNCT, ou par un propriétaire de point d'origine (2). Le concept de propriété joue un rôle important dans l'assurance de l'intégrité des cibles «configurées par le point d'origine».

Il existe deux procédures de configuration fondamentales (voir Figure 76). Ces procédures sont décrites comme suit:

- SNCT à point d'origine (flux 4) et SNCT à Cible (flux 5). Cette procédure consiste à configurer un appareil simple, les appareils obtenus ne contenant aucune donnée de configuration destinée à d'autres appareils;
- SNCT à point d'origine à Cible (flux 4 plus flux 6 ou 7). Cette procédure spéciale permet de configurer un appareil d'origine qui contient des données de configuration pour une cible;

- Le flux 6 constitue une procédure de duplication de la séquence d'opérations qui seraient exécutées autrement dans le flux 5;
- Le flux 7 constitue une procédure par laquelle la configuration est exécutée comme partie intégrante du traitement d'un service SafetyOpen.

Il existe deux méthodes de reconfiguration d'un appareil de remplacement à partir du point d'origine; ces méthodes sont décrites comme suit:

- Le flux 6 constitue une procédure de duplication de la séquence d'opérations qui seraient exécutées autrement dans le flux 5;
- Le flux 7 constitue une procédure par laquelle la configuration est exécutée comme partie intégrante du traitement d'un service SafetyOpen.

8.9.4 Lignes directrices pour la configuration de l'utilisateur

Le présent paragraphe 8.9.4 décrit les lignes directrices pour la configuration de l'utilisateur qui permettent de s'assurer de la configuration et de la protection appropriées d'un système de sécurité FSCP 2/1. Ces lignes directrices permettent de définir les exigences relatives au manuel de sécurité.

Les flux de données de configuration de l'utilisateur sont définis à la Figure 77.

- a) l'utilisateur du système de sécurité FSCP 2/1 doit s'assurer du verrouillage des appareils configurés par le SNCT (2) après vérification.

Les appareils dont la configuration peut s'effectuer via l'interface SNCT doivent inclure des recommandations concernant le manuel de sécurité qui indiquent à l'utilisateur de verrouiller l'appareil une fois la vérification effectuée.

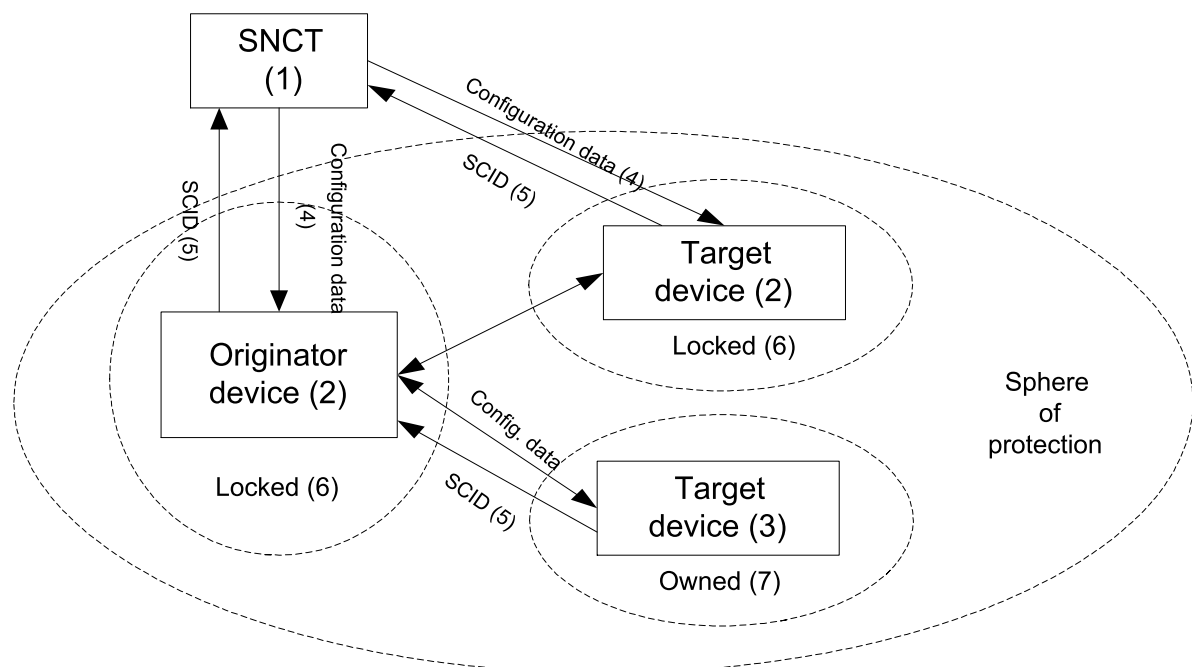
- b) l'utilisateur du système de sécurité FSCP 2/1 doit s'assurer que la propriété (7) de tous les appareils configurés par le point d'origine (3) est attribuée au point d'origine prévu.

Les appareils dont la configuration peut être effectuée par un service SafetyOpen de forme 1 doivent inclure des recommandations concernant le manuel de sécurité qui indiquent à l'utilisateur de vérifier que la propriété de tous les appareils de sécurité configurés par le point d'origine est attribuée comme partie intégrante du processus de vérification finale.

- c) l'utilisateur doit confirmer de manière visuelle (4) les données de configuration transmises, ainsi que leur téléchargement aval correct.

Tous les appareils de sécurité FSCP 2/1 doivent inclure des recommandations concernant le manuel de sécurité qui indiquent à l'utilisateur de vérifier de manière visuelle le téléchargement aval correct de toutes les données de configuration.

- d) l'utilisateur doit soumettre leur application à un essai de fonctionnement.
- e) l'utilisateur doit s'assurer du contrôle effectif SCID (5) par la cible et le point d'origine.



IEC

Anglais	Français
configuration data	donnée de configuration
target device	appareil cible
originator device	appareil d'origine
Locked	verrouillé
sphere of protection	zone de protection
Owned	avec propriétaire

Figure 77 – Mesures de protection des appareils de sécurité

8.9.5 Justification de niveau SIL3 du processus de configuration

Les mesures de sécurité associées à l'appareil de sécurité FSCP 2/1 téléchargé aval sont définies de manière à s'assurer de l'intégrité des données et des transferts de données tel que spécifié par le niveau SIL 3 de l'IEC 61508.

Le SNCT n'est par ailleurs pas évalué en raison des limites imposées au matériel informatique personnel, au système d'exploitation utilisé et aux outils de développement. En raison de ces facteurs, les techniques utilisées pour la configuration d'un appareil de sécurité exigent de l'appareil de sécurité et des procédures de l'utilisateur, et non pas du logiciel de poste de travail, qu'ils mettent en œuvre les mesures de protection.

La satisfaction aux exigences suivantes permet d'atteindre le niveau d'intégrité SIL3:

- un appareil SIL3 de réception doit calculer un SCCRC avec le niveau d'intégrité SIL3 et le comparer avec le SCCRC dans le SCID;
- pour les appareils configurés par la forme 1 ou un outil, la validation de configuration des données relatives à la sécurité téléchargées aval à partir du logiciel (ou du point d'origine) doit être effectuée avec un niveau d'intégrité SIL3;
- lorsque la configuration d'un appareil SIL3 s'effectue directement à partir d'un poste de travail, le manuel de sécurité de l'appareil doit indiquer à l'utilisateur de comparer le SCID et les données de configuration transférées avec le SCID et les données de configuration observées à l'origine au poste de travail;

- Le logiciel SNCT doit prévoir une fonctionnalité qui permet à l'utilisateur de confirmer le caractère correct des configurations téléchargées;
- les appareils SIL 3 doivent archiver/restaurer leurs données de configuration avec un niveau d'intégrité SIL3;
- les appareils SIL3 doivent traiter toutes les transitions d'état d'appareils avec un niveau d'intégrité SIL3;
- les sous-systèmes qu'il est nécessaire d'examiner et d'évaluer selon le niveau SIL3;
- le traitement de configuration des appareils cibles;
- l'archivage de configuration des appareils cibles;
- la validation de configuration des appareils cibles;
- les modes des appareils cibles.

8.9.6 Fonctions d'appareils pour configuration par outil

Le processus d'interaction du SNCT avec les points d'origine et les cibles est contrôlé par les installations définies dans l'objet Programme de contrôle de sécurité. Les caractéristiques telles que la protection par mot de passe et l'attribut Verrouillage de configuration s'associent pour assurer la sécurité de cette interface. Les détails d'interface sont communs dans la mesure où le Programme de contrôle de sécurité est fourni dans le profil de référence (voir 6.5.3) tant pour les cibles que pour les points d'origine de sécurité. Les paragraphes 8.9.7 à 8.9.12 définissent ces caractéristiques, ainsi que les méthodes d'utilisation de ces dernières par le SNCT.

8.9.7 Sécurité par mot de passe

L'interface SNCT définit les fonctions suivantes de sécurité par mot de passe facultative:

- Complément de fonctionnalité par mot de passe.

La prise en charge d'un mot de passe doit être mise en œuvre par les appareils qui prennent en charge l'interface SNCT.

Les mots de passe soumis aux appareils qui prennent en charge l'interface SNCT doivent être les valeurs obtenues par l'exécution de l'algorithme de cryptage défini en 7.1.2.3.

La valeur de mot de passe par défaut dans les appareils qui prennent en charge l'interface SNCT doit être nulle.

Le logiciel doit insérer la valeur «zéro» en toute transparence dans tous les services qui requièrent la valeur «1» jusqu'à ce qu'un utilisateur la règle sur une valeur différente.

- L'interface SNCT doit prendre en charge un service Mot de passe qui utilise des paramètres à 2 mots de passe, à savoir les mots de passe anciens et les mots de passe nouveaux.
- L'interface SNCT doit fournir un service Réinitialisation de mot de passe qui utilise un champ spécifique au fournisseur pour réinitialiser le mot de passe.

Chaque fournisseur doit choisir une méthode de réinitialisation de mots de passe et indiquer à l'utilisateur les éléments à insérer pour que l'appareil réinitialise le mot de passe. Le logiciel doit insérer uniquement la valeur saisie par l'utilisateur dans le champ de réinitialisation (voir le service Reset_Password dans la définition de l'objet Programme de contrôle de sécurité en 6.5.3).

Les commandes du programme de contrôle de sécurité qui comportent un paramètre de mot de passe définissent les exigences de traitement et les réponses d'erreur associées à ces paramètres.

8.9.8 Services d'interface SNCT

Le SNCT doit fournir les services suivants:

- L'interface SNCT doit fournir un service Demande de configuration qui requiert l'exécution du mot de passe, du TUNID et de l'OUNID.
- Dans l'interface SNCT, un appareil sans propriétaire doit saisir l'OUNID comme propriétaire de l'appareil à la réception de la première Configure_Request.
- L'interface SNCT doit fournir un service Validation de Configuration qui requiert l'exécution du SCID, du SCCRC et de la SCTS.
- L'interface SNCT doit fournir un service Application qui conduit l'appareil à sauvegarder la configuration dans la mémoire NV.
- L'interface SNCT doit fournir un service Réinitialisation spécial qui requiert l'exécution du mot de passe et du TUNID, et qui prend en charge les 2 types de réinitialisation communs, ainsi qu'un type de réinitialisation qui peut revenir à la valeur par défaut tout en protégeant le mot de passe.
- L'interface SNCT définit un service Changement de mode facultatif qui, si mis en œuvre, doit requérir l'exécution d'un mot de passe.

8.9.9 Verrouillage de configuration

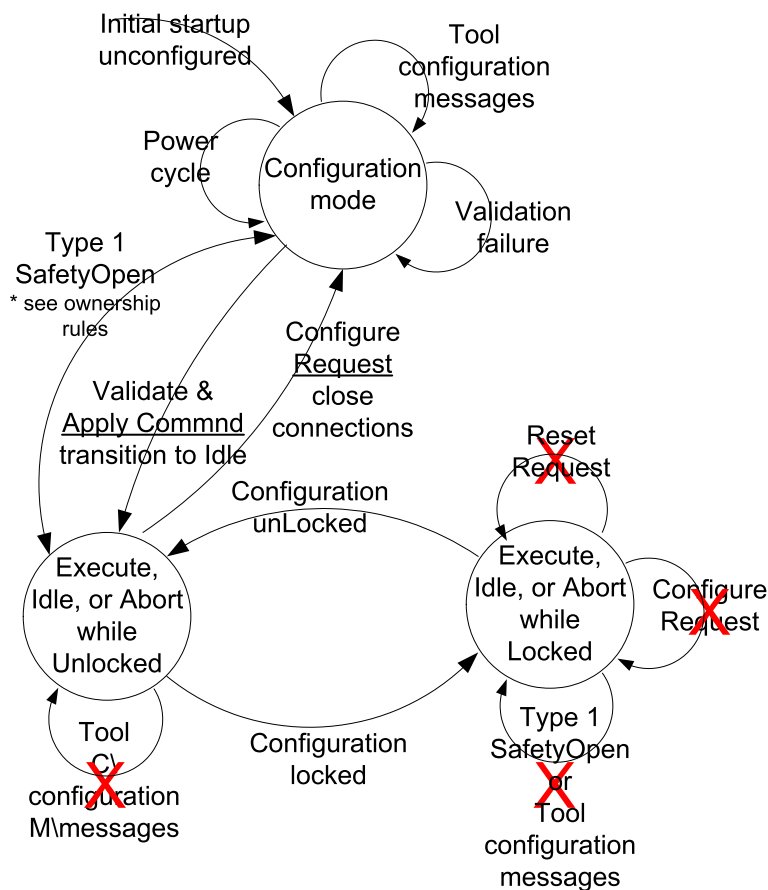
L'interface SNCT définit les fonctions suivantes pour le Verrouillage de configuration. Son objectif est de fournir une méthode de marquage par l'utilisateur qu'une configuration générée par outil a été soumise à essai et vérifiée comme valide. La signature (SCID) reflète en conséquence une configuration vérifiée. Le verrouillage de configuration a les caractéristiques suivantes.

- L'interface SNCT doit fournir un service Verrouillage de configuration qui requiert l'exécution du mot de passe et du TUNID.
- La valeur par défaut de l'attribut Verrouillage de configuration SNCT est «Non verrouillé».
- Les appareils de sécurité qui prennent en charge l'interface SNCT doivent exiger que l'attribut «Verrouillage de configuration» soit supprimé avant acceptation de toute commande de modification de l'état d'un appareil de sécurité à l'état de configuration (Configure_Request).
- Le verrouillage de configuration a un double objectif:
 - Indiquer que l'utilisateur a vérifié par essai et confirmé que la configuration par outil de cet appareil est correcte.
 - Exiger le mode «Outil uniquement». Une fois l'attribut Verrouillage de configuration défini, l'appareil doit refuser tous les messages SafetyOpen de forme 1.

Ces deux caractéristiques indiquent clairement que si le SNCT souhaite configurer tout nœud de sécurité, il doit prendre en charge les caractéristiques de définition et de suppression de l'attribut Verrouillage de configuration, et doit présenter le mot de passe approprié pour cette opération. Le diagramme séquentiel défini à la Figure 80 représente ces caractéristiques.

8.9.10 Influence du verrouillage de configuration sur le comportement des appareils

Figure 78 définit l'influence de la condition «configuration verrouillée» sur la capacité de configuration d'un appareil; l'objet Programme de contrôle de sécurité définit des exigences qui conduisent les appareils de sécurité à rejeter toutes les tentatives de modification d'une configuration verrouillée.



IEC

Anglais	Français
initial startup unconfigured	démarrage initial non configuré
tool configuration messages	messages de configuration par outil
power cycle	cycle d'alimentation
configuration mode	mode de configuration
validation failure	échec de validation
type 1 SafetyOpen	SafetyOpen de type 1
see ownership rules	voir règles de propriété
configure request	demande de configuration
close connections	connexions fermées
validate & apply command	commande de validation & application
transition to idle	transition vers Repos
reset request	demande de réinitialisation
configuration unlocked	configuration non verrouillée
execute, idle or abort while unlocked	exécution, repos ou abandon en déverrouillage
execute, idle or abort while locked	exécution, repos ou abandon en verrouillage
tool C\configuration M\messages	outil C configuration M\messages
configuration locked	configuration verrouillée
or tool configuration messages	ou messages de configuration par outil

Figure 78 – Relations entre configuration, essais et verrouillage

Le Tableau 106 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 forme 1, ladite configuration étant effectuée par le point d'origine ayant l'UNID du propriétaire. Un appareil verrouillé ne peut jamais être configuré sans tenir compte de son propriétaire.

Tableau 106 – Contrôle du propriétaire de configuration par rapport à l'état de l'appareil

Règles de propriété	Mode de configuration	Mode Exécution/Repos non verrouillé	Mode Exécution/Repos verrouillé
Configuration Sans propriétaire	Configuration par outil ou Acceptation de forme 1 par quiconque	Configuration par outil ou Acceptation de forme 1 par quiconque	Aucune configuration par outil, Aucune forme 1 acceptée
Point d'origine Avec propriétaire	Configuration par outil ou Forme 1 par le propriétaire uniquement	Aucune configuration par outil (doit réinitialiser au préalable) ou Forme 1 par le propriétaire uniquement	Aucune configuration par outil, Aucune forme 1 acceptée
Outil logiciel avec propriétaire	Configuration par outil uniquement Aucune forme 1 acceptée	Configuration par outil uniquement Aucune forme 1 acceptée	Aucune configuration par outil, Aucune forme 1 acceptée

8.9.11 Propriété de configuration

L'interface SNCT définit une fonctionnalité de traitement de l'identifiant de propriétaire de configuration pour un appareil. Cette fonction a été définie pour permettre à un appareil de fournir des droits de configuration exclusifs à une source de configuration particulière. La source peut également être attribuée exclusivement à un outil de configuration. Les fonctions suivantes sont fournies:

- Attribut UNID de configuration

La valeur par défaut est de permettre à tout appareil d'être propriétaire.

Les appareils doivent saisir la première source de configuration comme étant le propriétaire.

Les attributs et services du Programme de contrôle de sécurité sont définis de manière à permettre aux outils de constituer la source de configuration exclusive.

- L'outil SNCT a la capacité d'écraser une configuration même si un propriétaire a été attribué comme source de configuration. Le SNCT doit prévoir des mesures de protection qui permettent de s'assurer que l'utilisateur ne peut pas effectuer un écrasement sans avertissements et sans mot de passe correct.

8.9.12 Mode de configuration

Tous les appareils de sécurité doivent prendre en charge un mode de configuration non volatil; cela signifie que lorsqu'il est commandé à un appareil d'adopter le mode de configuration, il doit conserver ce mode jusqu'à la validation satisfaisante de la configuration.

8.9.13 Mesures d'assurance de l'intégrité du processus de configuration

8.9.13.1 Identifiant de configuration de sécurité (SCID)

Il est nécessaire d'identifier clairement la configuration des systèmes de sécurité. L'identification s'applique au cours de plusieurs opérations:

Téléchargement aval effectué par les outils – Ceci permet à l'utilisateur de vérifier que l'outil et l'appareil conviennent des informations téléchargées aval.

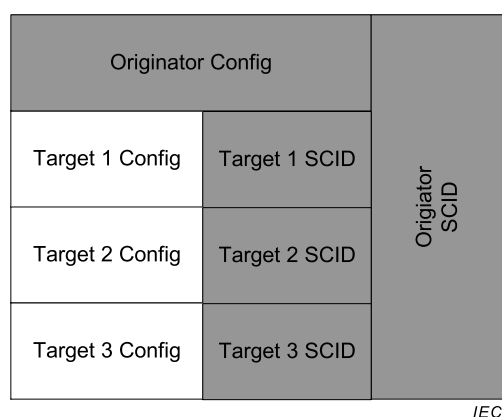
Remplacement des appareils – Si l'outil est utilisé pour le remplacement des appareils, l'utilisateur a la capacité de vérifier que la configuration est celle qui peut être téléchargée aval. Lorsque le point d'origine est utilisé pour une reconfiguration automatique d'un appareil, le SCID permet d'indiquer qu'une reconfiguration se révèle nécessaire et de s'assurer de l'intégrité de l'opération.

Établissement de connexion – Le point d'origine et la cible utilisent le SCID pour s'assurer que les deux appareils utilisent la même configuration.

Le SCID est une concaténation de la SCTS et du SCCRC décrits en 8.9.13.3 et 8.9.13.4 respectivement.

8.9.13.2 Couverture du SCID du point d'origine et de la cible

Lorsque les points d'origine permettent de configurer les cibles, la Figure 79 indique de quelle manière les SCID couvrent les différentes configurations. Le SCID des cibles configurées par les points d'origine n'est pas calculé par ces derniers; le calcul est effectué au poste de travail. Les configurations cibles sont protégées par leurs SCID respectifs.



Anglais	Français
originator config	configuration de point d'origine
target 1 config	config de cible 1
target 2 config	config de cible 2
target 3 config	config de cible 3
target 1 SCID	SCID de cible 1
target 2 SCID	SCID de cible 2
target 3 SCID	SCID de cible 3
originator SCID	SCID de point d'origine

Figure 79 – Données de configuration du point d'origine

8.9.13.3 CRC de configuration de sécurité (SCCRC)

Il s'agit d'un CRC couvrant les données de configuration d'appareil que comporte un service SafetyOpen. Il fait partie intégrante du SCID de l'appareil. Le SCCRC est décrit en 8.2.

La fonction de sécurité du SCCRC permet d'assurer le caractère approprié des données d'application relatives à la sécurité.

8.9.13.4 Datation de configuration de sécurité (SCTS)

Il s'agit d'une signature relative à la sécurité qui identifie la révision de la configuration d'appareil contenue dans un service SafetyOpen ou un appareil de sécurité. Elle fait partie intégrante du SCID de la configuration de l'appareil.

La fonction de sécurité de la SCTS permet d'assurer le caractère unique des données d'application relatives à la sécurité.

8.9.13.5 «Numéro de réseau de sécurité» unique pour l'ensemble du système (SNN)

Ce numéro identifie de manière unique un réseau parmi tous les réseaux du système de sécurité. L'utilisateur final est chargé d'attribuer un numéro unique à chaque réseau de sécurité ou sous-réseau de sécurité dans un système. Ce numéro doit être défini lors de la mise en service des nœuds (c'est-à-dire défini via le processus Propose_TUNID/Apply_TUNID explicité en 6.6.5.20 en cas de prise en charge de l'interface SNCT).

