



BSI Standards Publication

Industrial communication networks — Profiles

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

National foreword

This British Standard is the UK implementation of EN IEC 61784-3-13:2021. It is identical to IEC 61784-3-13:2021. It supersedes BS EN 61784-3-13:2017, which will be withdrawn on 23 June 2024.

The UK participation in its preparation was entrusted to Technical Committee GEL/65/3, Industrial communications: process measurement and control, including fieldbus.

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

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

© The British Standards Institution 2021
Published by BSI Standards Limited 2021

ISBN 978 0 539 18093 0

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 31 July 2021.

Amendments/corrigenda issued since publication

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

English Version

**Industrial communication networks - Profiles - Part 3-13:
Functional safety fieldbuses - Additional specifications for
CPF 13
(IEC 61784-3-13:2021)**

Réseaux de communication industriels - Profils - Partie 3-
13: Bus de terrain de sécurité fonctionnelle - Spécifications
supplémentaires pour CPF 13
(IEC 61784-3-13:2021)

Industrielle Kommunikationsnetze - Profile - Teil 3-13:
Funktional sichere Übertragung bei Feldbussen -
Zusätzliche Festlegungen für die
Kommunikationsprofilfamilie 13
(IEC 61784-3-13:2021)

This European Standard was approved by CENELEC on 2021-06-23. 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 CEN-CENELEC Management Centre 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 CEN-CENELEC Management Centre 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, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.



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

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

European foreword

The text of document 65C/1083/FDIS, future edition 3 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 approved by CENELEC as EN IEC 61784-3-13:2021.

The following dates are fixed:

- latest date by which the document has to be implemented at national (dop) 2022-03-23 level by publication of an identical national standard or by endorsement
- latest date by which the national standards conflicting with the (dow) 2024-06-23 document have to be withdrawn

This document supersedes EN 61784-3-13:2017 and all of its amendments and corrigenda (if any).

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

Endorsement notice

The text of the International Standard IEC 61784-3-13:2021 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 61000-1-2	NOTE	Harmonized as EN 61000-1-2
IEC 61000-6-7	NOTE	Harmonized as EN 61000-6-7
IEC 61010-2-201	NOTE	Harmonized as EN IEC 61010-2-201
IEC 61131-2	NOTE	Harmonized as EN 61131-2
IEC 61131-6	NOTE	Harmonized as EN 61131-6
IEC 61158 (series)	NOTE	Harmonized as EN 61158 (series)
IEC 61158-5 (series)	NOTE	Harmonized as EN 61158-5 (series)
IEC 61326-3-1	NOTE	Harmonized as EN 61326-3-1
IEC 61326-3-2	NOTE	Harmonized as EN IEC 61326-3-2
IEC 61496 (series)	NOTE	Harmonized as EN IEC 61496 (series)
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 61511 (series)	NOTE	Harmonized as EN 61511 (series)
IEC 61784-1	NOTE	Harmonized as EN IEC 61784-1
IEC 61784-3 (series)	NOTE	Harmonized as EN 61784-3 (series)
IEC 61784-5 (series)	NOTE	Harmonized as EN IEC 61784-5 (series)
IEC 61800-5-2	NOTE	Harmonized as EN 61800-5-2
IEC 62061	NOTE	Harmonized as EN 62061
IEC 62443 (series)	NOTE	Harmonized as EN IEC 62443 (series)
ISO 10218-1	NOTE	Harmonized as EN ISO 10218-1
ISO 13849 (series)	NOTE	Harmonized as EN ISO 13849 (series)
ISO 13849-1:2015	NOTE	Harmonized as EN ISO 13849-1:2015 (not modified)
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 documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

NOTE 1 Where an International Publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

NOTE 2 Up-to-date information on the latest versions of the European Standards listed in this annex is available here: www.cenelec.eu.

<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/IEEE 8802-3	EN IEC 61784-2	-
IEC 61784-3	2021	Industrial communication networks - Profiles - Part 3: Functional safety fieldbuses - General rules and profile definitions	EN IEC 61784-3	2021
IEC 61784-5-13	-	Industrial communication networks - Profiles - Part 5-13: installation of fieldbuses - Installation profiles for CPF 13	EN 61784-5-13	-

EN IEC 61784-3-13:2021 (E)

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
IEC 61918	-	Industrial communication networks - Installation of communication networks in industrial premises	EN IEC 61918	-
ISO/IEC 19501	-	Information technology - Open Distributed Processing - Unified Modeling Language (UML) Version 1.4.2	-	-

