



BSI Standards Publication

Industrial communication networks — Profiles -

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

NO COPYING WITHOUT BSI PERMISSION EXCEPT AS PERMITTED BY COPYRIGHT LAW

raising standards worldwide™

National foreword

This British Standard is the UK implementation of EN 61784-3-13:2010.

The UK participation in its preparation was entrusted to Technical Committee AMT/7, Industrial communications: process measurement and control, including fieldbus.

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

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© BSI 2010

ISBN 978 0 580 72033 8

ICS 25.040.40; 35.100.05

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

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 September 2010.

Amendments issued since publication

Date	Text affected
------	---------------

**Industrial communication networks -
Profiles -
Part 3-13: Functional safety fieldbuses -
Additional specifications for CPF 13
(IEC 61784-3-13:2010)**

Réseaux de communication industriels -
Partie 3-13: Bus de terrain à sécurité
fonctionnelle -
Spécifications complémentaires
pour le CPF 13
(CEI 61784-3-13:2010)

Industrielle Kommunikationsnetze -
Profile -
Teil 3-13: Funktional sichere Übertragung
bei Feldbussen -
Zusätzliche Festlegungen
für die Kommunikationsprofilfamilie 13
(IEC 61784-3-13:2010)

This European Standard was approved by CENELEC on 2010-07-01. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

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

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

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

CENELEC

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

Management Centre: Avenue Marnix 17, B - 1000 Brussels

Foreword

The text of document 65C/591A/FDIS, future edition 1 of IEC 61784-3-13, prepared by SC 65C, Industrial networks, of IEC TC 65, Industrial-process measurement, control and automation, was submitted to the IEC-CENELEC parallel vote and was approved by CENELEC as EN 61784-3-13 on 2010-07-01.

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

The following dates were fixed:

- | | | |
|--|-------|------------|
| – latest date by which the EN has to be implemented at national level by publication of an identical national standard or by endorsement | (dop) | 2011-04-01 |
| – latest date by which the national standards conflicting with the EN have to be withdrawn | (dow) | 2013-07-01 |

Annex ZA has been added by CENELEC.

Endorsement notice

The text of the International Standard IEC 61784-3-13:2010 was approved by CENELEC as a European Standard without any modification.

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

IEC 60204-1	NOTE	Harmonized as EN 60204-1.
IEC 61131-2	NOTE	Harmonized as EN 61131-2.
IEC 61158 series	NOTE	Harmonized in EN 61158 series (not modified).
IEC 61326-3-1	NOTE	Harmonized as EN 61326-3-1.
IEC 61326-3-2	NOTE	Harmonized as EN 61326-3-2.
IEC 61496 series	NOTE	Harmonized in EN 61496 series (partially modified).
IEC 61508-1:2010	NOTE	Harmonized as EN 61508-1:2010 (not modified).
IEC 61508-4:2010	NOTE	Harmonized as EN 61508-4:2010 (not modified).
IEC 61508-5:2010	NOTE	Harmonized as EN 61508-5:2010 (not modified).
IEC 61508-6:2010	NOTE	Harmonized as EN 61508-6:2010 (not modified).
IEC 61511 series	NOTE	Harmonized in EN 61511 series (not modified).
IEC 61784-1	NOTE	Harmonized as EN 61784-1.
IEC 61784-5 series	NOTE	Harmonized in EN 61784-5 series (not modified).
IEC 61800-5-2	NOTE	Harmonized as EN 61800-5-2.
IEC 62061	NOTE	Harmonized as EN 62061.
ISO 10218-1	NOTE	Harmonized as EN ISO 10218-1.
ISO 12100-1	NOTE	Harmonized as EN ISO 12100-1.
ISO 13849-1	NOTE	Harmonized as EN ISO 13849-1.
ISO 13849-2	NOTE	Harmonized as EN ISO 13849-2.

Annex ZA (normative)

Normative references to international publications with their corresponding European publications

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.

NOTE When an international publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
IEC 61131-3	-	Programmable controllers - Part 3: Programming languages	EN 61131-3	-
IEC 61158-3-13	-	Industrial communication networks - Fieldbus specifications - Part 3-13: Data-link layer service definition - Type 13 elements	EN 61158-3-13	-
IEC 61158-4-13	-	Industrial communication networks - Fieldbus specifications - Part 4-13: Data-link layer protocol specification - Type 13 elements	EN 61158-4-13	-
IEC 61158-5-13	-	Industrial communication networks - Fieldbus specifications - Part 5-13: Application layer service definition - Type 13 elements	EN 61158-5-13	-
IEC 61158-6-13	-	Industrial communication networks - Fieldbus specifications - Part 6-13: Application layer protocol specification - Type 13 elements	EN 61158-6-13	-
IEC 61508	Series	Functional safety of electrical/electronic/programmable electronic safety-related systems	EN 61508	Series
IEC 61784-2	-	Industrial communication networks - Profiles - Part 2: Additional fieldbus profiles for real-time networks based on ISO/IEC 8802-3	EN 61784-2	-
IEC 61784-3	2010	Industrial communication networks - Profiles - Part 3: Functional safety fieldbuses - General rules and profile definitions	EN 61784-3	2010
IEC 61918	-	Industrial communication networks - Installation of communication networks in industrial premises	EN 61918	-
ISO/IEC 19501	-	Information technology - Open Distributed Processing - Unified Modeling Language (UML)	-	-

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	143

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	104

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 – 1Object 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

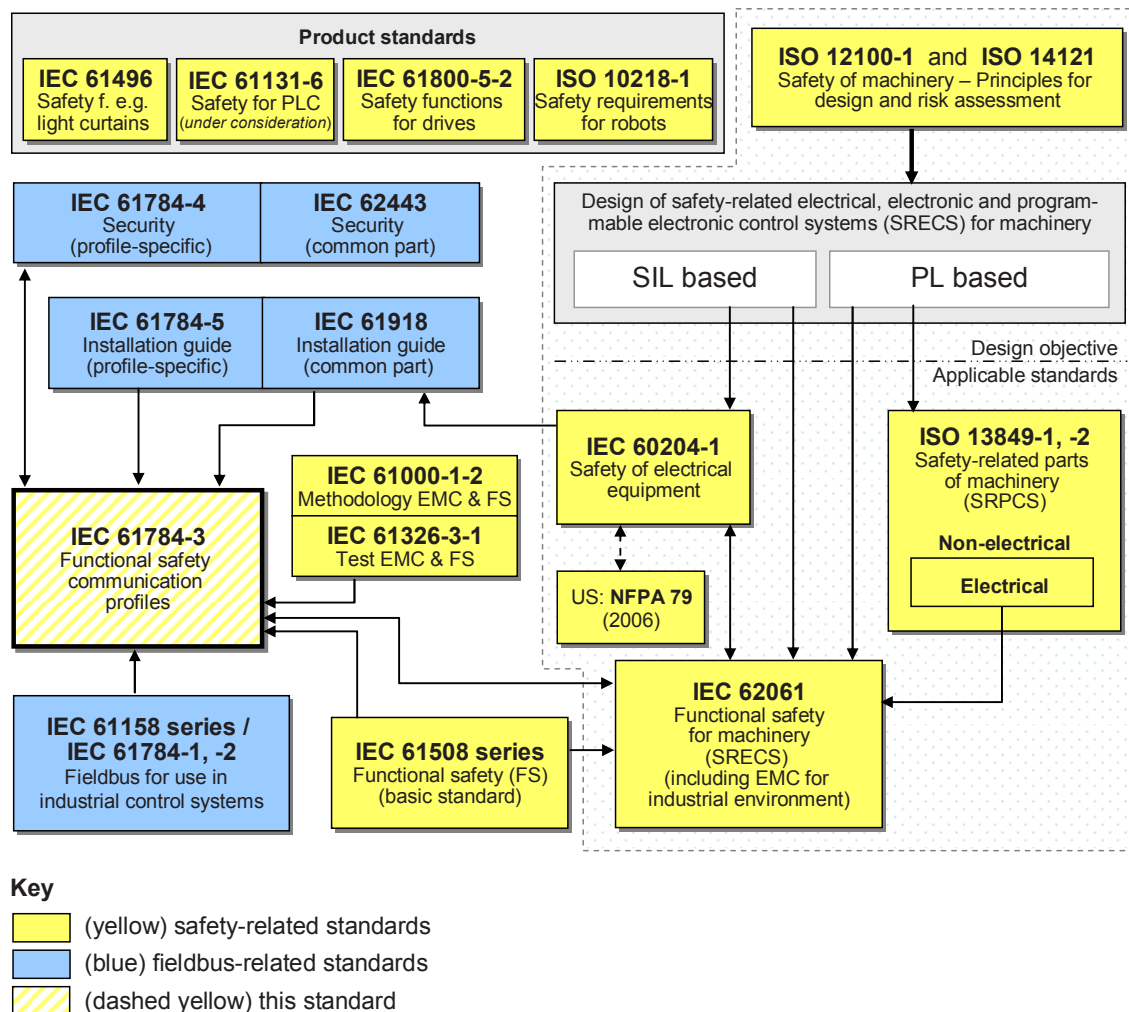
0 Introduction

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.