8.9.13.6 «Identifiant de nœud unique» pour l'ensemble du système (UNID)

Ce numéro identifie de manière unique un nœud parmi tous les réseaux du système de sécurité. Cette valeur est constituée du numéro de réseau de sécurité (SNN) et de l'adresse de nœud de l'appareil. Elle constitue ainsi une structure composée du SNN de 6 octets et de l'adresse de nœud de 4 octets. L'adresse de nœud de 4 octets est dimensionnée de façon à s'adapter à toutes les formes d'adresses de réseau CPF 2.

```
struct UNID
{
    DATE_AND_TIME    SNN;
    UDINT            NodeID;
};
```

Les NodeID de moins de 4 octets (c'est-à-dire CP 2/3) doivent être alignés sur l'octet de poids faible dans l'ordre petit-boutiste. Les octets non utilisés doivent être remplis de zéros.

La fonction de sécurité de l'UNID permet d'identifier de manière unique les points d'origine et/ou les cibles au cours du processus d'établissement de connexion.

Autres utilisations de l'UNID:

- TUNID = Identifiant de réseau unique de la cible. La fonction de sécurité du TUNID consiste à identifier la cible dans le service SafetyOpen et le message de mode de configuration.
- OUNID = Identifiant de réseau unique du point d'origine. La fonction de sécurité de l'OUNID consiste à identifier le point d'origine dans le service SafetyOpen.
- OCPUNID = UNID de propriété de point de connexion de sortie. La fonction de sécurité de l'OCPUNID consiste à identifier le propriétaire de la connexion de sortie dans la cible. Réglé sur l'OUNID du point d'origine dans le service safetyOpen qui obtient la propriété du point de connexion de sortie. Utilisé pour empêcher un d'origine non autorisé d'obtenir la propriété d'un point de connexion de sortie.
- CFUNID = UNID de propriété de configuration. La fonction de sécurité du CFUNID consiste à identifier le propriétaire de la configuration de sécurité dans la cible; il convient que ceci soit équivalent à l'OUNID en fonctionnement normal. Réglé sur l'OUNID du point d'origine dans le service SafetyOpen qui inclut les données de configuration et permet d'empêcher un point d'origine non autorisé de modifier la configuration.

8.9.13.7 CRC des paramètres de connexion (CPCRC)

CRC relatif à la sécurité couvrant les données d'établissement de connexion CPF 2 dans le service SafetyOpen. Ce CRC couvre également les paramètres supplémentaires exigés par le protocole de sécurité. Le CRC est défini en 7.1.2.3.

La fonction de sécurité du CPCRC consiste à assurer l'intégrité des données de connexion contenues dans le service SafetyOpen.

8.9.14 Processus de téléchargement aval

8.9.14.1 Présentation générale

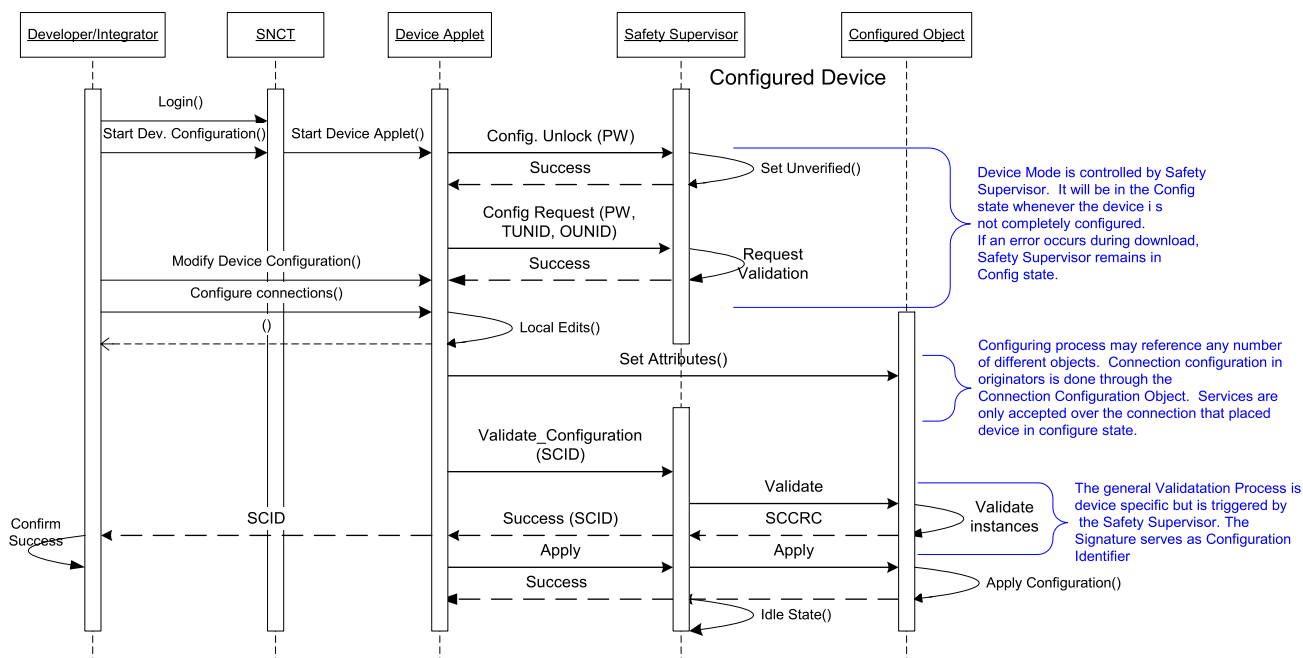
Le processus de téléchargement aval de sécurité assure que les données de configuration sont transférées avec une haute intégrité du SNCT ou du point d'origine vers l'appareil configuré. La configuration est considérée valide si le processus de téléchargement aval est effectué de manière satisfaisante. Deux processus de téléchargement aval sont utilisés avec les appareils de sécurité:

- téléchargements aval SNCT vers les points d'origine et les cibles;
- téléchargements aval des points d'origine vers les cibles utilisant un service SafetyOpen de forme 1.

Les paragraphes suivants décrivent les détails des processus de téléchargement aval des appareils de sécurité.

8.9.14.2 Téléchargement aval SNCT vers les points d'origine et les cibles

La Figure 80 représente le processus de téléchargement aval d'un appareil de sécurité à partir du SNCT. Le processus de téléchargement aval entre le SNCT et l'appareil configuré assure l'instanciation des données dans la mémoire de l'appareil configuré avec une haute intégrité.



IEC

Anglais	Français
developer/integrator	développeur/intégrateur

Anglais	Français
device applet	applet d'appareil
safety supervisor	programme de contrôle de sécurité
configured object	objet configuré
configured device	appareil configuré
start dev. configuration	démarrage de configuration d'appareil
start device applet	démarrage d'applet d'appareil
config. unlock	config. non verrouillée
success	réussite
set unverified	réglé à non vérifié
config request	demande de configuration
modify device configuration	modification de configuration d'appareil
request validation	demande de validation
configure connections	configuration des connexions
local edits	éditions locales
set attributes	régler les attributs
validate	validation
confirm success	confirmation de réussite
apply	application
validate instances	validation des instances
apply configuration	application de configuration
idle state	état Repos
device mode is controlled by Safety Supervisor. It will be in the Config state whenever the device is not completely configured. If an error occurs during download, Safety Supervisor remains in config state	le mode d'appareil est contrôlé par le programme de contrôle de sécurité. Il est à l'état Config. lorsque l'appareil n'est pas complètement configuré. En cas d'erreur au cours du téléchargement aval, le programme de contrôle de sécurité reste à l'état Config.
Configuring process may reference any number of different objects. Connection configuration in originators is done through the Connection Configuration Object. Services are only accepted over the connection that placed device in configure state	le processus de configuration peut référencer n'importe quel nombre d'objets différents. La configuration de connexion dans les points d'origine est réalisée par l'objet Configuration de connexion. Les services ne sont acceptés que sur la connexion qui a placé l'appareil à l'état Configuration
The general validation process is device specific but is triggered by the Safety Supervisor. The Signature serves as Configuration identifier	le processus général de validation est spécifique à l'appareil, mais est déclenché par le programme de contrôle de sécurité. La signature est utilisée comme identifiant de configuration

Figure 80 – Processus de téléchargement aval du SNCT à l'appareil

8.9.14.3 Etapes du processus de téléchargement aval du SNCT à l'appareil

Les étapes de processus suivantes représentent les étapes du processus de téléchargement aval du SNCT à l'appareil, tel que représenté à la Figure 80.

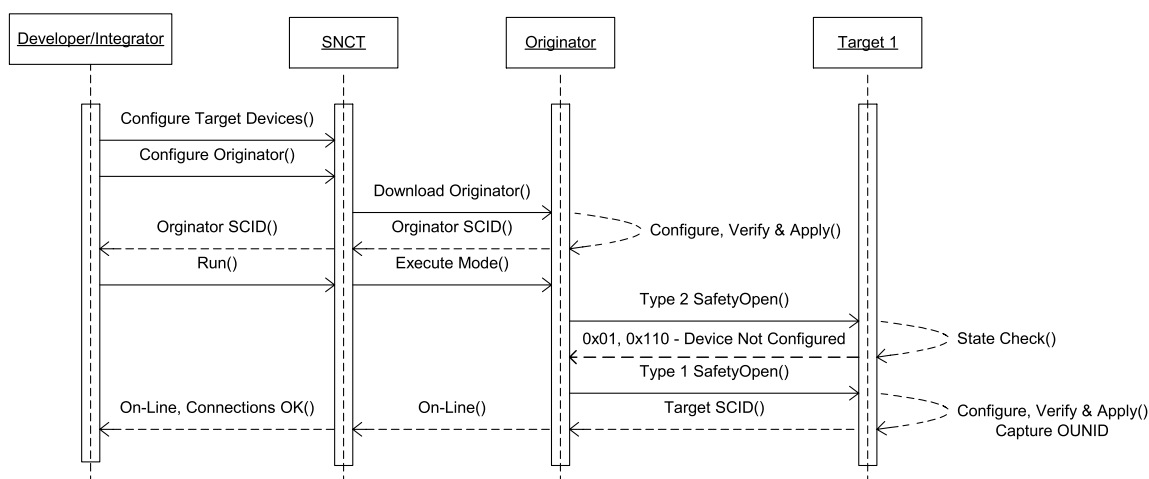
- a) Supprimer l'attribut Verrouillage de configuration
 - i) Appareil: Attribut Verrouillage de configuration supprimé
- b) Saisir l'état de configuration avec mot de passe, TUNID, OUNID
 - i) Appareil: Aucune connexion E/S de sécurité ne peut être active.
 - ii) Appareil: L'appareil sauvegarde le mode de Configuration dans la mémoire NV
 - A) Jusqu'aux étapes «Validation» et «Application», les cycles d'alimentation reviennent au mode de configuration
- c) Transfert des données de configuration

- i) Outil: Calculer le «SCCRC proposé» pour les données (partie SCCRC du SCID)
 - ii) Appareil: Les messages explicites sont autorisés à définir la configuration de l'appareil, mais ce dernier doit accepter uniquement les messages explicites relatifs à la sécurité sur la connexion qui le place en mode de configuration.
- d) Validation des données de configuration
- i) Outil: Transmettre Validate_Request avec le SCID (qui contient le SCCRC proposé)
 - ii) Appareil: Analyser les données de configuration
 - iii) Appareil: Calcule la valeur SCCRC et la compare au «SCCRC proposé»
 - iv) Appareil: Transmettre le SCID dans Validate_Reply
 - v) Outil: Compare le SCCRC renvoyé au «SCCRC proposé»
- e) Appliquer la configuration
- i) Appareil: Sauvegarder la configuration dans la mémoire NV avec le SCID
 - ii) Appareil: Marquer la configuration comme valide
 - iii) Appareil: Régler le mode sur Repos
 - iv) Outil: Saisir et archiver le SCID avec le fichier de configuration.

8.9.14.4 Téléchargements aval du SNCT vers les points d'origine qui réalisent la configuration cible de forme 1

La Figure 81 présente le processus de configuration initiale des points d'origine, ainsi que la méthode d'utilisation du service SafetyOpen de forme 1 pour le téléchargement aval des appareils cibles. Une fois les configurations d'origine et de cible définies dans le SNCT par l'utilisateur, elles sont transmises au point d'origine. Le SCID de point d'origine peut alors être confirmé par l'utilisateur. Ce processus permet de s'assurer que les données de configuration dans le SNCT et le point d'origine correspondent avec un degré d'intégrité élevé.

L'utilisateur doit alors placer le point d'origine en mode d'exécution pour obtenir le téléchargement aval des appareils cibles. Si la connexion est satisfaisante, la configuration cible/le SCID ont été acceptés par la cible et confirmés par le point d'origine. Cette action a également établi le point d'origine comme étant le propriétaire de la cible et empêche le téléchargement aval de la cible par tout autre appareil que le SNCT.



IEC

Anglais	Français
developer/integrator	développeur/intégrateur
originator	point d'origine

Anglais	Français
target	cible
configure target devices	configuration des appareils cibles
configure originator	configuration du point d'origine
originator SCID	SCID de point d'origine
download originator	téléchargement aval du point d'origine
configure, verify & apply	configuration, vérification & application
run	exécution
execute mode	mode d'exécution
type 2 safetyopen	SafetyOpen de type 2
device not configured	appareil non configuré
state check	vérification d'état
type 1 SafetyOpen	SafetyOpen de type 1
on-line connections OK	connexions en ligne OK
on-line	en ligne
target SCID	SCID de cible
capture OUNID	saisir l'OUNID

Figure 81 – Téléchargements aval du SNCT vers les points d'origine qui réalisent la configuration de forme 1

8.9.14.5 Téléchargements aval du SNCT vers les points d'origine qui réalisent la configuration de forme 1

Les étapes de processus suivantes représentent les étapes du processus de téléchargements aval du SNCT vers les points d'origine qui réalisent la configuration de forme 1, tel que représenté à la Figure 81.

- a) Supprimer l'attribut Verrouillage de configuration sur le point d'origine
 - i) Appareil: Attribut Verrouillage de configuration supprimé
- b) Saisir l'état de configuration avec mot de passe, TUNID, OUNID
 - i) Appareil: Aucune connexion E/S de sécurité ne peut être active.
 - ii) Appareil: L'appareil sauvegarde le mode Configuration dans la mémoire NV
 - iii) Jusqu'aux étapes «Validation» et «Application», les cycles d'alimentation reviennent au mode de Configuration
- c) Transfert des données de configuration
 - i) Outil: Calculer le «SCCRC proposé» pour les données (partie SCCRC du SCID)
 - ii) Outil: Les messages explicites sont autorisés à définir la configuration de l'appareil, mais ce dernier doit accepter uniquement les messages explicites relatifs sur la connexion qui le place en mode de configuration.
- d) Validation des données de configuration
 - i) Outil: Transmettre Validate_Request avec le SCID (qui contient le SCCRC proposé)
 - ii) Appareil: Analyser les données de configuration
 - iii) Appareil: Calcule la valeur SCCRC et la compare au «SCCRC proposé»
 - iv) Appareil: Transmettre le SCID dans Validate_Reply
 - v) Outil: Compare le SCCRC renvoyé au «SCCRC proposé»
- e) Appliquer la configuration
 - i) Appareil: Sauvegarder la configuration dans la mémoire NV avec le SCID

- ii) Appareil: Marquer la configuration comme valide
- iii) Appareil: Régler le mode sur Repos
- iv) Outil: Saisir et archiver le SCID avec le fichier de configuration.
- f) Régler le mode sur «Exécution»
 - i) Point d'origine: Transmet les services SafetyOpen de forme 2 (voir 8.8.5)
 - ii) la cible renvoie l'une des erreurs suivantes:
 - A) Non configuré: 01_{hex}, 0110_{hex} – Appareil non configuré
 - B) Avant configuration: 01_{hex}, 80C_{hex} – erreur de défaut d'adaptation SCID
 - iii) Point d'origine: Transmet un service SafetyOpen de forme 1
 - iv) Cibles: Vérifier et appliquer les données de configuration
 - v) Cibles: Renvoient le # SCID de cible aux points d'origine
 - vi) Point d'origine: Compare les # SCIS transmis et reçus
 - vii) Point d'origine: Renvoie l'état en ligne au SNCT

8.9.15 Processus de vérification

8.9.15.1 Présentation générale du processus de vérification

Le processus de vérification utilise les données transférées au cours des processus de téléchargement aval afin de permettre à l'utilisateur de vérifier de manière appropriée le caractère correct des données téléchargées ainsi que du fonctionnement du système, et de s'assurer que le système est prêt pour un fonctionnement SIL 3. Le processus de configuration comprend trois parties principales:

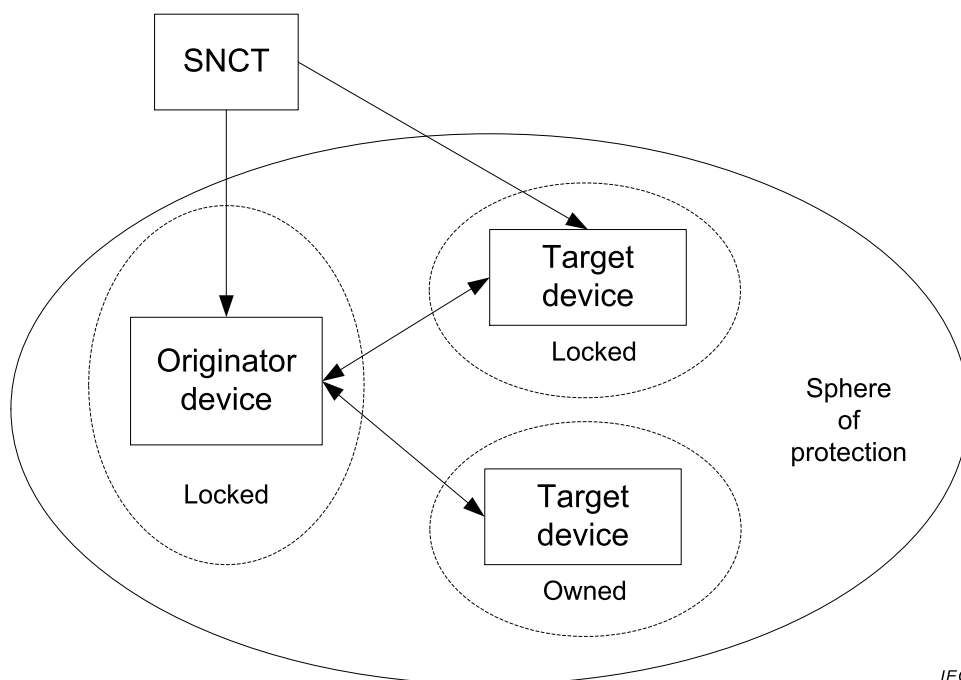
- vérification des données de configuration;
- essais de fonctionnement;
- verrouillage de configuration.

Exigences essentielles applicables au manuel de sécurité:

- Le manuel de sécurité des appareils doit contenir des recommandations spécifiant que les essais utilisateur constituent le moyen de validation de tous les téléchargements aval;
- Ce manuel doit contenir par ailleurs des recommandations spécifiant qu'il convient de considérer uniquement la signature comme «vérifiée» (et la configuration verrouillée) après les essais utilisateur.

Le manuel utilisateur des appareils doit contenir également des recommandations spécifiant que la configuration d'un point d'origine comportant des données de connexion et/ou de configuration de cible doit être téléchargée vers la cible de manière à pouvoir être soumise à essai et vérifiée. Les SCID provenant de la cible peuvent être confirmés uniquement à partir de cette étape.

Comme le représente la Figure 82, lorsque les points d'origine sont configurés par outil et les cibles sont configurées par le point d'origine, seul ce dernier est «verrouillé» après vérification et essais. La cible utilise dans ce cas les attributions de propriété à des fins de protection. La Figure 82 indique également que les cibles peuvent être configurées aussi par outil. Dans ce cas, ces cibles sont également «verrouillées» après vérification et essais.



IEC

Anglais	Français
target device	appareil cible
originator device	appareil d'origine
locked	verrouillé
sphere of protection	zone de protection
owned	avec propriétaire

Figure 82 – Protection contre le verrouillage et propriété

8.9.15.2 Vérification de la configuration par l'utilisateur et méthodes alternatives

8.9.15.2.1 Présentation générale

L'utilisateur a besoin de vérifier par examen visuel que la configuration téléchargée est correcte et constitue la configuration prévue pour l'appareil. Le présent paragraphe 8.9.15.2 présente quatre méthodes alternatives qui satisfont aux exigences relatives à la vérification par l'utilisateur des données de configuration des appareils. L'utilisateur a besoin, dans tous les cas, de vérifier la fonctionnalité des appareils configurés par un certain type d'essai de fonctionnement.

Une option ou une combinaison des options suivantes peut être appliquée pour satisfaire à l'exigence de vérification par l'utilisateur: comparaison par l'utilisateur de l'affichage logiciel d'origine et résultats de la relecture affichés par un appareil tiers.

8.9.15.2.2 Alternative 1 – relecture immédiate et comparaison diverse

Le poste de travail effectue la relecture des données de configuration des appareils et les présente à l'utilisateur qui emploie un chemin d'exécution divers dans le poste de travail, tel que représenté à la Figure 83.

