

INTERNATIONAL STANDARD

NORME INTERNATIONALE



**Industrial communication networks – Profiles –
Part 3-17: Functional safety fieldbuses – Additional specifications for CPF 17**

**Réseaux de communication industriels – Profils –
Partie 3-17: Bus de terrain de sécurité fonctionnelle – Spécifications
supplémentaires pour CPF 17**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 25.040.40, 35.100.05

ISBN 978-2-8322-3493-8

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.....	5
0 Introduction	7
0.1 General.....	7
0.2 Patent declaration	9
1 Scope.....	10
2 Normative references.....	10
3 Terms, definitions, symbols, abbreviated terms, and conventions.....	11
3.1 Terms and definitions	11
3.1.1 Common terms and definitions	11
3.1.2 CPF 17: Additional terms and definitions	17
3.2 Symbols and abbreviated terms.....	17
3.2.1 Common symbols and abbreviated terms.....	17
3.2.2 CPF 17: Additional symbols and abbreviated terms.....	18
3.3 Conventions.....	18
4 Overview of FSCP 17/1 (RAPIEnet Safety™).....	18
5 General	20
5.1 External documents providing specifications for the profile	20
5.2 Safety functional requirements	20
5.3 Safety measures	20
5.3.1 General	20
5.3.2 (Virtual) sequence number	21
5.3.3 Time expectation with watchdog	21
5.3.4 Connection authentication	21
5.3.5 Feedback message	21
5.3.6 Data integrity assurance.....	21
5.4 Safety communication layer structure	22
5.4.1 Principle of FSCP 17/1 safety communications	22
5.4.2 CPF 17 communication structures	22
5.5 Relationships with FAL (and DLL, PhL).....	22
5.5.1 General	22
5.5.2 Data types	23
6 Safety communication layer services.....	23
6.1 Overview.....	23
6.2 Functional Safety connection.....	23
6.2.1 General	23
6.2.2 Initiator class specification	23
6.2.3 Responder-class specification	24
6.2.4 Sender class specification	25
6.2.5 Receiver class specification	27
6.3 Functional Safety data transmission service.....	29
6.4 Functional Safety connection relation	29
7 Safety communication layer protocol	30
7.1 Safety PDU format	30
7.1.1 General	30
7.1.2 FSPDU command.....	31

7.1.3	Authentication key.....	31
7.1.4	FSPDU CRC	31
7.2	FSCP 17/1 communication procedure	34
7.2.1	FSCP 17/1 device states	34
7.3	Response to communication errors.....	42
7.3.1	General	42
7.4	State table for SCL of CPF 17	42
7.4.1	General	42
7.4.2	Events	43
7.4.3	State table for Initiator.....	44
7.4.4	State table for Responder.....	53
8	Safety communication layer management.....	62
8.1	FSCP 17/1 parameter handling.....	62
8.2	Functional Safety communication parameters	62
9	System requirements	62
9.1	Indicators and switches	62
9.2	Installation guidelines.....	62
9.3	Safety function response time.....	62
9.4	Duration of demands	65
9.5	Constraints for calculation of system characteristics	65
9.5.1	General	65
9.5.2	Number of devices	65
9.5.3	Probabilistic consideration.....	65
9.6	Maintenance	66
9.7	Safety manual	66
10	Assessment.....	66
Annex A (informative) Additional information for functional safety communication profiles of CPF 17.....		67
A.1	Hash function calculation.....	67
A.2		68
Annex B (informative) Information for assessment of the functional safety communication profiles of CPF 17		69
Bibliography		70
Figure 1 – Relationships of IEC 61784-3 with other standards (machinery).....		7
Figure 2 – Relationships of IEC 61784-3 with other standards (process)		8
Figure 3 – Communication relationships among FSCP 17 devices.....		19
Figure 4 – Safety layer architecture.....		22
Figure 5 – Functional Safety Cycle.....		29
Figure 6 – Connection relationships among FSCP 17/1 devices		30
Figure 7 – Functional Safety PDU for CPF 17 over type 21 PDU		30
Figure 8 – FSPDU CRC code generation process		32
Figure 9 – Example of sequence number changing		33
Figure 10 – CRC comparison operation		34
Figure 11 – FSCP 17/1 device states		35
Figure 12 – State diagram for Functional Safety device		43
Figure 13 – State diagram for Initiator		44

Figure 14 – State diagram for Responder	53
Figure 15 – Safety function response time	63
Figure 16 – Residual error rate of FSCP 17/1	66
Table 1 – Deployed measures to manage errors	21
Table 2 – General FSPDU	31
Table 3 – FSPDU command	31
Table 4 – FSPDU with 4 octets of safety data and RESET command after restart (reset connection) or error	36
Table 5 – FSPDU with 4 octets of safety data and RESET command to acknowledge a reset command from the Initiator	36
Table 6 – Connection request PDU for the Initiator in CONNECTION state	37
Table 7 – Connection response PDU for the Responder in CONNECTION state	37
Table 8 – Safety data transferred in the SET_PARA state	38
Table 9 – Sending FSPDU with 6 octets of safety data from the Initiator in SET_PARA state	38
Table 10 – Expected FSPDU with 6 octets of safety data from the Responder in SET_PARA state	39
Table 11 – Safety data from the Initiator in the WAIT_PARA state	39
Table 12 – Sending FSPDU with 6 octets of safety data from the Initiator in the WAIT_PARA state	40
Table 13 – Receiving FSPDU with 6 octets of safety data from the Responder in the WAIT_PARA state	40
Table 14 – FSPDU of Safety data in the DATA state	41
Table 15 – Example of 4 octets of safety data from a Sender	41
Table 16 – Example of ACK PDU from the Receiver with 4 octets of safety data	41
Table 17 – Functional Safety communication errors	42
Table 18 – Functional Safety communication error codes	42
Table 19 – States of the Functional Safety Initiator	43
Table 20 – States of the Functional Safety Responder	43
Table 21 – Events in the Functional Safety state	44
Table 22 – Functional Safety communication parameters	62
Table A.1 – the lookup table for FSCP 17/1	68

