IEC 61784-3-14

Edition 1.0 2010-06

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Industrial communication networks – Profiles – Part 3-14: Functional safety fieldbuses – Additional specifications for CPF 14

Réseaux de communication industriels – Profils – Partie 3-14: Bus de terrain de sécurité fonctionnelle – Spécifications supplémentaires pour CPF 14



IEC 61784-3-14:2010



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2010 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester.
If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de la CEI ou du Comité national de la CEI du pays du demandeur.
Si vous avez des questions sur le copyright de la CEI ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de la CEI de votre pays de résidence.

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
info@iec.ch
www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

Useful links:

IEC publications search - www.iec.ch/searchpub

The advanced search enables you to find IEC publications by a variety of criteria (reference number, text, technical committee,…).
It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

Stay up to date on all new IEC publications. Just Published details all new publications released. Available on-line and also once a month by email.

Electropedia - www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 30 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary (IEV) on-line.

Customer Service Centre - webstore.iec.ch/csc

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: csc@iec.ch.

A propos de la CEI

La Commission Electrotechnique Internationale (CEI) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications CEI

Le contenu technique des publications de la CEI est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Liens utiles:

Recherche de publications CEI - www.iec.ch/searchpub

La recherche avancée vous permet de trouver des publications CEI en utilisant différents critères (numéro de référence, texte, comité d'études,…).
Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

Just Published CEI - webstore.iec.ch/justpublished

Restez informé sur les nouvelles publications de la CEI. Just Published détaille les nouvelles publications parues. Disponible en ligne et aussi une fois par mois par email.

Electropedia - www.electropedia.org

Le premier dictionnaire en ligne au monde de termes électroniques et électriques. Il contient plus de 30 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans les langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (VEI) en ligne.

Service Clients - webstore.iec.ch/csc

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: csc@iec.ch.

IEC 61784-3-14

Edition 1.0 2010-06

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Industrial communication networks – Profiles – Part 3-14: Functional safety fieldbuses – Additional specifications for CPF 14

Réseaux de communication industriels – Profils – Partie 3-14: Bus de terrain de sécurité fonctionnelle – Spécifications supplémentaires pour CPF 14

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

PRICE CODE
CODE PRIX XB

ICS 25.040.40, 35.100.05

ISBN 978-2-88912-946-1

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.

® Registered trademark of the International Electrotechnical Commission
Marque déposée de la Commission Electrotechnique Internationale

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 14: Additional terms and definitions 16
3.2 Symbols and abbreviated terms 16
3.2.1 Common symbols and abbreviated terms 16
3.2.2 CPF 14: Additional symbols and abbreviated terms 17
3.3 Conventions 17
4 Overview of FSCP 14/1 (EPASafety®) 18
4.1 EPASafety® 18
4.2 Principle of EPA safety communications 18
4.3 Safety function processing 19
5 General 19
5.1 External documents providing specifications for the profile 19
5.2 Safety functional requirements 20
5.3 Safety measures 20
5.4 Safety communication layer structure 21
5.4.1 Combination of standard communication and safety communication systems 21
5.4.2 CP 14/1 safety communication structure 22
5.5 Relationships with FAL (and DLL, PhL) 23
5.5.1 Overview 23
5.5.2 Data types 23
6 Safety communication layer services 24
6.1 Overview 24
6.2 FSCP 14/1 object extensions 24
6.2.1 General 24
6.2.2 Functional safety communication management object 25
6.2.3 Functional Safety Link Object 26
6.2.4 Functional safety communication alert object 29
6.3 Extended services 30
6.3.1 General 30
6.3.2 SafetyCommunicationOpen 31
6.3.3 SafetyCommunicationClose 32
7 Safety communication layer protocol 34
7.1 Safety PDU format 34
7.1.1 General 34
7.1.2 APDU header structure 34
7.1.3 Functional safety PDU 34
7.2 Safety communication operation 36

7.2.1 Sequence number 36
7.2.2 RelationKey 36
7.2.3 Feedback message 37
7.2.4 CRC-cross-check 37
7.2.5 Scheduling number 37
7.2.6 Time stamp 39
7.2.7 Time expectation 39
7.2.8 Time synchronization monitoring 39
7.2.9 Communication scheduling precision monitoring 39
7.3 Safety communication behaviour 39
7.3.1 Protocol state description of periodic data transmission 39
7.3.2 Protocol state description of non-periodic data transmission 41
7.3.3 Protocol state description of alert report for communication fault 46
7.3.4 Function description 49
7.4 Code 51
7.4.1 Object code 51
7.4.2 Service code 53
8 Safety communication layer management 59
8.1 Time synchronization diagnostics 59
8.1.1 Time synchronization process 59
8.1.2 Time synchronization management 60
8.2 CSME diagnostics 60
8.2.1 General 60
8.2.2 CSME diagnostics management 60
8.3 Communication fault management 61
8.3.1 Configuration management 61
8.3.2 Communication fault report process 61
9 System requirements 64
9.1 Indicators and switches 64
9.2 Installation guidelines 64
9.3 Safety function response time 64
9.3.1 General 64
9.3.2 Calculation of the network reaction time 65
9.4 Duration of demands 66
9.5 Constraints for calculation of system characteristics 66
9.6 Maintenance 67
9.7 Safety manual 67
10 Assessment 67
Annex A (informative) Additional information for functional safety communication profiles of CPF 14 68
A.1 Hash function calculation 68
A.2 69
Annex B (informative) Information for assessment of the functional safety communication profiles of CPF 14 70
Bibliography 71

