



BSI Standards Publication

Industrial communication networks - Profiles

Part 3-3: Functional safety fieldbuses - Additional specifications for CPF 3 (IEC 61784-3-3:2016)

National foreword

This British Standard is the UK implementation of EN 61784-3-3:2017. It is identical to IEC 61784-3-3:2016. It supersedes BS EN 61784-3-3:2010, which is withdrawn.

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

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

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

© The British Standards Institution 2017
Published by BSI Standards Limited 2017

ISBN 978 0 580 94719 3

ICS 25.040.40; 35.100.05

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

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 November 2017.

Amendments/corrigenda issued since publication

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

English Version

**Industrial communication networks - Profiles - Part 3-3:
Functional safety fieldbuses - Additional specifications for CPF 3
(IEC 61784-3-3:2016)**

Réseaux de communication industriels - Profils - Partie 3-3:
Bus de terrain de sécurité fonctionnelle - Spécifications
supplémentaires pour CPF 3
(IEC 61784-3-3:2016)

Industrielle Kommunikationsnetze - Profile - Teil 3-3:
Funktional sichere Übertragung bei Feldbussen -
Zusätzliche Festlegungen für die
Kommunikationsprofilfamilie 3
(IEC 61784-3-3:2016)

This European Standard was approved by CENELEC on 2016-08-16. 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, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, 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: Avenue Marnix 17, B-1000 Brussels

European foreword

The text of document 65C/851/FDIS, future edition 3 of IEC 61784-3-3, 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 61784-3-3:2017.

The following dates are fixed:

- latest date by which the document has to be (dop) 2018-05-10
implemented at national level by
publication of an identical national
standard or by endorsement
- latest date by which the national (dow) 2020-11-10
standards conflicting with the
document have to be withdrawn

This document supersedes EN 61784-3-3:2010.

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 61784-3-3:2016 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 60870-5-1	NOTE	Harmonized as EN 60870-5-1.
IEC 61000-6-7	NOTE	Harmonized as EN 61000-6-7.
IEC 61131-6	NOTE	Harmonized as EN 61131-6.
IEC 61158 (all parts)	NOTE	Harmonized as EN 61158 (all parts).
IEC 61496 (all parts)	NOTE	Harmonized as EN 61496 (all parts).
IEC 61508-1:2010	NOTE	Harmonized as EN 61508-1:2010 (not modified).
IEC 61508-4:2010	NOTE	Harmonized as EN 61508-4:2010 (not modified).
IEC 61508-5:2010	NOTE	Harmonized as EN 61508-5:2010 (not modified).
IEC 61508-6:2010	NOTE	Harmonized as EN 61508-6:2010 (not modified).
IEC 61784-5 (all parts)	NOTE	Harmonized as EN 61784-5 (all parts).
IEC 61800-5-2	NOTE	Harmonized as EN 61800-5-2.
IEC 61804 (all parts)	NOTE	Harmonized as EN 61804 (all parts)
IEC 62443 (all parts)	NOTE	Harmonized as prEN 62443 (all parts)
IEC/TR 62685	NOTE	Harmonized as CLC/TR 62685.
ISO 10218-1	NOTE	Harmonized as EN ISO 10218-1.
ISO 12100	NOTE	Harmonized as EN ISO 12100.
ISO 13849 (all parts)	NOTE	Harmonized as EN ISO 13849 (all parts)

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 60204-1 (mod)	-	Safety of machinery - Electrical equipment - of machines - Part 1: General requirements	-	-
IEC 61000-6-2	-	Electromagnetic compatibility (EMC) - Part 6-2: Generic standards - Immunity standard for industrial environments	EN 61000-6-2	-
IEC 61010-1	-	Safety requirements for electrical equipment for measurement, control and laboratory use - Part 1: General requirements	EN 61010-1	-
IEC 61131-2	2007	Programmable controllers - Part 2: Equipment requirements and tests	EN 61131-2	2007
IEC 61131-3	-	Programmable controllers - Part 3: Programming languages	EN 61131-3	-
IEC 61158-2	-	Industrial communication networks - Fieldbus specifications - Part 2: Physical layer specification and service definition	EN 61158-2	-
IEC 61158-3-3	-	Industrial communication networks - Fieldbus specifications - Part 3-3: Data-link layer service definition - Type 3 elements	EN 61158-3-3	-
IEC 61158-4-3	-	Industrial communication networks - Fieldbus specifications - Part 4-3: Data-link layer protocol specification - Type 3 elements	EN 61158-4-3	-
IEC 61158-5-3	-	Industrial communication networks - Fieldbus specifications - Part 5-3: Application layer service definition - Type 3 elements	EN 61158-5-3	-
IEC 61158-5-10	-	Industrial communication networks - Fieldbus specifications - Part 5-10: Application layer service definition - Type 10 elements	EN 61158-5-10	-
IEC 61158-6-3	-	Industrial communication networks - Fieldbus specifications - Part 6-3: Application layer protocol specification - Type 3 elements	EN 61158-6-3	-
IEC 61158-6-10	-	Industrial communication networks - Fieldbus specifications - Part 6-10: Application layer protocol specification - Type 10 elements	EN 61158-6-10	-

IEC 61326-3-1	-	Electrical equipment for measurement, control and laboratory use – EMC requirements – Part 3-1: Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety) – General industrial applications	EN 61326-3-1	-
IEC 61326-3-2	-	Electrical equipment for measurement, control and laboratory use – EMC requirements – Part 3-2: Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety) – Industrial applications with specified electromagnetic environment	-	-
IEC 61508	series	Functional safety of electrical/electronic/programmable electronic safety-related systems	EN 61508	series
IEC 61508-2	-	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems	EN 61508-2	-
IEC 61511	series	Functional safety - Safety instrumented systems for the process industry sector	EN 61511	series
IEC 61784-1	-	Industrial communication networks - Profiles - Part 1: Fieldbus profiles	EN 61784-1	-
IEC 61784-2	-	Industrial communication networks - Profiles - Part 2: Additional fieldbus profiles for real-time networks based on ISO/IEC 8802-3	EN 61784-2	-
IEC 61784-3	-	Industrial communication networks - Profiles - Part 3: Functional safety fieldbuses - General rules and profile definitions	EN 61784-3	-
IEC 61784-5-3	-	Industrial communication networks - Profiles - Part 5-3: Installation of fieldbuses - Installation profiles for CPF 3	EN 61784-5-3	-
IEC 61918 (mod)	2013	Industrial communication networks - Installation of communication networks in industrial premises	EN 61918	2013
IEC 62061	-	Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems	EN 62061	-
IEC 62280	2014	Railway applications - Communication, signalling and processing systems - Safety related communication in transmission systems	-	-
ISO 13849-1	2006	Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design	EN ISO 13849-1	2008
ISO 13849-2	-	Safety of machinery - Safety-related parts of control systems - Part 2: Validation	EN ISO 13849-2	-
IEC/TR 62390	-	Common automation device - Profile guideline	-	-

CONTENTS

FOREWORD.....	8
0 Introduction	10
0.1 General.....	10
0.2 Patent declaration	12
1 Scope.....	14
2 Normative references.....	14
3 Terms, definitions, symbols, abbreviated terms and conventions.....	16
3.1 Terms and definitions	16
3.1.1 Common terms and definitions	16
3.1.2 CPF 3: Additional terms and definitions	22
3.2 Symbols and abbreviated terms.....	26
3.2.1 Common symbols and abbreviated terms.....	26
3.2.2 CPF 3: Additional symbols and abbreviated terms.....	27
3.3 Conventions.....	28
4 Overview of FSCP 3/1 (PROFIsafe™)	28
5 General	31
5.1 External documents providing specifications for the profile	31
5.2 Safety functional requirements	31
5.3 Safety measures	31
5.4 Safety communication layer structure	32
5.4.1 Principle of FSCP 3/1 safety communications	32
5.4.2 CPF 3 communication structures	33
5.5 Relationships with FAL (and DLL, PhL).....	36
5.5.1 Device model	36
5.5.2 Application and communication relationships	37
5.5.3 Data types	37
6 Safety communication layer services.....	38
6.1 F-Host services.....	38
6.2 F-Device services.....	41
6.3 Diagnosis.....	43
6.3.1 Safety alarm generation	43
6.3.2 F-Device safety layer diagnosis including the iPar-Server	43
7 Safety communication layer protocol	44
7.1 Safety PDU format	44
7.1.1 Safety PDU structure	44
7.1.2 Safety IO data.....	45
7.1.3 Status and Control Byte	45
7.1.4 (Virtual) MonitoringNumber	47
7.1.5 (Virtual) MNR mechanism (F_CRC_Seed=0).....	48
7.1.6 (Virtual) MNR mechanism (F_CRC_Seed=1).....	48
7.1.7 CRC2 Signature (F_CRC_Seed=0).....	50
7.1.8 CRC2 Signature (F_CRC_Seed=1).....	51
7.1.9 Non-safety IO data	52
7.2 FSCP 3/1 behavior	52
7.2.1 General	52

7.2.2	F-Host state diagram.....	53
7.2.3	F-Device state diagram	56
7.2.4	Sequence diagrams	60
7.2.5	Timing diagram for a MonitoringNumber reset.....	66
7.2.6	Monitoring of safety times	66
7.3	Reaction in the event of a malfunction	69
7.3.1	Unintended repetition	69
7.3.2	Loss	70
7.3.3	Insertion	70
7.3.4	Incorrect sequence	70
7.3.5	Corruption of safety data	70
7.3.6	Unacceptable delay.....	70
7.3.7	Masquerade.....	70
7.3.8	Addressing.....	71
7.3.9	Memory failures within switches	71
7.3.10	Loop-back.....	72
7.3.11	Network boundaries and router.....	72
7.4	F-Startup and parameter change at runtime	73
7.4.1	Standard startup procedure	73
7.4.2	iParameter assignment deblocking	73
8	Safety communication layer management.....	73
8.1	F-Parameter.....	73
8.1.1	Summary	73
8.1.2	F_Source/Destination_Address (Codename).....	74
8.1.3	F_WD_Time (F-Watchdog time).....	74
8.1.4	F_WD_Time_2 (secondary F-Watchdog time)	75
8.1.5	F_Prm_Flag1 (Parameters for the safety layer management)	75
8.1.6	F_Prm_Flag2 (Parameters for the safety layer management)	77
8.1.7	F_iPar_CRC (value of iPar_CRC across iParameters).....	78
8.1.8	F_Par_CRC calculation (across F-Parameters).....	79
8.1.9	Structure of the F-Parameter record data object.....	79
8.2	iParameter and iPar_CRC	79
8.3	Safety parameterization.....	80
8.3.1	Objectives.....	80
8.3.2	GSDL and GSDML safety extensions.....	81
8.3.3	Securing safety parameters and GSD data	83
8.4	Safety configuration	87
8.4.1	Securing the safety IO data description (CRC7)	87
8.4.2	Dataltem data type section examples	88
8.5	Data type information usage	92
8.5.1	F-Channel driver	92
8.5.2	Rules for standard F-Channel drivers	93
8.5.3	Recommendations for F-Channel drivers	94
8.6	Safety parameter assignment mechanisms	95
8.6.1	F-Parameter assignment	95
8.6.2	General iParameter assignment	95
8.6.3	System integration requirements for iParameterization tools	96
8.6.4	iPar-Server	98
9	System requirements	107