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**INDUSTRIAL COMMUNICATION NETWORKS –
PROFILES –****Part 3-17: Functional safety fieldbuses –
Additional specifications for CPF 17**

FOREWORD

- 1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
- 2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
- 3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
- 4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
- 5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
- 6) All users should ensure that they have the latest edition of this publication.
- 7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
- 8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.

International Standard IEC 61784-3-17 has been prepared by subcommittee 65C: Industrial networks, of IEC technical committee 65: Industrial-process measurement, control and automation.

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

FDIS	Report on voting
65C/851/FDIS	65C/854/RVD

Full information on the voting for the approval of this standard can be found in the report on voting indicated in the above table.

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

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

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC web site under "<http://webstore.iec.ch>" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

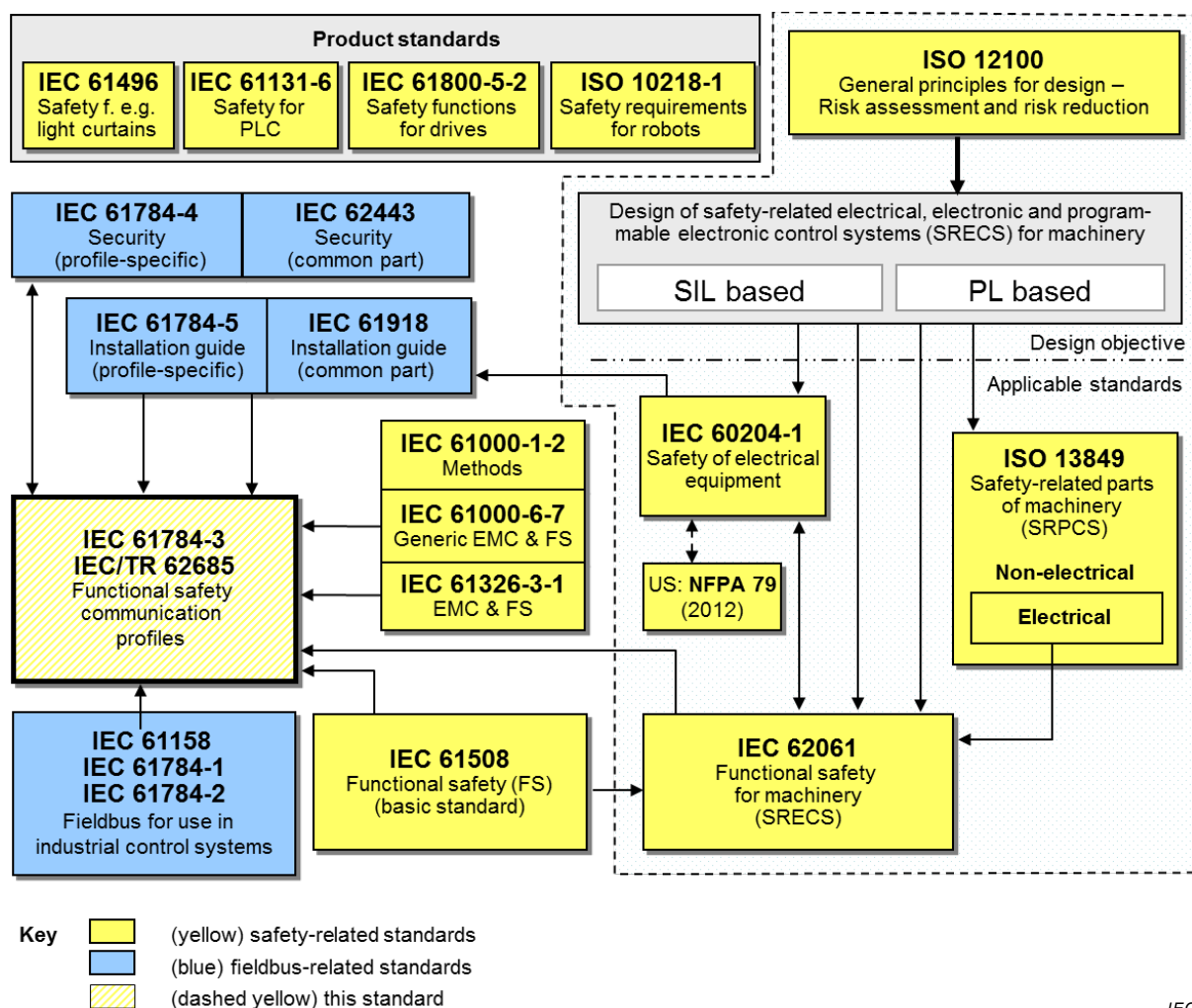
0 Introduction

0.1 General

The IEC 61158 fieldbus standard together with its companion standards IEC 61784-1 and IEC 61784-2 defines a set of communication protocols that enable distributed control of automation applications. Fieldbus technology is now considered well accepted and well proven. Thus fieldbus enhancements continue to emerge, addressing applications for areas such as real time, safety-related and security-related applications.

