

INTERNATIONAL STANDARD

NORME INTERNATIONALE



**Industrial communication networks – Profiles –
Part 3-1: Functional safety fieldbuses – Additional specifications for CPF 1**

**Réseaux de communication industriels – Profils –
Partie 3-1: Bus de terrain à sécurité fonctionnelle – Spécifications
complémentaires pour le CPF 1**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

PRICE CODE
CODE PRIX

XB

ICS 25.040.40; 35.100.05

ISBN 978-2-8322-1985-0

**Warning! Make sure that you obtained this publication from an authorized distributor.
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.**

CONTENTS

FOREWORD.....	6
INTRODUCTION.....	8
1 Scope.....	11
2 Normative references	11
3 Terms, definitions, symbols, abbreviated terms and conventions	12
3.1 Terms and definitions	12
3.1.1 Common terms and definitions	12
3.1.2 CPF 1: Additional terms and definitions	16
3.2 Symbols and abbreviated terms.....	17
3.2.1 Common symbols and abbreviated terms	17
3.2.2 CPF 1: Additional symbols and abbreviated terms	18
3.3 Conventions	18
3.3.1 State Diagrams.....	18
3.3.2 Use of colors in figures	19
4 Overview of FSCP 1/1 (FOUNDATION Fieldbus™ SIS)	20
4.1 General.....	20
4.2 Key concepts of FSCP 1/1.....	21
4.2.1 Black channel.....	21
4.2.2 Connection key.....	21
4.2.3 Cross-check	21
4.2.4 FSCP 1/1.....	21
4.2.5 Programmable electronic system.....	21
4.2.6 Queuing delays	21
4.2.7 Redundancy	22
4.2.8 SIL environment.....	22
4.3 Key components of FSCP 1/1.....	22
4.3.1 Overview.....	22
4.3.2 Black channel.....	22
4.4 Relationship to the ISO OSI basic reference model	23
5 General.....	23
5.1 External documents providing specifications for the profile	23
5.2 Safety functional requirements	23
5.2.1 Requirements for functional safety.....	23
5.2.2 Functional constraints.....	24
5.2.3 Device manufacturer requirements	24
5.3 Safety measures	25
5.3.1 Sequence number	25
5.3.2 Time stamp	25
5.3.3 Time expectation	25
5.3.4 Connection authentication	25
5.3.5 Data integrity assurance	25
5.3.6 Redundancy with cross checking	25
5.3.7 Different data integrity assurance systems	25
5.3.8 Relationships between errors and safety measures	25
5.4 Safety communication layer structure	26
5.4.1 Network topology and device connectivity.....	26

5.4.2	Device architecture	26
5.5	Relationships with FAL (and DLL, PhL)	27
5.5.1	General	27
5.5.2	Data Types	28
6	Safety communication layer services	28
6.1	Application Process (AP)	28
6.1.1	Overview	28
6.1.2	Network visible objects	29
6.1.3	Application layer interface	29
6.1.4	Object dictionary	29
6.1.5	Application program directory	29
6.2	Function block application processes	29
6.2.1	General	29
6.2.2	Function block model	29
6.2.3	Application process	32
6.3	Device to device communications	34
6.3.1	General	34
6.3.2	Client/server	34
6.3.3	Publisher/subscriber	35
6.3.4	Report distribution	35
6.3.5	FBAP operation in a linking device	35
6.3.6	System management kernel protocol (SMKP) communications	35
6.4	Profiles	35
6.4.1	General	35
6.4.2	FSCP 1/1 profile	35
6.5	Device descriptions	36
6.6	Common file formats	37
6.7	Configuration information	37
6.7.1	Overview	37
6.7.2	Level 1 configuration: manufacturer device definition	37
6.7.3	Level 2 configuration: network definition	37
6.7.4	Level 3 configuration: distributed application definition	37
6.7.5	Level 4 configuration: device configuration	37
7	Safety communication layer protocol	37
7.1	Safety PDU format	37
7.1.1	General	37
7.1.2	Safety communication layer CRC	38
7.1.3	Black channel time synchronization monitoring	38
7.1.4	Sequence number	38
7.1.5	Virtual header	39
7.1.6	Connection key	39
7.1.7	Redundancy and cross-check	40
7.2	Protocol extensions for use in safety-related systems	40
7.2.1	Overview	40
7.2.2	Publisher-subscriber interactions	40
7.2.3	Client-server interactions	46
7.2.4	Time synchronization	51
7.2.5	Device start-up	52
7.3	Communications entity	52

