

INTERNATIONAL STANDARD

NORME INTERNATIONALE



**Industrial communication networks – Profiles –
Part 3-6: Functional safety fieldbuses – Additional specifications for CPF 6**

**Réseaux de communications industriels – Profils –
Partie 3-6: Bus de terrain de sécurité fonctionnelle – Spécifications
supplémentaires pour la CPF 6**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

PRICE CODE
CODE PRIX

XC

ICS 25.040; 35.100.05

ISBN 978-2-8322-0845-8

**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.....	7
INTRODUCTION.....	9
1 Scope.....	12
2 Normative references	12
3 Terms, definitions, symbols, abbreviated terms and conventions	13
3.1 Terms and definitions	13
3.1.1 Common terms and definitions	13
3.1.2 CPF 6: Additional terms and definitions	17
3.2 Symbols and abbreviated terms.....	18
3.2.1 Common symbols and abbreviated terms	18
3.2.2 CPF 6: Additional symbols and abbreviated terms	18
3.3 Conventions	19
4 Overview of FSCP 6/7 (INTERBUS™ Safety)	19
4.1 General.....	19
4.2 Technical overview.....	19
4.3 Functional Safety Communication Profile 6/7.....	20
5 General	21
5.1 External documents providing specifications for the profile.....	21
5.2 Safety functional requirements.....	21
5.3 Safety measures	21
5.3.1 General.....	21
5.3.2 Sequence number	22
5.3.3 Time stamp	22
5.3.4 Time expectation	22
5.3.5 Acknowledgement	22
5.3.6 Connection authentication	22
5.3.7 Distinction between safety relevant messages and non-safety relevant messages – different data integrity assurance system.....	23
5.3.8 Parameterized shutdown time.....	23
5.4 Safety communication layer structure	23
5.4.1 Decomposition process.....	23
5.4.2 Definition of the safety function of the safety communication system	24
5.4.3 Decomposition of the safety function of a safety communication system into function blocks.....	25
5.4.4 Assignment of the function blocks to subsystems	26
5.4.5 Safety requirements and safety integrity requirements.....	29
5.4.6 Specification of the safe state.....	29
5.4.7 Response to a fault	30
5.4.8 Stop category.....	32
5.4.9 Safe Transmission.....	32
5.5 Relationships with FAL (and DLL, PhL)	33
5.5.1 Overview	33
5.5.2 Use of the AR-US service to initiate and parameterize.....	33
5.5.3 Use of the AR-US service to transmit safety data	34
5.5.4 Use of the AR-US service to abort	35
5.5.5 Data types	35

6	Safety communication layer services	35
6.1	General	35
6.2	Transmission principle for safety messages between SCLM and SCLS	35
6.3	Function block requirements	36
6.3.1	Input Safe Data function block	36
6.3.2	Output Safe Data function block	36
6.3.3	Safe Calculation function block	36
6.4	Context management	37
6.4.1	Initiate service	37
6.4.2	Abort service	38
6.5	Function block parameterization	39
6.5.1	Send application parameter service	39
6.5.2	Send application parameter ID service	40
6.5.3	Parameterize device service	41
6.6	Safe Process Data Mode	41
6.6.1	Transmit-Safety-Data	41
6.6.2	Set-Diagnostic-Data service	43
6.6.3	Set-Acknowledgement-Data service	43
7	Safety communication layer protocol	44
7.1	Safety PDU format	44
7.1.1	Structure of safety messages	44
7.1.2	Description of the polynomial used	45
7.1.3	Structure of safety messages for safe parameterization and idle	45
7.1.4	Structure of safety messages for the transmission of safety data	51
7.1.5	Messages for synchronization	52
7.1.6	Structure of safety messages for aborting connections	53
7.2	State description	54
7.2.1	SCLM and SCLS state machines	54
7.2.2	Initiate	55
7.2.3	Parameterization	56
7.2.4	Process data mode	59
7.2.5	Process data mode with diagnostic data transmission	64
7.2.6	Process data mode with Acknowledgement-Data transmission	65
7.2.7	Connection aborted	66
7.3	Abort	66
7.3.1	Connection abort in the event of an error detected by the SCLM	66
7.3.2	Abort of all connections in the event of an error detected by the SCLS	67
7.3.3	Abort of all connections in the event of an error detected by the SCLM	69
8	Safety communication layer management	70
8.1	General	70
8.2	Requirements of safety communication layer management	70
8.3	Set-Safety-Configuration service	70
8.4	Start IEC 61158 Type 8 service	72
9	System requirements	72
9.1	Indicators and switches	72
9.2	Installation guidelines	72
9.3	Safety function response time	72

9.3.1	General	72
9.3.2	Calculation of the parameterized shutdown time	73
9.4	Duration of demands	77
9.5	Constraints for calculation of system characteristics	77
9.5.1	System characteristics	77
9.5.2	Calculation of the number of telegrams per second	77
9.6	Maintenance	78
9.7	Safety manual	79
10	Certification	79
	Bibliography	80