This standard explains the relevant principles for functional safety communications with reference to IEC 61508 series and specifies several safety communication layers (profiles and corresponding protocols) based on the communication profiles and protocol layers of IEC 61784-2 and the IEC 61158 series. It does not cover electrical safety and intrinsic safety aspects.

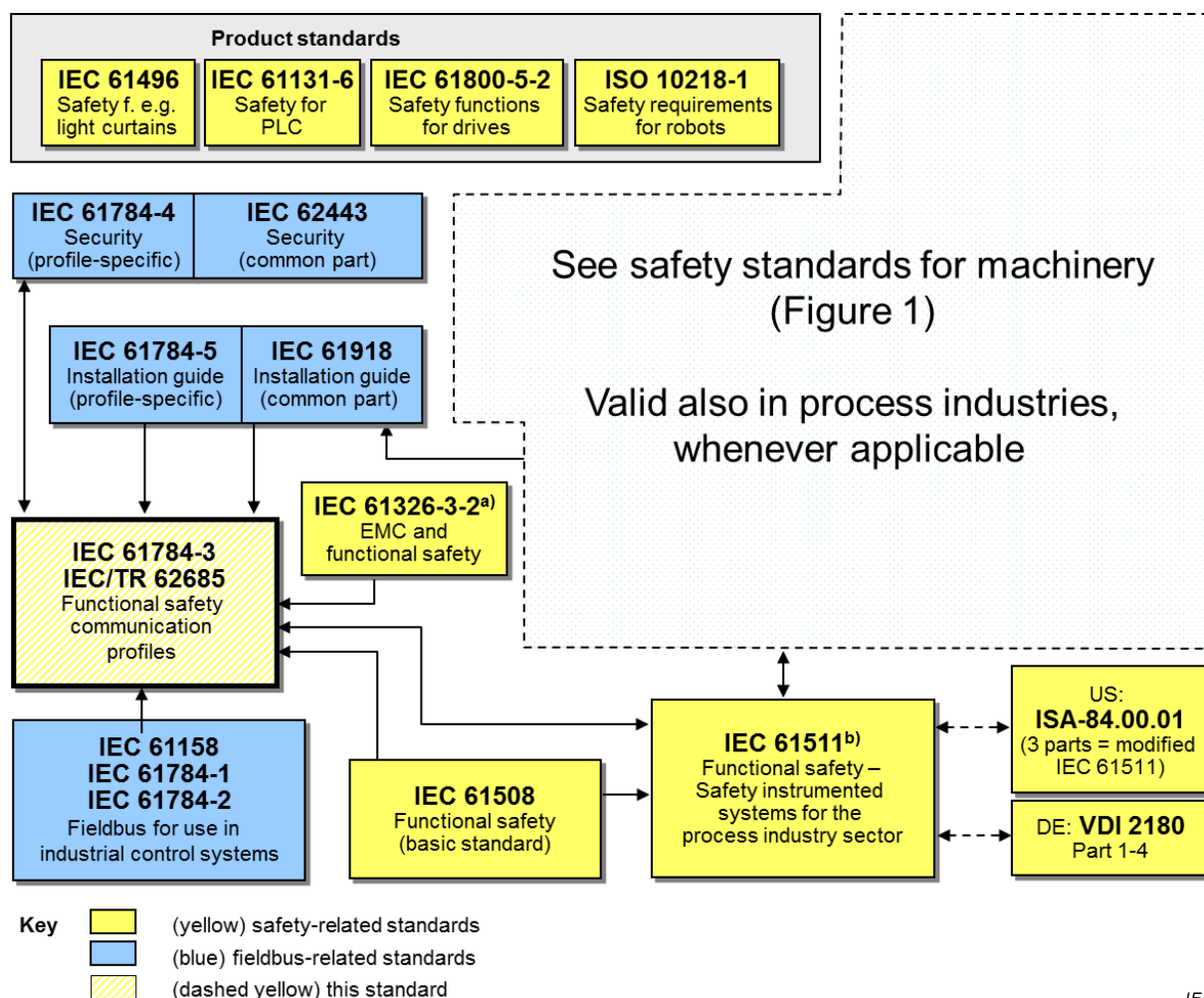
Figure 1 shows the relationships between this standard and relevant safety and fieldbus standards in a machinery environment.



NOTE Subclauses 6.7.6.4 (high complexity) and 6.7.8.1.6 (low complexity) of IEC 62061 specify the relationship between PL (Category) and SIL.

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

Figure 2 shows the relationships between this standard and relevant safety and fieldbus standards in a process environment.



^a For specified electromagnetic environments; otherwise IEC 61326-3-1 or IEC 61000-6-7.

^b EN ratified.

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

Safety communication layers which are implemented as parts of safety-related systems according to IEC 61508 series provide the necessary confidence in the transportation of messages (information) between two or more participants on a fieldbus in a safety-related system, or sufficient confidence of safe behaviour in the event of fieldbus errors or failures.

Safety communication layers specified in this standard do this in such a way that a fieldbus can be used for applications requiring functional safety up to the Safety Integrity Level (SIL) specified by its corresponding functional safety communication profile.

The resulting SIL claim of a system depends on the implementation of the selected functional safety communication profile (FSCP) within this system – implementation of a functional safety communication profile in a standard device is not sufficient to qualify it as a safety device.