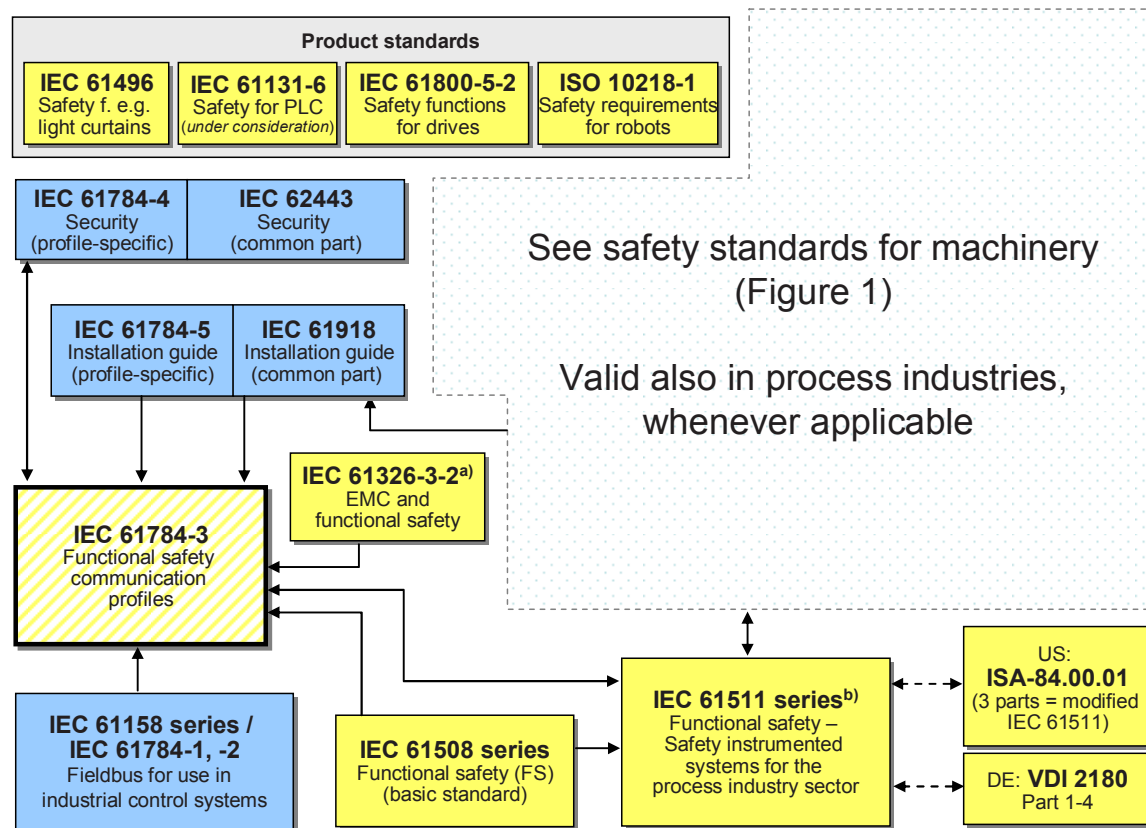
Figure 1 shows the relationships between this standard and relevant safety and fieldbus standards in a machinery environment.



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.



Key

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

^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.

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 Terms, definitions, symbols, abbreviated terms and conventions

3.1 Terms and definitions

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

3.1.1 Common terms and definitions

3.1.1.1 availability

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

3.1.1.2 black channel

communication channel without available evidence of design or validation according to IEC 61508

3.1.1.3 communication channel

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

3.1.1.4 communication system

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

3.1.1.5 connection

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

3.1.1.6 Cyclic Redundancy Check (CRC)

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

<method> procedure used to calculate the redundant data

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

³ In preparation.

NOTE 2 See also [37], [38]⁴.

3.1.1.7

error

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

[IEC 61508-4:2010⁵], [IEC 61158]

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

NOTE 2 Errors do not necessarily result in a *failure* or a *fault*.

3.1.1.8

failure

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

NOTE 1 The definition in IEC 61508-4 is the same, with additional notes.

[IEC 61508-4:2010, modified], [ISO/IEC 2382-14.01.11, modified]

NOTE 2 Failure may be due to an *error* (for example, problem with hardware/software design or message disruption)

3.1.1.9

fault

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

NOTE IEC 191-05-01 defines “fault” as a state characterized by the inability to perform a required function, excluding the inability during preventive maintenance or other planned actions, or due to lack of external resources.

[IEC 61508-4:2010, modified], [ISO/IEC 2382-14.01.10, modified]

3.1.1.10

fieldbus

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

3.1.1.11

fieldbus system

system using a *fieldbus* with connected devices

3.1.1.12

frame

denigrated synonym for DLPDU

3.1.1.13

hash function

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

NOTE 1 Hash functions can be used to detect data corruption.

NOTE 2 Common hash functions include parity, checksum or CRC.

⁴ Figures in square brackets refer to the bibliography.

⁵ To be published.

[IEC/TR 62210, modified]

3.1.1.14

hazard

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

3.1.1.15

message

ordered series of octets intended to convey information

[ISO/IEC 2382-16.02.01, modified]

3.1.1.16

performance level (PL)

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

[ISO 13849-1]

3.1.1.17

redundancy

existence of means, in addition to the means which would be sufficient for a functional unit to perform a required function or for data to represent information

NOTE The definition in IEC 61508-4 is the same, with additional example and notes.

[IEC 61508-4:2010, modified], [ISO/IEC 2382-14.01.12, modified]

3.1.1.18

reliability

probability that an automated system can perform a required function under given conditions for a given time interval (t_1, t_2)

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

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

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

NOTE 4 Reliability differs from availability.

[IEC 62059-11, modified]

3.1.1.19

risk

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

NOTE For more discussion on this concept see Annex A of IEC 61508-5:2010⁶.

[IEC 61508-4:2010], [ISO/IEC Guide 51:1999, definition 3.2]

3.1.1.20

safety communication layer (SCL)

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

⁶ To be published.

3.1.1.21

safety data

data transmitted across a safety network using a safety protocol

NOTE The Safety Communication Layer does not ensure safety of the data itself, only that the data is transmitted safely.

3.1.1.22

safety device

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

3.1.1.23

safety function

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

NOTE The definition in IEC 61508-4 is the same, with an additional example and reference.

[IEC 61508-4:2010, modified]

3.1.1.24

safety function response time

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

NOTE This concept is introduced in IEC 61784-3:2010⁷, 5.2.4 and addressed by the functional safety communication profiles defined in this part.

3.1.1.25

safety integrity level (SIL)

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

NOTE 1 The target failure measures (see IEC 61508-4:2010, 3.5.17) for the four safety integrity levels are specified in Tables 2 and 3 of IEC 61508-1:2010⁸.

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

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

[IEC 61508-4:2010]

3.1.1.26

safety measure

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

NOTE 1 In practice, several safety measures are combined to achieve the required safety integrity level.

NOTE 2 Communication *errors* and related safety measures are detailed in IEC 61784-3:2010, 5.3 and 5.4.

⁷ In preparation.

⁸ To be published.

3.1.1.27

safety-related application

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

3.1.1.28

safety-related system

system performing *safety functions* according to IEC 61508

3.1.1.29

slave

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

3.1.1.30

time stamp

time information included in a *message*

3.1.2 CPF 13: Additional terms and definitions

3.1.2.1

bit error rate

likelihood of a bit misinterpretation due to electrical noise

3.1.2.2

Device Vendor Information (DVI)

information for identifying a safety node

3.1.2.3

Safety Address (SADR)

address of a safety node within a safety domain

3.1.2.4

Safety Configuration Manager (SCM)

service which is responsible to manage safety related services

NOTE Examples of managed safety related services are configuration, parameterization.

3.1.2.5

Safety Node (SN)

node with safety function

3.1.2.6

Safety Domain (SD)

address space for up to 1023 safety nodes

3.1.2.7

Safety Domain Gateway (SDG)

gateway to share data between different safety domains

3.1.2.8

Safety Domain Number (SDN)

identification of a safety domain

3.1.2.9

Safety Network Management (SNMT)

services for safety layer management

3.1.2.10

Safety Object Dictionary (SOD)

repository of all data objects accessible using services of the functional safety fieldbus

3.1.2.11

Safety Process Data Object (SPDO)

object for process data exchange between different safety nodes

3.1.2.12

Safety Service Data Object (SSDO)

object for service data exchange between safety nodes

3.1.2.13

initialization

initial safety node communication state

3.1.2.14

operational

safety node communication state where all functional safety functions are working properly

3.1.2.15

pre-operational

safety node communication state where all application outputs are in safety state

3.1.2.16

Unique Device Identification (UDID)

worldwide unique identification of a device

3.2 Symbols and abbreviated terms

3.2.1 Common symbols and abbreviated terms

CP	Communication Profile	[IEC 61784-1]
CPF	Communication Profile Family	[IEC 61784-1]
CRC	Cyclic Redundancy Check	
DLL	Data Link Layer	[ISO/IEC 7498-1]
DLPDU	Data Link Protocol Data Unit	
EMC	Electromagnetic Compatibility	
EUC	Equipment Under Control	[IEC 61508-4:2010]
E/E/PE	Electrical/Electronic/Programmable Electronic	[IEC 61508-4:2010]
FAL	Fieldbus Application Layer	[IEC 61158-5]
FS	Functional Safety	
FSCP	Functional Safety Communication Profile	
MTBF	Mean Time Between Failures	
MTTF	Mean Time To Failure	
PDU	Protocol Data Unit	[ISO/IEC 7498-1]
PFH	Average frequency of dangerous failure [h ⁻¹] per hour	[IEC 61508-6:2010 ⁹]
PhL	Physical Layer	[ISO/IEC 7498-1]
PL	Performance Level	[ISO 13849-1]

⁹ To be published.

PLC	Programmable Logic Controller	
SCL	Safety Communication Layer	
SIL	Safety Integrity Level	[IEC 61508-4:2010]

3.2.2 CPF 13: Additional symbols and abbreviated terms

ACM	Automatic Configuration Mode	
ADR	Address information (source or destination)	
APDU	Application Protocol Data Unit	[ISO/IEC 7498-1]
CN	Controlled Node	[IEC 61158-3-13]
CT	Consecutive Time field	
DBx	Data Octet	
DSADR	Destination SADR	
DVI	Device Vendor Information	
ID	Frame Identification	
LE	Length field	
LSB	Least Significant Octet	
MAC	Medium Access Layer	
MCM	Manual Configuration Mode	
MN	Managing Node	[IEC 61158-3-13]
MSB	Most Significant Octet	
PDO	Process Data Object	[IEC 61158-3-13]
RxSPDO	Receive Process data objects	
SADR	Safety Address	
SCM	Safety Configuration Manager	
SCT	Safety Control Time	
SD	Safety Domain	
SDG	Safety Domain Gateway	
SDN	Safety Domain Number	
SDO	Service Data Object	[IEC 61158-3-13]
SN	Safety Node	
SNMT	Safety Network Management	
SOD	Safety Object Dictionary	
SPDO	Safety Process Data Object	
SPST	Safety Parameterization Software Tool	
SSDO	Safety Service Data Object	
SSADR	Source SADR	
TADR	Additional SADR for timing information	
TR	Time Request Distinctive Number	
TReq	Time Synchronization Request	
TRes	Time Synchronization Response	
TÜV	Technischer Überwachungsverein	
TxSPDO	Safety Transmit Process data objects	
UDID	Unique Device Identification	

3.3 Conventions

3.3.1 Hexadecimal values

Some values within this part are specified in hexadecimal notation. This shall be depicted by appending a "h" to the value itself. The characters 1, 2, 3, 4, 5, 6, 8, 9, 0, a, b, c, d, e, f, A, B, C, D, E and F shall be used. All values in hexadecimal notation shall depict whole octets; therefore a hexadecimal value representation always consists of an even number of characters.