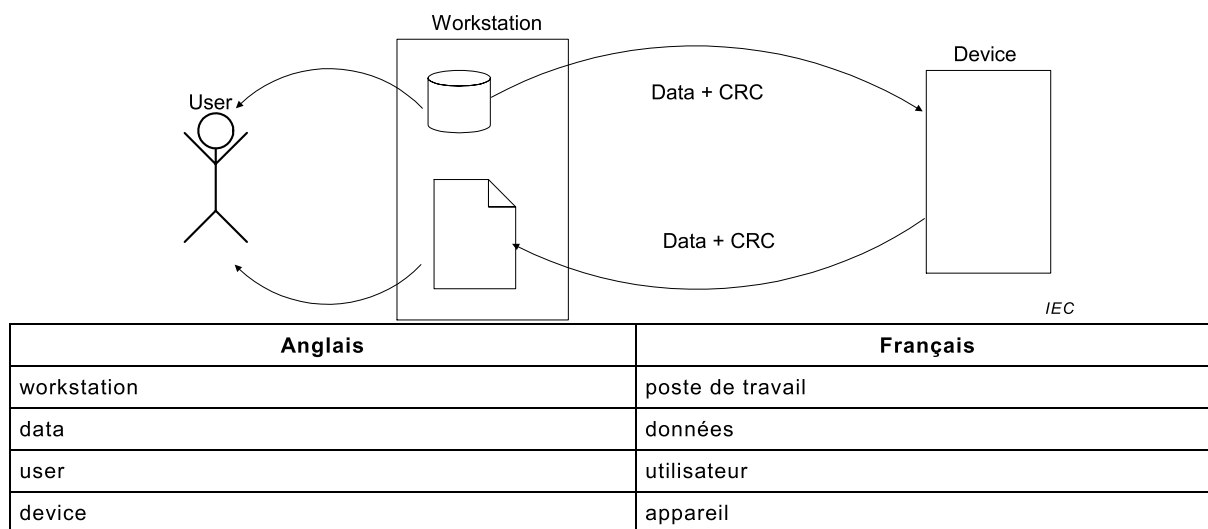


Figure 83 – Exemple de relecture et de comparaison du point d'origine et de l'exemplaire

Relecture de la configuration entière, comparaison de cette dernière avec les éléments d'affichage du logiciel et fourniture d'un exemplaire de la configuration des appareils afin que l'utilisateur le compare avec la configuration précédemment saisie. L'utilisateur doit examiner et comparer l'exemplaire avec les données d'origine afin de satisfaire aux exigences d'intégrité. Toute comparaison automatisée par les outils logiciels constitue un diagnostic, mais ne doit aucunement représenter une source fiable qui permet d'assurer l'intégrité.

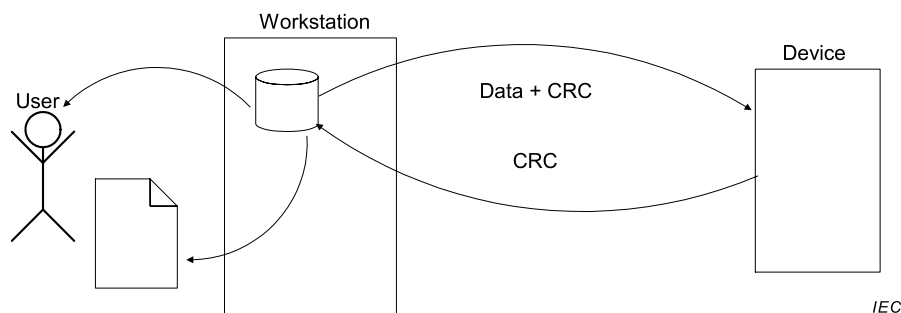
La relecture et l'affichage par un appareil tiers réduisent la possibilité d'une erreur systématique du poste de travail, occasionnant la même corruption de données à la saisie de ces dernières et une vérification par l'utilisateur, susceptible d'occasionner une erreur non détectée. Si, par exemple, une corruption s'est produite avant la génération du CRC, l'appareil interprète les données comme étant correctes, les mêmes données et CRC étant retransmis au poste de travail. Les contrôles automatisés des données d'origine et relues n'indiquent pas d'erreur dans la mesure où les données correspondent au CRC. Si l'affichage des données utilisait le même mécanisme que le mécanisme d'affichage d'origine, l'erreur pourrait toujours être masquée et ne pas être détectée. Il convient que les chemins d'affichage divers réduisent cette cause d'erreur commune.

8.9.15.2.3 Alternative 2 – affichage divers local

L'obtention du même niveau d'intégrité défini en 8.9.15.2.2 est possible dans la mesure où il peut être démontré que les données de configuration archivées dans la mémoire du poste de travail sont identiques aux données de configuration de l'appareil. La saisie des données de configuration et du CRC sur le pilote local du poste de travail permet de vérifier les données de configuration. Les données de configuration et le CRC du pilote local sont ensuite transmis à l'appareil. Ce dernier vérifie alors le bon déroulement du transfert par une comparaison des données et du CRC. Lorsque le transfert vers l'appareil est correct, ce dernier renvoie son CRC calculé au poste de travail afin de confirmer la transmission correcte des données. Le poste de travail compare alors le CRC de l'appareil au CRC archivé. La transmission correcte à l'appareil des données du poste de travail peut être supposée à cet instant. Il est important que le CRC soit calculé uniquement une seule fois par le poste de travail et archivé sur le pilote local. Il n'est pas recalculé à des fins de transferts. Ceci garantit également l'intégrité des données sur le pilote local. La transmission correcte à l'appareil des données du poste de travail peut être supposée à cet instant.

L'utilisateur doit, à des fins de vérification, observer les données de configuration «transmises» au moyen d'un appareil tiers afin de confirmer que la configuration correcte a été transmise à l'appareil. Dans la mesure où les données archivées dans la mémoire du poste de travail comportent un CRC, un appareil tiers d'affichage permet à l'utilisateur de

détecter les erreurs potentielles occasionnées par le poste de travail au moment de l'archivage des données. Cette opération duplique effectivement la fonctionnalité de la méthode intégrale de relecture sans les surcharges liées à la réalisation d'une relecture complète des données entre l'appareil et le poste de travail. La Figure 84 représente ce processus de manière graphique.

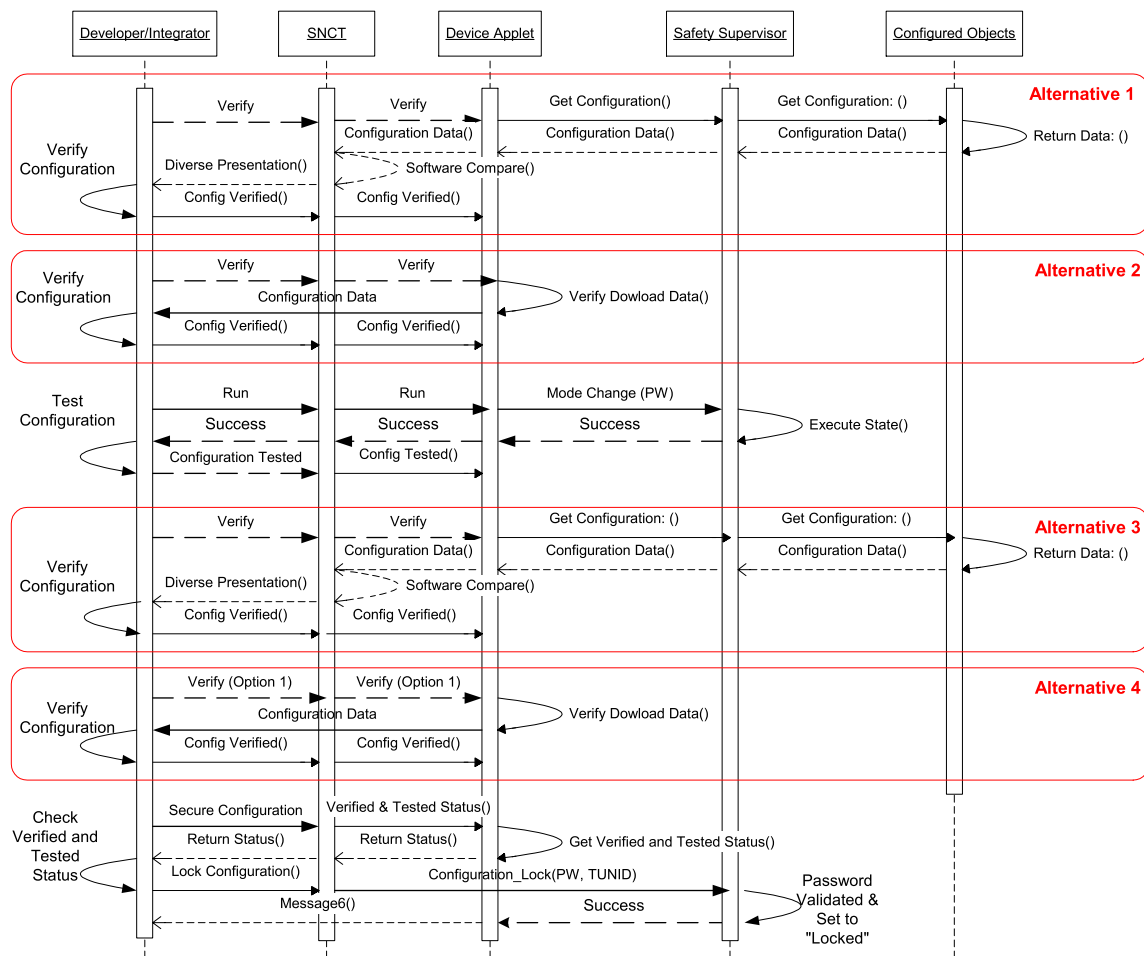


Anglais	Français
workstation	poste de travail
data	données
User	utilisateur
Device	appareil

Figure 84 – Affichage divers sans relecture complète des données

8.9.16 Processus de vérification

La Figure 85 définit le processus complet de vérification de la configuration des appareils de sécurité. Il est supposé que le téléchargement aval des données a été effectué par le processus décrit en 8.9.14, en s'assurant que le SNCT et l'appareil ont les mêmes données de configuration. Une méthode alternative doit être sélectionnée pour la vérification des données de configuration par l'utilisateur. Les appareils et le système sont prêts pour un fonctionnement de niveau SIL 3 une fois ce processus accompli.



IEC

Anglais	Français
developer/integrator	développeur/intégrateur
device applet	applet d'appareil
safety supervisor	programme de contrôle de sécurité
configured objects	objets configurés
verify	vérification
get configuration	obtenir configuration
verify configuration	vérification de la configuration
diverse presentation	présentation diverse
configuration data	données de configuration
return data	données de retour
software compare	comparaison par logiciel
config verified	config. vérifiée
verify download data	vérification des données téléchargées
test configuration	essai de la configuration
run	exécution
mode change	changement de mode
success	réussite
execute state	état d'exécution
check verified and tested status	contrôle de l'état vérifié et soumis à essai

Anglais	Français
secure configuration	sécurisation de la configuration
verified & tested status	état vérifié & soumis à essai
return status	état de retour
get verified and tested status	obtenir état vérifié et soumis à essai
lock configuration	verrouillage de la configuration
password validated & set to "locked"	mot de passe validé & réglé à "verrouillé"

Figure 85 – Processus de vérification comprenant toutes les méthodes alternatives

8.9.17 Analyse des erreurs de configuration

8.9.17.1 Relations entre erreurs de configuration et mesures de détection

Le Tableau 107 définit les erreurs et les mesures de détection prises en compte pour le processus de téléchargement aval et de configuration défini par l'interface SNCT.

Tableau 107 – Erreurs et mesures de détection

Erreurs	Mesures de détection							
	Authentification	Identification	Identification	Protection	Verrouillage	Contrôle	Essais de fonction	Relecture de
Configuration mal acheminée par l'utilisateur	X				X		X	
Configuration mal acheminée par le système	X		X		X		X	X
Message de configuration perdu				X			X	X
Configuration corrompue				X			X	X
Configuration au moment inapproprié						X		
Configuration erronée chargée par l'utilisateur		X					X	X
Interruption du processus de configuration						X		
^a L'authentification de l'utilisateur est une caractéristique facultative qui s'applique uniquement si l'utilisateur final en fait usage.								

8.9.17.2 Erreurs de configuration

8.9.17.2.1 Configuration mal acheminée par l'utilisateur

L'utilisateur doit soumettre à un essai de fonctionnement les appareils configurés, un mauvais acheminement par l'utilisateur pouvant ainsi être décelé au cours de l'essai.

Si l'utilisateur configure un nœud de manière intempestive sans que cela soit remarqué, le point d'origine qui se connecte au nœud ne comporte pas la signature d'adaptation et reconfigure alors l'appareil avec la bonne signature ou refuse la connexion. L'une ou l'autre de ces deux actions entraîne le passage du système vers un état de sécurité.

Si l'utilisateur final active les caractéristiques d'authentification, les utilisateurs ne peuvent pas configurer les nœuds pour lesquels ils n'ont pas d'autorisation. L'authentification de l'utilisateur est une caractéristique facultative.

8.9.17.2.2 Configuration mal acheminée par le système

Il existe deux cas différents de mauvais acheminement d'une configuration par un système. configuration exécutée lors de l'établissement d'une connexion par un service SafetyOpen de forme 1, et configuration à partir d'un poste de travail ou un processus de configuration O-à-T. Les alinéas suivants explicitent ces deux cas.

- Si une erreur d'acheminement se produit lors de l'établissement d'une session de configuration, l'appareil rejette le message de mode de configuration en raison du TUNID ou de l'OUNID erroné du message de mode.
- Si un message de configuration est mal acheminé dans une session de configuration, il est refusé par l'appareil de réception si le mode de ce dernier n'est pas correct ou s'il est reçu sur une connexion autre que la connexion qui permet d'établir le mode de configuration. Si l'appareil est en mode correct, le message de configuration devrait être adressé vers la classe, l'instance et l'attribut corrects à accepter, et serait détecté au cours des étapes de validation du SCID. L'appareil supposé avoir correctement reçu le message de configuration ne satisfait également pas à la validation du SCID. L'utilisateur détecte également cet état de fait au cours du contrôle de la relecture de configuration de l'appareil.

8.9.17.2.3 Message de configuration perdu

Les détections d'un message perdu sont identiques à celles d'un message mal acheminé.

8.9.17.2.4 Corruption de la configuration

En cas de corruption de la configuration pour quelque raison que ce soit, cette dernière est détectée par les contrôles SCID, les essais de fonctionnement de l'utilisateur et l'examen de la configuration par l'utilisateur.

8.9.17.2.5 Configuration au moment inapproprié

L'authentification de l'utilisateur et le paramétrage du mode de configuration empêchent toute configuration des appareils d'exploitation. Si un utilisateur tente de configurer un appareil pour lequel il n'a pas l'autorisation, la demande de mode est refusée. Si l'utilisateur transmet les messages de configuration à un appareil sans que le mode de configuration ne soit défini, l'appareil refuse les modifications.

8.9.17.2.6 Configuration erronée chargée par l'utilisateur

Chaque configuration est identifiée de manière unique par le SCID. Les utilisateurs doivent mettre en œuvre des procédures de vérification du caractère approprié de la configuration chargée pour l'application concernée.

8.9.17.2.7 Interruption du processus de configuration

En cas d'interruption du processus de configuration pour quelque raison que ce soit, l'appareil reste en mode configuration jusqu'au chargement d'une configuration valide et à la modification du mode.

En cas d'interruption du processus de configuration, il est nécessaire que ce dernier soit réamorcé dans le cas d'une nouvelle connexion avec une nouvelle demande de configuration.

8.9.17.3 Mesures de détection

8.9.17.3.1 Authentification de l'utilisateur

Tous les appareils de sécurité comportent une protection par mot de passe facultative. Les commandes Verrouillage de configuration, Demande de configuration, Changement de mode et Réinitialisation exigent toutes l'utilisation d'un mot de passe pour modifier l'état.

8.9.17.3.2 Identification du fichier de configuration

Tous les fichiers de configuration de sécurité sont identifiés de manière unique par le SCID.

8.9.17.3.3 Identification de la cible à configurer

Le message de mode de configuration et le message de vérification utilisent tous deux le TUNID pour identifier la cible.

8.9.17.3.4 Protection du CRC lors de la configuration

Le SCCRC fait partie intégrante du SCID. Le SCCRC est un CRC de 32 bits calculé avec les données de configuration de sécurité.

8.9.17.3.5 Propriété de configuration

Lorsqu'un appareil cible à l'état out-of-box est configuré par un point d'origine, il saisit l'OUNID et empêche ensuite sa configuration par tout autre pont d'origine. Ainsi, l'attribution de propriété (OUNID) fournit un moyen de verrouillage de cet appareil sur une source de configuration unique.

8.9.17.3.6 Contrôle de session de configuration

Un appareil doit être placé en mode de configuration avant d'être configuré. Le mode de configuration est persistant dans l'appareil et le reste jusqu'à ce que l'appareil soit réglé sur un autre mode par une commande. Le mode configuration des appareils de sécurité qui mettent en œuvre l'interface SNCT doit persister tout au long des cycles d'alimentation.

Lorsqu'ils adoptent le mode de configuration, les appareils qui mettent en œuvre l'interface SNCT doivent:

- archiver le mode de configuration dans la mémoire NV;
- marquer la configuration existante comme invalide;
- verrouiller tous les messages de configuration pour les connexions autres que celle qui définit le mode de configuration;

Pour adopter le mode de configuration, les appareils qui mettent en œuvre l'interface SNCT doivent:

- confirmer le mot de passe utilisateur dans la commande de mode de configuration;
- confirmer le TUNID dans la commande de mode de configuration.

8.9.17.3.7 Essais de fonctionnement par l'utilisateur

L'utilisateur doit soumettre à des essais de fonctionnement les appareils nouveaux et de remplacement avant d'utiliser le système dans un environnement SIL3.

8.9.17.3.8 Protection de la configuration

Tous les appareils configurés par outil sont verrouillés après réalisation de la configuration, des essais et de la vérification par l'utilisateur selon l'une des procédures définies en 8.9.16. Ces appareils sont les cibles, les points d'origine ou les deux à la fois. Cet état de verrouillage peut être lu de manière à indiquer la vérification de la configuration, et protège également le système contre les modifications de configuration intempestives, en exigeant de l'utilisateur qu'il déverrouille en premier lieu l'appareil.

Les essais par l'utilisateur attribuent un propriétaire aux appareils cibles configurés par le point d'origine, cette attribution rattache ces appareils à leurs propriétaires et verrouille effectivement ces appareils contre toute configuration intempestive par une autre source. Comme le représente la Figure 82, la combinaison des points d'origine configurés par outil et

verrouillés et des cibles avec propriétaire offre un environnement sécurisé qui protège le système vérifié contre les modifications non autorisées.

8.9.17.3.9 Protections par logiciel de diagnostic (non relatives à la sécurité)

Le logiciel peut également mettre en œuvre des mesures de protection des données de configuration de l'appareil comme mesure d'intégrité des données, et à destination du mécanisme de détection précoce des erreurs. Il est important de comprendre qu'il ne s'agit pas de mesures relatives à la sécurité, et qu'il n'est pas nécessaire que ces mesures atteignent un niveau SIL3 ou qu'elles soient évaluées. Les domaines concernés sont définis ici:

L'archivage des données de configuration sur disque dur, CD, etc. doit inclure le SCID et être vérifié lors du chargement d'un fichier.

Le transfert des données de configuration sur les interfaces logicielles doit inclure le SCID et être vérifié par la composante logicielle de réception.

8.9.17.4 Considérations portant sur l'architecture de la mémoire des appareils

Il est important de comprendre l'architecture de la mémoire que les appareils cibles pourraient utiliser afin de connaître son comportement potentiel lors de la configuration. Toutes ces architectures sont prises en charge par cette partie, mais modifient le comportement pour l'utilisateur.

Trois domaines de données distincts sont définis eu égard à la configuration:

- copie archivée dans la mémoire NV – configuration valide archivée dans la mémoire non volatile et utilisée pour la configuration d'un appareil de sécurité lors de sa mise sous tension;
- copie de mémoire vive (RAM) de travail – configuration valide qui constitue une copie fidèle de la configuration dans la mémoire NV, mais qui est utilisée lors de l'exécution;
- copie de mémoire vive (RAM) modifiable – espace de données pouvant être modifié par le logiciel en mode de configuration, mais qu'il faut toutefois appliquer;

Les développeurs de produits peuvent choisir de mettre en œuvre un domaine de données ou plus afin de renforcer la flexibilité de l'utilisateur.

Copie mémoire NV uniquement – Cette approche de conception conserve la configuration uniquement dans la mémoire NV. Lorsque le système est en mode de configuration, la configuration complète est invalidée, et toute restauration de la configuration est impossible. Le logiciel doit télécharger de manière satisfaisante une configuration complète et valide dans l'appareil. Une fois que la copie NV est validée et appliquée, elle est marquée comme «correcte». Ce type d'appareil ne prend pas en charge la commande de restauration.

Copie de mémoire NV et de mémoire de travail – Cette approche de conception conserve la configuration dans la mémoire NV et une copie de travail dans la mémoire vive. Lorsque l'appareil adopte l'état de configuration, la copie de travail est modifiée, mais jusqu'à validation et application de la configuration, l'ancienne configuration valide peut toujours être restaurée. Un cycle d'alimentation préalable à la phase Application retournerait à la dernière configuration dans la mémoire NV. La commande de restauration est prise en charge et recopie la version NV dans la mémoire vive de travail.

Copie de mémoire NV et copie de mémoire de travail avec mémoires tampons d'édition – cette approche de conception conserve une configuration de travail valide permanente jusqu'à l'exécution d'une phase «validation et application». Si l'appareil de configuration quitte l'état de configuration sans appliquer les modifications, la commande de restauration permet à l'appareil de quitter simplement l'état de configuration et de fonctionner avec les

données contenues dans la mémoire. La commande de restauration est prise en charge, aucune copie de la mémoire vive NV n'est nécessaire, et la copie de travail peut être utilisée.

8.10 Extensions de fiches techniques électroniques à des fins de sécurité

8.10.1 Règles générales applicables aux appareils de sécurité EDS

8.10.1.1 Généralités

La structure et les règles applicables aux EDS sont définies dans l'ISO 15745–3:2003, Annexe A et l'ISO 15745–4:2003, Annexe C. Les extensions de sécurité sont définies dans les paragraphes suivants.

8.10.1.2 Définition d'un ensemble de configuration de sécurité

Les appareils de sécurité peuvent être configurés à partir de la définition d'un fichier EDS. Les appareils de sécurité configurés via un fichier EDS doivent définir un Ensemble de configuration de sorte que le logiciel sache comment calculer le SCID. Une section d'ensemble EDS normalisé doit permettre de définir les différents paramètres contenus dans l'Ensemble de configuration de sécurité. Un champ et un mot clé ont été définis dans la section [Classe de paramètre] pour identifier l'Id instance de l'ensemble. Une entrée Gestionnaire de connexion doit également être utilisée pour référencer cet ensemble s'il doit être configurable avec un service SafetyOpen de forme 1.

8.10.1.3 CRC de configuration

Les appareils de sécurité SNCT et EDS doivent utiliser la même méthode de calcul du SCCRC. Les appareils de sécurité EDS doivent utiliser CRC-S4 avec la valeur de départ définie en 7.1.2.3. L'entrée de données de l'algorithme CRC est définie par l'Ensemble de configuration. Tout remplissage de l'ensemble de configuration est supposé être nul à des fins de calcul du SCCRC.

