



IEC 61784-3-13

Edition 1.0 2010-06

INTERNATIONAL STANDARD

NORME INTERNATIONALE



**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

PRICE CODE
CODE PRIX

XH

ICS 25.040.40, 35.100.05

ISBN 978-2-88912-945-4

**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.....	13
0 Introduction	15
0.1 General	15
0.2 Patent declaration	17
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	24
3.2 Symbols and abbreviated terms.....	25
3.2.1 Common symbols and abbreviated terms	25
3.2.2 CPF 13: Additional symbols and abbreviated terms	26
3.3 Conventions	27
3.3.1 Hexadecimal values.....	27
3.3.2 Binary values.....	27
3.3.3 Wildcard digits.....	27
3.3.4 Diagrams.....	27
4 Overview of FSCP 13/1 (Ethernet POWERLINK safety).....	27
4.1 Functional Safety Communication Profile 13/1.....	27
4.2 Technical overview.....	28
5 General	28
5.1 External documents providing specifications for the profile.....	28
5.2 Safety functional requirements	29
5.3 Safety measures	29
5.4 Safety communication layer structure	31
5.5 Relationships with FAL (and DLL, PhL)	32
5.5.1 General	32
5.5.2 Data types.....	32
6 Safety communication layer services	32
6.1 Modelling	32
6.1.1 Reference model	32
6.1.2 Communication model	33
6.1.3 Device roles and topology	34
6.2 Life cycle model	38
6.2.1 General	38
6.2.2 Concept, planning and implementation	38
6.2.3 Commissioning	39
6.2.4 Operation terms.....	40
6.2.5 Maintenance terms	42
6.3 Non safety communication layer	42
6.3.1 General	42
6.3.2 Requirements for data transport	42
6.3.3 Domain protection and separation	46
7 Safety communication layer protocol	46
7.1 Safety PDU format	46

7.1.1	General	46
7.1.2	Address field (ADR).....	48
7.1.3	PDU identification field (ID)	49
7.1.4	Length field (LE).....	50
7.1.5	Consecutive Time field (CT)	50
7.1.6	Payload data field (DB0 to DBn)	50
7.1.7	Cyclic Redundancy Check field (CRC-8 / CRC-16)	50
7.1.8	Time Request Address field (TADR)	50
7.1.9	Time Request Distinctive Number field (TR)	51
7.1.10	UDID of SCM coding (UDID of SCM)	51
7.2	Safety Process Data Objects (SPDO)	51
7.2.1	General	51
7.2.2	SPDO telegram types	51
7.2.3	Data Only telegram.....	51
7.2.4	Data with Time Request telegram	52
7.2.5	Data with Time Response telegram	53
7.3	Safety Service Data Object (SSDO)	54
7.3.1	General	54
7.3.2	SSDO telegram types	54
7.3.3	SSDO services and protocols	55
7.3.4	SSDO Initiate Download	56
7.3.5	SSDO Segmented Download.....	57
7.3.6	SSDO Initiate Upload	58
7.3.7	SSDO Segmented Upload	59
7.3.8	SSDO Abort.....	60
7.4	Safety Network Management (SNMT).....	62
7.4.1	General	62
7.4.2	SNMT telegram types	62
7.4.3	SNMT services and protocols	62
7.5	Safety Object dictionary (SOD).....	75
7.5.1	General	75
7.5.2	Object dictionary entry definition.....	75
7.5.3	Data type entry specification.....	81
7.5.4	Object description.....	82
7.6	Safety related PDO mapping	117
7.6.1	General	117
7.6.2	Transmit SPDOs.....	118
7.6.3	Receive SPDOs.....	118
7.6.4	SPDO mapping parameter.....	118
7.6.5	SPDO mapping example.....	119
7.6.6	SPDO error handling	121
7.7	State and sequence diagrams	121
7.7.1	Safety Process Data Object (SPDO).....	121
7.7.2	Time synchronization and validation	125
7.7.3	Safety Service Data Object (SSDO).....	134
7.7.4	SOD access	136
7.7.5	Safety Network Management Object (SNMT)	141
7.7.6	SN power up.....	143
7.7.7	SN power down	147

7.7.8	SN recovery after Restart / Error	147
7.7.9	SCM power up	147
7.7.10	Address verification	150
7.7.11	Commissioning mode	152
7.7.12	Handle single UDID mismatch	152
7.7.13	Activate SN	156
7.7.14	Device exchange	157
8	Safety communication layer management	157
8.1	General	157
8.2	Goals of parameterization	158
8.3	Initial configuration of a device	158
8.3.1	General	158
8.3.2	SD setup by only configuring the SCM	158
8.3.3	SD setup configuring each SN	159
8.4	Avoiding of parameterize the wrong device	159
8.5	Parameter check mechanism	159
9	System requirements	159
9.1	Indicators and switches	159
9.2	Installation guidelines	159
9.3	Safety function response time	159
9.4	Duration of demands	161
9.5	Constraints for calculation of system characteristics	161
9.5.1	General	161
9.5.2	Number of sinks limit	161
9.5.3	Message rate limit	161
9.5.4	Message payload limit	161
9.5.5	Residual error rate	161
9.6	Maintenance	161
9.6.1	Diagnostic information	161
9.6.2	Replacement of safety related devices	161
9.6.3	Modification	162
9.6.4	Machine part changing	162
9.6.5	Firmware update of safety related nodes	162
9.6.6	Machine check due to service interval	162
9.7	Safety manual	162
10	Assessment	162
10.1	General	162
10.2	CP 13/1 assessment	163
10.3	FSCP 13/1 conformance test	163
10.4	Approval of functional safety by competent assessment body	163
10.5	Summary	163
Annex A (informative) Additional information for functional safety communication profiles of CPF 13		164
A.1	Hash function calculation	164
A.2	Stochastic errors – general considerations	167
A.2.1	General	167
A.2.2	Error detection mechanisms	167
A.2.3	Calculations	169

A.3 Stochastic errors (case A)	169
A.3.1 General	169
A.3.2 Constraints	169
A.3.3 Residual error rate	169
A.3.4 Summary	170
A.4 Stochastic errors (case B)	170
A.4.1 General	170
A.4.2 Constraints	170
A.4.3 Bit error probability considerations	170
A.4.4 Residual error rate (payload 1—8)	171
A.4.5 Residual error rate (payload 9—254)	171
A.4.6 Summary	171
Annex B (informative) Information for assessment of the functional safety communication profiles of CPF 13	172
Bibliography	173
Table 1 – Communication errors and detection measures (cyclic)	29
Table 2 – Communication errors and detection measures (acyclic)	30
Table 3 – Device roles	35
Table 4 – PDU format	48
Table 5 – PDU identification field (ID)	49
Table 6 – Used ID field combinations	49
Table 7 – Request / response identification	49
Table 8 – Type of CRC depending on LE	50
Table 9 – SPDO telegram types (ID field, bits 2, 3 and 4)	51
Table 10 – Fields of SPDO_Data_Only telegram	52
Table 11 – Fields of SPDO_Data_with_Time_Request telegram	53
Table 12 – Fields of SPDO_Data_with_Time_Response telegram	53
Table 13 – SSDO telegram types (ID field, bits 2, 3 and 4)	54
Table 14 – SOD Access Command (SACmd) – bit coding	54
Table 15 – Fields of Initiate Download SSDO_Service_Request telegram	56
Table 16 – Fields of Initiate Download SSDO_Service_Response telegram	57
Table 17 – Fields of Segmented Download SSDO_Service_Request telegram	57
Table 18 – Fields of Segmented Download SSDO_Service_Response telegram	58
Table 19 – Fields of Initiate Upload SSDO_Service_Request telegram	58
Table 20 – Fields of Initiate Upload SSDO_Service_Response telegram	59
Table 21 – Fields of Segmented Upload SSDO_Service_Request telegram	60
Table 22 – Fields of Segmented Upload SSDO_Service_Response telegram	60
Table 23 – Fields of Segmented Upload SSDO_Service_Request telegram	60
Table 24 – Fields of Segmented Upload SSDO_Service_Response telegram	61
Table 25 – SSDO Abort codes	61
Table 26 – SNMT telegram types (ID field, bits 2, 3 and 4)	62
Table 27 – Fields of SNMT_Request_UDID telegram	63
Table 28 – Fields of SNMT_Response_UDID telegram	63

Table 29 – Fields of SNMT_Assign_SADR telegram	64
Table 30 – Fields of SNMT_SADR_Assigned telegram	65
Table 31 – Fields of SNMT_SN_reset_guarding_SCM telegram	65
Table 32 – SNMT request telegram types	66
Table 33 – SNMT response telegram types	66
Table 34 – Fields of SNMT_SN_set_to_PRE_OP telegram	66
Table 35 – Fields of SNMT_SN_status_PRE_OP telegram	67
Table 36 – Fields of SNMT_SN_set_to_OP telegram	68
Table 37 – Fields of SNMT_SN_status_OP telegram	68
Table 38 – Fields of SNMT_SN_busy telegram	68
Table 39 – Fields of SNMT_SN_FAIL telegram	69
Table 40 – SNMT_SN_FAIL Error Group values	69
Table 41 – SNMT_SN_FAIL Error Code values	69
Table 42 – Fields of SNMT_SN_ACK telegram	70
Table 43 – Fields of SNMT_SCM_set_to_STOP telegram	70
Table 44 – Fields of SNMT_SCM_set_to_OP telegram	71
Table 45 – Fields of SNMT_SCM_guard_SN telegram	72
Table 46 – Fields of SNMT_SN_status_OP/SNMT_SN_status_OP telegrams	72
Table 47 – Fields of SNMT_assign_additional_SADR telegram	73
Table 48 – Fields of SNMT_assigned_additional_SADR telegram	73
Table 49 – Fields of SNMT_assign_UDID_of_SCM telegram	74
Table 50 – Fields of SNMT_assigned_UDID_of_SCM telegram	74
Table 51 – Object type definition	75
Table 52 – Access attributes for data objects	77
Table 53 – SPDO mapping attributes for data objects	77
Table 54 – Basic data type object definition example	77
Table 55 – Compound data type object definition example	78
Table 56 – Sub index interpretation	78
Table 57 – NumberOfEntries sub index specification	79
Table 58 – RECORD type object sub index specification	79
Table 59 – ARRAY type object sub index specification	80
Table 60 – StructureOfObject encoding	80
Table 61 – Object dictionary data types	81
Table 62 – 0021h Compound data type description	82
Table 63 – 0021h Compound sub index descriptions	82
Table 64 – Standard objects	83
Table 65 – Common communication objects	83
Table 66 – Receive SPDO communication objects	83
Table 67 – Receive SPDO mapping objects	84
Table 68 – Transmit SPDO communication objects	84
Table 69 – Transmit SPDO mapping objects	84
Table 70 – SADR DVI list	84
Table 71 – Additional SADR list	85

