

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 © 2016 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
Fax: +41 22 919 03 00
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 corrigenda or an amendment might have been published.

IEC Catalogue - webstore.iec.ch/catalogue

The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

IEC publications search - www.iec.ch/searchpub

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 also once a month by email.

Electropedia - www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing 20 000 terms and definitions in English and French, with equivalent terms in 15 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary

65 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

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: csc@iec.ch.

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.

Catalogue IEC - webstore.iec.ch/catalogue

Application autonome pour consulter tous les renseignements bibliographiques sur les Normes internationales, Spécifications techniques, Rapports techniques et autres documents de l'IEC. Disponible pour PC, Mac OS, tablettes Android et iPad.

Recherche de publications IEC - www.iec.ch/searchpub

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 aussi une fois par mois par email.

Electropedia - www.electropedia.org

Le premier dictionnaire en ligne de termes électroniques et électriques. Il contient 20 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans 15 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

Glossaire IEC - std.iec.ch/glossary

65 000 entrées terminologiques électrotechniques, en anglais et en français, extraites des articles Termes et Définitions des publications IEC parues depuis 2002. Plus certaines entrées antérieures extraites des publications des CE 37, 77, 86 et CISPR de l'IEC.

Service Clients - webstore.iec.ch/csc

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

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 978-2-8322-3481-5

**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.....	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	84

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.

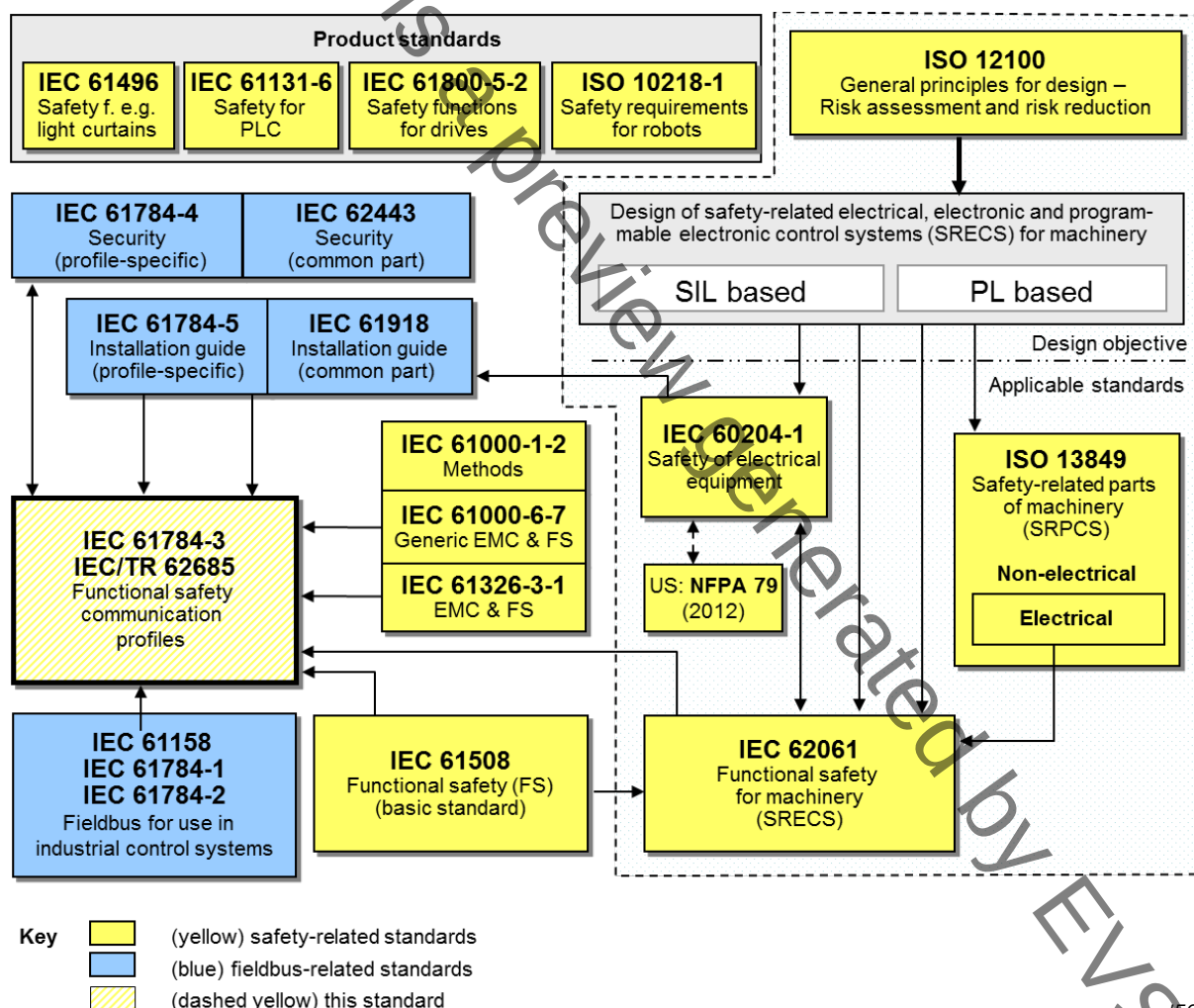
0 Introduction

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.