7.3.1	General	52
7.3.2	Network management	52
7.3.3	FMS	52
7.3.4	H1 stack	52
8	Safety communication layer management	53
8.1	Overview	53
8.2	SMK communications	53
8.3	FMS services	53
8.4	SMK services	53
8.4.1	General	53
8.4.2	Address assignment	53
8.4.3	Time synchronization	53
8.5	Safety communication layer configuration and start-up	53
8.5.1	H1 configuration and start-up	53
8.5.2	FSCP 1/1 FBAP	54
8.5.3	Testing	54
9	System requirements	54
9.1	Indicators and switches	54
9.2	Installation guidelines	54
9.3	Safety function response time	54
9.4	Duration of demands	55
9.5	Constraints for calculation of system characteristics	55
9.5.1	Message rate	55
9.5.2	SIL level	55
9.6	Maintenance	55
9.7	Safety manual	55
10	Certification	55
Annex A (informative) Additional information for functional safety communication profiles of CPF 1		56
A.1	Hash function calculation	56
A.2	Fault conditions arising from locations beyond the output function block	58
Bibliography		60
Table 1 – Example state transition table		19
Table 2 – Safety measures and possible communication errors		26
Table 3 – Data types used within FSCP 1/1		28
Table 4 – Fault state behaviour		31
Table 5 – Publisher states		41
Table 6 – Publisher state table - Received transitions		42
Table 7 – Publisher state table - Internal transitions		42
Table 8 – Subscriber states		44
Table 9 – Subscriber state table - Received transitions		45
Table 10 – Subscriber state table - Internal transitions		45
Table 11 – Server states during read operations		47
Table 12 – Received transitions for a FSCP 1/1 Server during read operations		48
Table 13 – States of a FSCP 1/1 server during write operations		49

Table 14 – Received transitions for a FSCP 1/1 Server during write operations	50
Table A.1 – Fault conditions arising from locations beyond the output function block	59

Figure 1 – Relationships of IEC 61784-3 with other standards (machinery)	8
Figure 2 – Relationships of IEC 61784-3 with other standards (process)	9
Figure 3 – Example state diagram	19
Figure 4 – Use of colors in figures	19
Figure 5 – Scope of FSCP 1/1	20
Figure 6 – FSCP 1/1 architecture (H1)	22
Figure 7 – Black channel	23
Figure 8 – FSCP 1/1 in system architecture	26
Figure 9 – FSCP 1/1 H1 device	27
Figure 10 – FSCP 1/1 protocol layers	27
Figure 11 – Relationship between FSCP 1/1 and the other layers of IEC 61158 Type 1	28
Figure 12 – Key write-lock	30
Figure 13 – Password write-lock	30
Figure 14 – Example of FSCP 1/1 communication	34
Figure 15 – Example of device description	36
Figure 16 – Safety PDU showing virtual content	41
Figure 17 – Safety PDU showing duplication of data and addition of CRC	41
Figure 18 – State transition diagram for a FSCP 1/1 Publisher	42
Figure 19 – Safety PDU showing duplication of data and addition of CRC	43
Figure 20 – Safety PDU showing virtual content	43
Figure 21 – State transition diagram for a FSCP 1/1 subscriber	44
Figure 22 – Safety PDU showing virtual content	46
Figure 23 – Safety PDU showing virtual content with sub index	46
Figure 24 – Safety PDU showing duplication of data, addition of sequence number and CRC	47
Figure 25 – State transition diagram for a FSCP 1/1 Server during read operations	47
Figure 26 – Safety PDU showing duplication of data and addition of sequence number and CRC	48
Figure 27 – Example of FSCP 1/1 write	49
Figure 28 – Example of FSCP 1/1 write with sub index	49
Figure 29 – State transition diagram for a FSCP 1/1 Server during write operations	50
Figure 30 – Safety PDU showing duplication of data and CRC	51
Figure 31 – Example of safety function response time components	54

INTERNATIONAL ELECTROTECHNICAL COMMISSION

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES

Part 3-1: Functional safety fieldbuses – Additional specifications for CPF 1

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

US 6,999,824	[FF]	System and method for implementing safety instrumented systems in a fieldbus architecture
--------------	------	---

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:

[FF]	Fieldbus Foundation
	9005 Mountain Ridge Drive
	Bowie Bldg. - Suite 190
	Austin, TX 78759-5316
	Tel: +1 512 794 8890

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 61784-3-1 has been prepared by subcommittee 65C: Industrial networks, of IEC technical committee 65: Industrial process measurement, control and automation.

This bilingual version (2014-12) corresponds to the 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.