9.1	Indicators and switches	107
9.2	Installation guidelines.....	107
9.3	Safety function response time.....	107
9.3.1	Model	107
9.3.2	Calculation and optimization.....	109
9.3.3	Adjustment of watchdog times for FSCP 3/1	111
9.3.4	Engineering tool support	112
9.3.5	Retries (repetition of messages).....	112
9.4	Duration of demands	113
9.5	Constraints for the calculation of system characteristics.....	114
9.5.1	Probabilistic considerations	114
9.5.2	Safety related assumptions	116
9.5.3	Non safety related constraints (availability).....	117
9.6	Maintenance	117
9.6.1	F-Module commissioning / replacement	117
9.6.2	Identification and maintenance functions	117
9.7	Safety manual	117
9.8	Wireless transmission channels.....	119
9.8.1	Black channel approach	119
9.8.2	Availability	119
9.8.3	Security measures	119
9.8.4	Stationary and mobile applications	122
9.9	Conformance classes	122
10	Assessment.....	124
10.1	Safety policy	124
10.2	Obligations.....	124
Annex A (informative) Additional information for functional safety communication profiles of CPF 3.....		126
A.1	Hash function calculation.....	126
A.2	Example values for MonitoringNumbers (MNR)	129
A.3	Response time measurements.....	130
Annex B (informative) Information for assessment of the functional safety communication profiles of CPF 3.....		133
Bibliography		134
Figure 1 – Relationships of IEC 61784-3 with other standards (machinery).....		10
Figure 2 – Relationships of IEC 61784-3 with other standards (process)		11
Figure 3 – Basic communication preconditions for FSCP 3/1		29
Figure 4 – Structure of an FSCP 3/1 safety PDU.....		29
Figure 5 – Safety communication on CPF 3		30
Figure 6 – Standard CPF 3 transmission system.....		32
Figure 7 – Safety layer architecture.....		33
Figure 8 – Basic communication layers.....		34
Figure 9 – Multiport switch bus structure		34
Figure 10 – Linear bus structure.....		35
Figure 11 – Crossing network borders with routers		35
Figure 12 – Complete safety transmission paths.....		36

Figure 13 – IO Device model	37
Figure 14 – FSCP 3/1 communication structure	38
Figure 15 – F user interface of F-Host driver instances	39
Figure 16 – Motivation for "Channel-related Passivation"	40
Figure 17 – F-Device driver interfaces	42
Figure 18 – Safety PDU for CPF 3.....	45
Figure 19 – Status Byte	45
Figure 20 – Control Byte	46
Figure 21 – The Toggle Bit function.....	47
Figure 22 – F-Device MonitoringNumber	48
Figure 23 – F-Host CRC2 signature generation (F_CRC_Seed=0)	50
Figure 24 – Details of the CRC2 signature calculation (F_CRC_Seed=0)	51
Figure 25 – CRC2 signature calculation (F_CRC_Seed=1).....	51
Figure 26 – Details of the CRC2 signature calculation (F_CRC_Seed=1)	52
Figure 27 – Safety layer communication relationship	52
Figure 28 – F-Host state diagram	53
Figure 29 – F-Device state diagram.....	57
Figure 30 – Interaction F-Host / F-Device during start-up	60
Figure 31 – Interaction F-Host / F-Device during F-Host power off → on	61
Figure 32 – Interaction F-Host / F-Device with delayed power on	62
Figure 33 – Interaction F-Host / F-Device during power off → on.....	63
Figure 34 – Interaction F-Host / F-Device while host recognizes CRC error	64
Figure 35 – Interaction F-Host / F-Device while device recognizes CRC error.....	65
Figure 36 – Impact of the MNR reset signal	66
Figure 37 – Monitoring the message transit time F-Host ↔ F-Output.....	67
Figure 38 – Monitoring the message transit time F-Input ↔ F-Host	67
Figure 39 – Extended watchdog time on request.....	69
Figure 40 – iParameter assignment deblocking by the F-Host	73
Figure 41 – Effect of F_WD_Time_2.....	75
Figure 42 – F_Prm_Flag1.....	75
Figure 43 – F_Check_SeqNr	76
Figure 44 – F_Check_iPar.....	76
Figure 45 – F_SIL	76
Figure 46 – F_CRC_Length.....	77
Figure 47 – F_CRC_Seed	77
Figure 48 – F_Prm_Flag2.....	77
Figure 49 – F_Passivation.....	78
Figure 50 – F_Block_ID	78
Figure 51 – F_Par_Version	78
Figure 52 – F-Parameter	79
Figure 53 – iParameter block	80
Figure 54 – F-Parameter extension within the GSDML specification	82
Figure 55 – F_Par_CRC signature including iPar_CRC	82

Figure 56 – Algorithm to build CRC0	84
Figure 57 – GSD example in GSDML notation	86
Figure 58 – DataItem section for F_IN_OUT_1	89
Figure 59 – DataItem section for F_IN_OUT_2	90
Figure 60 – DataItem section for F_IN_OUT_5	91
Figure 61 – DataItem section for F_IN_OUT_6	92
Figure 62 – F-Channel driver as "glue" between F-Device and user program	93
Figure 63 – Layout example of an F-Channel driver	94
Figure 64 – F-Parameter assignment for simple F-Devices and F-Slaves	95
Figure 65 – F and iParameter assignment for complex F-Devices	96
Figure 66 – System integration of CPD-Tools	97
Figure 67 – iPar-Server mechanism (commissioning)	98
Figure 68 – iPar-Server mechanism (for example F-Device replacement)	99
Figure 69 – iPar-Server request coding ("status model")	100
Figure 70 – Coding of SR_Type	101
Figure 71 – iPar-Server request coding ("alarm model")	102
Figure 72 – iPar-Server state diagram	104
Figure 73 – Example safety function with a critical response time path	108
Figure 74 – Simplified typical response time model	108
Figure 75 – Frequency distributions of typical response times of the model	109
Figure 76 – Context of delay times and watchdog times	110
Figure 77 – Timing sections forming the FSCP 3/1 F_WD_Time	111
Figure 78 – Frequency distribution of response times with message retries	112
Figure 79 – Retries with CP 3/1	113
Figure 80 – Retries with CP 3/RTE	113
Figure 81 – Residual error probabilities for the 24-bit CRC polynomial	114
Figure 82 – Residual error probabilities for the 32-bit CRC polynomial	115
Figure 83 – Monitoring of corrupted messages	116
Figure 84 – Considerations against systematic loop-back configuration errors	119
Figure 85 – Security for WLAN networks	120
Figure 86 – Security for Bluetooth networks	121
Figure A.1 – Typical "C" procedure of a cyclic redundancy check	126
Figure A.2 – Comparison of the response time model and a real application	130
Figure A.3 – Frequency distribution of measured response times	131
Figure A.4 – F-Host with standard and safety-related application programs	132
Table 1 – Deployed measures to master errors	32
Table 2 – Data types for FSCP 3/1	37
Table 3 – Safety layer diagnosis messages	44
Table 4 – MonitoringNumber of an F-Host PDU	48
Table 5 – MonitoringNumber of an F-Device PDU	48
Table 6 – MonitoringNumber of an F-Host PDU	49
Table 7 – MonitoringNumber of an F-Device PDU	49

Table 8 – Definition of terms used in F-Host state diagram	54
Table 9 – F-Host states and transitions	54
Table 10 – Definition of terms used in Figure 29	57
Table 11 – F-Device states and transitions	58
Table 12 – SIL monitor times	69
Table 13 – Remedies for switch failures	71
Table 14 – Safety network boundaries	72
Table 15 – Codename octet order	74
Table 16 – GSDL keywords for F-Parameters and F-IO structures	81
Table 17 – GSD example in GSDL notation	85
Table 18 – Serialized octet stream for the examples	86
Table 19 – IO data structure items	87
Table 20 – Sample F-Channel drivers	93
Table 21 – Requirements for iParameterization	96
Table 22 – Specifier for the iPar-Server Request	101
Table 23 – Structure of the Read_RES_PDU ("read record")	102
Table 24 – Structure of the Write_REQ_PDU ("write record")	103
Table 25 – Structure of the Pull_RES_PDU ("Pull")	103
Table 26 – Structure of the Push_REQ_PDU ("Push")	103
Table 27 – iPar-Server states and transitions	105
Table 28 – iPar-Server management measures	106
Table 29 – Definition of terms in Figure 83	116
Table 30 – Information to be included in the safety manual	118
Table 31 – Definition of terms in Figure 85	120
Table 32 – Security measures for WLAN (IEEE 802.11)	120
Table 33 – Definition of terms in Figure 86	121
Table 34 – Security measures for Bluetooth (IEEE 802.15.1)	122
Table 35 – F-Host conformance class requirements	122
Table 36 – Main characteristics of protocol versions	124
Table 37 – F-Host/F-Device conformance matrix	124
Table A.1 – The table "Crctab24" for 24 bit CRC signature calculations	127
Table A.2 – The table "Crctab32" for 32 bit CRC signature calculations	128
Table A.3 – The table "Crctab16" for 16 bit CRC signature calculations	129
Table A.4 – Values of CN_incrNR_64 and MNR for F-Host PDU	130

INTERNATIONAL ELECTROTECHNICAL COMMISSION

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

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

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

This third edition cancels and replaces the second edition published in 2010. This edition constitutes a technical revision. This edition includes the following significant technical changes with respect to the previous edition:

- Legacy V1-mode removed from this protocol edition;
- Protocol extensions to protect against possible loopbacks (LP extensions);
- Protocol extensions to keep SIL3 for safety networks with large numbers of participants (XP extensions) and subsequent new F-Parameter "F_CRC_Seed";
- Introduction of random and disjoint Codename based MonitoringNumbers (MNR) besides to the previous Consecutive Numbers;

- Provisions for Channel Granular Passivation and subsequent new F-Parameter "F_Passivation";
- GSD extensions due to new F-Parameters;
- Notations according to the CP3 family in IEC 61158 (e.g. IO Controller);
- Additional diagnosis message types;
- Diverse error corrections and fixes of typos;
- Updated documents in bibliography.

