IEC 61784-3-13

Edition 3.0 2021-05

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Industrial communication networks – Profiles – Part 3-13: Functional safety fieldbuses – Additional specifications for CPF 13

Réseaux de communication industriels – Profils – Partie 3-13: Bus de terrain de sécurité fonctionnelle – Spécifications supplémentaires pour CPF 13

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

ICS 25.040.40; 35.100.05

ISBN 978-2-8322-9759-9

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

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

CONTENTS

FOREWORD 14
0 Introduction 16
0.1 General 16
0.2 Patent declaration 18
1 Scope 19
2 Normative references 19
3 Terms, definitions, symbols, abbreviated terms and conventions 20
3.1 Terms and definitions 20
3.1.1 Common terms and definitions 20
3.1.2 CPF 13: Additional terms and definitions 25
3.2 Symbols and abbreviated terms 27
3.2.1 Common symbols and abbreviated terms 27
3.2.2 CPF 13: Additional symbols and abbreviated terms 27
3.3 Conventions 28
3.3.1 Hexadecimal values 28
3.3.2 Binary values 28
3.3.3 Wildcard digits 28
3.3.4 Diagrams 29
4 Overview of FSCP 13/1 (openSAFETY™) 29
4.1 Functional Safety Communication Profile 13/1 29
4.2 Technical overview 29
5 General 30
5.1 External documents providing specifications for the profile 30
5.2 Safety functional requirements 30
5.3 Safety measures 31
5.4 Safety communication layer structure 32
5.5 Relationships with FAL (and DLL, PhL) 34
5.5.1 General 34
5.5.2 Data types 34
6 Safety communication layer services 34
6.1 Modelling 34
6.1.1 Reference model 34
6.1.2 Communication model 35
6.1.3 Device roles and topology 36
6.2 Life cycle model 40
6.2.1 General 40
6.2.2 Concept, planning and implementation 40
6.2.3 Commissioning 41
6.2.4 Operation terms 43
6.2.5 Maintenance terms 44
6.3 Non safety communication layer 44
6.3.1 General 44
6.3.2 Requirements for data transport 44
6.3.3 Domain protection and separation 48
7 Safety communication layer protocol 48

7.1 Safety PDU format 48
7.1.1 Structure of Safety PDUs 48
7.1.2 Address field (ADR) 53
7.1.3 PDU identification field (ID) 53
7.1.4 Length field (LE) 55
7.1.5 Consecutive Time field (CT) 55
7.1.6 Payload data field (DB0 to DBn) 55
7.1.7 Cyclic Redundancy Check field (CRC-8 / CRC-16) 55
7.1.8 Time Request Address field (TADR) 56
7.1.9 Time Request Distinctive Number field (TR) 56
7.1.10 UDID of SCM coding (UDID of SCM) 56
7.2 Safety Process Data Object (SPDO) 57
7.2.1 General 57
7.2.2 SPDO telegram types 57
7.2.3 Data Only telegram 57
7.2.4 Data with Time Request telegram 58
7.2.5 Data with Time Response telegram 59
7.3 Safety Service Data Object (SSDO) 60
7.3.1 General 60
7.3.2 SSDO telegram types 60
7.3.3 SSDO services and protocols 61
7.3.4 SSDO Download Initiate 62
7.3.5 SSDO Download Segment 64
7.3.6 SSDO Download Initiate with Preload 64
7.3.7 SSDO Download Segment with Preload 66
7.3.8 SSDO Upload Initiate 67
7.3.9 SSDO Upload Segment 68
7.3.10 SSDO Upload Initiate with Preload 69
7.3.11 SSDO Upload Segment with Preload 70
7.3.12 SSDO Abort 71
7.3.13 SSDO Preload 73
7.4 Safety Network Management (SNMT) 74
7.4.1 General 74
7.4.2 SNMT telegram types 74
7.4.3 SNMT services and protocols 75
7.5 Safety Object dictionary (SOD) 89
7.5.1 General 89
7.5.2 Object dictionary entry definition 89
7.5.3 Data type entry specification 94
7.5.4 Object description 96
7.6 Safety related PDO mapping 141
7.6.1 General 141
7.6.2 Transmit SPDOs 142
7.6.3 Receive SPDOs 142
7.6.4 SPDO mapping parameter 142
7.6.5 SPDO mapping example 143
7.6.6 SDPO Feature Set 145
7.6.7 SPDO error handling 146
7.7 State and sequence diagrams 146

7.7.1 Safety Process Data Object (SPDO) 146
7.7.2 Time synchronization and validation 150
7.7.3 Safety Service Data Object (SSDO) 160
7.7.4 SOD access 162
7.7.5 Safety Network Management Object (SNMT) 171
7.7.6 SN power up 173
7.7.7 SN power down 180
7.7.8 SN recovery after Restart / Error 180
7.7.9 SCM power up 180
7.7.10 Address verification 183
7.7.11 Commissioning mode 185
7.7.12 Handle single UDID mismatch 185
7.7.13 Activate SN 189
7.7.14 Device exchange 190
8 Safety communication layer management 190
8.1 General 190
8.2 Configuration of a Safety Domain 191
8.3 Parameter check mechanism 191
9 System requirements 191
9.1 Indicators and switches 191
9.2 Installation guidelines 192
9.3 Safety function response time 192
9.4 Duration of demands 193
9.5 Constraints for calculation of system characteristics 193
9.5.1 General 193
9.5.2 Number of sinks limit 193
9.5.3 Message rate limit 193
9.5.4 Message payload limit 193
9.5.5 Bit error rate considerations 194
9.5.6 Residual error rate 194
9.6 Maintenance 195
9.6.1 Diagnostic information 195
9.6.2 Replacement of safety related devices 195
9.6.3 Modification 196
9.6.4 Machine part changing 196
9.6.5 Firmware update of safety related nodes 196
9.6.6 Machine check due to service interval 196
9.7 Safety manual 196
10 Assessment 196
10.1 General 196
10.2 CP 13/1 assessment 197
10.3 FSCP 13/1 conformance test 197
10.4 Approval of functional safety by competent assessment body 197
Annex A (informative) Additional information for functional safety communication profiles of CPF 13 198
A.1 Hash function calculation 198
A.2 Void 201
Annex B (informative) Information for assessment of the functional safety communication profiles of CPF 13 202

Bibliography 203

Figure 1 – Relationships of IEC 61784-3 with other standards (machinery) 16
Figure 2 – Relationships of IEC 61784-3 with other standards (process) 17
Figure 3 – Producer consumer example 30
Figure 4 – Client server example 30
Figure 5 – Communication layer structure 33
Figure 6 – Safety communication channel 34
Figure 7 – Characteristic producer / consumer communication 35
Figure 8 – Extended producer / consumer communication 36
Figure 9 – Client Server communication 36
Figure 10 – Topology overview 37
Figure 11 – Safety Domain protection (example) 38
Figure 12 – Safety Domain separation (example) 39
Figure 13 – Data flow example 43
Figure 14 – Communication model 45
Figure 15 – SPDO transport 46
Figure 16 – SSDO transport 47
Figure 17 – Diagnostic data representation 48
Figure 18 – Safety PDUs inside a CP 13/1 PDU 49
Figure 19 – Basic Safety PDU for n = 0 – 8 octet payload data 49
Figure 20 – Basic Safety PDU from 9 octet payload data 49
Figure 21 – Slim Safety PDU for n = 0 – 8 octet payload data 50
Figure 22 – Slim Safety PDU from 9 octet payload data 51
Figure 23 – Safety PDU with 40 bit counter for n = 0 – 8 octet payload data 52
Figure 24 – Safety PDU with 40 bit counter from 9 octet payload data 52
Figure 25 – SPDO_Data_Only telegram 58
Figure 26 – SPDO_Data_with_Time_Request telegram 58
Figure 27 – SPDO_Data_with_Time_Response telegram 59
Figure 28 – SSDO download protocols 62
Figure 29 – SSDO upload protocols 62
Figure 30 – SSDO Download Initiate protocol 63
Figure 31 – SSDO Download Segment protocol 64
Figure 32 – SSDO Download Initiate protocol with Preload 65
Figure 33 – SSDO Download Segment protocol with Preload 66
Figure 34 – SSDO Upload Initiate protocol 67
Figure 35 – SSDO Upload Segment protocol 68
Figure 36 – SSDO Upload Initiate protocol with Preload 69
Figure 37 – SSDO Upload Segment protocol with Preload 71
Figure 38 – SSDO Abort protocol 72
Figure 39 – UDID Request / Response protocol 75
Figure 40 – SADR Assignment protocol 76
Figure 41 – Reset Node Guarding Time protocol 77

Figure 42 – SN set to Pre-Operational protocol 79
Figure 43 – SN set to Operational protocol 80
Figure 44 – SN Acknowledge protocol 82
Figure 45 – SN set to stop protocol 83
Figure 46 – SCM set to Operational protocol 83
Figure 47 – Node Guarding protocol 84
Figure 48 – Additional SADR Assignment protocol 85
Figure 49 – UDID of SCM Assignment protocol 87
Figure 50 – Init CT value assignment protocol 88
Figure 51 – SPDO mapping example 143
Figure 52 – State diagram TxSPDO 146
Figure 53 – SPDO communication producer 147
Figure 54 – State diagram RxSPDO 148
Figure 55 – SPDO communication consumer 148
Figure 56 – State diagram process data 149
Figure 57 – Time synchronization and validation 150
Figure 58 – Time synchronization detail 151
Figure 59 – Calculation of propagation delay 153
Figure 60 – Time validation, propagation delay explanation limits 153
Figure 61 – Time synchronization on a nonsafe network 155
Figure 62 – Explanation of time synchronization 155
Figure 63 – Time synchronization failure 156
Figure 64 – State diagram time synchronization producer 157
Figure 65 – State diagram time synchronization consumer 158
Figure 66 – State diagram SSDO client 160
Figure 67 – State diagram SSDO server 161
Figure 68 – Expedited SOD access 162
Figure 69 – State diagram segmented SOD download access client 163
Figure 70 – Segmented SOD download access 164
Figure 71 – State diagram segmented SOD download access server 165
Figure 72 – State diagram SOD preload download access client 167
Figure 73 – SOD preload download access 168
Figure 74 – State diagram SOD preload download access server 170
Figure 75 – State diagram SNMT master 172
Figure 76 – State diagram SNMT slave 173
Figure 77 – State diagram SN power up 174
Figure 78 – State diagram SN Pre-Operational 176
Figure 79 – State diagram SN additional paramters 178
Figure 80 – State diagram SN Operational 179
Figure 81 – Life Guarding telegram 180
Figure 82 – State diagram SCM power up 181
Figure 83 – State diagram SCM Operational 182
Figure 84 – State diagram SCM address verification 184