EXAMPLE 1 12ABh, 05h, 1234ABCDh

To depict data where a sequence of octets shall explicitly be defined – to be independent from the exact memory representation (Big-Endian or Little-Endian) – a hexadecimal sequence notation shall be used. Every octet is shown by a two digit hexadecimal value (without the h suffix), the single octet representations shall be separated by a dash (-).

EXAMPLE 2 00-00-00-00-00-00, AC-3E

3.3.2 Binary values

Some values within this part are specified in binary notation. This shall be depicted by appending a "b" to the value itself. The characters 1 and 0 shall be used.

EXAMPLE 11001010b

3.3.3 Wildcard digits

If parts of constant values are "don't care", or have additional meaning outside the scope of the descriptive text, this shall be depicted by an x at the respective digit position.

EXAMPLE 12xBh, 1x0xx010b, 123x45

3.3.4 Diagrams

Graphical notations according to ISO/IEC 19501 are used throughout this part where appropriate.

4 Overview of FSCP 13/1 (Ethernet POWERLINK safety)

4.1 Functional Safety Communication Profile 13/1

Communication Profile Family 13 (commonly known as Ethernet POWERLINK¹⁰) defines communication profiles based on IEC 61158-3-13, IEC 61158-4-13, IEC 61158-5-13, and IEC 61158-6-13.

The basic profile CP 13/1 is defined in IEC 61784-2. The CPF 13 functional safety communication profile FSCP 13/1 (Ethernet POWERLINK safety) is based on the CPF 13 basic profiles in IEC 61784-2 and the safety communication layer specifications defined in this part.

¹⁰ Ethernet POWERLINK and Ethernet POWERLINK safety are trade names of the non-profit organization Ethernet POWERLINK Standardization Group (EPSG). This information is given for the convenience of users of this International Standard and does not constitute an endorsement by IEC of the trade name holder or any of its products. Compliance to this standard does not require use of the trade names Ethernet POWERLINK or Ethernet POWERLINK safety. Use of the trade names Ethernet POWERLINK or Ethernet POWERLINK safety requires permission of Ethernet POWERLINK Standardization Group (EPSG).

4.2 Technical overview

FSCP 13/1 defines an open safety protocol for Ethernet-based communication in the microsecond range.

The FSCP 13/1 services and protocol specifies safety related data communication between Safety Nodes (SNs). The FSCP 13/1 protocol technology is designed to provide SIL 3 safety function according to IEC 61508. The network configuration is done by using the Safety Configuration Manager (SCM). Safety Network Management (SNMT) services are used for booting and runtime diagnosis of FSCP 13/1 networks. The Safety Object Dictionary (SOD) is database provided by every SN containing configuration and user data. Safety Service Data Objects (SSDO) are used for the exchange of spontaneous data. Safety Process Data Objects (SPDO) provide services for exchange of synchronous data.

Synchronous data communication between SNs is modelled according to the publisher subscriber model (see Figure 3), whereas spontaneous data communication use the client server model (see Figure 4).

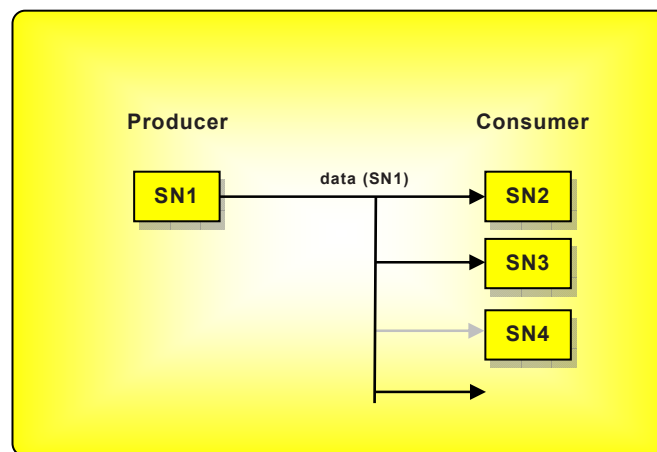


Figure 3 – Producer consumer example

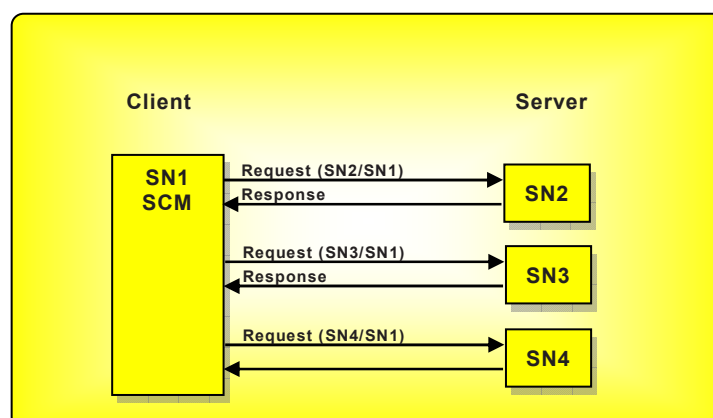


Figure 4 – Client server example

5 General

5.1 External documents providing specifications for the profile

The documents [51] and [52] may help understanding FSCP 13/1 concepts.

5.2 Safety functional requirements

The following requirements were used in the development of FSCP 13/1 and shall apply to the development of devices that implement the FSCP 13/1 protocol:

- FSCP 13/1 shall support Safety Integrity Level 3 (SIL 3) according to IEC 61508,
- the basic requirements for the development of FSCP 13/1 are specified in IEC 61784-3,
- FSCP 13/1 utilizes services defined in IEC 61158-5-13,
- FSCP 13/1 protocol is based on a black channel approach; there is no safety related dependency on the CPF 13 communication profile,
- implementations of FSCP 13/1 shall comply with IEC 61508,
- CPF 13 requirements shall be unchanged for safety unless specified otherwise in this part,
- safety communication and standard communication shall be independent. However, standard devices and FSCP 13/1 devices shall be able to use the same communication channel,
- non safety related network infrastructure devices shall be usable to build a FSCP 13/1 network,
- up to 1 023 safety related devices shall be supported within one safety domain,
- up to 1 023 safety domains shall be supported,
- bandwidth used by safety messages shall be kept as low as possible, safety PDUs shall be optimized for devices with less data (e.g. digital IO), and
- unless specified otherwise in this part, the safe state of any value shall be zero (0).

5.3 Safety measures

FSCP 13/1 shall use the safety measures listed in Table 1 to detect communication errors for cyclic data transferred in SPDO (see 7.2). The safety measures shall be processed and monitored within each FSCP 13/1 device.

Table 1 – Communication errors and detection measures (cyclic)

Communication errors	Safety measures							
	Sequence number	Time stamp	Time expectation	Connection authentication	Feedback message ^e	Data integrity assurance	Redundancy with cross checking	Different data integrity assurance systems
Corruption						X	X	
Unintended repetition		X						
Incorrect sequence		X						
Loss			x ^a					
Unacceptable delay		X	X					
Insertion			x ^b					
Masquerade			X			X	X	X
Addressing				X				
NOTE The errors "loss" and "insertion" will not be detected by the use of a time stamp. A loss of data is detected within the maximum reaction time by the use of a watchdog. If a message was sent more than once (insertion), the timestamp is unchanged and the receiving device ignores this message.								
^a Missing PDUs shall be detected within maximum reaction time.								
^b Only one message shall be accepted during a defined time frame.								

FSCP 13/1 shall use the safety measures listed in Table 2 to detect communication errors for acyclic data transferred in SSDO (see 7.3) or SNMT (see 7.4). The safety measures shall be processed and monitored within each FSCP 13/1 device.

Table 2 – Communication errors and detection measures (acyclic)

Communication errors	Safety measures							
	Sequence number	Time stamp	Time expectation	Connection authentication	Feedback message	Data integrity assurance	Redundancy with cross checking	Different data integrity assurance systems
Corruption					X	X	X	
Unintended repetition	X							
Incorrect sequence	X							
Loss	X				X			
Unacceptable delay								
Insertion	X				X			
Masquerade						X	X	X
Addressing				X				
NOTE The errors "loss" and "insertion" will not be detected by the use of a time stamp. A loss of data is detected within the maximum reaction time by the use of a watchdog. If a message was sent more than once (insertion), the timestamp is unchanged and the receiving device ignores this message.								

In order to avoid systematic and stochastic errors, the following guidelines shall be considered during development and implementation of FSCP 13/1 (see 7.1):

- The producer of safety data shall:
 - generate a time stamp,
 - NOTE Any new SPDU contains a new time stamp.
 - generate CRCs, and
 - duplicate the safety message;
- The consumer of a safety message data shall:
 - check PDU part one with CRC,
 - check PDU part two with CRC,
 - compare PDU part one and two data area bit-for-bit,
 - check the received address,
 - reset the internal watchdog (counter) if a new valid PDU has been received,
 - if a PDU has the same time stamp as the last one or an older one, the PDU shall be ignored,
 - if no valid PDU is received within a defined time (Safety Control Time, see 7.5.4.14), the device shall enter the safe state, and
 - if the watchdog (counter elapsed) has an overrun (not been reset within the maximum time), the device shall enter a safe state.

