

INTERNATIONAL STANDARD

NORME INTERNATIONALE



**Industrial communication networks – Profiles –
Part 3-12: Functional safety fieldbuses – Additional specifications for CPF 12**

**Réseaux de communication industriels – Profils –
Partie 3-12: Bus de terrain de sécurité fonctionnelle – Spécifications
supplémentaires pour CPF 12**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

PRICE CODE
CODE PRIX

XD

ICS 25.040.40, 35.100.05

ISBN 978-2-88912-944-7

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
0 Introduction	8
0.1 General	8
0.2 Patent declaration	10
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 12: 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 12: Additional symbols and abbreviated terms	18
3.3 Conventions	18
4 Overview of FSCP 12/1 (Safety-over-EtherCAT™)	18
5 General	20
5.1 External document providing specifications for the profile.....	20
5.2 Safety functional requirements	20
5.3 Safety measures	21
5.4 Safety communication layer structure	21
5.5 Relationships with FAL (and DLL, PhL)	22
5.5.1 General	22
5.5.2 Data types	22
6 Safety communication layer services	22
6.1 FSoE Connection	22
6.2 FSoE Cycle	22
6.3 FSoE services	23
7 Safety communication layer protocol	24
7.1 Safety PDU format	24
7.1.1 Safety PDU structure	24
7.1.2 Safety PDU command.....	25
7.1.3 Safety PDU CRC	25
7.2 FSCP 12/1 communication procedure.....	29
7.2.1 Message cycle.....	29
7.2.2 FSCP 12/1 node states.....	29
7.3 Reaction on communication errors	39
7.4 State table for FSoE Master	40
7.4.1 FSoE Master state machine.....	40
7.4.2 Reset state	44
7.4.3 Session state.....	45
7.4.4 Connection state	48
7.4.5 Parameter state	52
7.4.6 Data state.....	55
7.5 State table for FSoE Slave	58
7.5.1 FSoE Slave state machine.....	58
7.5.2 Reset state	62

7.5.3	Session state.....	64
7.5.4	Connection state	68
7.5.5	Parameter state	73
7.5.6	Data state.....	78
8	Safety communication layer management.....	81
8.1	FSCP 12/1 parameter handling.....	81
8.2	FSoE communication parameters	81
9	System requirements.....	82
9.1	Indicators and switches	82
9.1.1	Indicator states and flash rates	82
9.1.2	Indicators	83
9.2	Installation guidelines.....	84
9.3	Safety function response time	84
9.3.1	General	84
9.3.2	Determination of FSoE Watchdog time	85
9.3.3	Calculation of the worst case safety function response time	86
9.4	Duration of demands	87
9.5	Constraints for calculation of system characteristics.....	87
9.5.1	General	87
9.5.2	Probabilistic considerations	87
9.6	Maintenance.....	89
9.7	Safety manual	89
10	Assessment.....	89
Annex A (informative) Additional information for functional safety communication profiles of CPF 12.....		90
A.1	Hash function calculation.....	90
A.2		94
Annex B (informative) Information for assessment of the functional safety communication profiles of CPF 12.....		95
Bibliography.....		96
Table 1 – State machine description elements		18
Table 2 – Communication errors and detection measures		21
Table 3 – General Safety PDU		24
Table 4 – Shortest Safety PDU		25
Table 5 – Safety PDU command		25
Table 6 – CRC_0 calculation sequence.....		26
Table 7 – CRC_i calculation sequence (i>0)		26
Table 8 – Example for CRC_0 inheritance		27
Table 9 – Example for 4 octets of safety data with interchanging of octets 1-4 with 5-8.....		28
Table 10 – Safety Master PDU for 4 octets of safety data with command = Reset after restart (reset connection) or error		31
Table 11 – Safety Slave PDU for 4 octets of safety data with command = Reset for acknowledging a Reset command from the FSoE Master		31
Table 12 – Safety Slave PDU for 4 octets of safety data with command = Reset after restart (reset connection) or error		32