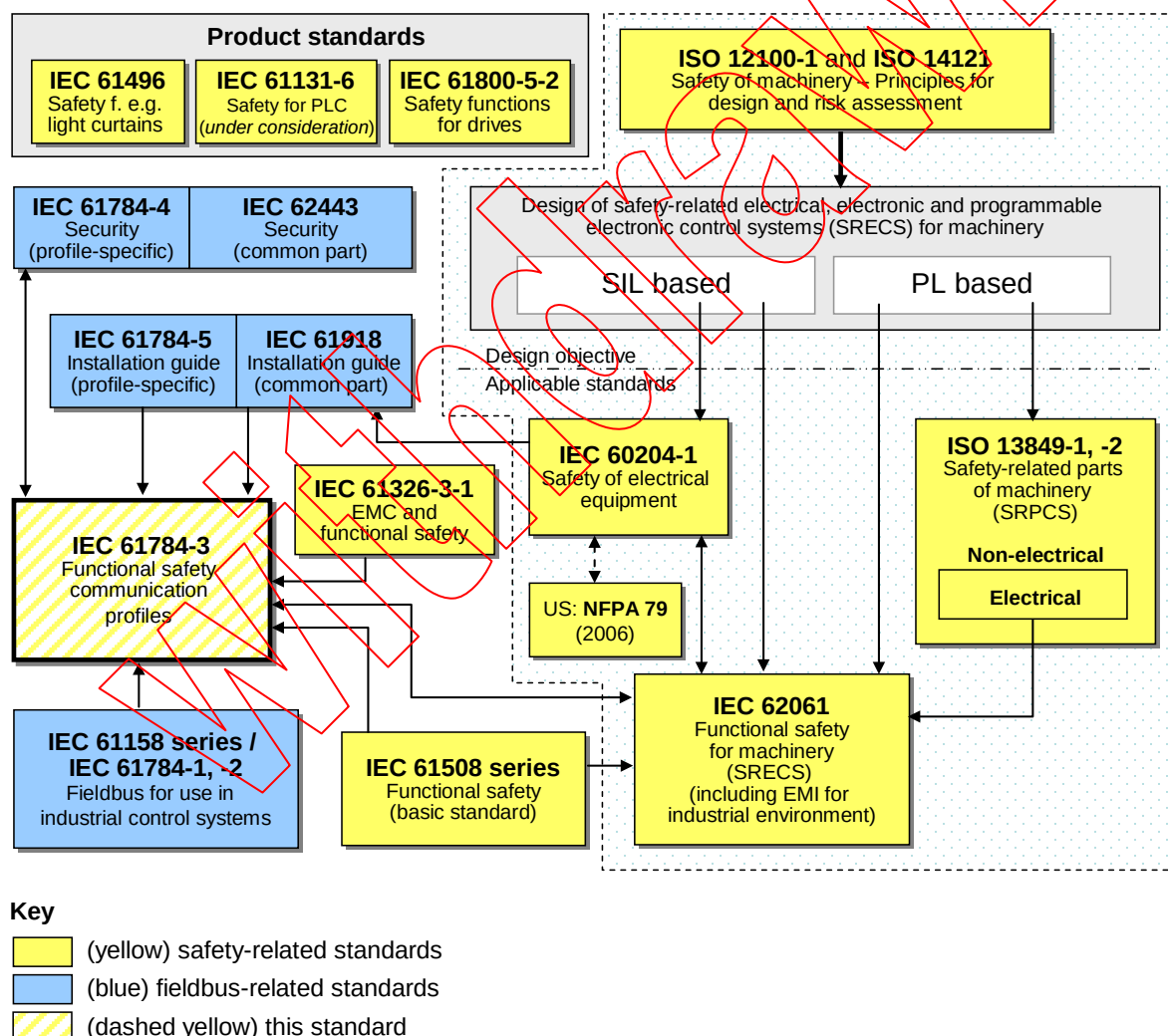
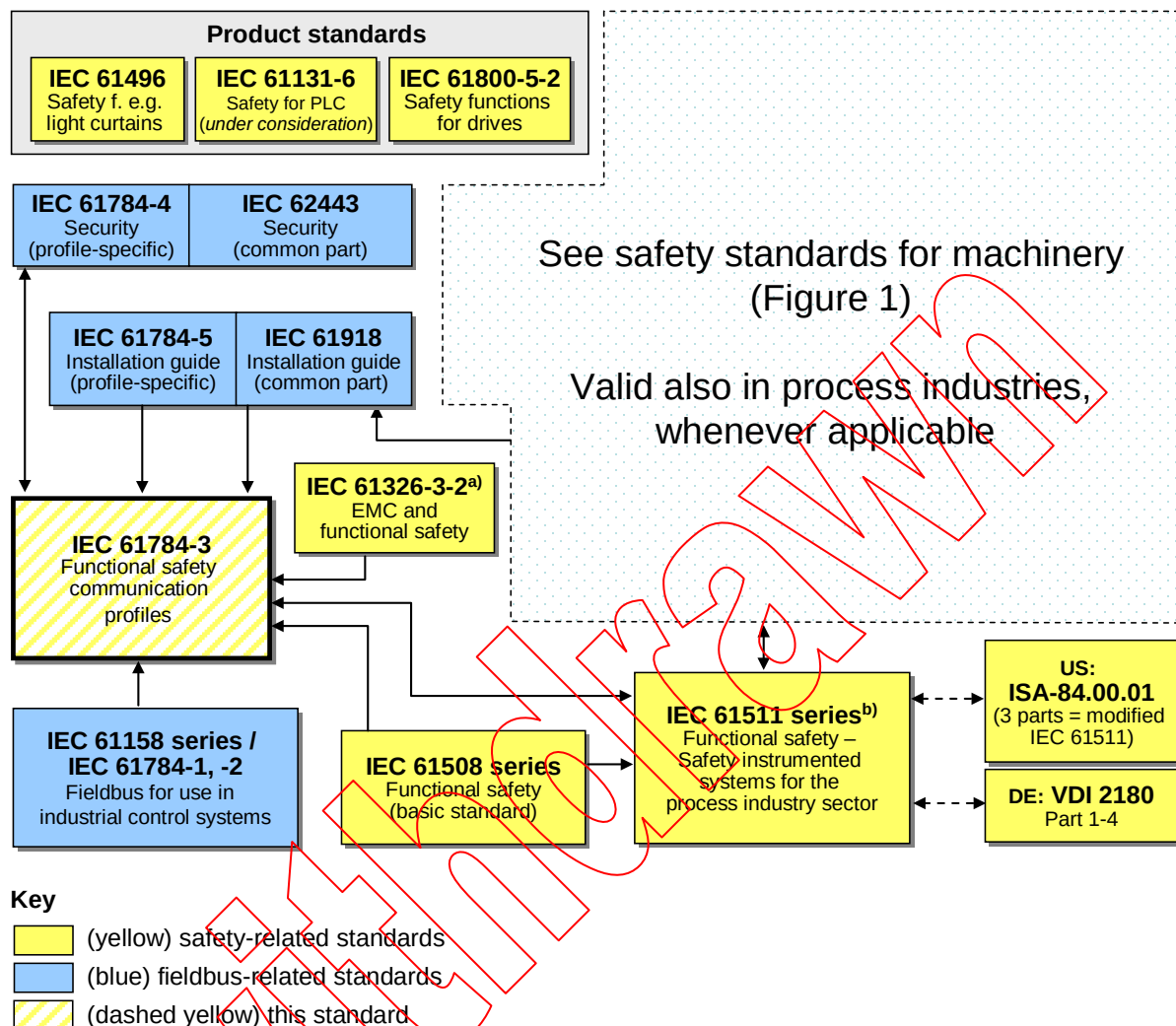