Table 1	– Overview of profile identifier usable for FSCP 6/7	21
Table 2	– Selection of the various measures for possible errors	22
Table 3	– List of function blocks and subsystems	26
Table 4	– Signal flow between the function blocks	28
Table 5	– Initiate service parameters	37
Table 6	– Parameterization mode and related services	38
Table 7	– Abort service parameters	38
Table 8	– Abort of a point-to-point connection by the SRP or SRC	39
Table 9	– Send application parameter service	39
Table 10	– Send application parameter ID service	40
Table 11	– Parameterize device parameters	41
Table 12	– Transmit-Safety-Data service parameters	42
Table 13	– Set-Diagnostic-Data service parameters	43
Table 14	– Set-Acknowledgement-Data service parameters	44
Table 15	– Parameter ID	47
Table 16	– Block 0: Device ID	48
Table 17	– Block 1: Parameter record ID	49
Table 18	– Block 2: Application parameter	49
Table 19	– TIME encoding	52
Table 20	– Abort_Info: Connection abort in the event of an error detected by the SCLM	67
Table 21	– Abort_Info: Abort of all connections in the event of an error detected by the SCLS	68
Table 22	– Abort_Info: Abort of all connections in the event of an error detected by the SCLM	70
Table 23	– Set-Safety-Configuration service	71
Table 24	– Error_Info	71
Table 25	– Calculation of t_{IB}	76
Table 26	– Calculation of t_{SRC}	77
Table 27	– Calculation of t_{PST}	77

Figure 1	– Relationships of IEC 61784-3 with other standards (machinery)	9
----------	---	---

Figure 2	– Relationships of IEC 61784-3 with other standards (process)	10
----------	---	----

Figure 3 – FSCP 6/7 communication preconditions	20
Figure 4 – Example of a safety function	24
Figure 5 – Decomposition of safety function into function blocks	25
Figure 6 – Overview of the results of the decomposition process	27
Figure 7 – Signal flow between the function blocks	27
Figure 8 – Interfaces between the safety devices within the safety communication system	28
Figure 9 – Signal flow and safe states	30
Figure 10 – Mapping of the Safe Transmission function block	32
Figure 11 – Relationship between SCL and the other layers of IEC 61158 Type 8	33
Figure 12 – Use of the AR-US service to initiate and parameterize	34
Figure 13 – Use of the AR-US service to transmit safety data	34
Figure 14 – Use of the AR-US service to abort	35
Figure 15 – Use of the AR-US service to abort	35
Figure 16 – Structure of the safety PDU	44
Figure 17 – Integration of safety data and deterministic remedial measures in the summation frame	45
Figure 18 – Write_Parameter_Byte_Req message	46
Figure 19 – Read_Parameter_Byte_Req message	46
Figure 20 – Parameter_Byte_Con message	46
Figure 21 – Set_Safety_Connection_ID_Req message	50
Figure 22 – Set_Safety_Connection_ID_Con message of safety slaves	50
Figure 23 – Parameter_Idle_Req	50
Figure 24 – Parameter_Idle_Con	50
Figure 25 – Parameter_Check_Con	51
Figure 26 – Parameter_Loc_ID_Changed_Con	51
Figure 27 – Transmit Safety Data Message	51
Figure 28 – Sync_a message of the SCLM	52
Figure 29 – Req_b message of the SCLM	53
Figure 30 – Req_c message of the SCLM	53
Figure 31 – Req_d message of the SCLM	53
Figure 32 – Abort_Connection message	54
Figure 33 – Safety-Slave_Error message	54
Figure 34 – SCLM state machine	54
Figure 35 – SCLS state machine	55
Figure 36 – Initiate sequence	56
Figure 37 – Send Application Parameter sequence	57
Figure 38 – Send Application Parameter ID sequence	58
Figure 39 – Parameterize device sequence	59
Figure 40 – Simultaneous transmission of safety data to the safety slaves	60
Figure 41 – Use of the sequence number in the SCLM and SCLS	61
Figure 42 – Startup and error-free operation	62
Figure 43 – Resynchronization during operation	63
Figure 44 – Invalid CRC 24 checksum detected by the SCLS	64

Figure 45 – Process data mode with diagnostic data transmission	65
Figure 46 – Process data mode with Acknowledgement-Data transmission	66
Figure 47 – Error when initiating a connection	67
Figure 48 – Error at an SCLS when aborting all connections.....	68
Figure 49 – Abort of all connections in the event of an error detected by the SCLM	69
Figure 50 – Overview of the shutdown time.....	74

Withdrawn

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**INDUSTRIAL COMMUNICATION NETWORKS –
PROFILES –****Part 3-6: Functional safety fieldbuses –
Additional specifications for CPF 6**

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 6 as follows, where the [xx] notation indicates the holder of the patent right:

DE 103 25 263 A1	[PxC]	Sicherstellung von maximalen Reaktionszeiten in komplexen oder verteilten sicheren und/oder nicht sicheren Systemen
DE 103 18 068 A1	[PxC]	Verfahren und Vorrichtung zum Paket-orientierten Übertragen sicherheitsrelevanter Daten

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:

[PxC]

Phoenix Contact GmbH & Co. KG
Intellectual Property Licenses &
Standards
Flachsmarktstr. 8
D-32825 Blomberg,
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 61784-3-6 has been prepared by subcommittee 65C: Industrial networks, of IEC technical committee 65: Industrial process measurement, control and automation.

This bilingual version (2013-07) 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.