Figure 85 – State diagram SCM handle single UDID mismatch 186
Figure 86 – State diagram SCM verify parameters 188
Figure 87 – State diagram activate SN 190
Figure 88 – Safety function response time 192
Figure 89 – Assessment flow of devices 197

Table 1 – Communication errors and detection measures (cyclic) 31
Table 2 – Communication errors and detection measures (acyclic) 32
Table 3 – Device roles 37
Table 4 – Basic Safety PDU format 50
Table 5 – Slim Safety PDU format 51
Table 6 – Safety PDU with 40 bit counter 53
Table 7 – PDU identification field (ID) 54
Table 8 – Used ID field combinations 54
Table 9 – Request / response identification 54
Table 10 – Type of CRC depending on LE 55
Table 11 – CRC polynoms for SPDUs 56
Table 12 – SPDO telegram types (ID field, bits 2, 3 and 4) 57
Table 13 – Fields of SPDO_Data_Only telegram 58
Table 14 – Fields of SPDO_Data_with_Time_Request telegram 59
Table 15 – Fields of SPDO_Data_with_Time_Response telegram 59
Table 16 – SSDO telegram types (ID field, bits 2, 3 and 4) 60
Table 17 – SOD Access Command (SACmd) – bit coding 61
Table 18 – Fields of Download Initiate SSDO_Service_Request telegram 63
Table 19 – Fields of Download Initiate SSDO_Service_Response telegram 63
Table 20 – Fields of Download Segment SSDO_Service_Request telegram 64
Table 21 – Fields of Download Segment SSDO_Service_Response telegram 64
Table 22 – Fields of Download Initiate SSDO_Service_Request telegram with Preload 65
Table 23 – Fields of Download Initiate SSDO_Service_Response telegram with Preload 65
Table 24 – Fields of Download Segment SSDO_Service_Request telegram with Preload 66
Table 25 – Fields of Download Segment SSDO_Service_Response telegram with Preload 67
Table 26 – Fields of Upload Initiate SSDO_Service_Request telegram 67
Table 27 – Fields of Upload Initiate SSDO_Service_Response telegram 68
Table 28 – Fields of Upload Segment SSDO_Service_Request telegram 69
Table 29 – Fields of Upload Segment SSDO_Service_Response telegram 69
Table 30 – Fields of Upload Initiate SSDO_Service_Request telegram with Preload 70
Table 31 – Fields of Upload Initiate SSDO_Service_Response telegram with Preload 70
Table 32 – Fields of Upload Segment SSDO_Service_Request telegram with PreLoad 71
Table 33 – Fields of Upload Segment SSDO_Service_Response telegram with Preload 71
Table 34 – Fields of SSDO Abort telegram 72
Table 35 – SSDO Abort codes 72
Table 36 – TR field usage for SSDO Preload 73
Table 37 – Bit fields inside TR field for SSDO Preload 74

Table 38 – SNMT telegram types (ID field, bits 2, 3 and 4) 74
Table 39 – Fields of SNMT_Request_UDID telegram 75
Table 40 – Fields of SNMT_Response_UDID telegram 76
Table 41 – Fields of SNMT_Assign_SADR telegram 77
Table 42 – Fields of SNMT_SADR_ Assigned telegram 77
Table 43 – Fields of SNMT_SN_reset_guarding_SCM telegram 78
Table 44 – SNMT request telegram types 78
Table 45 – SNMT response telegram types 78
Table 46 – Fields of SNMT_SN_set_to_PRE_OP telegram 79
Table 47 – Fields of SNMT_SN_status_PRE_OP telegram 79
Table 48 – Fields of SNMT_SN_set_to_OP telegram 80
Table 49 – Fields of SNMT_SN_status_OP telegram 80
Table 50 – Fields of SNMT_SN_busy telegram 81
Table 51 – Fields of SNMT_SN_FAIL telegram 81
Table 52 – SNMT_SN_FAIL Error Group values 81
Table 53 – SNMT_SN_FAIL Error Code values 81
Table 54 – SNMT_SN_FAIL Error Code values in case of Error Group Code 5 82
Table 55 – Fields of SNMT_SN_ACK telegram 82
Table 56 – Fields of SNMT_SCM_set_to_STOP telegram 83
Table 57 – Fields of SNMT_SCM_set_to_OP telegram 84
Table 58 – Fields of SNMT_SCM_guard_SN telegram 84
Table 59 – Fields of SNMT_SN_status_OP/SNMT_SN_status_OP telegrams 85
Table 60 – Fields of SNMT_assign_additional_SADR telegram 86
Table 61 – Fields of SNMT_assigned_additional_SADR telegram 86
Table 62 – Fields of SNMT_assign_UDID_of_SCM telegram 87
Table 63 – Fields of SNMT_assigned_UDID_of_SCM telegram 87
Table 64 – Fields of SNMT_assign_Init_CT telegram 88
Table 65 – Fields of SNMT_assigned_Init_CT telegram 88
Table 66 – Object type definition 89
Table 67 – Access attributes for data objects 91
Table 68 – SPDO mapping attributes for data objects 91
Table 69 – Basic data type object definition example 91
Table 70 – Compound data type object definition example 92
Table 71 – Sub index interpretation 92
Table 72 – NumberOfEntries sub index specification 93
Table 73 – RECORD type object sub index specification 93
Table 74 – ARRAY type object sub index specification 94
Table 75 – StructureOfObject encoding 94
Table 76 – Object dictionary data types 95
Table 77 – 0021h Compound data type description example 96
Table 78 – 0021h Compound sub index descriptions example 96
Table 79 – Standard objects 97
Table 80 – Common communication objects 97

Table 81 – Receive SPDO communication objects 97
Table 82 – Receive SPDO mapping objects 98
Table 83 – Transmit SPDO communication objects 98
Table 84 – User parameter (writeable at any time) 98
Table 85 – Transmit SPDO mapping objects 98
Table 86 – SADR DVI list 99
Table 87 – Additional SADR list 99
Table 88 – SADR UDID list 99
Table 89 – Additional parameter list 99
Table 90 – Object 1001h Error Register 100
Table 91 – Object 1001h Error Register value interpretation 100
Table 92 – Object 1002h Manufacturer status register 100
Table 93 – Object 1003h Pre defined error field 101
Table 94 – Object 1003h sub index 00h 101
Table 95 – Object 1003h sub index 01h 101
Table 96 – Object 1003h sub index 02h to FEh 102
Table 97 – Object 1003h Error statistics 102
Table 98 – Object 1004h sub index 00h 102
Table 99 – Object 1004h sub index 01h 103
Table 100 – Object 1004h sub index 02h 103
Table 101 – Object 1004h sub index 03h 103
Table 102 – Object 1004h sub index 04h 104
Table 103 – Object 1004h sub index 05h 104
Table 104 – Object 1004h sub index 06h 104
Table 105 – Object 1004h sub index 07h 105
Table 106 – Object 1004h sub index 08h 105
Table 107 – Object 1004h sub index 09h 105
Table 108 – Object 1004h sub index 0Ah 106
Table 109 – Object 1004h sub index 0Bh 106
Table 110 – Object 1004h sub index 0Ch 106
Table 111 – Object 1004h sub index 0Dh 107
Table 112 – Object 1004h sub index 0Eh 107
Table 113 – Object 100Ch Life Guarding 107
Table 114 – Object 100Ch sub index 00h 108
Table 115 – Object 100Ch sub index 01h 108
Table 116 – Object 100Ch sub index 02h 108
Table 117 – Object 100Dh Refresh Interval of Reset Guarding 109
Table 118 – Object 100Eh Number of Retries for Reset Guarding 109
Table 119 – Object 1018h Device Vendor Information 110
Table 120 – Object 1018h sub index 00h 110
Table 121 – Object 1018h sub index 01h 110
Table 122 – Object 1018h sub index 02h 111
Table 123 – Object 1018h sub index 03h 111

Table 124 – Object 1018h sub index 04h 111
Table 125 – Object 1018h sub index 05h 112
Table 126 – Object 1018h sub index 06h 112
Table 127 – Object 1018h sub index 07h 112
Table 128 – Object 1018h sub index 08h 113
Table 129 – Object 1018h sub index 09h 113
Table 130 – Structure of Revision Number 113
Table 131 – Structure of parameter checksum domain 114
Table 132 – CRC polynom for parameter checksum 114
Table 133 – Structure of Stack Version 114
Table 134 – Object 1019h Unique Device ID 115
Table 135 – Object 101Ah Parameter Download 115
Table 136 – Format of Parameter Download 116
Table 137 – Format of additional parameter header 116
Table 138 – Object 101Bh SCM Parameters 116
Table 139 – Object 101Bh sub index 00h 117
Table 140 – Object 101Bh sub index 01h 117
Table 141 – Object 1200h Common Communication Parameter 117
Table 142 – Object 1200h sub index 00h 118
Table 143 – Object 1200h sub index 01h 118
Table 144 – Object 1200h sub index 02h 118
Table 145 – Object 1200h sub index 03h 119
Table 146 – Object 1200h sub index 04h 119
Table 147 – Object 1201h SSDO Communication Parameter 120
Table 148 – Object 1201h sub index 00h 120
Table 149 – Object 1201h sub index 01h 120
Table 150 – Object 1201h sub index 02h 121
Table 151 – Object 1202h SNMT Communication Parameter 121
Table 152 – Object 1202h sub index 00h 121
Table 153 – Object 1202h sub index 01h 122
Table 154 – Object 1202h sub index 02h 122
Table 155 – Object 1400h – 17FEh RxSPDO Communication Parameter 122
Table 156 – Object 1400h – 17FEh sub index 00h 123
Table 157 – Object 1400h – 17FEh sub index 01h 123
Table 158 – Object 1400h – 17FEh sub index 02h 123
Table 159 – Object 1400h – 17FEh sub index 03h 124
Table 160 – Object 1400h – 17FEh sub index 04h 124
Table 161 – Object 1400h – 17FEh sub index 05h 124
Table 162 – Object 1400h – 17FEh sub index 06h 125
Table 163 – Object 1400h – 17FEh sub index 07h 125
Table 164 – Object 1400h – 17FEh sub index 08h 125
Table 165 – Object 1400h – 17FEh sub index 09h 126
Table 166 – Object 1400h – 17FEh sub index 0Ah 126

