

INTERNATIONAL STANDARD

NORME INTERNATIONALE



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

**Réseaux de communications 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

XE

ICS 25.040; 35.100.05

ISBN 978-2-83220-722-2

**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
INTRODUCTION.....	10
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	19
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	23
3.3 Conventions	24
4 Overview of FSCP 3/1 (PROFIsafe™)	25
5 General	27
5.1 External documents providing specifications for the profile.....	27
5.2 Safety functional requirements	27
5.3 Safety measures	28
5.4 Safety communication layer structure.....	29
5.4.1 Principle of FSCP 3/1 safety communications	29
5.4.2 CPF 3 communication structures	30
5.5 Relationships with FAL (and DLL, PhL)	33
5.5.1 Device model.....	33
5.5.2 Application and communication relationships.....	33
5.5.3 Message format.....	35
5.5.4 Data types	35
6 Safety communication layer services	36
6.1 F-Host services	36
6.2 F-Device services.....	39
6.3 Diagnosis	40
6.3.1 Safety alarm generation.....	40
6.3.2 F-Device safety layer diagnosis including the iPar-Server.....	40
7 Safety communication layer protocol	41
7.1 Safety PDU format	41
7.1.1 Safety PDU structure	41
7.1.2 Safety I/O data	42
7.1.3 Status and Control Byte.....	42
7.1.4 (Virtual) Consecutive Number	44
7.1.5 CRC2 Signature	45
7.1.6 Appended standard I/O data	46
7.2 FSCP 3/1 behavior	46
7.2.1 General	46
7.2.2 F-Host state diagram	47
7.2.3 F-Device state diagram.....	50
7.2.4 Sequence diagrams.....	54
7.2.5 Timing diagram for a counter reset	60

7.2.6	Monitoring of safety times.....	60
7.3	Reaction in the event of a malfunction.....	63
7.3.1	Repetition.....	63
7.3.2	Loss	63
7.3.3	Insertion	63
7.3.4	Incorrect sequence	63
7.3.5	Corruption of safety data	63
7.3.6	Delay.....	64
7.3.7	Masquerade	64
7.3.8	Memory failures within switches	65
7.3.9	Network boundaries and router.....	66
7.4	F-Startup and change coordination.....	66
7.4.1	Standard startup procedure	66
7.4.2	iParameter assignment deblocking	66
8	Safety communication layer management.....	67
8.1	F-Parameter	67
8.1.1	Summary	67
8.1.2	F_Source/Destination_Address (codename)	67
8.1.3	F_WD_Time (F-Watchdog time).....	68
8.1.4	F_Prm_Flag1 (Parameters for the safety layer management)	68
8.1.5	F_Prm_Flag2 (Parameters for the safety layer management)	69
8.1.6	F_iPar_CRC (value of iPar_CRC across iParameters).....	70
8.1.7	F_Par_CRC (CRC1 across F-Parameters).....	71
8.1.8	Structure of the F-Parameter record data object	71
8.1.9	F-Data fraction	71
8.2	iParameter and iPar_CRC	72
8.3	Safety parameterization.....	73
8.3.1	Objectives	73
8.3.2	GSD and GSDML safety extensions	73
8.3.3	Securing safety parameters and GSD data	74
8.4	Safety configuration	76
8.4.1	Securing the safety I/O data description (CRC7).....	76
8.4.2	Dataltem data type section examples	77
8.5	Data type information usage	79
8.5.1	F-Channel driver.....	79
8.5.2	Rules for standard F-Channel drivers	80
8.5.3	Recommendations for F-Channel drivers	80
8.6	Safety parameter assignment mechanisms.....	81
8.6.1	F-Parameter assignment	81
8.6.2	General iParameter assignment.....	82
8.6.3	System integration requirements for iParameterization tools.....	83
8.6.4	iPar-Server	84
9	System requirements.....	92
9.1	Indicators and switches	92
9.2	Installation guidelines.....	93
9.3	Safety function response time	93
9.3.1	Model	93
9.3.2	Calculation and optimization	95
9.3.3	Adjustment of watchdog times for FSCP 3/1	96

9.3.4	Engineering tool support.....	97
9.3.5	Retries (repetition of messages).....	97
9.4	Duration of demands	98
9.5	Constraints for the calculation of system characteristics	99
9.5.1	Probabilistic considerations	99
9.5.2	Safety related constraints	101
9.5.3	Non safety related constraints (availability).....	102
9.6	Maintenance.....	102
9.6.1	F-Module commissioning / replacement.....	102
9.6.2	Identification and maintenance functions	102
9.7	Safety manual	103
9.8	Wireless transmission channels.....	103
9.8.1	Black Channel approach.....	103
9.8.2	Availability.....	104
9.8.3	Security measures.....	104
9.8.4	Stationary and mobile applications	106
9.9	Conformance classes	106
10	Certification	107
10.1	Safety policy	107
10.2	Obligations	108
Annex A (informative) Additional information for functional safety communication profiles of CPF 3.....		109
A.1	Hash function calculation.....	109
A.2	Response time measurements.....	111
Bibliography.....		115
Table 1 – Deployed measures to master errors		28
Table 2 – Data types used for FSCP 3/1		35
Table 3 – Safety layer diagnosis messages		41
Table 4 – F-Host states and transitions.....		48
Table 5 – F-Device states and transitions		52
Table 6 – SIL monitor times		63
Table 7 – Remedies for switch failures.....		65
Table 8 – Safety network boundaries		66
Table 9 – I/O data structure items (Version 2).....		76
Table 10 – Sample F-Channel drivers		80
Table 11 – Requirements for iParameterization.....		83
Table 12 – Specifier for the iPar-Server Request		87
Table 13 – Structure of the Read_RES_PDU ("read record").....		88
Table 14 – Structure of the Write_REQ_PDU ("write record").....		89
Table 15 – Structure of the Pull_RES_PDU ("Pull").....		89
Table 16 – Structure of the Push_REQ_PDU ("Push")		89
Table 17 – iPar-Server states and transitions.....		91
Table 18 – iPar-Server management measures.....		92
Table 19 – Information to be included in the safety manual.....		103

Table 20 – Security measures for WLAN (IEEE 802.11i)	105
Table 21 – Security measures for Bluetooth (IEEE 802.15.1)	106
Table 22 – F-Host conformance class requirements	107
Table A.1 – The table "Crctab24" for 24 bit CRC signature calculations	110
Table A.2 – The table "Crctab32" for 32 bit CRC signature calculations	111
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	25
Figure 4 – Structure of an FSCP 3/1 safety PDU	26
Figure 5 – Safe communication modes	27
Figure 6 – Standard CPF 3 transmission system	29
Figure 7 – Safety layer architecture	30
Figure 8 – Basic communication layers	30
Figure 9 – Multiport switch bus structure	31
Figure 10 – Linear bus structure	31
Figure 11 – Crossing network borders with routers	32
Figure 12 – Complete safety transmission paths	32
Figure 13 – Device model	33
Figure 14 – Application relationships of a modular device	34
Figure 15 – Application and communication relationships (AR/CR)	34
Figure 16 – Message format	35
Figure 17 – FSCP 3/1 communication structure	37
Figure 18 – F user interface of F-Host driver instances	37
Figure 19 – F-Device driver interfaces	39
Figure 20 – Safety PDU for CPF 3	42
Figure 21 – Status Byte	42
Figure 22 – Control Byte	43
Figure 23 – The Toggle Bit function	44
Figure 24 – F-Device Consecutive Number	44
Figure 25 – CRC2 generation (F-Host output)	45
Figure 26 – Details of the CRC2 calculation (reverse order)	46
Figure 27 – Safety layer communication relationship	46
Figure 28 – F-Host state diagram	47
Figure 29 – F-Device state diagram	51
Figure 30 – Interaction F-Host / F-Device during start-up	54
Figure 31 – Interaction F-Host / F-Device during F-Host power off → on	55
Figure 32 – Interaction F-Host / F-Device with delayed power on	56
Figure 33 – Interaction F-Host / F-Device during power off → on	57
Figure 34 – Interaction F-Host / F-Device while host recognizes CRC error	58
Figure 35 – Interaction F-Host / F-Device while device recognizes CRC error	59
Figure 36 – Impact of the counter reset signal	60