5.4 Safety communication layer structure

The FSCP 13/1 protocol is layered on top of a standard communication channel, which shall be considered a black channel. Figure 5 shows how the safety communication layer relates to the standard communication channel.

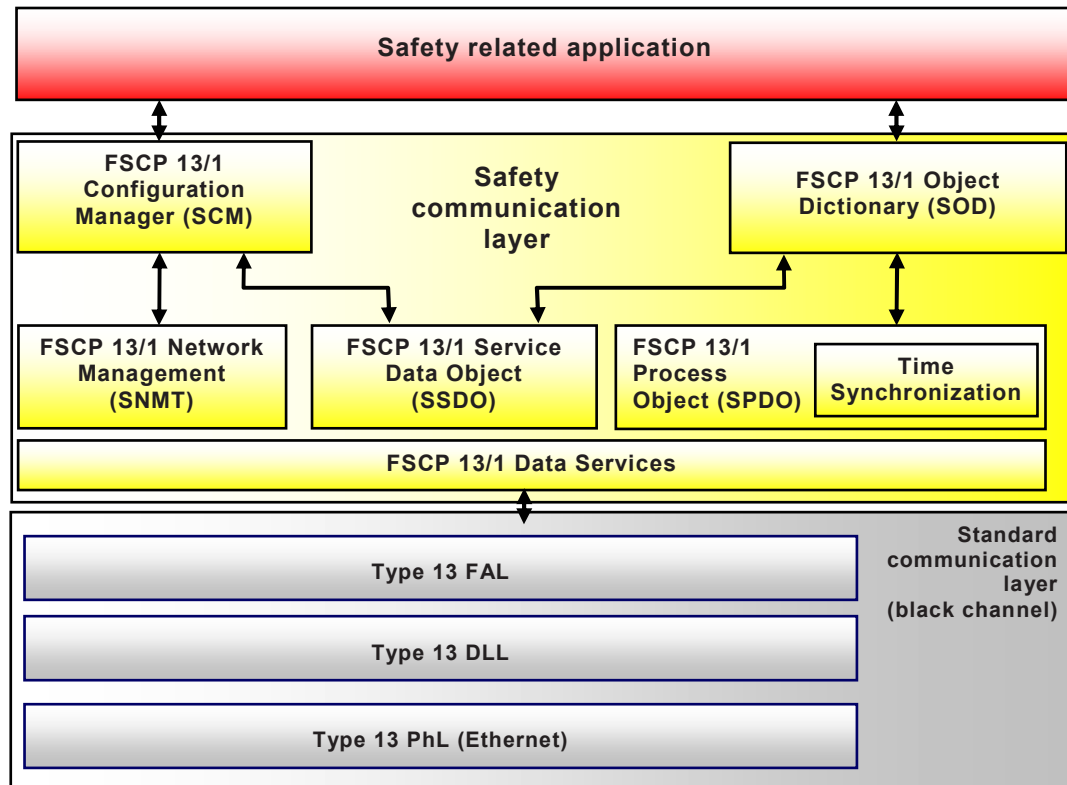


Figure 5 – Communication layer structure

Safety data is produced by the safety-related application entity. This data is encapsulated in a safety message by the safety communication layers and sent via the standard communication channel. The safety communication layer in the receiving device decodes the safety message and verifies integrity and timeliness of the data. The data is presented to the safety-related application entity. If no data is received within a defined time frame, the application entity is informed of this event, which may be used to set all outputs to the safe state.

The safety communication layer provides for:

- safe data transport (integrity and time monitoring),
- network bootup,
- run time diagnosis,
- commissioning,
- program and firmware download,
- parameterization, and
- device replacement.

All these functionalities can be accessed and controlled via the safety communication channel (see Figure 6).

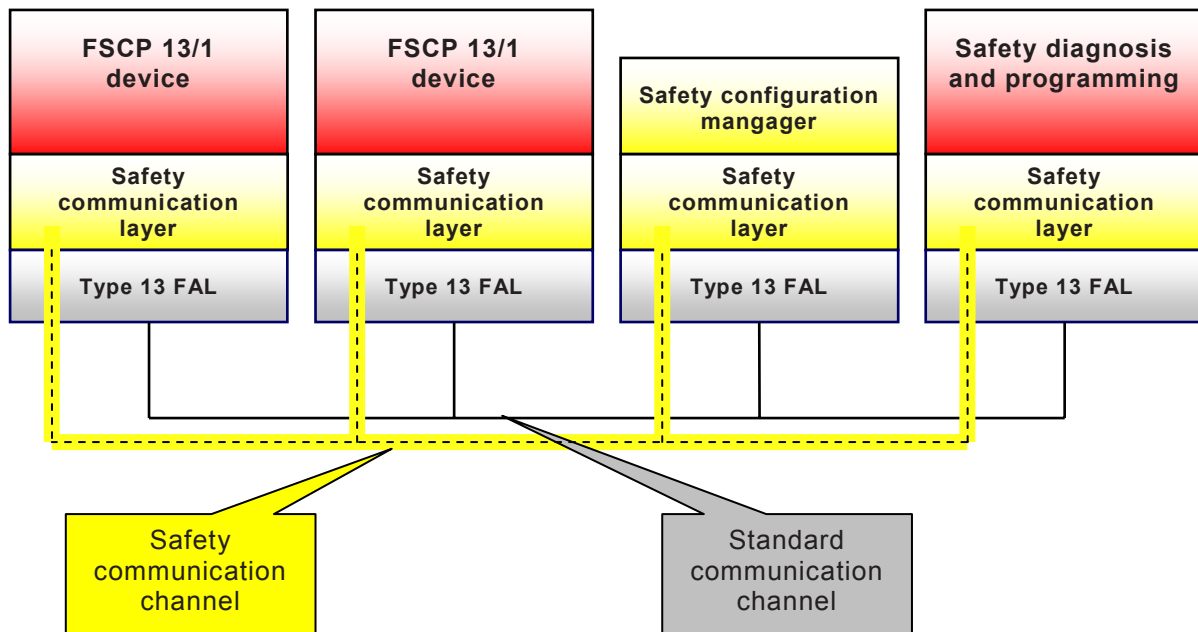


Figure 6 – Safety communication channel

5.5 Relationships with FAL (and DLL, PhL)

5.5.1 General

FSCP 13/1 shall use the services defined in IEC 61158-5-13.

5.5.2 Data types

Profiles defined in this part support all the CPF 13 data types as defined in IEC 61158-5-13.

6 Safety communication layer services

6.1 Modelling

6.1.1 Reference model

6.1.1.1 General

A FSCP 13/1 compliant implementation shall provide the following application objects:

- Safety Network Management (SNMT),
- Safety Configuration Manager (SCM),
- Safety Service Data Objects (SSDO),
- Safety Object Dictionary (SOD), and
- Safety Process Data Objects (SPDO).

How these application objects relate to each other is shown in Figure 5.

The usage of an underlying communication layer shall be mandatory.

6.1.1.2 Safety network management (SNMT)

The SNMT shall provide the required services for the Safety Configuration Manager (SCM) to configure and verify the safety related nodes within the network.

6.1.1.3 Safety service data objects (SSDO)

The SSDO shall provide the required services to access the Safety Object Dictionary (SOD) and to support the SCM.

6.1.1.4 Safety process data objects (SPDO)

The SPDO shall provide the required services for safety related process data exchange between certain entries within the SOD of communicating nodes. The time synchronization services, which are part of SPDO, shall verify the network performance between the communicating nodes.

6.1.1.5 Safety object dictionary (SOD)

The SOD shall describe the format and access services of the device specific data.

6.1.1.6 Safety configuration manager (SCM)

The SCM shall provide the required services for start-up, parameterization and all further measures to ensure safe operation over the entire life cycle of the application.

6.1.2 Communication model

FSCP 13/1 shall use FAL services defined in IEC 61158-5-13 for data exchange between Safety Nodes (SNs), FSCP 13/1 defines a producer / consumer communication model, built using these services. FSCP 13/1 nodes shall be logically separated into producer and consumer nodes.

Producer nodes shall send data identified by a specific Safety Address (SADR). Any SN within the Safety Domain may receive this data. This is done using the mechanism as described in 7.5. As a result of this communication model, the SADR uniquely identifies an SN as well as a safety PDU sent from a specific node.

Figure 7 shows characteristic producer / consumer communication. The producer node SN1 sends data. The data is uniquely identified by the producers SADR. Each node within the Safety Domain is able to receive this data.

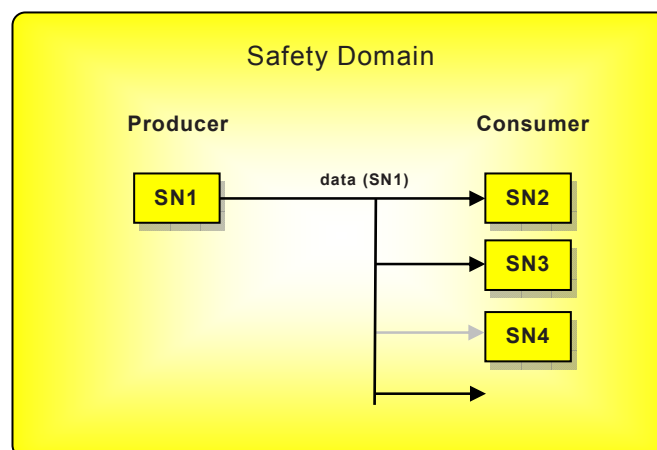


Figure 7 – Characteristic producer / consumer communication

Figure 8 demonstrates an extended version of the producer / consumer communication model which allows the producer to produce separated data for individual consumers. The producer shall use SADR for this. The Safety Configuration Manager (SCM) shall ensure that the SADR used are still unique within the Safety Domain.