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

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

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

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

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

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

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

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

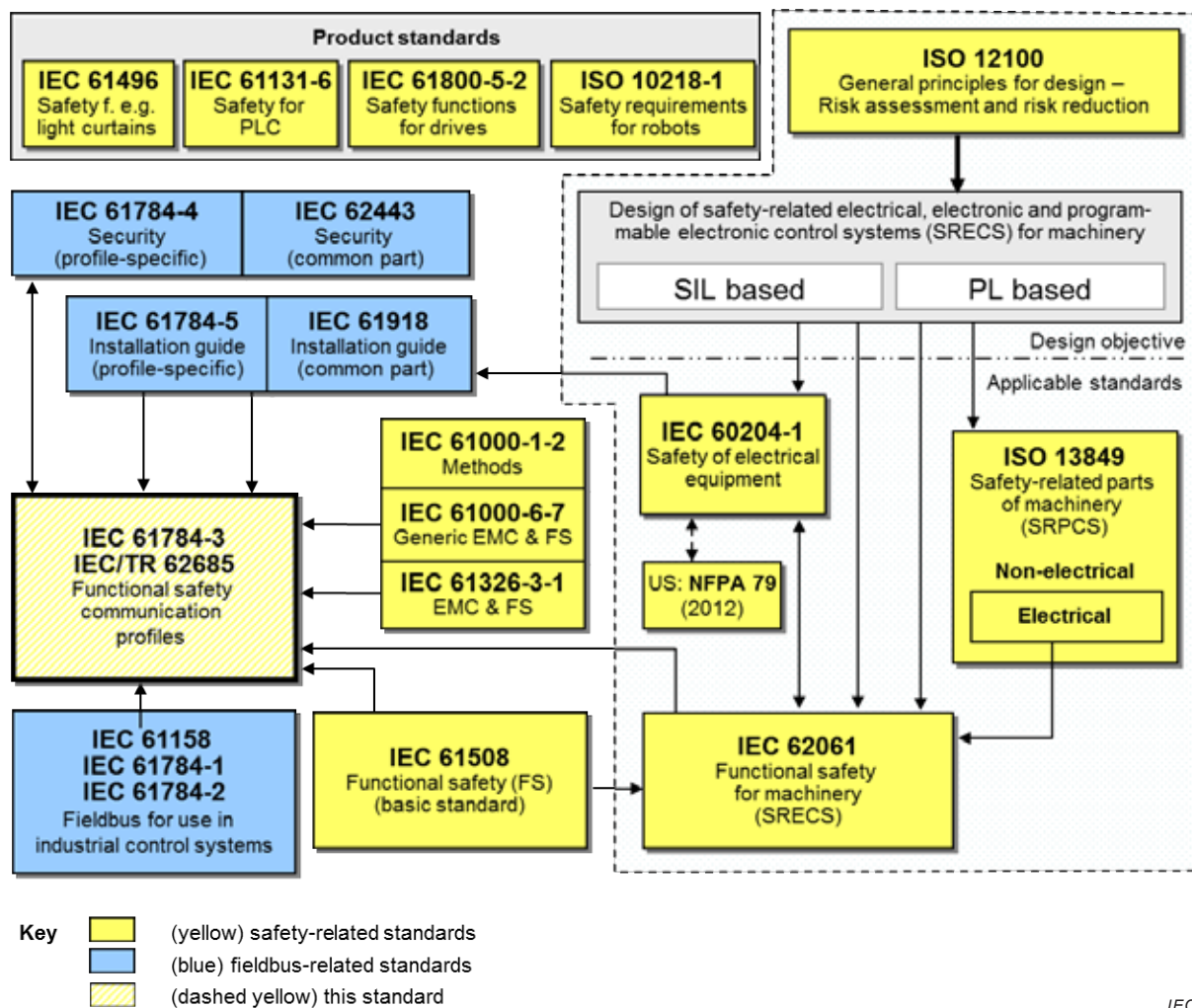
0 Introduction

0.1 General

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

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

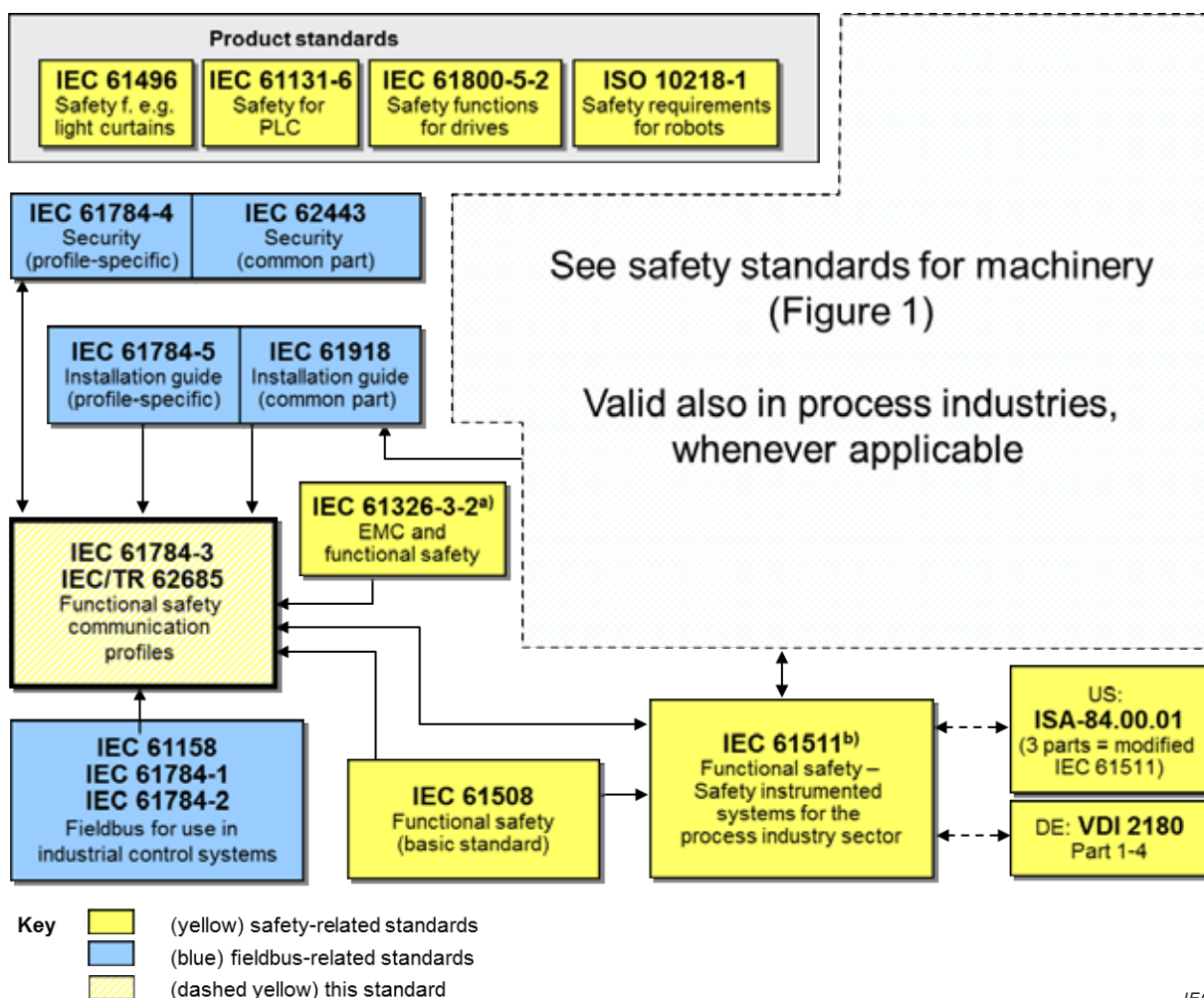
Figure 1 shows the relationships between this standard and relevant safety and fieldbus standards in a machinery environment.



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

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

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



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

^b EN ratified.

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

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

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

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

This standard describes:

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

0.2 Patent declaration

The International Electrotechnical Commission (IEC) draws attention to the fact that it is claimed that compliance with this document may involve the use of patents concerning the functional safety communication profiles for family 3 as follows, where the [xx] notation indicates the holder of the patent rights:

US 6907542	[SI] System, device and method for determining the reliability of data carriers in a failsafe system network
US 6725419 DE 59910661.1 EP 1064590	[SI] Automation system and method for operating an automation system
US 7808917 DE 50 2005 001 819.2 EP 1686732	[SI] Method and system for transmitting telegrams
US 7640480 DE 50 2005 004 305.7 EP 1802019	[SI] Detection of errors in the communication of data
EP 1921525	[SI] Security-related system component e.g. guard door, for automation system of production system, has comparing unit comparing signatures for identity, where component supports security-related operation during sameness of signatures
EP 13172092.2	[SI] Method and System for Detecting Errors when Transmitting Data from a Transmitter to at Least One Receiver

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

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

Information may be obtained from:

[SI] Siemens Aktiengesellschaft
CT IP M&A
Otto-Hahn-Ring 6
81739 München
GERMANY

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

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

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES –

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

1 Scope

This part of the IEC 61784-3 series specifies a safety communication layer (services and protocol) based on CPF 3 of IEC 61784-1, IEC 61784-2 (CP 3/1, CP 3/2, CP 3/4, CP 3/5 and CP 3/6) and IEC 61158 Types 3 and 10. It identifies the principles for functional safety communications defined in IEC 61784-3 that are relevant for this safety communication layer. This safety communication layer is intended for implementation in safety devices only.

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

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

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

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

2 Normative references

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

IEC 60204-1, *Safety of machinery – Electrical equipment of machines – Part 1: General requirements*

IEC 61000-6-2, *Electromagnetic compatibility (EMC) – Part 6-2: Generic standards – Immunity for industrial environments*

IEC 61010-1, *Safety requirements for electrical equipment for measurement, control, and laboratory use – Part 1: General requirements*

IEC 61131-2:2007, *Programmable controllers – Part 2: Equipment requirements and tests*

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

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

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

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

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

IEC 61158-4-3, *Industrial communication networks – Fieldbus specifications – Part 4-3: Data-link layer protocol specification – Type 3 elements*

IEC 61158-5-3, *Industrial communication networks – Fieldbus specifications – Part 5-3: Application layer service definition – Type 3 elements*

IEC 61158-5-10, *Industrial communication networks – Fieldbus specifications – Part 5-10: Application layer service definition – Type 10 elements*

IEC 61158-6-3, *Industrial communication networks – Fieldbus specifications – Part 6-3: Application layer protocol specification – Type 3 elements*

IEC 61158-6-10, *Industrial communication networks – Fieldbus specifications – Part 6-10: Application layer protocol specification – Type 10 elements*

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

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

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

IEC 61508-2, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*

IEC 61511 (all parts), *Functional safety – Safety instrumented systems for the process industry sector*

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

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

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

IEC 61784-5-3, *Industrial communication networks – Profiles – Part 5-3: Installation of fieldbuses – Installation profiles for CPF 3*

IEC 61918:2013, *Industrial communication networks – Installation of communication networks in industrial premises*

³ To be published.

IEC 62061, *Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems*

IEC 62280:2014, *Railway applications – Communication, signalling and processing systems – Safety-related communication in transmission systems*

IEC TR 62390, *Common automation device – Profile guideline*

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

ISO 13849-2, *Safety of machinery – Safety-related parts of control systems – Part 2: Validation*

3 Terms, definitions, symbols, abbreviated terms and conventions

3.1 Terms and definitions

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

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

3.1.1 Common terms and definitions

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

3.1.1.1

active network element

network element containing electrically and/or optically active components that allows extension of the network

Note 1 to entry: Examples of active network elements are repeaters and switches.

[SOURCE: IEC 61918:2013, 3.1.2]

3.1.1.2

availability

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

3.1.1.3

bit error probability

P_e

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

3.1.1.4

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.

3.1.1.5

communication channel

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

3.1.1.6**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

3.1.1.7**connection**

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

3.1.1.8**Cyclic Redundancy Check****CRC**

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

<method> procedure used to calculate the redundant data

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

Note 2 to entry: See also [33], [34]⁴.

3.1.1.9**defined communication system**

defined channel

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

3.1.1.10**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]

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

⁴ Figures in square brackets refer to the bibliography.

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

frame

denigrated synonym for DLPDU

3.1.1.16

Frame Check Sequence

FCS

redundant data derived from a block of data within a DLPDU (frame), using a hash function, and stored or transmitted together with the block of data, in order to detect data corruption

Note 1 to entry: An FCS can be derived using for example a CRC or other hash function.

Note 2 to entry: See also [33], [34].