Figure 37 – Monitoring the message transit time F-Host ↔ F-Output	61
Figure 38 – Monitoring the message transit time F-Input ↔ F-Host	61
Figure 39 – F-Parameter data and CRC	64
Figure 40 – iParameter assignment deblocking by the F-Host	67
Figure 41 – F_Prm_Flag1	68
Figure 42 – F_Check_SeqNr	68
Figure 43 – F_Check_iPar	69
Figure 44 – F_SIL	69
Figure 45 – F_CRC_Length	69
Figure 46 – F_Prm_Flag2	70
Figure 47 – F_Block_ID	70
Figure 48 – F_Par_Version	70
Figure 49 – F-Parameter	71
Figure 50 – iParameter block	72
Figure 51 – F-Parameter extension within the GSDML specification	74
Figure 52 – CRC1 including iPar_CRC	75
Figure 53 – Algorithm to build CRC0	75
Figure 54 – DataItem section for F_IN_OUT_1	77
Figure 55 – DataItem section for F_IN_OUT_2	78
Figure 56 – DataItem section for F_IN_OUT_5	78
Figure 57 – DataItem section for F_IN_OUT_6	79
Figure 58 – F-Channel driver as "glue" between F-Device and user program	79
Figure 59 – Layout example of an F-Channel driver	80
Figure 60 – F-Parameter assignment for simple F-Devices and F-Slaves	81
Figure 61 – F and iParameter assignment for complex F-Devices	82
Figure 62 – System integration of CPD-Tools	84
Figure 63 – iPar-Server mechanism (commissioning)	84
Figure 64 – iPar-Server mechanism (for example F-Device replacement)	85
Figure 65 – iPar-Server request coding ("status model")	86
Figure 66 – Coding of SR_Type	87
Figure 67 – iPar-Server request coding ("alarm model")	88
Figure 68 – iPar-Server state diagram	90
Figure 69 – Example safety function with a critical response time path	93
Figure 70 – Simplified typical response time model	94
Figure 71 – Frequency distributions of typical response times of the model	94
Figure 72 – Context of delay times and watchdog times	95
Figure 73 – Timing sections forming the FSCP 3/1 F_WD_Time	96
Figure 74 – Frequency distribution of response times with message retries	97
Figure 75 – Retries with CP 3/1	98
Figure 76 – Retries with CP 3/RTE	98
Figure 77 – Residual error probabilities for the 24-bit polynomial	99
Figure 78 – Properness of the 32-bit polynomial for 52 octets	100
Figure 79 – Properness of the 32-bit polynomial for 132 octets	100

Figure 80 – Monitoring of corrupted messages.....	101
Figure 81 – Security for WLAN networks.....	104
Figure 82 – Security for Bluetooth networks.....	105
Figure A.83 – Typical "C" procedure of a cyclic redundancy check.....	109
Figure A.84 – Comparison of the response time model and a real application	112
Figure A.85 – Frequency distribution of measured response times.....	113
Figure A.86 – F-Host with standard and safety-related application programs	114

Withdrawn

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 provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with an IEC Publication.
- 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.

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 right:

EP1267270-A2	[SI]	Verfahren zur Datenübertragung in einem Rechnersystem
WO00/045562-A1	[SI]	Method and device for determining the reliability of data carriers
WO99/049373-A1	[SI]	Shortened data message of an automation system

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 under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statement of the holders of these patent rights are registered with IEC.

Information may be obtained from:

[SI]	Siemens AG A&D AS FA TC Karlsruhe 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.

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 bilingual version (2013-05) corresponds to the monolingual English version, published in 2007-12.

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

FDIS	Report on voting
65C/470/FDIS	65C/481/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.

The French version of this standard has not been voted upon.

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

The committee has decided that the contents of this publication will remain unchanged until the maintenance result 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.

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

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.

INTRODUCTION

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 many fieldbus enhancements are emerging, addressing not yet standardized 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.