Table 13 – Safety Master PDU for 4 octets of safety data with command = Session.....	32
Table 14 – Safety Slave PDU for 4 octets of safety data with command = Session.....	33
Table 15 – Safety data transferred in the connection state.....	33
Table 16 – Safety Master PDU for 4 octets of safety data in Connection state	34
Table 17 – Safety Slave PDU for 4 octets of safety data in Connection state	34
Table 18 – Safety data transferred in the parameter state.....	35
Table 19 – First Safety Master PDU for 4 octets of safety data in parameter state	35
Table 20 – First Safety Slave PDU for 4 octets of safety data in parameter state	36
Table 21 – Second Safety Master PDU for 4 octets of safety data in parameter state	36
Table 22 – Second Safety Slave PDU for 4 octets of safety data in parameter state	37
Table 23 – Safety Master PDU for 4 octets of ProcessData in data state	37
Table 24 – Safety Slave PDU for 4 octets of ProcessData in data state	38
Table 25 – Safety Master PDU for 4 octets of fail-safe data in data state	38
Table 26 – Safety Slave PDU for 4 octets of fail-safe data in data state	39
Table 27 – FSoE communication error	39
Table 28 – FSoE communication error codes.....	40
Table 29 – States of the FSoE Master.....	40
Table 30 – Events in the FSoE Master state table.....	42
Table 31 – Functions in the FSoE Master state table	42
Table 32 – Variables in the FSoE Master state table.....	43
Table 33 – Macros in the FSoE Master state table	43
Table 34 – States of the FSoE Slave	58
Table 35 – Events in the FSoE Slave state table.....	60
Table 36 – Functions in the FSoE Slave state table	60
Table 37 – Variables in the FSoE Slave state table.....	61
Table 38 – Macros in the FSoE Slave state table	61
Table 39 – FSoE Communication parameters	82
Table 40 – Indicator States	82
Table 41 – FSoE STATUS indicator states.....	83
Table 42 – Definition of times	85
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 – Basic FSCP 12/1 system.....	19
Figure 4 – FSCP 12/1 software architecture.....	21
Figure 5 – FSoE Cycle.....	23
Figure 6 – FSCP 12/1 communication structure	23
Figure 7 – Safety PDU for CPF 12 embedded in Type 12 PDU.....	24
Figure 8 – FSCP 12/1 node states	30
Figure 9 – State diagram for FSoE Master	41
Figure 10 – State diagram for FSoE Slave	59
Figure 11 – Indicator flash rates	83

Figure 12 – Components of a safety function	84
Figure 13 – Calculation of the FSoE Watchdog times for input and output connections	85
Figure 14 – Calculation of the worst case safety function response time	86
Figure 15 – Safety PDU embedded in standard PDU	88
Figure 16 – Residual error rate for 8/16/24 bit safety data and up to 12 144 bit standard data.....	89

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**INDUSTRIAL COMMUNICATION NETWORKS –
PROFILES –****Part 3-12: Functional safety fieldbuses –
Additional specifications for CPF 12**

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 61784-3-12 has been prepared by subcommittee 65C: Industrial networks, of IEC technical committee 65: Industrial process measurement, control and automation.

This bilingual version (2012-02) corresponds to the monolingual English version, published in 2010-06.

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

FDIS	Report on voting
65C/591A/FDIS	65C/603/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.

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.