CONTENTS

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

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

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

Bibliography.....	203
Figure 1 – Relationships of IEC 61784-3 with other standards (machinery)	16
Figure 2 – Relationships of IEC 61784-3 with other standards (process).....	17
Figure 3 – Producer consumer example	30
Figure 4 – Client server example	30
Figure 5 – Communication layer structure	33
Figure 6 – Safety communication channel.....	34
Figure 7 – Characteristic producer / consumer communication.....	35
Figure 8 – Extended producer / consumer communication	36
Figure 9 – Client Server communication.....	36
Figure 10 – Topology overview	37
Figure 11 – Safety Domain protection (example).....	38
Figure 12 – Safety Domain separation (example).....	39
Figure 13 – Data flow example.....	43
Figure 14 – Communication model.....	45
Figure 15 – SPDO transport.....	46
Figure 16 – SSDO transport.....	47
Figure 17 – Diagnostic data representation	48
Figure 18 – Safety PDUs inside a CP 13/1 PDU.....	49
Figure 19 – Basic Safety PDU for $n = 0 - 8$ octet payload data	49
Figure 20 – Basic Safety PDU from 9 octet payload data	49
Figure 21 – Slim Safety PDU for $n = 0 - 8$ octet payload data	50
Figure 22 – Slim Safety PDU from 9 octet payload data	51
Figure 23 – Safety PDU with 40 bit counter for $n = 0 - 8$ octet payload data	52
Figure 24 – Safety PDU with 40 bit counter from 9 octet payload data	52
Figure 25 – SPDO_Data_Only telegram.....	58
Figure 26 – SPDO_Data_with_Time_Request telegram	58
Figure 27 – SPDO_Data_with_Time_Response telegram.....	59
Figure 28 – SSDO download protocols.....	62
Figure 29 – SSDO upload protocols	62
Figure 30 – SSDO Download Initiate protocol	63
Figure 31 – SSDO Download Segment protocol	64
Figure 32 – SSDO Download Initiate protocol with Preload	65
Figure 33 – SSDO Download Segment protocol with Preload	66
Figure 34 – SSDO Upload Initiate protocol.....	67
Figure 35 – SSDO Upload Segment protocol	68
Figure 36 – SSDO Upload Initiate protocol with Preload	69
Figure 37 – SSDO Upload Segment protocol with Preload	71
Figure 38 – SSDO Abort protocol.....	72
Figure 39 – UDID Request / Response protocol	75
Figure 40 – SADR Assignment protocol	76
Figure 41 – Reset Node Guarding Time protocol.....	77

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

Figure 85 – State diagram SCM handle single UDID mismatch	186
Figure 86 – State diagram SCM verify parameters	188
Figure 87 – State diagram activate SN	190
Figure 88 – Safety function response time	192
Figure 89 – Assessment flow of devices	197
Table 1 – Communication errors and detection measures (cyclic)	31
Table 2 – Communication errors and detection measures (acyclic)	32
Table 3 – Device roles	37
Table 4 – Basic Safety PDU format	50
Table 5 – Slim Safety PDU format	51
Table 6 – Safety PDU with 40 bit counter	53
Table 7 – PDU identification field (ID)	54
Table 8 – Used ID field combinations	54
Table 9 – Request / response identification	54
Table 10 – Type of CRC depending on LE	55
Table 11 – CRC polynoms for SPDUs	56
Table 12 – SPDO telegram types (ID field, bits 2, 3 and 4)	57
Table 13 – Fields of SPDO_Data_Only telegram	58
Table 14 – Fields of SPDO_Data_with_Time_Request telegram	59
Table 15 – Fields of SPDO_Data_with_Time_Response telegram	59
Table 16 – SSDO telegram types (ID field, bits 2, 3 and 4)	60
Table 17 – SOD Access Command (SACmd) – bit coding	61
Table 18 – Fields of Download Initiate SSDO_Service_Request telegram	63
Table 19 – Fields of Download Initiate SSDO_Service_Response telegram	63
Table 20 – Fields of Download Segment SSDO_Service_Request telegram	64
Table 21 – Fields of Download Segment SSDO_Service_Response telegram	64
Table 22 – Fields of Download Initiate SSDO_Service_Request telegram with Preload	65
Table 23 – Fields of Download Initiate SSDO_Service_Response telegram with Preload	65
Table 24 – Fields of Download Segment SSDO_Service_Request telegram with Preload	66
Table 25 – Fields of Download Segment SSDO_Service_Response telegram with Preload	67
Table 26 – Fields of Upload Initiate SSDO_Service_Request telegram	67
Table 27 – Fields of Upload Initiate SSDO_Service_Response telegram	68
Table 28 – Fields of Upload Segment SSDO_Service_Request telegram	69
Table 29 – Fields of Upload Segment SSDO_Service_Response telegram	69
Table 30 – Fields of Upload Initiate SSDO_Service_Request telegram with Preload	70
Table 31 – Fields of Upload Initiate SSDO_Service_Response telegram with Preload	70
Table 32 – Fields of Upload Segment SSDO_Service_Request telegram with Preload	71
Table 33 – Fields of Upload Segment SSDO_Service_Response telegram with Preload	71
Table 34 – Fields of SSDO Abort telegram	72
Table 35 – SSDO Abort codes	72
Table 36 – TR field usage for SSDO Preload	73
Table 37 – Bit fields inside TR field for SSDO Preload	74

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

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

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

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

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

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

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**INDUSTRIAL COMMUNICATION NETWORKS –
PROFILES –****Part 3-13: Functional safety fieldbuses –
Additional specifications for CPF 13****FOREWORD**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