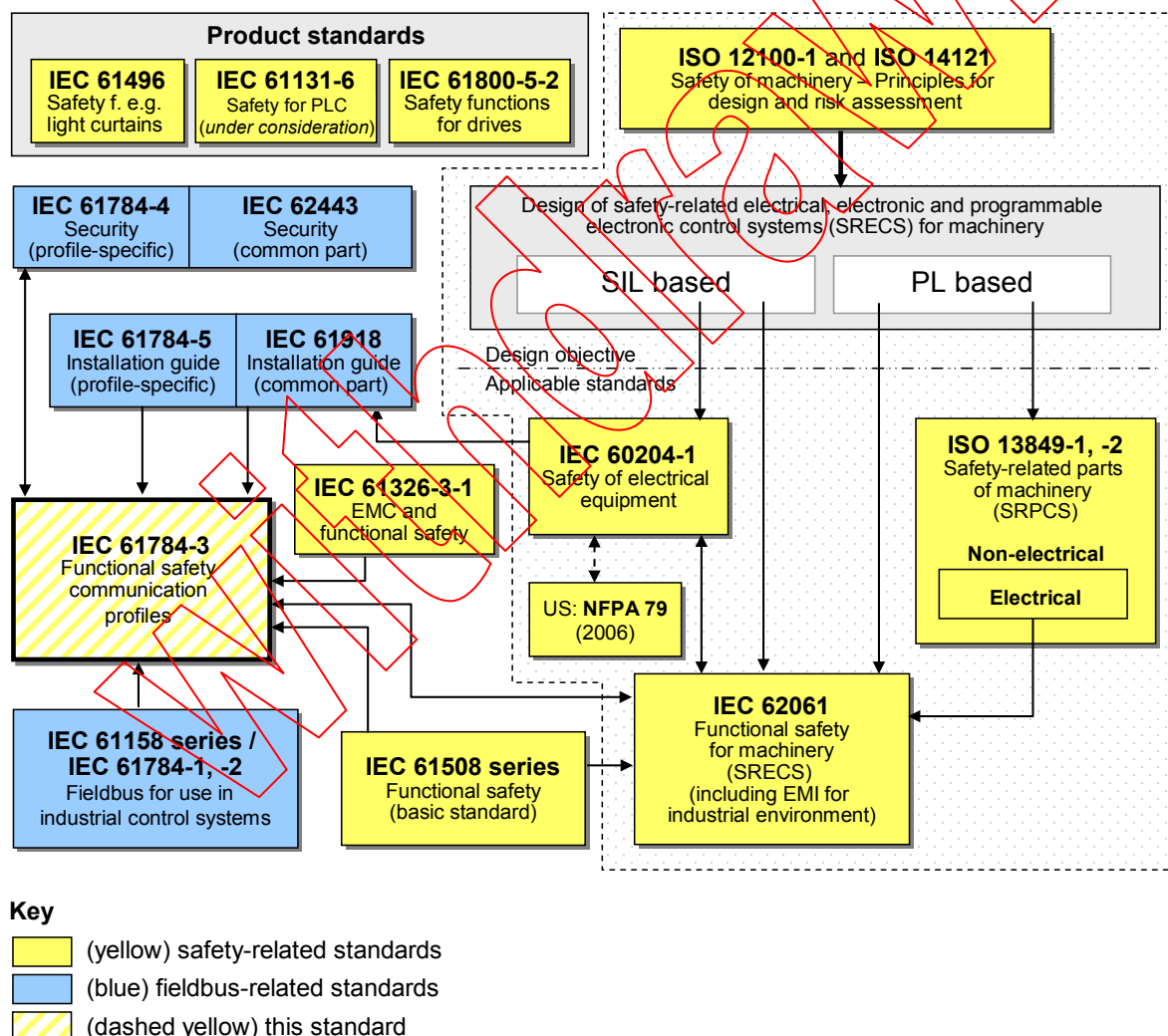
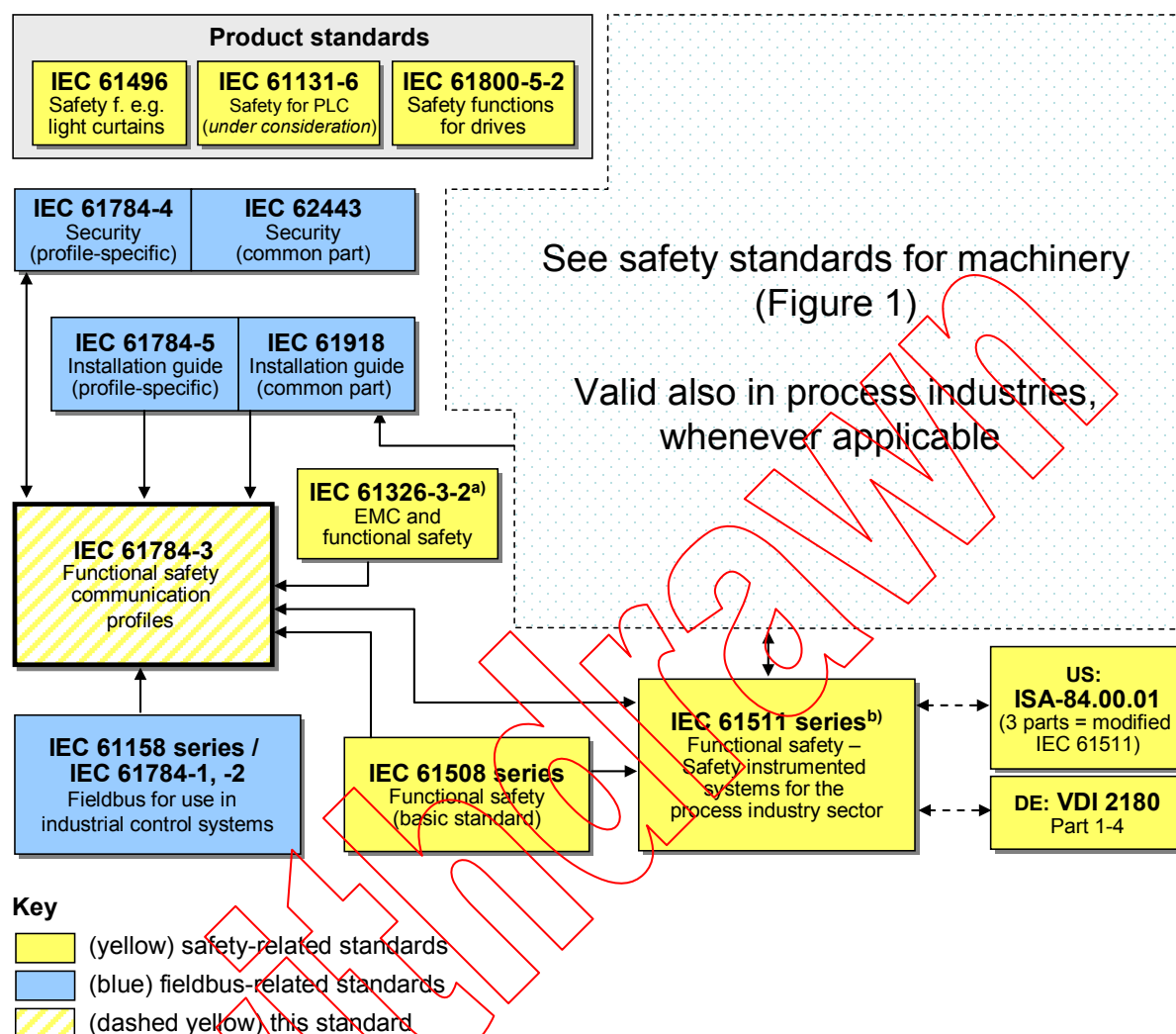


Figure 1 – Relationships of IEC 61784-3 with other standards (machinery)

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.

^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 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;
- individual description of functional safety profiles for several communication profile families in IEC 61784-1 and IEC 61784-2;
- safety layer extensions to the communication service and protocols sections of the IEC 61158 series.

Withdrawn

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.

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 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 referenced documents are indispensable for the application 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 61010-1, *Safety requirements for electrical equipment for measurement, control, and laboratory use – Part 1: General requirements*

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

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

IEC 61158 (all parts), *Industrial communication networks – Fieldbus specifications*

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*

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

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

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

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

IEC 61158-6-3, *Industrial communication networks – Fieldbus specifications – Part 4-3: Application layer protocol specification*

IEC 61158-6-10, *Industrial communication networks – Fieldbus specifications – Part 4-10: Application layer protocol specification*

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*²

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 EM environment*²

IEC 61508 (all parts), *Functional safety of 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, *Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions*

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

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

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

IEC 62280-1:2002, *Railway applications – Communication, signalling and processing systems – Part 1: Safety-related communication in closed transmission systems*

IEC 62280-2, *Railway applications – Communication, signalling and processing systems – Part 2: Safety-related communication in open transmission systems*

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

² To be published.

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

ISO 15745-3, *Industrial automation systems and integration – Open systems application integration framework – Part 3: Reference description for IEC 61158-based control systems*

ISO 15745-4, *Industrial automation systems and integration – Open systems application integration framework – Part 4: Reference description for Ethernet-based control systems – Amendment 1: PROFINET profiles*

