

INTERNATIONAL STANDARD

NORME INTERNATIONALE



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

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



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2021 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'IEC ou du Comité national de l'IEC du pays du demandeur. Si vous avez des questions sur le copyright de l'IEC ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de l'IEC de votre pays de résidence.

IEC Central Office
3, rue de Varembe
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigendum or an amendment might have been published.

IEC publications search - webstore.iec.ch/advsearchform

The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee, ...). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

IEC Customer Service Centre - webstore.iec.ch/csc

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

IEC online collection - oc.iec.ch

Discover our powerful search engine and read freely all the publications previews. With a subscription you will always have access to up to date content tailored to your needs.

Electropedia - www.electropedia.org

The world's leading online dictionary on electrotechnology, containing more than 22 000 terminological entries in English and French, with equivalent terms in 18 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

A propos de l'IEC

La Commission Electrotechnique Internationale (IEC) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications IEC

Le contenu technique des publications IEC est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Recherche de publications IEC - webstore.iec.ch/advsearchform

La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études, ...). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

IEC Just Published - webstore.iec.ch/justpublished

Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et une fois par mois par email.

Service Clients - webstore.iec.ch/csc

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: sales@iec.ch.

IEC online collection - oc.iec.ch

Découvrez notre puissant moteur de recherche et consultez gratuitement tous les aperçus des publications. Avec un abonnement, vous aurez toujours accès à un contenu à jour adapté à vos besoins.

Electropedia - www.electropedia.org

Le premier dictionnaire d'électrotechnologie en ligne au monde, avec plus de 22 000 articles terminologiques en anglais et en français, ainsi que les termes équivalents dans 16 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

INTERNATIONAL STANDARD

NORME INTERNATIONALE



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

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

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 25.040.40; 35.100.05

ISBN 978-2-8322-9749-0

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

CONTENTS

FOREWORD	9
0 Introduction	11
0.1 General.....	11
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	27
3.2.1 Common symbols and abbreviated terms.....	27
3.2.2 CPF 3: Additional symbols and abbreviated terms	28
3.3 Conventions.....	29
4 Overview of FSCP 3/1 (PROFIsafe™).....	29
5 General	32
5.1 External documents providing specifications for the profile	32
5.2 Safety functional requirements.....	32
5.3 Safety measures	32
5.4 Safety communication layer structure.....	33
5.4.1 Principle of FSCP 3/1 safety communications	33
5.4.2 CPF 3 communication structures	35
5.5 Relationships with FAL (and DLL, PhL)	37
5.5.1 Device model.....	37
5.5.2 Application and communication relationships.....	38
5.5.3 Data types	38
6 Safety communication layer services	39
6.1 F-Host driver services	39
6.2 F-Device driver services	43
6.3 Diagnosis.....	45
6.3.1 Safety alarm generation.....	45
6.3.2 F-(Sub)Module safety layer diagnosis	45
7 Safety communication layer protocol	46
7.1 Safety PDU format	46
7.1.1 Safety PDU structure	46
7.1.2 Safety IO data	47
7.1.3 Status and Control Byte	47
7.1.4 (Virtual) MonitoringNumber	49
7.1.5 (Virtual) MNR mechanism (F_CRC_Seed=0)	50
7.1.6 (Virtual) MNR mechanism (F_CRC_Seed=1)	50
7.1.7 CRC2 Signature (F_CRC_Seed=0)	52
7.1.8 CRC2 Signature (F_CRC_Seed=1)	53
7.1.9 Non-safety IO data	54
7.2 FSCP 3/1 behavior.....	54
7.2.1 General	54