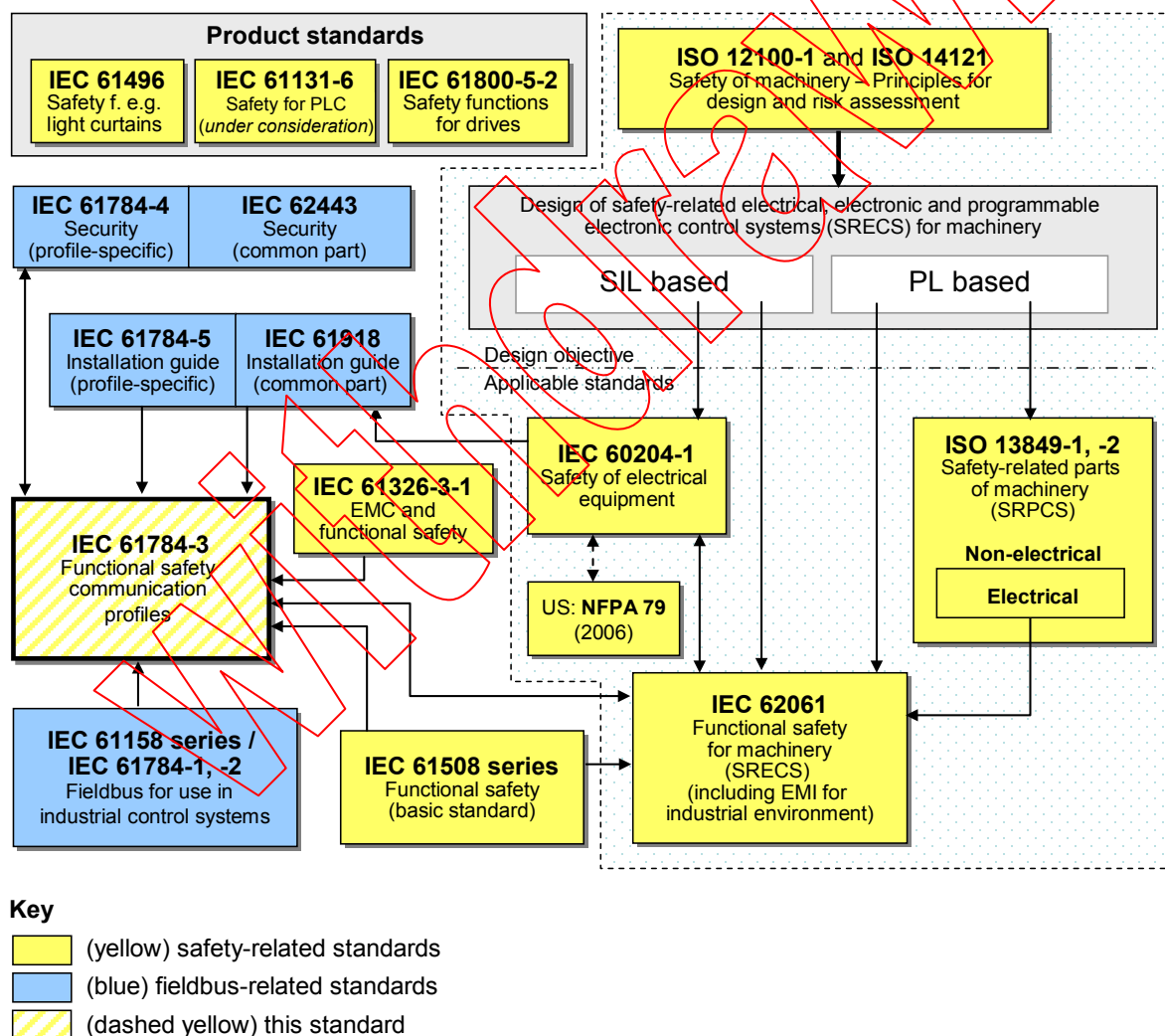
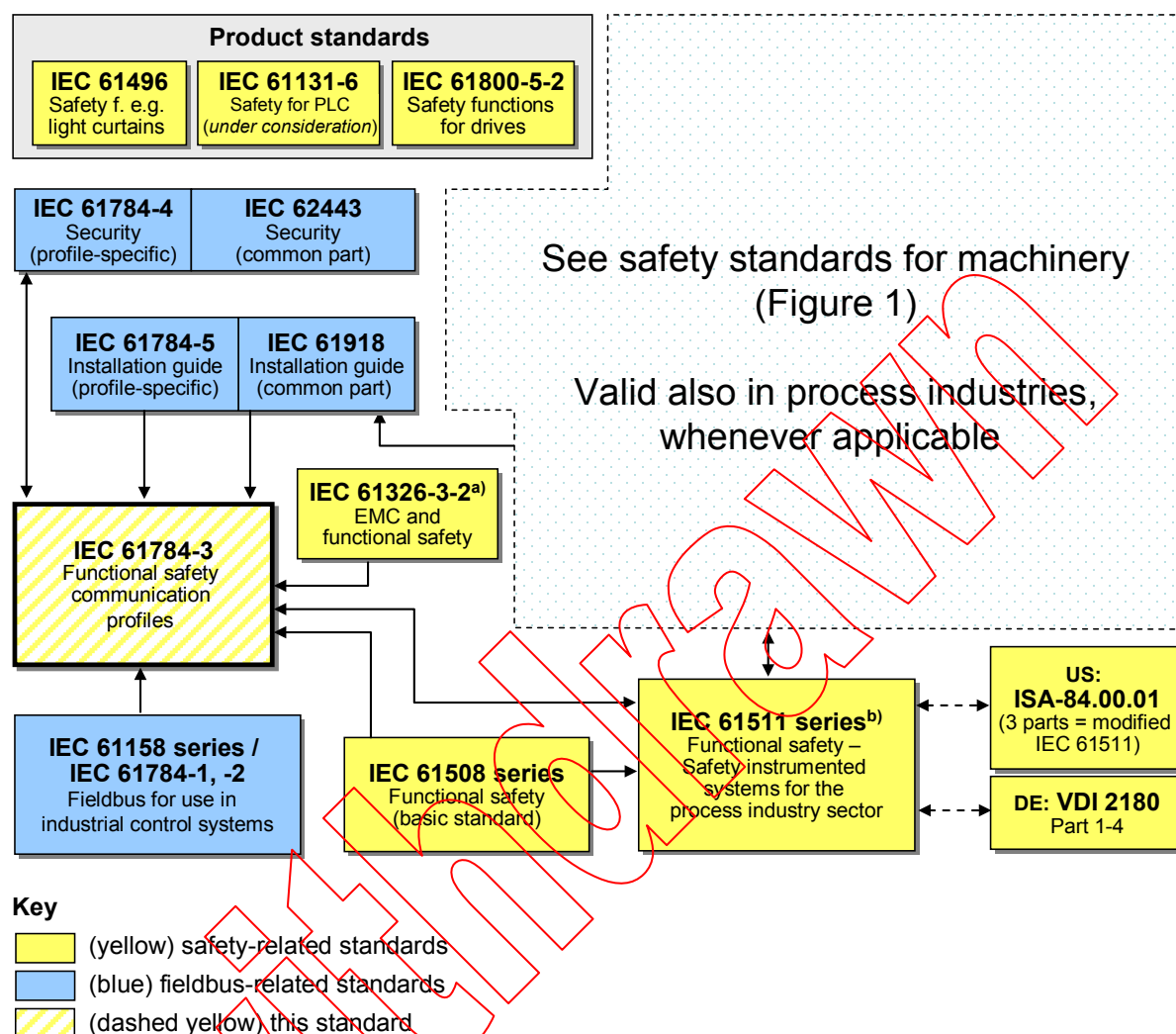