8.10.1.4 Cryptage du mot de passe pour les appareils EDS

Le SNCT et tout autre logiciel de configuration qui mettent en œuvre l'interface SNCT doivent disposer d'une méthode normalisée de cryptage des mots de passe appliquée préalablement à leur présentation à un appareil de sécurité. Les outils logiciels qui mettent en œuvre l'interface SNCT doivent utiliser CRC-S4 avec la valeur de départ définie en 7.1.2.3.

Lorsqu'un mot de passe crypté est plus petit que le paramètre de mot de passe à taille fixe, la méthode décrite dans le cadre du service Set_Password inclus dans la définition de l'objet Programme de contrôle de sécurité doit être employée.

8.10.2 Extensions EDS à des fins de sécurité

8.10.2.1 Sections supplémentaires de classe d'objet

Le Tableau 108 identifie les mots clés de section utilisés pour publier les informations de la classe d'objet Sécurité. Chacun des mots clé de section EDS suivants peut contenir le/les mot(s) clé(s) de l'Entrée de classe d'objet commune décrit(s) dans la CPF 2. Le tableau suivant contient les noms des sections de la classe d'objet Sécurité.

Tableau 108 – Mots clés des sections de classe d'objet

Objet du CIP	Code de classe	Nom du mot clé de la section	Exigé/ Facultatif
Objet Programme de contrôle de sécurité	39 _{hex}	[Classe Programme de contrôle de sécurité]	Facultatif
Objet de validation de sécurité	3A _{hex}	[Classe Objet de Validation de sécurité]	Facultatif
Objet Point de sortie discrète de sécurité	3B _{hex}	[Classe Point de sortie discrète de sécurité]	Facultatif
Objet Groupe de sorties discrètes de sécurité	3C _{hex}	[Classe Groupe de sorties discrètes de sécurité]	Facultatif
Objet Point d'entrée discrète de sécurité	3D _{hex}	[Classe Point d'entrée discrète de sécurité]	Facultatif
Objet Groupe d'entrées discrètes de sécurité	3E _{hex}	[Classe Groupe d'entrées discrètes de sécurité]	Facultatif
Objet Sortie de canal double de sécurité	3F _{hex}	[Classe Groupe de sorties discrètes de sécurité]	Facultatif
Objet Point d'entrée analogique de sécurité	49 _{hex}	[Classe Groupe d'entrées analogiques de sécurité]	Facultatif
Objet Groupe d'entrées analogiques de sécurité	4A _{hex}	[Classe Groupe d'entrées analogiques de sécurité]	Facultatif
Objet Entrée analogique de canal double de sécurité	4B _{hex}	[Classe Entrée analogique de canal double de sécurité]	Facultatif
Objet Liaison SERCOS III	4C _{hex}	[Classe Liaison SERCOS III]	Facultatif

8.10.2.2 Extension de la section [fichier] à des fins de sécurité

Les fichiers EDS dédiés à un appareil de sécurité doivent être protégés par un CRC. Le CRC-S4 avec la valeur de départ définie en 7.1.2.3 doit être utilisé.

La valeur CRC de fichier EDS doit être saisie dans la section [fichier] avec le mot clé d'entrée "EDSFileCRC=". Ce dernier doit figurer sur une seule ligne.

Le SNCT doit confirmer le CRC de fichier EDS avant toute utilisation du contenu du fichier tel que décrit ci-dessous:

- ouvrir le fichier comme un fichier binaire. Charger le fichier entier dans la mémoire.
- retirer la ligne complète y compris le retour chariot comportant l'entrée EDSFileCRC=;
- calculer le CRC sur le contenu restant du fichier;
- comparer le CRC calculé avec la valeur de l'entrée EDSFileCRC=.

Tous les fichiers EDS des appareils de sécurité doivent comporter un mot clé et une valeur "EDSFileCRC=". Si l'entrée [classification des appareils] décrit l'appareil comme comportant des capacités de sécurité et si le mot clé de l'entrée EDSFileCRC= n'existe pas, le SNCT ne doit pas utiliser le fichier.

8.10.2.3 Extension de la section [classification des appareils] à des fins de sécurité

Le fichier EDS dédié aux appareils de sécurité doit inclure une section [classification des appareils] qui doit contenir la ligne suivante:

Classe_x = Sécurité;

où

x est une valeur décimale.

Le mot clé de Classex, avec le champ Classification correspondant au champ Sécurité, est défini dans le Tableau 109.

Tableau 109- Format d'entrée de Classex de sécurité

Nom d'entrée	Numéro de champ	Type de données	Exigé/Facultatif
Classification	1	Mot clé du champ	Exigé
Réservé	2,3	Vide	
Instance de Port	4,5,...n	UINT	Conditionnel ^a
^a Exigé si l'appareil prend en charge plus d'1 port CIP.			

La valeur de Classification doit correspondre à celle de Sécurité.

Les champs d'Instance de Port sont les instances de l'Objet Port qui prennent en charge la sécurité.

8.10.2.4 Extension de la section [ParamClass] à des fins de sécurité

Les appareils de sécurité doivent utiliser le mot clé SafetyCfgAssembly pour identifier l'instance d'objet d'ensemble de configuration. Le mot clé est défini dans le Tableau 110.

Tableau 110 – Mots clés de classes de paramètres

Nom d'entrée	Mot clé d'entrée	Numéro de champ	Type de données	Exigé/Facultatif
Instance d'ensemble de sécurité	SafetyCfgAssembly	1	UINT	Conditionnel ^a
^a Doit être mis en œuvre pour les appareils de sécurité configurés via un fichier EDS				

SafetyCfgAssembly – Identifie le numéro d'instance de l'objet d'ensemble de configuration pour les paramètres relatifs à la sécurité de cet appareil.

Une entrée de mot clé "SafetyCfgAssembly=" doit être prévue pour les appareils de sécurité configurés via un fichier EDS. Cette valeur doit également correspondre à un mot clé d'entrée AssemN spécifié dans la section [Ensemble].

8.10.2.5 Extension de la section [Gestionnaire de connexion] à des fins de sécurité

8.10.2.5.1 Généralités

Le présent paragraphe décrit quatre nouveaux mots clés de sécurité. Le Tableau 111 récapitule ces mots clés.

Tableau 111 – Nouveaux mots clés de la section Gestionnaire de connexion à des fins de sécurité

Nom d'entrée	Mot clé d'entrée	Numéro de champ	Type de données	Exigé/Facultatif
Connexions de sécurité maximale	MaxSafetyConnections	1	USINT	Facultatif
Connexions d'entrée de sécurité maximale	MaxSafetyInputCnxns	1	USINT	Facultatif
Connexions de sortie de sécurité maximale	MaxSafetyOutputCnxns	1	USINT	Facultatif
Connexions de sécurité par défaut				
	Instance de connexion 1	1	UINT	Exigé
	Instance de connexion n	N	UINT	Conditionnel
Prise en charge de format étendu	ExtendedFormat	1	USINT	Facultatif

8.10.2.5.2 Connexions de sécurité maximale

Les appareils de sécurité prennent généralement en charge un grand nombre d'ensembles possibles qui mélangent et mettent en correspondance différentes combinaisons de données et/ou état E/S. Ces appareils comportent conjointement une limite concernant le nombre de connexions E/S de sécurité pouvant être établies à tout moment. Les mots clés de la section [Gestionnaire de connexion] définissent ces limites. Il n'existe aucune limite si le fichier EDS ne comporte aucune entrée.

8.10.2.5.3 Connexions de sécurité par défaut

Il existe souvent un ensemble de connexions les plus couramment utilisées. Les développeurs de produits peuvent éventuellement définir un ensemble de connexions par défaut qui permet à l'utilisateur d'ajouter rapidement et facilement ces connexions à une configuration d'origine. Le mot clé d'entrée DefaultSafetyConnections spécifie quelles entrées de gestionnaire de connexion constituent ces connexions "par défaut".

8.10.2.5.4 Prise en charge du format de sécurité

Un appareil qui prend en charge le format Etendu doit déclarer cette prise en charge en saisissant ce mot clé dans la section Gestionnaire de connexion de son fichier EDS. Par cette déclaration, les algorithmes de logiciel de configuration de connexion peuvent être activés pour configurer un nouvel attribut de type de format dans l'objet Configuration de connexion. Lorsqu'un fichier EDS ne comporte pas ce mot de passe, il est supposé que seul le format de base est pris en charge (équivalant à SafetyFormat = BaseOnly). Les options possibles sont les suivantes:

- SafetyFormat = 1; prise en charge du format de Base uniquement;
- SafetyFormat = 2; prise en charge du format Etendu uniquement;
- SafetyFormat = 3; prise en charge des formats de Base et Etendu.

8.10.2.5.5 Modifications et ajouts aux champs Gestionnaire de connexion

8.10.2.5.5.1 Présentation générale des modifications et ajouts

Une entrée de gestionnaire de connexion doit être définie pour chaque composante de sécurité à laquelle une connexion peut être établie. Les connexions de sécurité sont définies en utilisant la section Gestionnaire de connexion existante spécifiée dans l'Annexe A de l'ISO 15745-2:2003 avec les extensions suivantes. Le SNCT doit utiliser chaque entrée pour présenter à l'utilisateur un ensemble d'options de connexion qu'il est possible de réaliser à partir d'un point d'origine.

Le Tableau 112 énumère les champs actuels définis pour la section Gestionnaire de connexion.

Tableau 112 – Utilisation du champ Gestionnaire de connexion à des fins de sécurité

Nom de champ	Numéro de champ	Type de données	Utilisation à des fins de sécurité
Déclenchement et transport	1	DWORD	Classe: Doit être égale à zéro Déclenchement: doit être l'application Type d'application de transport: Tous types = 0 les producteurs doivent être Entrée uniquement les consommateurs doivent être Propriétaire exclusif EXEMPLE producteurs (clients): 02040001 _{hex} consommateurs (serveur): 84040001 _{hex}
Paramètres de connexion	2	DWORD	Taille O-à-T: doit être uniquement fixe Taille T-à-O: doit être uniquement fixe Octets par intervalle: toujours ignoré Format de transfert en temps réel: 5 = Sécurité Priorité: toujours élevée Type de connexion: Entrées: Multipoints ou point à point T-à-O Point à point O-à-T Sorties: Point à point O-à-T et T-à-O EXEMPLE Entrée multipoints (producteur): 22645505 _{hex} Sortie point à point (consommateur): 22445505 _{hex}
RPI O-à-T	3	Param	Laisser en blanc ou fournir une référence Param pour définir la capacité de l'appareil
taille O-à-T	4	UINT ou Param	Si laissé en blanc, attribution de la taille à partir de la référence ASSEM associée ou le logiciel utilise la taille de Coordination temporelle
format O-à-T	5	Assem	Pour les connexions de sortie de sécurité, ce champ doit indiquer l'ensemble de sortie de sécurité auquel la connexion est associée. Pour les connexions d'entrée de sécurité, ce champ doit être vide
RPI T-à-O	6	Param	Laisser en blanc ou fournir une référence Param pour définir la capacité de l'appareil
taille T-à-O	7	UINT ou Param	Si laissé en blanc, attribution de la taille à partir de la référence ASSEM ou le logiciel utilise la taille de Coordination temporelle
Format T-à-O	8	Assem	Pour les connexions d'entrée de sécurité, ce champ doit indiquer l'ensemble d'entrée de sécurité auquel la connexion est associée. Pour les connexions de sortie de sécurité, ce champ doit être vide
taille config #1	9	UINT ou Param	Peut être utilisé éventuellement
format config #1	10	Param ou Assem	Peut être utilisé éventuellement
taille config #2	11	UINT ou Param	Taille de l'ensemble de configuration lorsque l'appareil prend en charge la configuration via le service SafetyOpen de forme 1
format config #2	12	Param ou Assem	Ce champ peut indiquer quel ensemble contient les données de configuration SafetyOpen de forme 1

Nom de champ	Numéro de champ	Type de données	Utilisation à des fins de sécurité
Chaîne de nom de connexion	13	Matrice Eds_Char	Nom unique permettant à un utilisateur d'identifier l'ensemble d'application auquel cette instance est associée
Chaîne d'aide	14	Matrice Eds_Char	Message d'aide à l'utilisateur relatif à l'utilisation de la connexion
Chemin de données	15	Matrice Eds_Char	Chemin complet constitué des chemins Config., Consommé et Produit. Des chemins nuls sont insérés aux points où il n'existe aucun chemin (voir les formats possibles ci-dessous)
ASYN1	16	USINT	Il s'agit d'un champ exclusif FSCP 2/1 S'applique uniquement aux connexions de production. Il convient que le champ soit vide pour les connexions de consommation. Utilisé pour calculer le temps de réaction du réseau
Nombre maximal de consommateurs ^a	17	USINT	Il s'agit d'un champ exclusif FSCP 2/1 Lorsque les appareils de sécurité souhaitent définir des connexions multipoints et nécessitent de limiter le nombre maximal de consommateurs à une valeur inférieure à la valeur maximale par défaut de 15, ce champ peut définir la limite de produit. Si ce champ est vide, le SNCT doit toujours utiliser la valeur par défaut de 15 pour le nombre maximum de connexions multipoints. Ce champ peut être laissé vide pour les connexions point à point. Voir 7.7.5.11 (Max_Consumer_Number) pour la définition des valeurs légales applicables à ce champ
^a Ce champ est défini uniquement pour les spécifications relatives à la sécurité et doit être soit vide, soit omis pour les instances de gestionnaire de connexion non relatives à la sécurité.			

8.10.2.5.5.2 Champ Déclenchement et transport

Les appareils de sécurité définissent si une connexion est une connexion de production (client) ou de consommation (serveur) par le remplissage de ce champ. Les autres parties du champ comportent les définitions fixes ci-dessous:

- Classe: toujours 0;
- Déclenchement: toujours par l'application;
- Type de Transport: Tous types = 0.

8.10.2.5.5.3 Champ de paramètres de connexion

Ce champ permet aux appareils de sécurité de définir les types de connexions possibles pour une connexion donnée. Tous les autres champs présentent des valeurs fixes. Le Tableau 113 fournit les seules valeurs valides pour les appareils de sécurité.

Tableau 113 – Paramétrages du champ de paramètres de connexion à des fins de sécurité

Type de connexion	Paramétrage des paramètres de connexion
Connexion d'entrée de production (client)	22645505 _{hex} ou 22445505 _{hex} (aucune connexion multipoints)
Connexion de sortie de consommation (serveur)	22445505 _{hex}

8.10.2.5.5.4 Champ Chemin de données

L'IEC 61158-6-2 définit une méthode de réalisation d'un chemin d'application dans un service ForwardOpen pour 3 références: une référence pour la configuration, une référence pour les données consommées et une référence pour les données produites. L'introduction de

chemins NULL pour la sécurité s'accompagne d'exigences supplémentaires en matière de sécurité.

8.10.2.5.5.5 Champ ASYNC

Ce paramètre est nécessaire au calcul correct du temps de réaction de réseau pour une connexion de sécurité. Ce paramètre diffère généralement pour les connexions d'entrée et de sortie, mais dépend de la conception. La section Gestionnaire de connexion des connexions de production (client) doit comporter ce champ. Les appareils de production avec des connexions d'entrée doivent définir une valeur ASYNC pour ces connexions et les appareils de production avec des connexions de sortie (c'est-à-dire des appareils logiques ou des scrutateurs) doivent définir une valeur ASYNC pour ces mêmes connexions. Le logiciel ignore toute valeur fournie avec les connexions de consommation (serveur). Si un paramètre ASYNC n'est pas défini dans une connexion de production, le logiciel doit utiliser une valeur par défaut du cas le plus défavorable de 1. Les valeurs du paramètre ASYNC sont les suivantes:

- ASYNC = 0 = synchrone;
- ASYNC = 1 = asynchrone.

8.11 Exigences pour le profil CP 2/2

8.11.1 Règles EPI applicables aux messages de sécurité acheminés via CP 2/2

Les paquets de sécurité qui doivent être acheminés via CP 2/2 comportent certaines restrictions basées sur le format de sécurité utilisé pour l'établissement de la connexion.

Les connexions de sécurité qui utilisent le format de base et qui sont acheminées via CP 2/2 sont limitées à des EPI inférieurs à 100 ms. La méthode d'application effective de cette restriction relève d'une décision spécifique au fournisseur. Par exemple, la restriction peut être appliquée dans le logiciel de configuration d'origine ou dans les contrôles de l'établissement de connexion d'origine. Les fournisseurs sont chargés de s'assurer de la mise en place des restrictions appropriées.

Les connexions de sécurité qui utilisent le format Etendu peuvent utiliser la plage supérieure de 1 000 ms.

8.11.2 Service E/S de sécurité par défaut

Les connexions de sécurité prennent en charge tant les types de connexion point à point que multipoints, mais EtherNet/IP comporte de nombreuses complications système lors de l'application de services Multicast (multidestinatoires). Il est vivement recommandé que lors de la configuration de connexions de sécurité dans un point d'origine, il convient que le logiciel de configuration de sécurité présente une connexion point à point comme le service par défaut pour toutes les configurations de sécurité. Il convient que l'utilisateur ait la possibilité de choisir la connexion Multipoints, mais il convient d'utiliser une connexion point à point si ce choix n'est pas spécifiquement effectué.

Il convient que les appareils CP 2/2 de sécurité envisagent l'ajout d'une prise en charge de plusieurs connexions point à point avec le même ensemble d'entrée de sécurité afin de faciliter davantage l'utilisation d'une connexion point à point.

8.11.3 Duplication de détection IP

Les appareils de sécurité placés sur CP 2/2 doivent prendre en charge le mécanisme de détection de conflit d'adresse IPv4 défini dans le profil CP 2/2.

8.11.4 Priorité pour les connexions de sécurité

Les appareils de sécurité CP 2/2 doivent utiliser le programme de qualité de service CP 2/2 normalisé; voir l'IEC 61158-5-2 pour les détails de mise en œuvre. Les appareils de sécurité

CP 2/2 doivent mettre en œuvre les services QoS et prendre en charge le marquage de priorité via des points de code DiffServ (DSCP). Les appareils de sécurité CP 2/2 doivent utiliser la priorité «ordonnancée» comme la priorité par défaut pour les appareils E/S.

8.12 Exigences pour le profil CP 2/3

8.12.1 Attribution des identifiants CP 2/3

8.12.1.1 Généralités

Lors du processus de connexion d'un service SafetyOpen CP 2/3, le paquet d'unités disponible d'identifiants de groupe 1 CP 2/3 doit attribuer des identifiants de sécurité.

Les règles définies de 8.12.1.2 à 8.12.1.10 doivent être mises en œuvre pour l'attribution d'identifiants de connexion, et ce, pour protéger ces derniers.

8.12.1.2 Algorithme CP 2/3 de base (modèle général)

Les points d'origine de connexion de sécurité doivent demander initialement à la cible (via le service SafetyOpen) d'attribuer un, deux ou trois identifiants selon les règles énoncées dans le Tableau 114.

Tableau 114 – Règles d'attribution d'ID CP 2/3

Type de connexion	(Premier) saut intermédiaire	Dernier saut (uniquement) 1 ^{ère} tentative	Dernier saut (uniquement) 2 ^e tentative	Dernier saut (uniquement) 3 ^e tentative
Point à point	T ⇒ O: Routeur cible O ⇒ T: Point d'origine ou routeur d'origine	T ⇒ O: Cible O ⇒ T: Cible	Anomalie de connexion, La connexion ne peut pas être établie	Anomalie de connexion, La connexion ne peut pas être établie
Multipoints T ⇒ O (typique; module d'entrée, état de module de sortie)	T ⇒ O: Routeur cible O ⇒ T: Point d'origine ou routeur d'origine TC: Routeur cible	T ⇒ O: Cible O ⇒ T: Conditionnel TC: Cible	T ⇒ O: Cible O ⇒ T: Point d'origine (si la première demande était la cible) TC: Cible	Anomalie de connexion, La connexion ne peut pas être établie
Multipoints O ⇒ T	T ⇒ O: Routeur cible O ⇒ T: Point d'origine ou routeur d'origine TC: Point d'origine ou routeur d'origine	T ⇒ O: Cible O ⇒ T: Point d'origine TC: Point d'origine ou routeur d'origine	T ⇒ O: Point d'origine O ⇒ T: Point d'origine TC: Point d'origine ou routeur d'origine	Anomalie de connexion, La connexion ne peut pas être établie

Ceci est réalisé par l'insertion des identifiants 0xFFFFFFFF dans la demande SafetyOpen transmise à la cible.

Si une cible de sécurité ne peut ou refuse d'attribuer le ou les identifiants, elle doit répondre à la demande SafetyOpen par un état d'erreur générale 0x01 avec un état étendu 0x031F, qui indique l'absence de ressources de connexion.

Le point d'origine reçoit la réponse SafetyOpen.

Si la cible a attribué des identifiants à partir de son paquet d'unités, elle doit les intégrer dans la réponse satisfaisante SafetyOpen.

Le point d'origine accepte ces identifiants et la connexion est réalisée.

Si la cible n'a pas attribué d'identifiants à partir de son paquet d'unités, le point d'origine a la possibilité d'attribuer des identifiants à partir de son propre paquet d'unités. Si le point d'origine attribue le ou les identifiants, il doit acheminer ces données vers la cible (via un second service SafetyOpen).

Si le point d'origine ne peut ou refuse d'attribuer un identifiant, la connexion ne peut pas être établie.

8.12.1.3 Cas 1 (la cible attribue des identifiants)

Ce premier scénario exige du point d'origine qu'il demande à la cible d'attribuer les identifiants de connexion, la cible acceptant cette demande.

Le point d'origine de connexion demande à la cible (via le service SafetyOpen) d'attribuer un, deux ou trois identifiants.

- La cible consent à attribuer le(s) identifiant(s) et répond de manière satisfaisante à la demande Safety Open.
- Le point d'origine reçoit la réponse SafetyOpen et accepte ces identifiants, la connexion est ainsi réalisée.

8.12.1.4 Cas 2 (la cible ne peut pas attribuer d'identifiants)

Ce second scénario exige du point d'origine qu'il demande à la cible d'attribuer les identifiants de connexion, la cible ne pouvant toutefois y souscrire ou refusant cette demande.