Table 167 – Object 1400h – 17FEh sub index 0Bh 126
Table 168 – Object 1400h – 17FEh sub index 0Ch 127
Table 169 – Object 1800h – 1BFEh RxSPDO communication parameter 127
Table 170 – Object 1800h – 1BFEh sub index 00h 127
Table 171 – Object 1800h – 1BFEh sub index 01h 128
Table 172 – Object 1800h – 1BFEh sub index 02h – FEh 128
Table 173 – 1Object C00h – 1FFEh TxSPDO communication parameter 128
Table 174 – Object 1C00h – 1FFEh sub index 00h 129
Table 175 – Object 1C00h – 1FFEh sub index 01h 129
Table 176 – Object 1C00h – 1FFEh sub index 02h 129
Table 177 – Object 1C00h – 1FFEh sub index 03h 130
Table 178 – Object C000h – C3FEh TxSPDO mapping parameter 130
Table 179 – Object C000h – C3FEh sub index 00h 130
Table 180 – Object C000h – C3FEh sub index 01h 131
Table 181 – Object C000h – C3FEh sub index 02h – FEh 131
Table 182 – Object C400h – C7FEh SADR-DVI list 131
Table 183 – Object C400h – C7FEh sub index 00h 132
Table 184 – Object C400h – C7FEh sub index 01h 132
Table 185 – Object C400h – C7FEh sub index 02h 132
Table 186 – Object C400h – C7FEh sub index 03h 133
Table 187 – Object C400h – C7FEh sub index 04h 133
Table 188 – Object C400h – C4FEh sub index 05h 133
Table 189 – Object C400h – C7FEh sub index 06h 134
Table 190 – Object C400h – C7FEh sub index 07h 134
Table 191 – Object C400h – C7FEh sub index 08h 134
Table 192 – Object C400h – C7FEh sub index 09h 135
Table 193 – Object C400h – C7FEh sub index 0Ah 135
Table 194 – Object C400h – C7FEh sub index 0Bh 135
Table 195 – Object C400h – C7FEh sub index 0Ch 136
Table 196 – Bit field of optional features 136
Table 197 – Object C400h – C7FEh sub index 0Dh 136
Table 198 – Object C400h – C7FEh sub index 0Eh 136
Table 199 – Object C400h – C7FEh sub index 0Fh 137
Table 200 – Object C801h – CBFFh Additional SADR list 137
Table 201 – Object C801h – CBFFh sub index 00h 137
Table 202 – Object C801h – CBFFh sub index 01h 138
Table 203 – Object C801h – CBFFh sub index 02h 138
Table 204 – Object Additional SADR List Example 139
Table 205 – Object CC01h – CFFFh SADR-UDID list 139
Table 206 – Object CC01h – CFFFh sub index 00h 139
Table 207 – Object CC01h – CFFFh sub index 01h – FEh 140
Table 208 – SADR-UDID List Example 140
Table 209 – Object E400h – E7FEh SSCM additional parameter list 140

Table 210 – Object E400h – E7FEh sub index 00h 141
Table 211 – Object E400h – E7FEh sub index 01h – 10h 141
Table 212 – Structure of SPDO mapping entry 142
Table 213 – Mapping example table 1 143
Table 214 – Mapping example table 2 143
Table 215 – Mapping example table 3 144
Table 216 – Mapping example table 4 144
Table 217 – Mapping example table 5 144
Table 218 – Mapping example table 6 144
Table 219 – Mapping example table 7 145
Table 220 – SPDO telegram features (TR field, bits 2-7) 145
Table 221 – SPDO communication producer item description 147
Table 222 – SPDO communication producer state description 147
Table 223 – SPDO communication consumer item description 148
Table 224 – SPDO communication consumer state description 149
Table 225 – SPDO communication consumer telegram validation item description 150
Table 226 – SPDO communication consumer telegram validation state description 150
Table 227 – Time synchronization item description 152
Table 228 – Time validation item description 154
Table 229 – Extended time synchronization item description 156
Table 230 – Time synchronization producer item description 157
Table 231 – Time synchronization producer state description 158
Table 232 – Time synchronization consumer item description 159
Table 233 – Time synchronization consumer state description 159
Table 234 – SSDO client item description 161
Table 235 – SSDO client state description 161
Table 236 – SSDO server state description 161
Table 237 – SOD access item description 162
Table 238 – Segmented SOD access client item description 164
Table 239 – Segmented SOD download access client state description 164
Table 240 – Segmented SOD access server item description 166
Table 241 – Segmented SOD access server state description 166
Table 242 – SOD preload download access client item description 168
Table 243 – SOD preload download access client state description 169
Table 244 – SOD preload download access server item description 171
Table 245 – SOD preload download access server state description 171
Table 246 – SNMT master item description 172
Table 247 – SNMT master state description 172
Table 248 – SNMT slave state description 173
Table 249 – SN power up state description 174
Table 250 – State and communication object relation 174
Table 251 – SN Pre-Operational state item description 177
Table 252 – SN Pre-Operational state description 177

Table 253 – SN additional parameter state description 179
Table 254 – SN Operational state item description 180
Table 255 – SN Operational state description 180
Table 256 – SCM power up state description 181
Table 257 – State and communication object relation 181
Table 258 – SCM Operational state item description 183
Table 259 – SCM Operational state description 183
Table 260 – Address verification item description 185
Table 261 – Address verification state description 185
Table 262 – SCM handle single UDID mismatch state description 187
Table 263 – SCM verify parameters state description 189
Table 264 – Activate SN state description 190
Table 265 – Residual error rate 194

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES –

Part 3-13: Functional safety fieldbuses – Additional specifications for CPF 13

FOREWORD

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

IEC 61784-3-13 has been prepared by subcommittee 65C: Industrial networks, of IEC technical committee 65: Industrial-process measurement, control and automation. It is an International Standard.

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

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

- removal of block up-/download;
- addition of SSDO with preload;
- addition of SPDO feature sets;

- addition of SPDO with 40 bit counter;
- addition of SPDO dynamic SCT;
- addition of additional parameter sets;
- corrections and editorial improvements.