Figure 1 – Relationships of IEC 61784-3 with other standards (machinery)

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 3-1: Functional safety fieldbuses – Additional specifications for CPF 1

1 Scope

This part of the IEC 61784-3 series specifies a safety communication layer (services and protocol) based on CPF 1 of IEC 61784-1 and IEC 61158 Type 1 and 9. 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 series 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 61131-2, *Programmable controllers – Part 2: Equipment requirements and tests*

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

IEC 61158-3-1, *Industrial communication networks – Fieldbus specifications – Part 3-1: Data-link layer service definition – Type 1 elements*

IEC 61158-4-1, *Industrial communication networks – Fieldbus specifications – Part 4-1: Data-link layer protocol specification – Type 1 elements*

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

IEC 61158-5-9, *Industrial communication networks – Fieldbus specifications – Part 5-9: Application layer service definition – Type 9 elements*

IEC 61158-6-5, *Industrial communication networks – Fieldbus specifications – Part 6-5: Application layer protocol specification – Type 5 elements*

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

IEC 61158-6-9, *Industrial communication networks – Fieldbus specifications – Part 6-9: Application layer protocol specification – Type 9 elements*

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

IEC 61511 (all parts), *Functional safety – Safety instrumented systems for the process industry sector*

IEC 61784-1, *Industrial communication networks – Profiles – Part 1: Fieldbus profiles*

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

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

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

Withdrawing

SOMMAIRE

AVANT-PROPOS	66
INTRODUCTION.....	68
1 Domaine d'application	72
2 Références normatives	72
3 Termes, définitions, symboles, abréviations et conventions	73
3.1 Termes et définitions	73
3.1.1 Termes et définitions communs	73
3.1.2 CPF 1: Termes et définitions supplémentaires	77
3.2 Symboles et abréviations	78
3.2.1 Symboles et abréviations communs.....	78
3.2.2 CPF 1: Symboles et abréviations supplémentaires	78
3.3 Conventions	79
3.3.1 Diagrammes d'états.....	79
3.3.2 Utilisation de couleurs dans les figures.....	80
4 Présentation générale de FSCP 1/1 (FOUNDATION Fieldbus™ SIS).....	80
4.1 Généralités.....	80
4.2 Concepts clés du FSCP 1/1.....	81
4.2.1 Canal noir.....	81
4.2.2 Clé de connexion.....	82
4.2.3 Contre-vérification	82
4.2.4 FSCP 1/1.....	82
4.2.5 Système électronique programmable.....	82
4.2.6 Retards de mise en file d'attente	82
4.2.7 Redondance.....	82
4.2.8 Environnement SIL	82
4.3 Composantes clés du FSCP 1/1.....	83
4.3.1 Présentation générale	83
4.3.2 Canal noir.....	84
4.4 Relation avec le modèle de référence de base OSI de l'ISO	85
5 Généralités.....	85
5.1 Documents externes de spécifications applicables au profil.....	85
5.2 Exigences de sécurité fonctionnelle.....	85
5.2.1 Exigences relatives à la sécurité fonctionnelle	85
5.2.2 Contraintes de fonctionnement	86
5.2.3 Exigences du fabricant d'appareils	86
5.3 Mesures de sécurité	86
5.3.1 Numéro de séquence.....	86
5.3.2 Datation (horodatage).....	86
5.3.3 Délai.....	86
5.3.4 Authentification de connexion	86
5.3.5 Assurance d'intégrité des données	86
5.3.6 Redondance avec contre-vérification	86
5.3.7 Différents systèmes d'assurance d'intégrité des données	86
5.3.8 Relations entre les erreurs et les mesures de sécurité.....	86
5.4 Structure de la couche de communication de sécurité	87
5.4.1 Topologie de réseau et connectivité des appareils.....	87