Withdrawn

SOMMAIRE

AVANT-PROPOS	124
INTRODUCTION.....	126
1 Domaine d'application	130
2 Références normatives.....	130
3 Termes, définitions, symboles, abréviations et conventions	132
3.1 Termes et définitions	132
3.1.1 Termes et définitions communs	132
3.1.2 CPF 3: Termes et définitions supplémentaires	137
3.2 Symboles et abréviations	140
3.2.1 Symboles et abréviations communs.....	140
3.2.2 CPF 3: Symboles et abréviations supplémentaires	141
3.3 Conventions	142
4 Présentation générale de FSCP 3/1 (PROFIsafe™).....	142
5 Généralités.....	146
5.1 Documents externes de spécifications applicables au profil.....	146
5.2 Exigences fonctionnelles de sécurité	146
5.3 Mesures de sécurité	146
5.4 Structure de la couche de communication de sécurité	147
5.4.1 Principe des communications de sécurité FSCP 3/1	147
5.4.2 Structures de communication CPF 3.....	149
5.5 Relations avec la FAL (et DLL, PhL).....	154
5.5.1 Modèle de dispositif.....	154
5.5.2 Relations d'application et de communication	155
5.5.3 Format de message.....	157
5.5.4 Types de données	159
6 Services de la couche de communication de sécurité	159
6.1 Services de l'hôte F.....	159
6.2 Services du dispositif F	162
6.3 Diagnostic	165
6.3.1 Génération d'alarme de sécurité	165
6.3.2 Diagnostic de la couche de sécurité du dispositif F (y compris le serveur d'iParamètres)	165
7 Protocole de couche de communication de sécurité.....	166
7.1 Format PDU de sécurité	166
7.1.1 Structure PDU de sécurité	166
7.1.2 Données d'entrée-sortie de sécurité	167
7.1.3 Octet d'état et de contrôle	168
7.1.4 Numéro consécutif (virtuel).....	169
7.1.5 Signature CRC2	171
7.1.6 Données d'entrée-sortie standard ajoutées.....	173
7.2 Comportement FSCP 3/1.....	173
7.2.1 Généralités.....	173
7.2.2 Diagramme d'états de l'hôte F	173
7.2.3 Diagramme d'états du dispositif F.....	177
7.2.4 Diagrammes séquentiels	181
7.2.5 Chronogramme de réinitialisation d'un compteur	189

7.2.6	Surveillance des temps de sécurité	190
7.3	Réaction en cas de dysfonctionnement	193
7.3.1	Répétition	193
7.3.2	Perte	193
7.3.3	Insertion	193
7.3.4	Séquence incorrecte	193
7.3.5	Corruption des données de sécurité	193
7.3.6	Délai	194
7.3.7	Déguisement	194
7.3.8	Anomalies de mémoire dans les commutateurs	195
7.3.9	Limites du réseau et routeur	196
7.4	Démarrage F et coordination des modifications	196
7.4.1	Procédure de démarrage standard	196
7.4.2	Déblocage de l'attribution d'iParamètre	197
8	Gestion de la couche de communication de sécurité	197
8.1	Paramètre F	197
8.1.1	Récapitulatif	197
8.1.2	F_Source/Destination_Address (nom de code)	198
8.1.3	F_WD_Time (temps de fonctionnement du chien de garde F)	198
8.1.4	F_Prm_Flag1 (Paramètres de gestion de la couche de sécurité)	198
8.1.5	F_Prm_Flag2 (Paramètres de gestion de la couche de sécurité)	200
8.1.6	F_iPar_CRC (valeur d'iPar_CRC dans iParamètres)	201
8.1.7	F_Par_CRC (CRC1 parmi les paramètres F)	201
8.1.8	Structure de l'objet de données d'enregistrement du paramètre F	202
8.1.9	Fraction de données F	202
8.2	iParamètre et iPar_CRC	203
8.3	Paramétrage de sécurité	204
8.3.1	Objectifs	204
8.3.2	Extensions de sécurité GSD et GSDML	205
8.3.3	Protection des paramètres de sécurité et des données GSD	206
8.4	Configuration de la sécurité	208
8.4.1	Protection de la description des données d'entrée-sortie de sécurité (CRC7)	208
8.4.2	Exemples de section de type de données Dataltem	209
8.5	Utilisation des informations de type de données	212
8.5.1	Pilote de canal F	212
8.5.2	Règles pour les pilotes de canal F standard	212
8.5.3	Recommandations relatives aux pilotes de canal F	213
8.6	Mécanismes d'attribution de paramètres de sécurité	215
8.6.1	Attribution du paramètre F	215
8.6.2	Attribution générale d'iParamètre	216
8.6.3	Exigences d'intégration de système des outils d'iParamétrage	217
8.6.4	Serveur d'iParamètres	219
9	Exigences système	231
9.1	Voyants et commutateurs	231
9.2	Lignes directrices d'installation	231
9.3	Temps de réponse de la fonction de sécurité	231
9.3.1	Modèle	231
9.3.2	Calcul et optimisation	234

9.3.3	Ajustement des temps de fonctionnement du chien de garde pour FSCP 3/1	235
9.3.4	Prise en charge de l'outil de développement.....	237
9.3.5	Relances (répétition des messages)	237
9.4	Durée des demandes ou sollicitations	239
9.5	Contraintes liées au calcul des caractéristiques des systèmes	240
9.5.1	Considérations probabilistes.....	240
9.5.2	Contraintes relatives à la sécurité.....	244
9.5.3	Contraintes non relatives à la sécurité (disponibilité)	244
9.6	Maintenance.....	245
9.6.1	Mise en service/remplacement du module F	245
9.6.2	Fonctions d'identification et de maintenance.....	245
9.7	Manuel de sécurité	245
9.8	Canaux de transmission sans fil	246
9.8.1	Approche du canal noir.....	246
9.8.2	Disponibilité.....	246
9.8.3	Mesures de sécurité	246
9.8.4	Applications fixes et mobiles.....	250
9.9	Classes de conformité	250
10	Évaluation	251
10.1	Politique de sécurité.....	251
10.2	Obligations	252
Annexe A (informative) Informations supplémentaires pour les profils de communication de sécurité fonctionnelle de CPF 3		253
A.1	Calcul de la fonction de hachage.....	253
A.2	Mesures du temps de réponse.....	255
Bibliographie.....		259
Tableau 1 – Mesurées déployées pour maîtriser les erreurs		147
Tableau 2 – Types de données utilisés pour FSCP 1/3		159
Tableau 3 – Messages de diagnostic de la couche de sécurité		165
Tableau 4 – États et transitions de l'hôte F		175
Tableau 5 – États et transitions du dispositif F.....		179
Tableau 6 – Temps du dispositif de surveillance SIL		192
Tableau 7 – Solutions aux anomalies de commutation		195
Tableau 8 – Limites du réseau de sécurité.....		196
Tableau 9 – Éléments de structure de données d'entrée-sortie (Version 2)		208
Tableau 10 – Modèle de pilotes de canal F		213
Tableau 11 – Exigences pour l'iParamétrage		217
Tableau 12 – Spécificateur de la demande de serveur d'iParamètres.....		223
Tableau 13 – Structure de Read_RES_PDU (« Read Record »).....		226
Tableau 14 – Structure de Write_REQ_PDU (« Write Record »).....		226
Tableau 15 – Structure de Pull_RES_PDU (« Pull »).....		226
Tableau 16 – Structure de Push_REQ_PDU (« Push »)		226
Tableau 17 – États et transitions du serveur d'iParamètres.....		229
Tableau 18 – Mesures de gestion du serveur d'iParamètres		230