3.1.1.17

hash function

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

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

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

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

3.1.1.18

hazard

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

3.1.1.19

master

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

3.1.1.20

message

ordered series of octets intended to convey information

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

3.1.1.21

nuisance trip

spurious trip with no harmful effect

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

3.1.1.22

proof test

periodic test performed to detect dangerous hidden failures in a *safety-related system* so that, if necessary, a repair can restore the system to an “as new” condition or as close as practical to this condition

Note 1 to entry: A proof test is intended to confirm that the safety-related system is in a condition that assures the specified safety integrity.

[SOURCE: IEC 61508-4:2010, 3.8.5, modified – replacement of the four notes with another one]

3.1.1.23

performance level

PL

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

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

3.1.1.24

protective extra-low-voltage

PELV

electrical circuit in which the voltage cannot exceed a.c. 30 V r.m.s., 42,4 V peak or d.c. 60 V in normal and single-fault condition, except earth faults in other circuits

Note 1 to entry: A PELV circuit is similar to an SELV circuit that is connected to protective earth.

[SOURCE: IEC 61131-2:2007, 3.54]

3.1.1.25

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]

3.1.1.26

reliability

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

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

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

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

Note 4 to entry: Reliability differs from availability.

[SOURCE: IEC 62059-11:2002, 3.17, modified – use automated system, two notes added]

3.1.1.27

residual error probability

RP

probability of an error undetected by the SCL safety measures

3.1.1.28

residual error rate

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

3.1.1.29

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], [SOURCE: ISO/IEC Guide 51:2014, definition 3.9, modified – different note]

3.1.1.30

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.

3.1.1.31

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

3.1.1.32

safety connection

connection that utilizes the safety protocol for communications transactions

3.1.1.33

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.

3.1.1.34

safety device

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

3.1.1.35

safety extra-low-voltage

SELV

electrical circuit in which the voltage cannot exceed a.c. 30 V r.m.s., 42,4 V peak or d.c. 60 V in normal and single-fault condition, including earth faults in other circuits

Note 1 to entry: An SELV circuit is not connected to protective earth.

[SOURCE: IEC 61131-2:2007, 3.59]

3.1.1.36

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]

3.1.1.37**safety function response time**

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

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

3.1.1.38**safety integrity level**

SIL

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

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

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

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

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

3.1.1.39**safety measure**

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

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

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

3.1.1.40**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.

3.1.1.41**safety-related application**

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

3.1.1.42**safety-related system**

system performing *safety functions* according to IEC 61508

3.1.1.43**slave**

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

3.1.1.44

spurious trip

trip caused by the safety system without a process demand

3.1.1.45

uniform distribution

probability distribution where all values from a finite set are equally likely to occur

Note 1 to entry: For a field of bit length i the probability of occurrence of a particular field value is 2^{-i} since the sum of all probabilities of occurrence is equal to 1.

3.1.2 CPF 3: Additional terms and definitions

3.1.2.1

bit

binary digit

encoded binary information without a technical unit

3.1.2.2

Codename

unique identification between safety communication peers

Note 1 to entry: Instance of *connection authentication* as described in IEC 61784-3.

3.1.2.3

configuration

definition of the standard communication connections and communication parameters for bus entities of a particular application

Note 1 to entry: The configuration for safety communication comprises the definition of the safety connections and F-Parameters for safety-related bus entities of a particular safety-related application.

3.1.2.4

CPD-Tool

dedicated program in service computers connected to the fieldbus for the purpose of configuration, parameterization and diagnosis of particular field devices

3.1.2.5

cycle

interval at which a list of instructions or an activity is repetitively and continuously executed

3.1.2.6

device access point

DAP

item used to address a modular IO device as an entity

Note 1 to entry: Usually this is called a head station.

Note 2 to entry: This note applies to the French language only.

3.1.2.7

device acknowledgment time

DAT

elapsed time in an F-Device starting with the reception of a safety PDU with a new *MonitoringNumber* in the device access point until an appropriate response safety PDU has been generated and returned to the device access point

Note 1 to entry: This note applies to the French language only.

3.1.2.8**driver**

software module used for abstracting the hardware with respect to the remaining application software

3.1.2.9**fail-safe**

F

ability of a system that, by adequate technical or organizational measures, prevents from hazards either deterministically or by reducing the risk to a tolerable measure

Note 1 to entry: Equivalent to functional safety

3.1.2.10**fail-safe values**

FV

values which are issued instead of process values when the safety function is set to a fail-safe state

Note 1 to entry: In this part, the fail-safe values (FV) shall always be set to "0".

Note 2 to entry: This note applies to the French language only.

3.1.2.11**fail-safe state**

operational mode of a safety function or final element (actuator) that by adequate technical measures prevents from hazards either deterministically or by reducing the risk to a tolerable measure

Note 1 to entry: Depending on a particular safety function, de-energizing may not be the only possibility for a fail-safe state.

3.1.2.12**F-Device**

passive CP 3/RTE communication peer that is able to perform the FSCP 3/1 protocol, usually triggered by the F-Host for data exchange

3.1.2.13**F-Driver**

software administering safety PDUs within F-Hosts and F-Devices according to the FSCP 3/1 specifications

3.1.2.14**F-Host**

data processing unit that is able to perform the FSCP 3/1 protocol and to service the black channel

Note 1 to entry: This is usually a PLC or an IPC with an adequate operating system.

3.1.2.15**F-Module**

passive communication peer within a modular F-Device or F-Slave that is able to perform the FSCP 3/1 protocol, usually triggered by the F-Host for data exchange

Note 1 to entry: This is usually a safety-related input or output module.

3.1.2.16**F-Slave**

passive CP 3/1 or CP 3/2 communication peer that is able to perform the FSCP 3/1 protocol, usually triggered by the F-Host for data exchange

3.1.2.17 fault reaction

indication of a communication malfunction by setting the fault bits in the Status Byte and a corresponding automatic safe reaction within the components

Note 1 to entry:

Within F-Output:	Shutting down the outputs, and/or automatic safe reaction of the actuator unit.
Within F-CPU:	Corresponding user program reaction possible. F-IO data to be set to fail-safe values.
Within F-Input:	On communication faults detected from F-Input: Fault bits set in the Status Byte. On communication faults detected from F-Host: F-Input data to be set to fail-safe values.

3.1.2.18 function block FB

self-contained program part possessing a specific functionality

Note 1 to entry: This note applies to the French language only.

3.1.2.19 host acknowledgment time HAT

elapsed time in an F-Host starting with the reception of a safety PDU with a certain *MonitoringNumber* until an appropriate safety PDU with a changed *MonitoringNumber* has been generated and returned to the master/IO-Controller

Note 1 to entry: This note applies to the French language only.

3.1.2.20 IO-Controller

active communication entity able to initiate and schedule CP 3/RTE communication activities by other entities which may be IO-Controllers or IO-Devices

Note 1 to entry: Within CP 3/1 this task is corresponding to a master class 1.

Note 2 to entry: The IO-Controller interface is called FSPMCTL according to IEC 61158-5-10.

3.1.2.21 IO-Device

passive communication entity able to receive messages and send them in response to another CP 3/RTE communication entity which may be an IO-Controller or other IO-Devices

Note 1 to entry: Within CP 3/1 this task is corresponding to a slave.

Note 2 to entry: The IO-Device interface is called FSPMDEV according to IEC 61158-5-10.

3.1.2.22 IO-Module

addressable sub input/output unit within a modular IO-Device

3.1.2.23 IO-Supervisor

engineering station enabled to read and write data from and to an IO-Device

Note 1 to entry: It is used for commissioning or diagnostics purposes. In contrast to an IO-Controller it does not take over an active role during the run-up of an IO-System. An IO-Supervisor is not part of the IO-System.

3.1.2.24 IO-System

IO-Controller and its associated IO-Devices

3.1.2.25**iParameter**

individual or technology specific F-Device parameters

Note 1 to entry: Typical iParameters are the protection zone coordinates of a laser scanner.

3.1.2.26**iPar-Server**

standardised mechanism to store and retrieve individual or technology specific F-Device parameters within the standard part of an F-Host or its controlled subsystem

3.1.2.27**master**

active CP 3/1 communication peer triggering slaves for data exchange

Note 1 to entry: The term "master" alone is used as a short form for "master class 1".

3.1.2.28**MonitoringNumber**

MNR

means to ensure authenticity and the correct order of transmitted safety PDUs

Note 1 to entry: Instance of *sequence number* as described in IEC 61784-3.

Note 2 to entry: The MonitoringNumber is only secured via the transmitted CRC signature.

Note 3 to entry: This note applies to the French language only.

3.1.2.29**process values**

PV

input and output data (in a safety PDU) that are required to control an automated process

Note 1 to entry: This note applies to the French language only.

3.1.2.30**qualifier**

additional qualifying bits within *process values* indicating the status of each individual input

3.1.2.31**shared IO**

inputs and outputs in field devices that can be accessed by several controllers

Note 1 to entry: Even though CP 3/RTE is permitting shared IO, it is not permitted with FSCP 3/1.

3.1.2.32**toggle bit**

one bit of the Control and Status Byte to synchronize the (virtual) *MonitoringNumber* in both the F-Host and the F-Device

3.1.2.33**universal serial bus**

USB

external bus standard

Note 1 to entry: USB is replacing serial and parallel computer ports and is used for fast direct connections between service computers and field devices.

Note 2 to entry: This note applies to the French language only.

3.1.2.34

V2-mode

FSCP 3/1 services and protocol according to this part

3.1.2.35

VLAN tag

extension within Ethernet messages that enables particular user groups on large networks to run their own virtual network via priorities and VLAN-IDs, using appropriate switches, without impacting other user groups and vice versa

3.2 Symbols and abbreviated terms

3.2.1 Common symbols and abbreviated terms

BSC	Binary Symmetric Channel	
CP	Communication Profile	[IEC 61784-1/2]
CPF	Communication Profile Family	[IEC 61784-1/2]
CRC	Cyclic Redundancy Check	
DLL	Data Link Layer	[ISO/IEC 7498-1]
DLPDU	Data Link Protocol Data Unit	
EMC	Electromagnetic Compatibility	
EMI	Electromagnetic Interference	
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]
FCS	Frame Check Sequence	
FIT	Failure In Time (equals 10^{-9} failure per hour)	
FS	Functional Safety	
FSCP	Functional Safety Communication Profile	
HD	Hamming Distance	
IACS	Industrial Automation and Control System	
MTBF	Mean Time Between Failures	
MTTF	Mean Time To Failure	
NSR	Non Safety Related	
PDU	Protocol Data Unit	[ISO/IEC 7498-1]
Pe	Bit error probability	
PELV	Protective Extra Low Voltage	
PFD	Probability of dangerous Failure on Demand	[IEC 61508-4:2010]
PFH	Average frequency of dangerous failure [h^{-1}] per hour	[IEC 61508-4:2010]
PhL	Physical Layer	[ISO/IEC 7498-1]
PL	Performance Level	[ISO 13849-1]
PLC	Programmable Logic Controller	
RP	Residual Error Probability	
SCL	Safety Communication Layer	
SELV	Safety Extra Low Voltage	
SFRT	Safety Function Response Time	
SIL	Safety Integrity Level	[IEC 61508-4:2010]
SIS	Safety Instrumented Systems	
SL	Security Level	[IEC 62443]
SMS	Security Management System	[IEC 62443]