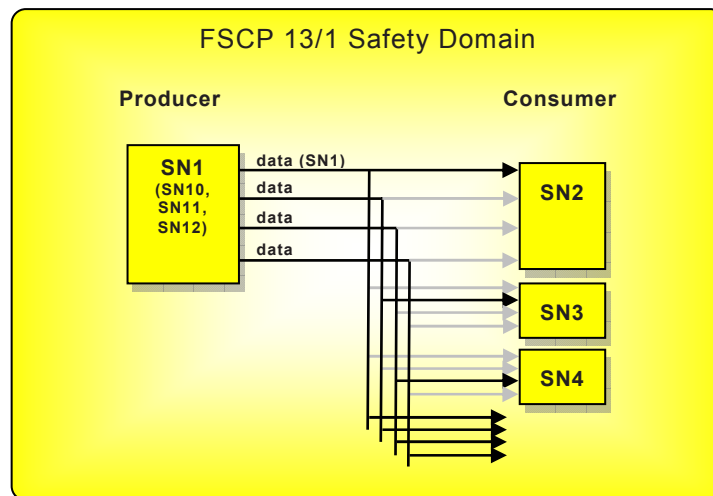


Figure 8 – Extended producer / consumer communication

Figure 9 shows the client server communication which shall be used for configuration services and network management. The SCM (or a dedicated configuration tool, see Clause 8) shall act as the client. SNs shall be limited to the server role.

Using the client server communication model, the client (SCM or Tool) sends a request to the server (SN) which is addressed within the ADR Field (see 7.1.2) using the server address and also contains the client address within the TADR Field (see 7.1.8). The server replies with a response which is addressed within the ADR Field (see 7.1.2) using the server address and also contains the client address within the TADR Field (see 7.1.8).

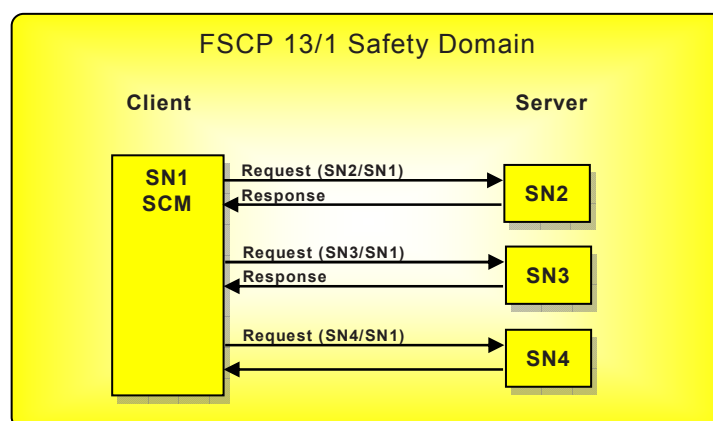


Figure 9 – Client Server communication

6.1.3 Device roles and topology

6.1.3.1 General

FSCP 13/1 device roles are defined in Table 3.

Table 3 – Device roles

Device role	Description
Safety Node (SN)	A FSCP 13/1 compliant device
Safety Configuration Manager(SCM)	Central service for managing a Safety Domain (SD) ^a
Safety Domain Gateway (SDG)	FSCP 13/1 device to exchange data between different SDs
^a A Safety Domain defines an isolated address space of up to 1 023 SNs.	

An FSCP 13/1 device shall implement the device role of an SN and may implement SCM and/or an SDG.

Figure 10 gives an overview of possible interrelationships of device roles and Safety Domains. SD1 gives an example of a simple Safety Domain. Safety related communication of the FSCP 13/1 devices within SD1 is limited to the SNs within SD1.

SD2 in combination with SD3 shows the possibility to set up a FSCP 13/1 communication between different Safety Domains. This is done using a special SDG which is able to communicate with different Safety Domains. Inter-domain communication is handled by the device internally. SDG capability is independent from the SCM capability of a device. The SDG shall have one SADR in SD2 and one SADR in SD3.

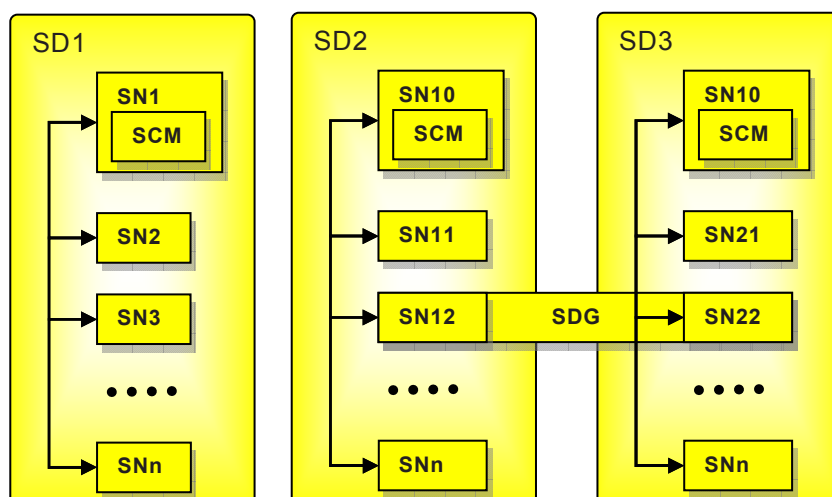


Figure 10 – Topology overview

6.1.3.2 Safety Node (SN)

An SN is a node within any network which conforms to this part. An SN shall be identified by:

- A logical address which is unique within an SD, called Safety Address (SADR). The number range for the SADR shall be 1 -- 1 023 (0 is reserved and shall not be used). The SADR shall be defined at the application planning stage. Duplicate SADRs within an SD shall be detected by the SCM during network verification at start-up of the SCM or at start-up of any node within the Safety Domain.
- A physical address which is globally unique within all FSCP 13/1 compliant devices, called Unique Device Identification (UDID). Duplicate UDIDs within an SD shall be detected by the SCM.

For operation, an SN may need further data like safety related parameters or application data. It depends on the capability of the device, where this data is stored:

- At least the device specific firmware, the UDID and the Device Vendor Information (DVI) (see 7.5.4.7) shall be stored permanently on the device. There shall be no support within FSCP 13/1 to change this data via the network.
- Simple SNs without permanent memory shall receive SDN, SADR and all further parameters from the SCM after start-up.

NOTE 1 This requires permanent storage of this SN specific data on the SCM.

- Complex SNs with permanent memory or physical switches to adjust the SDN and SADR shall hold their data permanently on the device.

NOTE 2 The SCM will store only the data which is not permanently stored on the SN; for all other data, the SCM will only verify it.

6.1.3.3 Safety Domain (SD)

6.1.3.3.1 General

A Safety Domain shall constitute an address space of up to 1 023 SADRs (1 – 1 023). Only SNs sharing the same SD shall be able to communicate directly with each other. SNs on different SDs shall be restricted to communication via a Safety Domain Gateway.

An SD is identified by the Safety Domain Number (SDN) having a number range of 1 -- 1 023 0 is reserved and shall not be used. The SDN is defined manually. When planning the application layout, unique SDNs shall be ensured.

6.1.3.3.2 Safety Domain protection

The danger of an external attack of FSCP 13/1 within the safety PDU process data (SPDO) is negligible. But there is a potential risk for the configuration services. When using the Internet in connection with FSCP 13/1, a reliable method of encryption (e.g. Virtual Private Network – VPN, Secure Socket Layer – SSL, IPsec) shall be used. Choosing an adequate encryption system is the responsibility of deployment planning and is outside the scope of this part. Within Local Area Networks (LANs), organizational actions like firewalls shall be implemented.

Figure 11 depicts an example of FSCP 13/1 Safety Domain protection.

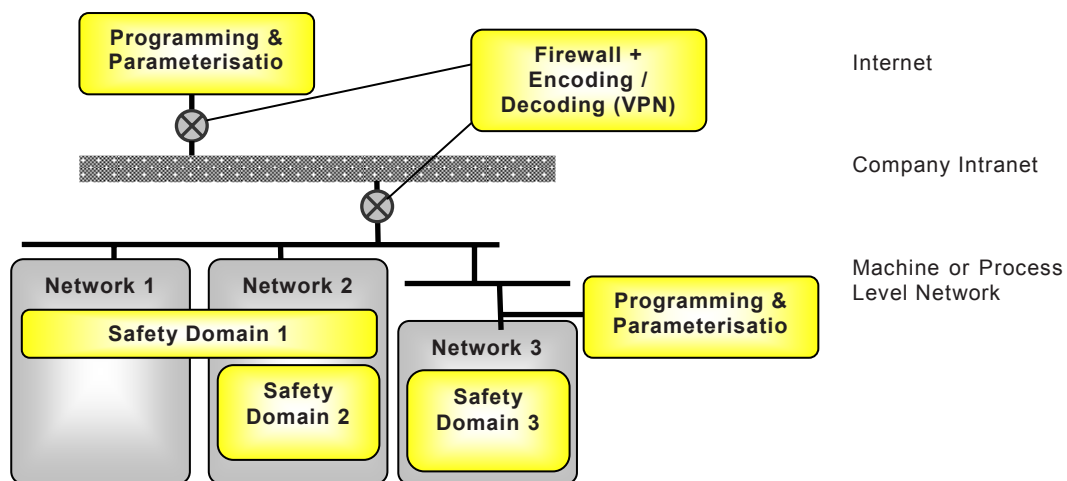


Figure 11 – Safety Domain protection (example)

6.1.3.3.3 Safety Domain separation

Interaction between Safety Domains as well as the danger of confusion during configuration and parameterization is excluded by using unique Safety Domain numbers.

NOTE If the size of the company intranet and the organization of the network management do not allow the administration of unique Safety Domain numbers, it's recommended to split it to several manageable network scopes and separate them by approved methods like firewalls.

To avoid safety critical situations, the SPDO and SSDO PDO data shall additionally be coded to be unique within a certain Safety Domain (see 7.1.10). Therefore Safety PDOs which erroneously are transmitted in the wrong domain can be identified and rejected.

Figure 12 depicts an example of Safety Domain separation.