Figure 1 – Relationships of IEC 61784-3 with other standards (machinery)

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 3-6: Functional safety fieldbuses – Additional specifications for CPF 6

1 Scope

This part of the IEC 61784-3 series specifies a safety communication layer (services and protocol) based on CPF 6 of IEC 61784-1, IEC 61784-2 and IEC 61158 Type 8. 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 61131-3, *Programmable controllers – Part 3: Programming languages*

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

IEC 61158-3-8, *Industrial communication networks – Fieldbus specifications – Part 3-8: Data-link layer service definition*

IEC 61158-4-8, *Industrial communication networks – Fieldbus specifications – Part 4-8: Data-link layer protocol specification*

IEC 61158-5-8, *Industrial communication networks – Fieldbus specifications – Part 5-8: Application layer service definition*

IEC 61158-6-8, *Industrial communication networks – Fieldbus specifications – Part 6-8: Application 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 61508 (all parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

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 61784-5-6, *Industrial communication networks – Profiles – Part 5: Installation of fieldbuses – Installation profiles for CPF 6*

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*

Withdrawn

SOMMAIRE

AVANT-PROPOS	89
INTRODUCTION.....	91
1 Domaine d'application	95
2 Références normatives.....	95
3 Termes, définitions, symboles, abréviations et conventions	96
3.1 Termes et définitions	96
3.1.1 Termes et définitions communs	96
3.1.2 CPF 6: Termes et définitions supplémentaires	100
3.2 Symboles et abréviations	101
3.2.1 Symboles et abréviations communs.....	101
3.2.2 CPF 6: Symboles et abréviations supplémentaires	101
3.3 Conventions	102
4 Présentation de FSCP 6/7 (INTERBUS™ Safety)	102
4.1 Généralités.....	102
4.2 Présentation générale d'ordre technique	103
4.3 Profil de communication de sécurité fonctionnelle 6/7.....	104
5 Généralités.....	104
5.1 Documents externes de spécifications applicables au profil.....	104
5.2 Exigences fonctionnelles de sécurité.....	104
5.3 Mesures de sécurité	105
5.3.1 Généralités	105
5.3.2 Numéro de séquence.....	106
5.3.3 Datation (horodatage).....	106
5.3.4 Délai.....	106
5.3.5 Acquiescement	106
5.3.6 Authentification de connexion	106
5.3.7 Distinction entre les messages relatifs et non relatifs à la sécurité – différents systèmes d'assurance d'intégrité des données.....	106
5.3.8 Temps d'arrêt paramétré	106
5.4 Structure de la couche de communication de sécurité	107
5.4.1 Processus de décomposition	107
5.4.2 Définition de la fonction de sécurité du système de communication de sécurité	107
5.4.3 Décomposition de la fonction de sécurité d'un système de communication de sécurité en blocs de fonction	108
5.4.4 Attribution des blocs de fonction aux sous-systèmes	110
5.4.5 Exigences de sécurité et exigences d'intégrité de sécurité.....	114
5.4.6 Spécification de l'état de sécurité	114
5.4.7 Réponse à une panne.....	116
5.4.8 Catégorie d'arrêt	117
5.4.9 Transmission sécurisée	118
5.5 Relations avec la FAL (et DLL, PhL).....	119
5.5.1 Présentation générale	119
5.5.2 Utilisation du service AR-US pour le démarrage et le paramétrage	119
5.5.3 Utilisation du service AR-US pour la transmission des données de sécurité	120
5.5.4 Utilisation du service AR-US pour l'abandon.....	121