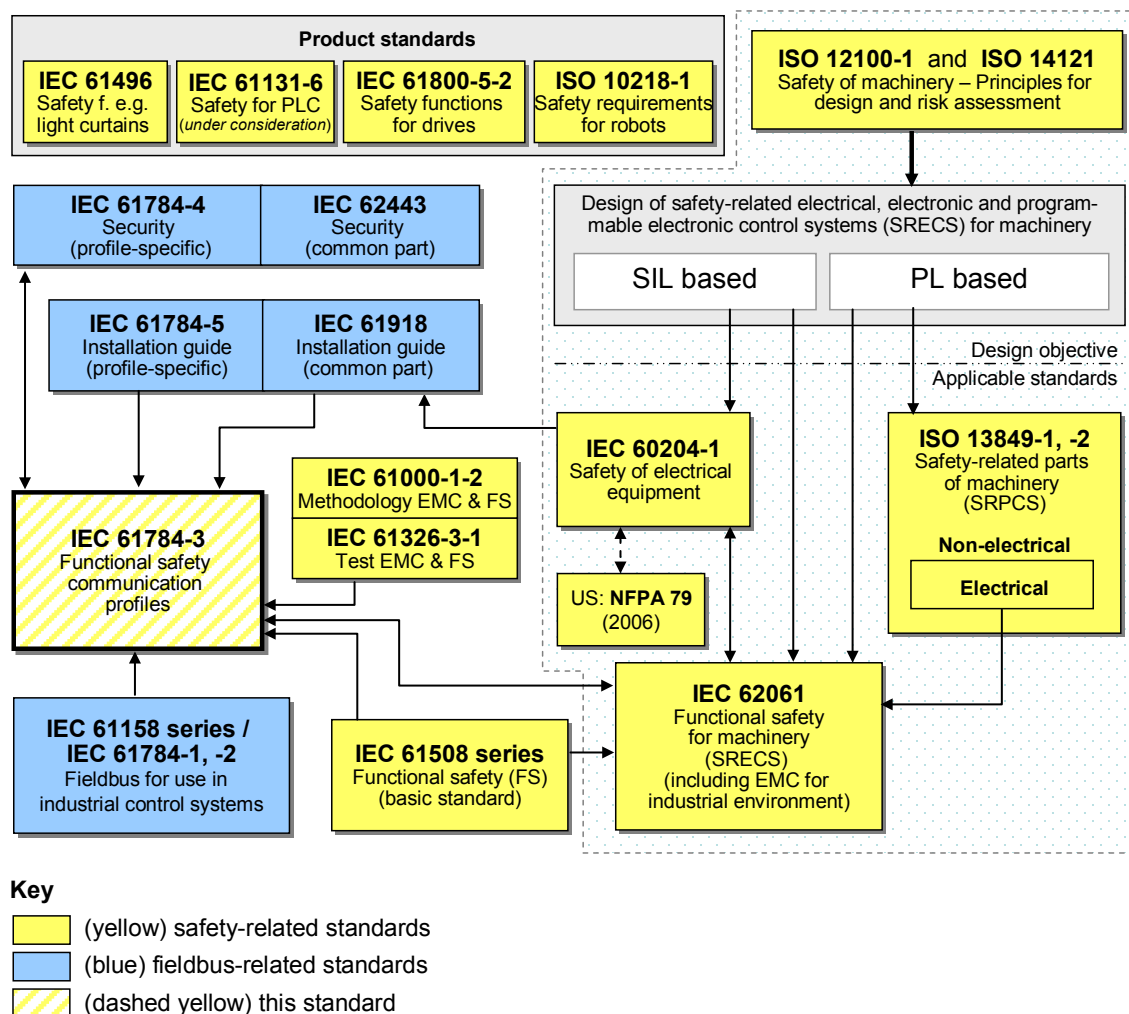
0 Introduction

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 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.

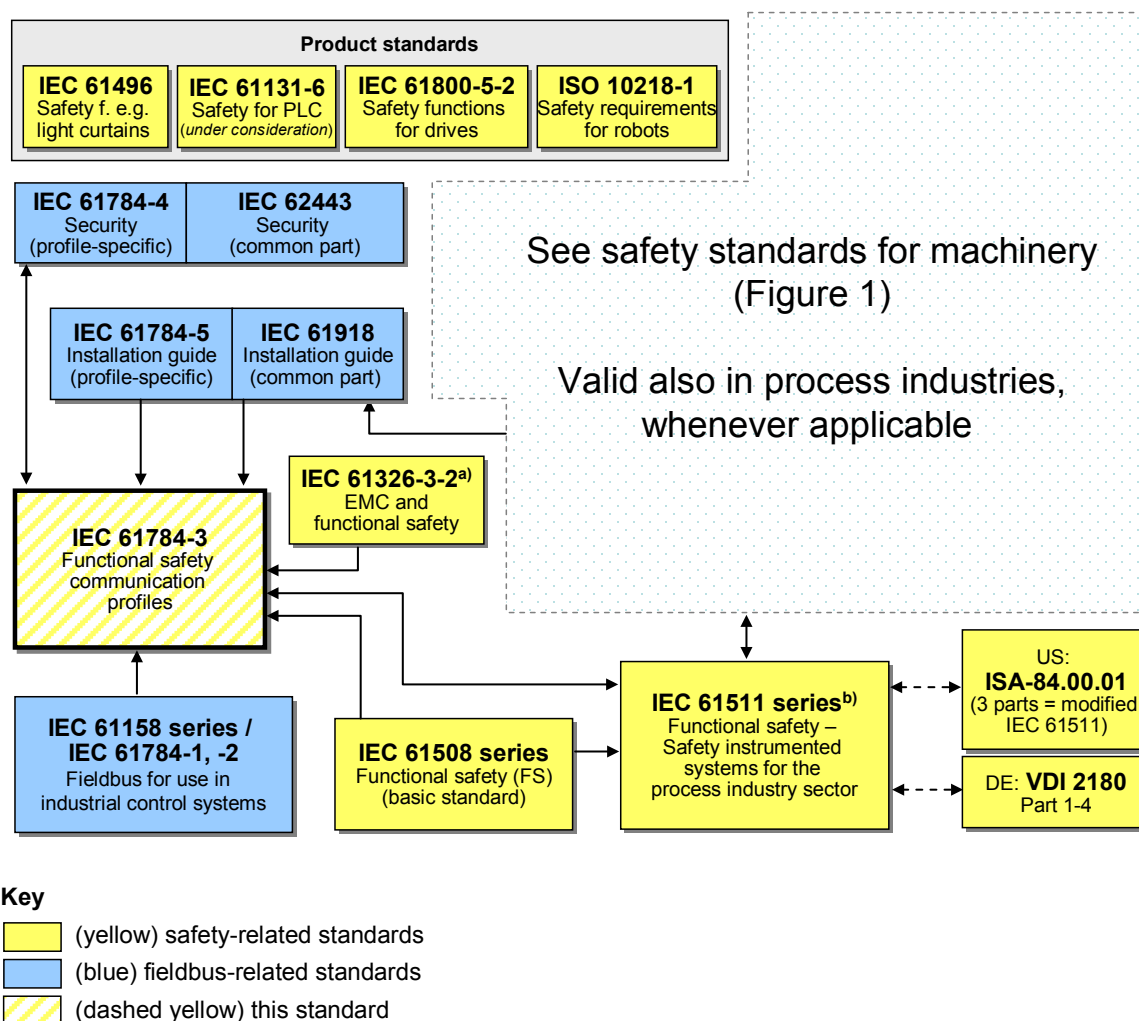
Figure 1 shows the relationships between this standard and relevant safety and fieldbus standards in a machinery environment.