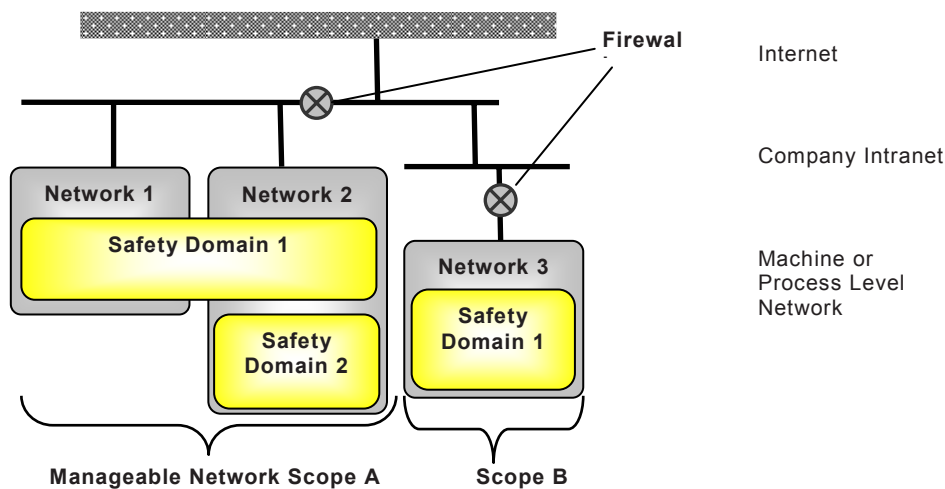


Figure 12 – Safety Domain separation (example)

6.1.3.4 Safety Domain Gateway (SDG)

This shall be a special FSCP 13/1 device role which is able to communicate with different Safety Domains (SD). Inter-domain communication is handled by the SDG internally. Within an SD, the SDG acts like a standard SN.

An SDG is responsible for:

- forward SSDO PDUs between Safety Domains, if an SN wants to send an SSDO to an SN in another Safety Domain, this SSDO is sent to the SDG which forwards the SSDO to the destination node, several SDG may have to be passed to reach the destination SN,
- forward SPDO data between Safety Domains, the SDG may provide means to read data from SPDOs in one Safety Domain and send this data into another Safety Domain inside the SPDO of the SDG.

The configuration of the SDG is vendor specific.

The scope of this part is to specify the safety related communication mechanisms which are needed for data exchange within a single Safety Domain. The communication between different Safety Domains (and the Safety Domain Gateway is a mean for this) is outside the scope of this part.

6.1.3.5 Configuration Manager (SCM)

The Safety Configuration Manager (SCM) shall be centrally responsible for managing FSCP 13/1. Within a Safety Domain, only one SN running the SCM service shall be permitted.

The SCM shall be responsible for:

- permanent storage of SN specific parameters which are not stored on the SN (see 6.1.3.2),
- unique assignment and verification of the SADR of the SNs within the SD,
- verification of the uniqueness of the UDID within the SD,
- verification of the expected parameters and DVI of the SNs, and
- sending a periodic life guard signal to all SNs within the SD.

NOTE This periodic life guard signal from the SCM is required within the SN to detect certain failure situations where no SCM is responsible for the SN.

6.2 Life cycle model

6.2.1 General

FSCP 13/1 supports the safety-related application during several phases of its life cycle, as defined in IEC 61508. The safety related communication is only one part of the complete safety concept of the machinery. Of course, the other safety related parts of the machinery shall be considered as well. This subclause focuses only on safety-related communication with FSCP 13/1.

6.2.2 Concept, planning and implementation

6.2.2.1 Application layout

When designing the application layout, the characteristics of FSCP 13/1 shall be taken into account. The following possibilities and restrictions shall be observed:

- Safety Domain, assigning SDNs,
- separation and protection of Safety Domains,
- Safety Addresses,
- Safety Configuration Manager, and
- inter-domain communication.

6.2.2.2 Programming and parameterization

6.2.2.2.1 General

Programming and parameterization shall be carried out using safety related tools. Application files and parameters shall be stored in the SCM device only or directly in the corresponding device depending on the device capabilities.

Programming and parameterization of the safety related application shall be comprised of the following tasks:

- accessing SNs within an SD is referenced by the SADR only,

NOTE This allows installing several identical applications with different SDNs without changing the application.

- communication to other SDs is only possible via an SDG,
- locate SCM service,
- list DVI of the devices,

- implement safety related application, and
- specify safety related parameters (see 7.5).

The SCM is the central node to verify the safety related devices. FSCP 13/1 shall support two different strategies for configuration. This is necessary to satisfy all requirements coming from the wide range of applications FSCP 13/1 is ready for. These two strategies shall be:

- Automatic Configuration Mode (ACM), and
- Manual Configuration Mode (MCM).

6.2.2.2.2 Automatic Configuration Mode (ACM)

Using the Automatic Configuration Mode (ACM), the system automatically gathers the UDID from the connected SNs. The ACM shall be used only if all of the following preconditions are fulfilled:

- all safety related devices can be connected at configuration time,
- one device (single UDID) for each SN with a specific SADR,
- if a safety related device is replaced, the SCM verifies that the new device is of the same type as the replaced one; If this is fulfilled, the new UDID will be gathered and the operator shall confirm the replacement.

6.2.2.2.3 Manual Configuration Mode (MCM)

Manual Configuration Mode (MCM) is applicable for all kinds of applications; however this mode requires manual configuration of the safety related devices. So, this mode is mainly intended for applications with the following features:

- all connectable safety related devices can not be connected at one time,

EXAMPLE 1 Robotic arm with several safety related tools.

- multiple devices (multiple UDID) for an SN with a specific SADR,

EXAMPLE 2 Consider a modular machine application with several machine lines within a plant. Machine module A (equals to the SADR) may be used for all machine lines. For bottleneck reasons, there is more than one piece of equipment (i.e. more than one UDID) for module A (=SADR), and these pieces of equipment (UDID) are all applicable on each machine line.

- module replacement shall be handled automatically without manual intervention.

6.2.3 Commissioning

6.2.3.1 General

Commissioning can be separated into three main steps:

- a) installing the application (see 6.2.3.2),
- b) setting up the configuration depending on the configuration mode (see 6.2.3.3),
- c) verification of the safety functionality (see 6.2.3.4).

6.2.3.2 Installation

Install applications and parameters on the FSCP 13/1 devices. This shall be done using one of the following methods:

- an FSCP 13/1 compliant programming tool which uses the specified FSCP 13/1 services (see 7.3), or
- proprietary safety related transfer protocol to exchange data from the programming system to a safety related device via network or direct communication connection (e.g. serial line).

During installation phase of the life cycle, the capability of the device shall determine what data and where the data shall be downloaded:

- if the device itself holds the data, the data shall be downloaded to the device,
- if the device is not able to hold the data, the data shall be stored on the SCM. The SCM shall ensure the proper update of all devices during power up using the FSCP 13/1 configuration services.

Following the installation of applications and parameters, the SDN shall be updated if needed (see 6.1.3.3).

6.2.3.3 Configuration setup

6.2.3.3.1 Configuration setup using ACM

A configuration setup using ACM shall be comprised of the following four steps:

- a) power up all safety related devices,
- b) ensure that communication layer works for all SNs,
- c) SCM starts gathering UDID (without operator interference),
- d) the commissioner shall acknowledge each device.

6.2.3.3.2 Configuration setup using MCM

A configuration setup using MCM shall be comprised of the following three steps:

- a) the commissioner shall enter the list of possible SADR with the corresponding UDIDs manually, for this a safety related configuration tool shall be used,
- b) the SCM shall accept all configured SADR / UDID combinations,
- c) the SCM shall not accept mismatches and shall not repair mismatches as done in the ACM. This means, all mismatches shall be corrected by the commissioner by entering the corrected value using the safety related configuration tool.

6.2.3.4 Verification

Verification shall be comprised of the following five steps:

- a) the commissioner shall verify the safety functionality against the safety specification for the application. In the case of device replacements or changes in the routing within the communication layer, the commissioner shall continue with step 6.2.3.3;
- b) If verification is carried out during commissioning, all combinations of exchangeable modules shall be verified;

NOTE This is especially important in the case of complex modular machines (in combination with MCM).

- c) If verification is carried out due to maintenance, only the safety related functionality affected by the maintenance task shall be verified;
- d) When verification is finished, an installation specific backup of the current configuration shall be made;
- e) In case of an SCM replacement, a download of application files, parameters, and the configuration shall be done; otherwise the commissioning steps (installation, configuration and verification) shall be repeated.

6.2.4 Operation terms

6.2.4.1 Transfer of safety related data

During operation, the safety related data transfer is handled by FSCP 13/1. The underlying network is responsible for the data transport between the nodes with a defined timing quality. Loss of timing or transport quality within the underlying communication layer is detected by

the FSCP 13/1 layer (see 7.7.2) and will result in loss of availability, but not in loss of safety (black channel approach).

EXAMPLE See Figure 13.

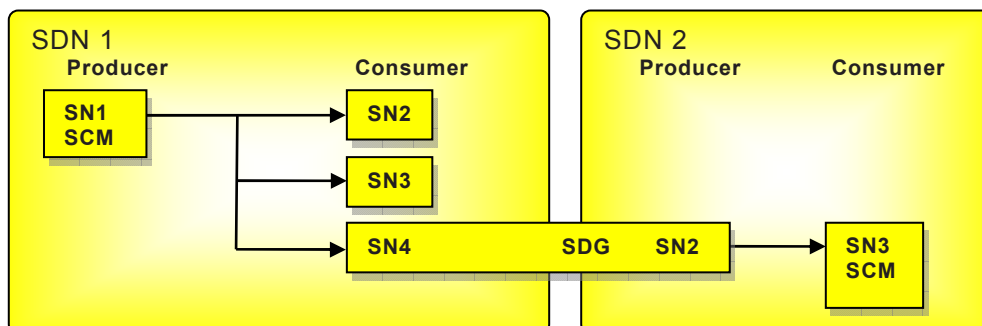


Figure 13 – Data flow example

6.2.4.2 Time synchronization and validation

In order to avoid any missed or sudden delays of data, network performance verification shall be done. From time to time each consumer shall query all connected producers for their relative time. By comparison of the relative time, the elapsed time and the time information from any transfer, the consumer shall check the timeliness of the received data.