Table 72 – SADR UDID list	85
Table 73 – Object 1001h Error Register	85
Table 74 – Object 1001h Error Register value interpretation	86
Table 75 – Object 1002h Manufacturer status register	86
Table 76 – Object 1003h Pre defined error field	87
Table 77 – Object 1003h sub index 00h	87
Table 78 – Object 1003h sub index 01h	87
Table 79 – Object 1003h sub index 02h to FDh.....	88
Table 80 – Object 100Ch Life Guarding	88
Table 81 – Object 100Ch sub index 00h.....	88
Table 82 – Object 100Ch sub index 01h.....	89
Table 83 – Object 100Ch sub index 02h.....	89
Table 84 – Object 100Dh Refresh Interval of Reset Guarding	90
Table 85 – Object 1018h Device Vendor Information.....	90
Table 86 – Object 1018h sub index 00h	90
Table 87 – Object 1018h sub index 01h	91
Table 88 – Object 1018h sub index 02h	91
Table 89 – Object 1018h sub index 03h	91
Table 90 – Object 1018h sub index 04h	92
Table 91 – Object 1018h sub index 05h	92
Table 92 – Object 1018h sub index 06h.....	92
Table 93 – Object 1018h sub index 07h.....	93
Table 94 – Structure of Revision Number.....	93
Table 95 – Object 1019h Unique Device ID.....	94
Table 96 – Object 101Ah Parameter Download.....	94
Table 97 – Object 101Bh SCM Parameters	95
Table 98 – Object 101Bh sub index 00h.....	95
Table 99 – Object 101Bh sub index 01h.....	95
Table 100 – Object 1200h Common Communication Parameter	96
Table 101 – Object 1200h sub index 00h	96
Table 102 – Object 1200h sub index 01h	96
Table 103 – Object 1200h sub index 02h	97
Table 104 – Object 1200h sub index 03h	97
Table 105 – Object 1200h sub index 04h	98
Table 106 – Object 1201h SSDO Communication Parameter	98
Table 107 – Object 1201h sub index 00h	98
Table 108 – Object 1201h sub index 01h	99
Table 109 – Object 1201h sub index 02h	99
Table 110 – Object 1202h SNMT Communication Parameter	99
Table 111 – Object 1202h sub index 00h	100
Table 112 – Object 1202h sub index 01h	100
Table 113 – Object 1202h sub index 02h	100
Table 114 – Object 1400h -- 17FEh RxSPDO Communication Parameter	101

Table 115 – Object 1400h -- 17FEh sub index 00h.....	101
Table 116 – Object 1400h -- 17FEh sub index 01h.....	101
Table 117 – Object 1400h -- 17FEh sub index 02h.....	102
Table 118 – Object 1400h -- 17FEh sub index 03h.....	102
Table 119 – Object 1400h -- 17FEh sub index 04h.....	102
Table 120 – Object 1400h -- 17FEh sub index 05h.....	103
Table 121 – Object 1400h -- 17FEh sub index 06h.....	103
Table 122 – Object 1400h -- 17FEh sub index 07h.....	103
Table 123 – Object 1400h -- 17FEh sub index 08h.....	104
Table 124 – Object 1400h -- 17FEh sub index 09h.....	104
Table 125 – Object 1400h -- 17FEh sub index 0Ah	104
Table 126 – Object 1400h -- 17FEh sub index 0Bh	105
Table 127 – Object 1400h -- 17FEh sub index 0Ch	105
Table 128 – Object 1800h -- 1BFEh RxSPDO communication parameter	105
Table 129 – Object 1800h -- 1BFEh sub index 00h	106
Table 130 – Object 1800h -- 1BFEh sub index 01h	106
Table 131 – Object 1800h -- 1BFEh sub index 02h -- FDh	106
Table 132 – Object C00h -- 1FFEh TxSPDO communication parameter	107
Table 133 – Object 1C00h -- 1FFEh sub index 00h.....	107
Table 134 – Object 1C00h -- 1FFEh sub index 01h.....	107
Table 135 – Object 1C00h -- 1FFEh sub index 02h.....	108
Table 136 – Object 1C00h -- 1FFEh sub index 03h.....	108
Table 137 – Object C000h -- C3FEh TxSPDO mapping parameter.....	108
Table 138 – Object C000h -- C3FEh sub index 00h.....	109
Table 139 – Object C000h -- C3FEh sub index 01h.....	109
Table 140 – Object C000h -- C3FEh sub index 02h -- FDh.....	109
Table 141 – Object C400h -- C7FEh SADR-DVI list	110
Table 142 – Object C000h -- C3FEh sub index 00h.....	110
Table 143 – Object C000h -- C3FEh sub index 01h.....	110
Table 144 – Object C000h -- C3FEh sub index 02h.....	111
Table 145 – Object C000h -- C3FEh sub index 03h.....	111
Table 146 – Object C000h -- C3FEh sub index 04h.....	111
Table 147 – Object C000h -- C3FEh sub index 05h.....	112
Table 148 – Object C000h -- C3FEh sub index 06h.....	112
Table 149 – Object C000h -- C3FEh sub index 07h.....	112
Table 150 – Object C000h -- C3FEh sub index 08h.....	113
Table 151 – Object C000h -- C3FEh sub index 09h.....	113
Table 152 – Object C000h -- C3FEh sub index 0Ah	113
Table 153 – Object C000h -- C3FEh sub index 0Bh	114
Table 154 – Object C801h -- CBFFh Additional SADR list.....	114
Table 155 – Object C801h -- CBFFh sub index 00h	114
Table 156 – Object C801h -- CBFFh sub index 01h	115
Table 157 – Object C801h -- CBFFh sub index 02h	115

Table 158 – Object Additional SADR List Example.....	116
Table 159 – Object CC01h -- CFFFh SADR-UDID list	116
Table 160 – Object C801h -- CBFFh sub index 00h	116
Table 161 – Object C801h -- CBFFh sub index 01h -- FDh.....	117
Table 162 – SADR-UDID List Example.....	117
Table 163 – Structure of SPDO mapping entry.....	118
Table 164 – Mapping example table 1	119
Table 165 – Mapping example table 2.....	119
Table 166 – Mapping example table 3.....	120
Table 167 – Mapping example table 4.....	120
Table 168 – Mapping example table 5.....	120
Table 169 – Mapping example table 6.....	120
Table 170 – Mapping example table 7.....	121
Table 171 – SPDO communication producer item description	122
Table 172 – SPDO communication producer state description	122
Table 173 – SPDO communication consumer item description	123
Table 174 – SPDO communication consumer state description	124
Table 175 – SPDO communication consumer telegram validation item description.....	125
Table 176 – SPDO communication consumer telegram validation state description.....	125
Table 177 – Time synchronization item description	126
Table 178 – Time validation item description	129
Table 179 – Extended time synchronization item description.....	131
Table 180 – Time synchronization producer item description	132
Table 181 – Time synchronization producer state description	132
Table 182 – Time synchronization consumer item description	133
Table 183 – Time synchronization consumer state description	134
Table 184 – SSDO client item description	135
Table 185 – SSDO client state description	135
Table 186 – SSDO server state description.....	136
Table 187 – SOD access item description.....	137
Table 188 – Segmented SOD access client item description	139
Table 189 – Segmented SOD download access client state description	139
Table 190 – Segmented SOD access server item description.....	141
Table 191 – Segmented SOD access server state description.....	141
Table 192 – SNMT master item description.....	142
Table 193 – SNMT master state description.....	142
Table 194 – SNMT slave state description	143
Table 195 – SN power up state description	144
Table 196 – State and communication object relation	144
Table 197 – SN Pre-Operational state item description	145
Table 198 – SN Pre-Operational state description.....	146
Table 199 – SN Operational state item description.....	147
Table 200 – SN Operational state description	147