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.

^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.

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

DE 10 2004 044 764.0 [BE] Datenübertragungsverfahren und Automatisierungssystem
zum Einsatz eines solchen Datenübertragungsverfahrens

EP 05 733 921.0 [BE] Sicherheitssteuerung

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:

[BE] Beckhoff Automation GmbH
Eiserstrasse 5, 33415 Verl
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.

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES –

Part 3-12: Functional safety fieldbuses – Additional specifications for CPF 12

1 Scope

This part of the IEC 61784-3 series specifies a safety communication layer (services and protocol) based on CPF 12 of IEC 61784-2 and IEC 61158 Type 12. 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 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 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 60204-1, *Safety of machinery – Electrical equipment of machines – Part 1: General requirements*

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

IEC 61158-3-12, *Industrial communication networks – Fieldbus specifications – Part 3-12: Data-link layer service definition – Type 12 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 61158-4-12, *Industrial communication networks – Fieldbus specifications – Part 4-12: Data-link layer protocol specification – Type 12 elements*

IEC 61158-5-12, *Industrial communication networks – Fieldbus specifications – Part 5-12: Application layer service definition – Type 12 elements*

IEC 61158-6-12, *Industrial communication networks – Fieldbus specifications – Part 6-12: Application layer protocol specification – Type 12 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 61784-2, *Industrial communication networks – Profiles – Part 2: Additional fieldbus profiles for real-time networks based on ISO/IEC 8802-3*

IEC 61784-3:2010³, *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*

³ In preparation.

SOMMAIRE

AVANT-PROPOS	102
0 Introduction	104
0.1 Généralités.....	104
0.2 Déclaration de droits de propriété.....	108
1 Domaine d'application	110
2 Références normatives	110
3 Termes, définitions, symboles, abréviations et conventions	111
3.1 Termes et définitions	111
3.1.1 Termes et définitions communs	111
3.1.2 CPF 12: Termes et définitions supplémentaires	116
3.2 Symboles et abréviations	117
3.2.1 Symboles et abréviations communs.....	117
3.2.2 CPF 12: Symboles et abréviations supplémentaires	117
3.3 Conventions	117
4 Vue d'ensemble du FSCP 12/1 (Safety-over-EtherCAT™)	118
5 Généralités.....	119
5.1 Document externe de spécifications applicables au profil	119
5.2 Exigences fonctionnelles de sécurité	119
5.3 Mesures de sécurité	120
5.4 Structure de la couche de communication de sécurité	121
5.5 Relations avec la FAL (et DLL, PhL).....	122
5.5.1 Généralités.....	122
5.5.2 Types de données	122
6 Services de la couche de communication de sécurité	122
6.1 Connexion FSoE	122
6.2 Cycle FSoE	122
6.3 Services FSoE	123
7 Protocole de couche de communication de sécurité.....	124
7.1 Format de PDU de sécurité	124
7.1.1 Structure de PDU de Sécurité.....	124
7.1.2 PDU de sécurité "Commande"	126
7.1.3 CRC de PDU de sécurité	127
7.2 Procédure de communication FSCP 12/1	130
7.2.1 Cycle de message	130
7.2.2 Etats de nœuds FSCP 12/1	131
7.3 Réaction en cas d'erreurs de communication.....	141
7.4 Table d'états pour Maître FSoE	143
7.4.1 Diagramme d'état de Maître FSoE	143
7.4.2 Etat Reset (Réinitialisation)	147
7.4.3 Etat Session	148
7.4.4 Etat Connexion.....	151
7.4.5 Etat Paramètre	155
7.4.6 Etat Données.....	158
7.5 Table d'états pour Esclave FSoE.....	161
7.5.1 Diagramme d'état d'Esclave FSoE	161