The network performance verification is part of the data transfer. At first, a consumer sends a “Time Request” PDU to the connected producer. After receiving this PDU, the producer sends its data with an additional code, which enables the consumer to identify this message as a “Time Response”. By measuring the time delay between the “Time Request” and the “Time Response”, the consumer is able to check whether the network is fast enough to meet the requirements of the application depending on the worst case reaction time.

For a detailed description refer to 7.7.2.

6.2.4.3 Life guarding

With the service Life Guarding (see 7.5.4.5), the FSCP 13/1 shall ensure that only configured SNs are Operational in an FSCP 13/1 network. An SN expects frequent Life Guarding signals to stay in the Operational state. Otherwise it shall change to the state Pre-Operational where it is of no risk to the safety related network.

The interval of the Life Guarding signal shall be application specific, and is typically determined by the amount of time needed to verify the application safety functions.

Using an organizational measure like switching off all SNs in case of reconfiguring the SCM, may eliminate the risk in this situation. As a result, the interval for Life Guarding may be set to a very large value (several days) for these cases.

6.2.4.4 Startup after power up or reset

After power up, the SCM (see 7.7.9) shall do the network verification. If there was no change within the network, no special tasks are required.

6.2.4.5 Recover from network failure

Following a network breakdown, all affected SNs will enter the Pre-Operational state. Since the corresponding consumer SNs will get no further data, these nodes shall enter the safe state.

After recovery of the network, all affected SNs shall send an SNMT_SN_in_PRE_OP information to the SCM. The SCM, then, shall start with the initialization of the SNs.

6.2.5 Maintenance terms

See 9.6.

6.3 Non safety communication layer

6.3.1 General

This subclause lists the requirements on the non safety communication layer for transportation of safety PDUs. Communication protocols according to CFP 13 (see IEC 61784-2, IEC 61158-3-13, IEC 61158-4-13, IEC 61158-5-13 and IEC 61158-6-13) fulfil all these requirements.

6.3.2 Requirements for data transport

6.3.2.1 General

The non safety communication layer is responsible for transporting the data between the SNs. The coexistence of not safety related nodes and safety related nodes is allowed.

6.3.2.2 Masquerading

To avoid any possibilities of masquerading data as safety PDUs, non safety related nodes shall not

- contain code according to Clause 7,
- contain code which is able to generate safety PDUs according to Clause 7, or
- apply any mechanisms as defined in Clause 7.

See Clause 7 for specific information about handling this issue by protocol mechanisms.

The non safety communication layer is permitted read only access of data within a safety PDU. This shall be done by accessing the data within the safety PDUs without using the safety PDUs specific data integrity measures, such as CRC and data repetition of PDU part one in PDU part two.

6.3.2.3 Communication model

Seen from the view of CPF 13, Figure 14 depicts the common safety communication model of CNs with 0 to n SNs.

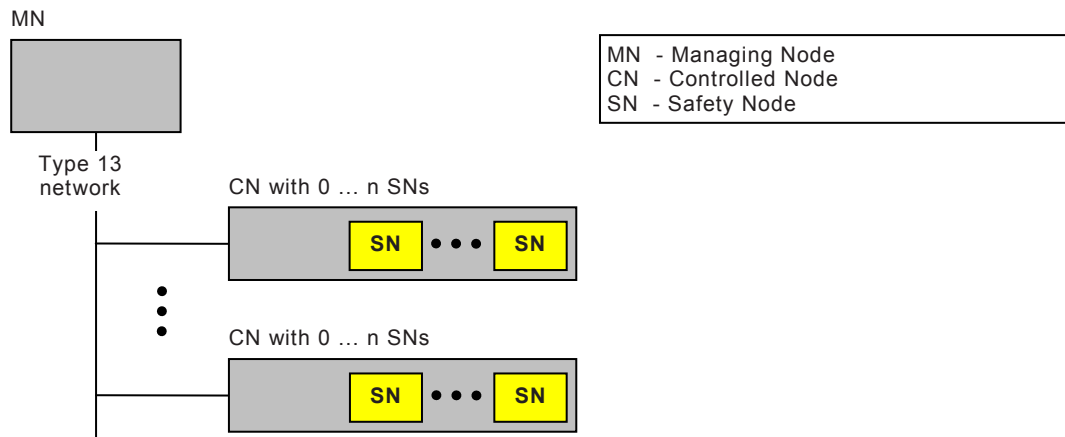


Figure 14 – Communication model

The MN and CN functionality is as defined in IEC 61158-3-13; the MN and CN are not involved in any safety function.

The safety function is implemented by an entity inside the CN which is called the Safety Node (SN). Different cases are possible:

- CN without an SN,
- CN with only one SN,
- CN with several safety related devices represented as a single SN. The safety of the module bus and the add-on modules itself shall be ensured by the vendor,
- CN with multiple SNs, or
- CN as a modular system and multiple SNs. The safety of the bus connecting the modules is provided by FSCP 13/1.

6.3.2.4 Transport of SPDO

The non safety communication layer shall transport the SPDO data between the SNs. The services as defined in IEC 61158-5-13 shall be used.

NOTE 1 SPDO payload is used for cyclic process data, like the state of an input or output. SPDOs are cyclically retransmitted within a certain time. Sending an SPDO is solely time triggered and not bound to a change in the data itself.

SPDO data shall be transmitted as safety PDUs inside Type 13 application layer PDUs (APDUs). Isoc2 APDUs according to IEC 61158-6-13 shall be used. An SPDO is generated cyclically by an SN, the producer, this SPDO can have one or many target SNs, the consumers. To transport an SPDO from its producer to its consumers, Type 13 mechanisms shall be used.

The basic principle of SPDO transport is shown in Figure 15.

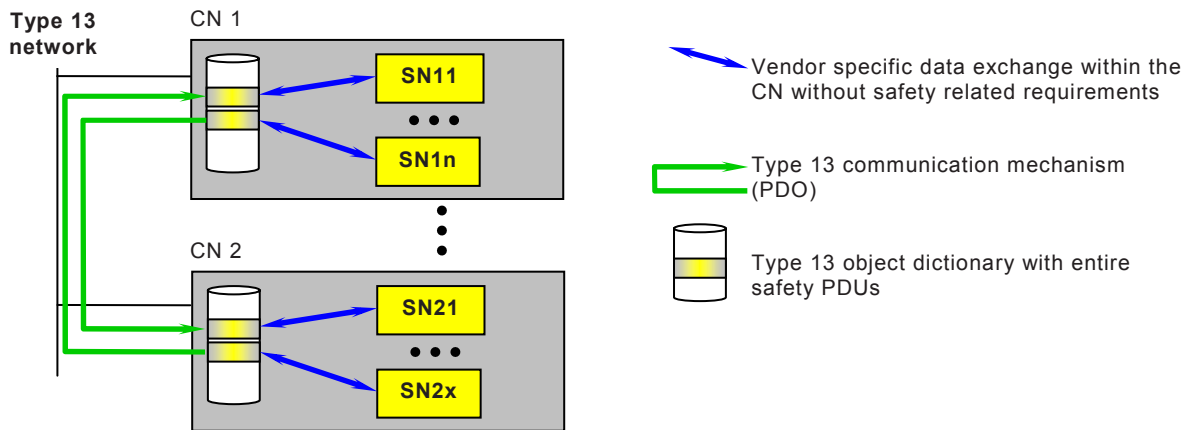


Figure 15 – SPDO transport

The transmission path between the producer SN and the consumer SN is defined as:

- the producer SN builds an SPDU,
- in the CN to which the producer SN is connected (producer CN), an object dictionary entry of data type Domain shall be defined to embody the SPDU (within the communication path, the SPDU shall not be fragmented),
- it is the responsibility of the producer CN implementation to move the SPDU data to the object dictionary entry,
- this object dictionary entry, then, shall be transmitted in a Type 13 application layer PDU (APDU), which is sent cyclically using the process data object ASE (PDO-ASE) as specified in IEC 61158-5-13,
- the object dictionary of the receiving CN (consumer CN) shall define an object of data type Domain, matching the definition of the producer's object dictionary entry; The consumer CN shall receive the APDU and copy the contained safety PDU to the Domain object mentioned before, and
- in the last step, the consumer CN implementation is responsible to move the SPDU data from the object dictionary entry to the consumer SN.

The mechanisms involved in transmitting the SPDO between the CN's object dictionary and the SNs (depicted by blue arrows in Figure 15) are outside the scope of this part and may be vendor specific.

NOTE 2 From the view of the Type 13 communication services and protocol it is not necessary to distinguish communication of SPDO from other data. There is no special treatment of safety data by Type 13 mechanisms. This fits with the black channel approach applied.

NOTE 3 The SNs involved in the communication do not need any knowledge about the Type 13 communication path.

6.3.2.5 Transport of SSDO

The non safety communication layer shall transport the SSDO data between the SNs. The services as defined in IEC 61158-5-13 shall be used.

The basic principle of SSDO transport is shown in Figure 16.

NOTE 1 SPDO payload is used for spontaneous data communication, like configuration or parameterization.