Table 201 – SCM power up state description	148
Table 202 – State and communication object relation	148
Table 203 – SCM Operational state item description	150
Table 204 – SCM Operational state description	150
Table 205 – Address verification item description	152
Table 206 – Address verification state description	152
Table 207 – SCM handle single UDID mismatch state description	153
Table 208 – SCM verify parameters state description	156
Table 209 – Activate SN state description	157
Figure 1 – Relationships of IEC 61784-3 with other standards (machinery)	15
Figure 2 – Relationships of IEC 61784-3 with other standards (process)	16
Figure 3 – Producer consumer example	28
Figure 4 – Client server example	28
Figure 5 – Communication layer structure	31
Figure 6 – Safety communication channel	32
Figure 7 – Characteristic producer / consumer communication	33
Figure 8 – Extended producer / consumer communication	34
Figure 9 – Client Server communication	34
Figure 10 – Topology overview	35
Figure 11 – Safety Domain protection (example)	36
Figure 12 – Safety Domain separation (example)	37
Figure 13 – Data flow example	41
Figure 14 – Communication model	43
Figure 15 – SPDO transport	44
Figure 16 – SSDO transport	45
Figure 17 – Diagnostic data representation	46
Figure 18 – Safety PDUs inside a CP 13/1 PDU	47
Figure 19 – Safety PDU for n = 0 -- 8 octet payload data	47
Figure 20 – Safety PDU for n = 9 -- 254 octet payload data	47
Figure 21 – SPDO_Data_Only telegram	52
Figure 22 – SPDO_Data_with_Time_Request telegram	52
Figure 23 – SPDO_Data_with_Time_Response telegram	53
Figure 24 – SSDO download protocols	55
Figure 25 – SSDO upload protocols	56
Figure 26 – SSDO Initiate Download protocol	56
Figure 27 – SSDO Segmented Download protocol	57
Figure 28 – SSDO Initiate Upload protocol	58
Figure 29 – SSDO Segmented Upload protocol	59
Figure 30 – SSDO Abort protocol	60
Figure 31 – UDID Request / Response protocol	63
Figure 32 – SADR Assignment protocol	64

Figure 33 – Reset Node Guarding Time protocol.....	65
Figure 34 – SN set to Pre-Operational protocol.....	66
Figure 35 – SN set to Operational protocol	67
Figure 36 – SN Acknowledge protocol	69
Figure 37 – SN set to stop protocol.....	70
Figure 38 – SCM set to Operational protocol.....	71
Figure 39 – Node Guarding protocol	71
Figure 40 – Additional SADR Assignment protocol.....	73
Figure 41 – UDID of SCM Assignment protocol.....	74
Figure 42 – SPDO mapping example	119
Figure 43 – State diagram TxSPDO	121
Figure 44 – SPDO communication producer.....	122
Figure 45 – State diagram RxSPDO.....	123
Figure 46 – SPDO communication consumer	123
Figure 47 – State diagram process data.....	124
Figure 48 – Time synchronization and validation.....	125
Figure 49 – Time synchronization detail	126
Figure 50 – Calculation of propagation delay	128
Figure 51 – Time validation, propagation delay explanation limits.....	128
Figure 52 – Time synchronization on a nonsafe network	130
Figure 53 – Explanation of time synchronization.....	130
Figure 54 – Time synchronization failure.....	131
Figure 55 – State diagram time synchronization producer	132
Figure 56 – State diagram time synchronization consumer.....	133
Figure 57 – State diagram SSDO client.....	135
Figure 58 – State diagram SSDO server	136
Figure 59 – Expedited SOD access.....	137
Figure 60 – State diagram segmented SOD download access client	138
Figure 61 – Segmented SOD download access.....	139
Figure 62 – State diagram segmented SOD download access server	140
Figure 63 – State diagram SNMT master	142
Figure 64 – State diagram SNMT slave.....	143
Figure 65 – State diagram SN power up.....	144
Figure 66 – State diagram SN Pre-Operational	145
Figure 67 – State diagram SN Operational.....	146
Figure 68 – Life Guarding telegram.....	147
Figure 69 – State diagram SCM power up.....	148
Figure 70 – State diagram SCM Operational.....	149
Figure 71 – State diagram SCM address verification.....	151
Figure 72 – State diagram SCM handle single UDID mismatch	153
Figure 73 – State diagram SCM verify parameters	155
Figure 74 – State diagram activate SN.....	157
Figure 75 – Safety function response time	160

Figure 76 – Assessment flow of devices	163
Figure A.1 – Structure of safety PDU	168
Figure A.2 – Error detection by the use of a CRC	168
Figure A.3 – Residual errors per hour	170
Figure A.4 – Residual errors per hour (payload 9-254).....	171

Withdrawn

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.

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

This bilingual version (2012-02) corresponds to the monolingual English version, published in 2010-06.

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

FDIS	Report on voting
65C/591A/FDIS	65C/603/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.

The French version of this standard has not been voted upon.

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.

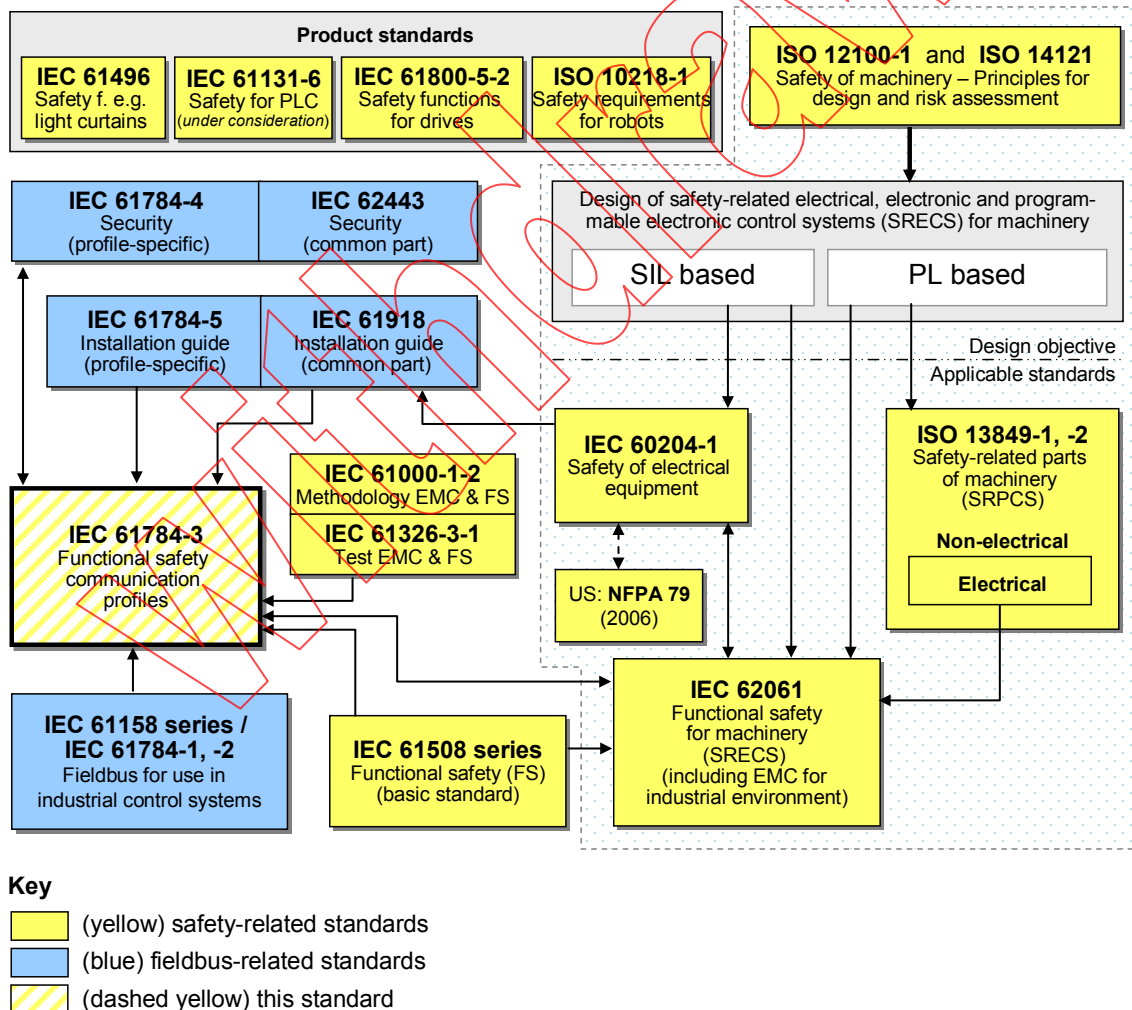
0 Introduction

0.1 General

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

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

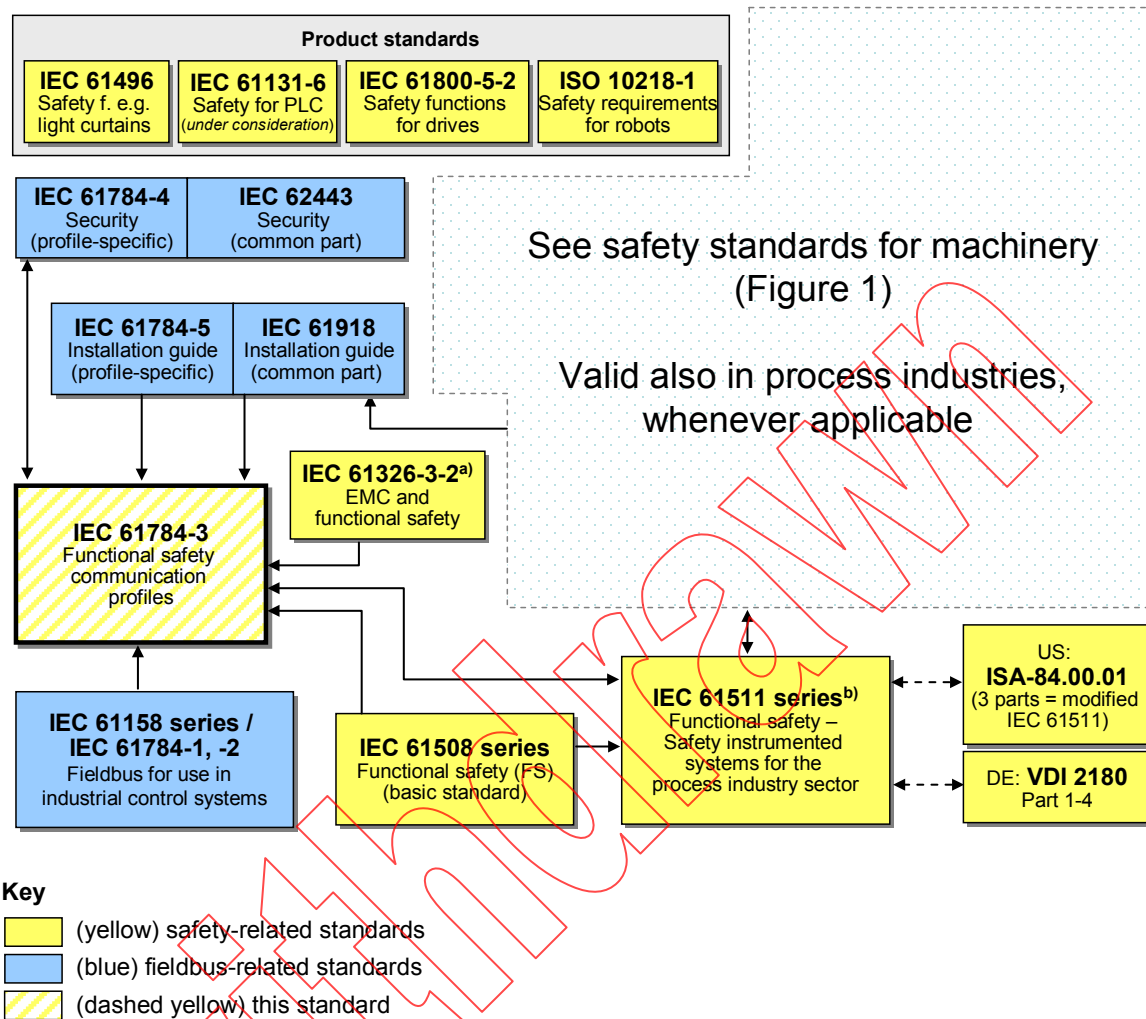
Figure 1 shows the relationships between this standard and relevant safety and fieldbus standards in a machinery environment.