5.5.5	Types de données	121
6	Services de la couche de communication de sécurité	121
6.1	Généralités.....	121
6.2	Principe de transmission des messages de sécurité entre le SCLM et le SCLS	121
6.3	Exigences relatives au bloc de fonction	122
6.3.1	Bloc de fonction Données d'entrée sécurisées.....	122
6.3.2	Bloc de fonction Données de sortie sécurisées	122
6.3.3	Bloc de fonction Calcul sécurisé	122
6.4	Gestion de contexte	123
6.4.1	Service Initiate	123
6.4.2	Service Abort (Abandon)	124
6.5	Paramétrage du bloc de fonction	125
6.5.1	Service Send Application Parameter (Envoi du paramètre d'application).....	125
6.5.2	Service Send Application Parameter ID (Envoi de l'ID du paramètre d'application).....	126
6.5.3	Service Parameterize Device.....	127
6.6	Mode de données de processus sécurisé	127
6.6.1	Transmit-Safety-Data (Transmission de données de sécurité)	127
6.6.2	Service Set-Diagnostic-Data (Définition des données de diagnostic)	129
6.6.3	Service Set-Acknowledgement-Data (Définition des données d'acquittement).....	129
7	Protocole de couche de communication de sécurité.....	130
7.1	Format PDU de sécurité	130
7.1.1	Structure des messages de sécurité	130
7.1.2	Description du polynôme utilisé	131
7.1.3	Structure des messages de sécurité du paramétrage sécurisé et de l'état de repos	131
7.1.4	Structure des messages de sécurité pour la transmission des données de sécurité.....	137
7.1.5	Messages de synchronisation.....	138
7.1.6	Structure des messages de sécurité d'abandon des connexions.....	140
7.2	Description d'état	140
7.2.1	Diagrammes d'états du SCLM et du SCLS.....	140
7.2.2	Initiate (Lancement).....	142
7.2.3	Paramétrage.....	144
7.2.4	Mode de données de processus	150
7.2.5	Mode de données de processus avec transmission de données de diagnostic.....	155
7.2.6	Mode de données de processus avec transmission de données d'acquittement.....	156
7.2.7	Connexion abandonnée	157
7.3	Abort (Abandon).....	157
7.3.1	Abandon de connexion en cas d'erreur détectée par le SCLM	157
7.3.2	Abandon de toutes les connexions en cas d'erreur détectée par le SCLS.....	158
7.3.3	Abandon de toutes les connexions en cas d'erreur détectée par le SCLM	160
8	Gestion de la couche de communication de sécurité.....	162
8.1	Généralités.....	162

8.2	Exigences en matière de gestion de la couche de communication de sécurité	162
8.3	Service Set-Safety-Configuration.....	162
8.4	Service Start IEC 61158 Type 8	163
9	Exigences système.....	163
9.1	Voyants et commutateurs	163
9.2	Lignes directrices d'installation.....	163
9.3	Temps de réponse de la fonction de sécurité.....	164
9.3.1	Généralités.....	164
9.3.2	Calcul du temps d'arrêt paramétré	164
9.4	Durée des demandes	168
9.5	Contraintes liées au calcul des caractéristiques des systèmes	169
9.5.1	Caractéristiques des systèmes	169
9.5.2	Calcul du nombre de messages par seconde	169
9.6	Maintenance.....	170
9.7	Manuel de sécurité	170
10	Certification	170
	Bibliographie.....	172
	Tableau 1 – Présentation générale de l'identifiant de profil applicable au protocole FSCP 6/7	104
	Tableau 2 – Sélection des différentes mesures correspondant aux erreurs possibles.....	105
	Tableau 3 – Liste des blocs de fonction et des sous-systèmes.....	110
	Tableau 4 – Flux de signal entre les blocs de fonction	113
	Tableau 5 – Paramètres du service Initiate	123
	Tableau 6 – Mode de paramétrage et services connexes	124
	Tableau 7 – Paramètres du service Abort	124
	Tableau 8 – Abandon d'une connexion point à point par le SRP ou le SRC.....	125
	Tableau 9 – Service Send Application Parameter.....	125
	Tableau 10 – Service Send Application Parameter ID	126
	Tableau 11 – Paramètres du service Parameterize Device.....	127
	Tableau 12 – Paramètres du service Transmit-Safety-Data.....	128
	Tableau 13 – Paramètres du service Set-Diagnostic-Data.....	129
	Tableau 14 – Paramètres du service Set-Acknowledgement-Data.....	130
	Tableau 15 – ID de paramètre	133
	Tableau 16 – Bloc 0: ID de dispositif.....	134
	Tableau 17 – Bloc 1: ID d'enregistrement de paramètre.....	135
	Tableau 18 – Bloc 2: Paramètre d'application	135
	Tableau 19 – Codage TIME	138
	Tableau 20 – Abort_Info: Abandon de connexion en cas d'erreur détectée par le SCLM	158
	Tableau 21 – Abort_Info: Abandon de toutes les connexions en cas d'erreur détectée par le SCLS	160
	Tableau 22 – Abort_Info: Abandon de toutes les connexions en cas d'erreur détectée par le SCLM.....	161
	Tableau 23 – Service Set-Safety-Configuration.....	162
	Tableau 24 – Error_Info	163
	Tableau 25 – Calcul de t_{IB}	168