SPDU	Safety PDU
SR	Safety Related

3.2.2 CPF 3: Additional symbols and abbreviated terms

AES-CCMP	Advanced Encryption Standard – Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
AP	Application Process
API	Application Process Identifier
AR	Application Relationship
ASE	Application Service Element
ASIC	Application Specific Integrated Circuit
C	Coverage
CGP	Channel-granular Passivation
CiR	Configure in Run
CP 3/1	Communication profile commonly known as PROFIBUS DP ⁵
CP 3/2	Communication profile commonly known as PROFIBUS PA
CP 3/RTE	Communication profile commonly known as PROFINET IO
CPU	Central Processing Unit
CR	Communication Relationship
CRC_FP	16 bit CRC2 seed value of the F-Host (across F-Parameter = F_Par_CRC)
CRC_FP+	32 bit CRC value across F-Parameter
DAP	Device Access Point
DAT	Device Acknowledgment Time
DP	Decentralized Peripherals
F	Identifier for safety items (fail-safe, functional safe)
FB	Function Block
FV	Fail-safe Values
GSD	General Station Description (file associated with device)
GSDL	General Station Description Language (for CP 3/1 and CP 3/2 devices)
GSDML	General Station Description Markup Language (for CP 3/RTE devices)
HAT	Host Acknowledgment Time
IO	Input/Output
LED	Light Emitting Diode
MNR	MonitoringNumber
PA	Process Automation
PN IO	PROFINET IO = CP 3/4 to 3/6
PSK	Pre-shared Key
PV	Process Values
RADIUS	Remote Authentication Dial In User Service
S	<i>Standard</i>
SR	(Functional) Safety-Related
SSID	Service Set Identifier
UML	Unified Modeling Language

[52]

⁵ For trade name declarations, see Clause 4.

USB	Universal Serial Bus	[57]
VLAN	Virtual Local Area Network	
WCDT	Worst Case Delay Time	
WDTime	Watchdog Time	
WPA2	Wi-Fi Protected Access 2	[29]
XML	eXtensible Markup Language	[54], [55], [56]

3.3 Conventions

This part uses UML2 notation for the drawing of the state charts and a condensed form for sequence charts [52]. The transition tables are depicted following the recommendations of IEC 62390.

In this part the abbreviation "F" is an indication for safety related items, technologies, systems, and units (fail-safe, functional safe).

In this part, the default data that shall be sent in case of unit failures or errors, are called fail-safe values (FV) and are set to "0".

In this part, reserved bit ("res") within the Status/Control Byte and the F-Parameters shall be set to "0" and ignored by the receiver in order to avoid hassles with future versions of the FSCP 3/1 devices.

In this part, any CRC signature calculation resulting in a "0" value, will use the value "1" instead.

In this part the abbreviation "CP 3/RTE" comprises the three communication profiles CP 3/4, CP 3/5, and CP 3/6. CP 3/RTE is commonly known as PROFINET IO.

4 Overview of FSCP 3/1 (PROFIsafe™)

Communication Profile Family 3 (commonly known as PROFIBUS™, PROFINET™⁶) defines communication profiles based on IEC 61158-2 Type 3, IEC 61158-3-3, IEC 61158-4-3, IEC 61158-5-3, IEC 61158-5-10, IEC 61158-6-3, and IEC 61158-6-10.

The basic profiles CP 3/1 and CP 3/2 are defined in IEC 61784-1; CP 3/4, CP 3/5 and CP 3/6 are defined in IEC 61784-2. The CPF 3 functional safety communication profile FSCP 3/1 (PROFIsafe™⁶) is based on the CPF 3 basic profiles in IEC 61784-1 and IEC 61784-2 and the safety communication layer specifications defined in this part.

FSCP 3/1 is based on the cyclic data exchange of a (bus) controller with its associated (field) devices using a one-to-one communication relationship (Figure 3). One controller can operate any mix of standard and safety devices connected to the network. Assigning safety tasks and standard tasks to different controllers also is possible. Any so-called acyclic communications between devices and controllers or supervisors such as programming devices are intended for configuration, parameterization, diagnosis, and maintenance purposes.

For the realisation of FSCP 3/1, the following four measures have been chosen:

⁶ PROFIBUS™, PROFINET™ and PROFIsafe™ are trade names of the non-profit organization PROFIBUS Nutzerorganisation e.V. (PNO). This information is given for the convenience of users of this International Standard and does not constitute an endorsement by IEC of the trade name holder or any of its products. Compliance to this standard does not require use of the registered logos for PROFIBUS™, PROFINET™ or PROFIsafe™. Use of the registered logos for PROFIBUS™, PROFINET™ or PROFIsafe™ requires permission of PNO and compliance with conditions for their use (such as testing and validation).

- (virtual) MonitoringNumber (MNR);
- watchdog time monitoring with acknowledgment;
- Codename per communication relationship (Codename is the basis for the MNR. The direction is differentiated via the one's complement of the MNR);
- cyclic redundancy checking for data integrity.

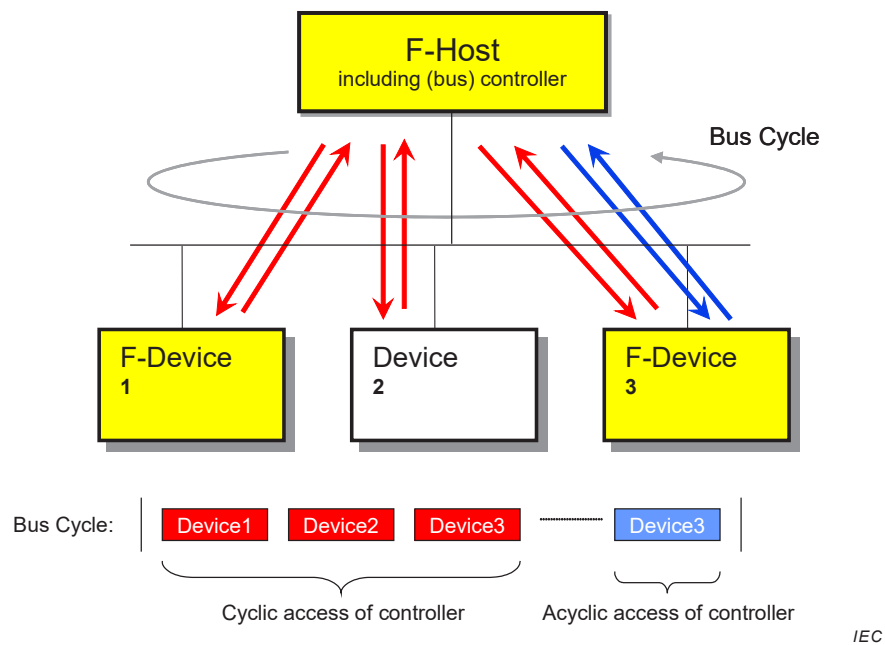


Figure 3 – Basic communication preconditions for FSCP 3/1

The MonitoringNumber uses a range that is large enough to secure any malfunction caused by message storing network elements. Every safety device returns a message with a safety PDU for acknowledgment even if there are no process data. A separate watchdog timer on both the sender and the receiver side is used for each one-to-one communication relationship. The unique Codename per communication relationship (and via additional measures the source-sink direction) is established for authentication reasons and is encoded within an initial CRC signature value for the cyclically calculated and transmitted CRC2 signature (Figure 4).

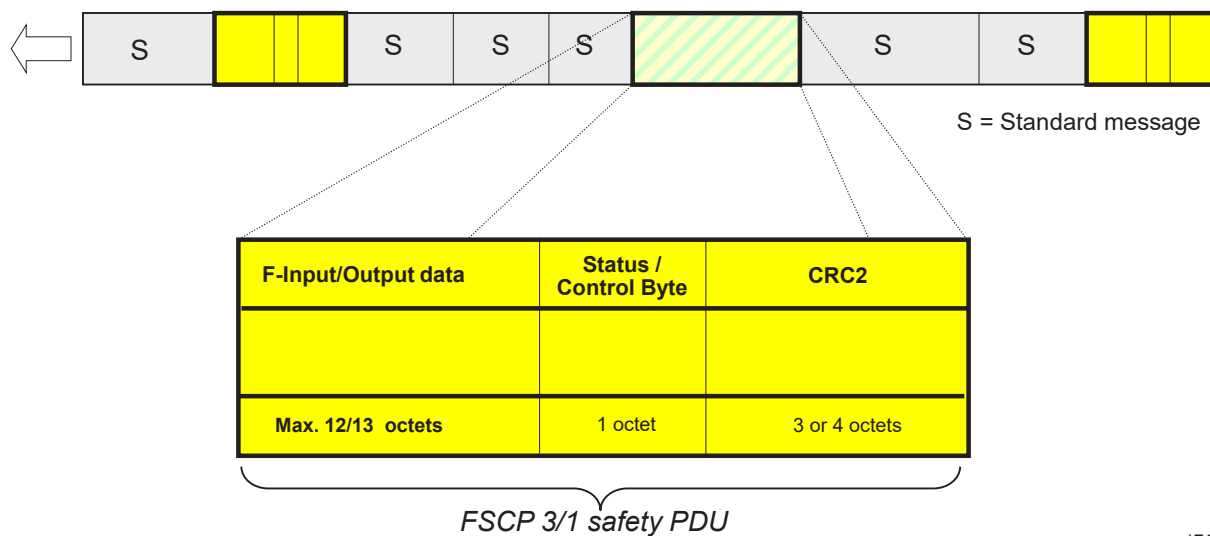


Figure 4 – Structure of an FSCP 3/1 safety PDU

FSCP 3/1 provides the so-called V2-mode. The V2-mode specified in this version covers recent developments within the Ethernet based CP 3/RTE such as programmable routing of messages and scientific findings on CRC properties.

Figure 5 provides an overview on FSCP 3/1 within the CP 3/1 and CP 3/RTE architectures.

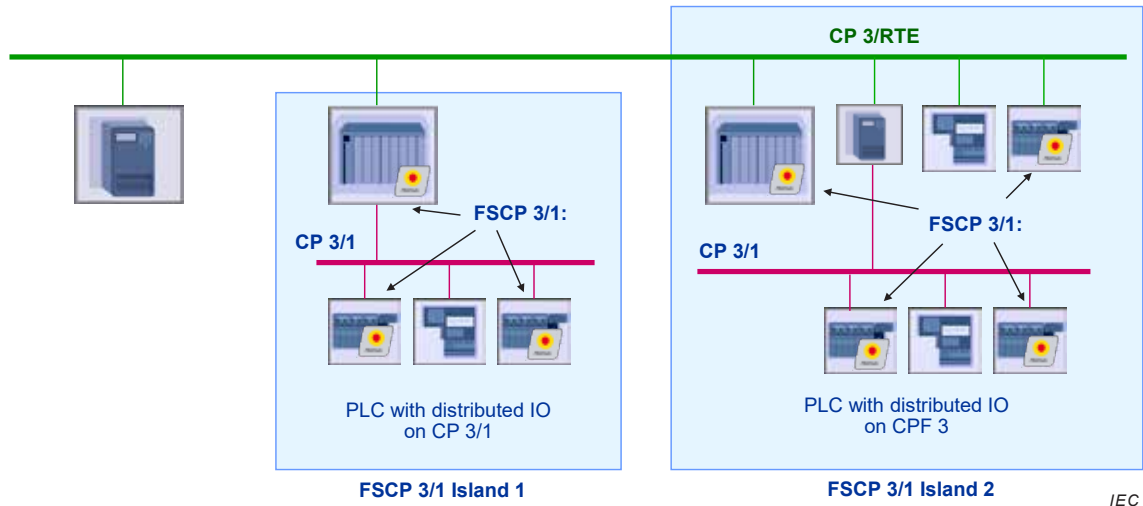


Figure 5 – Safety communication on CPF 3

While automation solutions with distributed IO gained widely acceptance through PROFIBUS (CP 3/1 and CP 3/2) and the industrial Ethernet based PROFINET (CP 3/RTE), safety applications were still relying on a second layer of conventional electrical techniques or special busses thus limiting the seamless engineering and interoperability. Additionally, modern safety devices such as laser scanners or drives with integrated safety could not be fostered as needed due to missing system support. It is the purpose of this part and related documents to provide the corresponding enabling technologies.