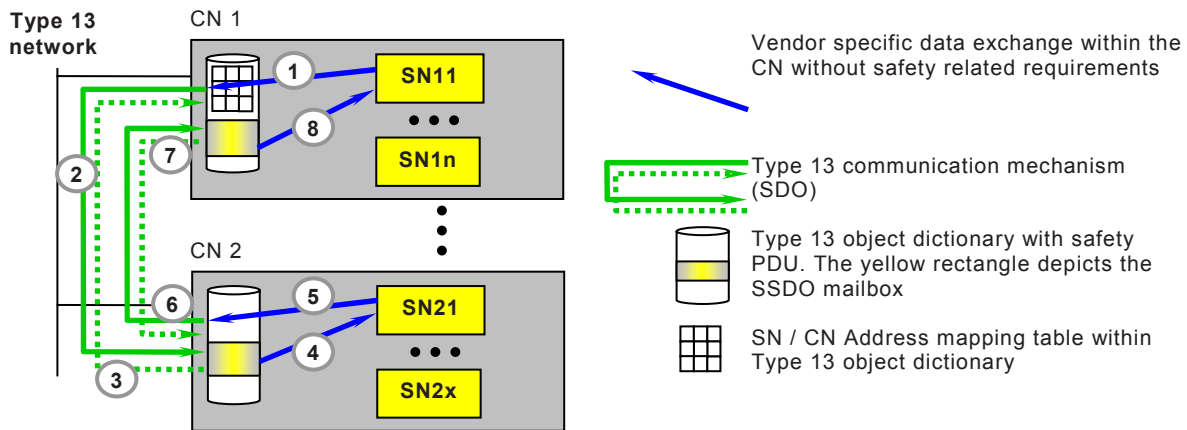


Figure 16 – SSDO transport

SSDO data shall be transmitted as safety PDUs inside Type 13 application layer PDUs (APDUs). Asyn2 APDUs with pduBody type SDO according to IEC 61158-6-13 shall be used.

An SSDO is generated spontaneously by an SN (the source SN) which is transmitted to exactly one target SN. To transport an SSDO from its source to its destination, Type 13 mechanisms shall be used.

Exchanging SSDOs between SNs is done using Type 13 services and protocols in combination with a mailbox mechanism (figures in parentheses references Figure 16):

- (1) The source SN generates an SSDO request to a specific destination SN and builds a corresponding SPDU,
- (2) the CN serving the source SN creates an SDO write access to the mailbox of the CN serving the destination SN, the SPDU of step (1) is written into the object dictionary of the target CN; This requires an SN to CN address mapping table within the CN serving the source SN, to get the Type 13 node ID of the CN serving the destination SN (target CN); It is the responsibility of the Type 13 system configuration to provide this address mapping table,
the mailbox shall be a Type 13 object dictionary entry of data type Domain which should be defined to embody an SPDU,
- (3) the SDO write access is confirmed by the SDO protocol, the connection is kept open,
- (4) the destination CN redirects the data (SPDU) within the mailbox to the destination SN, for this the destination CN shall read the address information inside the SPDU,
- (5) the destination SN generates an SSDO response and builds a corresponding SPDU,
- (6) the destination CN creates an SDO write access to the mailbox of the source CN and writes the response SPDU into the object dictionary of the source CN,
- (7) the SDO write access is confirmed, the connection is closed, and
- (8) the source CN redirects the data (SPDU) within the mailbox to the destination SN, for this the source CN shall read the address information inside the SPDU.

The mechanisms involved in transmitting the SPDO between the CN's object dictionary and the SNs (depicted by blue arrows in Figure 16) are outside the scope of this part and may be vendor specific.

NOTE 2 From the view of the Type 13 communication services and protocol it is not necessary to distinguish communication of SSDO from other data. There is no special treatment of safety data by Type 13 mechanisms. This fits with the black channel approach applied.

NOTE 3 The SNs involved in the communication do not need any knowledge about the Type 13 communication path.

6.3.2.6 Representation of diagnostic data

The non safety communication layer shall support services to provide FSCP 13/1 specific diagnostic data according to Clause 7.

The basic principle of diagnostic data representation is shown in Figure 17.

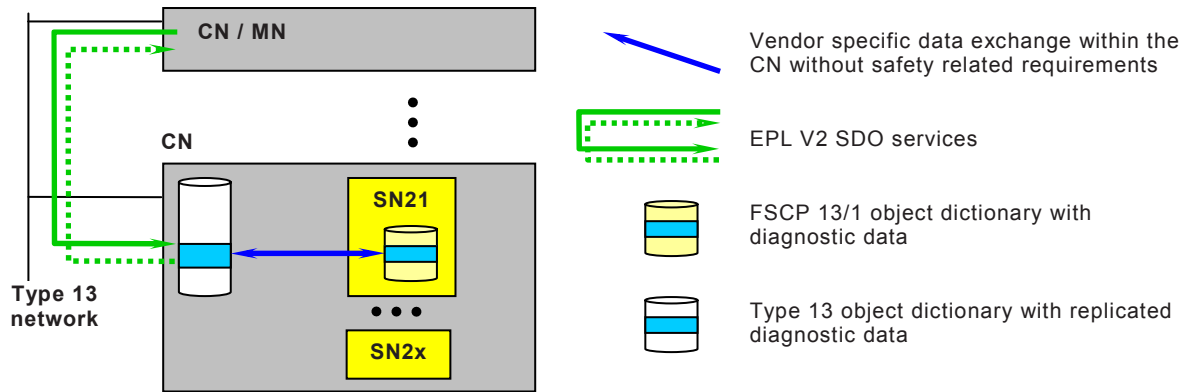


Figure 17 – Diagnostic data representation

Diagnostic data within an SN is stored in the SOD (see Clause 7).

NOTE Usually this diagnostic data is requested from distinguished nodes (e.g. central controller, human machine interface, service equipment) to process the diagnostic data and to report them to the end user.

The CN shall replicate the diagnostic data from the SOD in the Type 13 object dictionary within the CN, where they can access using Type 13 SDO services.

6.3.3 Domain protection and separation

In accordance with 6.1.3.3.2 and 6.1.3.3.3, the communication layer shall support proper security features to protect the domain against attacks from outside and to avoid interferences between separated domains.

7 Safety communication layer protocol

7.1 Safety PDU format

7.1.1 General

A safety PDU is transferred within the data part of a Type 13 APDU. One Type 13 APDU may contain zero to many safety PDUs, each reflecting a producer / consumer relationship between SNs, see Figure 18. Safety and non safety data can be mixed within a Type 13 APDU.

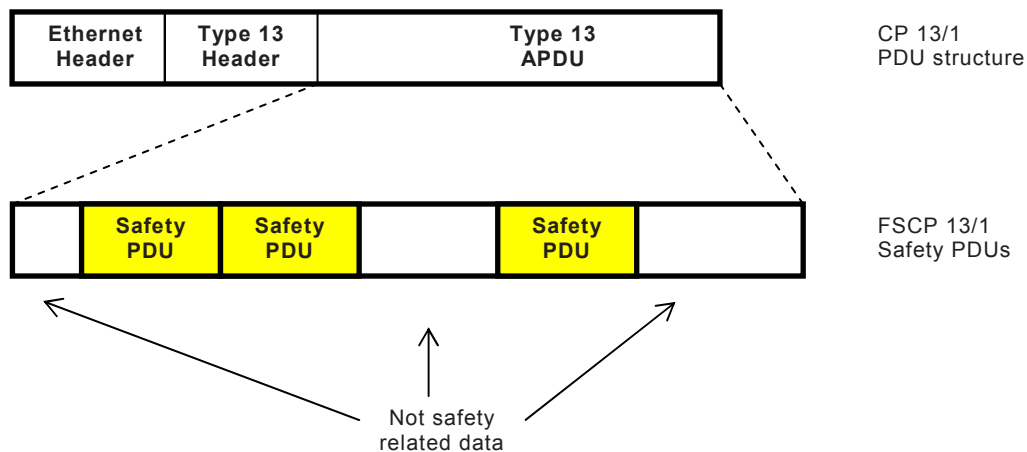
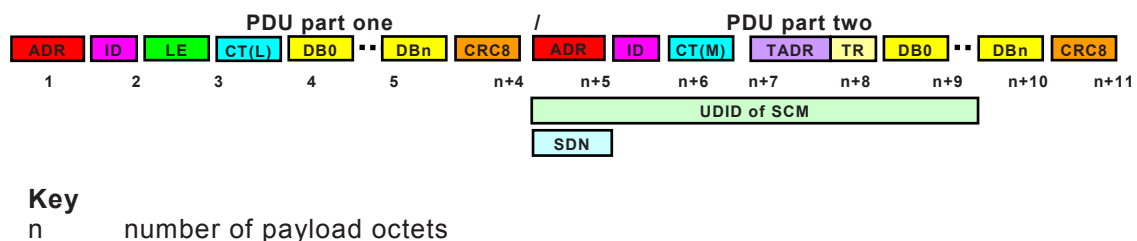


Figure 18 – Safety PDUs inside a CP 13/1 PDU

The structure of the safety PDU shall be as shown in Figure 19 and Figure 20. The safety PDU shall consist of two sub parts and is able to transport up to 254 octets of payload data. For discussion of error probability and hamming distance with respect to the safety PDU length see A.3 and A.4.

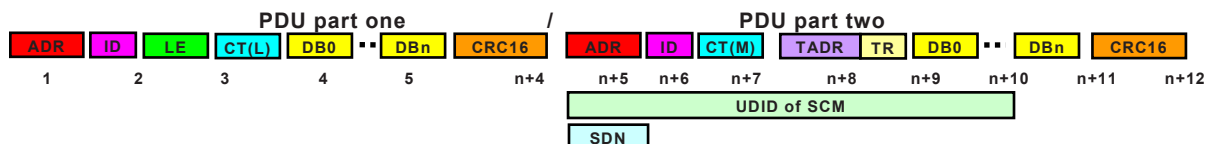
Depending on payload length two types of safety PDUs shall be used:

- 1 -- 8 octets of payload: PDU format as shown in Figure 19 shall be used (with an 8 bit CRC);
- 9 -- 254 octets of payload: PDU format as shown in Figure 20 shall be used (with a 16 bit CRC).



Key
n number of payload octets

Figure 19 – Safety PDU for n = 0 -- 8 octet payload data



Key
n number of payload octets

Figure 20 – Safety PDU for n = 9 -- 254 octet payload data

Application of this part according to the requirements defined in IEC 61784-3:2010, 5.6.1 (calculation of the residual error rate) results in a restriction of payload octets to the range starting from 9 to 25 octets.