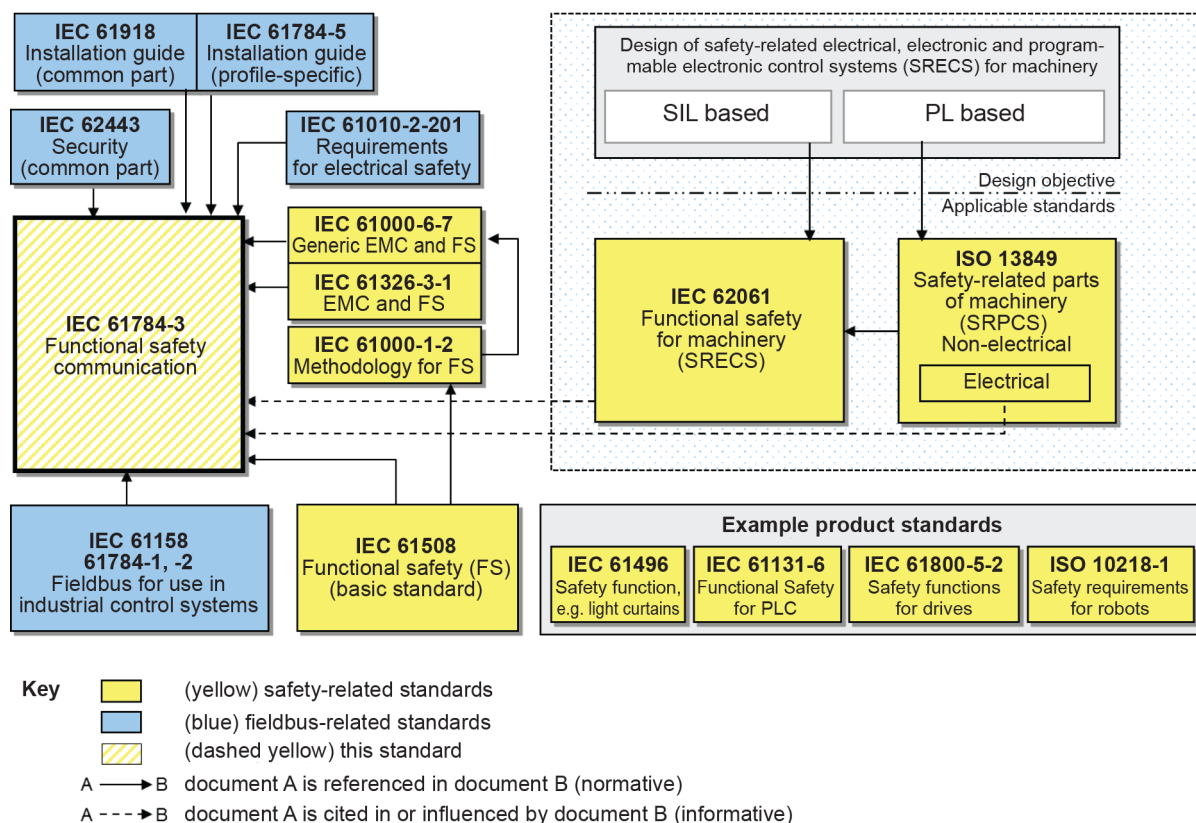
0 Introduction

0.1 General

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

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

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

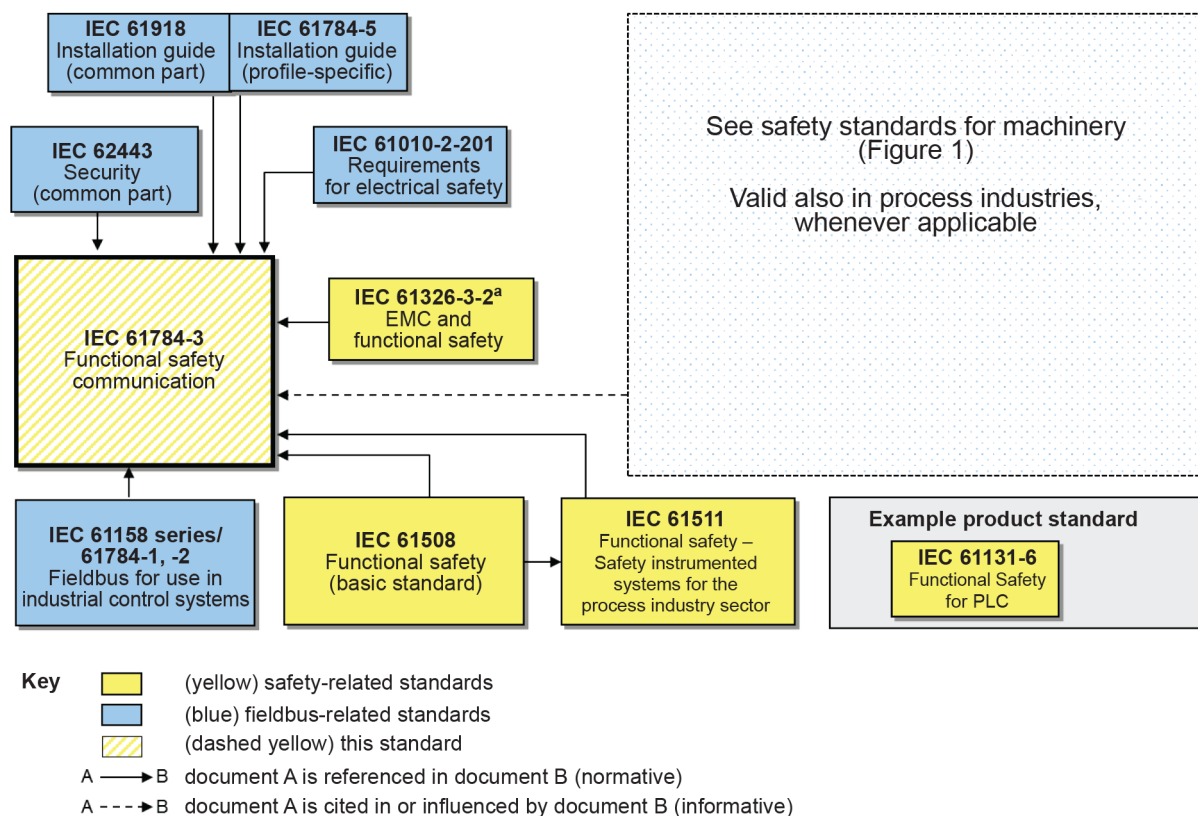


IEC

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

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

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



IEC

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

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

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

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

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

IEC 61784-3 (all parts) describes:

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

0.2 Patent declaration

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

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

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

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES –

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

1 Scope

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

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

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

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

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

2 Normative references

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

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

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

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

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

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

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

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

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

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

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

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

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

3 Terms, definitions, symbols, abbreviated terms and conventions

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC 61784-3 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at <http://www.electropedia.org/>
- ISO Online browsing platform: available at <http://www.iso.org/obp>

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

3.1.1 Common terms and definitions

NOTE These common terms and definitions are inherited from IEC 61784-3:2021.

3.1.1.1

bit error probability

P_e

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

3.1.1.2

black channel

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

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

3.1.1.3

closed communication system

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

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

3.1.1.4**communication channel**

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

3.1.1.5**communication system**

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

3.1.1.6**connection**

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

3.1.1.7**Cyclic Redundancy Check****CRC**

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

<method> procedure used to calculate the redundant data

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

Note 2 to entry: See also [31], [32]².

3.1.1.8**defined communication system**

defined channel

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

3.1.1.9**DLPDU**

DEPRECATED: frame

Data Link Protocol Data Unit

3.1.1.10**error**

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

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

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

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

² Figures in square brackets refer to the bibliography.

3.1.1.11

failure

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

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

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

3.1.1.12

fault

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

Note 1 to entry: IEC 60050-191:1990, 191-05-01 defines "fault" as a state characterized by the inability to perform a required function, excluding the inability during preventive maintenance or other planned actions, or due to lack of external resources.

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

3.1.1.13

fieldbus

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

3.1.1.14

fieldbus system

system using a *fieldbus* with connected devices

3.1.1.15

hash function

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

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

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

3.1.1.16

hazard

potential source of harm

Note 1 to entry: The term includes danger to persons arising within a short time scale (for example, fire and explosion) and also those that have a long-term effect on a person's health (for example, release of a toxic substance).

[SOURCE: IEC 61508-4:2010, 3.1.2 and ISO/IEC Guide 51:2014, definition 3.2]

3.1.1.17

master

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

3.1.1.18

message

<information theory and communication theory> ordered sequence of characters (usually octets) intended to convey information

[SOURCE: ISO/IEC 2382:2015, 2123205, modified – insertion of "(usually octets)", deletion of notes and source]

3.1.1.19
performance level

PL

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

[SOURCE: ISO 13849-1:2015, 3.1.23]

3.1.1.20
redundancy

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

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

3.1.1.21
residual error rate

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

3.1.1.22
risk

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

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

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

3.1.1.23
safety communication channel

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

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

3.1.1.24
safety communication layer

SCL

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

3.1.1.25
safety data

data transmitted across a safety network using a safety protocol

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

3.1.1.26
safety device

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

3.1.1.27

safety function

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

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

3.1.1.28

safety function response time

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

Note 1 to entry: This concept is introduced in IEC 61784-3:2021, 5.2.4 and addressed by the functional safety communication profiles defined in this document.

3.1.1.29

safety integrity level

SIL

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

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

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

Note 3 to entry: A safety integrity level (SIL) is not a property of a system, subsystem, element or component. The correct interpretation of the phrase "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.

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

3.1.1.30

safety measure

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

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

Note 2 to entry: Communication *errors* and related safety measures are detailed in IEC 61784-3:2021, 5.3 and 5.4.

3.1.1.31

safety PDU

SPDU

PDU transferred through the *safety communication channel*

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

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

3.1.1.32

safety-related application

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

3.1.1.33**safety-related system**

system performing *safety functions* according to IEC 61508

3.1.1.34**slave**

communication entity able to receive *messages* and send them in response to another communication entity which may be a *master* or a slave, but not to initiate communication activities

3.1.1.35**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 1 to entry: 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 1 023 *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 safe 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 (all parts)]
FS	Functional Safety	
FSCP	Functional Safety Communication Profile	
MTBF	Mean Time Between Failures	
MTTF	Mean Time To Failure	
PDU	Protocol Data Unit	[ISO/IEC 7498-1]
PFH	Average frequency of dangerous failure [h-1] per hour	[IEC 61508-4:2010]
PhL	Physical Layer	[ISO/IEC 7498-1]
PL	Performance Level	[ISO 13849-1]
PLC	Programmable Logic Controller	
SCL	Safety Communication Layer	
SIL	Safety Integrity Level	[IEC 61508-4:2010]
SPDU	Safety PDU	

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	PDU 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 document 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 document 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 document where appropriate.

4 Overview of FSCP 13/1 (openSAFETY™)

4.1 Functional Safety Communication Profile 13/1

Communication Profile Family 13 (commonly known as Ethernet POWERLINK™³) 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 (openSAFETY™) is based on the CPF 13 basic profiles in IEC 61784-2 and the safety communication layer specifications defined in this document.

4.2 Technical overview

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

The FSCP 13/1 services and protocol specify 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 uses the client server model (see Figure 4).