7.5.2	Etat Réinitialisation.....	165
7.5.3	Etat Session	167
7.5.4	Etat Connexion.....	171
7.5.5	Etat Paramètre	176
7.5.6	Etat Données.....	181
8	Gestion de la couche de communication de sécurité.....	184
8.1	Traitement des paramètres FSCP 12/1	184
8.2	Paramètres de communication FSoE	184
9	Exigences relatives au système.....	185
9.1	Voyants et commutateurs	185
9.1.1	Etats des voyants et fréquences de clignotement	185
9.1.2	Voyants	186
9.2	Recommandations d'installation	187
9.3	Temps de réponse de la fonction de sécurité.....	187
9.3.1	Généralités.....	187
9.3.2	Détermination du temps du chien de garde FSoE	189
9.3.3	Calcul du temps de réponse de la fonction de sécurité le plus défavorable	190
9.4	Durée des demandes	191
9.5	Contraintes de calcul des caractéristiques du système	191
9.5.1	Généralités.....	191
9.5.2	Considérations d'ordre probabiliste.....	192
9.6	Maintenance.....	193
9.7	Manuel de sécurité	193
10	Evaluation	194
Annexe A (informative) Informations supplémentaires pour les profils de communication de sécurité fonctionnelle CPF 12		195
A.1	Calcul de la fonction de hachage	195
A.2		199
Annexe B (informative) Information pour l'évaluation des profils de communication de sécurité fonctionnelle CPF 12		200
Bibliographie.....		201
Tableau 1 – Eléments descriptifs d'un diagramme d'état		118
Tableau 2 – Erreurs de communication et mesures de détection		120
Tableau 3 – PDU de sécurité générale.....		126
Tableau 4 – PDU de sécurité courte		126
Tableau 5 – PDU de sécurité "Commande"		127
Tableau 6 – Séquence de calcul du CRC_0		127
Tableau 7 – Séquence de calcul du CRC_i (i>0)		128
Tableau 8 – Exemple d'héritage du CRC_0.....		129
Tableau 9 – Exemple pour des données de sécurité de 4 octets avec échange des octets 1 à 4 par les octets 5 à 8		130
Tableau 10 – PDU de Maître de Sécurité pour 4 octets de données de sécurité avec la commande = Réinitialisation après redémarrage (réinitialisation de la connexion) ou erreur		133

Tableau 11 – PDU d'Esclave de Sécurité pour 4 octets de données de sécurité avec la commande = Réinitialisation pour acquittement d'une commande Réinitialisation en provenance du Maître FSoE	133
Tableau 12 – PDU d'Esclave de Sécurité pour 4 octets de données de sécurité avec la commande = Réinitialisation après redémarrage (réinitialisation de la connexion) ou erreur	134
Tableau 13 – PDU de Maître de Sécurité pour 4 octets de données de sécurité avec la commande = Session.....	134
Tableau 14 – PDU d'Esclave de Sécurité pour 4 octets de données de sécurité avec la commande = Session.....	135
Tableau 15 – Données de sécurité transmises dans l'état Connexion	136
Tableau 16 – PDU de Maître de Sécurité pour 4 octets de données de sécurité dans l'état Connexion	136
Tableau 17 – PDU d'Esclave de Sécurité pour 4 octets de données de sécurité dans l'état Connexion	137
Tableau 18 – Données de sécurité transmises dans l'état Paramètre	137
Tableau 19 – Première PDU de Maître de Sécurité pour 4 octets de données de sécurité dans l'état Paramètre	138
Tableau 20 – Première PDU d'Esclave de Sécurité pour 4 octets de données de sécurité dans l'état Paramètre	138
Tableau 21 – Seconde PDU de Maître de Sécurité pour 4 octets de données de sécurité dans l'état Paramètre	139
Tableau 22 – Seconde PDU d'Esclave de Sécurité pour 4 octets de données de sécurité dans l'état Paramètre	139
Tableau 23 – PDU de Maître de Sécurité pour 4 octets de ProcessData dans l'état Données	140
Tableau 24 – PDU d'Esclave de Sécurité pour 4 octets de ProcessData dans l'état Données	140
Tableau 25 – PDU de Maître de Sécurité pour 4 octets de données de sécurité intégrée dans l'état Données.....	141
Tableau 26 – PDU d'Esclave de Sécurité pour 4 octets de données de sécurité intégrée dans l'état Données.....	141
Tableau 27 – Erreurs de communication FSoE	142
Tableau 28 – Codes d'erreurs de communication FSoE	142
Tableau 29 – Etats du Maître FSoE	143
Tableau 30 – Evénements dans la table d'états de Maître FSoE	145
Tableau 31 – Fonctions dans la table d'états de Maître FSoE	145
Tableau 32 – Variables dans la table d'états de Maître FSoE.....	146
Tableau 33 – Macros dans la table d'états de Maître FSoE	146
Tableau 34 – Etats de l'Esclave FSoE	161
Tableau 35 – Evénements dans la table d'états d'Esclave FSoE	163
Tableau 36 – Fonctions dans la table d'états d'Esclave FSoE	163
Tableau 37 – Variables dans la table d'états d'Esclave FSoE.....	164
Tableau 38 – Macros dans la table d'états d'Esclave FSoE.....	164
Tableau 39 – Paramètres de communication FSoE	185
Tableau 40 – Etats des voyants	185
Tableau 41 – Etats du voyant STATUS FSoE.....	187
Tableau 42 – Définition des temps	188

