

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 © 2010 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 la CEI ou du Comité national de la CEI du pays du demandeur.

Si vous avez des questions sur le copyright de la CEI ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de la CEI de votre pays de résidence.

IEC Central Office
3, rue de Varembé
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.

Useful links:

IEC publications search - www.iec.ch/searchpub

The advanced search enables you 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It also gives information on projects, replaced and withdrawn publications.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 on-line and also once a month by email.

Electropedia - www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 30 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary (IEV) on-line.

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 la CEI

La Commission Electrotechnique Internationale (CEI) 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 CEI

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

Liens utiles:

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

La recherche avancée vous permet de trouver des publications CEI 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.

Just Published CEI - webstore.iec.ch/justpublished

Restez informé sur les nouvelles publications de la CEI. 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 au monde de termes électroniques et électriques. Il contient plus de 30 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans les langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (VEI) en ligne.

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

PRICE CODE
CODE PRIX

XF

ICS 25.040.40, 35.100.05

ISBN 978-2-88912-943-0

**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.....	8
0 Introduction	10
0.1 General.....	10
0.2 Patent declaration	12
1 Scope.....	13
2 Normative references	13
3 Terms, definitions, symbols, abbreviated terms and conventions	15
3.1 Terms and definitions	15
3.1.1 Common terms and definitions	15
3.1.2 CPF 3: Additional terms and definitions	20
3.2 Symbols and abbreviated terms.....	23
3.2.1 Common symbols and abbreviated terms	23
3.2.2 CPF 3: Additional symbols and abbreviated terms	24
3.3 Conventions	25
4 Overview of FSCP 3/1 (PROFIsafe™)	25
5 General	28
5.1 External documents providing specifications for the profile.....	28
5.2 Safety functional requirements	28
5.3 Safety measures	29
5.4 Safety communication layer structure	30
5.4.1 Principle of FSCP 3/1 safety communications	30
5.4.2 CPF 3 communication structures	31
5.5 Relationships with FAL (and DLL, PhL)	34
5.5.1 Device model.....	34
5.5.2 Application and communication relationships.....	34
5.5.3 Message format	36
5.5.4 Data types.....	36
6 Safety communication layer services	37
6.1 F-Host services	37
6.2 F-Device services.....	39
6.3 Diagnosis	41
6.3.1 Safety alarm generation.....	41
6.3.2 F-Device safety layer diagnosis including the iPar-Server.....	41
7 Safety communication layer protocol	42
7.1 Safety PDU format	42
7.1.1 Safety PDU structure	42
7.1.2 Safety I/O data	43
7.1.3 Status and Control Byte.....	43
7.1.4 (Virtual) Consecutive Number	44
7.1.5 CRC2 Signature	46
7.1.6 Appended standard I/O data	47
7.2 FSCP 3/1 behavior	47
7.2.1 General	47
7.2.2 F-Host state diagram	47
7.2.3 F-Device state diagram.....	51
7.2.4 Sequence diagrams.....	55

7.2.5	Timing diagram for a counter reset	61
7.2.6	Monitoring of safety times	61
7.3	Reaction in the event of a malfunction	64
7.3.1	Repetition	64
7.3.2	Loss	65
7.3.3	Insertion	65
7.3.4	Incorrect sequence	65
7.3.5	Corruption of safety data	65
7.3.6	Delay	66
7.3.7	Masquerade	66
7.3.8	Memory failures within switches	66
7.3.9	Network boundaries and router	67
7.4	F-Startup and change coordination	68
7.4.1	Standard startup procedure	68
7.4.2	iParameter assignment deblocking	68
8	Safety communication layer management	69
8.1	F-Parameter	69
8.1.1	Summary	69
8.1.2	F_Source/Destination_Address (codename)	69
8.1.3	F_WD_Time (F-Watchdog time)	69
8.1.4	F_WD_Time_2 (secondary F-Watchdog time)	70
8.1.5	F_Prm_Flag1 (Parameters for the safety layer management)	70
8.1.6	F_Prm_Flag2 (Parameters for the safety layer management)	72
8.1.7	F_iPar_CRC (value of iPar_CRC across iParameters)	73
8.1.8	F_Par_CRC (CRC1 across F-Parameters)	73
8.1.9	Structure of the F-Parameter record data object	74
8.1.10	F-Data fraction	74
8.2	iParameter and iPar_CRC	74
8.3	Safety parameterization	75
8.3.1	Objectives	75
8.3.2	GSDL and GSDML safety extensions	76
8.3.3	Securing safety parameters and GSD data	77
8.4	Safety configuration	80
8.4.1	Securing the safety I/O data description (CRC7)	80
8.4.2	DataItem data type section examples	81
8.5	Data type information usage	84
8.5.1	F-Channel driver	84
8.5.2	Rules for standard F-Channel drivers	85
8.5.3	Recommendations for F-Channel drivers	86
8.6	Safety parameter assignment mechanisms	87
8.6.1	F-Parameter assignment	87
8.6.2	General iParameter assignment	87
8.6.3	System integration requirements for iParameterization tools	88
8.6.4	iPar-Server	90
9	System requirements	99
9.1	Indicators and switches	99
9.2	Installation guidelines	99
9.3	Safety function response time	99
9.3.1	Model	99