Table 1 – Relationships between errors and safety measures 21
Table 2 – Data types used within FSCP 14/1 24

Table 3 – FSCP 14/1 object extensions 24
Table 4 – Functional safety service extension 31
Table 5 – SafetyCommunicationOpen Service Parameters 31
Table 6 – SafetyCommunicationClose Service Parameters 33
Table 7 – Encoding of APDU Header 34
Table 8 – Structure of Functional Safety PDU (FSPDU) Header 35
Table 9 – CRC calculation polynomials 37
Table 10 – Functional safety communication state description 40
Table 11 – States and transitions of periodic data transmission 40
Table 12 – Functional safety communication states description 42
Table 13 – States and transitions of non-periodic data transmission 42
Table 14 – Communication alert state description 47
Table 15 – Communication alert states and transitions 47
Table 16 – LinkObjectType function description 49
Table 17 – CRCCheck function description 49
Table 18 – CrossCheck function description 50
Table 19 – TimeDelayCheck function description 50
Table 20 – PeriodUncomfrimedSNCheck function description 50
Table 21 – Non-periodicSNCheck function description 50
Table 22 – Functional safety communication management object encoding 51
Table 23 – Functional safety link object encoding 51
Table 24 – Functional safety communication alert object encoding 53
Table 25 – Encoding of SafetyCommunicationOpen request parameters 56
Table 26 – SafetyCommunicationOpen positive response parameters 56
Table 27 – SafetyCommunicationOpen negative response parameters 57
Table 28 – SafeCommunicationClose request parameters 57
Table 29 – SafeCommunicationClose positive response parameters 57
Table 30 – SafeCommunicationClose negative response parameters 57
Table 31 – Error class and code 58
Table 32 – Communication process of confirmed service between two devices 61
Table 33 – Settings for time expectation margin 65
Table 34 – Constraints for system characteristics at $\varepsilon = 10^{-2}$ 67

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 – Safety communication architecture 19
Figure 4 – Safety function processing 19
Figure 5 – Standard communication and safety communication 22
Figure 6 – CP 14/1 protocol hierarchy 23
Figure 7 – Relationship between the SCL and the other layers of CP 14/1 23
Figure 8 – Functional safety communication message structure 34
Figure 9 – Structure of Functional Safety PDU (FSPDU) 35
Figure 10 – Structure of Virtual Safety Check Message (VSCM) 35

Figure 11 – FSPDU mapping 36
Figure 12 – Time-sharing communication scheduling 38
Figure 13 – Format of EndofNonPeriodicDataSending PDU 38
Figure 14 – State transfer figure of periodic data transmission 40
Figure 15 – Functional safety communication state transfer 41
Figure 16 – Communication alert report state transfer figure 46
Figure 17 – CRC check for time synchronization process 59
Figure 18 – The process of communication fault report 63
Figure 19 – Example application for FSCP 14/1 communication 64
Figure 20 – Calculation of the network reaction time 65

INTERNATIONAL ELECTROTECHNICAL COMMISSION

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES –

Part 3-14: Functional safety fieldbuses – Additional specifications for CPF 14

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 61784-3-14 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.