This standard describes:

- basic principles for implementing the requirements of IEC 61508 series for safety-related data communications, including possible transmission faults, remedial measures and considerations affecting data integrity;
- functional safety communication profiles for several communication profile families in IEC 61784-1 and IEC 61784-2, including safety layer extensions to the communication service and protocols sections of the IEC 61158 series.

0.2 Patent declaration

The International Electrotechnical Commission (IEC) draws attention to the fact that it is claimed that compliance with this document may involve the use of patents concerning the functional safety communication profiles for family 17 as follows, where the [xx] notation indicates the holder of the patent right:

PCT/KR2012/008651	[LSIS]	Communication apparatus and Communication method
PCT/KR2012/008653	[LSIS]	Communication apparatus and Communication method
PCT/KR2012/008654	[LSIS]	Communication apparatus and Communication method
PCT/KR2012/008655	[LSIS]	Communication apparatus and Communication method
KR 10-1389604	[LSIS]	Communication Device and communication method
KR 10-1442963	[LSIS]	Communication Device and communication method
KR 10-1389646	[LSIS]	Communication Device and communication method

IEC takes no position concerning the evidence, validity and scope of these patent rights.

The holders of these patents rights have assured the IEC that they are willing to negotiate licences either free of charge or under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statements of the holders of these patent rights are registered with IEC.

Information may be obtained from:

[LSIS] LSIS Co Ltd
 LS Tower
 1026-6, Hogue-Dong
 Dongan-Gu
 Anyang, Gyeonggi-Do, 431-848
 South Korea

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.

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES –

Part 3-17: Functional safety fieldbuses – Additional specifications for CPF 17

1 Scope

This part of the IEC 61784-3 series specifies a safety communication layer (services and protocol) based on CPF 17 of IEC 61784-2 (CP 17/1) and IEC 61158 Type 21. It identifies the principles for functional safety communications defined in IEC 61784-3 that are relevant for this safety communication layer. This safety communication layer is intended for implementation in safety devices only.

NOTE 1 It does not cover electrical safety and intrinsic safety aspects. Electrical safety is related to hazards such as electrical shock. Intrinsic safety is related to hazards associated with potentially explosive atmospheres.

This part¹ defines mechanisms for the transmission of safety-relevant messages among participants within a distributed network using fieldbus technology in accordance with the requirements of IEC 61508 series² for functional safety. These mechanisms may be used in various industrial applications such as process control, manufacturing automation, and machinery.

This part provides guidelines for both developers and assessors of compliant devices and systems.

NOTE 2 The resulting SIL claim of a system depends on 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 for it to qualify as a safety device.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 61000-6-2, *Electromagnetic compatibility (EMC) – Part 6-2: Generic standards – Immunity for industrial environments*

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

IEC 61158-3-21:2010, *Industrial communication networks – Fieldbus specifications – Part 3-21: Data-link layer service definition – Type 21 elements*

IEC 61158-4-21:2010, *Industrial communication networks – Fieldbus specifications – Part 4-21: Data-link layer protocol specification – Type 21 elements*

IEC 61158-5-21:2010, *Industrial communication networks – Fieldbus specifications – Part 5-21: Application layer service definition – Type 21 elements*

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

2 In the following pages of this standard, “IEC 61508” will be used for “IEC 61508 series.”

IEC 61158-6-21:2010, *Industrial communication networks – Fieldbus specifications – Part 6-21: Application layer protocol specification – Type 21 elements*

IEC 61326-3-1, *Electrical equipment for measurement, control, and laboratory use – EMC requirements – Part 3-1: Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety) – General industrial applications*

IEC 61326-3-2, *Electrical equipment for measurement, control, and laboratory use – EMC requirements – Part 3-2: Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety) – Industrial applications with specified electromagnetic environment*

IEC 61508 (all parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

IEC 61508-1:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements*

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

IEC 61784-3:—³, *Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions*

IEC 61784-5-17:2013, *Industrial communication networks – Profiles – Part 5: Installation of fieldbuses – Installation profiles for CPF 17*

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

³ To be published.

SOMMAIRE

AVANT-PROPOS	77
0 Introduction	79
0.1 Généralités	79
0.2 Déclaration de droits de propriété	82
1 Domaine d'application.....	84
2 Références normatives	84
3 Termes, définitions, symboles, abréviations et conventions	85
3.1 Termes et définitions	85
3.1.1 Termes et définitions communs	85
3.1.2 CPF 17: Termes et définitions supplémentaires	91
3.2 Symboles et abréviations	92
3.2.1 Symboles et abréviations communs	92
3.2.2 CPF 17: Symboles et abréviations supplémentaires	92
3.3 Conventions.....	93
4 Présentation générale de FSCP 17/1 (RAPIEnet Safety™)	93
5 Généralités.....	95
5.1 Documents externes de spécifications applicables au profil.....	95
5.2 Exigences fonctionnelles de sécurité	95
5.3 Mesures de sécurité	95
5.3.1 Généralités	95
5.3.2 Numéro de séquence (virtuel).....	96
5.3.3 Délai avec le chien de garde	96
5.3.4 Authentification de connexion.....	96
5.3.5 Message de réaction	96
5.3.6 Assurance d'intégrité des données	96
5.4 Structure de la couche de communication de sécurité	97
5.4.1 Principe des communications de sécurité FSCP 17/1	97
5.4.2 Structures de communication CPF 17	97
5.5 Relations avec la FAL (et DLL, PhL)	98
5.5.1 Généralités	98
5.5.2 Types de données.....	98
6 Services de la couche de communication de sécurité	98
6.1 Présentation générale	98
6.2 Connexion de sécurité fonctionnelle	98
6.2.1 Généralités	98
6.2.2 Spécification de classe d'initiateur	99
6.2.3 Spécification de la classe du répondeur.....	100
6.2.4 Spécification de classe d'émetteur.....	101
6.2.5 Spécification de classe de récepteur	103
6.3 Service de transmission de données de sécurité fonctionnelle.....	104
6.4 Relation de connexion de sécurité fonctionnelle.....	105
7 Protocole de couche de communication de sécurité.....	106
7.1 Format PDU de sécurité	106
7.1.1 Généralités	106
7.1.2 Commande FSPDU	107