³ Ethernet POWERLINK™ and openSAFETY™ are trade names of the non-profit organization Ethernet POWERLINK™ Standardization Group (EPSPG). This information is given for the convenience of users of this document and does not constitute an endorsement by IEC of the trade name holder or any of its products. Compliance to this document does not require use of the trade names Ethernet POWERLINK™ or openSAFETY™. Use of the trade names Ethernet POWERLINK™ or openSAFETY™ requires permission of Ethernet POWERLINK Standardization Group (EPSPG) and compliance with conditions for their use (such as testing and validation).

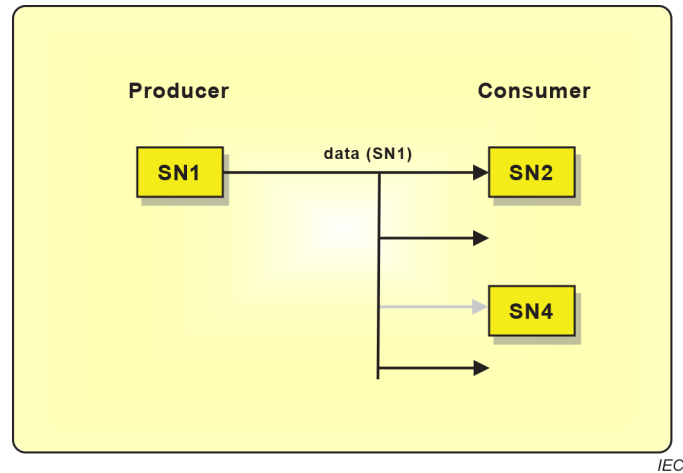


Figure 3 – Producer consumer example

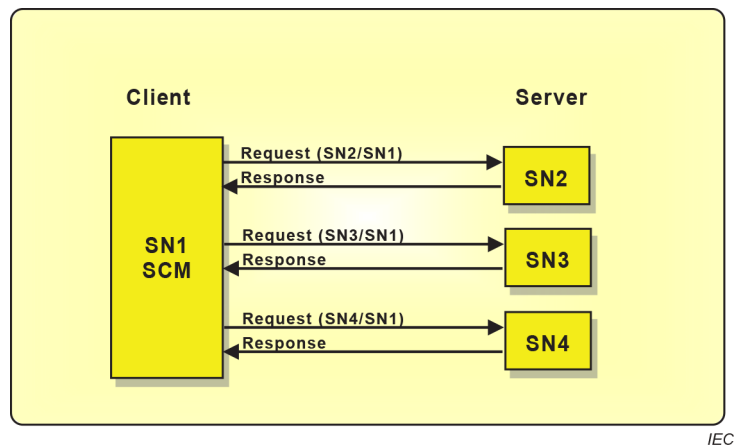


Figure 4 – Client server example

5 General

5.1 External documents providing specifications for the profile

The documents [38] and [39] 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 document,

- 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 document, 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	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			X					
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 depending on the used Safety PDU;
- 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 SCT_U32, Table 158), 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.