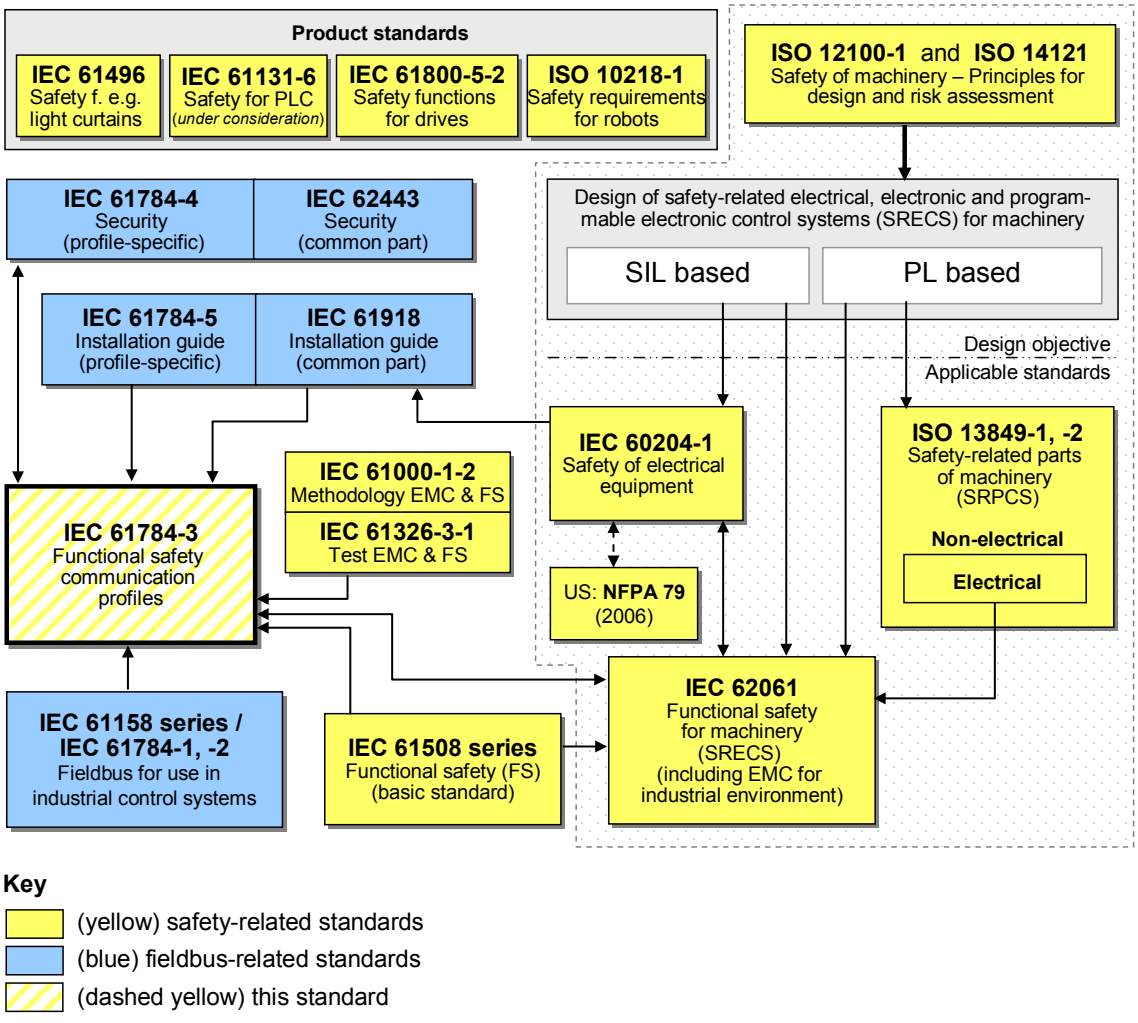
0 Introduction

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.