Tableau 26 – Calcul de t_{SRC}	168
Tableau 27 – Calcul de t_{SRC}	168
Figure 1 – Relation entre la CEI 61784–3 et d’autres normes (machines)	92
Figure 2 – Relation entre la CEI 61784–3 et d’autres normes (procédés industriels)	94
Figure 3 – Conditions préalables de communication FSCP 6/7	103
Figure 4 – Exemple de fonction de sécurité	108
Figure 5 – Décomposition de la fonction de sécurité en blocs de fonction	109
Figure 6 – Présentation des résultats du processus de décomposition	111
Figure 7 – Flux de signal entre les blocs de fonction	112
Figure 8 – Interfaces entre les dispositifs de sécurité au sein du système de communication de sécurité	114
Figure 9 – Flux de signal et états de sécurité	115
Figure 10 – Mise en correspondance du bloc de fonction Transmission sécurisée	118
Figure 11 – Relation entre la SCL et les autres couches du Type 8 de la CEI 61158	119
Figure 12 – Utilisation du service AR-US pour le démarrage et le paramétrage	120
Figure 13 – Utilisation du service AR-US pour la transmission des données de sécurité	120
Figure 14 – Utilisation du service AR-US pour l’abandon	121
Figure 15 – Utilisation du service AR-US pour l’abandon	121
Figure 16 – Structure du PDU de sécurité	130
Figure 17 – Intégration des données de sécurité et des mesures correctives déterministes dans la trame unique	131
Figure 18 – Message Write_Parameter_Byte_Req	132
Figure 19 – Message Read_Parameter_Byte_Req	132
Figure 20 – Message Parameter_Byte_Con	132
Figure 21 – Message Set_Safety_Connection_ID_Req	136
Figure 22 – Message Set_Safety_Connection_ID_Con des esclaves de sécurité	136
Figure 23 – Parameter_Idle_Req	136
Figure 24 – Parameter_Idle_Con	137
Figure 25 – Parameter_Check_Con	137
Figure 26 – Parameter_Loc_ID_Changed_Con	137
Figure 27 – Message de transmission des données de sécurité	137
Figure 28 – Message Sync_a du SCLM	138
Figure 29 – Message Req_b du SCLM	139
Figure 30 – Message Req_c du SCLM	139
Figure 31 – Message Req_d du SCLM	139
Figure 32 – Message Abort_Connection	140
Figure 33 – Message Safety-Slave_Error	140
Figure 34 – Diagramme d’états du SCLM	141
Figure 35 – Diagramme d’états du SCLS	142
Figure 36 – Séquence de lancement	143
Figure 37 – Séquence d’envoi du paramètre d’application	146
Figure 38 – Séquence d’envoi de l’ID du paramètre d’application	148
Figure 39 – Séquence de paramétrage du dispositif	150

Figure 40 – Transmission simultanée des données de sécurité aux esclaves de sécurité.....	151
Figure 41 – Utilisation du numéro de séquence dans le SCLM et le SCLS	152
Figure 42 – Démarrage et fonctionnement exempt d'erreurs	153
Figure 43 – Resynchronisation pendant le fonctionnement.....	154
Figure 44 – Somme de contrôle CRC 24 non valide détectée par le SCLS	155
Figure 45 – Mode de données de processus avec transmission de données de diagnostic	156
Figure 46 – Mode de données de processus avec transmission de données d'acquittement	157
Figure 47 – Erreur lors de l'établissement d'une connexion	158
Figure 48 – Erreur au niveau d'un SCLS lors de l'abandon de toutes les connexions	159
Figure 49 – Abandon de toutes les connexions en cas d'erreur détectée par le SCLM	161
Figure 50 – Présentation du temps d'arrêt	165

Withdrawing

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

RÉSEAUX DE COMMUNICATIONS INDUSTRIELS –
PROFILS –Partie 3-6: Bus de terrain de sécurité fonctionnelle –
Spécifications supplémentaires pour la CPF 6

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 propriété intellectuelle ou de droits analogues. La CEI ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété 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 les dispositions du présent document peut impliquer l'utilisation d'un brevet intéressant les profils de communication de sécurité fonctionnelle pour la famille 6, où la notation [xx] désigne le détenteur des droits de propriété.

DE 103 25 263 A1 [PxC]

Sicherstellung von maximalen Reaktionszeiten in komplexen oder verteilten sicheren und/oder nicht sicheren Systemen

DE 103 18 068 A1 [PxC]

Verfahren und Vorrichtung zum Paket-orientierten Übertragen sicherheitsrelevanter Daten

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

Le détenteur de ces droits de propriété a donné l'assurance à la CEI qu'il consent à négocier des licences avec des demandeurs du monde entier, à des termes et conditions raisonnables et non discriminatoires. A ce propos, la déclaration du détenteur des droits de propriété est enregistrée à la CEI.

Des informations peuvent être demandées à:

[PxC]

Phoenix Contact GmbH & Co. KG
Intellectual Property Licenses &
Standards
Flachsmarktstr. 8
D-32825 Blomberg,
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 qui sont 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 61784-3-6 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 (2013-07) correspond à la version anglaise monolingue publiée en 2007-12.