Tableau 19 – Informations à inclure dans le manuel de sécurité	245
Tableau 20 – Mesures de sécurité d'un réseau WLAN (IEEE 802.11i).....	248
Tableau 21 – Mesures de sécurité pour Bluetooth (IEEE 802.15.1).....	249
Tableau 22 – Exigences de classe de conformité de l'hôte F	251
Tableau A.1 – Tableau Crctab24 de calcul de la signature CRC 24 bits	254
Tableau A.2 – Tableau Crctab32 de calcul de la signature CRC 32 bits	255
Figure 1 - Relation entre la CEI 61784–3 et d'autres normes (machines)	127
Figure 2 - Relations entre la CEI 61784–3 et d'autres normes (transformation).....	129
Figure 3 – Conditions préalables de communication de base pour le protocole FSCP 3/1 ...	143
Figure 4 – Structure d'un PDU de sécurité FSCP 3/1	144
Figure 5 – Modes de communication de sécurité.....	145
Figure 6 – Système de transmission CPF 3 standard	148
Figure 7 – Architecture de la couche de sécurité.....	149
Figure 8 – Couches de communication de base	150
Figure 9 – Structure de bus de commutateur à plusieurs ports.....	151
Figure 10 – Structure de bus linéaire	152
Figure 11 – Croisement des limites du réseau avec les routeurs	152
Figure 12 – Voies de transmission de sécurité complètes	154
Figure 13 – Modèle de dispositif	155
Figure 14 – Relations d'application d'un dispositif modulaire.....	156
Figure 15 – Relations d'application et de communication (AR/CR)	157
Figure 16 – Format de message	158
Figure 17 – Structure de communication FSCP 3/1	160
Figure 18 – Interface utilisateur F des instances du pilote de l'hôte F	161
Figure 19 – Interfaces du pilote du dispositif F.....	164
Figure 20 – PDU de sécurité pour CPF 3	167
Figure 21 – Octet d'état	168
Figure 22 – Octet de contrôle.....	168
Figure 23 – Fonction du bit de basculement.....	169
Figure 24 – Numéro consécutif du dispositif F.....	170
Figure 25 – Génération de CRC2 (sortie de l'hôte F).....	172
Figure 26 – Détails du calcul CRC2 (ordre inverse).....	172
Figure 27 – Relation de communication de la couche de sécurité	173
Figure 28 – Diagramme d'états de l'hôte F.....	174
Figure 29 – Diagramme d'états du dispositif F	178
Figure 30 – Interaction de l'hôte F et du dispositif F pendant le démarrage.....	182
Figure 31 – Interaction de l'hôte F et du dispositif F pendant la mise hors tension de l'hôte F → sous tension	183
Figure 32 – Interaction de l'hôte F et du dispositif F pendant un report de mise sous tension.....	184
Figure 33 – Interaction de l'hôte F et du dispositif F pendant la mise hors tension → sous tension	186

Figure 34 – Interaction de l'hôte F et du dispositif F lorsque l'hôte détecte une erreur CRC	187
Figure 35 – Interaction de l'hôte F et du dispositif F lorsque le dispositif détecte une erreur CRC	189
Figure 36 – Impact du signal de réinitialisation du compteur	189
Figure 37 – Surveillance de la durée d'acheminement du message Hôte F ↔ Sortie F	190
Figure 38 – Surveillance de la durée d'acheminement du message Entrée F ↔ Hôte F	191
Figure 39 – Données de paramètre F et CRC	194
Figure 40 – Déblocage de l'attribution d'iParamètre par l'hôte F	197
Figure 41 – F_Prm_Flag1	199
Figure 42 – F_Check_SeqNr	199
Figure 43 – F_Check_iPar	199
Figure 44 – F_SIL	200
Figure 45 – F_CRC_Length	200
Figure 46 – F_Prm_Flag2	200
Figure 47 – F_Block_ID	201
Figure 48 – F_Par_Version	201
Figure 49 – Paramètre F	202
Figure 50 – Bloc iParamètre	204
Figure 51 – Extension du paramètre F dans la spécification GSDML	206
Figure 52 – CRC1 incluant iPar_CRC	207
Figure 53 – Algorithme de génération de CRC0	208
Figure 54 – Section DataItem de F_IN_OUT_1	210
Figure 55 – Section DataItem de F_IN_OUT_2	210
Figure 56 – Section DataItem de F_IN_OUT_5	211
Figure 57 – Section DataItem de F_IN_OUT_6	211
Figure 58 – Pilote de canal F en tant que « colle » entre le dispositif F et le programme utilisateur	212
Figure 59 – Exemple de présentation d'un pilote de canal F	213
Figure 60 – Attribution du paramètre F pour de simples dispositifs F et esclaves F	215
Figure 61 – Attribution de paramètre F et d'iParamètre pour les dispositifs F complexes	217
Figure 62 – Intégration système des outils CPD	219
Figure 63 – Mécanisme de serveur d'iParamètres (mise en service)	220
Figure 64 – Principe de fonctionnement du serveur d'iParamètres (remplacement du dispositif F, par exemple)	221
Figure 65 – Codage de la demande de serveur d'iParamètres (« modèle d'état »)	223
Figure 66 – Codage de SR_Type	224
Figure 67 – Codage de la demande de serveur d'iParamètres (« modèle d'alarme »)	225
Figure 68 – Diagramme d'états du serveur d'iParamètres	228
Figure 69 – Exemple de fonction de sécurité avec chemin de temps de réponse critique	232
Figure 70 – Modèle simplifié de temps de réponse classique	233
Figure 71 – Distributions de fréquence des temps de réponse classiques du modèle	233
Figure 72 – Contexte de délais et de temps de fonctionnement du chien de garde	235
Figure 73 – Sections de temporisation formant le F_WD_Time de FSCP 3/1	236

Figure 74 – Distribution de fréquence des temps de réponse avec relances de message	237
Figure 75 – Relances avec CP 3/1	238
Figure 76 – Relances avec CP 3/RTE	239
Figure 77 – Probabilités d'erreurs résiduelles du polynôme 24 bits	240
Figure 78 – Exactitude du polynôme 32 bits pour 52 octets	241
Figure 79 – Exactitude du polynôme 32 bits pour 132 octets	242
Figure 80 – Contrôle des messages corrompus	243
Figure 81 – Sécurité des réseaux WLAN	247
Figure 82 – Sécurité des réseaux Bluetooth	249
Figure A.83 – Procédure « C » classique de contrôle de redondance cyclique	253
Figure A.84 – Comparaison du modèle de temps de réponse et d'une application réelle	256
Figure A.85 – Distribution de fréquence des temps de réponse mesurés	257
Figure A.86 – Hôte F avec programmes d'application standard et programmes d'application relatifs à la sécurité	258

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

RÉSEAUX DE COMMUNICATIONS INDUSTRIELS – PROFILS –

Partie 3-3: Bus de terrain de sécurité fonctionnelle – Spécifications supplémentaires pour CPF 3

AVANT-PROPOS

- 1) La Commission Electrotechnique Internationale (CEI) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de la CEI). La CEI a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, la CEI – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de la CEI"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec la CEI, participent également aux travaux. La CEI collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
- 2) Les décisions ou accords officiels de la CEI concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de la CEI intéressés sont représentés dans chaque comité d'études.
- 3) Les Publications de la CEI se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de la CEI. Tous les efforts raisonnables sont entrepris afin que la CEI s'assure de l'exactitude du contenu technique de ses publications; la CEI ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
- 4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de la CEI s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de la CEI dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de la CEI et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
- 5) La CEI elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de la CEI. La CEI n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
- 6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
- 7) Aucune responsabilité ne doit être imputée à la CEI, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de la CEI, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de la CEI ou de toute autre Publication de la CEI, ou au crédit qui lui est accordé.
- 8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
- 9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de la CEI peuvent faire l'objet de droits de brevet. La CEI ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

La commission électrotechnique internationale (CEI) attire l'attention sur le fait qu'il est déclaré que la conformité avec le présent document peut impliquer l'utilisation de brevets concernant les profils de communication de sécurité fonctionnelle pour la famille 3, où la notation [xx] désigne le détenteur des droits de propriété.