- Le point d'origine de connexion demande à la cible (via le service SafetyOpen) d'attribuer un, deux ou trois identifiants (identifiant = 0xFFFFFFFF).
- La cible choisit de ne pas attribuer le ou les identifiants et répond à la demande SafetyOpen par un code d'erreur générale 0x01 avec un état étendu 0x05, qui indique l'absence des ressources nécessaires.
- Le point d'origine reçoit la réponse SafetyOpen, constate que la cible ne peut pas attribuer d'identifiants, puis choisit d'attribuer ces mêmes identifiants à partir de son propre paquet d'unités.
- Le point d'origine constitue alors un second service SafetyOpen avec les identifiants spécifiés.
- La cible accepte ce service SafetyOpen et la connexion est réalisée.

8.12.1.5 Cas 3 (le point d'origine attribue des identifiants)

Ce troisième scénario exige du point d'origine qu'il décide d'attribuer ses propres identifiants avec sollicitation de la cible.

- Le point d'origine de connexion attribue les identifiants de son paquet d'unités et saisit ces valeurs dans le service SafetyOpen transmis ensuite à la cible.
- La cible accepte ce service SafetyOpen et répond de manière satisfaisante.
- Le point d'origine reçoit la réponse SafetyOpen et la connexion est réalisée.

8.12.1.6 Ordre d'attribution des MSGID

Comme indiqué ci-dessus, chaque nœud comporte un nombre total de 12 identifiants de groupe 1 pouvant être utilisés pour les connexions de sécurité. La règle suivante d'attribution des identifiants doit être suivie afin d'assurer une certaine cohérence entre les producteurs et les consommateurs. Le premier MSGID devant être attribué doit commencer à la valeur disponible la plus élevée et évoluer vers le bas.

Ainsi, le premier MSGID serait B(hex) ou 1011(binaire), et le suivant serait A(hex) ou 1010(binaire).

8.12.1.7 Règles d'attribution des ID de connexion

Les règles suivantes d'attribution des ID CP 2/3 doivent être suivies par les cibles, points d'origine et ponts de sécurité. Ces règles prévoient l'attribution d'ID reproductibles pour un système avec lequel un seul ou aucun routeur n'est connecté au CP 2/3, et où les ID non utilisés des appareils cibles sont transmis aux ponts. Dans la mesure où une ressource, à savoir le routeur, est autorisée à solliciter ces ressources, il convient qu'elle fonctionne correctement. Toute tentative d'extension de cette fonctionnalité à d'autres points d'origine peut toutefois aboutir à une situation où une mise sous tension reproductible n'est pas réalisable.

- Règle 1: tous les points d'origine multipoints en liaison fournissent le troisième ID de groupe 1 lors de l'établissement d'une connexion.
- Règle 2: tous les points d'origine de connexion multipoints hors liaison (routeurs) sollicitent le troisième ID de groupe 1 auprès de la cible
- Règle 3: Les ID de groupe 1 des cibles sont répartis en 2 types, réservés et libres:
 - Les ID réservés équivalent à $2 \times$ le nombre maximal de connexions de sécurité qu'un appareil peut prendre en charge. Le nombre maximal de connexions est spécifié lorsqu'un appareil est configuré.
 - Le nombre d'ID libres est égal à ID de groupe 1 max. (12) – ID réservés.
 - Dans la plupart des appareils cibles, ceci peut être une valeur par défaut et il n'est jamais nécessaire que l'utilisateur la modifie.
- Règle 4: chaque cible fournit 2 ID de groupe 1 réservés aux points d'origine multipoints ou point à point jusqu'à l'épuisement de ses ID réservés. Une fois ses ID réservés épuisés, la cible rejette les demandes d'établissement de nouvelles connexions. Elle permet toutefois aux points d'origine de tenter d'établir une connexion multipoints à des productions multipoints déjà établies.
- Règle 5: chaque cible fournit le troisième ID de groupe 1 aux points d'origine multipoints à partir de son paquet d'unités libre. Une fois le paquet d'unités épuisé, la cible rejette la demande et il est nécessaire que le point d'origine fournisse le troisième ID.

8.12.1.8 Connexions de messages point à point

L'algorithme de base décrit de 8.12.1.2 à 8.12.1.7 s'applique à ces types de connexion.

8.12.1.9 Connexions de messages multipoints

Les producteurs multipoints doivent attribuer un identifiant de leur propre paquet d'unités, c'est-à-dire que le MACID source doit être celui du producteur. Les producteurs multipoints doivent refuser toute demande de connexion qui tente d'attribuer des ID pour ses données produites ou de correction temporelle. Le consommateur multidestinaires peut appliquer l'algorithme de base décrit ci-dessus.

8.12.1.10 Exigences relatives à la mise en quarantaine des ID CP 2/3

Il est nécessaire que les appareils cibles veillent à ne réattribuer aucun ID de groupe 1 jusqu'à ce qu'ils soient certains que les ID ne sont plus utilisés par l'appareil auquel ils ont été précédemment attribués. L'algorithme suivant doit être appliqué afin de s'assurer que cette condition ne se produit pas.

Lorsqu'un appareil de sécurité ferme une connexion dans laquelle des ID de groupe 1 ont été attribués à un autre appareil, l'ID de groupe 1 doit être mis en quarantaine pendant une période égale à $(\text{connection\_EPI} \times \text{Ping\_Interval\_Multiplier}) \times (\text{Timeout\_Multiplier.PI} + 2)$. Pendant cette période, l'ID ne peut être utilisé ou attribué à aucun autre appareil.

Si un point d'origine ayant emprunté un ID détecte la défaillance de la communication et rémet une nouvelle demande de connexion avant que ces ID ne soient plus mis en quarantaine, les appareils peuvent définir des programmes de détection de ces demandes et

extraire rapidement les ID de leur quarantaine et les renvoyer au point d'origine. Il doit toutefois être veillé à s'assurer que cette opération est réalisée avec intégrité.

8.12.2 Exigences supplémentaires

Aucune.

8.13 Exigences pour le profil CP 16/3

8.13.1 Architecture générale de la CPF 2 sur CP 16/3

La couche de sécurité de FSCP 2/1 sur CP 16/3 est mise en œuvre conformément à la spécification de FSCP 2/1 sans aucune modification. Cela signifie notamment que

- FSCP 2/1 sur CP 16/3 utilise les formats de message de sécurité définis dans la présente norme,
- les mêmes polynômes de CRC, mêmes valeurs de départ CRC et mêmes algorithmes CRC sont utilisés, et
- tous les objets et services FSCP 2/1 sont mis en œuvre conformément à la présente norme.

Par conséquent, le profil FSCP 2/1 sur CP 16/3 ne repose sur aucune mesure permettant d'assurer l'intégrité des données fournie par la couche de transport CP 16/3. Le CP 16/3 peut pleinement être considéré comme partie intégrante du canal noir.

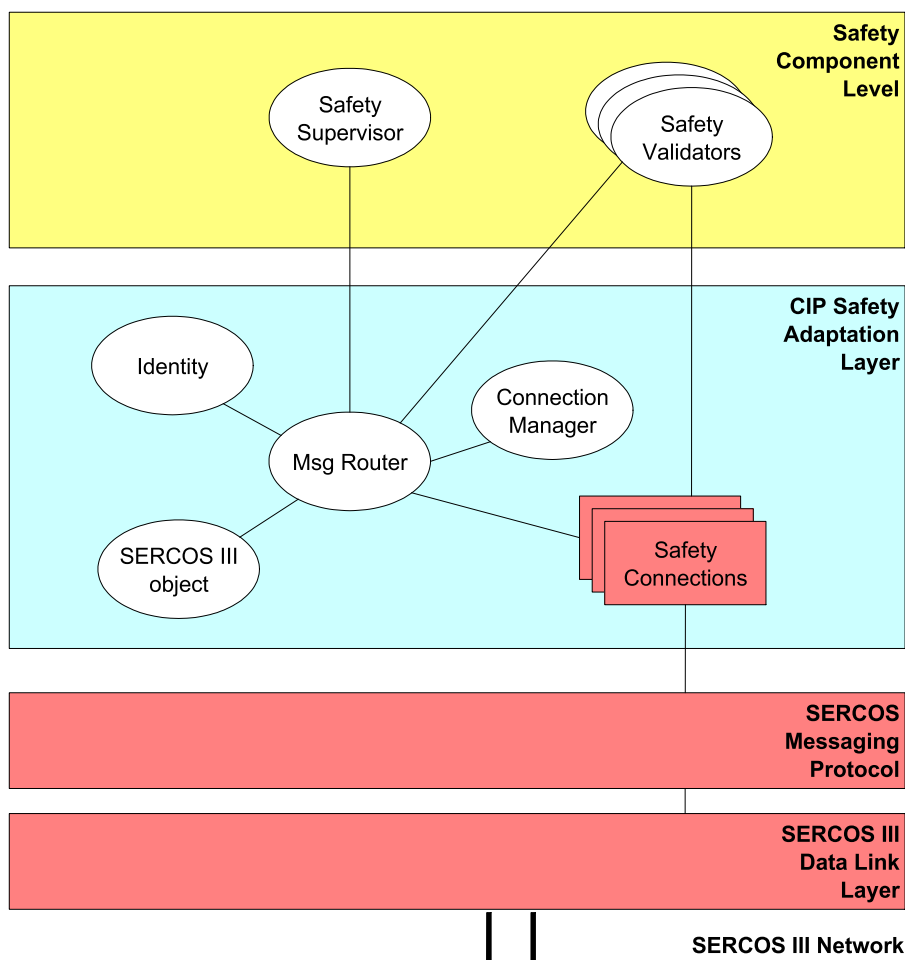
Le FSCP 2/1 se fonde sur un ensemble de base d'objets et services CIP normalisés pour établir des connexions de transport et échanger des données cycliques. Dans la mesure où le CP 16/3 ne fournit aucune mise en œuvre de la couche application CIP, une couche d'adaptation est exigée pour combler l'écart entre la couche de transport CP 16/3 et le FSCP 2/1.

Bien que tous les mécanismes aient été adoptés à partir de la spécification FSCP 2/1 existante, il a fallu apporter certains ajouts et modifications à la spécification. Tous les ajouts et modifications n'affectent pas les mesures définies par le profil FSCP 2/1 pour assurer l'intégrité des données.

8.13.2 FSCP 2/1 de référence pour appareils CP 16/3

La fonctionnalité exigée pour mettre en œuvre le FSCP 2/1 dans un appareil CP 16/3 est encapsulée dans une couche d'adaptation à la partie supérieure des mécanismes de communication CP 16/3 normalisés. Le groupe de fonctions CP 16/3 "S 0 1830 Connexion de sécurité" fournit la fonctionnalité qui permet la configuration des connexions à la fois explicites et d'E/S, et l'échange de données via le Protocole de messagerie CP 16/3 (SMP).

La Figure 86 représente la manière dont la couche d'adaptation FSCP 2/1 fournit une fonctionnalité CIP similaire à celle de l'appareil de sécurité de référence défini en 6.6.



IEC

Anglais	Français
Safety supervisor	Programme de contrôle de sécurité
Safety validator	Objet de validation de sécurité
Identity	Identité
SERCOS III object	Objet SERCOS III
Msg router	Routeur de message
Safety connections	Connexions de sécurité
Connection manager	Gestionnaire de connexion
Safety component level	Niveau de composante de sécurité
CIP Safety adaptation layer	Couche d'adaptation de sécurité CIP
SERCOS III messaging protocol	Protocole de messagerie SERCOS III
SERCOS III Data link layer	Couche de liaison de données SERCOS III
SERCOS III network	réseau SERCOS III

Figure 86 – FSCP 2/1 de référence des appareils CP 16/3

8.13.3 Objets et services pris en charge dans les appareils CP 16/3

8.13.3.1 Généralités

Les appareils CP 16/3 doivent prendre en charge les objets CPF 2 tel que spécifié de 8.13.3.2 à 8.13.3.8.

8.13.3.2 Objet Identité (code de classe 0x01)

Tous les services exigés doivent être pris en charge.

8.13.3.3 Objet Gestionnaire de connexion (code de classe 0x06)

L'objet Gestionnaire de connexion offre les services exigés pour ouvrir et fermer les connexions FSCP 2/1.

- ForwardClose (0x4E);
- ForwardOpen (0x54).

Bien que l'objet Gestionnaire de connexion fournisse l'interface à ces services, il faut que la majeure partie du traitement soit effectuée dans la couche FSCP 2/1 pour assurer une haute intégrité. Il s'agit de l'objectif de l'unité d'établissement de connexion de l'objet de validation représentée à la Figure 88. La couche d'adaptation FSCP 2/1 ne veille qu'à la préparation du canal noir pour la connexion de sécurité en établissant les sessions SMP nécessaires.

8.13.3.4 Objet Configuration de connexion (code de classe 0xF3)

Habituellement, l'objet Configuration de connexion n'est mis en œuvre que pour les points d'origine de connexion.

Chaque instance de cet objet maintient les données de configuration pour une connexion exigée pour formuler un message de service ForwardOpen à la cible de connexion.

8.13.3.5 Objet Routeur de message (code de classe 0x02)

L'objet Routeur de message ne fournit aucun service accessible. Il distribue des messages entrants explicites à tous les autres objets contenus dans un appareil.

8.13.3.6 Objet Programme de contrôle de sécurité (code classe de 0x39)

Les appareils CP 16/3 doivent prendre en charge le niveau de référence de l'objet Programme de contrôle de sécurité à un minimum donné.

8.13.3.7 Objet de validation de sécurité (code de classe 0x3A)

Les appareils CP 16/3 doivent prendre en charge l'Objet de validation de sécurité dans son intégralité.

8.13.3.8 Objet Liaison SERCOS III (code de classe 0x4C)

Les appareils CP 16/3 doivent prendre en charge l'objet Liaison SERCOS III dans son intégralité.

8.13.4 Exigences relatives aux couches de transport

8.13.4.1 Généralités

Le FSCP 2/1 des appareils CP 16/3 doit utiliser le protocole de messagerie CP 16/3 (SMP) pour l'échange des messages de sécurité. Le SMP définit un ensemble de conteneurs de messagerie pouvant être acheminés via des connexions CP 16/3.

8.13.4.2 Considérations relatives aux couches de transport

Le CP 16/3 offre deux mécanismes de base pour l'échange de données entre deux appareils.

- Connexions cycliques

Une connexion CP 16/3 cyclique transporte d'un producteur à un consommateur un paquet de données contenant une ou plusieurs valeurs de données. La taille du paquet de données, le contenu et le taux de production sont généralement configurables pendant qu'un appareil est à l'étape de paramétrage. Lorsqu'il quitte l'étape de paramétrage, la configuration reste statique. Le producteur de la connexion produit alors des données cycliques au taux configuré.

- Voie de service

Il s'agit d'un canal de communication acyclique commandé exclusivement par le maître CP 16/3. Le maître peut envoyer des données à ou récupérer des données d'un appareil esclave.

Ni les connexions cycliques, ni la voie de service ne peuvent satisfaire à toutes les exigences de FSCP 2/1 sur CP 16/3. Par conséquent, la couche d'adaptation FSCP 2/1 utilise le protocole de messagerie CP 16/3 (SMP) pour échanger des messages FSCP 2/1 avec d'autres appareils CP 16/3. Ce protocole est posé en couche au-dessus des connexions cycliques CP 16/3. Il fournit un API comme "send () / recv ()" à la couche application (dans ce cas, à la couche d'adaptation FSCP 2/1). La couche application du producteur peut envoyer à un consommateur des messages de longueur arbitraire. Le SMP utilise un conteneur de données de longueur fixe dans une connexion cyclique pour acheminer ces messages. Les messages de taille plus grande que le conteneur de données sont divisés en plusieurs fragments qui sont ensuite transportés séquentiellement. Un mécanisme de priorisation permet à des messages de haute priorité d'interrompre la transmission de longs messages fragmentés de moindre priorité. Cela permet un multiplexage efficace de plusieurs canaux de communication logiques sur un seul conteneur de transport.

Faisant partie de la couche de transport CP 16/3, la pile de protocole de messagerie CP 16/3 fait également partie intégrante du canal noir. Elle n'affecte aucun des mécanismes et aucune des mesures d'intégrité de données mis en œuvre par la couche FSCP 2/1.

L'exemple de la Figure 87 présente une configuration possible du SMP pour une seule connexion FSCP 2/1. Deux conteneurs SMP sont utilisés, l'un étant configuré dans l'AT pour transporter des messages à partir de l'esclave CP 16/3 au maître CP 16/3, tandis que l'autre conteneur est configuré dans le MDT pour transporter des messages du maître CP 16/3 à l'esclave CP 16/3. Le maître CP 16/3, agissant comme point d'origine de connexion, initie la connexion de sécurité par l'envoi d'un service CIP ForwardOpen comme un message explicite non connecté à l'esclave. Ce message est transporté par le conteneur SMP 2. L'esclave répond par un message de Réponse ForwardOpen transporté par le conteneur SMP 1. Dans le même temps, il commence à produire des messages de données FSCP 2/1 qui sont transportés dans le même conteneur. L'utilisation d'une session à identifiant permet un multiplexage efficace de plusieurs canaux de communication logiques sur un seul conteneur de transport.

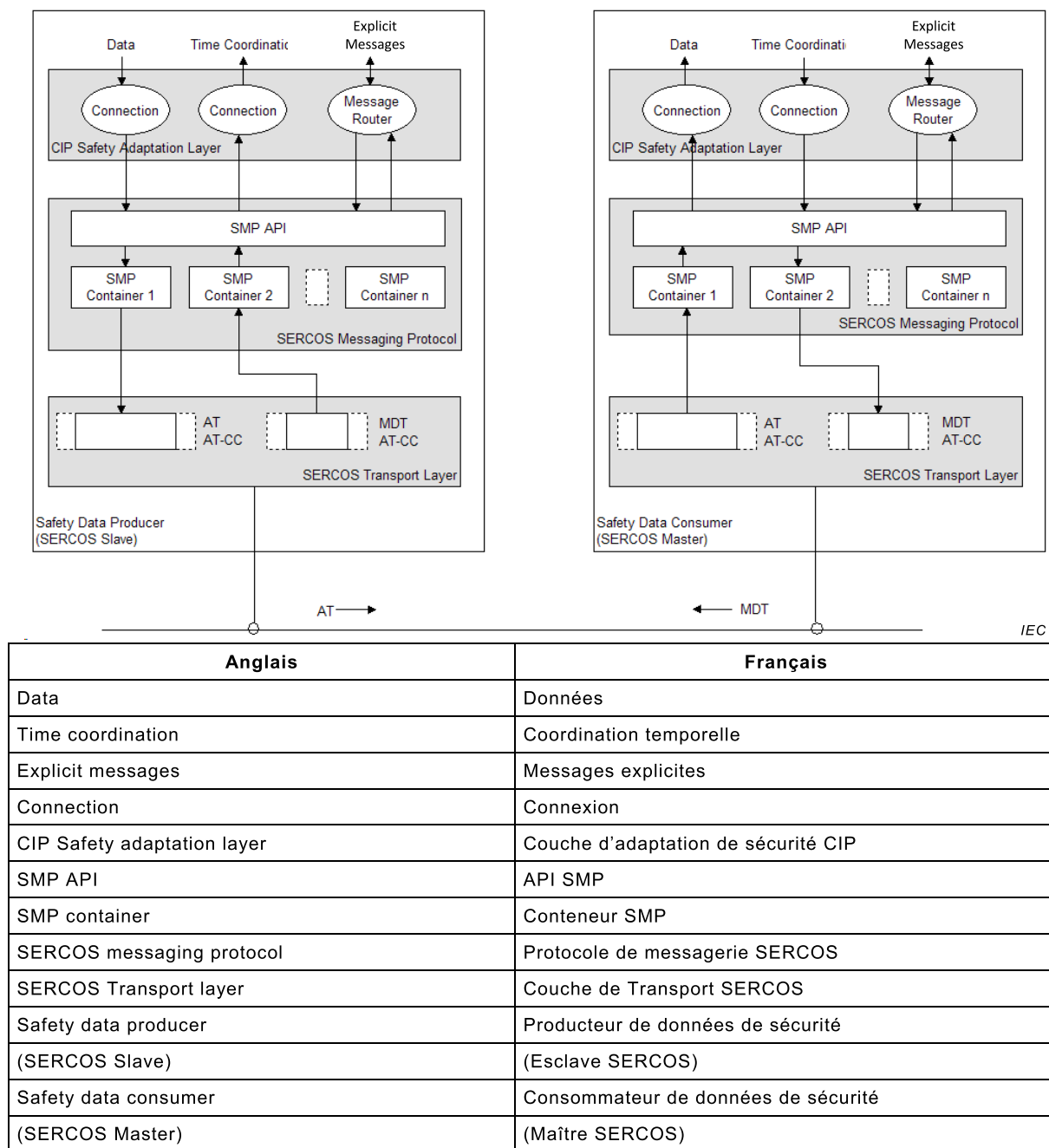


Figure 87 – Interaction entre Couche d'adaptation FSCP 2/1 et SMP

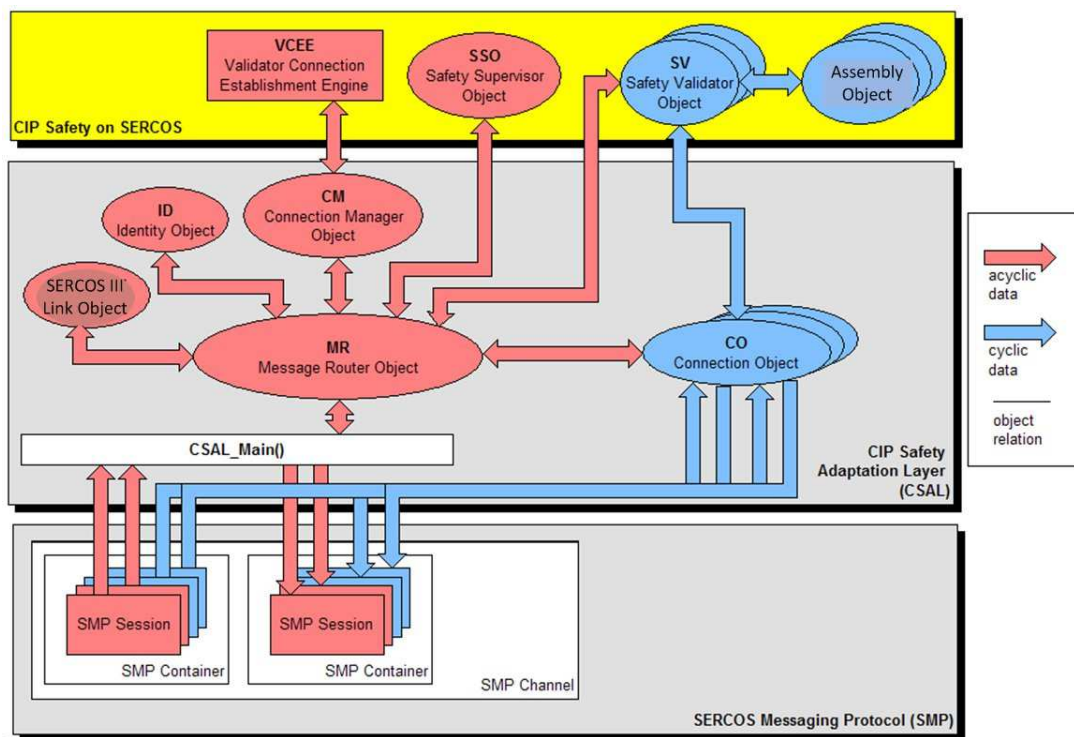
8.13.4.3 Connexions à multidestinataires

Les connexions MS (maître-esclave) CP 16/3 doivent servir uniquement à réaliser des connexions de sécurité point à point. Les connexions CC (communication transversale) CP 16/3 peuvent être utilisées pour réaliser des connexions de sécurité point à point ou multipoints.