9.3.2	Calculation and optimization	101
9.3.3	Adjustment of watchdog times for FSCP 3/1	103
9.3.4	Engineering tool support.....	104
9.3.5	Retries (repetition of messages).....	104
9.4	Duration of demands	105
9.5	Constraints for the calculation of system characteristics	106
9.5.1	Probabilistic considerations	106
9.5.2	Safety related constraints	108
9.5.3	Non safety related constraints (availability).....	109
9.6	Maintenance.....	109
9.6.1	F-Module commissioning / replacement.....	109
9.6.2	Identification and maintenance functions	109
9.7	Safety manual	110
9.8	Wireless transmission channels.....	111
9.8.1	Black channel approach	111
9.8.2	Availability.....	111
9.8.3	Security measures.....	111
9.8.4	Stationary and mobile applications.....	113
9.9	Conformance classes	113
10	Assessment.....	114
10.1	Safety policy	114
10.2	Obligations.....	115
	Annex A (informative) Additional information for functional safety communication profiles of CPF 3.....	116
A.1	Hash function calculation.....	116
A.2	Response time measurements.....	118
	Annex B (informative) Information for assessment of the functional safety communication profiles of CPF 3	122
	Bibliography.....	123
	Table 1 – Deployed measures to master errors	29
	Table 2 – Data types used for FSCP 3/1	36
	Table 3 – Safety layer diagnosis messages	41
	Table 4 – F-Host states and transitions.....	49
	Table 5 – F-Device states and transitions	53
	Table 6 – SIL monitor times	64
	Table 7 – Remedies for switch failures.....	67
	Table 8 – Safety network boundaries	68
	Table 9 – GSDL keywords for F-Parameters and F-I/O structures.....	76
	Table 10 – I/O data structure items (Version 2).....	80
	Table 11 – Sample F-Channel drivers	85
	Table 12 – Requirements for iParameterization.....	88
	Table 13 – Specifier for the iPar-Server Request	92
	Table 14 – Structure of the Read_RES_PDU ("read record").....	94
	Table 15 – Structure of the Write_REQ_PDU ("write record").....	95
	Table 16 – Structure of the Pull_RES_PDU ("Pull").....	95

Table 17 – Structure of the Push_REQ_PDU ("Push")	95
Table 18 – iPar-Server states and transitions.....	97
Table 19 – iPar-Server management measures.....	98
Table 20 – Information to be included in the safety manual.....	110
Table 21 – Security measures for WLAN (IEEE 802.11i).....	112
Table 22 – Security measures for Bluetooth (IEEE 802.15.1).....	113
Table 23 – F-Host conformance class requirements.....	114
Table A.1 – The table "Crctab24" for 24 bit CRC signature calculations	117
Table A.2 – The table "Crctab32" for 32 bit CRC signature calculations	118
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	26
Figure 4 – Structure of an FSCP 3/1 safety PDU.....	27
Figure 5 – Safety communication modes.....	28
Figure 6 – Standard CPF 3 transmission system.....	30
Figure 7 – Safety layer architecture	31
Figure 8 – Basic communication layers.....	31
Figure 9 – Multiport switch bus structure.....	32
Figure 10 – Linear bus structure	32
Figure 11 – Crossing network borders with routers	33
Figure 12 – Complete safety transmission paths	33
Figure 13 – Device model	34
Figure 14 – Application relationships of a modular device	35
Figure 15 – Application and communication relationships (AR/CR)	35
Figure 16 – Message format	36
Figure 17 – FSCP 3/1 communication structure	37
Figure 18 – F user interface of F-Host driver instances	38
Figure 19 – F-Device driver interfaces	40
Figure 20 – Safety PDU for CPF 3	42
Figure 21 – Status Byte	43
Figure 22 – Control Byte	44
Figure 23 – The Toggle Bit function	45
Figure 24 – F-Device Consecutive Number	45
Figure 25 – CRC2 generation (F-Host output).....	46
Figure 26 – Details of the CRC2 calculation (reverse order).....	47
Figure 27 – Safety layer communication relationship.....	47
Figure 28 – F-Host state diagram.....	48
Figure 29 – F-Device state diagram	52
Figure 30 – Interaction F-Host / F-Device during start-up.....	55
Figure 31 – Interaction F-Host / F-Device during F-Host power off → on.....	56
Figure 32 – Interaction F-Host / F-Device with delayed power on.....	57