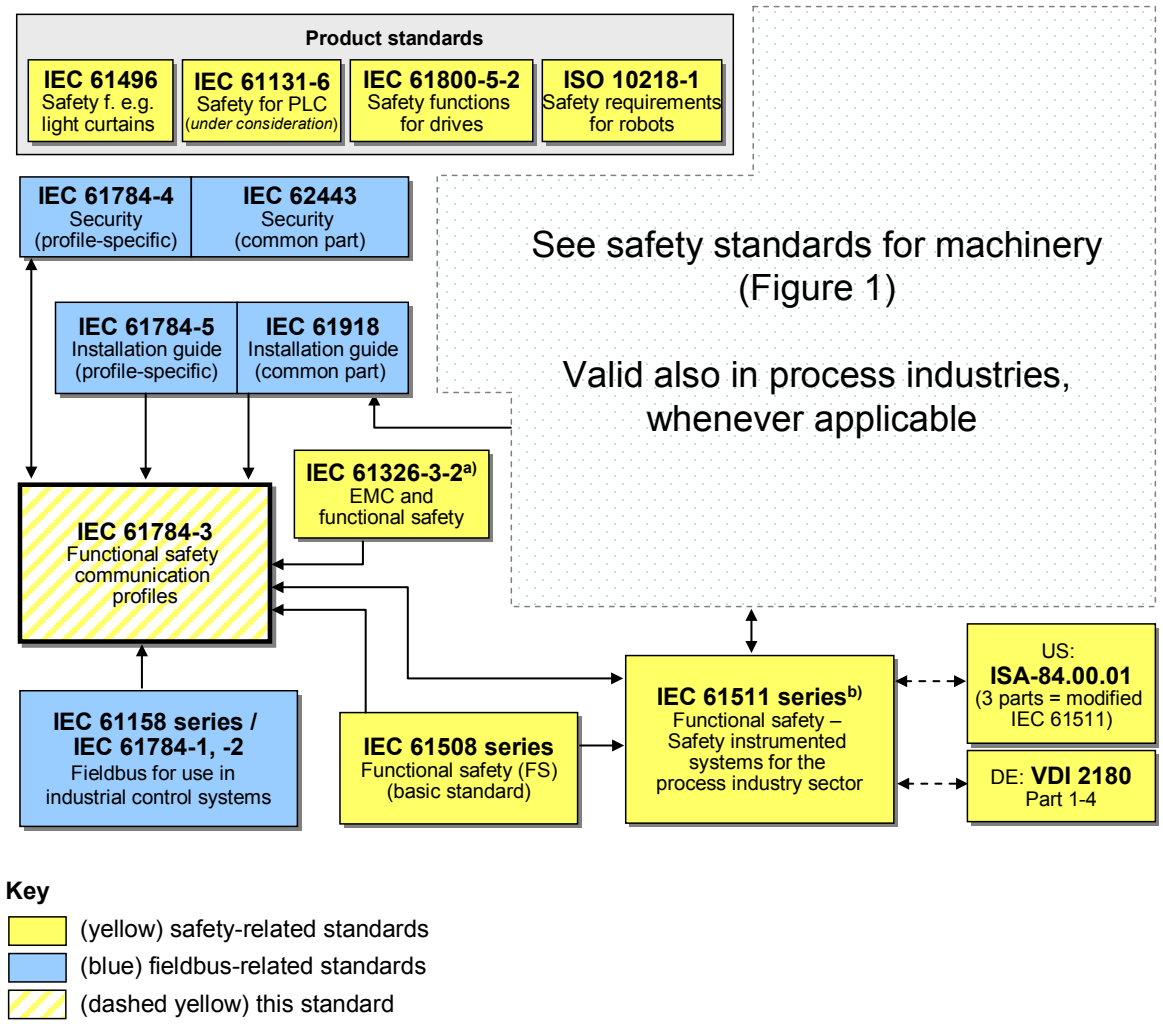
Figure 1 shows the relationships between this standard and relevant safety and fieldbus standards in a machinery environment.



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

CN1960247	[SxZ]	Method of Safety communication for industrial network
CN1929373	[SxZ]	The safety communication for the safety instrument system applied in industrial process.
CN101035030	[SxZ]	The diagnosis method and the equipment for monitoring the industrial Ethernet message.

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:

[SxZ] SUPCON and Zhejiang university
Dongqin FENG

(1) Zhejiang SUPCON Technology Co., Ltd.
Liuhe Road 309, Bingjiang District,
Hangzhou, CHINA 310053

(2) Zhejiang University
Zheda Road 38,
Hangzhou CHINA 310027

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 3-14: Functional safety fieldbuses – Additional specifications for CPF 14

1 Scope

This part of the IEC 61784-3 series specifies a safety communication layer (services and protocol) based on CPF 14 of IEC 61784-2 and IEC 61158 Type 14. 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 part[1] 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[2] 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 61158 (all parts), *Industrial communication networks – Fieldbus specifications*

IEC 61158-3-14, *Industrial communication networks – Fieldbus specifications – Part 3-14: Data-link layer service definition – Type 14 elements*

IEC 61158-4-14, *Industrial communication networks – Fieldbus specifications – Part 4-14: Data-link layer protocol specification – Type 14 elements*

IEC 61158-5-14, *Industrial communication networks – Fieldbus specifications – Part 5-14: Application layer service definition – Type 14 elements*

IEC 61158-6-14, *Industrial communication networks – Fieldbus specifications – Part 6-14: Application layer protocol specification – Type 14 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 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 61588, *Precision clock synchronization protocol for networked measurement and control systems*

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

IEC 61784-3:2010[3], *Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions*

ISO/IEC 8802-3, *Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications*

3 Terms, definitions, symbols, abbreviated terms and conventions

3.1 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1.1 Common terms and definitions

3.1.1.1
availability
probability for an automated system that for a given period of time there are no unsatisfactory system conditions such as loss of production

3.1.1.2
black channel
communication channel without available evidence of design or validation according to IEC 61508

3.1.1.3
bridge
abstract device that connects multiple network segments along the data link layer

3.1.1.4
communication channel
logical connection between two end-points within a *communication system*

3.1.1.5
communication system
arrangement of hardware, software and propagation media to allow the transfer of *messages* (ISO/IEC 7498 application layer) from one application to another

3.1.1.6
connection
logical binding between two application objects within the same or different devices

---

[3] In preparation.