8.13.4.4 Couche d'adaptation FSCP 2/1 pour Services CIP

Le CP 16/3 ne prend pas en charge le Protocole industriel commun (CIP). Par conséquent, l'adoption de FSCP 2/1 comme couche de sécurité pour les appareils CP 16/3 crée la nécessité d'une couche d'adaptation qui met en œuvre un ensemble de base de services et objets CIP.

Les objets et services offerts par la couche d'adaptation FSCP 2/1 représentée à la Figure 88 ne font pas partie du protocole de sécurité proprement dit. Par conséquent, il n'est pas nécessaire que ces services soient effectués avec une haute intégrité. La couche d'adaptation FSCP 2/1 peut être considérée comme partie intégrante du canal noir.



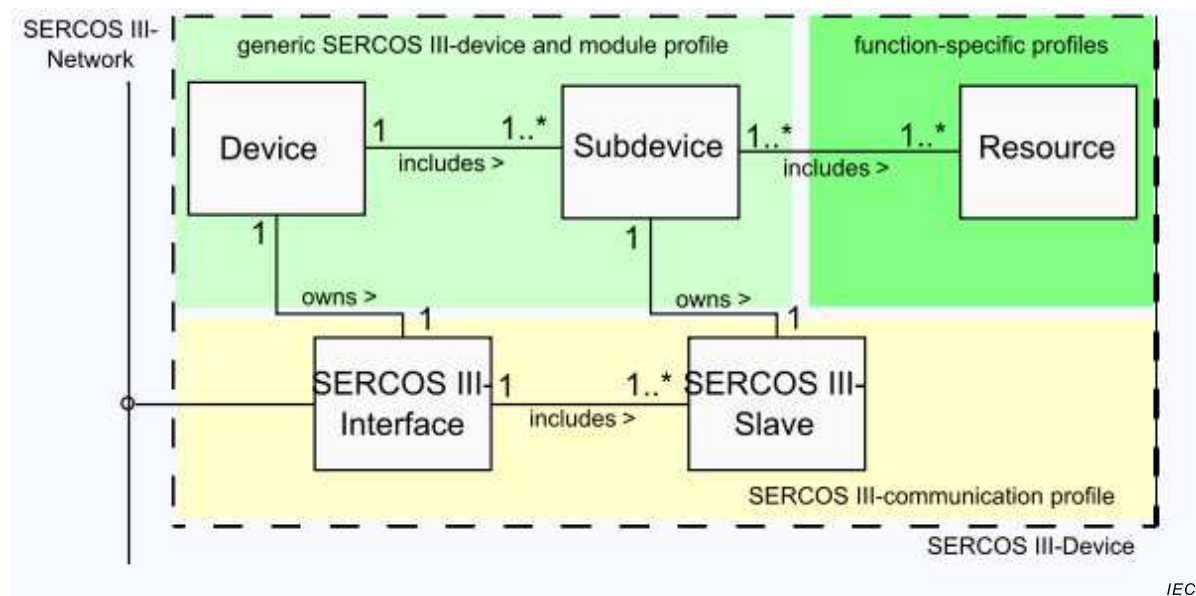
IEC

Anglais	Français
CIP safety on SERCOS	Sécurité CIP de SERCOS
Validator connection establishment engine	Unité d'établissement de connexion de l'objet de validation
Safety supervisor object	Objet Programme de contrôle de sécurité
Safety validator object	Objet de validation de sécurité
Assembly object	Objet Ensemble
SERCOS III link object	Objet liaison SERCOS III
Identity object	Objet Identité
Connection manager object	Objet Gestionnaire de connexion
Message router object	Objet Routeur de messages
Connection object	Objet de connexion
SMP session	Session SMP
SMP container	Conteneur SMP
SMP channel	Canal SMP
CIP Safety adaptation layer	Couche d'adaptation de sécurité CIP
SERCOS messaging protocol	Protocole de messagerie SERCOS
Acyclic data	Données acycliques
Cyclic data	Données cycliques
Object relation	Relation entre objets

Figure 88 – Couche d'adaptation FSCP 2/1

8.13.5 FSCP 2/1 et modèle d'appareil CP 16/3

La Figure 89 indique les composants d'un appareil CP 16/3 générique. Les composants relatifs à la communication sont nettement distincts des composants relatifs aux appareils. Les composants relatifs à la communication sont définis dans le profil de communication CP 16/3 (SCP). Le composant d'interface CP 16/3 représente l'interface physique avec le réseau CP 16/3, tandis que le composant esclave CP 16/3 fournit une interface logique avec une adresse esclave CP 16/3 unique pour le réseau CP 16/3. Cette structure permet une conception d'appareil modulaire comprenant plusieurs sous-appareils qui partagent une seule interface physique.



Anglais	Français
SERCOS III-network	réseau SERCOS III
generic SERCOS III-device and module profile	appareil SERCOS III générique et profil de module
function-specific profiles	profils spécifiques à la fonction
device	appareil
includes	comprend
subdevice	sous-appareil
resource	ressource
owns	détient
SERCOS III-interface	interface SERCOS III
SERCOS III-Slave	esclave SERCOS III
SERCOS III-communication profile	profil de communication SERCOS III
SERCOS III-Device	appareil SERCOS III

Figure 89 – Modèle d'appareil CP 16/3

Dans ce contexte, une «conception modulaire» n'implique la modularité du matériel de l'appareil. Un appareil monolithique peut intrinsèquement être considéré comme modulaire s'il comporte plusieurs sous-appareils indépendants. Par exemple, un contrôleur d'entraînement en CA à deux axes peut intrinsèquement être modélisé comme un appareil unique comportant deux sous-appareils indépendants avec deux adresses CP 16/3 différentes, qui sont connectés au réseau CP 16/3 via la même interface.

Dans la terminologie CP 16/3, la fonctionnalité de sécurité est modélisée comme un profil spécifique à la fonction qui met en œuvre une ou plusieurs ressources dans un sous-appareil.

Ceci implique qu'un appareil CP 16/3 peut comporter plusieurs appareils de sécurité indépendants tels que définis par la présente partie. Dans la mesure où il existe une différence essentielle entre un «appareil» et un «appareil de sécurité» dans le contexte CP 16/3, il convient de veiller à ne pas confondre ces termes.

Les appareils E/S modulaires sont modélisés comme un appareil CP 16/3 unique qui comporte habituellement un seul sous-appareil. Chaque module E/S est représenté par un ensemble de groupes de fonctions dans ce sous-appareil.

8.13.6 Attribution de l'UNID sur CP 16/3

8.13.6.1 Généralités

Le profil FSCP 2/1 exige l'attribution à l'échelle de l'usine d'un ID de nœud unique (UNID) à chaque appareil de sécurité. L'UNID à 10 octets comprend un Numéro de réseau de sécurité (SNN) à 6 octets combiné avec le NodeID à 4 octets du nœud (MACID sur CP2/3, adresse IP sur CP 2/2, SDID sur CP 16/3).

Pour un appareil de sécurité CP 16/3, un ID d'appareil de sécurité CP 16/3 à 4 octets (SDID) doit se substituer à la partie adresse MACID/IPNodeID de l'UNID. Les SDID et SNN doivent tous deux être archivés comme attributs de l'objet CP 16/3.

```
struct UNID
{
    S_SNNDate_AND_Time    SNN;
    UDINT                 SDID;
}
```

8.13.6.2 ID d'appareil de sécurité CP 16/3

Le 8.13.5 consacré au modèle d'appareil CP 16/3 a montré que l'adresse de nœud de réseau (adresse esclave CP 16/3) ne permet pas d'identifier de manière unique un module de sécurité dans un appareil modulaire.

D'autre part, l'exclusion de l'adresse de nœud de réseau de la partie NodeID de l'UNID entraîne une meilleure séparation entre la configuration d'appareil normalisée et la configuration de sécurité. Cette séparation facilite la mise en service des appareils, dans la mesure où un module peut être déplacé vers un lieu physique différent après vérification et verrouillage de la configuration de sécurité. Seules les parties de la configuration non relatives à la sécurité doivent être adaptées à la nouvelle topologie de réseau en changeant les adresses CP 16/3. La couche de sécurité permet toujours de s'assurer de l'établissement des seules connexions de sécurité configurées pour cet appareil de sécurité.

Par conséquent, dans un réseau CP 16/3, la partie MACID de l'UNID doit être choisie par l'outil de configuration ou définie dans l'appareil de sécurité par d'autres moyens (par exemple, commutateurs DIP), et ne doit être associée ni à l'adresse de nœud de réseau normalisé, ni à la position physique d'un module sur le bus local de l'appareil.

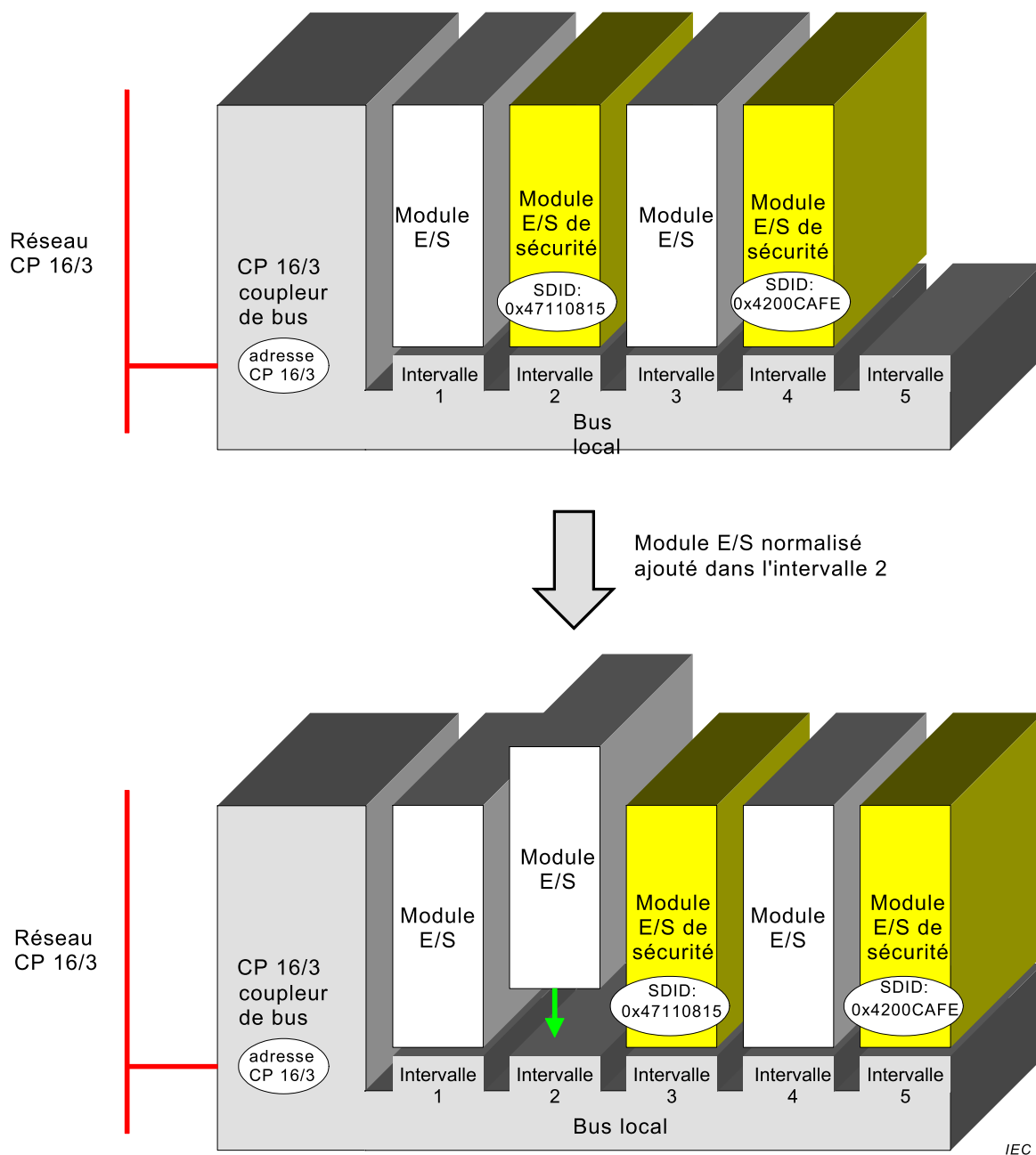


Figure 90 – Ajout d'un module normalisé à un appareil modulaire

Il faut s'assurer également du déplacement vers le nouvel emplacement du câblage fixé à un module, lors du déplacement d'un module de sécurité sans actualisation de la configuration du réseau de sécurité. Le fabricant d'un FSCP 2/1 sur un appareil CP 16/3 doit veiller à ce déplacement par des moyens appropriés ou par l'ajout de recommandations tout aussi appropriées dans le manuel de sécurité de l'appareil.

8.13.6.3 Attribution de numéros de réseau de sécurité

Le FSCP 2/1 exige l'attribution de numéros de réseau de sécurité (SNN) dans tous les modules FSCP 2/1 sur les nœuds CP 16/3. Les SNN et MACID forment ensemble l'UNID qui doit être unique pour chaque appareil d'un système de sécurité. Une valeur SNN ne se limite pas au périmètre d'un réseau CP 16/3 unique étant donné que la partie SDID de l'UNID n'est

pas associée à l'adresse de réseau normalisé d'un appareil de sécurité. Plusieurs réseaux CP 16/3 peuvent utiliser le même SNN tant qu'ils appartiennent au même segment de configuration (un groupe de réseaux CP 16/3 configurés par un seul outil de configuration). L'outil de configuration doit être chargé de l'attribution de différentes valeurs SDID à tous les appareils de sécurité dans un seul segment de configuration.

9 Exigences système

9.1 Voyants et commutateurs

9.1.1 Exigences générales concernant les voyants

Les appareils de sécurité FSCP 2/1 doivent comporter des voyants de module et de réseau.

Les développeurs d'appareils peuvent tout à fait équiper leurs produits de voyants supplémentaires s'ils le souhaitent.

Important: Les appareils de sécurité FSCP 2/1 doivent fournir une LED d'état de module et une LED d'état de réseau distinctes. Dans ce cas, ces voyants fournissent à l'utilisateur des informations relatives à la sécurité supplémentaires importantes qui ne peuvent être obtenues avec un voyant État de réseau/module combiné.

Important: En cas de problème lié au positionnement de la LED sur «Arrêt» (couleur rouge) ou sur «Marche» (couleur verte), il convient de positionner cette dernière sur «Arrêt» (rouge).

9.1.2 Indications LED pour le paramétrage de l'UNID des appareils

Le Tableau 115 définit la méthode d'utilisation des indications LED pour le paramétrage de l'UNID.

Tableau 115 – Indications LED pour le paramétrage de l'UNID

État/Événement du Programme de contrôle de sécurité	LED MOD	LED RES
Autovérification	Clignotement Rouge/vert	Arrêt
Attente de TUNID	Clignotement Rouge/vert	Dépendant de la connexion
Attente de TUNID Proposed UNID Rcvd	Clignotement Rouge/vert	Clignotement Rouge/vert 250 ms / 250 ms Réutilisation du modèle de groupe 4 CP 2/3
Configuration	Clignotement Rouge/vert	Dépendant de la connexion
Repos	Vert clignotant	Dépendant de la connexion
Exécution	Vert	Dépendant de la connexion

9.1.3 LED État du module

Cette LED bicolore (vert/rouge) fournit l'état de l'appareil. Elle indique si ce dernier est sous tension ou non et s'il fonctionne correctement. Le Tableau 116 définit les états de la LED État du module. Ce tableau définit les conditions de la LED État du module pour les appareils de sécurité (il faut que l'objet Programme de contrôle de sécurité soit utilisé). Les états indiqués reflètent les états d'appareil spécifiés dans l'objet Identité. Ces états sont également mis en correspondance avec les états définis dans l'objet Programme de contrôle de sécurité.

Pour les appareils de sécurité qui utilisent l'interface SNCT, les états du Programme de contrôle de sécurité doivent constituer ce qui détermine l'état de la LED Module.

Tableau 116 – LED État du module

Pour l'état du Programme de contrôle de sécurité:	La LED est:	Pour indiquer:
Aucune alimentation	Arrêt	Aucune alimentation de l'appareil
Exécution	Vert	L'appareil fonctionne normalement
Repos	Vert clignotant ^a	L'appareil est au repos ou en attente. Référencement de l'objet Identité (6.4) ou de l'objet Programme de contrôle de sécurité (6.5.3) ^b
Abandon	Rouge clignotant ^a	Anomalie récupérable
Anomalie critique	Rouge	L'appareil présente une anomalie non récupérable, son remplacement peut se révéler nécessaire
Autovérification de l'appareil, Waiting_for_TUNID ou Configuration ²	Rouge/Vert clignotant ^a	L'appareil fait l'objet d'une autovérification ou doit être mis en service en raison de l'absence ou du caractère incomplet ou incorrect de la configuration ou de l'UNID ^c . Référencement de l'objet Identité (6.4) ou de l'objet Programme de contrôle de sécurité (6.5.3) ^b
^a La fréquence de clignotement est environ de 1 clignotement par seconde. Il convient que la LED soit allumée pendant 0,5 s ou éteinte pendant environ 0,5 s. ^b L'objet Programme de contrôle de sécurité détermine l'état des appareils de sécurité. ^c Il convient qu'un appareil de sécurité non configuré/sans propriétaire ne soit pas autorisé à continuer de fonctionner lorsqu'il est connecté à un système de sécurité actif.		

9.1.4 Avertissement lié aux voyants

Le manuel de sécurité pour l'utilisateur doit comporter un avertissement qui stipule que les «LED NE sont PAS des voyants fiables et qu'il n'est pas certain qu'elles fournissent des informations précises». Il convient d'utiliser les LED UNIQUEMENT pour un diagnostic général lors de la mise en service ou de la recherche d'anomalies. Ne pas tenter d'utiliser les LED comme voyants opérationnels».

9.1.5 LED État de réseau

Cette LED bicolore (vert/rouge) indique l'état de la liaison de communication. Les indications propres à cette LED sont définies dans le Tableau 117.

Tableau 117 – États de la LED État de réseau

Pour l'état du Programme de contrôle de sécurité:	La LED est:	Pour indiquer:
Hors tension/connexion	Arrêt	L'appareil est hors connexion. L'appareil n'a pas encore subi l'essai Dup_MAC_ID. Il se peut que l'appareil ne soit pas sous tension, examiner la LED État du module
Connecté, non connecté	Vert clignotant ^a	L'appareil est connecté, mais aucune connexion n'est effectivement établie. L'appareil a satisfait à l'essai Dup_MAC_ID, est connecté, mais il n'existe aucune connexion établie avec d'autres nœuds. Pour un appareil du seul groupe 2, cela signifie que cet appareil n'est pas attribué à un maître. Pour un appareil de capacité UCMM, cela signifie que l'appareil ne comporte aucune connexion établie. Pour les appareils de sécurité, une connexion peut être établie, mais l'Objet de validation n'a pas procédé à un échange initial de coordination temporelle
Liaison OK, en ligne, connecté	Vert	L'appareil est en ligne, avec des connexions effectivement établies.
Temporisation de connexion	Rouge clignotant ^a	Une connexion E/S ou plus est (sont) dans l'état Temporisation
Défaillance de liaison critique	Rouge	Défaillance de l'appareil de communication. L'appareil a détecté une erreur qui lui a interdit toute communication sur le réseau
Défaillance de communication et réception d'une demande d'identification de défaillance de communication – Réception d'un protocole long ou d'un service Propose_TUNID.	Rouge/Vert clignotant	Appareil spécifique en état "défaillance de communication". L'appareil a détecté une erreur d'accès au réseau et son état est «Défaillance de communication». L'appareil a ensuite reçu et accepté un message de demande d'identification de défaillance de communication – Protocole long. Les appareils de sécurité utilisent cette indication pour permettre au personnel de maintenance de mettre en service l'UNID dans un appareil de sécurité.
^a La fréquence de clignotement est environ de 1 clignotement par seconde. Il convient que la LED soit allumée pendant 0,5 s ou éteinte pendant environ 0,5 s.		

9.1.6 Commutateurs

9.1.6.1 Commutateurs NodeID

L'algorithme suivant peut également être appliqué au traitement du commutateur de débit en bauds lorsqu'il est mis en œuvre. Lorsque des commutateurs mécaniques sont utilisés pour le paramétrage du NodeID et/ou du débit en bauds, la manière dont ces valeurs sont traitées dans les appareils de sécurité présente certaines différences. Le présent paragraphe 9.1.6 présente l'algorithme dans les grandes lignes.

Il existe une relation directe entre le paramétrage du NodeID et la partie NodeID de l'UNID cible (TUNID) dans le programme de contrôle de sécurité. Voir l'objet Programme de contrôle de sécurité (6.5.3) pour plus d'informations.