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

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

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

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

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

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

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

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

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

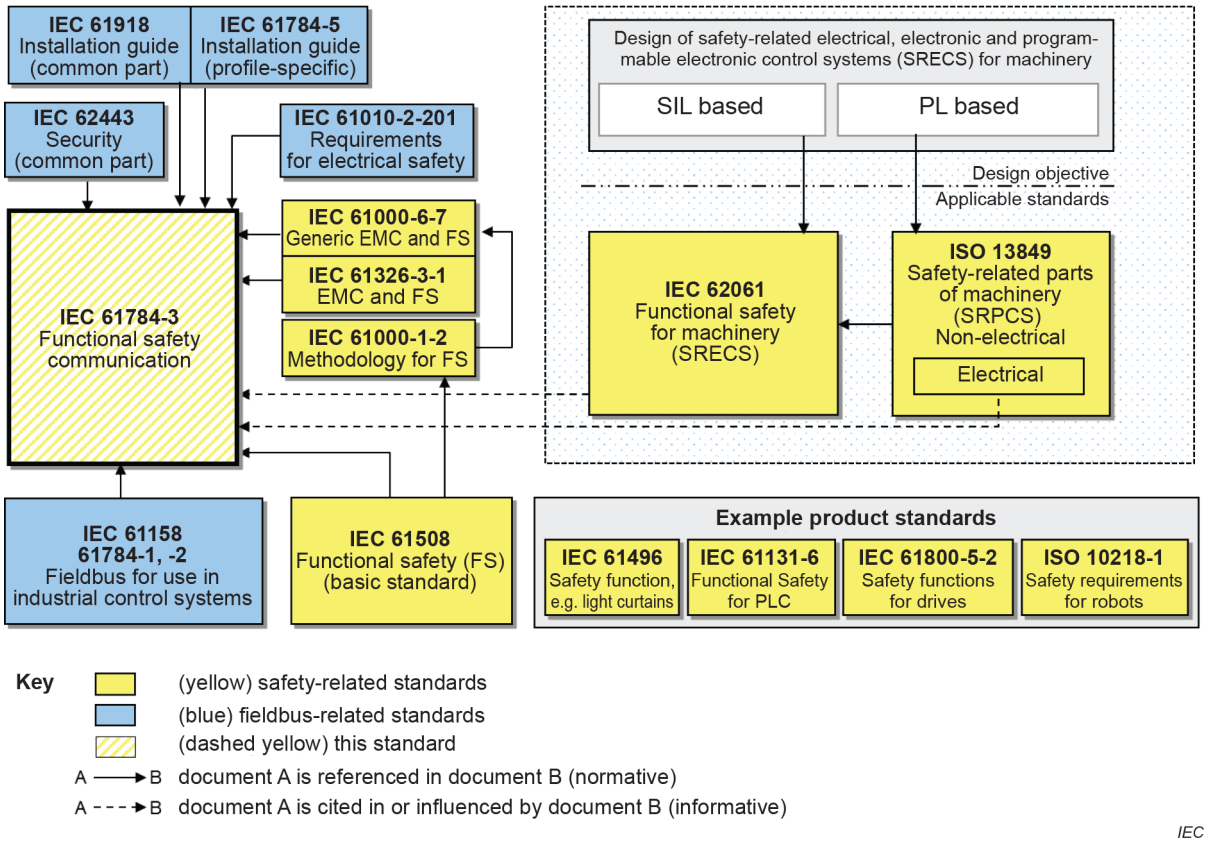
0 Introduction

0.1 General

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

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

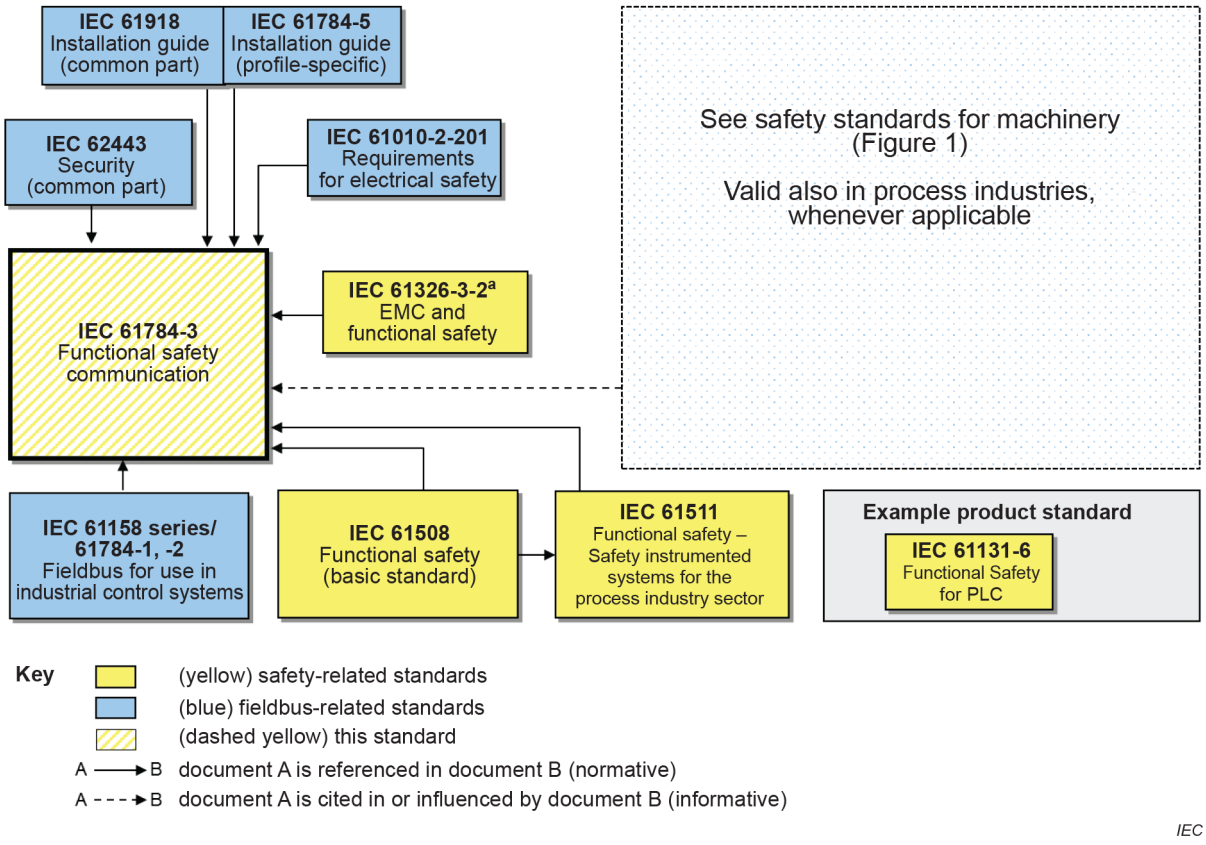
Figure 1 shows the relationships between IEC 61784-3 (all parts) and relevant safety and fieldbus standards in a machinery environment.



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

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

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



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

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

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

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

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

IEC 61784-3 (all parts) describes:

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

0.2 Patent declaration

The International Electrotechnical Commission (IEC) draws attention to the fact that it is claimed that compliance with this document may involve the use of patents concerning the functional safety communication profiles for family 13. IEC takes no position concerning the evidence, validity, and scope of these patent rights.

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

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

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES –

Part 3-13: Functional safety fieldbuses – Additional specifications for CPF 13

1 Scope

This part of IEC 61784-3 (all parts) specifies a safety communication layer (services and protocol) based on CPF 13 of IEC 61784-2 and IEC 61158 Type 13. It identifies the principles for functional safety communications defined in IEC 61784-3 that are relevant for this safety communication layer. This safety communication layer is intended for implementation in safety devices only.

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

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

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

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

2 Normative references

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

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

IEC 61158-3-13, *Industrial communication networks – Fieldbus specifications – Part 3-13: Data-link layer service definition – Type 13 elements*

IEC 61158-4-13, *Industrial communication networks – Fieldbus specifications – Part 4-13: Data-link layer protocol specification – Type 13 elements*

IEC 61158-5-13, *Industrial communication networks – Fieldbus specifications – Part 5-13: Application layer service definition – Type 13 elements*

IEC 61158-6-13, *Industrial communication networks – Fieldbus specifications – Part 6-13: Application layer protocol specification – Type 13 elements*

---

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

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

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

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

IEC 61784-5-13, *Industrial communication networks – Profiles – Part 5-13: Installation of fielbuses – Installation profiles for CPF 13*

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

ISO/IEC 19501, *Information technology – Open Distributed Processing – Unified Modeling Language (UML) Version 1.4.2*

SOMMAIRE

AVANT-PROPOS 218
0 Introduction 220
0.1 Généralités 220
0.2 Déclaration de brevets 222
1 Domaine d'application 223
2 Références normatives 223
3 Termes, définitions, symboles, abréviations et conventions 224
3.1 Termes et définitions 224
3.1.1 Termes et définitions communs 224
3.1.2 CPF 13: Termes et définitions supplémentaires 229
3.2 Symboles et abréviations 232
3.2.1 Symboles et abréviations communs 232
3.2.2 CPF 13: Symboles et abréviations supplémentaires 232
3.3 Conventions 233
3.3.1 Valeurs hexadécimales 233
3.3.2 Valeurs binaires 234
3.3.3 Chiffres en caractères génériques 234
3.3.4 Diagrammes 234
4 Présentation générale de FSCP 13/1 (openSAFETY™) 234
4.1 Profil de communication de sécurité fonctionnelle 13/1 234
4.2 Aperçu technique 234
5 Généralités 235
5.1 Documents externes de spécifications applicables au profil 235
5.2 Exigences fonctionnelles de sécurité 236
5.3 Mesures de sécurité 236
5.4 Structure de la couche de communication de sécurité 238
5.5 Relations avec la FAL (et DLL, PhL) 240
5.5.1 Généralités 240
5.5.2 Types de données 240
6 Services de la couche de communication de sécurité 240
6.1 Modélisation 240
6.1.1 Modèle de référence 240
6.1.2 Modèle de communication 241
6.1.3 Rôles des appareils et topologie 243
6.2 Modèle de cycle de vie 247
6.2.1 Généralités 247
6.2.2 Concept, planification et mise en œuvre 247
6.2.3 Mise en service 248
6.2.4 Conditions de fonctionnement 249
6.2.5 Conditions de maintenance 251
6.3 Couche de communication non relative à la sécurité 251
6.3.1 Généralités 251
6.3.2 Exigences pour le transport des données 251
6.3.3 Protection et séparation des domaines 255
7 Protocole de couche de communication de sécurité 255

7.1 Format PDU de sécurité 255
7.1.1 Structure des PDU de sécurité 255
7.1.2 Champ d'adresse (ADR) 260
7.1.3 Champ d'identification de PDU (ID) 261
7.1.4 Champ de longueur (LE) 262
7.1.5 Champ de temps consécutifs (CT) 262
7.1.6 Champ de données utiles (DB0 à DBn) 262
7.1.7 Champ de contrôle de redondance cyclique (CRC-8/CRC-16) 263
7.1.8 Champ d'adresse de demande de temps (TADR) 263
7.1.9 Champ de numéro distinctif de demande de temps (TR) 263
7.1.10 UDID de codage SCM (UDID de SCM) 263
7.2 Objet de données de processus de sécurité (SPDO) 264
7.2.1 Généralités 264
7.2.2 Types de télégrammes SPDO 264
7.2.3 Télégramme de données uniquement 265
7.2.4 Données avec télégramme de demande de temps 265
7.2.5 Données avec télégramme de réponse de temps 266
7.3 Objet de données de service de sécurité (SSDO) 267
7.3.1 Généralités 267
7.3.2 Types de télégrammes SSDO 267
7.3.3 Services et protocoles SSDO 269
7.3.4 Lancer téléchargement aval SSDO 270
7.3.5 Segmenter téléchargement aval SSDO 272
7.3.6 Lancer téléchargement aval SSDO avec préchargement 273
7.3.7 Segmenter téléchargement aval SSDO avec préchargement 274
7.3.8 Lancer téléchargement amont SSDO 275
7.3.9 Segmenter téléchargement amont SSDO 276
7.3.10 Lancer téléchargement amont SSDO avec préchargement 278
7.3.11 Segmenter téléchargement amont SSDO avec préchargement 279
7.3.12 Abandonner SSDO 280
7.3.13 Préchargement SSDO 282
7.4 Gestion de réseau de sécurité (SNMT) 283
7.4.1 Généralités 283
7.4.2 Types de télégrammes SNMT 283
7.4.3 Services et protocoles SNMT 283
7.5 Dictionnaire d'objets de sécurité (SOD) 298
7.5.1 Généralités 298
7.5.2 Définition d'une entrée de dictionnaire d'objets 298
7.5.3 Spécification d'une entrée de type de données 304
7.5.4 Description des objets 306
7.6 Mapping des PDO de sécurité 352
7.6.1 Généralités 352
7.6.2 SPDO d'émission 353
7.6.3 SPDO de réception 353
7.6.4 Paramètres de mapping SPDO 353
7.6.5 Exemple de mapping SPDO 354
7.6.6 Jeu de fonctionnalités SDPO 356
7.6.7 Gestion d'erreurs de SPDO 357
7.7 Diagrammes d'états et diagrammes séquentiels 358

7.7.1 Objet de données de processus de sécurité (SPDO) 358
7.7.2 Synchronisation et validation temporelles 362
7.7.3 Objet de données de service de sécurité (SSDO) 374
7.7.4 Accès au SOD 376
7.7.5 Objet de gestion de réseau de sécurité (SNMT) 386
7.7.6 Mise sous tension du SN 388
7.7.7 Mise hors tension du SN 396
7.7.8 Récupération du SN après Redémarrage/Erreur 396
7.7.9 Mise sous tension du SCM 396
7.7.10 Vérification d'adresse 399
7.7.11 Mode de mise en service 401
7.7.12 Traitement d'une discordance d'UDID unique 401
7.7.13 Activer SN 405
7.7.14 Echange d'appareil 406
8 Gestion de la couche de communication de sécurité 406
8.1 Généralités 406
8.2 Configuration d'un domaine de sécurité 407
8.3 Mécanisme de vérification des paramètres 407
9 Exigences système 408
9.1 Voyants et commutateurs 408
9.2 Lignes directrices d'installation 408
9.3 Temps de réponse de la fonction de sécurité 408
9.4 Durée des demandes (ou sollicitations) 409
9.5 Contraintes liées au calcul des caractéristiques du système 409
9.5.1 Généralités 409
9.5.2 Limite du nombre de collecteurs 409
9.5.3 Limite de taux des messages 410
9.5.4 Limite de charge utile des messages 410
9.5.5 Considérations relatives au taux d'erreurs sur les bits 410
9.5.6 Taux d'erreurs résiduelles 410
9.6 Maintenance 412
9.6.1 Informations de diagnostic 412
9.6.2 Remplacement d'appareils de sécurité 412
9.6.3 Modification 412
9.6.4 Remplacement d'une pièce de machine 412
9.6.5 Mise à jour du micrologiciel des nœuds de sécurité 413
9.6.6 Contrôle périodique des machines 413
9.7 Manuel de sécurité 413
10 Evaluation 413
10.1 Généralités 413
10.2 Evaluation CP 13/1 414
10.3 Essai de conformité FSCP 13/1 414
10.4 Approbation de la sécurité fonctionnelle par un organisme d'évaluation compétent 414
Annexe A (informative) Informations supplémentaires pour les profils de communication de sécurité fonctionnelle de la CPF 13 415
A.1 Calcul de la fonction de hachage 415
A.2 Vide 418