EP1267270-A2	[SI]	Verfahren zur Datenübertragung in einem Rechnersystem
WO00/045562-A1	[SI]	Méthode et dispositif pour déterminer la fiabilité d'un support de données
WO99/049373-A1	[SI]	Télégramme de données abrégé d'un système d'automatisation

La CEI ne prend pas position eu égard à la preuve, la validité et la portée de ces droits de propriété.

Les détenteurs de ces droits de propriété ont donné l'assurance à la CEI qu'ils consentent à négocier des licences avec des demandeurs du monde entier, en des termes et à des conditions raisonnables et non discriminatoires. A ce propos, la déclaration des détenteurs de ces droits de propriété est enregistrée à la CEI.

Des informations peuvent être obtenues auprès de:

[SI]	Siemens AG A&D AS FA TC Karlsruhe ALLEMAGNE
------	--

L'attention est attirée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété autres que ceux mentionnés ci-dessus. La CEI ne doit pas être tenue pour responsable de ne pas avoir dûment signalé tout ou partie de ces droits de propriété.

La Norme internationale CEI 61784-3-3 a été établie par le sous-comité 65C: Réseaux de communications industriels, du comité d'études 65 de la CEI: Mesure, commande et automation dans les processus industriels.

La présente version bilingue (2013-05) correspond à la version anglaise monolingue publiée en 2007-12.

Le texte anglais de cette norme est issu des documents 65C/470/FDIS et 65V/481/RVD.

Le rapport de vote 65C/481/RVD donne toute information sur le vote ayant abouti à l'approbation de cette norme.

La version française de cette norme n'a pas été soumise au vote.

Cette publication a été rédigée selon les Directives ISO/CEI, Partie 2.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de stabilité indiquée sur le site web de la CEI sous "<http://webstore.iec.ch>" dans les données relatives à la publication recherchée. A cette date, la publication sera

- reconduite,
- supprimée,
- remplacée par une édition révisée, ou
- amendée.

Une liste de toutes les parties de la série CEI 61784-3, publiées sous le titre général *Réseaux de communications industriels – Profils – Bus de terrain de sécurité fonctionnelle*, est disponible sur le site web de la CEI.

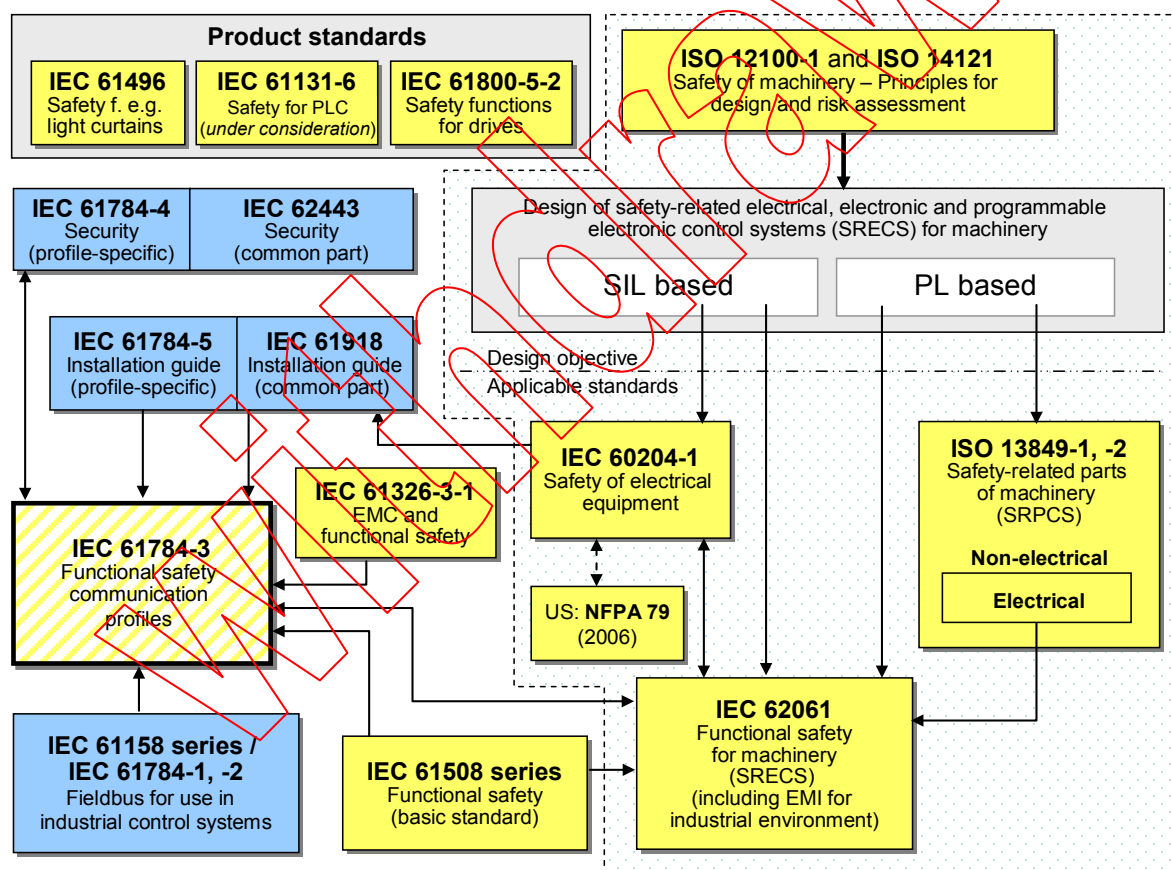
IMPORTANT – Le logo "colour inside" qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

INTRODUCTION

La CEI 61158 relative aux bus de terrain, ainsi que ses normes associées CEI 61784-1 et CEI 61784-2, définit un ensemble de protocoles de communication qui assurent la commande répartie d'applications automatisées. La technologie de bus de terrain est désormais reconnue et bien éprouvée. Ainsi de nombreuses améliorations des bus de terrain se développent pour traiter de domaines non encore normalisés tels que les applications en temps réel relatives à la sécurité et à la sûreté.

La présente norme définit les principes pertinents applicables aux communications en termes de sécurité fonctionnelle en référence à la série CEI 61508, et spécifie plusieurs couches de communication de sécurité (profils et protocoles correspondants) basées sur les profils de communication et les couches de protocole de la CEI 61784-1, de la CEI 61784-2 et de la série CEI 61158. Elle ne couvre pas les aspects relatifs à la sécurité électrique et à la sécurité intrinsèque.

La Figure 1 illustre les relations entre la présente norme et les normes pertinentes relatives à la sécurité et au bus de terrain dans un environnement machines.