SOMMAIRE

AVANT-PROPOS 78
0 Introduction 80
0.1 Généralités 80
0.2 Déclaration de droits de propriété 84
1 Domaine d'application 86
2 Références normatives 86
3 Termes, définitions, symboles, abréviations et conventions 87
3.1 Termes et définitions 87
3.1.1 Termes et définitions communs 87
3.1.2 CPF 14: Termes et définitions supplémentaires 91
3.2 Symboles et abréviations 92
3.2.1 Symboles et abréviations communs 92
3.2.2 CPF 14: Symboles et abréviations supplémentaires 92
3.3 Conventions 93
4 Vue d'ensemble de FSCP 14/1 (EPASafety®) 93
4.1 EPASafety® 93
4.2 Principe des communications de sécurité EPA 94
4.3 Traitement de la fonction de sécurité 94
5 Généralités 95
5.1 Documents externes de spécifications applicables au profil 95
5.2 Exigences fonctionnelles de sécurité 95
5.3 Mesures de sécurité 96
5.4 Structure de la couche de communication de sécurité 97
5.4.1 Combinaison des systèmes de communication standard et de communication de sécurité 97
5.4.2 Structure de la communication de sécurité CP 14/1 98
5.5 Relations avec la FAL (et DLL, PhL) 99
5.5.1 Vue d'ensemble 99
5.5.2 Types de données 100
6 Services de la couche de communication de sécurité 100
6.1 Vue d'ensemble 100
6.2 Extensions des objets FSCP 14/1 100
6.2.1 Généralités 100
6.2.2 Objet de gestion de communication de sécurité fonctionnelle 101
6.2.3 Objet de liaison de sécurité fonctionnelle 102
6.2.4 Objet d'alerte de communication de sécurité fonctionnelle 105
6.3 Services étendus 107
6.3.1 Généralités 107
6.3.2 SafetyCommunicationOpen 107
6.3.3 SafetyCommunicationClose 109
7 Protocole de couche de communication de sécurité 111
7.1 Format PDU de sécurité 111
7.1.1 Généralités 111
7.1.2 Structure d'en-tête APDU 111
7.1.3 PDU de sécurité fonctionnelle 111

7.2 Fonctionnement de la communication de sécurité 113
7.2.1 Numéro de séquence 113
7.2.2 RelationKey 113
7.2.3 Message de réaction 114
7.2.4 Contre-vérification du CRC 114
7.2.5 Numéro de programmation 115
7.2.6 Datation (horodatage) 116
7.2.7 Délai 116
7.2.8 Contrôle de la synchronisation temporelle 116
7.2.9 Contrôle de précision de la programmation de communication 117
7.3 Comportement de la communication de sécurité 117
7.3.1 Description d'état de protocole d'une transmission de données périodiques 117
7.3.2 Description d'état de protocole d'une transmission de données non périodiques 118
7.3.3 Description des états de protocole du rapport d'alerte applicable à l'anomalie de communication 123
7.3.4 Description des fonctions 126
7.4 Code 128
7.4.1 Code d'objet 128
7.4.2 Code de service 132
8 Gestion de la couche de communication de sécurité 138
8.1 Diagnostic de la synchronisation temporelle 138
8.1.1 Processus de synchronisation temporelle 138
8.1.2 Gestion de la synchronisation temporelle 138
8.2 Diagnostic CSME 139
8.2.1 Généralités 139
8.2.2 Gestion de diagnostic CSME 139
8.3 Gestion des anomalies de communication 140
8.3.1 Gestion de configuration 140
8.3.2 Processus de signalement des anomalies de communication 140
9 Exigences système 143
9.1 Voyants et commutateurs 143
9.2 Lignes directrices d'installation 143
9.3 Temps de réponse de la fonction de sécurité 143
9.3.1 Généralités 143
9.3.2 Calcul du temps de réaction du réseau 144
9.4 Durée des demandes 145
9.5 Contraintes liées au calcul des caractéristiques des systèmes 145
9.6 Maintenance 146
9.7 Manuel de sécurité 146
10 Evaluation 146
Annexe A (informative) Informations supplémentaires pour les profils de communication de sécurité fonctionnelle de CPF 14 147
A.1 Calcul de la fonction de hachage 147
A.2 148
Annexe B (informative) Informations pour l'évaluation des profils de communication de sécurité fonctionnelle de CPF 14 149
Bibliographie 150