Annexe B (informative) Informations pour l'évaluation des profils de communication de sécurité fonctionnelle de la CPF 13 419
Bibliographie 420

Figure 1 – Relations entre l'IEC 61784-3 et d'autres normes (machines) 220
Figure 2 – Relations entre l'IEC 61784-3 et d'autres normes (processus) 221
Figure 3 – Exemple de relation producteur/consommateur 235
Figure 4 – Exemple de relation client/serveur 235
Figure 5 – Structure de la couche de communication 239
Figure 6 – Canal de communication de sécurité 240
Figure 7 – Communication type producteur/consommateur 242
Figure 8 – Communication étendue producteur/consommateur 242
Figure 9 – Communication client/serveur 243
Figure 10 – Présentation générale de la topologie 244
Figure 11 – Protection des domaines de sécurité (exemple) 245
Figure 12 – Séparation des domaines de sécurité (exemple) 246
Figure 13 – Exemple de flux de données 250
Figure 14 – Modèle de communication 251
Figure 15 – Transport des SPDO 252
Figure 16 – Transport des SSDO 253
Figure 17 – Représentation des données de diagnostic 255
Figure 18 – PDU de sécurité dans un PDU CP 13/1 256
Figure 19 – PDU de sécurité de base pour n = 0 à 8 octets de données utiles 256
Figure 20 – PDU de sécurité de base à partir de 9 octets de données utiles 256
Figure 21 – PDU de sécurité Slim pour n = 0 à 8 octets de données utiles 257
Figure 22 – PDU de sécurité Slim à partir de 9 octets de données utiles 258
Figure 23 – PDU de sécurité avec un compteur 40 bits pour n = 0 à 8 octets de données utiles 259
Figure 24 – PDU de sécurité avec un compteur 40 bits à partir de 9 octets de données utiles 259
Figure 25 – Télégramme SPDO_Data_Only 265
Figure 26 – Télégramme SPDO_Data_with_Time_Request 266
Figure 27 – Télégramme SPDO_Data_with_Time_Response 267
Figure 28 – Protocoles de téléchargement aval SSDO 270
Figure 29 – Protocoles de téléchargement amont SSDO 270
Figure 30 – Protocole Lancer téléchargement aval SSDO 271
Figure 31 – Protocole Segmenter téléchargement aval SSDO 272
Figure 32 – Protocole Lancer téléchargement aval SSDO avec préchargement 273
Figure 33 – Protocole Segmenter téléchargement aval SSDO avec préchargement 274
Figure 34 – Protocole Lancer téléchargement amont SSDO 275
Figure 35 – Protocole Segmenter téléchargement amont SSDO 277
Figure 36 – Protocole Lancer téléchargement amont SSDO avec préchargement 278
Figure 37 – Protocole Segmenter téléchargement amont SSDO avec préchargement 279
Figure 38 – Protocole Abandonner SSDO 280

Figure 39 – Protocole Demande/réponse d'UDID 284
Figure 40 – Protocole Attribution d'une SADR 285
Figure 41 – Protocole Réinitialiser intervalle de sauvegarde de nœud 286
Figure 42 – Protocole SN mis à l'état préopérationnel 287
Figure 43 – Protocole SN mis à l'état opérationnel 289
Figure 44 – Protocole Acquitter SN 291
Figure 45 – Protocole SN mis à l'arrêt 292
Figure 46 – Protocole SCM mis à l'état opérationnel 292
Figure 47 – Protocole de sauvegarde du nœud 293
Figure 48 – Protocole Attribution d'une SADR supplémentaire 294
Figure 49 – Protocole Attribution d'UDID de SCM 296
Figure 50 – Protocole Attribution de valeur CT d'initialisation 297
Figure 51 – Exemple de mapping SPDO 354
Figure 52 – Diagramme d'états de TxSPDO 358
Figure 53 – Producteur de communication SPDO 358
Figure 54 – Diagramme d'états de RxSPDO 360
Figure 55 – Consommateur de communication SPDO 360
Figure 56 – Diagramme d'états des données de processus 361
Figure 57 – Synchronisation et validation temporelles 363
Figure 58 – Synchronisation temporelle complète 363
Figure 59 – Calcul du délai de propagation 365
Figure 60 – Validation temporelle, limites explicatives du délai de propagation 366
Figure 61 – Synchronisation temporelle sur un réseau non relatif à la sécurité 368
Figure 62 – Explication de la synchronisation temporelle 368
Figure 63 – Défaillance de la synchronisation temporelle 369
Figure 64 – Diagramme d'états du producteur de synchronisation temporelle 370
Figure 65 – Diagramme d'états du consommateur de synchronisation temporelle 372
Figure 66 – Diagramme d'états du client SSDO 374
Figure 67 – Diagramme d'états du serveur SSDO 375
Figure 68 – Accès accéléré au SOD 376
Figure 69 – Diagramme d'états du client d'accès au SOD en téléchargement aval segmenté 377
Figure 70 – Accès au SOD en téléchargement aval segmenté 378
Figure 71 – Diagramme d'états du serveur d'accès au SOD en téléchargement aval segmenté 380
Figure 72 – Diagramme d'états du client d'accès au SOD en téléchargement aval avec préchargement 382
Figure 73 – Accès au SOD en téléchargement aval de bloc 383
Figure 74 – Diagramme d'états du serveur d'accès au SOD en téléchargement aval avec préchargement 385
Figure 75 – Diagramme d'états du maître SNMT 387
Figure 76 – Diagramme d'états de l'esclave SNMT 388
Figure 77 – Diagramme d'états de mise sous tension du SN 389
Figure 78 – Diagramme d'états préopérationnels du SN 391

Figure 79 – Diagramme d'états des paramètres supplémentaires du SN 394
Figure 80 – Diagramme d'états opérationnels du SN 395
Figure 81 – Télégramme de sauvegarde 396
Figure 82 – Diagramme d'états de mise sous tension du SCM 397
Figure 83 – Diagramme d'états opérationnels du SCM 398
Figure 84 – Diagramme d'états de vérification d'adresse SCM 400
Figure 85 – Diagramme d'états de traitement SCM d'une discordance d'UDID unique 402
Figure 86 – Diagramme d'états de vérification SCM des paramètres 404
Figure 87 – Diagramme d'états d'activation du SN 406
Figure 88 – Temps de réponse de la fonction de sécurité 408
Figure 89 – Organigramme d'évaluation des appareils 413

Tableau 1 – Erreurs de communication et mesures de détection (cycliques) 237
Tableau 2 – Erreurs de communication et mesures de détection (acycliques) 237
Tableau 3 – Rôles des appareils 243
Tableau 4 – Format de PDU de sécurité de base 257
Tableau 5 – Format de PDU de sécurité Slim 258
Tableau 6 – PDU de sécurité avec un compteur 40 bits 260
Tableau 7 – Champ d'identification de PDU (ID) 261
Tableau 8 – Combinaisons de champs ID utilisées 261
Tableau 9 – Identifiant de demande/réponse 262
Tableau 10 – Type de CRC en fonction de LE 262
Tableau 11 – Polynômes du CRC pour les SPDU 263
Tableau 12 – Types de télégrammes SPDO (bits 2, 3 et 4 du champ ID) 264
Tableau 13 – Champs du télégramme SPDO_Data_Only 265
Tableau 14 – Champs du télégramme SPDO_Data_with_Time_Request 266
Tableau 15 – Champs du télégramme SPDO_Data_with_Time_Response 267
Tableau 16 – Types de télégrammes SSDO (bits 2, 3 et 4 du champ ID) 268
Tableau 17 – Codage binaire de la commande d'accès au SOD (SACmd) 268
Tableau 18 – Champs du télégramme SSDO_Service_Request Lancer téléchargement aval 271
Tableau 19 – Champs du télégramme SSDO_Service_Response Lancer téléchargement aval 272
Tableau 20 – Champs du télégramme SSDO_Service_Request Segmenter téléchargement aval 272
Tableau 21 – Champs du télégramme SSDO_Service_Response Segmenter téléchargement aval 273
Tableau 22 – Champs du télégramme SSDO_Service_Request Lancer téléchargement aval avec préchargement 273
Tableau 23 – Champs du télégramme SSDO_Service_Response Lancer téléchargement aval avec préchargement 274
Tableau 24 – Champs du télégramme SSDO_Service_Request Segmenter téléchargement aval avec préchargement 275
Tableau 25 – Champs du télégramme SSDO_Service_Response Segmenter téléchargement aval avec préchargement 275

Tableau 26 – Champs du télégramme SSDO_Service_Request Lancer téléchargement amont 276
Tableau 27 – Champs du télégramme SSDO_Service_Response Lancer téléchargement amont 276
Tableau 28 – Champs du télégramme SSDO_Service_Request Segmenter téléchargement amont 277
Tableau 29 – Champs du télégramme SSDO_Service_Response Segmenter téléchargement amont 277
Tableau 30 – Champs du télégramme SSDO_Service_Request Lancer téléchargement amont avec préchargement 278
Tableau 31 – Champs du télégramme SSDO_Service_Response Lancer téléchargement amont avec préchargement 279
Tableau 32 – Champs du télégramme SSDO_Service_Request Segmenter téléchargement amont avec préchargement 280
Tableau 33 – Champs du télégramme SSDO_Service_Response Segmenter téléchargement amont avec préchargement 280
Tableau 34 – Champs du télégramme Abandonner SSDO 281
Tableau 35 – Codes d'abandon SSDO 281
Tableau 36 – Utilisation du champ TR pour le préchargement SSDO 282
Tableau 37 – Champs de bits dans le champ TR pour le préchargement SSDO 282
Tableau 38 – Types de télégrammes SNMT (bits 2, 3 et 4 du champ ID) 283
Tableau 39 – Champs du télégramme SNMT_Request_UDID 284
Tableau 40 – Champs du télégramme SNMT_Response_UDID 284
Tableau 41 – Champs du télégramme SNMT_Assign_SADR 285
Tableau 42 – Champs du télégramme SNMT_SADR_Assigned 286
Tableau 43 – Champs du télégramme SNMT_SN_reset_guarding_SCM 286
Tableau 44 – Types de télégrammes de demande SNMT 287
Tableau 45 – Types de télégrammes de réponse SNMT 287
Tableau 46 – Champs du télégramme SNMT_SN_set_to_PRE_OP 288
Tableau 47 – Champs du télégramme SNMT_SN_status_PRE_OP 288
Tableau 48 – Champs du télégramme SNMT_SN_set_to_OP 289
Tableau 49 – Champs du télégramme SNMT_SN_status_OP 289
Tableau 50 – Champs du télégramme SNMT_SN_busy 290
Tableau 51 – Champs du télégramme SNMT_SN_FAIL 290
Tableau 52 – Valeurs du groupe d'erreurs SNMT_SN_FAIL 290
Tableau 53 – Valeurs du code d'erreur SNMT_SN_FAIL 290
Tableau 54 – Valeurs du code d'erreur SNMT_SN_FAIL en cas de code de groupe d'erreurs égal à 5 291
Tableau 55 – Champs du télégramme SNMT_SN_ACK 291
Tableau 56 – Champs du télégramme SNMT_SCM_set_to_STOP 292
Tableau 57 – Champs du télégramme SNMT_SCM_set_to_OP 293
Tableau 58 – Champs du télégramme SNMT_SCM_guard_SN 293
Tableau 59 – Champs des télégrammes SNMT_SN_status_OP/SNMT_SN_status_OP 294
Tableau 60 – Champs du télégramme SNMT_assign_additional_SADR 295
Tableau 61 – Champs du télégramme SNMT_assigned_additional_SADR 295
Tableau 62 – Champs du télégramme SNMT_assign_UDID_of_SCM 296