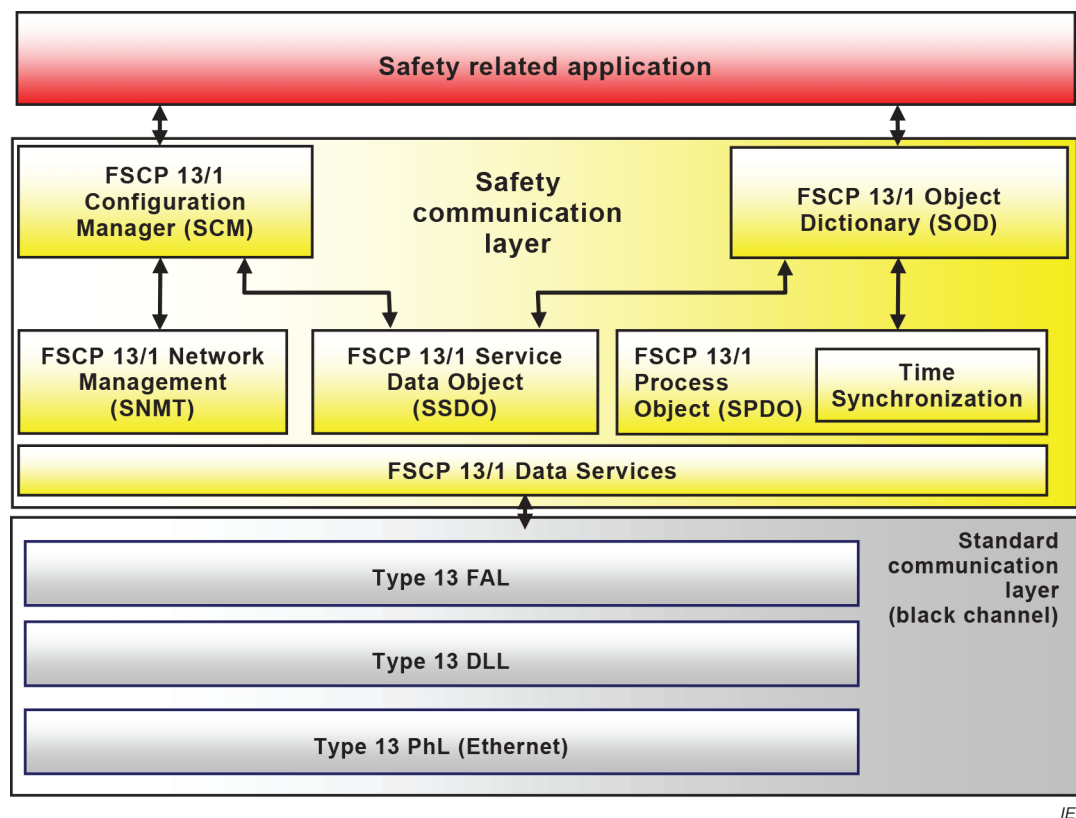


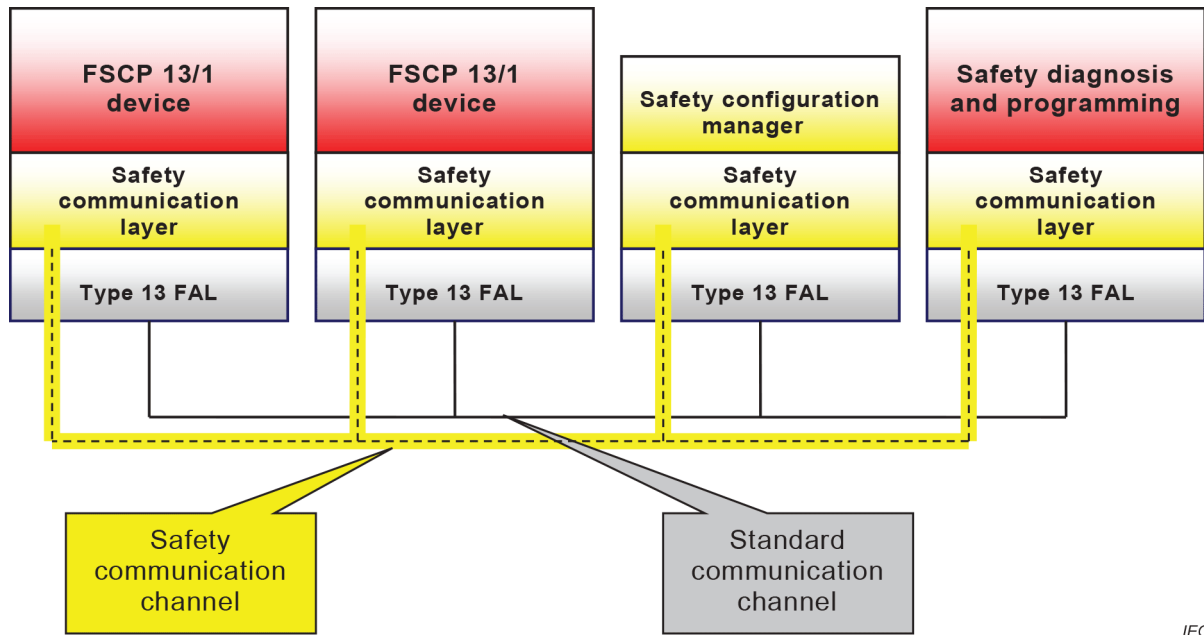
Figure 5 – Communication layer structure

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).



IEC

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 document 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)

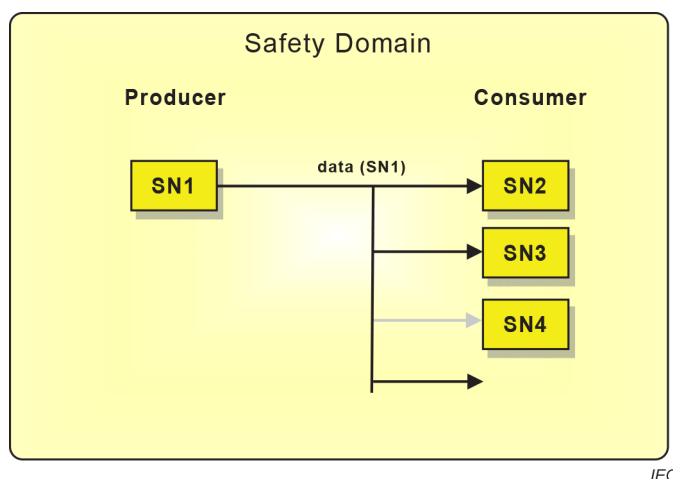
The SCM shall provide the required services for start-up, parameterization and all further measures to ensure safe operation over the entire life cycle of the application.

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.



IEC

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.

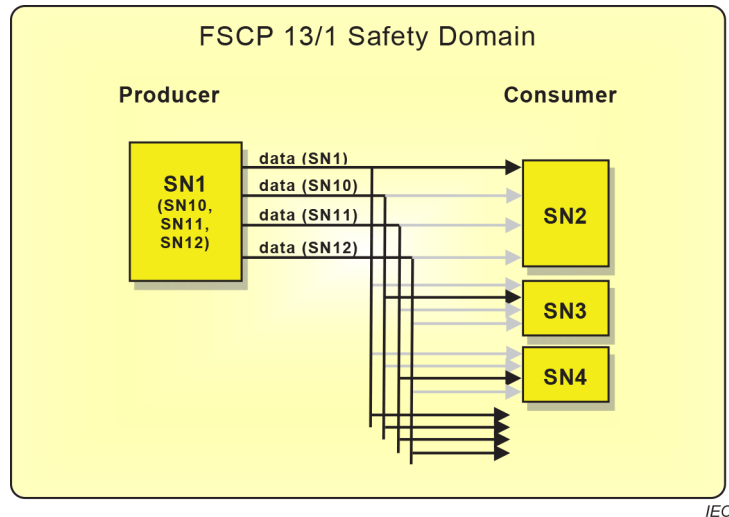


Figure 8 – Extended producer / consumer communication

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).