7.2.2	F-Host driver state diagram	55
7.2.3	F-Device driver state diagram	58
7.2.4	F-Device driver restart	62
7.2.5	Sequence diagrams	62
7.2.6	Timing diagram for a MonitoringNumber reset	69
7.2.7	Monitoring of safety times	69
7.3	Reaction in the event of a malfunction	72
7.3.1	Corruption of safety data	72
7.3.2	Unintended repetition	72
7.3.3	Incorrect sequence	73
7.3.4	Loss	73
7.3.5	Unacceptable delay	73
7.3.6	Insertion	73
7.3.7	Masquerade	73
7.3.8	Addressing	73
7.3.9	Out-of-sequence	74
7.3.10	Loop-back	74
7.3.11	Network boundaries and router	74
7.4	F-Startup and parameter change at runtime	75
7.4.1	Standard startup procedure	75
8	Safety communication layer management	75
8.1	F-Parameter	75
8.1.1	Summary	75
8.1.2	F_Source/Destination_Address (Codename)	76
8.1.3	F_WD_Time (F-Watchdog time)	77
8.1.4	F_WD_Time_2 (secondary F-Watchdog time)	77
8.1.5	F_Prm_Flag1 (Parameters for the safety layer management)	77
8.1.6	F_Prm_Flag2 (Parameters for the safety layer management)	80
8.1.7	F_iPar_CRC (value of iPar_CRC across iParameters)	81
8.1.8	F_Par_CRC calculation (across F-Parameters)	81
8.1.9	Structure of the F-Parameter record data object	82
8.2	iParameter and iPar_CRC	82
8.3	Safety parameterization	83
8.3.1	Objectives	83
8.3.2	GSDL and GSDML safety extensions	84
8.3.3	Securing safety parameters and GSD data	86
8.4	Safety configuration	90
8.4.1	Order of IO data types	90
8.4.2	Securing the safety IO data description	90
8.4.3	DataItem data type section examples	91
8.5	Data type information usage	95
8.5.1	F-Host Channel driver	95
8.5.2	Rules for standard F-Host Channel drivers	96
8.5.3	Recommendations for the use of F-Host Channel drivers	97
8.6	Safety parameter assignment mechanisms	98
8.6.1	F-Parameter assignment	98
8.6.2	General iParameter assignment	98
8.6.3	System integration requirements for iParameterization tools	98
8.6.4	iPar-Server	100

9	System requirements	111
9.1	Indicators and switches	111
9.2	Installation guidelines	111
9.3	Safety function response time	111
9.3.1	Model	111
9.3.2	Calculation and optimization	113
9.3.3	Adjustment of watchdog times for FSCP 3/1	115
9.3.4	Engineering tool support	116
9.3.5	Retries (repetition of messages)	116
9.4	Duration of demands	117
9.5	Constraints for the calculation of system characteristics	117
9.5.1	Probabilistic considerations	117
9.5.2	Safety related assumptions	119
9.5.3	Non safety related constraints (availability)	120
9.6	Maintenance	120
9.6.1	F-(Sub)Module commissioning / replacement	120
9.6.2	Identification and maintenance functions	120
9.7	Safety manual	121
9.8	Wireless transmission channels	122
9.8.1	Black channel approach	122
9.8.2	Availability	122
9.8.3	Security measures	122
9.8.4	Stationary and mobile applications	122
9.9	Relationship between functional safety and security	123
9.10	Conformance classes	123
10	Assessment	125
10.1	Safety policy	125
10.2	Obligations	125
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)	130
Annex B (informative) Information for assessment of the functional safety communication profiles of CPF 3		131
Annex C (normative) Optional features		132
C.1	Reaction on Device_Fault in F-Host	132
C.1.1	Situation	132
C.1.2	Documentation for the user	132
C.1.3	Optional extensions of F-Host driver Transition Table	132
C.1.4	Recommendation for the case without Extensions of F-Host driver Transitions	135
C.2	Optional extensions of F-Host driver to "Disable F-(Sub)Module"	135
C.3	Combination of "Disable F-(Sub)Module" and "reaction on Device_Fault"	139
C.4	FSCP 3/1 and PROFIenergy	141
C.4.1	Use of FSCP 3/1-Devices with PROFIenergy	141
C.4.2	Sequence in case of PROFIenergy power off on	141
C.5	Requirement multiple F-Hosts communicate with single F-(Sub)Module	141
C.6	FSCP 3/1 PIR	142
Bibliography		143