After this introduction, subclause 5.1 holds additional references for the development of the FSCP 3/1 technology and 5.2 holds its functional requirements. The four safety measures of FSCP 3/1 are listed in 5.3. The network topologies within CP 3/RTE and their crossovers to CP 3/1 and CP 3/2 are mentioned in 5.4. A brief introduction into the communication relationships and objects of the fieldbus standard is following in 5.5.

For safety and efficiency reasons the list of possible fieldbus data types is reduced to a concise set and described in 5.5.3. Subclauses 6.1 to 6.3 are unveiling the F-Host and F-Device services as well as the possible diagnosis messages of the safety layer.

Clause 7 starts with an overview on the safety PDU (7.1), continues with a description of the state machines in F-Host and F-Device and sequence diagrams in the Unified Modeling Language 2 format (7.2.2 to 7.2.4). Associated timing constraints are contained in 7.2.5 and 7.2.6. Following the format in IEC 61784-3:— Annex D, subclause 7.3 illustrates the system reactions in the event of the possible malfunctions. Other system functions such as start-up of the safety layer are contained in 7.4. The layer management of safety devices focuses on safety communication specific F-Parameters (8.1) and on device specific individual iParameters (8.2). The requirements for handling and supply of the F-Parameters are described in 8.3. Subclause 8.4 deals with securing the data structures that are to be exchanged between the communicating partners and that represent the configuration of a device. Subclause 8.5 shows how the data structure information can be used to configure F-Channel drivers for more complex F-Devices to save programming effort. The requirements for the system integration of iParameterization means and tools are listed in 8.6. The aspects of response times, installation guidelines, and duration of demands, maintenance, safety manual, wireless transmission, and F-Host conformance classes are covered 9. The reasoning for assessment is pointed out in 10.1 and the details in 10.2. An informative annex

contains examples for fast CRC signature calculations and a bibliography. Two additional FSCP 3/1 guidelines for electrical safety and assessment shall be observed ([41], [70]).

5 General

5.1 External documents providing specifications for the profile

In addition to the normative references in Clause 2, the technology in this part meets the requirements of NE97 [53].

5.2 Safety functional requirements

The following requirements apply for the development of the FSCP 3/1 technology.

- a) Safety communication and standard communication shall be independent. However, standard devices and safety devices shall be able to use the same communication channel.
- b) Safety communication shall be suitable for Safety Integrity Level SIL3 (see IEC 61508) and PL e (see ISO 13849-1).
- c) Safety communication shall use a single-channel communication system. Redundancy may only be used optionally for increased availability.
- d) Implementation of the safety transmission protocol shall be restricted to the communication end devices (F-Host or F-CPU – F-Device and /or F- Module).
- e) There shall always be a 1:1 communication relationship between an F-Device and its F-Host.
- f) The transmission duration times shall be monitored.
- g) Environmental conditions shall be according to general automation requirements, mainly IEC 61326-3-1 or IEC 61326-3-2, if there are no particular product standards.
- h) Transmission equipment such as controllers, ASICs, links, couplers, etc. shall remain unmodified (black channel). The safety functions shall be above OSI layer 7 (i.e. profile, no standard protocol changes or enhancements)
- i) The safety communication shall not reduce the permitted number of devices. Restrictions may occur during mapping in case of CP 3/2 applications due to message limitations (see CP 3/2 in IEC 61784-1).
- j) Safety communication shall be suitable for NE97 [53] and meet the requirements of IEC 61784-3:— Annex D.

5.3 Safety measures

The safety measures mentioned in Table 1 for mastering possible transmission errors are one significant component of the FSCP 3/1 profile. The selection in Table 1 of the generic safety measures listed in IEC 61784-3:—, 5.5 is required for FSCP 3/1.

The safety measures shall be processed and monitored within one safety unit.

Table 1 – Deployed measures to master errors

Communication error	Safety measures			
	(virtual) MonitoringNumber ^a	Timeout with receipt ^b	Codename for sender and receiver ^c	Data integrity check ^d
Corruption	–	–	–	X
Unintended repetition	–	X	–	–
Incorrect sequence	X	–	–	–
Loss	X	X	–	–
Unacceptable delay	–	X	–	–
Insertion	X	–	–	–
Masquerade	–	–	–	X
Addressing	X	–	X	–
Out-of-sequence	X	–	–	–
Loop-back of messages	X ^e	–	–	–

^a Instance of "sequence number" of IEC 61784-3.
^b Instance of "time expectation" (Timeout) and "feedback message" (Receipt) of IEC 61784-3.
^c Instance of "connection authentication" of IEC 61784-3.
^d Instance of "data integrity assurance" of IEC 61784-3.
^e In mode F_CRC_seed =0 via status bit 7, in mode F_CRC_seed =1 via one's complement of MNR

5.4 Safety communication layer structure

5.4.1 Principle of FSCP 3/1 safety communications

FSCP 3/1's way of safety communication is based on the experience made in the railway signaling technique as it has been laid down in earlier versions of IEC 62280.

On this basis, safety communication is performed by

- a standard transmission system (Figure 6), and
- an additional safety transmission protocol on top of this standard transmission system.

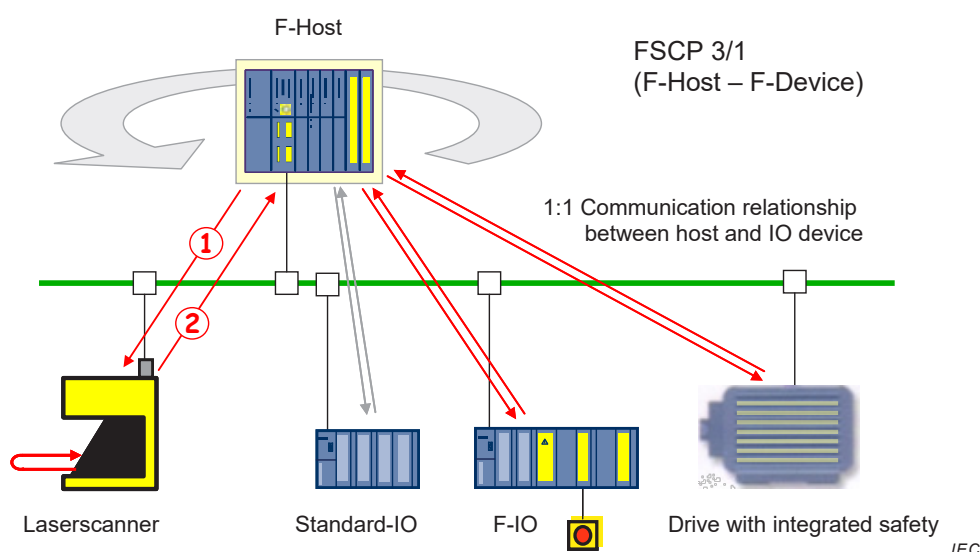


Figure 6 – Standard CPF 3 transmission system

The standard transmission system includes the entire hardware of the transmission system and the related protocol functions (i.e. OSI layers 1, 2 and 7 according to Figure 7).

Safety applications and standard applications are sharing the same standard CPF 3 communication systems at the same time. The safe transmission function comprises all measures to deterministically discover all possible faults / hazards that could be infiltrated by the standard transmission system or to keep the residual error (fault) probability under a certain limit. This includes

- Random malfunctions, for example due to electromagnetic interference on the transmission channel;
- Failures / faults of the standard hardware;
- Systematic malfunctions of components within the standard hardware and software.

This principle delimits the assessment effort to the "safe transmission functions". The "standard transmission system" (black channel) does not need any additional safety assessment.

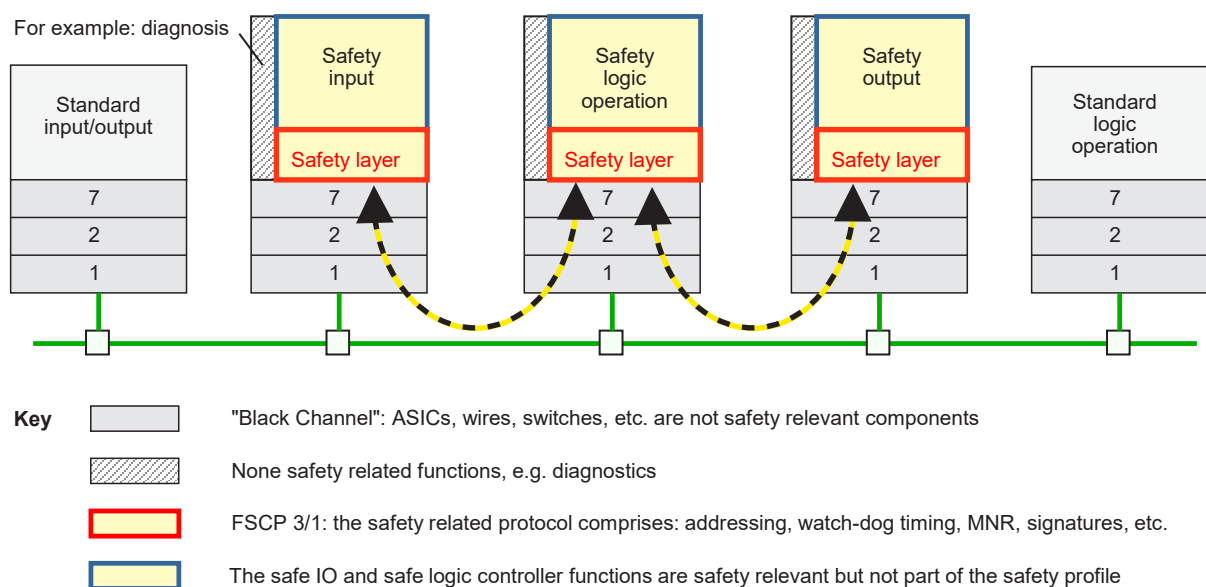


Figure 7 – Safety layer architecture

Transmission is performed via electrical or optical conductors. Permissible topologies and transmission features of the standard transmission system and the components of the "black channel" are described in 5.4.2.

5.4.2 CPF 3 communication structures

The basic communication layers of CP 3/RTE are shown in Figure 8. While the cyclic safety communication of FSCP 3/1 is using the realtime channels RT or IRT (CP 3/RTE of IEC 61784-2) the other services are using the so-called open channel via TCP/IP or UDP.