Key

- (yellow) safety-related standards
- (blue) fieldbus-related standards
- (dashed yellow) this standard

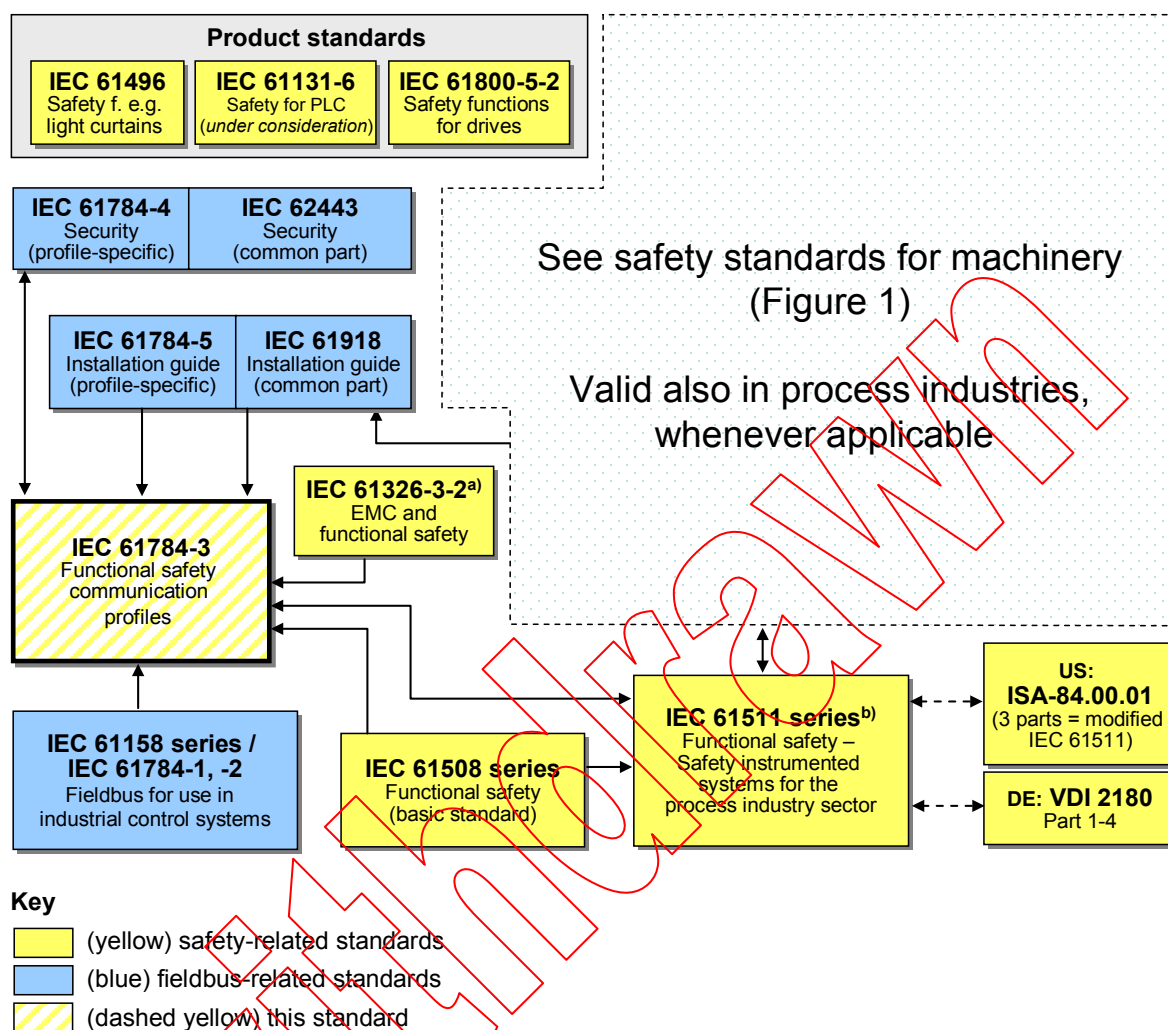
Légende

Anglais	Français
Product standards	Normes de produits

Anglais	Français
Safety function, e.g. light curtains	Fonction de sécurité, par exemple rideaux de lumière
Safety for PLC (under consideration)	Sécurité relative aux automates programmables (à l'étude)
Safety functions for drives	Fonctions de sécurité applicables aux entraînements
Safety of machinery - ... assessment	Sécurité des machines – Principes généraux de conception et appréciation du risque
Security (profile-specific)	Sûreté (spécifique au profil)
Security (common part)	Sûreté (partie commune)
Design of safety-related for machinery	Conception des systèmes de commande électriques, électroniques et électroniques programmables relatifs à la sécurité pour les machines
SIL based	Basé sur SIL
PL based	Basé sur PL
Installation guide (profile-specific)	Guide d'installation (spécifique au profil)
Installation guide (common part)	Guide d'installation (partie commune)
Design objective	Objectif de conception
Applicable standards	Normes applicables
Safety of electrical equipment	Sécurité des équipements électriques
Safety-related parts of machinery	Parties des systèmes de commande relatives à la sécurité
Non-electrical	Non électrique
Electrical	Électrique
Test EMC & functional safety	Essai CEM et sécurité fonctionnelle
Functional safety communication profiles	Profils de communication de sécurité fonctionnelle
IEC 61158 series / Fieldbus for use in industrial control systems	Série CEI 61158 / Bus de terrain pour utilisation dans des systèmes de commande industriels
IEC 61508 series, Functional safety (basic standard)	Série CEI 61508 Sécurité fonctionnelle (norme de base)
Functional safety for machinery for industrial environment)	Sécurité fonctionnelle des systèmes de commande électriques, électroniques et électroniques programmables (y compris les interférences électromagnétiques dans l'environnement industriel)
Key	Légende
(yellow) safety-related standards	(jaune) normes relatives à la sécurité
(blue) fieldbus-related standards	(bleu) normes relatives au bus de terrain
(dashed) yellow) this standard	(jaune pointillé) la présente norme
IEC	CEI

Figure 1 – Relation entre la CEI 61784-3 et d'autres normes (machines)

La Figure 2 illustre les relations entre la présente norme et les normes pertinentes relatives à la sécurité et au bus de terrain dans un environnement de transformation.



Légende

Anglais	Français
Product standards	Normes de produits
Safety function, e.g. light curtains	Fonction de sécurité, par exemple rideaux de lumière
Safety for PLC (under consideration)	Sécurité relative aux automates programmables (à l'étude)
Safety functions for drives	Fonctions de sécurité applicables aux entraînements
Security (profile-specific)	Sûreté (spécifique au profil)
Security (common part)	Sûreté (partie commune)
Installation guide (profile-specific)	Guide d'installation (spécifique au profil)
Installation guide (common part)	Guide d'installation (partie commune)
See safety standards for machinery (Figure 1)	Voir normes de sécurité pour les machines (Figure 1)
Valid also ... applicable	Valable également dans les industries de transformation, le cas échéant
Functional safety communication profiles	Profils de communication de sécurité fonctionnelle
EMC and functional safety	CEM et sécurité fonctionnelle

Anglais	Français
IEC 61158 series Fieldbus for use in industrial control systems	Série CEI 61158/CEI 61784-1,-2 Bus de terrain pour utilisation dans des systèmes de commande industriels
IEC 61508 series, Functional safety (basic standard)	Série CEI 61508 Sécurité fonctionnelle (norme de base)
IEC 61511 series Functional safety ... sector	Série CEI 61511 ^{b)} Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur des industries de transformation
(3 parts = modified IEC 61511)	(3 parties = CEI 61511 modifiée)
Part 1 –4	Parties 1 à 4
Key	Légende
(yellow) safety-related standards	(jaune) normes relatives à la sécurité
(blue) fieldbus-related standards	(bleu) normes relatives au bus de terrain
(dashed) yellow) this standard	(jaune pointillé) la présente norme
IEC	CEI

^a Pour des environnements électromagnétiques spécifiés, sinon CEI 61326-3-1.

^b EN ratifiée.

Figure 2 – Relations entre la CEI 61784-3 et d'autres normes (transformation)

Les couches de communication de sécurité mises en œuvre dans le cadre de systèmes relatifs à la sécurité conformément à la série CEI 61508, assurent la confiance nécessaire à accorder à la transmission de messages (information) entre deux participants ou plus sur un bus de terrain dans un système relatif à la sécurité, ou une fiabilité suffisante dans le comportement de sécurité en cas d'erreurs ou de défaillances du bus de terrain.