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

La 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.

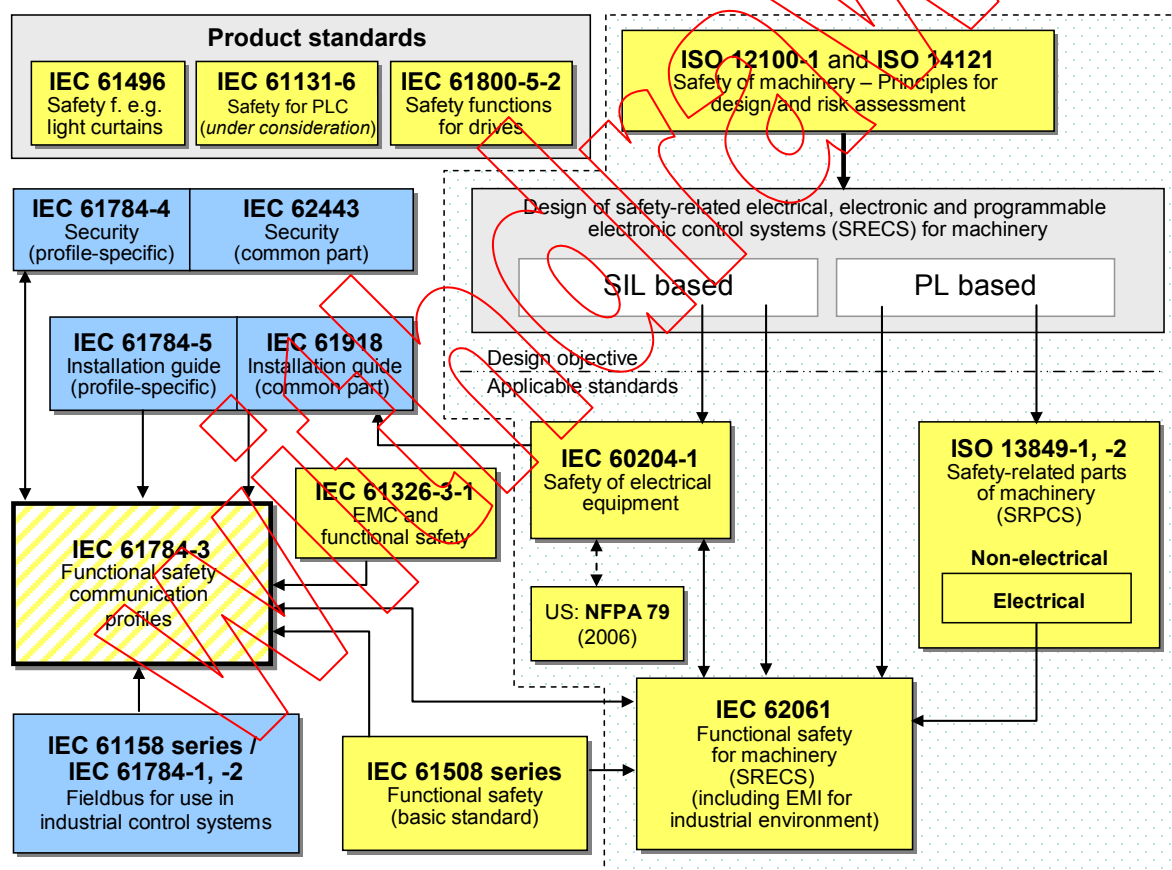
IMPORTANT – Le logo "colour inside" qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante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

INTRODUCTION

La CEI 61158 relative aux bus de terrain, ainsi que ses normes associées CEI 61784-1 et CEI 61784-2, définissent 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 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