NOTE Subclauses 6.7.6.4 (high complexity) and 6.7.8.1.6 (low complexity) of IEC 62061 specify the relationship between PL (Category) and SIL.

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

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



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

^b EN ratified.

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

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

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

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

This standard describes:

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

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 as follows, where the [xx] notation indicates the holder of the patent right:

AT 31/2007	[BR]	Anordnung und ein Verfahren zur sicheren Datenkommunikation über ein nicht sicheres Netzwerk
DE 102004055978.3	[BR]	Verfahren zur Zeitsynchronisation innerhalb eines sicherheitsgerichteten Netzwerkes
DE 102004055685.7	[BR]	Verfahren zur Abgrenzung eines sicheren Netzwerkes
DE 102004055684.9	[BR]	Verfahren zur Absicherung des Datentransfers in einem sicheren Netzwerk mit CRC's variabler Länge
EP 08150038	[BR]	Arrangement and a method for safe data communication via a non-safe network
US 11/970178	[BR]	Arrangement and a method for safe data communication via a non-safe network

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

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

Information may be obtained from:

[BR] Bernecker + Rainer
Industrie-Elektronik Ges.m.b.H.
B&R Strasse 1
5142 Eggelsberg
AUSTRIA

Tel.: +43 7748 6586– 0
Fax.: +43 7748 6586 – 26

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.

Withdrawn

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES –

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

1 Scope

This part of the IEC 61784-3 series 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.

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

IEC 61131-3, *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 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 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 8802-3*

IEC 61784-3:2010³, *Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions*

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*

³ In preparation.

SOMMAIRE

AVANT-PROPOS	187
0 Introduction	189
0.1 Généralités	189
0.2 Déclaration de droits de propriété	193
1 Domaine d'application	195
2 Références normatives	195
3 Termes, définitions, symboles, abréviations et conventions	196
3.1 Termes et définitions	196
3.1.1 Termes et définitions communs	196
3.1.2 CPF 13: Termes et définitions supplémentaires	200
3.2 Symboles et abréviations	202
3.2.1 Symboles et abréviations communs	202
3.2.2 CPF 13: Symboles et abréviations supplémentaires	202
3.3 Conventions	203
3.3.1 Valeurs hexadécimales	203
3.3.2 Valeurs binaires	204
3.3.3 Chiffres en caractères joker (métacaractères)	204
3.3.4 Diagrammes	204
4 Présentation de FSCP 13/1 (Ethernet POWERLINK safety)	204
4.1 Profil de communication de sécurité fonctionnelle 13/1	204
4.2 Aperçu technique	204
5 Généralités	205
5.1 Documents externes de spécifications applicables au profil	205
5.2 Exigences fonctionnelles de sécurité	205
5.3 Mesures de sécurité	206
5.4 Structure de la couche de communication de sécurité	208
5.5 Relations avec la FAL (et DLL, PhL)	209
5.5.1 Généralités	209
5.5.2 Types de données	209
6 Services de la couche de communication de sécurité	209
6.1 Modélisation	209
6.1.1 Modèle de référence	209
6.1.2 Modèle de communication	210
6.1.3 Rôles des dispositifs et topologie	211
6.2 Modèle de cycle de vie	215
6.2.1 Généralités	215
6.2.2 Concept, planification et mise en œuvre	215
6.2.3 Mise en service	217
6.2.4 Conditions de fonctionnement	218
6.2.5 Conditions de maintenance	219
6.3 Couche de communication non sécuritaire	219
6.3.1 Généralités	219
6.3.2 Exigences pour le transport des données	220
6.3.3 Protection et séparation des domaines	224
7 Protocole de couche de communication de sécurité	224

7.1	Format de PDU de sécurité	224
7.1.1	Généralités.....	224
7.1.2	Champ d'adresse (ADR)	226
7.1.3	Champ d'identification de PDU (ID)	226
7.1.4	Champ de longueur (LE).....	227
7.1.5	Champ de Temps consécutifs (CT).....	227
7.1.6	Champ de données utiles (DB0 à DBn).....	228
7.1.7	Champ de contrôle de redondance cyclique (CRC-8 / CRC-16)	228
7.1.8	Champ d'adresse de demande de temps (TADR).....	228
7.1.9	Champ de numéro distinctif de demande de temps (TR).....	228
7.1.10	UDID de codage SCM (UDID de SCM)	228
7.2	Objets de données de processus de sécurité (SPDO).....	229
7.2.1	Généralités.....	229
7.2.2	Types de télégrammes SPDO.....	229
7.2.3	Télégramme de données uniquement	229
7.2.4	Données avec télégramme de demande de temps	230
7.2.5	Données avec télégramme de réponse de temps	231
7.3	Objet de données de service de sécurité (SSDO).....	231
7.3.1	Généralités.....	231
7.3.2	Types de télégrammes SSDO.....	231
7.3.3	Services et protocoles SSDO.....	233
7.3.4	Lancer Téléchargement aval de SSDO	233
7.3.5	Téléchargement aval segmenté de SSDO.....	235
7.3.6	Lancer Téléchargement amont de SSDO	236
7.3.7	Téléchargement amont segmenté de SSDO	237
7.3.8	Abandonner SSDO	238
7.4	Gestion du réseau de sécurité (SNMT).....	240
7.4.1	Généralités.....	240
7.4.2	Types de télégramme SNMT	240
7.4.3	Services et protocoles SNMT.....	240
7.5	Dictionnaire d'objets de sécurité (SOD).....	252
7.5.1	Généralités.....	252
7.5.2	Définition d'une entrée de dictionnaire d'objets.....	253
7.5.3	Spécification de l'entrée type de données.....	259
7.5.4	Description des objets	261
7.6	Mise en correspondance de PDO sécuritaires	292
7.6.1	Généralités.....	292
7.6.2	SPDO d'émission.....	293
7.6.3	SPDO de réception.....	293
7.6.4	Paramètres de mise en correspondance SPDO	293
7.6.5	Exemple de mise en correspondance de SPDO	294
7.6.6	Gestion d'erreur de SPDO	296
7.7	Diagrammes d'états et diagrammes séquentiels	297
7.7.1	Objet de données de processus de sécurité (SPDO)	297
7.7.2	Synchronisation temporelle et validation.....	301
7.7.3	Objet de données de service de sécurité (SSDO)	312
7.7.4	Accès au SOD	314
7.7.5	Objet Gestion de réseau de sécurité (SNMT).....	320
7.7.6	Mise sous tension du SN	322

7.7.7	Mise hors tension du SN.....	326
7.7.8	Récupération du SN après Redémarrage / Erreur.....	326
7.7.9	Mise sous tension du SCM	326
7.7.10	Vérification d'Adresse.....	329
7.7.11	Mode de mise en service.....	331
7.7.12	Traitement d'une discordance d'UDID unique	331
7.7.13	Activer SN	335
7.7.14	Échange de dispositif	336
8	Gestion de la couche de communication de sécurité.....	336
8.1	Généralités.....	336
8.2	Objectifs du paramétrage	337
8.3	Configuration initiale d'un dispositif	337
8.3.1	Généralités.....	337
8.3.2	Mise en place du SD en configurant uniquement le SCM	337
8.3.3	Mise en place du ST en configurant chaque SN.....	338
8.4	Élimination des risques de paramétrage du mauvais dispositif.....	338
8.5	Mécanisme de vérification des paramètres	338
9	Exigences systémiques	338
9.1	Voyants et commutateurs	338
9.2	Recommandations d'installation.....	338
9.3	Temps de réponse de la fonction de sécurité.....	338
9.4	Durée des demandes	340
9.5	Contraintes de calcul des caractéristiques du système	340
9.5.1	Généralités.....	340
9.5.2	Limite du nombre de collecteurs d'information	340
9.5.3	Limite de taux de messages	340
9.5.4	Limite de données utiles des messages.....	340
9.5.5	Taux d'erreurs résiduelles	340
9.6	Maintenance.....	340
9.6.1	Informations de diagnostic.....	340
9.6.2	Remplacement de dispositifs sécuritaires	341
9.6.3	Modification.....	341
9.6.4	Remplacement d'une pièce de machine.....	341
9.6.5	Mise à jour de microprogrammes de nœuds sécuritaires	341
9.6.6	Contrôle périodique des machines	341
9.7	Manuel de sécurité	341
10	Évaluation	342
10.1	Généralités.....	342
10.2	Évaluation CP 13/1.....	342
10.3	Essai de conformité FSCP 13/1	342
10.4	Approbation de la sécurité fonctionnelle par un organisme d'évaluation compétent	342
10.5	Résumé.....	343
Annexe A (informative) Informations supplémentaires pour les profils de communication de sécurité fonctionnelle CPF 13		344
A.1	Calcul de la fonction de hachage.....	344
A.2	Erreurs stochastiques – considérations de caractère général	347
A.2.1	Généralités.....	347
A.2.2	Mécanismes de détection d'erreurs	347