9.1.6.2 Détermination du NodeID

Les commutateurs NodeID sont lus par le micrologiciel de l'appareil lors de l'initialisation de ce dernier.

L'attribut NodeID (si pris en charge) de l'objet CP 2/3 doit toujours refléter la valeur utilisée.

La logique suivante s'applique:

- Lors de la lecture des commutateurs, si ces derniers spécifient un NodeID valide (valeur de NodeID comprise entre 0 et 63), cette valeur doit être utilisée comme le NodeID;
- Lors de la lecture des commutateurs, si le NodeID spécifié diffère de la valeur archivée dans l'attribut NodeID de l'objet CP 2/3 (valeurs NVRAM), le ou les attributs appropriés doivent être actualisés et sauvegardés dans la mémoire NVRAM;
- Lors de la lecture des commutateurs, si ces derniers spécifient un NodeID invalide (valeur supérieure à 63), il convient que l'appareil applique l'une des options recommandées dans l'IEC 62026-3;
- Lors de la lecture des commutateurs, si les commutateurs utilisés pour spécifier le NodeID sont réglés sur une valeur valide (valeur de NodeID comprise entre 0 et 63), l'attribut NodeID doit avoir un accès Obtenir uniquement;
- Lors de la lecture des commutateurs, si ces derniers sont réglés sur le mode programmable par logiciel (>63 pour le NodeID), l'attribut NodeID doit avoir un accès Définir;
- Lorsqu'un appareil ne comporte pas de commutateur, il doit utiliser les valeurs par défaut pour le NodeID dans sa configuration out-of-box (63 pour le NodeID). Pour FSCP 2/1 sur CP 16/3, il faut que le SDID dans l'objet Liaison SERCOS III soit réglé sur des valeurs par défaut;
- Lorsque l'appareil est out-of-box, il doit utiliser les paramétrages de commutateur NodeID courants si ces derniers sont des valeurs valides.

Les appareils de sécurité doivent contrôler et détecter les variations de la valeur NodeID ou des paramétrages de l'attribut IP et du commutateur de débit en bauds (le cas échéant). Les développeurs ont toute liberté de déterminer une période de prélèvement appropriée pour cette détection.

En cas de détection d'un changement de paramétrage du commutateur NodeID, l'appareil doit actualiser l'attribut MACID_Switch_Value. Lorsque le commutateur NodeID équivaut au NodeID utilisé ou lorsque les commutateurs NodeID sont supérieurs à la valeur 63 et réglables par logiciel, supprimer l'attribut modifié par le NodeID et ne pas modifier l'état de l'appareil; dans le cas contraire, définir l'attribut modifié par le NodeID et passer à l'état ABANDON (voir organigramme à la Figure 91).

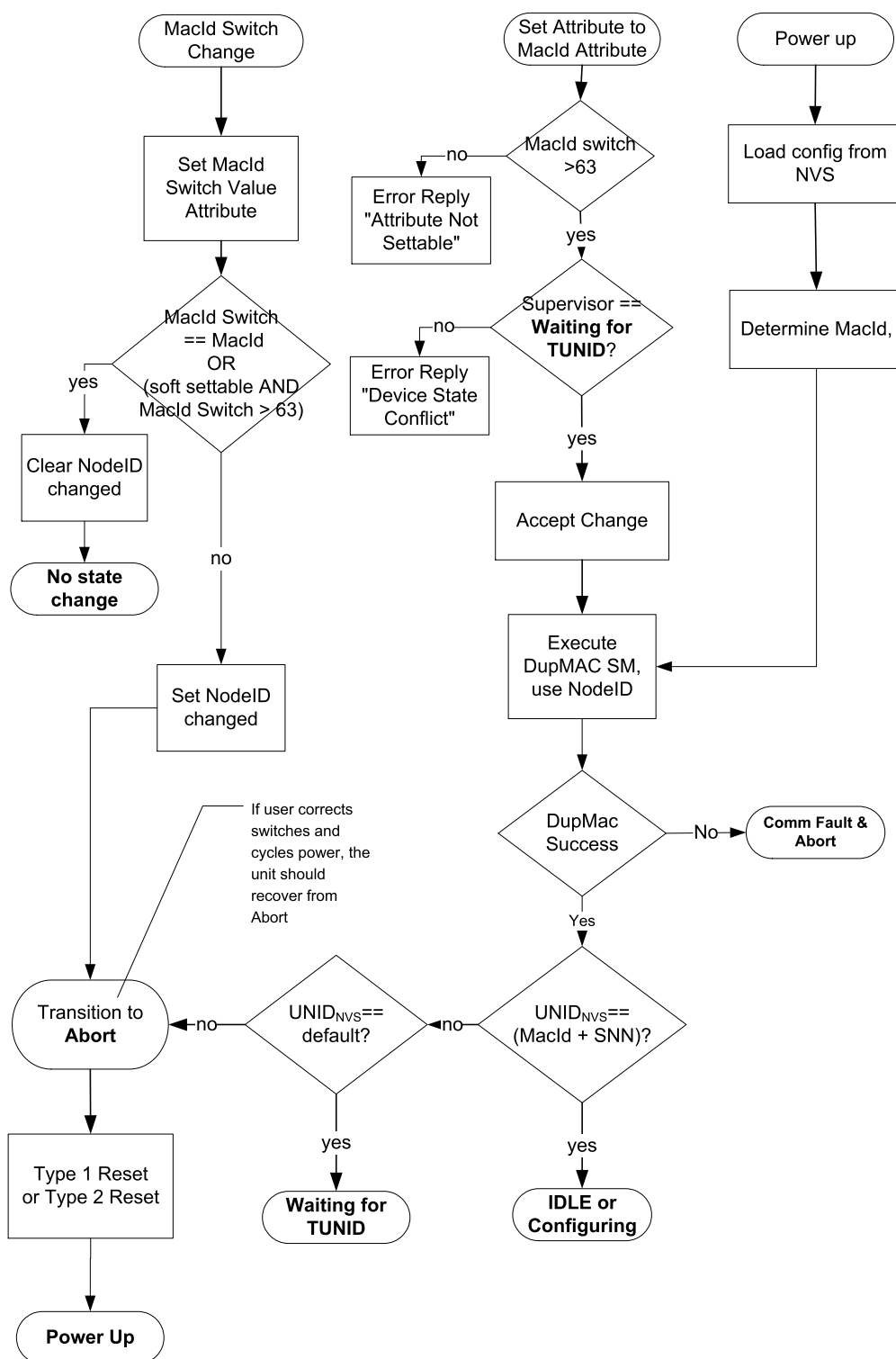
Lorsqu'un changement de paramétrage de commutateur IP est détecté, il doit être déterminé si ce changement génère une condition de défaut d'adaptation. Si le commutateur IP est différent de l'attribut Adresse IP, il doit passer à l'état ABANDON.

En cas de détection d'un changement de paramétrage du commutateur de débit en bauds, l'appareil doit actualiser l'attribut Baud_Rate_Switch_Changed et l'attribut Baud_Rate_Switch_Value, puis passer à l'état ABANDON.

Si un appareil de sécurité FSCP 2/1 prend en charge le service Set_Attribute pour l'attribut NodeID, et si les commutateurs NodeID sont réglés de manière à activer le service défini, les appareils de sécurité doivent accepter uniquement le Set_Attribute tout en étant dans l'état

“Attente du TUNID”. Dans le cas contraire, l'appareil doit répondre par un «Conflit d'état d'appareil».

Si un appareil de sécurité FSCP 2/1 prend en charge le service Set_Attribute pour l'attribut Débit en bauds, les appareils de sécurité doivent accepter uniquement le Set_Attribute tout en étant dans l'état “Attente du TUNID”. Dans le cas contraire, l'appareil doit répondre par un «Conflit d'état d'appareil».



Anglais	Français
macid switch change	modification du commutateur MACID
set attribute to Macid attribute	régler l'attribut sur l'attribut Macid
power up	mise sous tension
set macid switch value attribute	régler l'attribut de valeur du commutateur Macid
no	Non
macid switch	commutateur Macid
error reply "attribute not settable"	réponse d'erreur "attribut non réglable"
load config from NVS	charger la config. depuis NVS
yes	Oui
OR	OU
(soft settable AND	réglable par logiciel ET
error reply "device state conflict"	réponse d'erreur "conflit d'état d'appareil"
supervisor	programme de contrôle
waiting for TUNID?	attente du TUNID?
determine Macid	déterminer le MACID
clear NodeID changed	supprimer le NodeID modifié
accept change	accepter la modification
no state change	pas de changement d'état
execute DupMac SM, use NodeID	exécuter SM DupMac, utiliser NodeID
set NodeID changed	régler le NodeID modifié
if user corrects switches and cycles power, the unit should recover from Abort	si l'utilisateur corrige les commutateurs et l'alimentation des cycles, il convient que l'unité récupère de l'état Abandon
DupMac success	DupMac satisfaisant
comm fault & abort	anomalie comm & abandon
transition to Abort	transition vers Abandon
default?	par défaut?
type 1 reset or type 2 reset	réinitialisation de type 1 ou 2
idle or configuring	Repos ou configuration
power up	mise sous tension

Figure 91 – Logique de traitement du NodeID des appareils de sécurité

9.1.6.3 Commutateur de réinitialisation

Si un appareil de sécurité comporte un commutateur de réinitialisation, il doit exécuter une réinitialisation de type 2 du Programme de contrôle de sécurité (c'est-à-dire réinitialisation à l'état out-of-box, mais conservation du mot de passe).

9.2 Lignes directrices d'installation

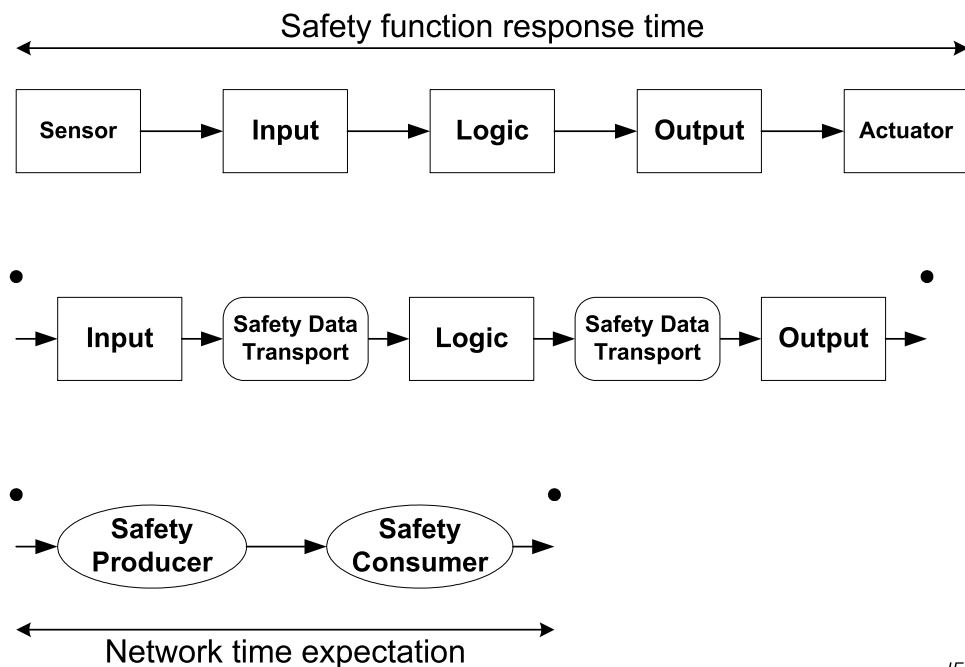
Les lignes directrices d'installation de l'IEC 61918 et de l'IEC 61784-5-2 pour la CPF 2 doivent s'appliquer.

9.3 Temps de réponse de la fonction de sécurité

9.3.1 Présentation générale

Le temps de réponse de la fonction de sécurité correspond au temps le plus défavorable qui s'écoule entre un événement relatif à la sécurité comme élément d'entrée du système ou

comme anomalie du système, jusqu'au moment où le système est dans un état de sécurité. La portée du temps de réaction est définie à la Figure 92.



IEC

Anglais	Français
safety function response time	temps de réponse de la fonction de sécurité
sensor	Capteur
input	Entrée
logic	Logique
output	Sortie
actuator	actionneur
safety data transport	transport de données de sécurité
safety producer	producteur de sécurité
safety consumer	consommateur de sécurité
network time expectation	délai du réseau

Figure 92 – Temps de réponse de la fonction de sécurité

Pour déterminer le temps de la fonction de sécurité de toute chaîne de commande, l'utilisateur doit additionner les composants de la chaîne de sécurité.

Selon l'exemple de la Figure 92, le temps de réponse de la fonction de sécurité serait le suivant:

$$\begin{aligned}
 \text{Temps de réponse de la fonction de sécurité} = & \text{Temps de réaction du capteur} \\
 & + \text{Temps de réaction de l'entrée} \\
 & + \text{Temps de réaction du réseau} \\
 & + \text{Temps de réaction du contrôleur} \\
 & + \text{Temps de réaction du réseau} \\
 & + \text{Temps de réaction de la sortie} \\
 & + \text{Temps de réaction de l'actionneur}
 \end{aligned}
 \quad (13)$$

9.3.2 Délai du réseau

Partie du temps de réponse de la fonction de sécurité. Le délai du réseau correspond au temps le plus défavorable, entre le moment de la saisie des données par le producteur de données de sécurité et le moment où l'application de consommation reconnaît un état de sécurité. Ceci inclut également les erreurs de production et de consommation.

Le `Network_Time_Expectation_Multiplier` utilisé dans les paragraphes précédents de la présente partie, représente le temps mesuré le plus défavorable entre le moment de la saisie des données par le producteur de données de sécurité et le moment où l'application de consommation reconnaît l'indication d'un état de sécurité.

La valeur `Network_Time_Expectation_Multiplier` nécessaire pour s'assurer de la non-détection d'une erreur de temporisation est la suivante:

$$\begin{aligned} \text{Network\_Time\_Expectation\_Multiplier} > & \text{EPI} \times \text{Timeout\_Multiplier} & (14) \\ & + \text{Safety\_Message\_Time(max)} \\ & + \text{Time\_Coord\_Message\_Time(max))} / 128 \mu\text{s} \\ & + \text{Connection\_Correction\_Constant} \end{aligned}$$

où:

`Safety_Message_Time(max)` est le temps réel entre la saisie des données par le producteur de données de sécurité et le moment du transfert de ces données à l'application de consommation en vue de leur utilisation.

`Time_Coord_Message_Time(max)` est le temps maximum potentiel de transmission des informations de coordination temporelle entre le consommateur et le producteur. Ce temps maximum est mesuré entre le moment de la saisie de `Consumer_Clk_Count` sur `Consumer_Time_Value` et le moment de la saisie de `Producer_Clk_Count` sur `Producer_Rcvd_Time_Value`.

`Timeout_Multiplier` est un paramètre exigé par le traitement du protocole de sécurité. Cette valeur détermine le nombre de messages susceptibles d'être perdus préalablement à toute déclaration d'erreur de connexion. Un `Timeout_Multiplier` de 1 indique qu'aucun message ne peut être perdu. Un `Timeout_Multiplier` de 2 indique que 1 message peut être perdu, etc. Outre les contrôles de `Timeout_Multiplier` dans le cadre du protocole, des contrôles du temps de réaction sont également effectués. Une valeur par défaut raisonnable du `Timeout_Multiplier` serait une valeur égale à 2. Une limite raisonnable consisterait, pour le logiciel de configuration, à restreindre le `Timeout_Multiplier` à des valeurs entières comprises entre 1 et 4. Pour le `ExtendedFormat`, la valeur du `Timeout_Multiplier` peut être portée à 255 tant que la valeur de délai du réseau ne dépasse pas 5,8 s.

`Connection_Correction_Constant` est une valeur d'incrément de 128 μs soustraite de la datation afin de représenter l'erreur la plus défavorable due à la dérive temporelle, la nature asynchrone des horloges du producteur et du consommateur, et le temps minimal de transfert du message de coordination temporelle entre le consommateur et le producteur.

`Timeout_Multiplier` et `Connection_Correction_Constant` sont décrits en 7.7.5.8 et 7.7.5.15 respectivement.

9.3.3 Équation de calcul des temps de réaction du réseau

L'emplacement le plus logique de définition et de détermination des temps de réaction du réseau par l'utilisateur est l'appareil logique, dans la mesure où ce dernier est très vraisemblablement le support de configuration et le point d'origine de connexion.

Il existe deux cas de temps de réaction de connexion de sécurité pour la plupart des appareils logiques. Il s'agit:

- du temps de réaction des connexions d'entrée;

- du temps de réaction des connexions de sortie.

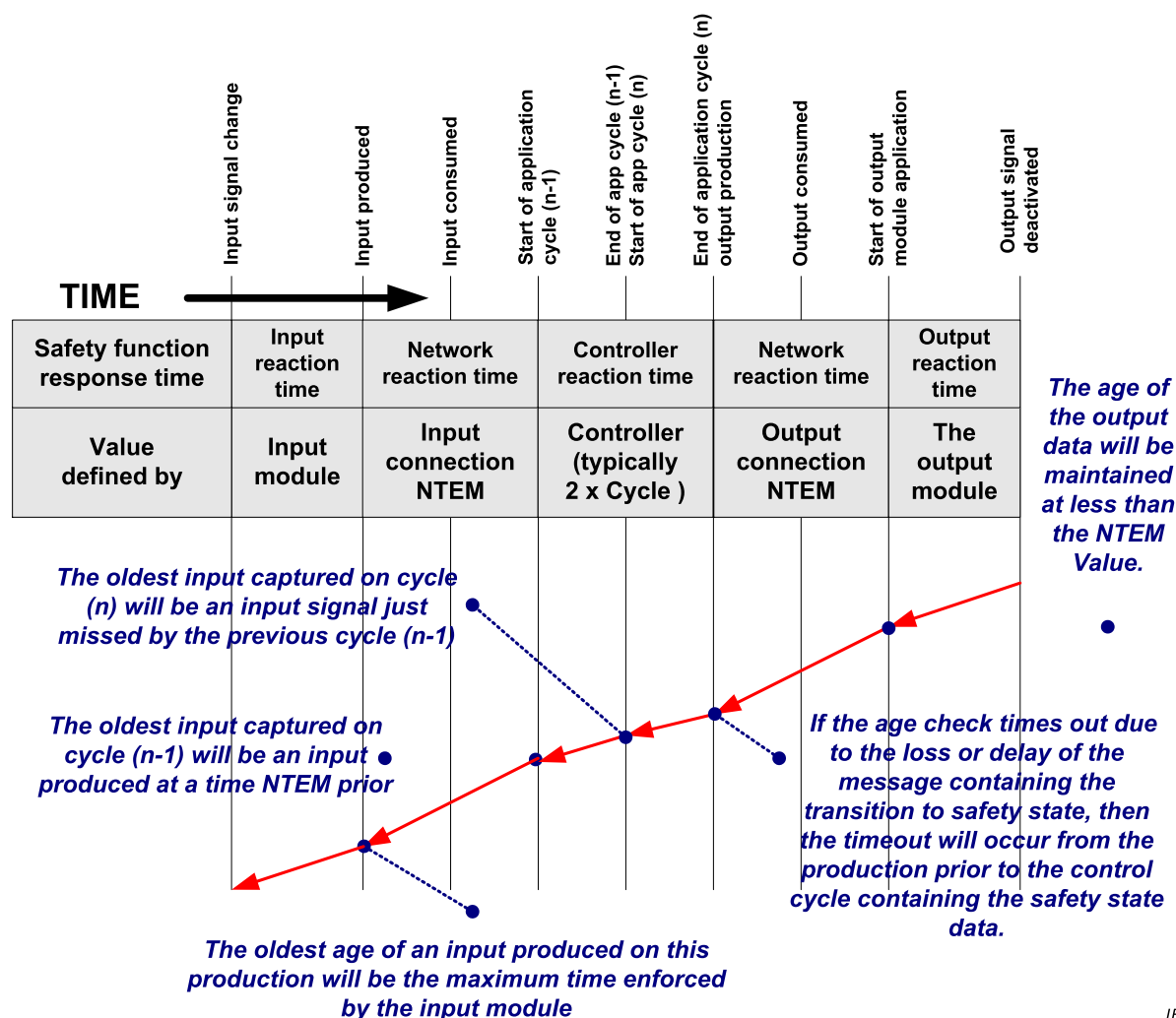
Le Tableau 118 définit les applications de production et de consommation pour les cas de temps de réaction de réseau susmentionnés.

Tableau 118 – Type de temps de réaction de connexion – applications de production/consommation

Type de temps de réaction de connexion	Application de production	Application de consommation
Entrée de sécurité	Module d'entrée	Contrôleur
Sortie de sécurité	Contrôleur	Module de sortie

La Figure 93 présente l'analyse des composantes du temps de réponse de la fonction de sécurité. L'analyse d'application temporelle s'effectue entre le retour du signal de sortie vers le signal d'entrée. Cette analyse permet d'observer les effets des productions asynchrones.

L'analyse pose l'hypothèse de l'existence d'un cycle interne au module de sortie qui vérifie l'âge des dernières données de sortie reçues. L'âge de ces données de sortie est maintenu à une valeur inférieure à la valeur Network_Time_Expectation_Multiplier (NTEM).



Anglais	Français
input signal change	modification du signal d'entrée

Anglais	Français
input produced	entrée produite
input consumed	entrée consommée
start of application cycle	début du cycle d'application
end of app. cycle	fin du cycle d'application
output production	production de sortie
start of output module application	début d'application du module de sortie
output signal deactivated	signal de sortie désactivé
TIME	TEMPS
safety function response time	temps de réponse de la fonction de sécurité
input reaction time	temps de réaction de l'entrée
network reaction time	temps de réaction du réseau
controller reaction time	temps de réaction du contrôleur
output reaction time	temps de réaction de la sortie
value defined by	valeur définie par
input module	module d'entrée
input connection NTEM	NTEM de connexion d'entrée
controller	contrôleur
typically	généralement
output connection	connexion de sortie
the output module	le module de sortie
the age of the output data will be maintained at less than the NTEM value	l'âge des données de sortie est maintenu à une valeur inférieure à la valeur NTEM
the oldest input captured on cycle (n) will be an input signal just missed by the previous cycle (n-1)	l'entrée la plus ancienne saisie sur le cycle (n) est un signal d'entrée omis par le cycle précédent (n-1)
the oldest input captured on cycle (n-1) will be an input produced at a time NTEM prior	l'entrée la plus ancienne saisie sur le cycle (n-1) est une entrée produite à un temps NTEM précédent
if the age check times out due to the loss or delay of the message containing the transition to safety state, then the timeout will occur from the production prior to the control cycle containing the safety data	si le contrôle de l'âge est temporisé du fait de la perte ou du retard du message contenant la transition vers l'état de sécurité, la temporisation a lieu à partir de la production précédant le cycle de contrôle contenant les données d'état de sécurité
the oldest age of an input produced on this production will be the maximum time enforced by the input module	l'âge le plus ancien d'une entrée produite sur cette production est égal au temps maximal appliqué par le module d'entrée

Figure 93 – Composantes du temps de réponse de la fonction de sécurité

D'un point de vue analytique, une connexion entre contrôleurs serait traitée de la même manière qu'une connexion d'entrée.