7.1.3	Clé d'authentification.....	108
7.1.4	FSPDU CRC	108
7.2	Procédure de communication FSCP 17/1	111
7.2.1	États de l'appareil FSCP 17/1.....	111
7.3	Réponse aux erreurs de communication	119
7.3.1	Généralités	119
7.4	Table d'état de la SCL de CPF 17.....	120
7.4.1	Généralités	120
7.4.2	Événements.....	121
7.4.3	Table d'état de l'initiateur	122
7.4.4	Table d'état du répondeur	128
8	Gestion de la couche de communication de sécurité.....	135
8.1	Gestion des paramètres FSCP 17/1.....	135
8.2	Paramètres de communication de sécurité fonctionnelle.....	135
9	Exigences système	135
9.1	Voyants et commutateurs	135
9.2	Lignes directrices d'installation	135
9.3	Temps de réponse de la fonction de sécurité	135
9.4	Durée des demandes	138
9.5	Contraintes liées au calcul des caractéristiques du système.....	138
9.5.1	Généralités	138
9.5.2	Nombre d'appareils	138
9.5.3	Considération en matière de probabilité.....	138
9.6	Maintenance	139
9.7	Manuel de sécurité.....	139
10	Évaluation	140
Annexe A (informative) Informations supplémentaires pour les profils de communication de sécurité fonctionnelle de CPF 17		141
A.1	Calcul de la fonction de hachage	141
A.2		142
Annexe B (informative) Informations pour l'évaluation des profils de communication de sécurité fonctionnelle de CPF 17		143
Bibliographie		144
Figure 1 – Relations entre l'IEC 61784-3 et d'autres normes (machines).....		80
Figure 2 – Relations entre l'IEC 61784-3 et d'autres normes (transformation).....		82
Figure 3 – Relations de communication entre les appareils FSCP 17		94
Figure 4 – Architecture de couche de sécurité		98
Figure 5 – Cycle de sécurité fonctionnelle		105
Figure 6 – Relations de connexion parmi les appareils FSCP 17/1		106
Figure 7 – PDU de sécurité fonctionnelle pour CPF 17 sur PDU de type 21		107
Figure 8 – Processus de génération du code FSPDU CRC.....		109
Figure 9 – Exemple de modification de numéro de séquence		110
Figure 10 – Opération de comparaison CRC.....		111
Figure 11 – États de l'appareil FSCP 17/1		112
Figure 12 – Diagramme d'états de l'appareil de sécurité fonctionnelle		121
Figure 13 – Diagramme d'états de l'initiateur		122

Figure 14 – Diagramme d'états du répondeur	128
Figure 15 – Temps de réponse de la fonction de sécurité	136
Figure 16 – Taux d'erreurs résiduelles de FSCP 17/1	139
Tableau 1 – Mesures déployées pour maîtriser les erreurs	96
Tableau 2 – FSPDU général.....	107
Tableau 3 – Commande FSPDU.....	108
Tableau 4 – FSPDU avec 4 octets de données de sécurité et la commande RESET après redémarrage (connexion de réinitialisation) ou après une erreur.....	113
Tableau 5 – FSPDU avec 4 octets de données de sécurité et la commande RESET pour acquitter une commande de réinitialisation à partir de l'initiateur	114
Tableau 6 – PDU de demande de connexion pour l'initiateur à l'état CONNECTION	114
Tableau 7 – PDU de réponse de connexion pour le répondeur à l'état CONNECTION	115
Tableau 8 – Données de sécurité transférées à l'état SET_PARA	115
Tableau 9 – Envoi d'un FSPDU avec 6 octets de données de sécurité de la part de l'initiateur à l'état SET_PARA	116
Tableau 10 – FSPDU prévu avec 6 octets de données de sécurité provenant du répondeur à l'état SET_PARA	116
Tableau 11 – Données de sécurité provenant de l'initiateur à l'état WAIT_PARA	117
Tableau 12 – Envoi d'un FSPDU avec 6 octets de données de sécurité de la part de l'initiateur à l'état WAIT_PARA	117
Tableau 13 – Réception du FSPDU avec 6 octets de données de sécurité provenant du répondeur à l'état WAIT_PARA state.....	118
Tableau 14 – FSPDU de données de sécurité à l'état DATA.....	119
Tableau 15 – Exemple de 4 octets de données de sécurité provenant d'un émetteur	119
Tableau 16 – Exemple d'ACK PDU provenant du récepteur avec 4 octets de données de sécurité	119
Tableau 17 – Erreurs de communication de sécurité fonctionnelle.....	120
Tableau 18 – Codes d'erreur de communication de sécurité fonctionnelle	120
Tableau 19 – États de l'initiateur de sécurité fonctionnelle	121
Tableau 20 – États du répondeur de sécurité fonctionnelle	121
Tableau 21 – Événements de l'état de sécurité fonctionnelle.....	122
Tableau 22 – Paramètres de communication de sécurité fonctionnelle	135
Tableau A.1 – Table de recherche pour FSCP 17/1	142