Tableau 63 – Champs du télégramme SNMT_assigned_UDID_of_SCM 296
Tableau 64 – Champs du télégramme SNMT_assign_Init_CT 297
Tableau 65 – Champs du télégramme SNMT_assigned_Init_CT 297
Tableau 66 – Définition des types d'objets 298
Tableau 67 – Attributs d'accès pour des objets de données 300
Tableau 68 – Attributs de mapping SPDO pour des objets de données 300
Tableau 69 – Exemple de définition d'objet de type de données de base 301
Tableau 70 – Exemple de définition d'objet de type de données composé 301
Tableau 71 – Interprétation des sous-index 301
Tableau 72 – Spécification du sous-index NumberOfEntries 302
Tableau 73 – Spécification du sous-index d'objet de type RECORD 302
Tableau 74 – Spécification du sous-index d'objet de type ARRAY 303
Tableau 75 – Codage de StructureOfObject 303
Tableau 76 – Types de données du dictionnaire d'objets 304
Tableau 77 – Exemple de description du type de données composé 0021h 305
Tableau 78 – Exemple de description des sous-index composés 0021h 305
Tableau 79 – Objets normalisés 306
Tableau 80 – Objets de communication communs 306
Tableau 81 – Objets de communication des SPDO de réception 307
Tableau 82 – Objets de mapping des SPDO de réception 307
Tableau 83 – Objets de communication des SPDO d'émission 307
Tableau 84 – Paramètre utilisateur (inscriptible à tout moment) 307
Tableau 85 – Objets de mapping des SPDO d'émission 308
Tableau 86 – Liste de DVI – SADR 308
Tableau 87 – Liste de SADR supplémentaires 308
Tableau 88 – Liste d'UDID – SADR 308
Tableau 89 – Liste de paramètres supplémentaires 309
Tableau 90 – Objet 1001h Registre d'erreurs 309
Tableau 91 – Interprétation des valeurs de l'objet 1001h Registre d'erreurs 309
Tableau 92 – Objet 1002h Registre d'états du fabricant 310
Tableau 93 – Objet 1003h Champ d'erreurs prédéfini 310
Tableau 94 – Objet 1003h sous-index 00h 310
Tableau 95 – Objet 1003h sous-index 01h 311
Tableau 96 – Objet 1003h sous-index 02h à FEh 311
Tableau 97 – Objet 1003h Statistiques d'erreurs 311
Tableau 98 – Objet 1004h sous-index 00h 312
Tableau 99 – Objet 1004h sous-index 01h 312
Tableau 100 – Objet 1004h sous-index 02h 312
Tableau 101 – Objet 1004h sous-index 03h 313
Tableau 102 – Objet 1004h sous-index 04h 313
Tableau 103 – Objet 1004h sous-index 05h 313
Tableau 104 – Objet 1004h sous-index 06h 314
Tableau 105 – Objet 1004h sous-index 07h 314

Tableau 106 – Objet 1004h sous-index 08h 314
Tableau 107 – Objet 1004h sous-index 09h 315
Tableau 108 – Objet 1004h sous-index 0Ah 315
Tableau 109 – Objet 1004h sous-index 0Bh 315
Tableau 110 – Objet 1004h sous-index 0Ch 316
Tableau 111 – Objet 1004h sous-index 0Dh 316
Tableau 112 – Objet 1004h sous-index 0Eh 316
Tableau 113 – Objet 100Ch Sauvegarde 317
Tableau 114 – Objet 100Ch sous-index 00h 317
Tableau 115 – Objet 100Ch sous-index 01h 317
Tableau 116 – Objet 100Ch sous-index 02h 318
Tableau 117 – Objet 100Dh Intervalle de rafraîchissement de la réinitialisation de sauvegarde 318
Tableau 118 – Objet 100Eh Nombre de nouvelles tentatives pour la réinitialisation de sauvegarde 319
Tableau 119 – Objet 1018h Informations de fournisseur d'appareil 319
Tableau 120 – Objet 1018h sous-index 00h 320
Tableau 121 – Objet 1018h sous-index 01h 320
Tableau 122 – Objet 1018h sous-index 02h 320
Tableau 123 – Objet 1018h sous-index 03h 321
Tableau 124 – Objet 1018h sous-index 04h 321
Tableau 125 – Objet 1018h sous-index 05h 321
Tableau 126 – Objet 1018h sous-index 06h 322
Tableau 127 – Objet 1018h sous-index 07h 322
Tableau 128 – Objet 1018h sous-index 08h 322
Tableau 129 – Objet 1018h sous-index 09h 323
Tableau 130 – Structure du numéro de révision 323
Tableau 131 – Structure du domaine de somme de contrôle des paramètres 323
Tableau 132 – Polynôme du CRC pour la somme de contrôle des paramètres 323
Tableau 133 – Structure de la version de pile 324
Tableau 134 – Objet 1019h ID unique d'appareil 325
Tableau 135 – Objet 101Ah Téléchargement aval de paramètres 325
Tableau 136 – Format de Téléchargement aval de paramètres 326
Tableau 137 – Format d'en-tête de paramètre supplémentaire 326
Tableau 138 – Objet 101Bh Paramètres du SCM 326
Tableau 139 – Objet 101Bh sous-index 00h 327
Tableau 140 – Objet 101Bh sous-index 01h 327
Tableau 141 – Objet 1200h Paramètre de communication commun 327
Tableau 142 – Objet 1200h sous-index 00h 328
Tableau 143 – Objet 1200h sous-index 01h 328
Tableau 144 – Objet 1200h sous-index 02h 328
Tableau 145 – Objet 1200h sous-index 03h 329
Tableau 146 – Objet 1200h sous-index 04h 329
Tableau 147 – Objet 1201h Paramètre de communication SSDO 330

Tableau 148 – Objet 1201h sous-index 00h 330
Tableau 149 – Objet 1201h sous-index 01h 330
Tableau 150 – Objet 1201h sous-index 02h 331
Tableau 151 – Objet 1202h Paramètre de communication SNMT 331
Tableau 152 – Objet 1202h sous-index 00h 331
Tableau 153 – Objet 1202h sous-index 01h 332
Tableau 154 – Objet 1202h sous-index 02h 332
Tableau 155 – Objet 1400h à 17FEh Paramètre de communication RxSPDO 332
Tableau 156 – Objet 1400h à 17FEh sous-index 00h 333
Tableau 157 – Objet 1400h à 17FEh sous-index 01h 333
Tableau 158 – Objet 1400h à 17FEh sous-index 02h 333
Tableau 159 – Objet 1400h à 17FEh sous-index 03h 334
Tableau 160 – Objet 1400h à 17FEh sous-index 04h 334
Tableau 161 – Objet 1400h à 17FEh sous-index 05h 334
Tableau 162 – Objet 1400h à 17FEh sous-index 06h 335
Tableau 163 – Objet 1400h à 17FEh sous-index 07h 335
Tableau 164 – Objet 1400h à 17FEh sous-index 08h 335
Tableau 165 – Objet 1400h à 17FEh sous-index 09h 336
Tableau 166 – Objet 1400h à 17FEh sous-index 0Ah 336
Tableau 167 – Objet 1400h à 17FEh sous-index 0Bh 336
Tableau 168 – Objet 1400h à 17FEh sous-index 0Ch 337
Tableau 169 – Objet 1800h à 1BFEh Paramètre de communication RxSPDO 337
Tableau 170 – Objet 1800h à 1BFEh sous-index 00h 337
Tableau 171 – Objet 1800h à 1BFEh sous-index 01h 338
Tableau 172 – Objet 1800h à 1BFEh sous-index 02h à FEh 338
Tableau 173 – Objet 1C00h à 1FFEh Paramètre de communication TxSPDO 338
Tableau 174 – Objet 1C00h à 1FFEh sous-index 00h 339
Tableau 175 – Objet 1C00h à 1FFEh sous-index 01h 339
Tableau 176 – Objet 1C00h à 1FFEh sous-index 02h 339
Tableau 177 – Objet 1C00h à 1FFEh sous-index 03h 340
Tableau 178 – Objet C000h à C3FEh Paramètre de mapping TxSPDO 340
Tableau 179 – Objet C000h à C3FEh sous-index 00h 341
Tableau 180 – Objet C000h à C3FEh sous-index 01h 341
Tableau 181 – Objet C000h à C3FEh sous-index 02h à FEh 341
Tableau 182 – Objet C400h à C7FEh Liste de DVI – SADR 342
Tableau 183 – Objet C400h à C7FEh sous-index 00h 342
Tableau 184 – Objet C400h à C7FEh sous-index 01h 342
Tableau 185 – Objet C400h à C7FEh sous-index 02h 343
Tableau 186 – Objet C400h à C7FEh sous-index 03h 343
Tableau 187 – Objet C400h à C7FEh sous-index 04h 343
Tableau 188 – Objet C400h à C4FEh sous-index 05h 344
Tableau 189 – Objet C400h à C7FEh sous-index 06h 344
Tableau 190 – Objet C400h à C7FEh sous-index 07h 344