A.2.3 Calculs	349
A.3 Erreurs stochastiques (Cas A)	349
A.3.1 Généralités.....	349
A.3.2 Contraintes.....	349
A.3.3 Taux d'erreurs résiduelles	350
A.3.4 Résumé.....	350
A.4 Erreurs stochastiques (Cas B)	350
A.4.1 Généralités.....	350
A.4.2 Contraintes.....	350
A.4.3 Considérations relatives à la probabilité d'erreurs sur les bits.....	351
A.4.4 Taux d'erreurs résiduelles (données utiles de 1 à 8).....	351
A.4.5 Taux d'erreurs résiduelles (données utiles de 9 à 254).....	351
A.4.6 Résumé.....	352
Annexe B (informative) Informations pour l'évaluation des profils de communication de sécurité fonctionnelle CPF 13	353
Bibliographie.....	354
Tableau 1 – Erreurs de communication et mesures de détection (cycliques)	206
Tableau 2 – Erreurs de communication et mesures de détection (acycliques)	207
Tableau 3 – Rôles des dispositifs.....	212
Tableau 4 – Format de PDU.....	225
Tableau 5 – Champ d'identification de PDU (ID).....	226
Tableau 6 – Combinaisons de champs ID utilisées	227
Tableau 7 – Identifiant de demande / réponse	227
Tableau 8 – Type de CRC en fonction de LE	227
Tableau 9 – Types de télégrammes SPDO (champ ID, bits 2, 3 et 4)	229
Tableau 10 – Champs du télégramme SPDO_Data_Only	230
Tableau 11 – Champs de télégramme SPDO_Data_with_Time_Request.....	230
Tableau 12 – Champs de télégramme SPDO_Data_with_Time_Response	231
Tableau 13 – Types de télégrammes SSDO (champ ID, bits 2, 3 et 4)	232
Tableau 14 – Codage binaire de la Commande d'accès SOD (SACmd).....	232
Tableau 15 – Champs de télégramme de SSDO_Service_Request Lancer Téléchargement aval	234
Tableau 16 – Champs de télégramme de SSDO_Service_Response Lancer Téléchargement aval	234
Tableau 17 – Champs de télégramme SSDO_Service_Request de téléchargement aval segmenté.....	235
Tableau 18 – Champs de télégramme SSDO_Service_Response de téléchargement aval segmenté	235
Tableau 19 – Champs de télégramme de SSDO_Service_Request Lancer Téléchargement amont	236
Tableau 20 – Champs de télégramme de SSDO_Service_Response Lancer Téléchargement amont	236
Tableau 21 – Champs de télégramme de SSDO_Service_Request de téléchargement amont segmenté	237
Tableau 22 – Champs de télégramme de SSDO_Service_Response de téléchargement amont segmenté	238

Tableau 23 – Champs de télégramme de SSDO_Service_Request de téléchargement amont segmenté	238
Tableau 24 – Champs de télégramme SSDO_Service_Response de téléchargement amont segmenté	239
Tableau 25 – Codes d'abandon SSDO	239
Tableau 26 – Types de télégrammes SNMT (champ ID, bits 2, 3 et 4)	240
Tableau 27 – Champs d'un télégramme SNMT_Request_UDID	241
Tableau 28 – Champs d'un télégramme SNMT_Response_UDID	241
Tableau 29 – Champs d'un télégramme SNMT_Assign_SADR	242
Tableau 30 – Champs d'un télégramme SNMT_SADR_Assigned	242
Tableau 31 – Champs d'un télégramme SNMT_SN_reset_guarding_SCM	243
Tableau 32 – Types de télégrammes de demande SNMT	243
Tableau 33 – Types de télégramme de réponse SNMT	244
Tableau 34 – Champs d'un télégramme SNMT_SN_set_to_PRE_OP	244
Tableau 35 – Champs d'un télégramme SNMT_SN_status_PRE_OP	244
Tableau 36 – Champs d'un télégramme SNMT_SN_set_to_OP	245
Tableau 37 – Champs d'un télégramme SNMT_SN_status_OP	246
Tableau 38 – Champs d'un télégramme SNMT_SN_busy	246
Tableau 39 – Champs d'un télégramme SNMT_SN_FAIL	246
Tableau 40 – Valeurs du groupe d'erreurs SNMT_SN_FAIL	247
Tableau 41 – Valeurs du code d'erreur SNMT_SN_FAIL	247
Tableau 42 – Champs d'un télégramme SNMT_SN_ACK	247
Tableau 43 – Champs d'un télégramme SNMT_SCM_set_to_STOP	248
Tableau 44 – Champs d'un télégramme SNMT_SCM_set_to_OP	249
Tableau 45 – Champs d'un télégramme SNMT_SCM_guard_SN	250
Tableau 46 – Champs de télégrammes SNMT_SN_status_OP/SNMT_SN_status_OP	250
Tableau 47 – Champs d'un télégramme SNMT_assign_additional_SADR	251
Tableau 48 – Champs d'un télégramme SNMT_assigned_additional_SADR	251
Tableau 49 – Champs d'un télégramme SNMT_assign_UDID_of_SCM	252
Tableau 50 – Champs d'un télégramme SNMT_assigned_UDID_of_SCM	252
Tableau 51 – Définition des types d'objet	253
Tableau 52 – Attributs d'accès pour des objets de données	255
Tableau 53 – Attributs de mise en correspondance SPDO pour des objets de données	255
Tableau 54 – Exemple de définition d'objets de type de données de base	255
Tableau 55 – Exemple de définition d'objets de type de données composé	256
Tableau 56 – Interprétation des sous-index	256
Tableau 57 – Spécification du sous-index NumberOfEntries	257
Tableau 58 – Spécification du sous-index d'objet de type RECORD	257
Tableau 59 – Spécification du sous-index d'objet de type ARRAY	258
Tableau 60 – Codage de StructureOfObject	259
Tableau 61 – Types de données de dictionnaire d'objets	259
Tableau 62 – Description du type de données composé 0021h	260
Tableau 63 – Description des sous-index composés 0021h	260
Tableau 64 – Objets normalisés	261

Tableau 65 – Objets de communication communs.....	261
Tableau 66 – Objets de communication de SPDO de réception.....	262
Tableau 67 – Objets de mise en correspondance de SPDO de réception.....	262
Tableau 68 – Objets de communication de SPDO d'émission.....	262
Tableau 69 – Objets de mise en correspondance de SPDO d'émission.....	262
Tableau 70 – Liste de DVI - SADR.....	263
Tableau 71 – Liste de SADR supplémentaires.....	263
Tableau 72 – Liste d'UDID - SADR.....	263
Tableau 73 – Objet 1001h: Registre d'erreurs.....	264
Tableau 74 – Interprétation des valeurs de l'objet 1001h: registre d'erreurs.....	264
Tableau 75 – Objet 1002h: Registre d'états du fabricant.....	264
Tableau 76 – Objet 1003h: Champ d'erreurs prédéfini.....	265
Tableau 77 – Objet 1003h sous-index 00h.....	265
Tableau 78 – Objet 1003h sous-index 01h.....	265
Tableau 79 – Objet 1003h sous-index 02h à FDh.....	266
Tableau 80 – Objet 100Ch: Sauvegarde.....	266
Tableau 81 – Objet 100Ch sous-index 00h.....	266
Tableau 82 – Objet 100Ch sous-index 01h.....	267
Tableau 83 – Objet 100Ch Sous-index 02h.....	267
Tableau 84 – Objet 100Dh: Intervalle de rafraîchissement de la sécurité de réinitialisation.....	267
Tableau 85 – Objet 1018h: Informations de fournisseur de dispositif.....	268
Tableau 86 – Objet 1018h sous-index 00h.....	268
Tableau 87 – Objet 1018h sous-index 01h.....	268
Tableau 88 – Objet 1018h sous-index 02h.....	269
Tableau 89 – Objet 1018h sous-index 03h.....	269
Tableau 90 – Objet 1018h sous-index 04h.....	269
Tableau 91 – Objet 1018h sous-index 05h.....	270
Tableau 92 – Objet 1018h sous-index 06h.....	270
Tableau 93 – Objet 1018h sous-index 07h.....	270
Tableau 94 – Structure du numéro de révision.....	271
Tableau 95 – Objet 1019h: Id unique de dispositif.....	271
Tableau 96 – Objet 101Ah: Téléchargement aval de paramètres.....	271
Tableau 97 – Objet 101Bh: Paramètres du SCM.....	272
Tableau 98 – Objet 101Bh sous-index 00h.....	272
Tableau 99 – Objet 101Bh sous-index 01h.....	272
Tableau 100 – Objet 1200h: Paramètre de communication commun.....	273
Tableau 101 – Objet 1200h sous-index 00h.....	273
Tableau 102 – Objet 1200h sous-index 01h.....	274
Tableau 103 – Objet 1200h sous-index 02h.....	274
Tableau 104 – Objet 1200h sous-index 03h.....	274
Tableau 105 – Objet 1200h sous-index 04h.....	275
Tableau 106 – Objet 1201h: Paramètre de communication SSDO.....	275