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

RÉSEAUX DE COMMUNICATION INDUSTRIELS – PROFILS –

Partie 3-17: Bus de terrain de sécurité fonctionnelle – Spécifications supplémentaires pour CPF 17

AVANT-PROPOS

- 1) La Commission Electrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. À cet effet, l'IEC – 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 l'IEC"). 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 l'IEC, participent également aux travaux. L'IEC 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 l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
- 3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC 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 l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
- 5) L'IEC 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 l'IEC. L'IEC 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 l'IEC, 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 l'IEC, 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 l'IEC ou de toute autre Publication de l'IEC, 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.

La Norme internationale IEC 61784-3-17 a été établie par le sous-comité 65C: Réseaux industriels, du comité d'études 65 de l'IEC: Mesure, commande et automation dans les processus industriels.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
65C/851/FDIS	65C/854/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à l'approbation de cette norme.

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

Une liste de toutes les parties de la série IEC 61784-3, publiées sous le titre général *Réseaux de communication industriels – Profils – Bus de terrain de sécurité fonctionnelle*, peut être consultée sur le site web de l'IEC.

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 l'IEC sous "<http://webstore.iec.ch>" dans les données relatives à la publication recherchée. À cette date, la publication sera

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

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.

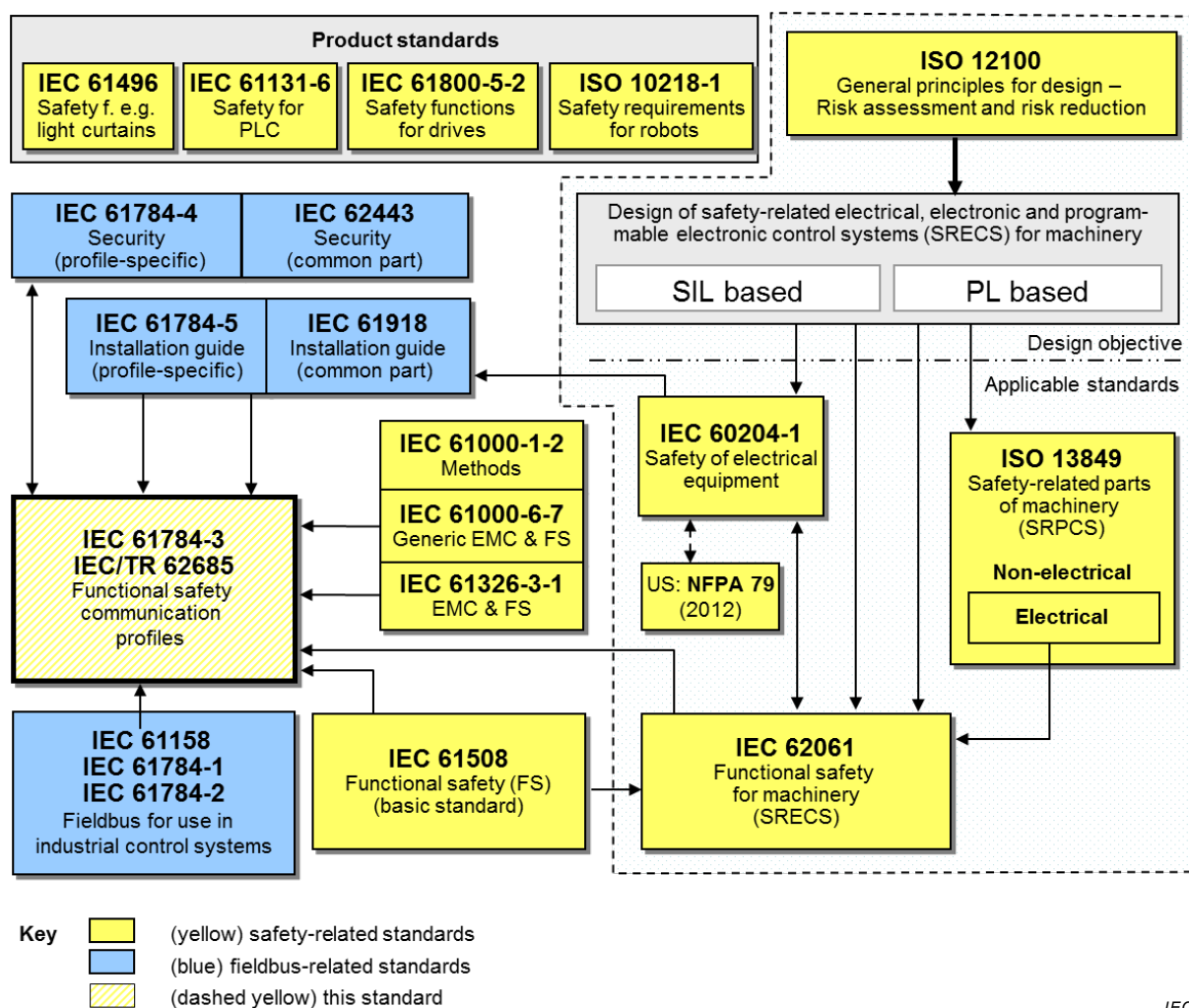
0 Introduction

0.1 Généralités

L'IEC 61158 relative aux bus de terrain, ainsi que ses normes associées IEC 61784-1 et IEC 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, les améliorations des bus de terrain continuent à se développer, traitant des applications pour des domaines 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 IEC 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 l'IEC 61784-2 et de la série IEC 61158. Elle ne couvre pas les aspects relatifs à la sécurité électrique et à la sécurité intrinsèque.