5.4.2	Architecture des appareils	88
5.5	Relations avec la FAL (et DLL, PhL).....	89
5.5.1	Généralités.....	89
5.5.2	Types de données	89
6	Services de la couche de communication de sécurité	90
6.1	Processus d'Application (AP).....	90
6.1.1	Présentation générale	90
6.1.2	Objets visibles de réseau.....	90
6.1.3	Interface de couche application	90
6.1.4	Dictionnaire d'objets	90
6.1.5	Répertoire de programmes d'application.....	90
6.2	Processus d'application de blocs de fonctions	90
6.2.1	Généralités.....	90
6.2.2	Modèle de blocs de fonctions	91
6.2.3	Processus d'Application.....	93
6.3	Communications entre appareils	96
6.3.1	Généralités.....	96
6.3.2	Client/serveur	97
6.3.3	Editeur/abonné	97
6.3.4	Diffusion de rapports	97
6.3.5	Opération FBAP dans un appareil de liaison.....	97
6.3.6	Communications de protocole de noyau de gestion de système (SMKP).....	97
6.4	Profils.....	97
6.4.1	Généralités.....	97
6.4.2	Profil FSCP 1/1.....	98
6.5	Descriptions d'appareils	98
6.6	Formats de fichiers communs.....	99
6.7	Informations de configuration	99
6.7.1	Présentation générale	99
6.7.2	Configuration de niveau 1: définition des appareils du fabricant.....	99
6.7.3	Configuration de niveau 2: définition de réseau	100
6.7.4	Configuration de niveau 3: définition d'une application répartie	100
6.7.5	Configuration de niveau 4: Configuration des appareils	100
7	Protocole de couche de communication de sécurité.....	100
7.1	Format PDU de sécurité	100
7.1.1	Généralités.....	100
7.1.2	CRC de couche de communication de sécurité	100
7.1.3	Contrôle de la synchronisation temporelle par le canal noir	100
7.1.4	Numéro de séquence.....	101
7.1.5	En-tête virtuel.....	102
7.1.6	Clé de connexion.....	102
7.1.7	Redondance et contre-vérification	102
7.2	Extensions de protocole pour utilisation dans des systèmes relatifs à la sécurité	103
7.2.1	Présentation générale	103
7.2.2	Interactions éditeur-abonné	103
7.2.3	Interactions client-serveur	108
7.2.4	Synchronisation temporelle.....	115

7.2.5	Démarrage de l'appareil	116
7.3	Entité de communications.....	116
7.3.1	Généralités.....	116
7.3.2	Gestion de Réseau	116
7.3.3	FMS	116
7.3.4	Pile H1	116
8	Gestion de la couche de communication de sécurité.....	116
8.1	Présentation générale	116
8.2	Communications SMK	117
8.3	Services FMS.....	117
8.4	Services SMK.....	117
8.4.1	Généralités.....	117
8.4.2	Attribution d'adresse.....	117
8.4.3	Synchronisation temporelle.....	117
8.5	Configuration de la couche de communication de sécurité et démarrage	117
8.5.1	Configuration H1 et démarrage.....	117
8.5.2	FBAP FSCP 1/1.....	117
8.5.3	Essais	117
9	Exigences système.....	117
9.1	Voyants et commutateurs	117
9.2	Lignes directrices d'installation.....	117
9.3	Temps de réponse de la fonction de sécurité.....	118
9.4	Durée des demandes	118
9.5	Contraintes liées au calcul des caractéristiques des systèmes	118
9.5.1	Taux de messages	118
9.5.2	Niveau SLL.....	119
9.6	Maintenance.....	119
9.7	Manuel de sécurité.....	119
10	Certification.....	119
Annexe A (informative) Informations supplémentaires pour les profils de communication de sécurité fonctionnelle de protocole CPF 1		120
A.1	Calcul de la fonction de hachage.....	120
A.2	Conditions de panne issues d'emplacements situés au-delà du bloc de fonctions de sortie	122
Bibliographie.....		124
Tableau 1 – Exemple de tableau de transitions d'état		80
Tableau 2 – Mesures de sécurité et erreurs de communication possibles		87
Tableau 3 – Types de données utilisés dans le protocole FSCP 1/1.....		90
Tableau 4 – Comportement d'états d'anomalie.....		93
Tableau 5 – Etats de l'éditeur		104
Tableau 6 – Tableau d'états de l'éditeur – Transitions reçues		105
Tableau 7 - Tableau d'états de l'éditeur – Transitions internes.....		105
Tableau 8 – Etats de l'abonné		107
Tableau 9 - Tableau d'états de l'abonné – Transitions reçues		108
Tableau 10 - Tableau d'états de l'abonné – Transitions internes		108
Tableau 11 – Etats du serveur pendant les opérations de lecture		110