Tableau 191 – Objet C400h à C7FEh sous-index 08h 345
Tableau 192 – Objet C400h à C7FEh sous-index 09h 345
Tableau 193 – Objet C400h à C7FEh sous-index 0Ah 345
Tableau 194 – Objet C400h à C7FEh sous-index 0Bh 346
Tableau 195 – Objet C400h à C7FEh sous-index 0Ch 346
Tableau 196 – Champ de bits des fonctionnalités facultatives 346
Tableau 197 – Objet C400h à C7FEh sous-index 0Dh 347
Tableau 198 – Objet C400h à C7FEh sous-index 0Eh 347
Tableau 199 – Objet C400h à C7FEh sous-index 0Fh 347
Tableau 200 – Objet C801h à CBFFh Liste de SADR supplémentaires 348
Tableau 201 – Objet C801h à CBFFh sous-index 00h 348
Tableau 202 – Objet C801h à CBFFh sous-index 01h 348
Tableau 203 – Objet C801h à CBFFh sous-index 02h 349
Tableau 204 – Exemple d'objet: Liste de SADR supplémentaires 349
Tableau 205 – Objet CC01h à CFFFh Liste d'UDID – SADR 350
Tableau 206 – Objet CC01h à CFFFh sous-index 00h 350
Tableau 207 – Objet CC01h à CFFFh sous-index 01h à FEh 350
Tableau 208 – Exemple de Liste d'UDID – SADR 350
Tableau 209 – Objet E400h à E7FEh Liste de paramètres supplémentaires SSCM 351
Tableau 210 – Objet E400h à E7FEh sous-index 00h 351
Tableau 211 – Objet E400h à E7FEh sous-index 01h à 10h 352
Tableau 212 – Structure d'entrées de mapping SPDO 353
Tableau 213 – Exemple 1 de table de mapping 354
Tableau 214 – Exemple 2 de table de mapping 355
Tableau 215 – Exemple 3 de table de mapping 355
Tableau 216 – Exemple 4 de table de mapping 355
Tableau 217 – Exemple 5 de table de mapping 355
Tableau 218 – Exemple 6 de table de mapping 356
Tableau 219 – Exemple 7 de table de mapping 356
Tableau 220 – Types de télégrammes SPDO (bits 2 à 7 du champ TR) 357
Tableau 221 – Description des éléments du producteur de communication SPDO 359
Tableau 222 – Description des états du producteur de communication SPDO 359
Tableau 223 – Description des éléments du consommateur de communication SPDO 360
Tableau 224 – Description des états du consommateur de communication SPDO 361
Tableau 225 – Description des éléments de validation de télégramme du consommateur de communication SPDO 362
Tableau 226 – Description des états de validation du télégramme du consommateur de communication SPDO 362
Tableau 227 – Description des éléments de synchronisation temporelle 364
Tableau 228 – Description des éléments de validation temporelle 366
Tableau 229 – Description des éléments de synchronisation temporelle étendue 369
Tableau 230 – Description des éléments de producteur de synchronisation temporelle 371
Tableau 231 – Description des états du producteur de synchronisation temporelle 371

Tableau 232 – Description des éléments du consommateur de synchronisation temporelle 373
Tableau 233 – Description des états du consommateur de synchronisation temporelle 373
Tableau 234 – Description des éléments du client SSDO 375
Tableau 235 – Description des états du client SSDO 375
Tableau 236 – Description des états du serveur SSDO 376
Tableau 237 – Description des éléments d'accès au SOD 377
Tableau 238 – Description des éléments du client d'accès segmenté au SOD 378
Tableau 239 – Description des états du client d'accès au SOD en téléchargement aval segmenté 378
Tableau 240 – Description des éléments du serveur d'accès segmenté au SOD 380
Tableau 241 – Description des états du serveur d'accès segmenté au SOD 381
Tableau 242 – Description des éléments du client d'accès au SOD en téléchargement aval avec préchargement 383
Tableau 243 – Description des états du client d'accès au SOD en téléchargement aval avec préchargement 384
Tableau 244 – Description des éléments du serveur d'accès au SOD en téléchargement aval avec préchargement 386
Tableau 245 – Description des états du serveur d'accès au SOD en téléchargement aval avec préchargement 386
Tableau 246 – Description des éléments du maître SNMT 387
Tableau 247 – Description des états du maître SNMT 387
Tableau 248 – Description des états de l'esclave SNMT 388
Tableau 249 – Description des états de mise sous tension du SN 389
Tableau 250 – Relations entre états et objets de communication 389
Tableau 251 – Description des éléments d'état préopérationnel du SN 392
Tableau 252 – Description des états préopérationnels du SN 392
Tableau 253 – Description des états des paramètres supplémentaires du SN 395
Tableau 254 – Description des éléments d'état opérationnel du SN 396
Tableau 255 – Description des états opérationnels du SN 396
Tableau 256 – Description des états de mise sous tension du SCM 397
Tableau 257 – Relations entre états et objets de communication 397
Tableau 258 – Description des éléments d'état opérationnel du SCM 399
Tableau 259 – Description des états opérationnels du SCM 399
Tableau 260 – Description des éléments de vérification d'adresse 401
Tableau 261 – Description des états de vérification d'adresse 401
Tableau 262 – Description des états de traitement SCM d'une discordance d'UDID unique 403
Tableau 263 – Description des états de vérification SCM des paramètres 405
Tableau 264 – Description des états d'activation du SN 406
Tableau 265 – Taux d'erreurs résiduelles 411

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

RÉSEAUX DE COMMUNICATION INDUSTRIELS – PROFILS –

Partie 3-13: Bus de terrain de sécurité fonctionnelle – Spécifications supplémentaires pour CPF 13

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets.

L'IEC 61784-3-13 a été établie par le sous-comité 65C: Réseaux industriels, du comité d'études 65 de l'IEC: Mesure, commande et automation dans les processus industriels. Il s'agit d'une Norme internationale.

Cette troisième édition annule et remplace la deuxième édition parue en 2016. Cette édition constitue une révision technique.

Cette édition inclut les modifications techniques majeures suivantes par rapport à l'édition précédente:

- suppression du téléchargement amont/aval de bloc;
- ajout de SSDO avec préchargement;

- ajout de jeux de fonctionnalités SPDO;
- ajout de SPDO avec un compteur 40 bits;
- ajout du SCT dynamique de SPDO;
- ajout de jeux de paramètres supplémentaires;
- corrections et améliorations rédactionnelles.

Le texte de cette Norme internationale est issu des documents suivants:

FDIS	Rapport de vote
65C/1083/FDIS	65C/1087/RVD

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

La version française de cette norme n'a pas été soumise au vote.

La langue employée pour l'élaboration de cette Norme internationale est l'anglais.

Le présent document a été rédigé selon les Directives ISO/IEC, Partie 2, il a été développé selon les Directives ISO/IEC, Partie 1 et les Directives ISO/IEC, Supplément IEC, disponibles sous www.iec.ch/members_experts/refdocs. Les principaux types de documents développés par l'IEC sont décrits plus en détail sous www.iec.ch/standardsdev/publications.

Une liste de toutes les parties de la série IEC 61784-3, publiées sous le titre général *Réseaux de communication industriels – Profils – Bus de terrain de sécurité fonctionnelle*, peut être consultée sur le site web de l'IEC.

Le comité a décidé que le contenu du présent document ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous "http://webstore.iec.ch" dans les données relatives au document recherché. A cette date, le document sera

- reconduit,
- supprimé,
- remplacé par une édition révisée, ou
- amendé.

IMPORTANT – Le logo "colour inside" qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

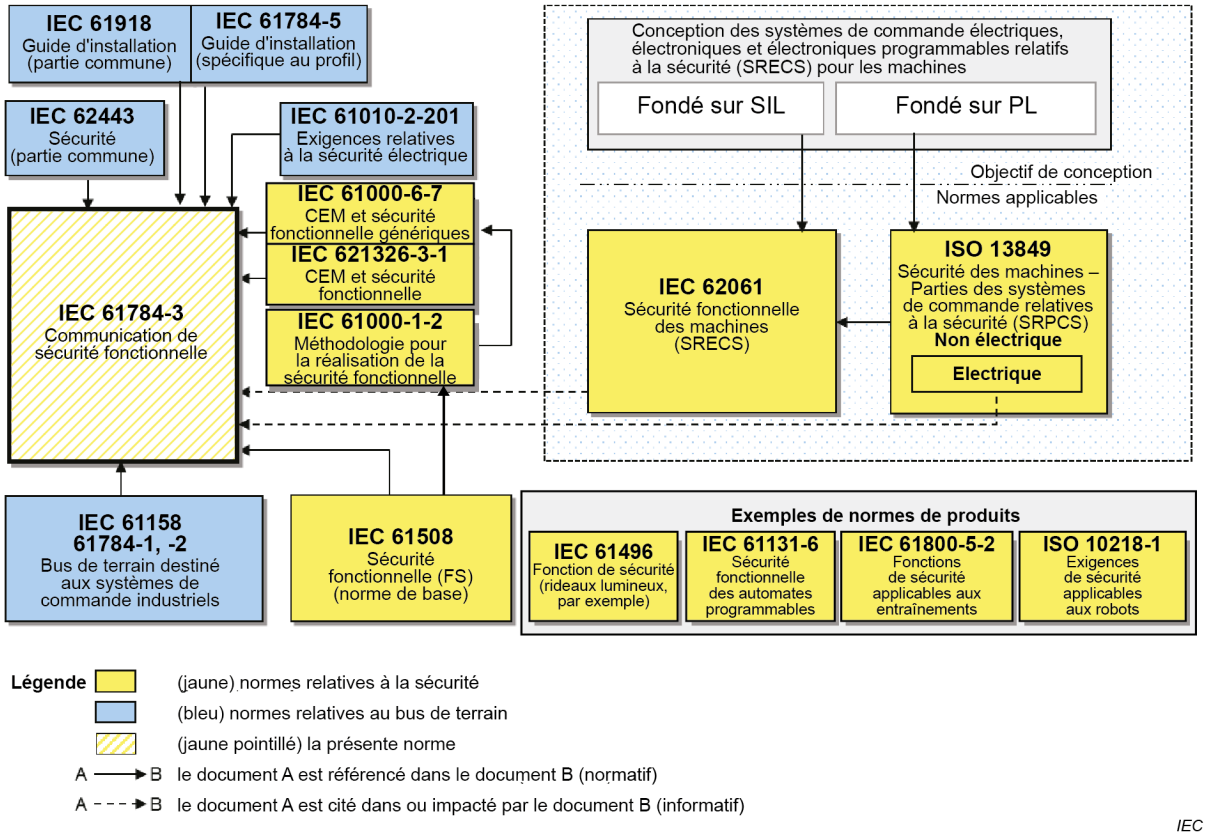
0 Introduction

0.1 Généralités

L'IEC 61158 (toutes les parties), relative aux bus de terrain, ainsi que ses normes associées IEC 61784-1 et IEC 61784-2, définissent un ensemble de protocoles de communication qui assurent la commande répartie d'applications automatisées. La technologie de bus de terrain est désormais reconnue et bien éprouvée. Les améliorations des bus de terrain se poursuivent; elles couvrent des applications pour des domaines comme les applications en temps réel relatives à la sécurité.