Tableau 107 – Objet 1201h sous-index 00h	275
Tableau 108 – Objet 1201h sous-index 01h	275
Tableau 109 – Objet 1201h sous-index 02h	276
Tableau 110 – Objet 1202h: Paramètre de communication SNMT	276
Tableau 111 – Objet 1202h sous-index 00h	276
Tableau 112 – Objet 1202h sous-index 01h	277
Tableau 113 – Objet 1202h sous-index 02h	277
Tableau 114 – Objet 1400h à 17FEh: Paramètre de communication RxSPDO	277
Tableau 115 – Objet 1400h à 17FEh sous-index 00h	278
Tableau 116 – Objet 1400h à 17FEh sous-index 01h	278
Tableau 117 – Objet 1400h à 17FEh sous-index 02h	278
Tableau 118 – Objet 1400h à 17FEh sous-index 03h	278
Tableau 119 – Objet 1400h à 17FEh sous-index 04h	279
Tableau 120 – Objet 1400h à 17FEh sous-index 05h	279
Tableau 121 – Objet 1400h à 17FEh sous-index 06h	279
Tableau 122 – Objet 1400h à 17FEh sous-index 07h	280
Tableau 123 – Objet 1400h à 17FEh sous-index 08h	280
Tableau 124 – Objet 1400h à 17FEh sous-index 09h	280
Tableau 125 – Objet 1400h à 17FEh sous-index 0Ah	281
Tableau 126 – Objet 1400h à 17FEh sous-index 0Bh	281
Tableau 127 – Objet 1400h à 17FEh sous-index 0Ch	281
Tableau 128 – Objet 1800h à 1BFEh: Paramètre de communication RxSPDO	282
Tableau 129 – Objet 1800h à 1BFEh sous-index 00h	282
Tableau 130 – Objet 1800h à 1BFEh sous-index 01h	282
Tableau 131 – Objet 1800h à 1BFEh sous-index 02h à FDh	282
Tableau 132 – Objet C00h à 1FFEh: Paramètre de communication TxSPDO	283
Tableau 133 – Objet 1C00h à 1FFEh sous-index 00h	283
Tableau 134 – Objet 1C00h à 1FFEh sous-index 01h	283
Tableau 135 – Objet 1C00h à 1FFEh sous-index 02h	284
Tableau 136 – Objet 1C00h à 1FFEh sous-index 03h	284
Tableau 137 – Objet C000h à C3FEh: Paramètre de mise en correspondance TxSPDO	284
Tableau 138 – Objet C000h à C3FEh sous-index 00h	285
Tableau 139 – Objet C000h à C3FEh sous-index 01h	285
Tableau 140 – Objet C000h à C3FEh sous-index 02h à FDh	285
Tableau 141 – Objet C400h à C7FEh: Liste de DVI - SADR	286
Tableau 142 – Objet C000h à C3FEh sous-index 00h	286
Tableau 143 – Objet C000h à C3FEh sous-index 01h	286
Tableau 144 – Objet C000h à C3FEh sous-index 02h	286
Tableau 145 – Objet C000h à C3FEh sous-index 03h	287
Tableau 146 – Objet C000h à C3FEh sous-index 04h	287
Tableau 147 – Objet C000h à C3FEh sous-index 05h	287
Tableau 148 – Objet C000h à C3FEh sous-index 06h	287
Tableau 149 – Objet C000h à C3FEh sous-index 07h	288

Tableau 150 – Objet C000h à C3FEh sous-index 08h	288
Tableau 151 – Objet C000h à C3FEh sous-index 09h	288
Tableau 152 – Objet C000h à C3FEh sous-index 0Ah	289
Tableau 153 – Objet C000h à C3FEh sous-index 0Bh	289
Tableau 154 – Objet C801h à CBFFh: Liste de SADR supplémentaires	289
Tableau 155 – Objet C801h à CBFFh sous-index 00h	290
Tableau 156 – Objet C801h à CBFFh sous-index 01h	290
Tableau 157 – Objet C801h à CBFFh sous-index 02h	290
Tableau 158 – Exemple d'objet: Liste de SADR supplémentaires	291
Tableau 159 – Objet CC01h à CFFFh: Liste d'UDID - SADR	291
Tableau 160 – Objet C801h à CBFFh sous-index 00h	291
Tableau 161 – Objet C801h à CBFFh sous-index 01h à FDh	292
Tableau 162 – Exemple de Liste d'UDID - SADR	292
Tableau 163 – Structure d'entrées de mise en correspondance SPDO	293
Tableau 164 – Exemple 1 de tableau de mise en correspondance	294
Tableau 165 – Exemple 2 de tableau de mise en correspondance	295
Tableau 166 – Exemple 3 de tableau de mise en correspondance	295
Tableau 167 – Exemple 4 de tableau de mise en correspondance	295
Tableau 168 – Exemple 5 de tableau de mise en correspondance	295
Tableau 169 – Exemple 6 de tableau de mise en correspondance	296
Tableau 170 – Exemple 7 de tableau de mise en correspondance	296
Tableau 171 – Description des éléments de producteur de communication SPDO	298
Tableau 172 – Description des états du producteur de communication SPDO	298
Tableau 173 – Description des éléments de consommateur de communication SPDO	299
Tableau 174 – Description des états de consommateur de communication SPDO	300
Tableau 175 – Description des éléments de validation de télégramme de consommateur de communication SPDO	301
Tableau 176 – Description des états de validation de télégramme de consommateur de communication SPDO	301
Tableau 177 – Description des éléments de synchronisation temporelle	303
Tableau 178 – Description des éléments de validation temporelle	305
Tableau 179 – Description des éléments de synchronisation temporelle étendue	309
Tableau 180 – Description des éléments de producteur de synchronisation temporelle	310
Tableau 181 – Description des états du producteur de synchronisation temporelle	310
Tableau 182 – Description des éléments de consommateur de synchronisation temporelle	311
Tableau 183 – Description des états du consommateur de synchronisation temporelle	312
Tableau 184 – Description des éléments de client SSDO	313
Tableau 185 – Description des états du client SSDO	313
Tableau 186 – Description des états de serveur SSDO	314
Tableau 187 – Description des éléments d'accès au SOD	315
Tableau 188 – Description des éléments du client d'accès segmenté au SOD	317
Tableau 189 – Description des états du client d'accès au SOD en téléchargement segmenté	317

Tableau 190 – Description des éléments du serveur d'accès segmenté au SOD	319
Tableau 191 – Description des états du serveur d'accès segmenté au SOD	320
Tableau 192 – Description des éléments de maître SNMT	321
Tableau 193 – Description des états de maître SNMT	321
Tableau 194 – Description des états d'esclave SNMT	322
Tableau 195 – Description des états de mise sous tension du SN	322
Tableau 196 – Relations entre états et objets de communication	323
Tableau 197 – Description des éléments d'états pré-opérationnels du SN	324
Tableau 198 – Description des états pré-opérationnels du SN	325
Tableau 199 – Description des éléments d'état opérationnel du SN	326
Tableau 200 – Description des états Opérationnels du SN	326
Tableau 201 – Description des états de mise sous tension du SCM	327
Tableau 202 – Relations entre états et objets de communication	327
Tableau 203 – Description des éléments d'état opérationnel du SCM	329
Tableau 204 – Description des états opérationnels du SCM	329
Tableau 205 – Description des éléments de vérification d'adresse	331
Tableau 206 – Description des états de vérification d'adresse	331
Tableau 207 – Description des états du traitement SCM de discordance d'UDID unique	332
Tableau 208 – Description des états de la Vérification SCM de paramètres	335
Tableau 209 – Description des états d'activation du SN	336
Figure 1 – Relations entre la CEI 61784-3 et d'autres normes (machines)	191
Figure 2 – Relations entre la CEI 61784-3 et d'autres normes (processus)	193
Figure 3 – Exemple de relation producteur/consommateur	205
Figure 4 – Exemple de relation client/serveur	205
Figure 5 – Structure de la couche de communication	208
Figure 6 – Canal de communication de sécurité	209
Figure 7 – Communication type entre producteur et consommateur	210
Figure 8 – Communication étendue entre producteur et consommateur	211
Figure 9 – Communication client / serveur	211
Figure 10 – Aperçu de la topologie	212
Figure 11 – Protection de domaine de sécurité (exemple)	214
Figure 12 – Séparation entre domaines de sécurité (exemple)	214
Figure 13 – Exemple de flux de données	218
Figure 14 – Modèle de communication	220
Figure 15 – Transport de SPDO	221
Figure 16 – Transport de SSDO	222
Figure 17 – Représentation des données de diagnostic	223
Figure 18 – PDU de sécurité dans une PDU CP 13/1	224
Figure 19 – PDU de sécurité pour n = 0 à 8 octets de données utiles	225
Figure 20 – PDU de sécurité pour n = 9 à 254 octets de données utiles	225
Figure 21 – Télégramme SPDO_Data_Only	229