Tableau 12 – Transitions reçues pour un serveur FSCP 1/1 pendant les opérations de lecture	111
Tableau 13 – Etats d'un serveur FSCP 1/1 au cours des opérations d'écriture	113
Tableau 14 – Transitions reçues pour un serveur FSCP 1/1 pendant les opérations d'écriture	114
Tableau A.1 - Conditions de panne issues d'emplacements situés au-delà du bloc de fonctions de sortie	123
Figure 1 - Relation entre la CEI 61784–3 et d'autres normes (machines)	69
Figure 2 - Relations entre la CEI 61784–3 et d'autres normes (transformation)	71
Figure 3 – Exemple de diagramme d'états	79
Figure 4 – Utilisation de couleurs dans les figures	80
Figure 5 – Domaine d'application du FSCP 1/1	81
Figure 6 – Architecture du protocole FSCP 1/1 (H1)	84
Figure 7 – Canal noir	84
Figure 8 – Protocole FSCP 1/1 dans l'architecture de système	87
Figure 9 – Appareil H1 FSCP 1/1	88
Figure 10 – Couches de protocole FSCP 1/1	89
Figure 11 - Relation entre le FSCP 1/1 et les autres couches du type 1 de la CEI 61158	89
Figure 12 – Système d'interdiction d'écriture à clé	92
Figure 13 – Système d'interdiction d'écriture à mots de passe	92
Figure 14 – Exemple de communication FSCP 1/1	96
Figure 15 – Exemple de description d'appareils	99
Figure 16 – Illustration du contenu virtuel d'un PDU de sécurité	104
Figure 17 – PDU de sécurité illustrant la duplication des données et l'ajout du CRC	104
Figure 18 – Diagramme de transition d'états pour un éditeur FSCP 1/1	105
Figure 19 – PDU de sécurité illustrant la duplication des données et l'ajout du CRC	106
Figure 20 – Illustration du contenu virtuel d'un PDU de sécurité	106
Figure 21 – Diagramme de transition d'états pour un abonné FSCP 1/1	107
Figure 22 – Illustration du contenu virtuel d'un PDU de sécurité	109
Figure 23 – Illustration du contenu virtuel d'un PDU de sécurité avec sous-index	109
Figure 24 – PDU de sécurité illustrant la duplication des données et l'ajout du numéro de séquence et du CRC	110
Figure 25 – Diagramme de transition d'états pour un serveur FSCP 1/1 pendant les opérations de lecture	111
Figure 26 – PDU de sécurité illustrant la duplication des données et l'ajout du numéro de séquence et du CRC	112
Figure 27 – Exemple d'écriture FSCP 1/1	112
Figure 28 – Exemple d'écriture FSCP 1/1 avec sous-index	113
Figure 29 – Diagramme de transition d'états pour un serveur FSCP 1/1 pendant les opérations d'écriture	114
Figure 30 – PDU de sécurité illustrant la duplication des données et le CRC	115
Figure 31 – Exemple des composantes du temps de réponse de la fonction de sécurité	118

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

RÉSEAUX DE COMMUNICATION INDUSTRIELS – PROFILS –

Partie 3-1: Bus de terrain à sécurité fonctionnelle - Spécifications complémentaires pour le CPF 1

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 n'a prévu aucune procédure de marquage valant indication d'approbation et n'engage pas sa responsabilité pour les équipements déclarés conformes à une de ses Publications.
- 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.

La commission électrotechnique internationale (CEI) attire l'attention sur le fait qu'il est déclaré que la conformité avec le présent document peut impliquer l'utilisation de brevets concernant les profils de communication de sécurité fonctionnelle pour la famille 1, où la notation [xx] désigne le détenteur des droits de propriété.

US 6,999,824

[FF]

Système et méthode de mise en œuvre des systèmes instrumentés de sécurité dans une architecture de bus de terrain

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

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

Des informations peuvent être obtenues auprès de:

[FF]

Fieldbus Foundation

9005 Mountain Ridge Drive

Bowie Bldg. - Suite 190

Austin, TX 78759-5316

USA

Tel: +1 512 794 8890

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

La Norme internationale CEI 61784-3-1 a été établie par le sous-comité 65C: Réseaux industriels, du comité d'études 65 de la CEI: Mesure, commande et automation dans les processus industriels.