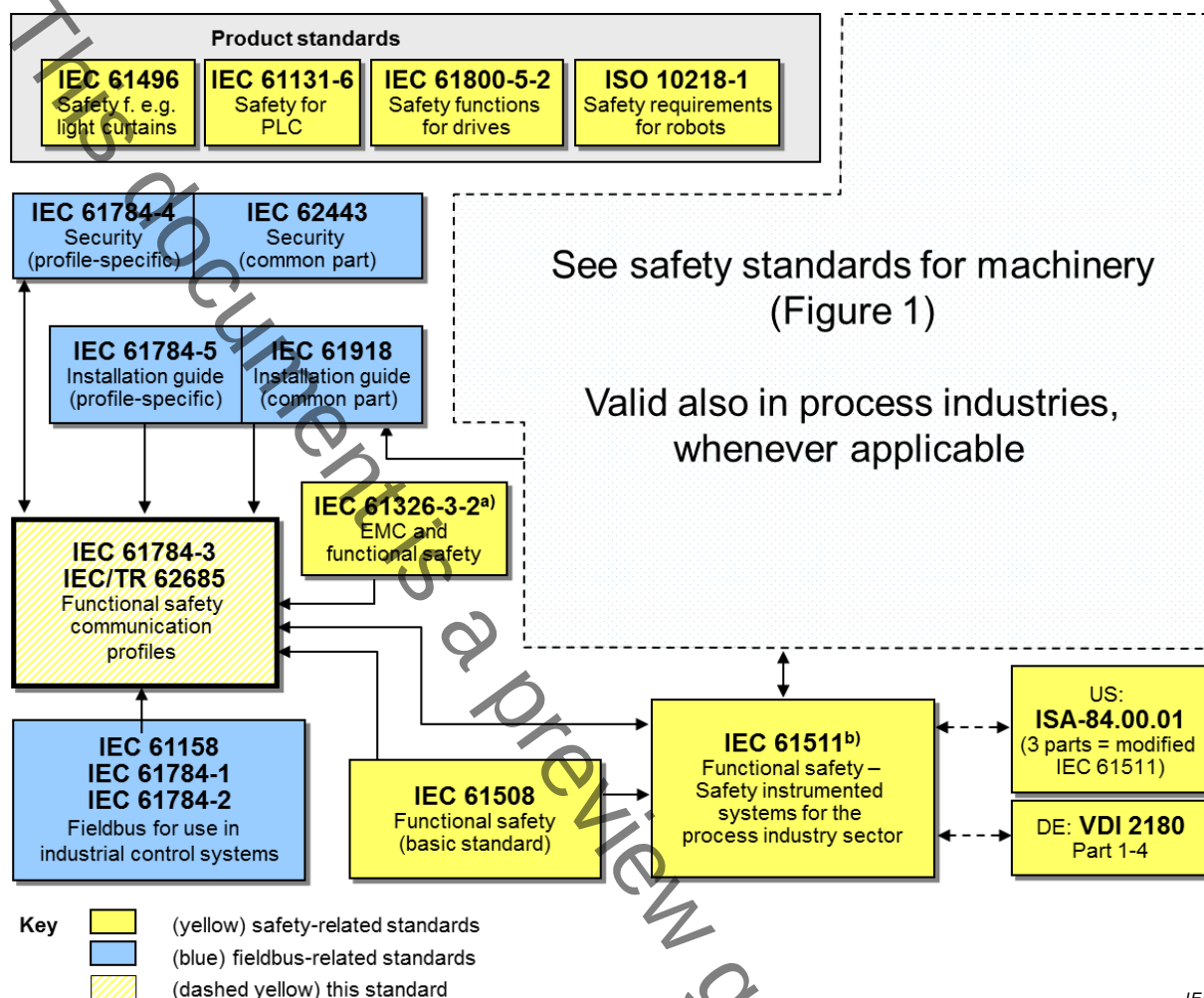
Figure 1 shows the relationships between this standard and relevant safety and fieldbus standards in a machinery environment.



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.

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 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*