Figure 1 – Relations entre la CEI 61784-3 et d'autres normes (machines)	106
Figure 2 – Relations entre la CEI 61784-3 et d'autres normes (processus)	108
Figure 3 – Système FSCP 12/1 de base.....	119
Figure 4 – Architecture logicielle du protocole FSCP 12/1	121
Figure 5 – Cycle FSoE	123
Figure 6 – Structure de communication FSCP 12/1	124
Figure 7 – PDU de sécurité pour CPF 12 intégrée dans une PDU de type 12	125
Figure 8 – Etats de nœuds FSCP 12/1	132
Figure 9 – Diagramme d'état du Maître FSoE.....	144
Figure 10 – Diagramme d'état de l'Esclave FSoE	162
Figure 11 – Fréquences de clignotement des voyants.....	186
Figure 12 – Composantes d'une fonction de sécurité	188
Figure 13 – Calcul des temps de chien de garde FsoE pour les connexions d'entrée et de sortie	189
Figure 14 – Calcul du temps de réponse le plus défavorable de la fonction de sécurité.....	190
Figure 15 – PDU de sécurité intégrée dans une PDU normale	192
Figure 16 – Taux d'erreurs résiduelles pour des données de sécurité de 8/16/24 bits et jusqu'à 12 144 bits de données normales	193

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

RÉSEAUX DE COMMUNICATION INDUSTRIELS – PROFILS –

Partie 3-12: Bus de terrain de sécurité fonctionnelle – Spécifications supplémentaires pour CPF 12

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.

La Norme internationale CEI 61784-3-12 a été établie par le sous-comité 65C: Réseaux de communication industriels, du comité d'études 65 de la CEI: Mesure, commande et automation dans les processus industriels.

La présente version bilingue (2012-02) correspond à la version anglaise monolingue publiée en 2010-06.

Le texte anglais de cette norme est issu des documents 65C/591A/FDIS et 65C/603/RVD.

Le rapport de vote 65C/603/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.

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

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.

IMPORTANT – Le logo “couleur 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.