Tableau 1 – Relations entre les erreurs et les mesures de sécurité 97
Tableau 2 – Types de données utilisés dans le cadre du protocole FSCP 14/1 100
Tableau 3 – Extensions des objets FSCP 14/1 101
Tableau 4 – Extension de services de sécurité fonctionnelle 107
Tableau 5 – Paramètres du service SafetyCommunicationOpen 108
Tableau 6 – Paramètres du service SafetyCommunicationClose 110
Tableau 7 – Codage de l'en-tête APDU 111
Tableau 8 – Structure de l'en-tête de la PDU de sécurité fonctionnelle (FSPDU) 112
Tableau 9 – Polynômes de calcul CRC 115
Tableau 10 – Description des états de communication de sécurité fonctionnelle 117
Tableau 11 – Etats et transitions d'une transmission de données périodiques 118
Tableau 12 – Description des états de communication de sécurité fonctionnelle 119
Tableau 13 – Etats et transitions d'une transmission de données non périodiques 119
Tableau 14 – Description des états d'alerte de communication 124
Tableau 15 – Etats et transitions d'alerte de communication 125
Tableau 16 – Description de la fonction LinkObjectType 126
Tableau 17 – Description de la fonction CRCCheck 127
Tableau 18 – Description de la fonction CrossCheck 127
Tableau 19 – Description de la fonction TimeDelayCheck 127
Tableau 20 – Description de la fonction PeriodUncomfrimedSNCheck 128
Tableau 21 – Description de la fonction Non-periodicSNCheck 128
Tableau 22 – Codage de l'objet de gestion de communication de sécurité fonctionnelle 128
Tableau 23 – Codage de l'objet de liaison de sécurité fonctionnelle 129
Tableau 24 – Codage de l'objet d'alerte de communication de sécurité fonctionnelle 131
Tableau 25 – Codage des paramètres de demande SafetyCommunicationOpen 135
Tableau 26 – Paramètres de réponse positive du service SafetyCommunicationOpen 135
Tableau 27 – Paramètres de réponse négative du service SafetyCommunicationOpen 135
Tableau 28 – Paramètres de demande SafeCommunicationClose 136
Tableau 29 – Paramètres de réponse positive du service SafetyCommunicationClose 136
Tableau 30 – Paramètres de réponse négative du service SafetyCommunicationClose 136
Tableau 31 – Classe et code d'erreurs 137
Tableau 32 – Processus de communication du service confirmé entre deux dispositifs 141
Tableau 33 – Paramètres applicables à la marge de délai 145
Tableau 34 – Contraintes liées aux caractéristiques des systèmes avec $\varepsilon = 10^{-2}$ 146

Figure 1 – Relation entre la CEI 61784–3 et d'autres normes (machines) 82
Figure 2 – Relation entre la CEI 61784–3 et d'autres normes (machines) 84
Figure 3 – Architecture de communication de sécurité 94
Figure 4 – Traitement de fonction de sécurité 94
Figure 5 – Communication standard et communication de sécurité 98
Figure 6 – Hiérarchie de protocole CP 14/1 99

Figure 7 – Relation entre la SCL et les autres couches de CP 14/1 99
Figure 8 – Structure de message de communication de sécurité fonctionnelle 111
Figure 9 – Structure de la PDU de sécurité fonctionnelle (FSPDU) 112
Figure 10 – Structure du message de contrôle de sécurité virtuel (VCSM) 112
Figure 11 – Mise en correspondance FSPDU 113
Figure 12 – Programmation de communication de partage de temps 116
Figure 13 – Format de la PDU EndofNonPeriodicDataSending 116
Figure 14 – Schéma de transfert d'états d'une transmission de données périodiques 117
Figure 15 – Transfert des états de communication de sécurité fonctionnelle 119
Figure 16 – Schéma de transfert des états du rapport d'alerte de communication 124
Figure 17 – Contrôle CRC applicable au processus de synchronisation temporelle 138
Figure 18 – Processus de signalement des anomalies de communication 142
Figure 19 – Exemple d'application de communication FSCP 14/1 143
Figure 20 – Calcul du temps de réaction du réseau 144

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

RÉSEAUX DE COMMUNICATION INDUSTRIELS – PROFILS –

Partie 3-14: Bus de terrain de sécurité fonctionnelle – Spécifications supplémentaires pour CPF 14

AVANT-PROPOS

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

La Norme internationale CEI 61784-3-14 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 "colour inside" qui se trouve sur la page de garde de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à la bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