Figure 33 – Interaction F-Host / F-Device during power off → on	58
Figure 34 – Interaction F-Host / F-Device while host recognizes CRC error	59
Figure 35 – Interaction F-Host / F-Device while device recognizes CRC error	60
Figure 36 – Impact of the counter reset signal	61
Figure 37 – Monitoring the message transit time F-Host ↔ F-Output	62
Figure 38 – Monitoring the message transit time F-Input ↔ F-Host	62
Figure 39 – Extended watchdog time on request	64
Figure 40 – F-Parameter data and CRC	65
Figure 41 – iParameter assignment deblocking by the F-Host	68
Figure 42 – Effect of F_WD_Time_2	70
Figure 43 – F_Prm_Flag1	70
Figure 44 – F_Check_SeqNr	71
Figure 45 – F_Check_iPar	71
Figure 46 – F_SIL	71
Figure 47 – F_CRC_Length	72
Figure 48 – F_Prm_Flag2	72
Figure 49 – F_Block_ID	72
Figure 50 – F_Par_Version	73
Figure 51 – F-Parameter	74
Figure 52 – iParameter block	75
Figure 53 – F-Parameter extension within the GSDML specification	77
Figure 54 – CRC1 including iPar_CRC	78
Figure 55 – Algorithm to build CRC0 (GSDL)	79
Figure 56 – Algorithm to build CRC0 (GSDML)	80
Figure 57 – DataItem section for F_IN_OUT_1	82
Figure 58 – DataItem section for F_IN_OUT_2	83
Figure 59 – DataItem section for F_IN_OUT_5	83
Figure 60 – DataItem section for F_IN_OUT_6	84
Figure 61 – F-Channel driver as "glue" between F-Device and user program	85
Figure 62 – Layout example of an F-Channel driver	86
Figure 63 – F-Parameter assignment for simple F-Devices and F-Slaves	87
Figure 64 – F and iParameter assignment for complex F-Devices	88
Figure 65 – System integration of CPD-Tools	89
Figure 66 – iPar-Server mechanism (commissioning)	90
Figure 67 – iPar-Server mechanism (for example F-Device replacement)	91
Figure 68 – iPar-Server request coding ("status model")	92
Figure 69 – Coding of SR_Type	93
Figure 70 – iPar-Server request coding ("alarm model")	94
Figure 71 – iPar-Server state diagram	96
Figure 72 – Example safety function with a critical response time path	100
Figure 73 – Simplified typical response time model	100
Figure 74 – Frequency distributions of typical response times of the model	101
Figure 75 – Context of delay times and watchdog times	102

Figure 76 – Timing sections forming the FSCP 3/1 F_WD_Time	103
Figure 77 – Frequency distribution of response times with message retries	104
Figure 78 – Retries with CP 3/1	105
Figure 79 – Retries with CP 3/RTE	105
Figure 80 – Residual error probabilities for the 24-bit polynomial	106
Figure 81 – Properness of the 32-bit polynomial for 52 octets	107
Figure 82 – Properness of the 32-bit polynomial for 132 octets	107
Figure 83 – Monitoring of corrupted messages.....	108
Figure 84 – Security for WLAN networks.....	111
Figure 85 – Security for Bluetooth networks.....	112
Figure A.1 – Typical "C" procedure of a cyclic redundancy check.....	116
Figure A.2 – Comparison of the response time model and a real application	119
Figure A.3 – Frequency distribution of measured response times.....	120
Figure A.4 – F-Host with standard and safety-related application programs	121

Withdrawing