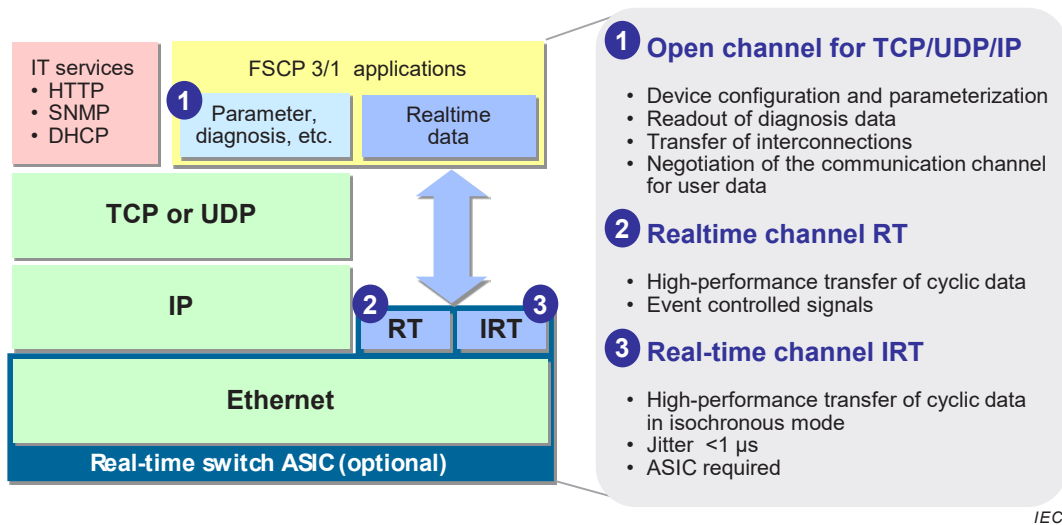


Figure 8 – Basic communication layers

Figure 9 shows the typical (star) topology of one possible CP 3/RTE wiring with multiport switches. One failing device will not shut down the whole network. However, the wiring effort may be unfavorable.

CP 3/RTE provides an alternative via Switch-ASIC that each device may integrate in its communication interface. This way a line topology much like CP 3/1 is possible.

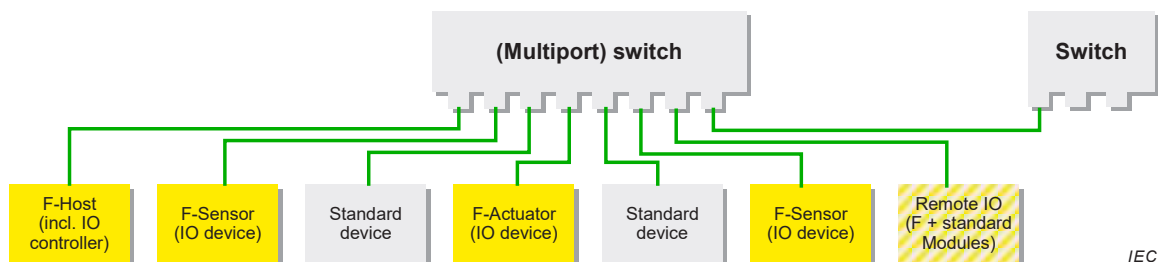


Figure 9 – Multiport switch bus structure

In order to avoid a system shut down in case of a failing device a ring structure (see Figure 10) is highly recommended. However, in this case some restrictions exist:

- At least one participant within the ring (in Figure 10 the F-Host) shall have a redundancy management to detect any interruption and to reorganize the transmission to the destinations.
- The changeover time of the switch management in such a case shall not exceed the minimum watchdog time of any F-Device within the same island.

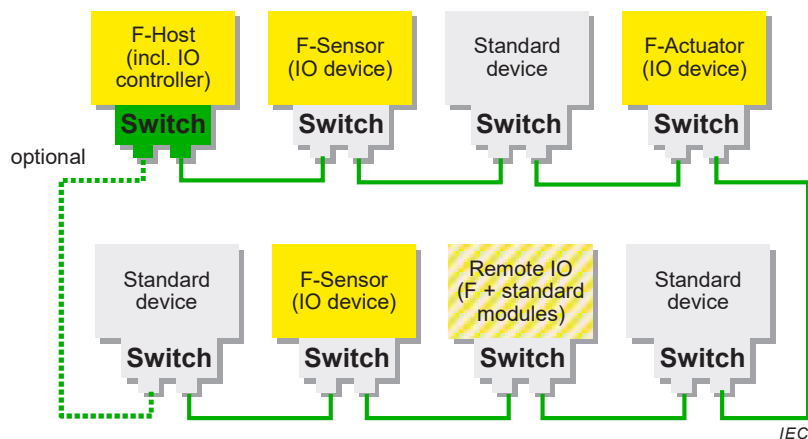


Figure 10 – Linear bus structure

The networks in Figure 9 and Figure 10 belong each to one CP 3/RTE system with one particular IP-Address as the Real-Time protocol (RT or IRT) in layer 2 cannot pass beyond this IP-Address space (see Figure 8). It is the (OSI layer 3) task of routers to redirect messages on an IP-Address level (see Figure 11). Thus routers are natural borders for CP 3/RTE systems where RT_CLASS_UDP is not permitted or not supported.

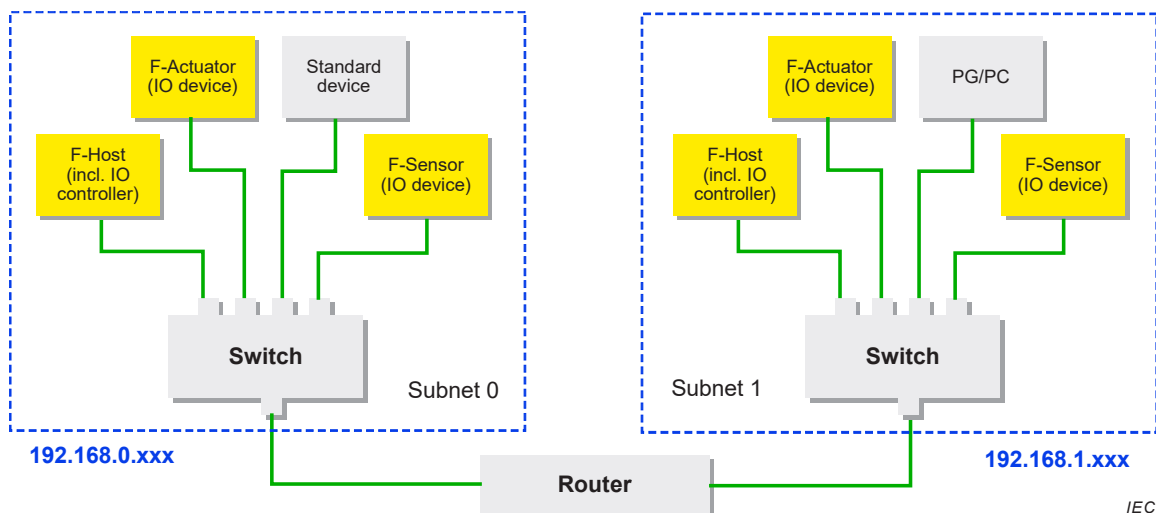


Figure 11 – Crossing network borders with routers

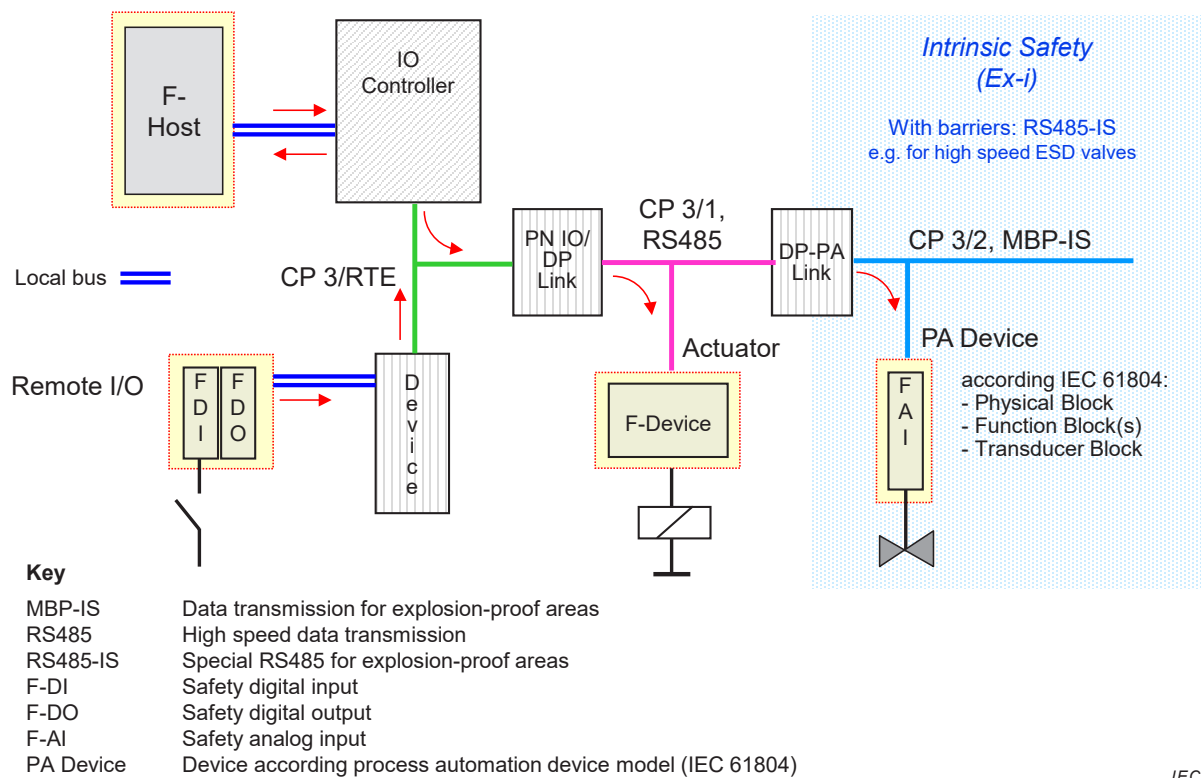
The following restrictions apply for FSCP 3/1.

- Wireless LAN permitted. However, uniqueness of Codenames ("F_S/D_Addresses") shall be guaranteed within islands.
- Single port routers are not permitted (7.3.11).

If Real-Time protocols are crossing routers, the Codenames within the entire network shall be unambiguous and the Codename checks shall identify unambiguous relationships and via additional measures both transmission directions.

In contrast to the fieldbus system configuration, Figure 12 shows the possible network structure, i.e. how far the safety profile extents into the individual units. A standard remote IO, for example, can comprise an F-Module for the connection of an emergency stop pushbutton. Thus the whole FSCP 3/1 transmission path reaches from the F-Host across its backplane bus via CP 3/RTE into the IO-Device and across a possible other backplane into the final F-Module. The safety layer is implemented within these far ends of communication.

Multi-controller or multi-master operation of F-Hosts is permitted. "Shared F-Inputs" are not permitted. A mix of F-Host and standard host is possible.



IEC

Figure 12 – Complete safety transmission paths

5.5 Relationships with FAL (and DLL, PhL)

5.5.1 Device model

The CP 3/RTE as well as the CP 3/1 device model is assuming one or several application processes (AP) within the device. Figure 13 shows the internal structure of an application process for a modular field device. Optionally it could have several of these APs. The application process is subdivided into as many slots and subslots as needed to represent the physical IOs of the device. In contrast to CP 3/1, CP 3/RTE provides one hierarchical level more: the subslots.