Pour une connexion d'entrée ou entre contrôleurs:

$$\text{Temps de réaction du réseau} = \text{Network\_Time\_Expectation\_Multiplier} \times 128 \mu\text{S} \quad (15)$$

Pour une connexion à un module de sortie:

Si la production de sortie est asynchrone avec le cycle du contrôleur:

$$\text{Temps de réaction du réseau} = \text{Network\_Time\_Expectation\_Multiplier} \times 128 \mu\text{S} \quad (16)$$

Si la production de sortie est synchrone avec le cycle du contrôleur:

$$\text{Temps de réaction du réseau} = \text{Network\_Time\_Expectation\_Multiplier} \times 128 \mu\text{S} - \text{EPI\_in\_Sec} \quad (17)$$

Les cas de connexion de sortie peuvent être simplifiés comme suit:

$$\text{Temps de réaction du réseau} = \text{Multiplicateur de délai de réseau} \times 128 \mu\text{S} + (\text{EPI\_in\_Sec} \times (\text{ASYNC} - 1)) \quad (18)$$

où le paramètre ASYNC est défini comme suit:

paramètre ASYNC

Si l'application de production est synchrone avec la production de données, ASYNC = 0. Si l'application de production est asynchrone avec la production de données, ASYNC = 1. L'effet réseau de cette différence réside dans l'ajout d'un EPI supplémentaire au temps de réaction du réseau pour les appareils asynchrones. Il convient de fournir ce paramètre ASYNC au logiciel de configuration de sécurité via une entrée de fichier EDS. La valeur par défaut dans les cas où ce paramètre n'est pas fourni, doit être 0.

9.4 Durée des demandes (ou sollicitations)

La durée de la demande entre l'application relative à la sécurité et la couche de communication de sécurité doit être suffisante de manière à ce que l'EPI le plus long sélectionné par l'application puisse détecter cette demande.

9.5 Contraintes liées au calcul des caractéristiques du système

9.5.1 Nombre de nœuds

Les mises en œuvre de type CP 2/3 se limitent à un nombre maximum de 32 nœuds de production et de 32 nœuds de consommation pour ce profil de sécurité. Les mises en œuvre de type CP 2/2 ne comportent pas de limites concernant le nombre de producteurs et de consommateurs pour ce même profil.

9.5.2 PFH de réseau

Le présent paragraphe 9.5.2 décrit les calculs qui permettent de déterminer la PFH du réseau. Les systèmes SIL3 constituent la cible du réseau. La PFH doit par conséquent être $<10^{-9}$ (ou $<10^{-7}$ si les calculs intègrent un facteur de 1 %).

Le protocole de réseau de sécurité comprend quatre parties, à savoir, les données de sécurité, les informations de datation, les informations concernant la correction de temps multipoints et la réponse à demande Ping de coordination temporelle. Chacune de ces parties a sa propre protection qui contribue à la PFH.

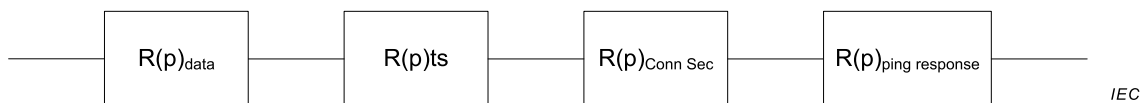


Figure 94 – Schéma de principe de fiabilité de protocole de réseau (RBD)

Selon le schéma de principe de la Figure 94, l'équation applicable au taux d'erreurs résiduelles de réseau global est la suivante:

$$R(p)T = R(p) \text{ data} + R(p)ts + R(p)\text{time coord} + R(p) \text{ time\_corr} \quad (19)$$

Lorsque les taux d'erreurs résiduelles sont appliqués dans le calcul de la PFH, il est important de tenir compte du fait que les informations concernant la coordination temporelle et la correction de temps multipoints sont transmises à des taux autres que le taux de transmission de la datation et des données. Sur la base des différents taux de transmission et des informations issues du schéma de principe, l'équation de calcul de la PFH globale pour une connexion point à point est la suivante:

$$\Lambda = 3\,600 \times (((R(p)t_s + R(p)t_{data}) \times v_{msg}) + (R(p)t_{coord} \times v_{ping})) \times (NoProd - 1) \times 100 \quad (20)$$

où

v_{msg}	est le taux de transmission en messages/seconde
v_{ping}	est le taux de transmission en messages/seconde
NoP	est le nombre de producteurs
3 600	est la conversion des heures en secondes
100	est le facteur de 1%

L'équation PFH pour une PFH multipoints est la suivante:

$$\Lambda = 3\,600 \times (((R(p)t_s + R(p)t_{data}) \times v_{msg} \times NoP) + ((R(p)t_{coord} + R(p)t_{corr}) \times v_{ping} \times NoC/P)) \times 100 \quad (21)$$

où

v_{msg}	est le taux de transmission en messages/seconde
v_{ping}	est le taux de transmission en messages/seconde
NoC/P	est le nombre de consommateurs par producteur
NoP	est le nombre de producteurs
3 600	est la conversion des heures en secondes
100	est le facteur de 1%

La Figure 95 et la Figure 96 récapitulent le résultat le plus défavorable. Les nombres sont obtenus à partir des calculs détaillés et des équations ci-dessus.

Entrées			
Intervalle de paquets attendu (EPI)		0,010	Secondes
Intervalle Ping		1,000	Secondes
Nombre de nœuds (m)		63	
Consommateurs multipoints		15	
Probabilité d'erreurs sur les bits		0,001	
Résultats			
		Point à point	Multipoints
R(p)data <= 2 octets	Section de données R(p) – 2 octets de données	$7,02 \times 10^{-20}$	$7,02 \times 10^{-20}$
R(p)data >= 3 octets	Section de données R(p) – 250 octets de données	$8,54 \times 10^{-19}$	$8,54 \times 10^{-19}$
R(p)data	Section de données R(p)	$8,54 \times 10^{-19}$	$8,54 \times 10^{-19}$
R(p)ts	Section de datation R(p)	$3,18 \times 10^{-18}$	$3,18 \times 10^{-18}$
R(p)multi	Message de correction de temps R(p)		$2,68 \times 10^{-18}$
R(p)reply	Message de coordination temporelle R(p)	$2,68 \times 10^{-18}$	$2,68 \times 10^{-18}$
Msg_per_sec	Messages par seconde = 1 / EPI	100	100
Rpl_per_sec	Réponses par seconde = 1 / Ping_Interval	1,00	1,00
	λ	$9,07 \times 10^{-9}$	$1,08 \times 10^{-8}$
	% d'objectif 1,00E-07, OK jusqu'à 100 %	9,07 %	10,80 %
	PFH = λ / 100	$9,07 \times 10^{-11}$	$1,08 \times 10^{-10}$
	% de SIL 3 (1,00E-07) limite PFD, OK jusqu'à 1 %	0,090 7 %	0,108 0 %

Figure 95 – Synthèse de la PFH de réseau

Entrées			
Intervalle de paquets attendu (EPI)		0,010	Secondes
Intervalle Ping		0,524	Secondes
Nombre de nœuds (m)		63	
Consommateurs multipoints		15	
Probabilité d'erreurs sur les bits		0,001	
Résultats			
		Point à point	Multipoints
R(p)data <= 2 octets	Section de données R(p) – 2 octets de données	$5,05 \times 10^{-22}$	$5,05 \times 10^{-22}$
R(p)data >= 3 octets	Section de données R(p) – 250 octets de données	$4,34 \times 10^{-25}$	$4,34 \times 10^{-25}$
R(p)data	Section de données R(p)	$5,05 \times 10^{-22}$	$5,05 \times 10^{-22}$
R(p)ts	Section de datation R(p)	$1,26 \times 10^{-22}$	$1,26 \times 10^{-22}$
R(p)multi	Message de correction de temps R(p)		$1,31 \times 10^{-18}$
R(p)reply	Message de coordination temporelle R(p)	$1,13 \times 10^{-18}$	$1,31 \times 10^{-18}$
Msg_per_sec	Messages par seconde = $1 / \text{EPI}$	100	100
Rpl_per_sec	Réponses par seconde = $1 / \text{Ping\_Interval}$	1,00	1,00
	λ	$2,66 \times 10^{-11}$	$8,18 \times 10^{-10}$
	% d'objectif 1,00E-07, OK jusqu'à 100 %	0,022 6 %	0,818 %
	PFH = $\lambda / 100$	$2,66 \times 10^{-13}$	$8,18 \times 10^{-12}$
	% de SIL 3 (1,00E-07) limite PFD, OK jusqu'à 1 %	0,000 3 %	0,008 2 %

Figure 96 – Synthèse de la PFH de format étendu

9.5.3 Taux d'erreurs sur les bits (BER)

9.5.3.1 Généralités

L'IEC 61784-3 exige l'application d'un taux d'erreurs sur les bits (BER) de 0,01 dans les calculs PDF/PFH, à moins qu'il ne soit démontré que ce BER n'est pas réalisable. Un BER de 0,01 signifie que 1 bit sur 100 bits transmis est transmis de manière incorrecte. Ceci constitue bien évidemment une condition non réaliste pour un réseau de systèmes de contrôle industriels dont la disponibilité doit être maintenue.

9.5.3.2 BER de CP 2/3

La taille de paquet minimale utilisée avec le protocole FSCP 2/1 dans les appareils CP 2/3 est de 108 bits. Un appareil CP 2/3 comporte un système de limitation extensive des erreurs et tous les nœuds d'un système CP 2/3 vérifient tous les messages à chaque transmission. En présence d'erreurs persistantes, un appareil CP 2/3 interrompt le bus (c'est-à-dire que le nœud cesse toutes les activités du réseau) et conserve cet état jusqu'aux cycles d'alimentation. Un système CP 2/3 cesse de fonctionner en présence d'un nombre élevé d'erreurs sur les bits en raison des vérifications généralisées et diverses et du traitement obligatoire des erreurs. Il peut être démontré qu'un réseau CP 2/3 ne peut pas fonctionner avec un BER supérieur à 0,001. L'incapacité à fonctionner est vraie pour les CP 2/3 et FSCP 2/1.

9.5.3.3 BER de CP 2/2

La taille de paquet minimale utilisée avec un protocole FSCP 2/1 dans un appareil CP 2/2 est de 720 bits, ce qui constitue une taille bien plus grande que la taille de 108 bits utilisée avec l'appareil CP 2/3. Tout comme l'appareil CP 2/3, l'appareil CP 2/2 ne fonctionne pas avec un BER supérieur à 0,001, bien que le mécanisme de vérification soit différent dans le cas de l'appareil CP 2/2. Ce dernier utilise le mécanisme de délai interne au protocole FSCP 2/1 afin de s'assurer de la remise des messages dans les délais impartis. La non-remise d'un message correct dans la période prévue entraîne la fermeture de la connexion et le transfert de l'appareil à l'état de sécurité. En présence de BER élevés (supérieurs à 0,001), la connexion de sécurité est fermée et le réseau n'est pas en mesure de fonctionner. Il n'est tout simplement pas disponible.

Justification pour le paramétrage d'un BER maximum à la valeur 0,001 pour un appareil CP 2/2:

- a) Si le pourcentage de paquets non remis correctement est suffisamment élevé, certains messages ne sont pas remis avant la temporisation de la connexion.
- b) Si la temporisation des connexions est fréquente, le réseau n'est pas disponible et ne peut pas être utilisé.
- c) Si un réseau n'est pas disponible, il est protégé.

9.5.3.4 Synthèse

Un $BER < 0,001$ conduit le protocole de sécurité à dépasser la limite temporelle de 7 RPI suffisamment souvent pour rendre le réseau non disponible pour toute utilisation pratique. Un $BER = 0,001$ a par conséquent été utilisé pour tous les calculs.

9.6 Maintenance

Il n'existe aucune exigence de maintenance particulière pour ce protocole.

9.7 Manuel de sécurité

Les ingénieurs d'application de la présente partie doivent fournir un manuel de sécurité contenant au minimum les informations suivantes:

- a) le manuel de sécurité doit informer les utilisateurs des contraintes liées au calcul des caractéristiques des systèmes, voir 9.5.
- b) le manuel de sécurité doit informer les utilisateurs de leurs responsabilités eu égard au paramétrage approprié de l'appareil, voir 8.9.
- c) le manuel de sécurité doit fournir des avertissements concernant la bonne utilisation des LED, voir 9.1.4.

Outre les exigences stipulées dans le présent paragraphe 9.7, le manuel de sécurité doit respecter toutes les exigences de l'IEC 61508.

10 Évaluation

Il est fortement recommandé aux ingénieurs d'application du FSCP 2/1 d'obtenir la vérification pour tous les aspects de sécurité fonctionnelle du produit, tant du protocole que de toute application, conformément aux exigences d'indépendance et de compétence spécifiées à l'Article 8 de l'IEC 61508-1:2010. Il est fortement recommandé aux ingénieurs d'application du FSCP 2/1 d'obtenir la preuve qu'un essai de conformité approprié a été réalisé.

Annexe A (informative)

Informations supplémentaires pour les profils de communication de sécurité fonctionnelle de la CPF 2

A.1 Exemple de code de fonction de hachage

```
#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, 0xBF06116,
0x21B4F4B5, 0x56B3C423, 0xCFBA9599, 0xB8BDA50F,
0x2802B89E, 0x5F058808, 0xC60CD9B2, 0xB10BE924,
0x2F6F7C87, 0x58684C11, 0xC1611DAB, 0xB6662D3D,
0x76DC4190, 0x01DB7106, 0x98D220BC, 0xEF5102A,
0x71B18589, 0x06B6B51F, 0x9FBE4A5, 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,
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, 0x4FDDF252,
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, 0xCA7, 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,
0xEEDB, 0xE6D4, 0xFEC5, 0xF6CA, 0xC EE7, 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,
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,
};

```

```

// polynomial 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,
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, 0x0022fbfa, 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)
```

```
{
    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

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

/** 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.
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

/xx ComputeCRCS3Ref1

\param Purpose:
Compute crc given 1 bytes of data and a preset for the crc.

\param Scope: public

\param Input: \b data      Value to compute CRC on
\param Input: \b preset    Preset value for CRC

\param Edit History:

x/
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++)
{
    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()
{
    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;

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++)
    {
        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;

    //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();

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 ...

Vide

Annexe B (informative)

Information pour l'évaluation des profils de communication de sécurité fonctionnelle de la CPF 2

Selon les règles de l'IEC, la présente norme n'énonce pas les conditions de validation de la conformité. Toutefois, les essais et validation de conformité des appareils FSCP 17/1 à l'IEC 61784-3-2 peuvent être exigés par la loi.

L'information correspondante relative aux essais et à la conformité à la présente norme peut être obtenue auprès des comités nationaux locaux de l'IEC ou de l'organisation de bus de terrain compétente.

NOTE Pour l'IEC 61784-3-2, l'organisation de bus de terrain compétente est ODVA, voir www.odva.org.

Bibliographie

- [1] IEC 60050 (toutes parties), *Vocabulaire Electrotechnique International* (disponible à l'adresse <<http://www.electropedia.org/>>)
- NOTE Voir également le dictionnaire multilingue de l'IEC – Electricité, électronique et télécommunications (disponible sur CD-ROM et à l'adresse <<http://www.electropedia.org/>>).
- [2] IEC 60204-1, *Sécurité des machines – Équipement électrique des machines – Partie 1: Règles générales*
- [3] IEC/TS 61000-1-2, *Electromagnetic compatibility (EMC) – Part 1-2: General – Methodology for the achievement of the functional safety of electrical and electronic equipment with regard to electromagnetic phenomena* (disponible en anglais seulement)
- [4] IEC 61000-6-7, *Compatibilité électromagnétique (CEM) – Partie 6-7: Normes génériques – Exigences d'immunité pour les équipements visant à exercer des fonctions dans un système lié à la sécurité (sécurité fonctionnelle) dans des sites industriels*
- [5] IEC 61131-6, *Automates programmables – Partie 6: Sécurité fonctionnelle*
- [6] IEC 61158 (all parts), *Réseaux de communication industriels – Spécifications des bus de terrain*
- [7] IEC 61496 (toutes parties), *Sécurité des machines – Équipements de protection électro-sensibles*
- [8] IEC 61508-1:2010, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 1: Exigences générales*
- [9] IEC 61508-4:2010, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 4: Définitions et abréviations*
- [10] IEC 61508-5:2010, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 5: Exemples de méthodes pour la détermination des niveaux d'intégrité de sécurité*
- [11] IEC 61511 (toutes parties), *Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur des industries de transformation*
- [12] IEC 61784-4¹¹, *Industrial communication networks – Profiles – Part 4: Secure communications for fieldbuses* (disponible en anglais seulement)
- [13] IEC 61784-5 (toutes les parties), *Réseaux de communication industriels – Profils – Partie 5: Installation des bus de terrain – Profils d'installation pour CPF x*
- [14] IEC 61800-5-2, *Entraînements électriques de puissance à vitesse variable – Partie 5-2: Exigences de sécurité – Fonctionnelle*
- [15] IEC TR 62059-11:2002, *Équipements de comptage de l'électricité – Sûreté de fonctionnement – Partie 11: Concepts généraux*

¹¹ Proposition d'un nouveau sujet d'étude à l'étude.

- [16] IEC 62061, *Sécurité des machines – Sécurité fonctionnelle des systèmes de commande électriques, électroniques et électroniques programmables relatifs à la sécurité*
- [17] IEC TR 62210:2003, *Power system control and associated communications – Data and communication security* (disponible en anglais seulement)
- [18] IEC 62280:2014, *Applications ferroviaires – Systèmes de signalisation, de télécommunication et de traitement – Communication de sécurité dans les systèmes de transmission*
- [19] IEC 62443 (toutes les parties), *Réseaux industriels de communication – Sécurité dans les réseaux et les systèmes*
- [20] IEC TR 62685, *Réseaux de communication industriels – Profils – Lignes directrices pour l'évaluation des appareils de sécurité utilisant les profils de communication pour la sécurité fonctionnelle (FSCP) de la CEI 61784-3*
- [21] Guide ISO/IEC 51:2014, *Aspects liés à la sécurité – Principes directeurs pour les inclure dans les normes*
- [22] ISO/IEC 2382-14, *Technologies de l'information – Vocabulaire – Partie 14: Fiabilité, maintenabilité et disponibilité*
- [23] ISO/IEC 2382-16:1996, *Technologies de l'information – Vocabulaire – Partie 16: Théorie de l'information*
- [24] ISO/IEC 7498-1, *Technologies de l'information – Modèle de référence de base pour l'interconnexion de systèmes ouverts (OSI): Le modèle de base* (disponible en anglais seulement)
- [25] ISO/IEC 19501:2005, *Technologies de l'information – Traitement distribué ouvert – Langage de modélisation unifié (UML), version 1.4.2* (disponible en anglais seulement)
- [26] ISO 10218-1, *Robots et dispositifs robotiques – Exigences de sécurité pour les robots industriels – Partie 1: Robots*
- [27] ISO 12100, *Sécurité des machines – Principes généraux de conception – Appréciation du risque et réduction du risque*
- [28] ISO 13849 (toutes les parties), *Sécurité des machines – Parties des systèmes de commande relatives à la sécurité*
- [29] ANSI/ISA-84.00.01-2004 (all parts), *Functional Safety: Safety Instrumented Systems for the Process Industry Sector* (disponible en anglais seulement)
- [30] GS-ET-26¹², *Grundsatz für die Prüfung und Zertifizierung von Bussystemen für die Übertragung sicherheitsrelevanter Nachrichten, May 130. HVBG, Gustav-Heinemann-Ufer 50968, D- Köln ("Principles for Test and Certification of Bus Systems for Safety relevant Communication")* (disponible en allemand seulement)
- [31] VDI/VDE 2180 (all parts), *Safeguarding of industrial process plants by means of process control engineering* (disponible en anglais seulement)

¹² Ce document constitue l'un des points de départ de l'élaboration de la présente partie. Il fait actuellement l'objet d'une révision importante.

- [32] ANDREW S. TANENBAUM, DAVID J. WETHERALL, *Computer Networks*, 5th Edition, Prentice Hall, N.J., ISBN-10: 0132126958, ISBN-13: 978-0132126953 (disponible en anglais seulement)
- [33] W. WESLEY PETERSON, EDWARD J. WELDON, *Error-Correcting Codes*, 2nd Edition 1972, MIT-Press, ISBN 0-262-16-039-0 (disponible en anglais seulement)
- [34] NFPA79 (2012), *Electrical Standard for Industrial Machinery* (disponible en anglais seulement)
- [35] GUY E. CASTAGNOLI, *On the Minimum Distance of Long Cyclic Codes and Cyclic Redundancy-Check Codes*, 1989, Dissertation No. 8979 of ETH Zurich, Switzerland (disponible en anglais seulement)
- [36] 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 (disponible en anglais seulement)
- [37] The CIP Networks Library Volume 5: *CIP Safety Specification*, Edition 2.6, November 2012, disponible à l'adresse <http://www.odva.org> (disponible en anglais seulement)
- [38] The CIP Networks Library Volume 1: *CIP Common*, Edition 3.18, April 2015, disponible à l'adresse <<http://www.odva.org>> (disponible en anglais seulement)
- [39] IEC 62026-3, *Appareillage à basse tension – Interfaces appareil de commande-appareil (CDI) – Partie 3: DeviceNet*

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

3, rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

Tel: + 41 22 919 02 11
Fax: + 41 22 919 03 00
info@iec.ch
www.iec.ch