Les couches de communication de sécurité spécifiées dans la présente norme permettent de garantir cette assurance en utilisant un bus de terrain dans des applications nécessitant une sécurité fonctionnelle jusqu'au niveau d'intégrité de sécurité (SIL) spécifié par son profil de communication de sécurité fonctionnelle correspondant.

La revendication du SIL qui en résulte pour un système dépend de la mise en œuvre du profil de communication de sécurité fonctionnelle retenu au sein du système – la mise en œuvre du profil de communication de sécurité fonctionnelle dans un dispositif normal ne suffit pas à le qualifier de dispositif de sécurité.

La présente norme décrit:

- les principes de base de mise en œuvre des exigences de la série CEI 61508 pour les communications de données relatives à la sécurité, y compris les défauts de transmission potentiels, les mesures correctives et les considérations concernant l'intégrité des données;
- la description individuelle des profils de sécurité fonctionnelle pour plusieurs familles de profils de communication dans la CEI 61784-1 et la CEI 61784-2;
- les extensions de la couche de sécurité aux sections relatives au service et aux protocoles de communication de la série CEI 61158.

RÉSEAUX DE COMMUNICATIONS INDUSTRIELS – PROFILS –

Partie 3-3: Bus de terrain de sécurité fonctionnelle – Spécifications supplémentaires pour CPF 3

1 Domaine d'application

La présente partie de la série CEI 61784-3 spécifie une couche de communication relative à la sécurité (services et protocole) fondée sur la CPF 3 de la CEI 61784-1 et les types 3 et 10 de la CEI 61784-2 (CP 3/1, CP 3/2, CP 3/4, CP 3/5 et CP 3/6) et de la CEI 61158. Elle identifie les principes applicables aux communications de sécurité fonctionnelle définies dans la CEI 61784-3, et appropriés à cette couche de communication de sécurité.

NOTE 1 Elle ne couvre pas les aspects relatifs à la sécurité électrique et à la sécurité intrinsèque. La sécurité électrique concerne les dangers tels que les chocs électriques. La sécurité intrinsèque concerne les dangers associés aux atmosphères explosibles.

La présente partie¹ définit les mécanismes de transmission des messages propres à la sécurité entre les participants d'un réseau réparti, en utilisant la technologie de bus de terrain conformément aux exigences de la série CEI 61508 concernant la sécurité fonctionnelle. Ces mécanismes peuvent être utilisés dans diverses applications industrielles, telles que la commande de processus, l'usinage automatique et les machines.

La présente partie fournit des lignes directrices tant pour les développeurs que pour les évaluateurs de dispositifs et systèmes conformes.

NOTE 2 La revendication du SIL qui en résulte pour un système dépend de la mise en œuvre du profil de communication de sécurité fonctionnelle retenu au sein du système – la mise en œuvre du profil de communication de sécurité fonctionnelle, conforme à la présente partie, dans un dispositif normal ne suffit pas à le qualifier de dispositif de sécurité.

2 Références normatives

Les documents de référence suivants sont indispensables pour l'application du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

IEC 61010-1, *Safety requirements for electrical equipment for measurement, control, and laboratory use – Part 1: General requirements* (disponible en anglais seulement)

IEC 61131-2, *Programmable controllers – Part 2: Equipment requirements and tests* (disponible en anglais seulement)

IEC 61131-3, *Programmable controllers – Part 3: Programming languages* (disponible en anglais seulement)

IEC 61158 (all parts), *Industrial communication networks – Fieldbus specifications* (disponible en anglais seulement)

¹ Dans les pages suivantes de la présente norme, "la présente partie" se substitue à "cette partie de la série CEI 61784-3".

IEC 61158-2, *Industrial communication networks – Fieldbus specifications – Part 2: Physical layer specification and service definition* (disponible en anglais seulement)

IEC 61158-3-3, *Industrial communication networks – Fieldbus specifications – Part 3-3: Data-link layer service definition* (disponible en anglais seulement)

IEC 61158-4-3, *Industrial communication networks – Fieldbus specifications – Part 4-3: Data-link layer protocol specification* (disponible en anglais seulement)

IEC 61158-5-3, *Industrial communication networks – Fieldbus specifications – Part 5-3: Application layer service definition* (disponible en anglais seulement)

IEC 61158-5-10, *Industrial communication networks – Fieldbus specifications – Part 5-10: Application layer service definition* (disponible en anglais seulement)

IEC 61158-6-3, *Industrial communication networks – Fieldbus specifications – Part 4-3: Application layer protocol specification* (disponible en anglais seulement)

IEC 61158-6-10, *Industrial communication networks – Fieldbus specifications – Part 4-10: Application layer protocol specification* (disponible en anglais seulement)

CEI 61326-3-1, *Matériel électrique de mesure, de commande et de laboratoire – Exigences relatives à la CEM – Partie 3-1: Exigences d'immunité pour les systèmes relatifs à la sécurité et pour les matériels destinés à réaliser des fonctions relatives à la sécurité (sécurité fonctionnelle) – Applications industrielles générales²*

CEI 61326-3-2, *Matériel électrique de mesure, de commande et de laboratoire – Exigences relatives à la CEM – Partie 3-2: Exigences d'immunité pour les systèmes relatifs à la sécurité et pour les matériels destinés à réaliser des fonctions relatives à la sécurité (sécurité fonctionnelle) – Applications industrielles dont l'environnement électromagnétique est spécifié*

CEI 61508 (toutes les parties), *Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité*

CEI 61511 (toutes les parties), *Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur des industries de transformation*

IEC 61784-1, *Industrial communication networks – Profiles – Part 1: Fieldbus profiles* (disponible en anglais seulement)

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

IEC 61784-3, *Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions* (disponible en anglais seulement)

IEC 61784-5-3, *Industrial communication networks – Profiles – Part 5: Installation of fieldbuses – Installation profiles for CPF 3* (disponible en anglais seulement)

IEC 61918, *Industrial communication networks – Installation of communication networks in industrial premises* (disponible en anglais seulement)

CEI 62061, *Sécurité des machines – Sécurité fonctionnelle des systèmes de commande électriques, électroniques et électroniques programmables relatifs à la sécurité*

² A publier.

CEI 62280-1:2002, *Applications ferroviaires – Systèmes de signalisation, de télécommunication et de traitement – Partie 1: Communication de sécurité sur des systèmes de transmission fermés*

CEI 62280-2, *Applications ferroviaires – Systèmes de signalisation, de télécommunication et de traitement – Partie 2: Communication de sécurité sur des systèmes de transmission ouverts*

IEC/TR 62390, *Common automation device – Profile guideline* (disponible en anglais seulement)

ISO 13849-1, *Sécurité des machines – Parties des systèmes de commande relatives à la sécurité – Partie 1: Principes généraux de conception*

ISO 15745-3, *Systèmes d'automatisation industrielle et intégration – Cadre d'application d'intégration pour les systèmes ouverts – Partie 3: Description de référence pour les systèmes de contrôle fondés sur la CEI 61158*

ISO 15745-4, *Systèmes d'automatisation industrielle et intégration – Cadre d'application d'intégration pour les systèmes ouverts – Partie 4: Description de référence pour les systèmes de contrôle fondés sur Ethernet – Amendement 1: profils PROFINET*

Withdrawing