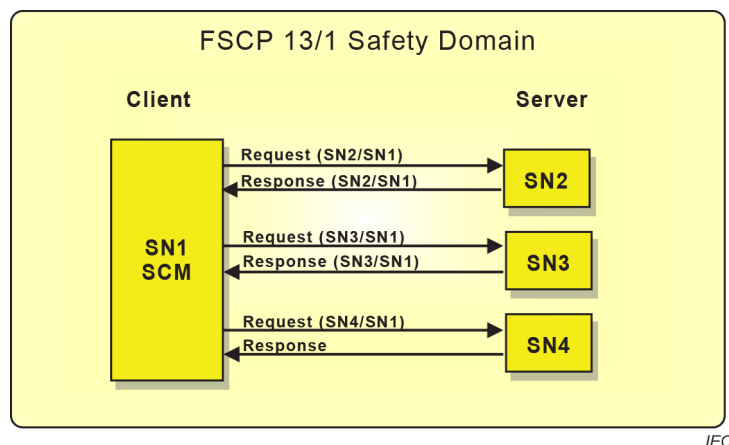


Figure 9 – Client Server communication

6.1.3 Device roles and topology

6.1.3.1 General

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

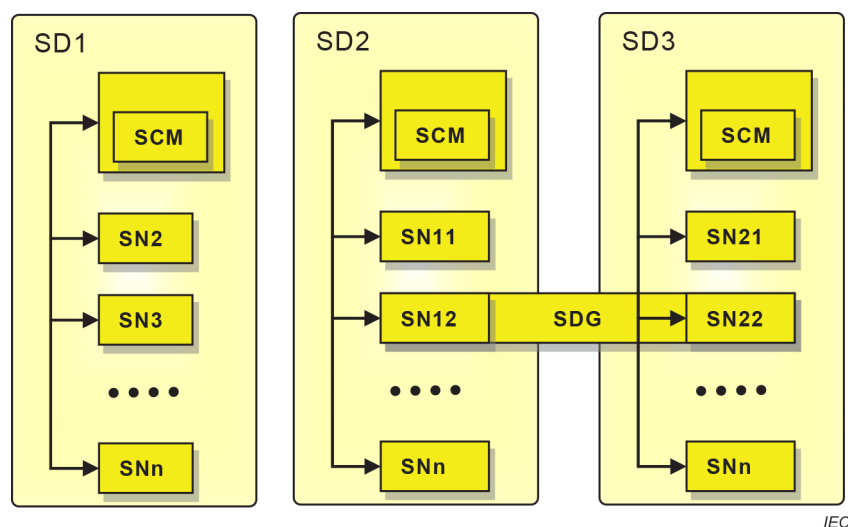
Table 3 – Device roles

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 document. 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 7.5.4.9) 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 The SCM will store all this SN specific data.

- 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

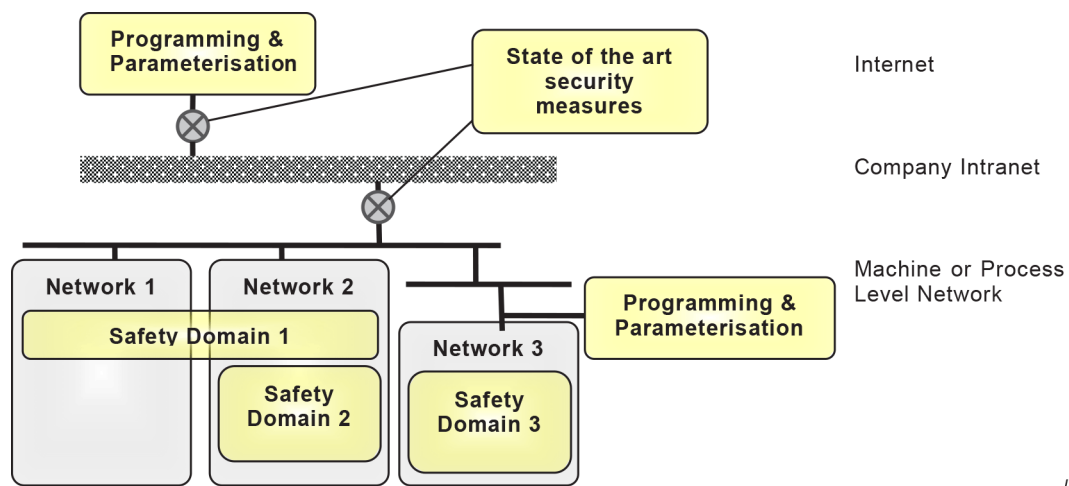
A Safety Domain shall constitute an address space of up to 1 023 SADRs (1 – 1 023). Only SNs sharing the same SD shall be able to communicate directly with each other. SNs on different SDs shall be restricted to communication via a Safety Domain Gateway.

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, the security of the system shall be observed. Choosing an adequate encryption system is the responsibility of deployment planning and is outside the scope of this document. Proper state of the art security measures shall be applied.