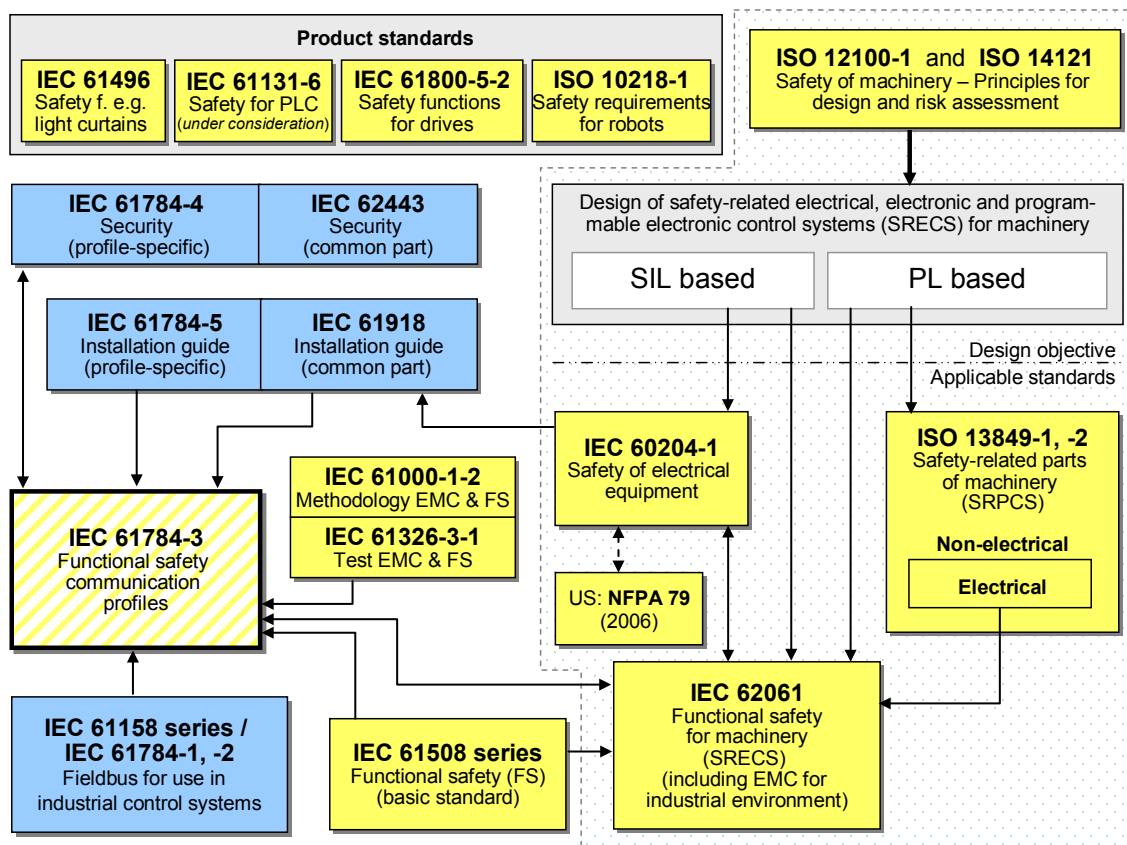
0 Introduction

0.1 Généralités

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 de 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 protocoles 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.



Légende

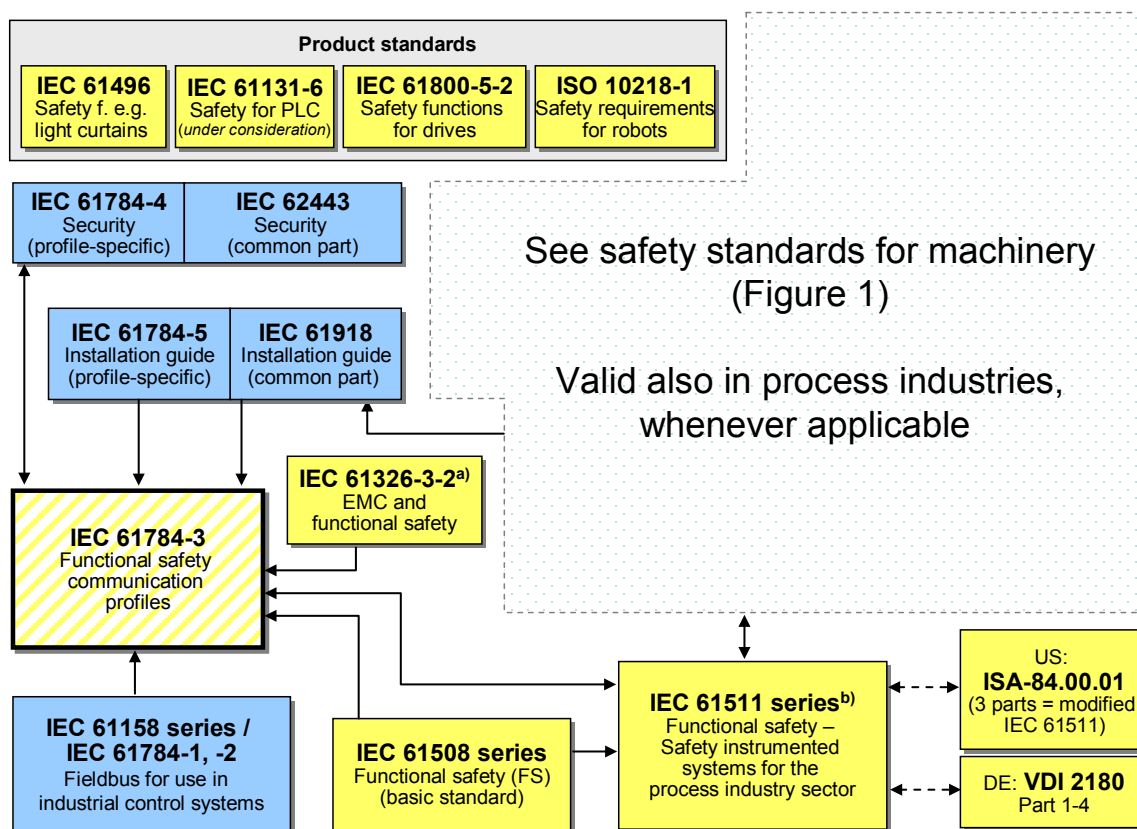
Anglais	Français
Product standards	Normes de produits
Safety function, e.g. light curtains	Fonction de sécurité, par exemple rideaux de lumière
Safety for PLC (under consideration)	Sécurité relative aux automates programmables (à l'étude)
Safety functions for drives	Fonctions de sécurité applicables aux entraînements
Safety requirements for robots	Exigences de sécurité applicables aux robots
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)