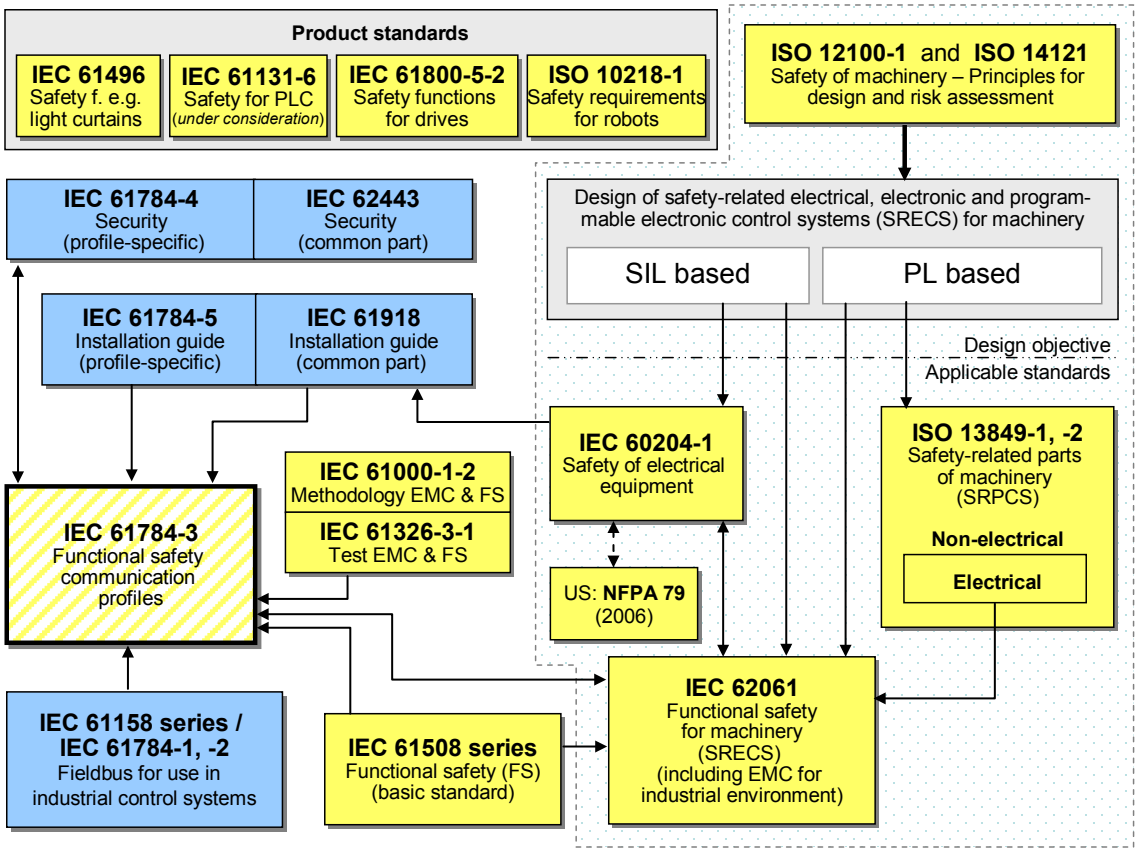
0 Introduction

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 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

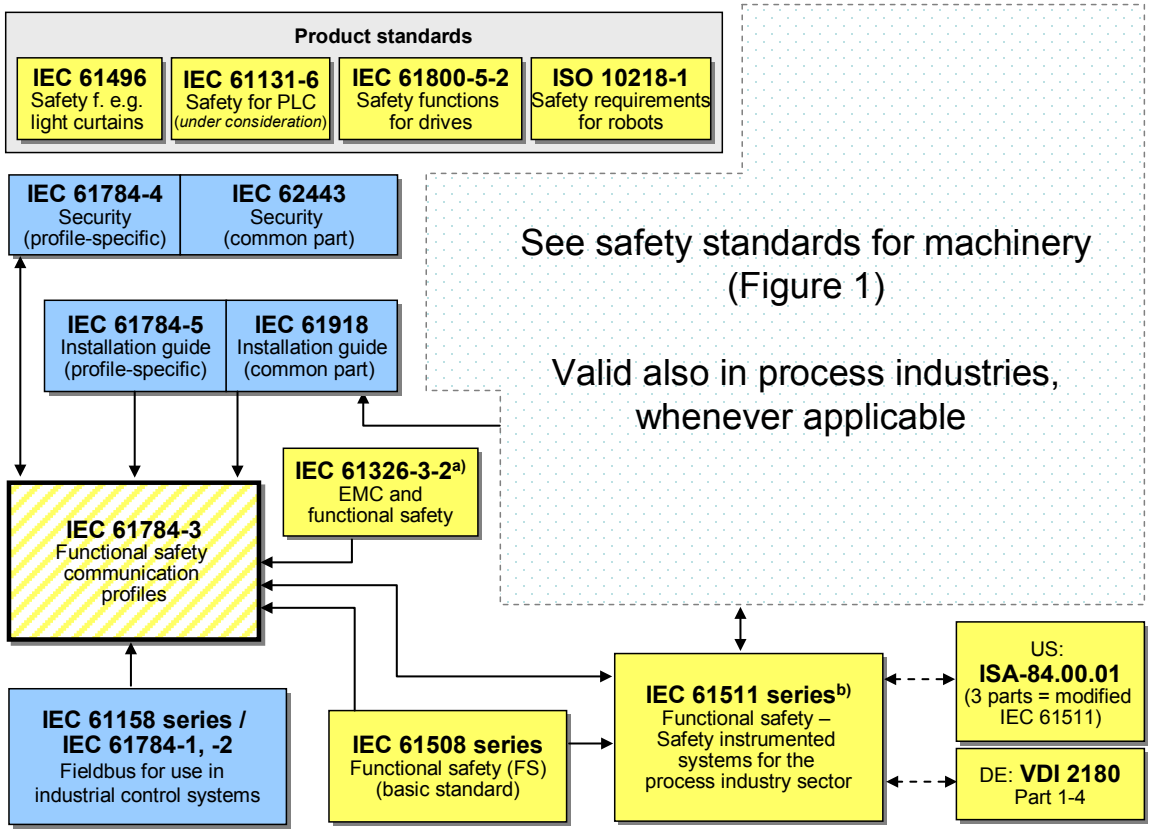
Anglais	Français
Product standards	Normes de produits
Safety function, e.g. light curtains	Fonction de sécurité, par exemple rideaux de lumière
Safety for PLC (under consideration)	Sécurité relative aux automates programmables (à l'étude)
Safety functions for drives	Fonctions de sécurité applicables 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	Electrique
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 (haute complexité) et 6.7.8.1.6 (faible complexité) de la CEI 62061 spécifient la relation entre PL (catégorie) et 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, sinon CEI 61326-3-1.