Figure 1 – Relationships of IEC 61784-3 with other standards (machinery)	11
Figure 2 – Relationships of IEC 61784-3 with other standards (process)	12
Figure 3 – Basic communication preconditions for FSCP 3/1	30
Figure 4 – Structure of an FSCP 3/1 safety PDU	30
Figure 5 – Safety communication on CPF 3	31
Figure 6 – Standard CPF 3 transmission system	34
Figure 7 – Safety layer architecture	35
Figure 8 – Basic communication layers	35
Figure 9 – Crossing network borders with routers	36
Figure 10 – Complete safety transmission paths	37
Figure 11 – IO Device model	38
Figure 12 – FSCP 3/1 communication structure	39
Figure 13 – F application interface of F-Host driver instances	40
Figure 14 – Motivation for "Channel-related Passivation"	41
Figure 15 – F-Device driver interfaces	43
Figure 16 – Safety PDU for CPF 3	47
Figure 17 – Status Byte	47
Figure 18 – Control Byte	48
Figure 19 – The Toggle Bit function	49
Figure 20 – MonitoringNumber integration	50
Figure 21 – F-Host driver CRC2 signature generation (F_CRC_Seed=0)	52
Figure 22 – Details of the CRC2 signature calculation (F_CRC_Seed=0)	53
Figure 23 – CRC2 signature calculation (F_CRC_Seed=1)	53
Figure 24 – Details of the CRC2 signature calculation (F_CRC_Seed=1)	54
Figure 25 – Safety layer communication relationship	54
Figure 26 – F-Host driver state diagram	55
Figure 27 – F-Device driver state diagram	59
Figure 28 – Interaction F-Host driver / F-Device driver during start-up	63
Figure 29 – Interaction F-Host driver / F-Device driver during F-Host power off > on	64
Figure 30 – Interaction F-Host driver / F-Device driver with delayed power on	65
Figure 31 – Interaction F-Host driver / F-Device driver during power off → on	66
Figure 32 – Interaction while F-Host driver recognizes CRC error	67
Figure 33 – Interaction while F-Device driver recognizes CRC error	68
Figure 34 – Impact of the MNR reset signal	69
Figure 35 – Monitoring the message transit time F-Host ↔ F-(Sub)Module	70
Figure 36 – Extended watchdog time on request	72
Figure 37 – Effect of F_WD_Time_2	77
Figure 38 – F_Prm_Flag1	78
Figure 39 – F_Check_iPar	78
Figure 40 – F_SIL	78
Figure 41 – F_CRC_Length	79
Figure 42 – F_CRC_Seed	79

Figure 43 – F_Prm_Flag2	80
Figure 44 – F_Passivation	80
Figure 45 – F_Block_ID	80
Figure 46 – F_Par_Version	81
Figure 47 – F-Parameter	82
Figure 48 – iParameter block	83
Figure 49 – F-Parameter extension within the GSDML specification.....	85
Figure 50 – F_Par_CRC signature including iPar_CRC	86
Figure 51 – F-Host Channel driver as "glue" between F-(Sub)Module and application program	96
Figure 52 – Layout example of an F-Host Channel driver	97
Figure 53 – F-Parameter assignment for F-(Sub)Modules	98
Figure 54 – System integration of CPD-Tools.....	99
Figure 55 – iPar-Server mechanism (commissioning).....	100
Figure 56 – iPar-Server mechanism (for example F-(Sub)Module replacement)	102
Figure 57 – iPar-Server request coding ("status model")	103
Figure 58 – Coding of SR_Type	104
Figure 59 – iPar-Server request coding ("alarm model").....	105
Figure 60 – iPar-Server state diagram	108
Figure 61 – Example safety function with a critical response time path	112
Figure 62 – Simplified typical response time model.....	112
Figure 63 – Frequency distributions of typical response times of the model	113
Figure 64 – Context of delay times and watchdog times.....	114
Figure 65 – Timing sections forming the FSCP 3/1 F_WD_Time	115
Figure 66 – Frequency distribution of response times with message retries	116
Figure 67 – Residual error probabilities for the 24-bit CRC polynomial.....	117
Figure 68 – Residual error probabilities for the 32-bit CRC polynomial.....	118
Figure 69 – Monitoring of corrupted messages.....	119
Figure A.1 – Typical "C" procedure of a cyclic redundancy check.....	126
Figure C.1 – F-Host driver application interface with feature Reaction on Device_Fault	132
Figure C.2 – F-Host driver application interface with feature Disable F-(Sub)Module	136
Figure C.3 – Timing diagram to use Disable F-(Sub)Module.....	136
Table 1 – Deployed measures to master errors	33
Table 2 – Data types for FSCP 3/1.....	38
Table 3 – F_MessageTrailer for FSCP 3/1	38
Table 4 – Safety layer diagnosis messages	45
Table 5 – Buffer entry on CRC2 error	46
Table 6 – MonitoringNumber of an F-Host driver SPDU	50
Table 7 – MonitoringNumber of an F-Device driver SPDU	50
Table 8 – MonitoringNumber of an F-Host driver SPDU	51
Table 9 – MonitoringNumber of an F-Device driver SPDU	51
Table 10 – Definition of terms used in F-Host driver state diagram.....	55