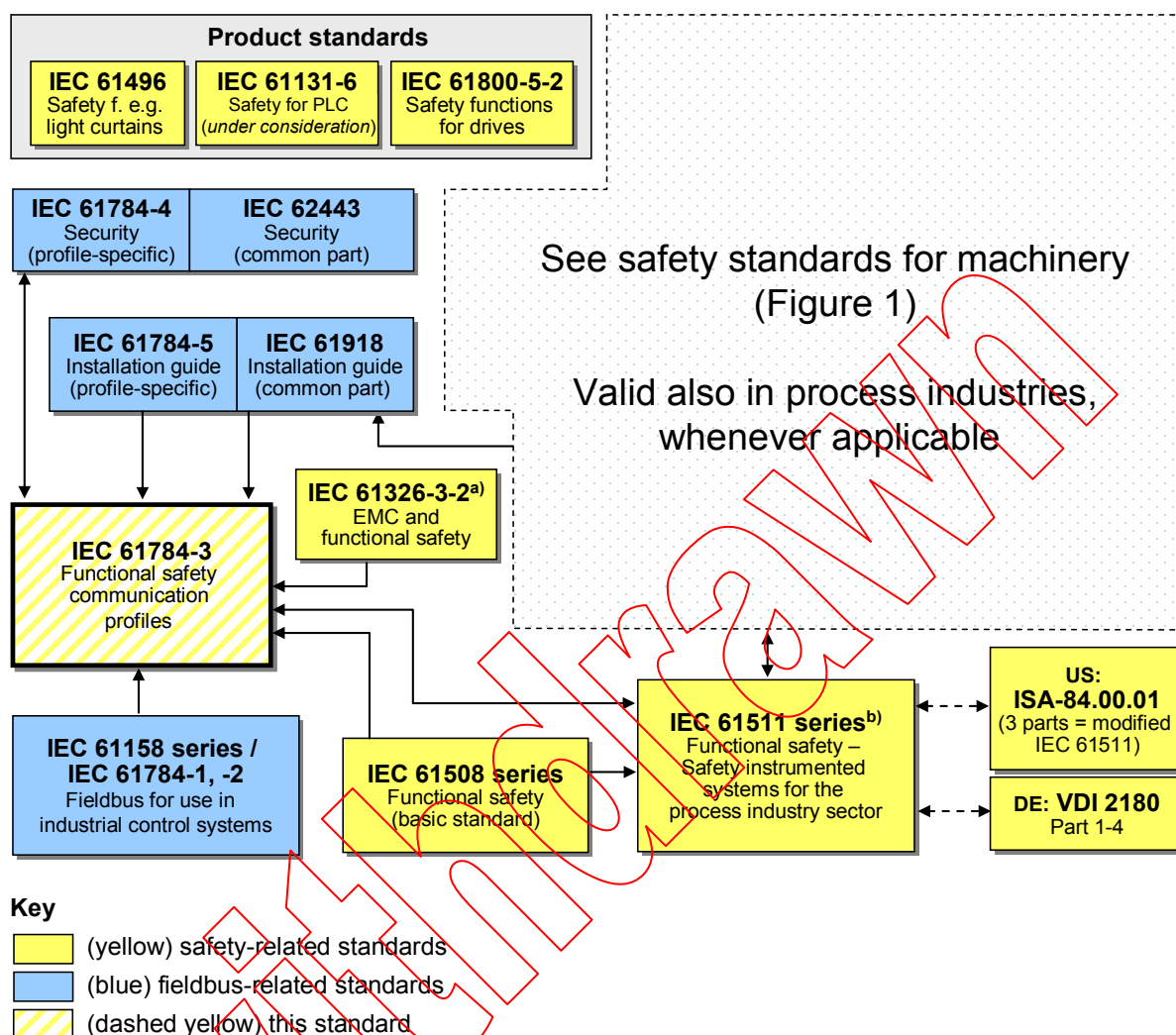
Légende

Anglais	Français
Product standards	Normes de produits

Anglais	Français
Safety function, e.g. light curtains	Fonction de sécurité, par exemple barrières photo électriques
Safety for PLC (under consideration)	Sécurité relative aux automates programmables (à l'étude)
Safety functions for drives	Fonctions de sécurité applicables aux entraînements
Safety requirements for robots	Exigences de sécurité applicables aux robots
Safety of machinery - ... assessment	Sécurité des machines – principes généraux de conception et d'appréciation du risque
Security (profile-specific)	Sûreté (spécifique au profil)
Security (common part)	Sûreté (partie commune)
Design of safety-related electrical, electronic and programmable electronic control system (SRECS) 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
EMC and functional safety	Compatibilité électromagnétique 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 (SRECS) (including EMI 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

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 barrières photo électriques
Safety for PLC (under consideration)	Sécurité relative aux automates programmables (à l'étude)
Safety functions for drives	Fonctions de sécurité applicables aux entraînements
Safety requirements for robots	Exigences de sécurité applicables aux robots
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 in process industries, whenever applicable	Valable également dans les industries de transformation, le cas échéant

Anglais	Français
Functional safety communication profiles	Profils de communication de sécurité fonctionnelle
EMC and functional safety	CEM & 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)
IEC 61511 series Functional safety – safety instrumented systems for the process industry sector	Série CEI 61511 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

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

b EN ratifiée.

Figure 2 – Relation entre la CEI 61784-3 et d'autres normes (procédés industriels)

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 3-6: Bus de terrain de sécurité fonctionnelle – Spécifications supplémentaires pour la CPF 6

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 6 de la CEI 61784-1, la CEI 61784-2 et le Type 8 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 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 61131-3, *Programmable controllers – Part 3 Programming languages* (disponible uniquement en anglais)

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

IEC 61158-3-8, *Industrial communication networks – Fieldbus specifications – Part 3-8: Data-link layer service definition* (disponible uniquement en anglais)

IEC 61158-4-8, *Industrial communication networks – Fieldbus specifications – Part 4-8: Data-link layer protocol specification* (disponible uniquement en anglais)

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

IEC 61158-5-8, *Industrial communication networks – Fieldbus specifications – Part 5-8: Application layer service definition* (disponible uniquement en anglais)

IEC 61158-6-8, *Industrial communication networks – Fieldbus specifications – Part 6-8: Application layer protocol specification* (disponible uniquement en anglais)

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

CEI 61784-1, *Réseaux de communications industriels – Profils – Part 1: Profils de bus de terrain*

CEI 61784-2, *Réseaux de communication industriels – Profils – Partie 2: Profils de bus de terrain supplémentaires pour les réseaux en temps réel basés sur l'ISO/CEI 8802-3*

CEI 61784-3, *Réseaux de communication industriels – Profils – Partie 3: Bus de terrain de sécurité fonctionnelle – Règles générales et définitions de profil*

IEC 61784-5-6, *Industrial communication networks – Profiles – Part 5: Installation of fieldbuses – Installation profiles for CPF 6* (disponible uniquement en anglais)

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

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