La présente version bilingue (2014-12) 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. À 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 communication industriels – Profils – Bus de terrain de sécurité fonctionnelle*, peut être consultée sur le site Web de la CEI.

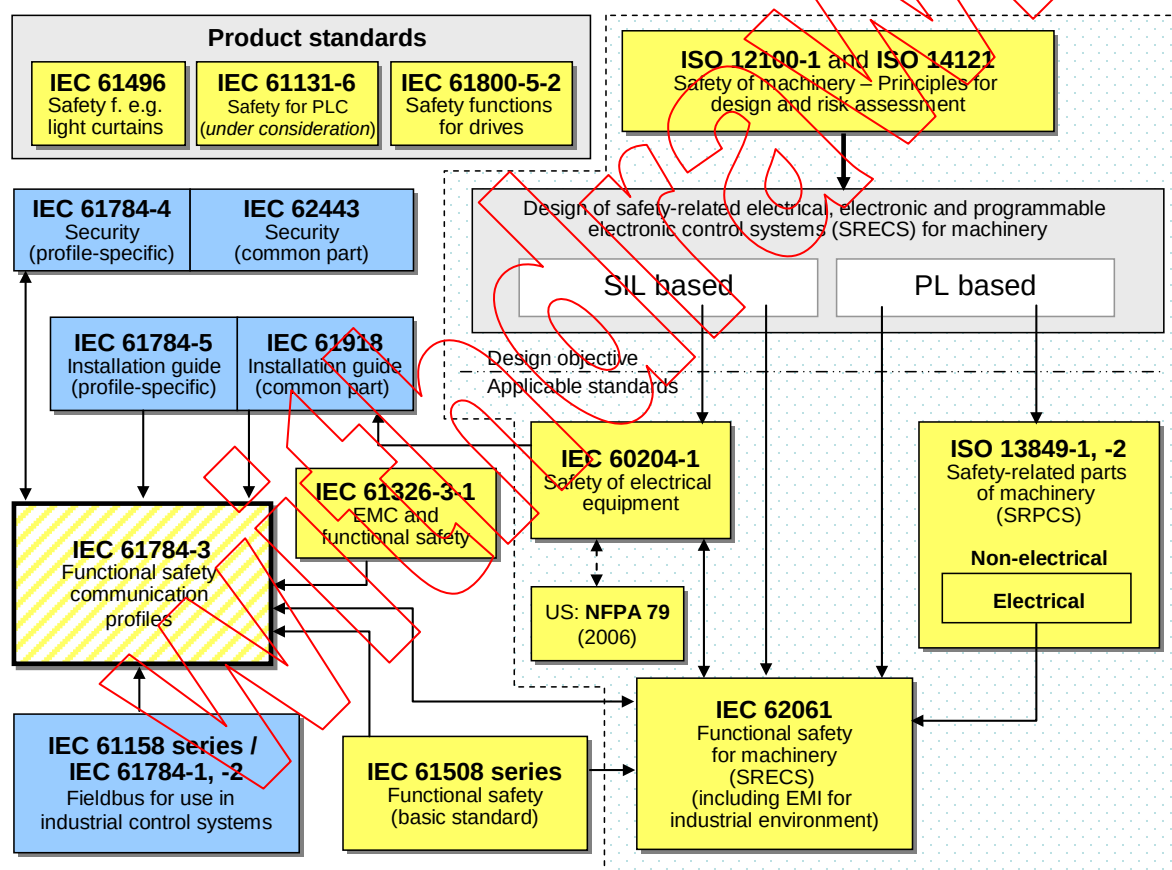
IMPORTANT – Le logo "colour inside" qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante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

INTRODUCTION

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

La présente norme définit les principes pertinents applicables aux communications en termes de sécurité fonctionnelle en référence à la série CEI 61508, et spécifie plusieurs couches de communication de sécurité (profils et protocoles correspondants) basées sur les profils de communication et les couches de protocole de la CEI 61784-1, la CEI 61784-2 et 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