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



IEC

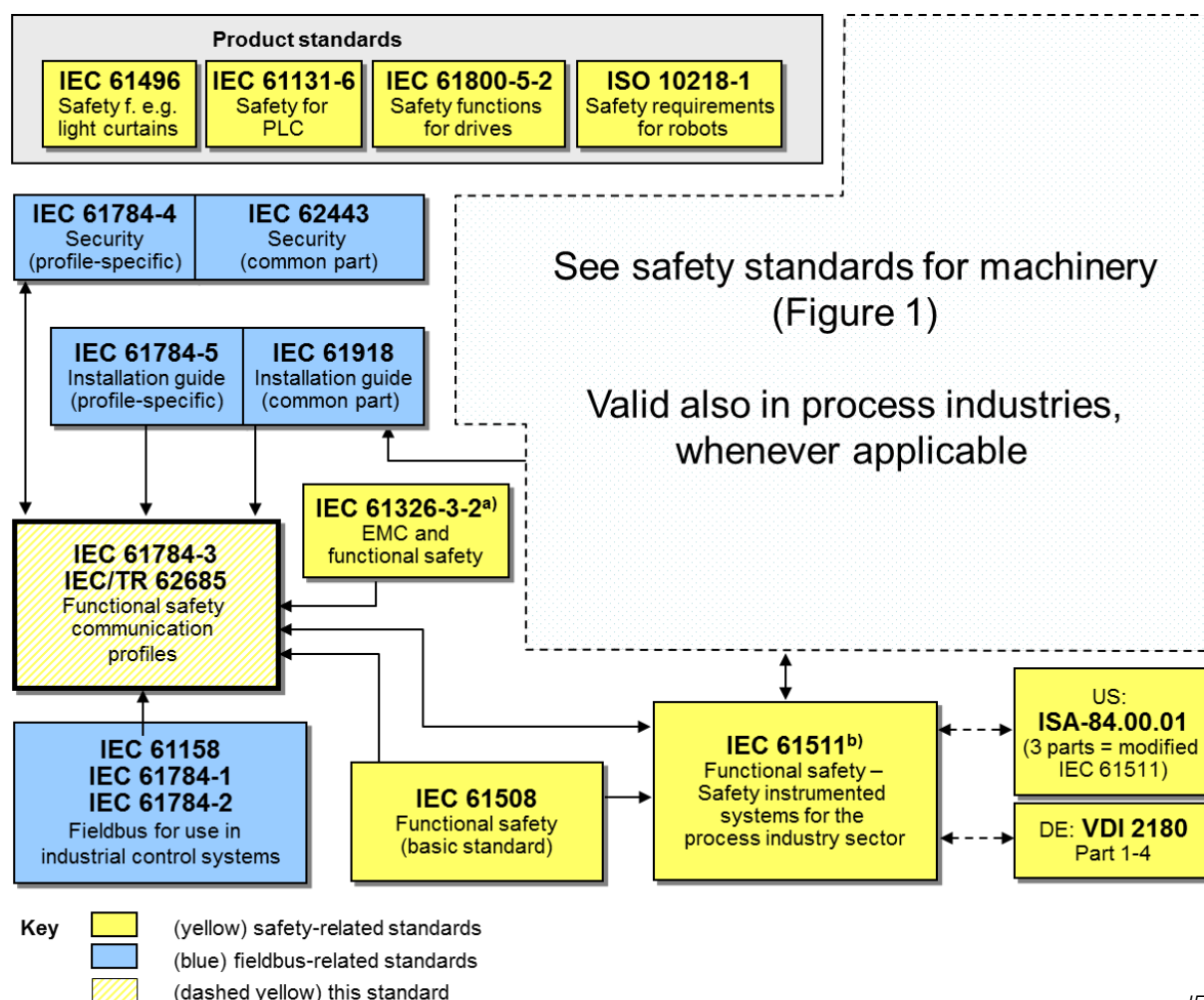
Anglais	Français
Product standards	Normes de produits
Safety function, e.g. light curtains	Fonction de sécurité, par exemple rideaux de lumière
Safety for PLC	Sécurité relative aux automates programmables

Anglais	Français
Safety functions for drives	Fonctions de sécurité applicables aux entraînements
Safety requirements for robots	Exigences de sécurité applicables aux robots
General principles for design – Risk assessment and risk reduction	Principes généraux de conception – Appréciation du risque et réduction 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 systems (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
Methods	Méthodes
Generic EMC & FS	CEM & FS génériques
EMC & FS	CEM & FS
Safety of electrical equipment	Sécurité des équipements électriques
Safety-related parts of machinery (SRPCS)	Sécurité des machines – Parties des systèmes de commande relatives à la sécurité
Non-electrical	Non électrique
Electrical	Électrique
Functional safety communication profiles	Profils de communication de sécurité fonctionnelle
Fieldbus for use in industrial control systems	Bus de terrain pour utilisation dans des systèmes de commande industriels
Functional safety (FS) (basic standard)	Sécurité fonctionnelle (FS) (norme de base)
Functional safety for machinery (SRECS)	Sécurité fonctionnelle des machines
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

NOTE Les paragraphes 6.7.6.4 (haute complexité) et 6.7.8.1.6 (faible complexité) de l'IEC 62061 spécifient la relation entre PL (catégorie) et SIL.