Table 11 – F-Host driver states and transitions	56
Table 12 – Definition of terms used in Figure 27	59
Table 13 – F-Device driver states and transitions.....	60
Table 14 – SIL monitor times	71
Table 15 – Safety network boundaries	75
Table 16 – Codename octet order	76
Table 17 – Allowed combinations of F_CRC_Seed and F_Passivation	79
Table 18 – GSDL keywords for F-Parameters and F-IO structures	84
Table 19 – Algorithm to build CRC0	87
Table 20 – GSD example in GSDL notation.....	88
Table 21 – GSD example in GSDML notation.....	89
Table 22 – Serialized octet stream for the examples	89
Table 23 – Order of IO data types	90
Table 24 – IO data structure items	91
Table 25 – Dataltem section for F_IN_OUT_1.....	92
Table 26 – DATA_STRUCTURE_CRC for F_IN_OUT_1.....	92
Table 27 – Dataltem section for F_IN_OUT_2.....	93
Table 28 – DATA_STRUCTURE_CRC for F_IN_OUT_2.....	93
Table 29 – Dataltem section for F_IN_OUT_5.....	94
Table 30 – DATA_STRUCTURE_CRC for F_IN_OUT_5.....	94
Table 31 – Dataltem section for F_IN_OUT_6.....	95
Table 32 – DATA_STRUCTURE_CRC for F_IN_OUT_6.....	95
Table 33 – Sample F-Host Channel drivers	96
Table 34 – Requirements for iParameterization.....	99
Table 35 – Specifier for the iPar-Server Request	104
Table 36 – Structure of the Read_RES_PDU ("read record").....	106
Table 37 – Structure of the Write_REQ_PDU ("write record").....	106
Table 38 – Structure of the Pull_RES_PDU ("Pull").....	106
Table 39 – Structure of the Push_REQ_PDU ("Push").....	107
Table 40 – iPar-Server states and transitions.....	109
Table 41 – iPar-Server management measures.....	110
Table 42 – Definition of terms in Figure 69.....	119
Table 43 – Information to be included in the safety manual	121
Table 44 – F-Host conformance class requirements.....	123
Table 45 – Main characteristics of protocol versions	124
Table 46 – F-Host driver / F-Device driver 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
Table C.1 – Definition of additional terms used in driver transitions	133
Table C.2 – F-Host driver transitions – added with reaction on Device_Fault	133
Table C.3 – Prevent unintentional restart by application measures.....	135

Table C.4 – F-Host driver transitions – with feature Disable F-(Sub)Module	137
Table C.5 – F-Host driver transitions – added with "reaction on Device_Fault" and "Disable F-(Sub)Module"	139

This document is a preview generated by EVS

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.
- 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 61784-3-3 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 fourth edition cancels and replaces the third edition published in 2016. This edition constitutes a technical revision.