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



IEC

Figure 11 – Safety Domain protection (example)

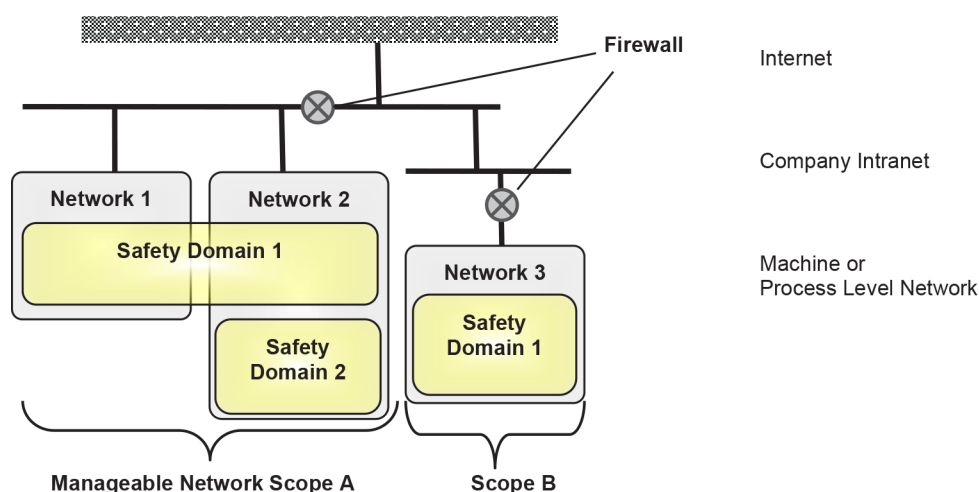
6.1.3.3.3 Safety Domain separation

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

If the size of the company intranet and the organization of the network management do not allow the administration of unique Safety Domain numbers, the network should be split into several manageable network scopes and separated by established 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.



IEC

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 document 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 document.

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 With this periodic life guard signal from the SCM the SN detects 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. Subclause 6.2 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 configure and verify the safety related devices. FSCP 13/1 uses a single datastream to configure a device. This is necessary to satisfy all requirements coming from the wide range of applications FSCP 13/1 is ready for. Configuration modes are:

- 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

Installation of applications and parameters on the FSCP 13/1 devices 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 should 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.

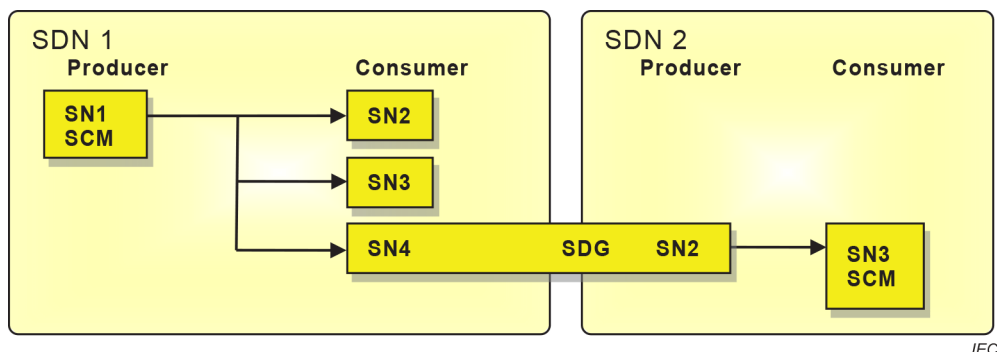


Figure 13 – Data flow example

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 7.5.4.6), 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 and therefore no longer being a 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 organizational measurements like switching off all SNs in case of reconfiguring the SCM, may eliminate the risk in this situation. As a result, the interval for the life guarding signal 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

Subclause 6.3 lists the requirements on the non safety communication layer for transportation of safety PDUs. Communication protocols according to CPF 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.

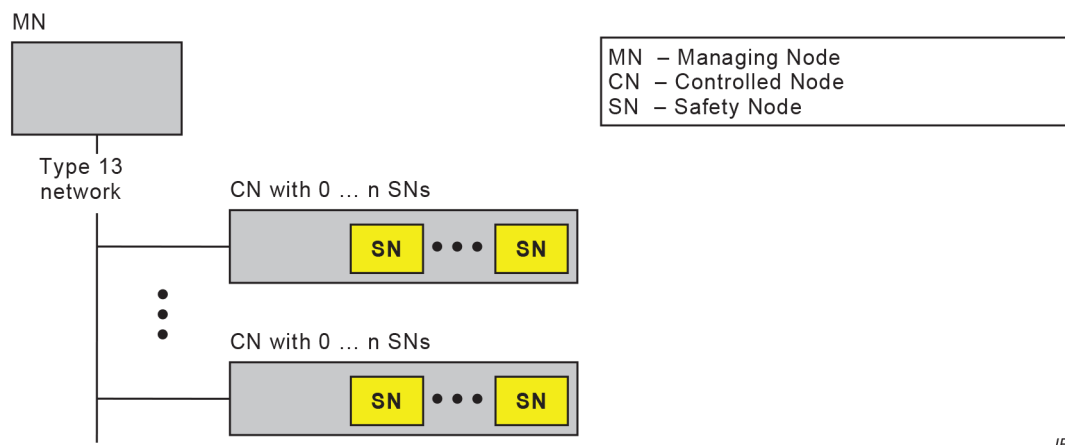
6.3.2.2 Masquerading

To avoid any possibilities of masquerading data as safety PDUs, non safety related nodes shall not contain code which is able to generate safety PDUs according to Clause 7.

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.



IEC

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.