Figure 1 – Relations entre l'IEC 61784-3 et d'autres normes (machines)

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



IEC

Anglais	Français
Product standards	Normes de produits
Safety function, e.g. light curtains	Fonction de sécurité, par exemple rideaux de lumière
Safety for PLC	Sécurité relative aux automates programmables
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
Functional safety communication profiles	Profils de communication de sécurité fonctionnelle
EMC and functional safety	CEM et sécurité fonctionnelle
Fieldbus for use in industrial control systems	Bus de terrain pour utilisation dans des systèmes de commande industriels
Functional safety (basic standard)	Sécurité fonctionnelle (norme de base)
Functional safety – Safety instrumented systems for the process industry sector	Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur des industries de transformation
3 parts = modified IEC 61511	3 parties = IEC 61511 modifiée

Anglais	Français
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 IEC 61326-3-1 ou IEC 61000-6-7

b EN ratifiée.

Figure 2 – Relations entre l'IEC 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 IEC 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 (FSCP) retenu au sein du système – la mise en œuvre du profil de communication de sécurité fonctionnelle dans un appareil normal ne suffit pas à le qualifier d'appareil de sécurité.

La présente norme décrit:

- les principes de base de la mise en œuvre des exigences de la série IEC 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;
- les profils de communication de sécurité fonctionnelle pour plusieurs familles de profils de communication dans l'IEC 61784-1 et l'IEC 61784-2, y compris les extensions de la couche de sécurité aux sections relatives au service et aux protocoles de communication de la série IEC 61158.

0.2 Déclaration de droits de propriété

La Commission Électrotechnique Internationale (IEC) attire l'attention sur le fait qu'il est déclaré que la conformité aux dispositions du présent document peut impliquer l'utilisation de brevets intéressant les profils de communication de sécurité fonctionnelle pour la famille 17 tels que définis ci-après, où la notation [xx] désigne le détenteur des droits de propriété:

PCT/KR2012/008651	[LSIS]	Appareil de communication et méthode de communication
PCT/KR2012/008653	[LSIS]	Appareil de communication et méthode de communication
PCT/KR2012/008654	[LSIS]	Appareil de communication et méthode de communication
PCT/KR2012/008655	[LSIS]	Appareil de communication et méthode de communication
KR 10-1389604	[LSIS]	Appareil de communication et méthode de communication

KR 10-1442963 [LSIS] Appareil de communication et méthode de communication

KR 10-1389646 [LSIS] Appareil de communication et méthode de communication

L'IEC ne prend pas position quant à la preuve, à la validité et à la portée de ces droits de propriété.

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

Des informations peuvent être demandées à:

[LSIS] LSIS Co Ltd
 LS Tower
 1026-6, Hogle-Dong
 Dongan-Gu
 Anyang, Gyeonggi-Do, 431-848
 Corée du Sud

L'attention est d'autre part attirée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété intellectuelle autres que ceux identifiés ci-dessus. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et de ne pas avoir signalé leur existence.

RÉSEAUX DE COMMUNICATION INDUSTRIELS – PROFILS –

Partie 3-17: Bus de terrain de sécurité fonctionnelle – Spécifications supplémentaires pour CPF 17

1 Domaine d'application

La présente partie de la série IEC 61784-3 spécifie une couche de communication de sécurité (services et protocole) reposant sur CPF 17 de l'IEC 61784-2 (CP 17/1) et de l'IEC 61158 Type 21. Elle identifie les principes en matière de communications de sécurité fonctionnelle définies dans l'IEC 61784-3 pertinents pour cette couche de communication de sécurité. Cette couche de communication de sécurité est destinée à la mise en œuvre sur les appareils de sécurité uniquement.

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 IEC 61508² pour 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 d'appareils 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 appareil normal ne suffit pas à le qualifier d'appareil de sécurité.

2 Références normatives

Les documents suivants sont cités en référence de manière normative, en intégralité ou en partie, dans le présent document et sont indispensables pour son application. 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 61000-6-2, *Compatibilité électromagnétique (CEM) – Partie 6-2: Normes génériques – Immunité pour les environnements industriels*

IEC 61131-2, *Automates programmables – Partie 2: Exigences et essais des équipements*

IEC 61158-3-21:2010, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 3-21: Définition des services de la couche liaison de données – Éléments de Type 21*

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

² Dans les pages suivantes de la présente norme, "IEC 61508" se substitue à "série IEC 61508".

IEC 61158-4-21:2010, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 4-21: Spécification du protocole de la couche liaison de données – Éléments de Type 21*

IEC 61158-5-21:2010, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 5-21: Définition des services de la couche application – Éléments de Type 21*

IEC 61158-6-21:2010, *Industrial communication networks – Fieldbus specifications – Part 6 21: Application layer protocol specification – Type 21 elements* (disponible en anglais seulement)

IEC 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 générales*

IEC 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*

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

IEC 61508-1:2010, *Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité – Partie 1: Exigences générales*

IEC 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*

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

IEC 61784-5-17:2013, *Réseaux de communication industriels – Profils – Partie 5-17: Installation des bus de terrain – Profils d'installation pour CPF 17*

IEC 61918, *Réseaux de communication industriels – Installation de réseaux de communication dans des locaux industriels*

³ A publier.