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

- editorial changes regarding timeliness, transformation of comments in the chart into instructions;
- use abbreviations of PROFINET;
- information added about checks and safety manual for PROFIsafe Address Type 1 and 2;
- information added about PFDavg, support of automatic test, add diagnosis messages;

- explanation and specification of optional statemachines for reaction on device fault;
- new optional variable "OAD_Nec_C" for optional feature "Reaction of Device_Fault in F_Host";
- specification of the optional F-Host feature for "Disable F-(Sub)Module";
- specify requirements for FSCP 3/1 and PROFIenergy;
- specify requirement for multiple F-Hosts communicating with a single F-(Sub)Module; Update of the Safety Manual;
- diverse error corrections, fixes of typos, and reference updates;
- updated bibliography.

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.

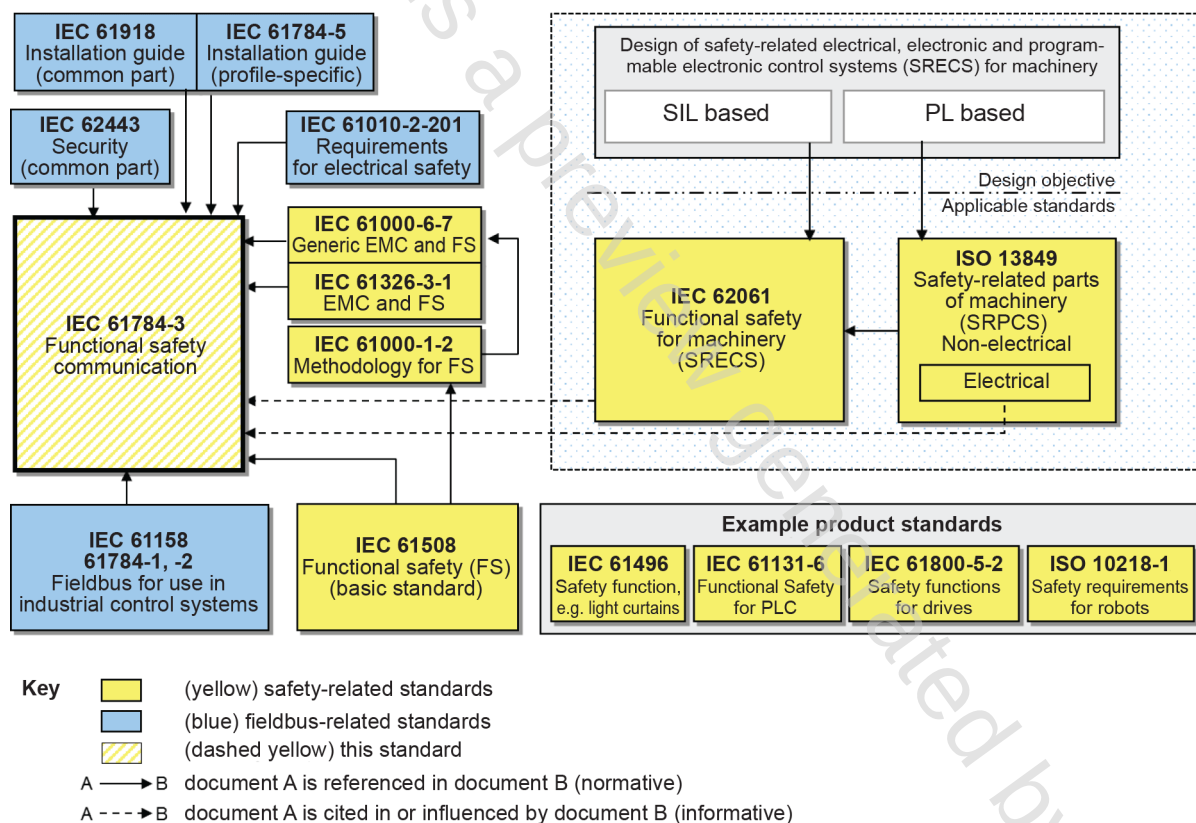
0 Introduction

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.