Anglais	Français
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
Methodology EMC & functional safety	Méthodologie en matière de compatibilité électromagnétique & sécurité fonctionnelle
Test EMC & functional safety	Essai CEM et sécurité fonctionnelle
Functional safety communication profiles	Profils de communication de sécurité fonctionnelle
IEC 61158 series / Fieldbus for use in industrial control systems	Série CEI 61158 / Bus de terrain pour utilisation dans des systèmes de commande industriels
IEC 61508 series, Functional safety (basic standard)	Série CEI 61508 Sécurité fonctionnelle (norme de base)
Functional safety for machinery for industrial environment)	Sécurité fonctionnelle des systèmes de commande électriques, électroniques et électroniques programmables (y compris les interférences électromagnétiques dans l'environnement industriel)
Key	Légende
(yellow) safety-related standards	(jaune) normes relatives à la sécurité
(blue) fieldbus-related standards	(bleu) normes relatives au bus de terrain
(dashed) yellow) this standard	(jaune pointillé) la présente norme
IEC	CEI

NOTE Les paragraphes 6.7.6.4 (complexité élevée) et 6.7.8.1.6 (faible complexité) de la CEI 62061 précisent la relation entre le niveau de performance PL (catégorie) et le niveau d'intégrité de sécurité SIL.

Figure 1 – Relations 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.



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 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
Functional safety communication profiles	Profils de communication de sécurité fonctionnelle

Anglais	Français
IEC 61326-3-2 a) EMC and functional safety	CEI 61326-3-2 a) CEM & sécurité fonctionnelle
IEC 61158 series/ IEC 61784-1-2, Fieldbus for use in industrial control systems	Série CEI 61158/ CEI 61784-1,-2 Bus de terrain pour utilisation dans des systèmes de commande industriels
IEC 61508 series, Functional safety (basic standard)	Série CEI 61508 Sécurité fonctionnelle (norme de base)
IEC 61511 seriesb) Functional safety–safety instrumented systems for the process industry sector	Série CEI 61511b) sécurité fonctionnelle – systèmes instrumentés de sécurité pour le secteur des industries de transformation
US: ISA 84.00.1 (3 parts = modified IEC 61511)	US: ISA 84.00.1 (3 parties = CEI 61511 modifiée)
DE : VDI 2180 Part 1 –4	DE : VDI 2180 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; Autrement, la CEI 61326-3-1 s'applique.

^b EN ratifiée.

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

Les couches de communication de sécurité mises en oeuvre 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 sécuritaire, 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 oeuvre du profil de communication de sécurité fonctionnelle retenu au sein du système – la mise en oeuvre 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 oeuvre 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.

0.2 Déclaration de droits de propriété

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 12 comme suit, où la notation [xx] désigne le détenteur des droits de propriété:

DE 10 2004 044 764.0 [BE] Datenübertragungsverfahren und Automatisierungssystem
zum Einsatz eines solchen Datenübertragungsverfahrens

EP 05 733 921.0 [BE] Sicherheitssteuerung

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

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

Des informations peuvent être obtenues auprès de:

[BE] Beckhoff Automation GmbH
Eiserstrasse 5, 33415 Verl
ALLEMAGNE

L'attention est par ailleurs attirée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues autres que ceux identifiés ci-dessus. 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.

RÉSEAUX DE COMMUNICATION INDUSTRIELS – PROFILS –

Partie 3-12: Bus de terrain de sécurité fonctionnelle – Spécifications supplémentaires pour CPF 12

1 Domaine d'application

La présente partie de la série CEI 61784-3 spécifie une couche de communication sécuritaire (services et protocole) fondée sur la CPF 12 de la CEI 61784-2 et le type 12 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 partie ¹ 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 ² 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 oeuvre du profil de communication de sécurité fonctionnelle retenu au sein du système – la mise en oeuvre 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).

CEI 60204-1, *Sécurité des machines – Equipement électrique des machines – Partie 1: Règles générales*

CEI 61000-6-2, *Compatibilité électromagnétique (CEM) – Partie 6-2: Normes génériques – Immunité pour les environnements industriels*

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

IEC 61158-2, *Industrial communication networks – Fieldbus specifications – Part 2: Physical layer specification and service definition* (disponible uniquement en anglais)³

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

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

³ Les publications monolingues des séries IEC 61158 et IEC 61784 sont actuellement en cours de traduction.

IEC 61158-3-12, *Industrial communication networks – Fieldbus specifications – Part 3-12: Data-link layer service definition – Type 12 elements* (disponible uniquement en anglais)

IEC 61158-4-12, *Industrial communication networks – Fieldbus specifications – Part 4-12: Data-link layer protocol specification – Type 12 elements* (disponible uniquement en anglais)

IEC 61158-5-12, *Industrial communication networks – Fieldbus specifications – Part 5-12: Application layer service definition – Type 12 elements* (disponible uniquement en anglais)

IEC 61158-6-12, *Industrial communication networks – Fieldbus specifications – Part 6-12: Application layer protocol specification – Type 12 elements* (disponible uniquement en anglais)

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

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

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

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

IEC 61784-3:2010⁴, *Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions* (disponible uniquement en anglais)

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

⁴ En cours d'élaboration.