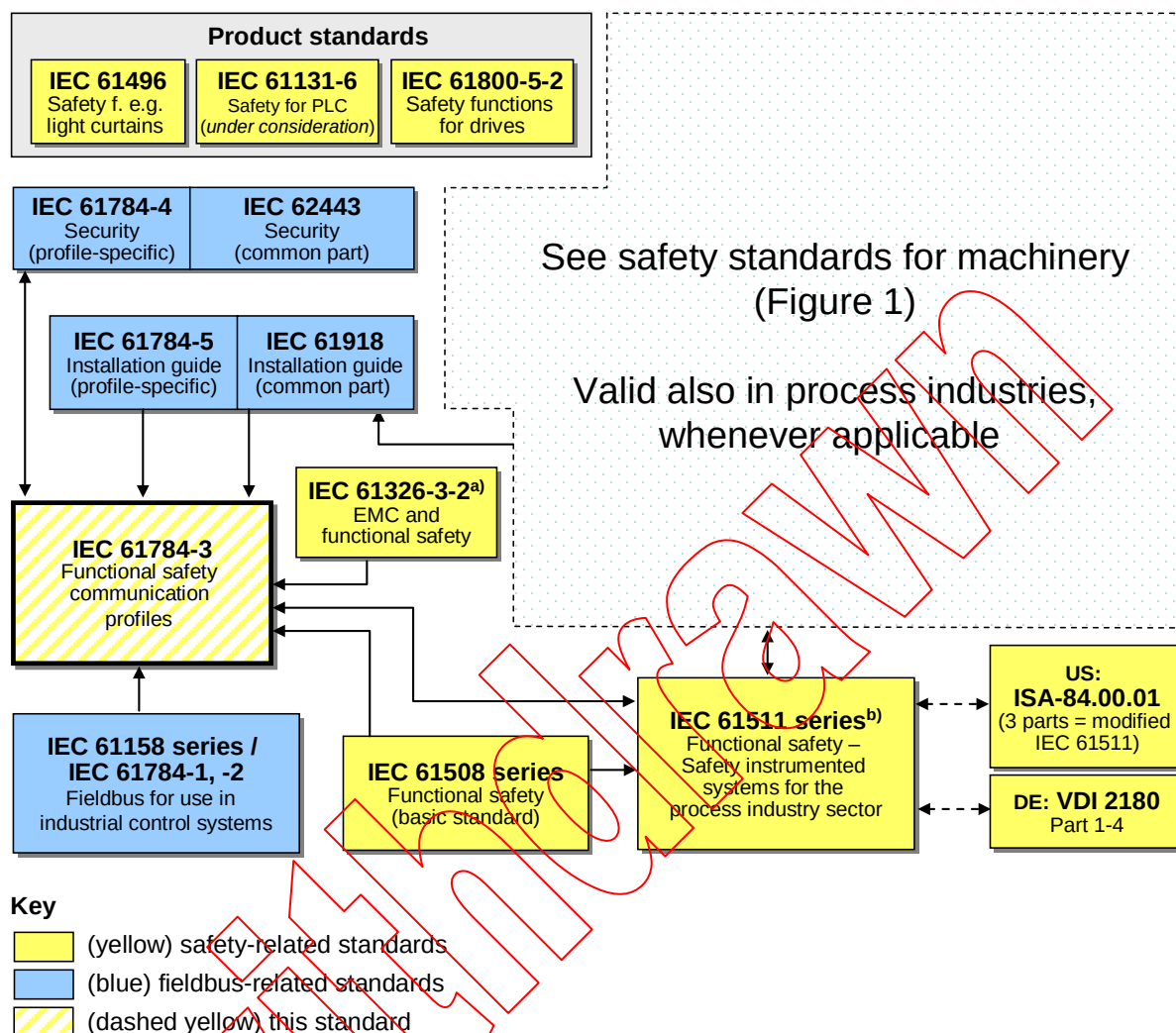
Légende

Anglais	Français
Product standards	Normes de produits
Safety function, e.g. light curtains	Fonction de sécurité, par exemple rideaux de lumière

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

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

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



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

^b EN ratifiée.

Légende

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

Anglais	Français
	transformation, le cas échéant
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 ... 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
IEC	CEI

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

Les couches de communication de sécurité mises en œuvre dans la trame 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 appareil normal ne suffit pas à le qualifier d'appareil 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 les CEI 61784-1 et 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 COMMUNICATION INDUSTRIELS – PROFILS –

Partie 3-1: Bus de terrain à sécurité fonctionnelle - Spécifications complémentaires pour le CPF 1

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 1 de la CEI 61784-1 et les types 1 et 9 de la CEI 61158. Elle identifie les principes applicables aux communications de sécurité fonctionnelle définies dans la CEI 61784-3, et appropriés à cette couche de communication de sécurité.

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

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

La présente partie fournit des lignes directrices tant pour les développeurs que pour les évaluateurs 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 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 61131-2, *Programmable controllers – Part 2: Equipment requirements and tests* (disponible en anglais seulement)

CEI 61158-2, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 2: Spécification et définition des services de la couche physique*

CEI 61158-3-1, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 3-1: Définition des services de la couche liaison de données – Éléments de type 1*

CEI 61158-4-1, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 4-1: Spécification du protocole de la couche liaison de données – Éléments de type 1*

CEI 61158-5-5, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 5-5: Définition des services de la couche liaison de données – Éléments de type 5*

CEI 61158-5-9, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 5-9: Définition des services de la couche application – Éléments de type 9*

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

CEI 61158-6-5, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 6-5: Spécification du protocole de la couche application – Éléments de type 5*

CEI 61158-6-9, *Réseaux de communication industriels – Spécifications des bus de terrain – Part 6-9: Spécification du protocole de la couche application – Éléments de type 9*

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

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

CEI 61784-1, *Réseaux de communication industriels – Profils – Partie 1: Profils de bus de terrain*

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

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

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