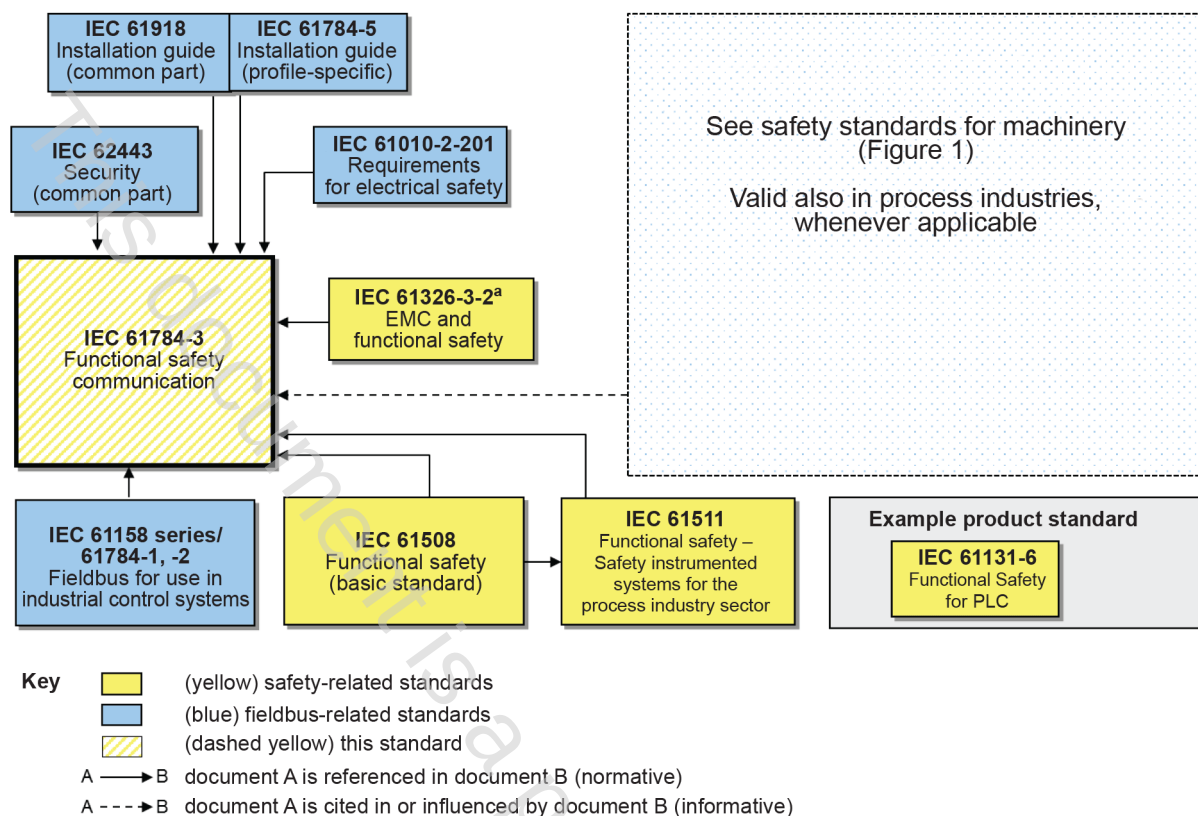


IEC

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 3. 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.

This document is a preview generated by EVS

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES –

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

1 Scope

This part of IEC 61784-3 (all parts) 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 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 60204-1, *Safety of machinery – Electrical equipment of machines – Part 1: General requirements*

IEC 61000-6-7, *Electromagnetic compatibility (EMC) – Part 6-7: Generic standards – Immunity requirements for equipment intended to perform functions in a safety-related system (functional safety) in industrial locations*

IEC 61010-2-201:2017, *Safety requirements for electrical equipment for measurement, control and laboratory use – Part 2-201: Particular requirements for control equipment*

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

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

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/IEEE 8802-3*

IEC 61784-3:2021, *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 61918:2018, *Industrial communication networks – Installation of communication networks in industrial premises*

IEC 62061, *Safety of machinery – Functional safety of safety-related control systems*

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

IEC 62443 (all parts), *Industrial communication networks – Network and system security*

ISO 13849-1:2015, *Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design*

ISO 13849-2:2012, *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 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

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 61918:2018, 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