[b] EN ratifiée.

Figure 2 – Relation 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 dispositif normal ne suffit pas à le qualifier de dispositif de sécurité.

La présente norme décrit:

— les principes de base de mise en œuvre des exigences de la série CEI 61508 pour les communications de données relatives à la sécurité, y compris les défauts de transmission potentiels, les mesures correctives et les considérations concernant l'intégrité des données;

— la description individuelle des profils de sécurité fonctionnelle pour plusieurs familles de profils de communication dans 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 14, où la notation [xx] désigne le détenteur des droits de propriété.

CN1960247	[SxZ]	Method of Safety communication for industrial network
CN 1929373	[SxZ]	The safety communication for the safety instrument system applied in industrial process.
CN101035030	[SxZ]	The diagnosis method and the equipment for monitoring the industrial Ethernet message.

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:

[SxZ] SUPCON and Zhejiang university
Dongqin FENG

(1) Zhejiang SUPCON Technology Co., Ltd.
Liuhe Road 309, Bingjiang District,
Hangzhou, CHINE 310053

(2) Zhejiang University
Zheda Road 38,
Hangzhou CHINE 310027

L'attention est 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 mentionnés 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 3-14: Bus de terrain de sécurité fonctionnelle – Spécifications supplémentaires pour CPF 14

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 14 de la CEI 61784-2 et le Type 14 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 œuvre du profil de communication de sécurité fonctionnelle retenu au sein du système – la mise en œuvre du profil de communication de sécurité fonctionnelle, conforme à la présente partie, dans un dispositif normal ne suffit pas à le qualifier de dispositif de sécurité.

2 Références normatives

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

IEC 61158 (all parts), *Industrial communication networks – Fieldbus specifications* (disponible uniquement en anglais)[3]

IEC 61158-3–14, *Industrial communication networks – Fieldbus specifications – Part 3-14: Data-link layer service definition – Type 14 elements* (disponible uniquement en anglais)

IEC 61158-4-14, *Industrial communication networks – Fieldbus specifications – Part 4-14: Data-link layer protocol specification – Type 14 elements* (disponible uniquement en anglais)

---

1 Dans les pages suivantes de la présente norme, "la présente partie" se substitue à "cette partie de la série CEI 617843".

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 61158-5-14, *Industrial communication networks – Fieldbus specifications – Part 5-14: Application layer service definition – Type 14 elements* (disponible uniquement en anglais)

IEC 61158-6-14, *Industrial communication networks – Fieldbus specifications – Part 6-14: Application layer protocol specification – Type 14 elements* (disponible uniquement en anglais)

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

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

IEC 61588, *Precision clock synchronization protocol for networked measurement and control systems* (disponible uniquement en anglais)

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 61784-3:2010[4], *Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions* (disponible uniquement en anglais)

ISO/IEC 8802-3, *Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications* (disponible uniquement en anglais)

3 Termes, définitions, symboles, abréviations et conventions

3.1 Termes et définitions

Pour les besoins du présent document, les termes et définitions suivants s'appliquent.

3.1.1 Termes et définitions communs

3.1.1.1
disponibilité
probabilité, pour un système automatisé, qu'il ne se produise pas de conditions opérationnelles non satisfaisantes, telles que la perte de production, pendant une période donnée

3.1.1.2
canal noir
canal de communication sans preuve existante de conception ou de validation conformément à la CEI 61508

3.1.1.3
pont
dispositif abstrait qui relie des segments de réseau multiples le long de la couche de liaison de données

3.1.1.4
canal de communication
connexion logique entre deux points limites d'un *système de communication*

---

4 En cours d'élaboration.