Figure 22 – Télégramme SPDO_Data_with_Time_Request.....	230
Figure 23 – Télégramme SPDO_Data_with_Time_Response	231
Figure 24 – Protocoles de téléchargement aval de SSDO	233
Figure 25 – Protocoles de téléchargement amont de SSDO	233
Figure 26 – Protocole de lancement de téléchargement aval de SSDO	234
Figure 27 – Protocole de téléchargement aval segmenté de SSDO	235
Figure 28 – Protocole de lancement de téléchargement amont de SSDO	236
Figure 29 – Protocole de téléchargement amont segmenté de SSDO.....	237
Figure 30 – Protocole Abandonner SSDO	238
Figure 31 – Protocole de demande / réponse d'UDID	241
Figure 32 – Protocole d'attribution d'une SADR	242
Figure 33 – Protocole du service Réinitialiser intervalle de sauvegarde de nœud.....	243
Figure 34 – Protocole SN mis à l'état pré-opérationnel.....	244
Figure 35 – Protocole SN mis à l'état opérationnel.....	245
Figure 36 – Protocole Acquitter SN	247
Figure 37 – Protocole SN mis à l'état arrêté	248
Figure 38 – Protocole SCM mis à l'état opérationnel.....	249
Figure 39 – Protocole de sauvegarde du nœud	249
Figure 40 – Protocole d'attribution d'une SADR supplémentaire	250
Figure 41 – Protocole d'Attribution d'UDID de SCM.....	252
Figure 42 – Exemple de mise en correspondance de SPDO.....	294
Figure 43 – Diagramme d'état de TxSPDO.....	297
Figure 44 – Producteur de communication SPDO	297
Figure 45 – Diagramme d'état de RxSPDO	299
Figure 46 – Consommateur de communication SPDO	299
Figure 47 – Diagramme d'état des données de processus.....	300
Figure 48 – Synchronisation temporelle et validation	302
Figure 49 – Synchronisation temporelle détaillée	303
Figure 50 – Calcul du délai de propagation	304
Figure 51 – Validation temporelle, limites de l'explication du délai de propagation	305
Figure 52 – Synchronisation temporelle sur un réseau non sécuritaire	307
Figure 53 – Explication de la synchronisation temporelle	308
Figure 54 – Échec de la synchronisation temporelle.....	308
Figure 55 – Diagramme d'état du producteur de synchronisation temporelle	310
Figure 56 – Diagramme d'état du consommateur de synchronisation temporelle	311
Figure 57 – Diagramme d'état de client SSDO	313
Figure 58 – Diagramme d'état de serveur SSDO	314
Figure 59 – Accès accéléré au SOD	315
Figure 60 – Diagramme d'état du client d'accès au SOD en téléchargement segmenté	316
Figure 61 – Accès au SOD en téléchargement segmenté.....	317
Figure 62 – Diagramme d'état du serveur d'accès au SOD en téléchargement segmenté.....	319
Figure 63 – Diagramme d'état de Maître SNMT.....	320

Figure 64 – Diagramme d'état d'esclave SNMT	321
Figure 65 – Diagramme d'état de mise sous tension du SN	322
Figure 66 – Diagramme d'état pré-opérationnel du SN	324
Figure 67 – Diagramme d'état opérationnel du SN	325
Figure 68 – Télégramme de sauvegarde	326
Figure 69 – Diagramme d'état de mise sous tension du SCM	327
Figure 70 – Diagramme d'état opérationnel du SCM	328
Figure 71 – Diagramme d'état de la vérification SCM d'adresse	330
Figure 72 – Diagramme d'état du traitement SCM de discordance d'UDID unique	332
Figure 73 – Diagramme d'état de la Vérification SCM de paramètres	334
Figure 74 – Diagramme d'état "activer SN"	336
Figure 75 – Temps de réponse de la fonction de sécurité	339
Figure 76 – Organigramme d'évaluation des dispositifs	342
Figure A.1 – Structure d'une PDU de Sécurité	348
Figure A.2 – Détection d'erreurs par CRC	348
Figure A.3 – Erreurs résiduelles par heure	350
Figure A.4 – Erreurs résiduelles par heure (données utiles de 9 à 254)	352

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 (CEI) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de la CEI). La CEI 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, la CEI – 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 la CEI"). 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 la CEI, participent également aux travaux. La CEI 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 la CEI concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de la CEI intéressés sont représentés dans chaque comité d'études.
- 3) Les Publications de la CEI se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de la CEI. Tous les efforts raisonnables sont entrepris afin que la CEI s'assure de l'exactitude du contenu technique de ses publications; la CEI 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 la CEI s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de la CEI dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de la CEI et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
- 5) La CEI 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 la CEI. La CEI 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 la CEI, 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 la CEI, 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 la CEI ou de toute autre Publication de la CEI, 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.

La Norme internationale CEI 61784-3-13 a été établie par le sous-comité 65C: Réseaux de communication industriels, du comité d'études 65 de la CEI: Mesure, commande et automation dans les processus industriels.

La présente version bilingue (2012-02) correspond à la version anglaise monolingue publiée en 2010-06.

Le texte anglais de cette norme est issu des documents 65C/591A/FDIS et 65C/603/RVD.

Le rapport de vote 65C/603/RVD donne toute information sur le vote ayant abouti à l'approbation de cette norme.

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

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

Une liste de toutes les parties de la série CEI 61784-3, présentées sous le titre général *Réseaux de communication industriels – Profils – Bus de terrain de sécurité fonctionnelle*, est disponible sur le site web de la CEI.

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 la CEI sous "<http://webstore.iec.ch>" dans les données relatives à la publication recherchée. A 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 garde 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.

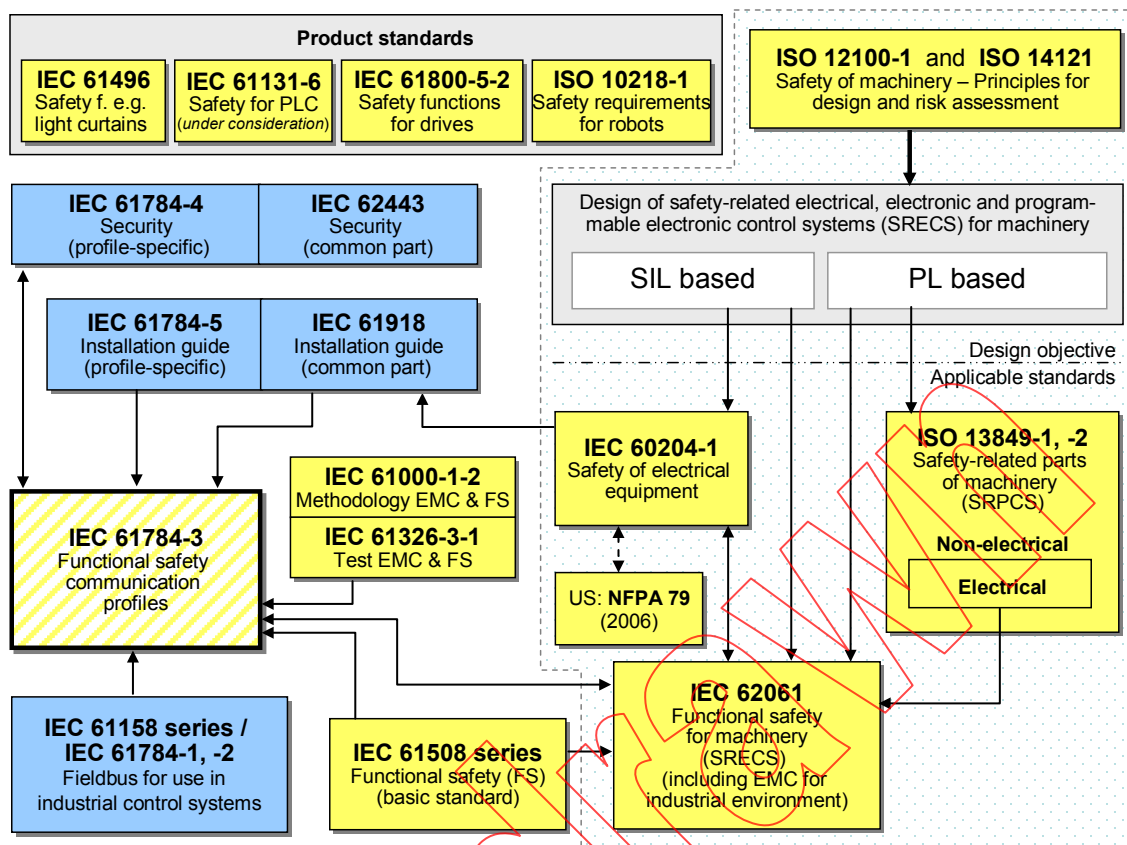
0 Introduction

0.1 Généralités

La norme CEI 61158 relative aux bus de terrain, ainsi que ses normes associées CEI 61784-1 et CEI 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. Ainsi, de nombreuses améliorations des bus de terrain se développent pour traiter de domaines non encore normalisés tels que les applications en temps réel relatives à la sécurité et de sûreté.