La série IEC 61784-3 (toutes les parties) explique les principes pertinents pour les communications de sécurité fonctionnelle en référence à l'IEC 61508 (toutes les parties) et spécifie plusieurs couches de communication de sécurité (profils et protocoles correspondants) qui reposent sur les profils de communication et les couches de protocole de l'IEC 61784-1, l'IEC 61784-2 et l'IEC 61158 (toutes les parties). Elle ne couvre pas les aspects relatifs à la sécurité électrique et à la sécurité intrinsèque. Elle ne couvre pas non plus les aspects relatifs à la sûreté et ne prévoit aucune exigence en matière de sûreté.

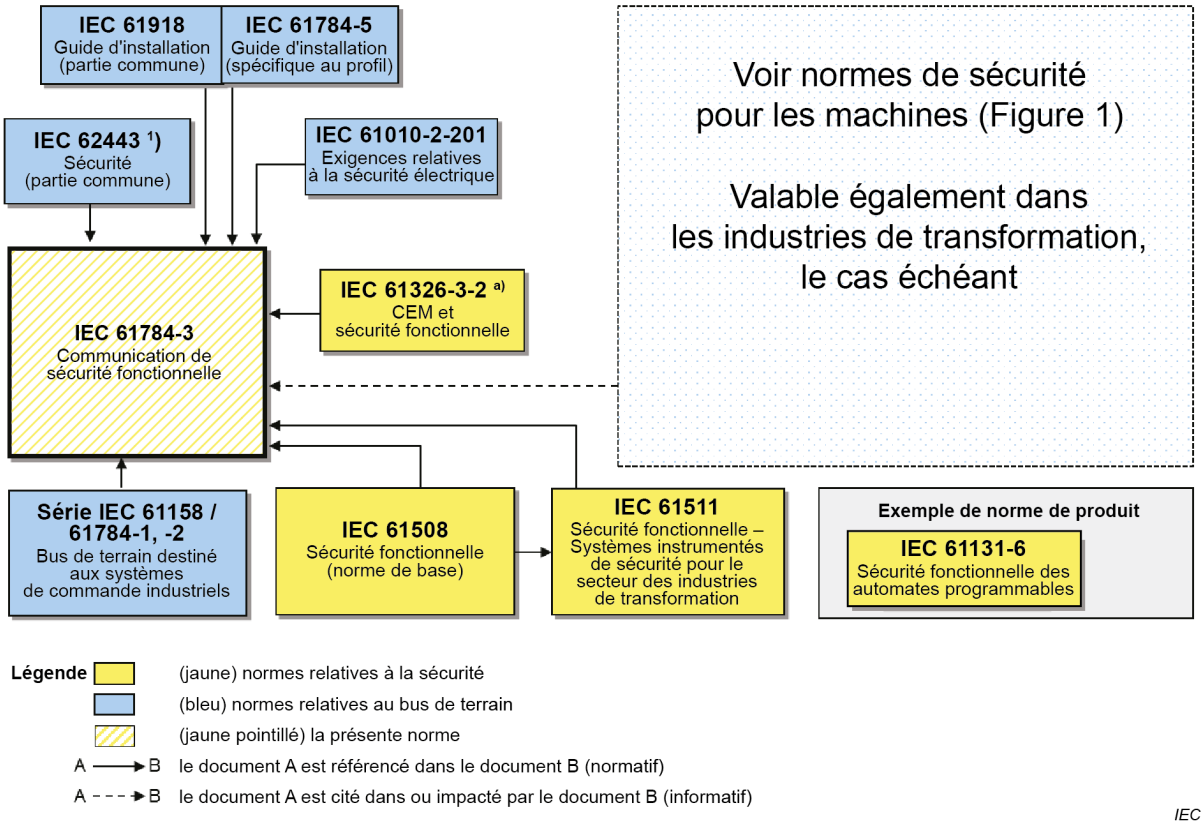
La Figure 1 représente les relations entre l'IEC 61784-3 (toutes les parties) et les normes pertinentes relatives à la sécurité et aux bus de terrain dans un environnement de machines.



NOTE L'IEC 62061 spécifie la relation entre PL (Catégorie) et SIL.

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

La Figure 2 représente les relations entre l'IEC 61784-3 (toutes les parties) et les normes pertinentes relatives à la sécurité et aux bus de terrain dans un environnement de processus.



[a] Pour les environnements électromagnétiques spécifiés; sinon, l'IEC 61326-3-1 ou l'IEC 61000-6-7 s'applique.

Figure 2 – Relations entre l'IEC 61784-3 et d'autres normes (processus)

Les couches de communication de sécurité mises en œuvre dans le cadre de systèmes relatifs à la sécurité conformément à l'IEC 61508 (toutes les parties) assurent la confiance nécessaire à accorder à la transmission de messages (informations) entre plusieurs participants sur un bus de terrain dans un système relatif à la sécurité ou une fiabilité suffisante dans le comportement de sécurité en cas d'erreurs ou de défaillances du bus de terrain.

Les couches de communication de sécurité spécifiées dans l'IEC 61784-3 (toutes les parties) permettent de s'assurer qu'un bus de terrain peut être utilisé dans des applications qui nécessitent une sécurité fonctionnelle jusqu'au niveau d'intégrité de sécurité (SIL) spécifié par son profil de communication de sécurité fonctionnelle correspondant.

La revendication du SIL qui en résulte pour un système dépend de la mise en œuvre du profil de communication de sécurité fonctionnelle (FSCP) retenu au sein du système (la mise en œuvre du profil de communication de sécurité fonctionnelle dans un appareil normal ne suffit pas à le qualifier d'appareil de sécurité).

L'IEC 61784-3 (toutes les parties) décrit:

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

0.2 Déclaration de brevets

La Commission Electrotechnique Internationale (IEC) attire l'attention sur le fait qu'il est déclaré que la conformité avec les dispositions du présent document peut impliquer l'utilisation de brevets intéressant les profils de communication de sécurité fonctionnelle pour la famille 13. L'IEC ne prend pas position quant à la preuve, à la validité et à la portée de ces droits de propriété.

Le détenteur de ces droits de propriété a donné l'assurance à l'IEC qu'il consent à négocier des licences avec des demandeurs du monde entier à des termes et conditions raisonnables et non discriminatoires. A ce propos, la déclaration du détenteur des droits de propriété est enregistrée à l'IEC. Des informations peuvent être obtenues dans la base de données des droits de propriété, disponible à l'adresse suivante: http://patents.iec.ch.

L'attention est attirée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété autres que ceux figurant dans la base de données des brevets. L'IEC ne saurait être tenue pour responsable de l'identification de ces droits de propriété en tout ou partie.

RÉSEAUX DE COMMUNICATION INDUSTRIELS – PROFILS –

Partie 3-13: Bus de terrain de sécurité fonctionnelle – Spécifications supplémentaires pour CPF 13

1 Domaine d'application

La présente partie de la série IEC 61784-3 (toutes les parties) spécifie une couche de communication de sécurité (services et protocole) qui repose sur la CPF 13 de l'IEC 61784-2 et le type 13 de l'IEC 61158. Elle identifie les principes applicables aux communications de sécurité fonctionnelle définies dans l'IEC 61784-3, qui correspondent à cette couche de communication de sécurité. Cette couche de communication de sécurité est destinée à être mise en œuvre uniquement sur les appareils de sécurité.

NOTE 1 Elle ne couvre pas les aspects relatifs à la sécurité électrique et à la sécurité intrinsèque. La sécurité électrique concerne les dangers tels que les chocs électriques. La sécurité intrinsèque concerne les dangers associés aux atmosphères explosibles.

Le présent document définit les mécanismes de transmission des messages relatifs à la sécurité entre les participants d'un réseau réparti, en utilisant la technologie de bus de terrain conformément aux exigences de la série IEC 61508 (toutes les parties)[1] concernant la sécurité fonctionnelle. Ces mécanismes peuvent être utilisés dans différentes applications industrielles, par exemple la commande de processus, l'usinage automatique et les machines.

Le présent document fournit des lignes directrices aux développeurs, ainsi qu'aux évaluateurs d'appareils et de systèmes conformes.

NOTE 2 La revendication du SIL qui en résulte pour un système dépend de la mise en œuvre du profil de communication de sécurité fonctionnelle retenu au sein du système (la mise en œuvre d'un profil de communication de sécurité fonctionnelle conforme au présent document dans un appareil normal ne suffit pas à le qualifier d'appareil de sécurité).

2 Références normatives

Les documents suivants sont cités dans le texte de sorte qu'ils constituent, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

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

IEC 61158-3-13, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 3-13: Définition des services de la couche liaison de données – Eléments de type 13*

IEC 61158-4-13, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 4-13: Spécification du protocole de couche de liaison de données – Eléments de type 13*

IEC 61158-5-13, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 5-13: Définition des services de la couche application – Eléments de type 13*

---

[1] Dans les pages suivantes du présent document, "IEC 61508" remplace "IEC 61508 (toutes les parties)".

IEC 61158-6-13, *Réseaux de communication industriels – Spécification des bus de terrain – Partie 6-13: Spécification du protocole de la couche application – Eléments de type 13*

IEC 61508 (toutes les parties), *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité*

IEC 61784-2, *Réseaux de communication industriels – Profils – Partie 2: Profils de bus de terrain supplémentaires pour les réseaux en temps réel fondés sur l'ISO/IEC/IEEE 8802-3*

IEC 61784-3:2021, *Réseaux de communication industriels – Profils – Partie 3: Bus de terrain de sécurité fonctionnelle – Règles générales et définitions de profils*

IEC 61784-5-13, *Réseaux de communication industriels – Profils – Partie 5-13: Installation des bus de terrain – Profils d'installation pour le CPF 13*

IEC 61918, *Réseaux de communication industriels – Installation de réseaux de communication dans des locaux industriels*

ISO/IEC 19501, *Information technology – Open Distributed Processing – Unified Modeling Language (UML) Version 1.4.2* (disponible en anglais seulement)