Within the subslots, application service elements (ASE) provide a set of standardized services for conveying requests and responses to and from application processes and their data objects such as IO data, Context (Parameterization), Diagnosis, Alarms, and Record Data.

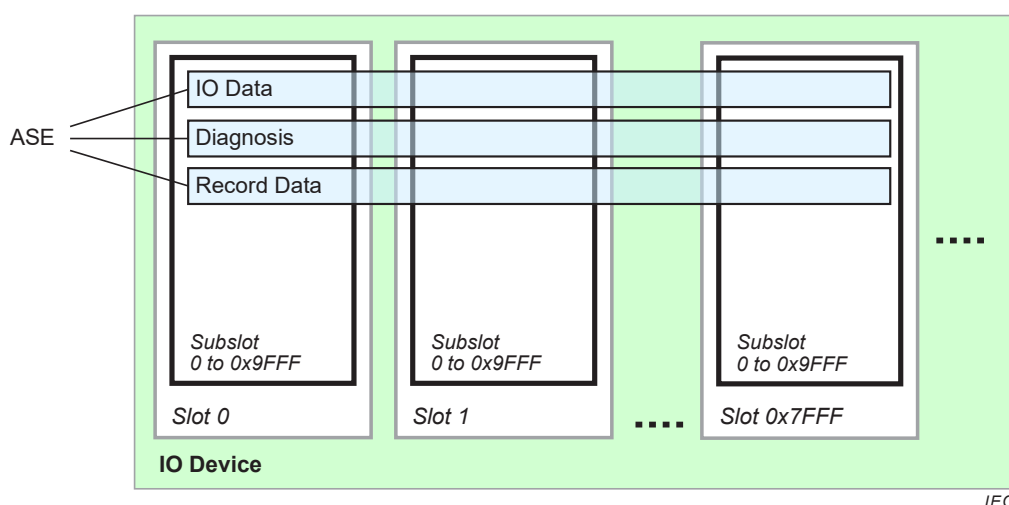


Figure 13 – IO Device model

The device manufacturer is responsible for the specification (GSD) of F-Modules that can be plugged into Slots or Subslots.

5.5.2 Application and communication relationships

CP 3/RTE in general permits shared input. Since FSCP3/1 is based on 1:1 communication relationships, shared input cannot be used for functional safety.

5.5.3 Data types

CPF 3 uses the basic data types listed in IEC 61158-5-10. Table 2 shows a restricted number of data types for FSCP 3/1.

Table 2 – Data types for FSCP 3/1

Data type name	Number of octets
Integer16	2
Integer32	4
Unsigned8 (used as bits)	1
Unsigned16 (used as bits) ^a	2
Unsigned32 (used as bits) ^a	4
Float32	4
Unsigned8+Unsigned8	2
Float32+Unsigned8 (enumerated)	5
F_MessageTrailer4Byte	4
F_MessageTrailer5Byte	5
^a It is highly recommended to use multiple Unsigned8 instead.	

Single bits shall be coded within Unsigned8 data type due to its higher efficiency in comparison to the data type Boolean.

See [62] for general information on data types and 8.4.1 for functional safety coding.

6 Safety communication layer services

6.1 F-Host services

Figure 14 shows that each F-Input and each F-Output requires a safety PDU management (F driver) in order to handle the FSCP 3/1 protocol. The corresponding F-Host operates with an instance of an F driver for each F-Input or F-Output respectively. Thus each and every 1:1 relationship between an instance of the F driver and the corresponding partner within an F-Device is identified by a unique *Codename* (one of the F-Parameters).

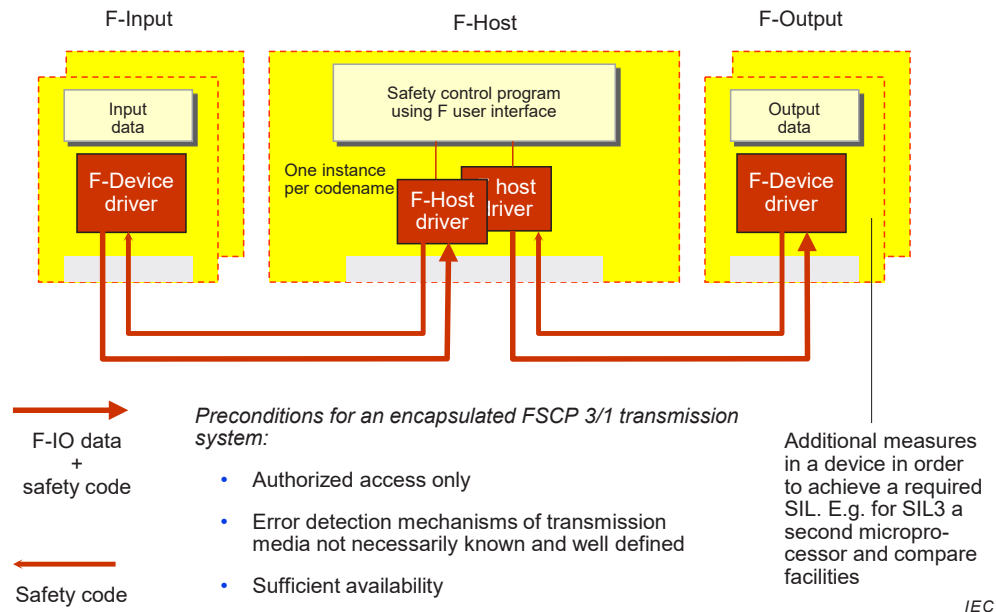


Figure 14 – FSCP 3/1 communication structure

The entire standard CPF 3 communication equipment between F-Drivers belongs to the black channel. The arrows in Figure 14 are indicating the cyclic data transport between the F drivers: the safety addenda (Status or Control Byte and CRC2) are transferred in addition to the F-Input data from the F-Input to the F-Host.

As an acknowledgment, the F-Input merely receives the safety addenda (safety code). Accordingly, the F-Output receives the safety addenda in addition to the F-Output data, and uses it for acknowledgment.

NOTE It is possible for F-Devices/F-Modules to provide F-Input and F-Output data.

Safety PDU management and F-Parameterization are tasks of the F drivers within the F-Host and the F-Devices. They provide also the measures to support the additional system features "Configure in Run" (CiR) according to [64] and "Channel-granular Passivation" based on [66].

The F user interface at the safety control program level is shown in Figure 15.

"Configure in Run" (CiR) or "Maintenance of Fault Tolerant Systems" according to [64] are planned activities that shall be monitored by authorized personnel only. CiR shall only be activated and de-activated by an operator. It shall not be set/reset via the "F User Program".

The design of corresponding safety-related parts of the F-Host shall exclude any unintended activation of CiR as well as guarantee the deactivation of CiR after terminating the reconfiguration.

The F-Host shall set and reset "use_TO2" (CiR) for all the F-Devices thus affecting all F-Devices simultaneously.

The F-Host shall extend the regular (primary) watchdog time (F_WD_Time) by a secondary watchdog time (F_WD_Time_2) once only (see Figure 20, Figure 28, Figure 29, 7.2.6.2, 8.1.1, 8.1.4).

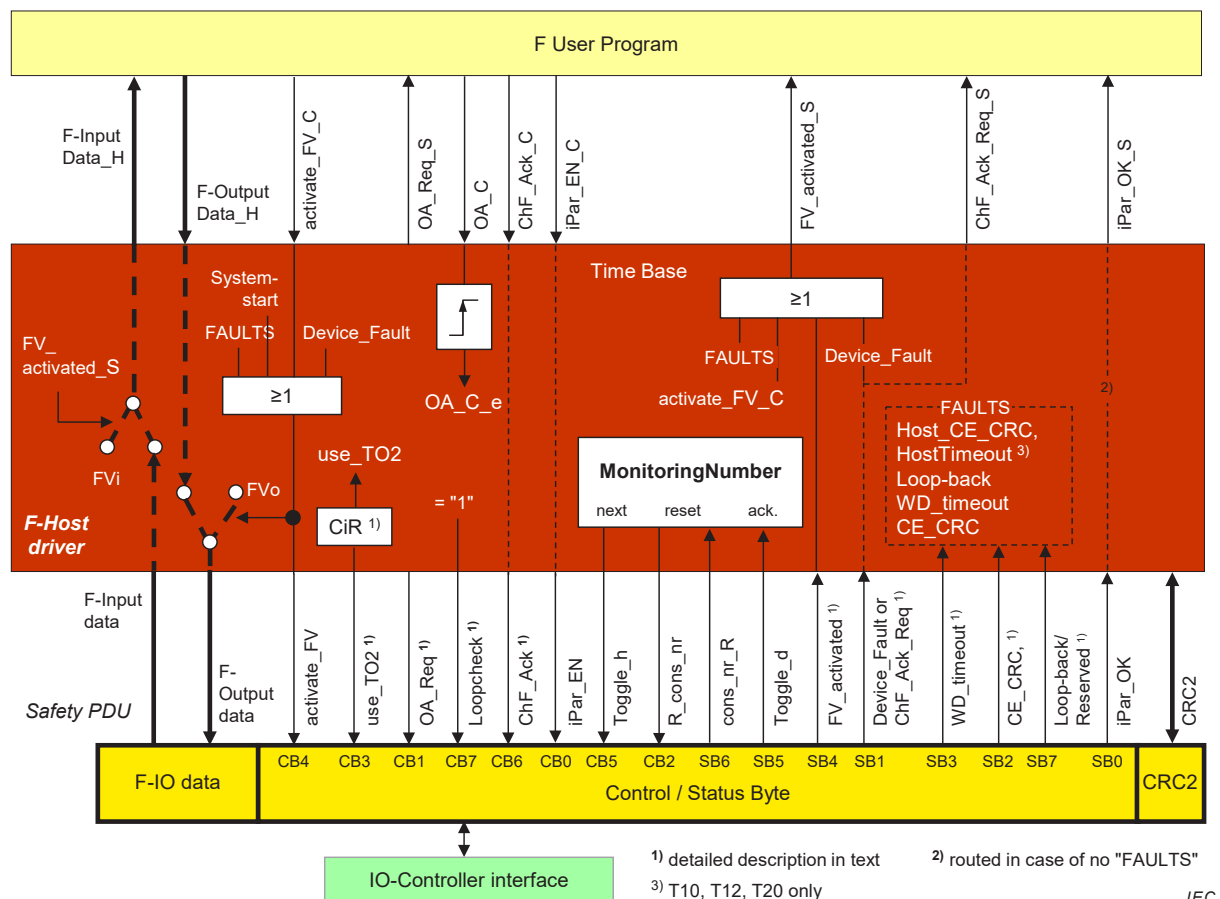


Figure 15 – F user interface of F-Host driver instances

The need for "Channel-granular Passivation" can be seen in 5.4.2 and Figure 12. The FSCP 3/1 transmission path reaches for example an F-Module of a Remote IO. Usually, the F-Module provides several signal channels each for a safety sensor as shown in Figure 16. Each signal channel can be associated with an individual safety function. In case one channel fails, the F-Module will cause all associated safety functions to enter the fail-safe state. The option "Channel-granular Passivation" based on [66] allows for an individual fail-safe state only for that safety function, which is impacted by the failed signal channel.