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

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



Key

- (yellow) safety-related standards
- (blue) fieldbus-related standards
- (dashed yellow) this standard

Légende

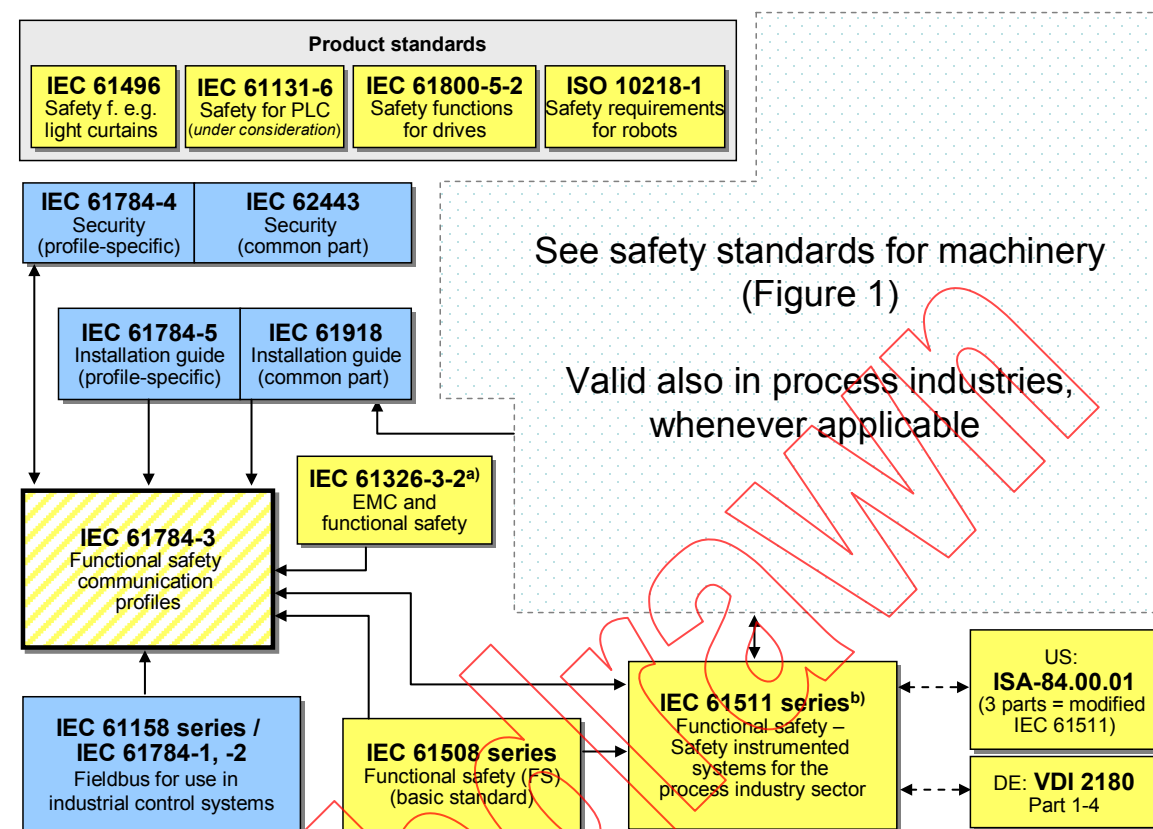
Anglais	Français
Product standards	Normes de produits
Safety function, e.g. light curtains	Fonction de sécurité, par exemple rideaux de lumière
Safety for PLC (under consideration)	Sécurité relative aux automates programmables (à l'étude)
Safety functions for drives	Fonctions de sécurité applicables aux entraînements
Safety requirements for robots	Exigences de sécurité applicables aux robots
Safety of machinery - ... assessment	Sécurité des machines – principes généraux de conception et appréciation du risque
Security (profile-specific)	Sûreté (spécifique au profil)
Security (common part)	Sûreté (partie commune)
Design of safety-related 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)

Anglais	Français
Design objective	Objectif de conception
Applicable standards	Normes applicables
Safety of electrical equipment	Sécurité des équipements électriques
Safety-related parts of machinery	Parties des systèmes de commande relatives à la sécurité
Non-electrical	Non électrique
Electrical	Électrique
Methodology EMC & functional safety	Méthodologie en matière de compatibilité électromagnétique & sécurité fonctionnelle
Test EMC & functional safety	Essai CEM et sécurité fonctionnelle
Functional safety communication profiles	Profils de communication de sécurité fonctionnelle
IEC 61158 series / Fieldbus for use in industrial control systems	Série CEI 61158 / Bus de terrain pour utilisation dans des systèmes de commande industriels
IEC 61508 series, Functional safety (basic standard)	Série CEI 61508 Sécurité fonctionnelle (norme de base)
Functional safety for machinery for industrial environment)	Sécurité fonctionnelle des systèmes de commande électriques, électroniques et électroniques programmables (y compris les interférences électromagnétiques dans l'environnement industriel)
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
IEC	CEI

NOTE Les paragraphes 6.7.6.4 (complexité élevée) et 6.7.8.1.6 (faible complexité) de la CEI 62061 précisent la relation entre le niveau de performance PL (catégorie) et le niveau d'intégrité de sécurité SIL.

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

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



Key

- (yellow) safety-related standards
- (blue) fieldbus-related standards
- (dashed yellow) this standard

Légende

Anglais	Français
Product standards	Normes de produits
Safety function, e.g. light curtains	Fonction de sécurité, par exemple barrières photo électriques
Safety for PLC (under consideration)	Sécurité relative aux automates programmables (à l'étude)
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

Anglais	Français
IEC 61326-3-2 a) EMC and functional safety	CEI 61326-3-2 a) CEM & sécurité fonctionnelle
IEC 61158 series/ IEC 61784-1-2, Fieldbus for use in industrial control systems	Série CEI 61158/ CEI 61784-1,-2 Bus de terrain pour utilisation dans des systèmes de commande industriels
IEC 61508 series, Functional safety (basic standard)	Série CEI 61508 Sécurité fonctionnelle (norme de base)
IEC 61511 series ^b) Functional safety–safety instrumented systems for the process industry sector	Série CEI 61511 ^b) sécurité fonctionnelle – systèmes instrumentés de sécurité pour le secteur des industries de transformation
US: ISA 84.00.1 (3 parts = modified IEC 61511)	US: ISA 84.00.1 (3 parties = CEI 61511 modifiée)
DE : VDI 2180 Part 1 –4	DE : VDI 2180 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; autrement, la CEI 61326-3-1.

^b EN ratifiée.

Figure 2 – Relations entre la CEI 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 CEI 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 sécuritaire, 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 retenu au sein du système – la mise en œuvre du profil de communication de sécurité fonctionnelle dans un dispositif normal ne suffit pas à le qualifier de dispositif de sécurité.

La présente norme décrit:

- les principes de base de mise en œuvre des exigences de la série CEI 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;
- la description individuelle des profils de sécurité fonctionnelle pour plusieurs familles de profils de communication dans les CEI 61784-1 et CEI 61784-2;
- les extensions de la couche de sécurité aux sections relatives au service et aux protocoles de communication de la série CEI 61158.

0.2 Déclaration de droits de propriété

La commission électrotechnique internationale (CEI) attire l'attention sur le fait qu'il est déclaré que la conformité avec le présent document peut impliquer l'utilisation de brevets concernant les profils de communication de sécurité fonctionnelle pour la famille 13 comme suit, où la notation [xx] désigne le détenteur des droits de propriété:

AT 31/2007	[BR]	Anordnung und ein Verfahren zur sicheren Datenkommunikation über ein nicht sicheres Netzwerk
DE 102004055978.3	[BR]	Verfahren zur Zeitsynchronisation innerhalb eines sicherheitsgerichteten Netzwerkes
DE 102004055685.7	[BR]	Verfahren zur Abgrenzung eines sicheren Netzwerkes
DE 102004055684.9	[BR]	Verfahren zur Absicherung des Datentransfers in einem sicheren Netzwerk mit CRC's variabler Länge
EP 08150038	[BR]	Arrangement and a method for safe data communication via a non-safe network
US 11/970178	[BR]	Arrangement and a method for safe data communication via a non-safe network

La CEI ne prend pas position eu égard à la preuve, la validité et la portée de ces droits de propriété.

Les détenteurs de ces droits de propriété ont donné l'assurance à la CEI qu'ils consentent à négocier des licences avec des demandeurs du monde entier, en des termes et à des conditions raisonnables et non discriminatoires. De ce fait, les déclarations des détenteurs desdits droits de brevets sont enregistrées auprès de la CEI.

Des informations peuvent être obtenues auprès de:

[BR] Bernecker + Rainer
Industrie-Elektronik Ges.m.b.H.
B&R Strasse 1
5142 Eggelsberg
AUTRICHE

Tél.: +43 7748 6586– 0
Télécopie: +43 7748 6586 – 26

L'attention est par ailleurs attirée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues autres que ceux identifiés ci-dessus. La CEI ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et de ne pas avoir signalé leur existence.

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 CEI 61784-3 spécifie une couche de communication sécuritaire (services et protocole) fondée sur la CPF 13 de la CEI 61784-2 et le type 13 de la CEI 61158. Elle identifie les principes applicables aux communications de sécurité fonctionnelle définies dans la CEI 61784-3, et appropriés à cette couche de communication 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 partie ¹ définit les mécanismes de transmission des messages propres à la sécurité entre les participants d'un réseau réparti, en utilisant la technologie de bus de terrain conformément aux exigences de la série CEI 61508 ² 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 de dispositifs 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 dispositif normal ne suffit pas à le qualifier de dispositif de sécurité.

2 Références normatives

Les documents de référence suivants sont indispensables pour l'application 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).

CEI 61131-3, *Programmable controllers – Part 3: Programming languages* (disponible uniquement en anglais)

IEC 61158-3-13, *Industrial communication networks – Fieldbus specifications – Part 3-13: Data-link layer service definition – Type 13 elements* (disponible uniquement en anglais)³

IEC 61158-4-13, *Industrial communication networks – Fieldbus specifications – Part 4-13: Data-link layer protocole specification – Type 13 elements* (disponible uniquement en anglais)

IEC 61158-5-13, *Industrial communication networks – Fieldbus specifications – Part 5-13: Application layer service definition – Type 13 elements* (disponible uniquement en anglais)

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

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

³ Les publications monolingues des séries IEC 61158 et IEC 61784 sont actuellement en cours de traduction.

IEC 61158-6-13, *Industrial communication networks – Fieldbus specifications – Part 6-13: Application layer protocole specification – Type 13 elements* (disponible uniquement en anglais)

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

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

IEC 61784-3:2010⁴, *Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions* (disponible uniquement en anglais)

IEC 61918, *Industrial communication networks – Installation of communication networks in industrial premises* (disponible uniquement en anglais)

ISO/CEI 19501, *Technologies de l'information – Traitement distribué ouvert – Langage de modélisation unifié (UML), version 1.4.2*

⁴ En cours d'élaboration.