IEC 61784-3-6

Edition 2.0 2010-06

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

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

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



IEC 61784-3-6:2010



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
Email: inmail@iec.ch
Web: 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.

- Catalogue of IEC publications: www.iec.ch/searchpub

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 It also gives information on projects, withdrawn and replaced publications.

- IEC Just Published: www.iec.ch/online_news/justpub

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

- Electropedia: www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 20 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary online.

- Customer Service Centre: www.iec.ch/webstore/custserv

If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us:
Email: csc@iec.ch
Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00

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.

- Catalogue des publications de la CEI: www.iec.ch/searchpub/cur_fut-f.htm

Le Catalogue en-ligne de la CEI vous permet d'effectuer des recherches en utilisant différents critères (numéro de référence, texte, comité d'études,…). Il donne aussi des informations sur les projets et les publications retirées ou remplacées.

- Just Published CEI: www.iec.ch/online_news/justpub

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

- Electropedia: www.electropedia.org

Le premier dictionnaire en ligne au monde de termes électroniques et électriques. Il contient plus de 20 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans les langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International en ligne.

- Service Clients: www.iec.ch/webstore/custserv/custserv_entry-f.htm

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions, visitez le FAQ du Service clients ou contactez-nous:
Email: csc@iec.ch
Tél.: +41 22 919 02 11
Fax: +41 22 919 03 00

IEC 61784-3-6

Edition 2.0 2010-06

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

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

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

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

PRICE CODE
CODE PRIX XC

ICS 25.040.40; 35.100.05

ISBN 978-2-88912-812-9

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

CONTENTS

FOREWORD 7
0 Introduction 9
0.1 General 9
0.2 Patent declaration 11
1 Scope 12
2 Normative references 12
3 Terms, definitions, symbols, abbreviated terms and conventions 13
3.1 Terms and definitions 13
3.1.1 Common terms and definitions 13
3.1.2 CPF 6: Additional terms and definitions 18
3.2 Symbols and abbreviated terms 18
3.2.1 Common symbols and abbreviated terms 18
3.2.2 CPF 6: Additional symbols and abbreviated terms 19
3.3 Conventions 20
4 Overview of FSCP 6/7 (INTERBUS™ Safety) 20
4.1 General 20
4.2 Technical overview 20
4.3 Functional Safety Communication Profile 6/7 21
5 General 22
5.1 External documents providing specifications for the profile 22
5.2 Safety functional requirements 22
5.3 Safety measures 22
5.3.1 General 22
5.3.2 Sequence number 23
5.3.3 Time stamp 23
5.3.4 Time expectation 23
5.3.5 Acknowledgement 23
5.3.6 Connection authentication 23
5.3.7 Distinction between safety relevant messages and non-safety relevant messages – different data integrity assurance system 24
5.3.8 Parameterized shutdown time 24
5.4 Safety communication layer structure 24
5.4.1 Decomposition process 24
5.4.2 Definition of the safety function of the safety communication system 25
5.4.3 Decomposition of the safety function of a safety communication system into function blocks 26
5.4.4 Assignment of the function blocks to subsystems 27
5.4.5 Safety requirements and safety integrity requirements 30
5.4.6 Specification of the safe state 30
5.4.7 Response to a fault 31
5.4.8 Stop category 33
5.4.9 Safe Transmission 33
5.5 Relationships with FAL (and DLL, PhL) 33
5.5.1 Overview 33
5.5.2 Use of the AR-US service to initiate and parameterize 34
5.5.3 Use of the AR-US service to transmit safety data 35

5.5.4 Use of the AR-US service to abort 36
5.5.5 Data types 36
6 Safety communication layer services 36
6.1 General 36
6.2 Transmission principle for safety messages between SCLM and SCLS 36
6.3 Function block requirements 37
6.3.1 Input Safe Data function block 37
6.3.2 Output Safe Data function block 37
6.3.3 Safe Calculation function block 37
6.4 Context management 38
6.4.1 Initiate service 38
6.4.2 Abort service 39
6.5 Function block parameterization 40
6.5.1 Send application parameter service 40
6.5.2 Send application parameter ID service 41
6.5.3 Parameterize device service 42
6.6 Safe Process Data Mode 42
6.6.1 Transmit-Safety-Data 42
6.6.2 Set-Diagnostic-Data service 44
6.6.3 Set-Acknowledgement-Data service 44
7 Safety communication layer protocol 45
7.1 Safety PDU format 45
7.1.1 Structure of safety messages 45
7.1.2 Description of the polynomial used 46
7.1.3 Structure of safety messages for safe parameterization and idle 46
7.1.4 Structure of safety messages for the transmission of safety data 52
7.1.5 Messages for synchronization 53
7.1.6 Structure of safety messages for aborting connections 54
7.2 State description 54
7.2.1 SCLM and SCLS state machines 54
7.2.2 Initiate 56
7.2.3 Parameterization 57
7.2.4 Process data mode 61
7.2.5 Process data mode with diagnostic data transmission 66
7.2.6 Process data mode with Acknowledgement-Data transmission 66
7.2.7 Connection aborted 67
7.3 Abort 67
7.3.1 Connection abort in the event of an error detected by the SCLM 67
7.3.2 Abort of all connections in the event of an error detected by the SCLS 68
7.3.3 Abort of all connections in the event of an error detected by the SCLM 70
8 Safety communication layer management 71
8.1 General 71
8.2 Requirements of safety communication layer management 71
8.3 Set-Safety-Configuration service 71
8.4 Start IEC 61158 Type 8 service 73
9 System requirements 73
9.1 Indicators and switches 73

9.2 Installation guidelines 73
9.3 Safety function response time 73
9.3.1 General 73
9.3.2 Calculation of the parameterized shutdown time 74
9.4 Duration of demands 78
9.5 Constraints for calculation of system characteristics 78
9.5.1 System characteristics 78
9.5.2 Calculation of the number of telegrams per second 78
9.6 Maintenance 79
9.7 Safety manual 80
10 Assessment 80
Annex A (informative) Additional information for functional safety communication profiles of CPF 6 81
Annex B (informative) Information for assessment of the functional safety communication profiles of CPF 6 82
Bibliography 83

Table 1 – Overview of profile identifier usable for FSCP 6/7 22
Table 2 – Selection of the various measures for possible errors 23
Table 3 – List of function blocks and subsystems 27
Table 4 – Signal flow between the function blocks 29
Table 5 – Initiate service parameters 38
Table 6 – Parameterization mode and related services 39
Table 7 – Abort service parameters 39
Table 8 – Abort of a point-to-point connection by the SRP or SRC 40
Table 9 – Send application parameter service 40
Table 10 – Send application parameter ID service 41
Table 11 – Parameterize device parameters 42
Table 12 – Transmit-Safety-Data service parameters 43
Table 13 – Set-Diagnostic-Data service parameters 44
Table 14 – Set-Acknowledgement-Data service parameters 45
Table 15 – Parameter ID 48
Table 16 – Block 0: Device ID 48
Table 17 – Block 1: Parameter record ID 49
Table 18 – Block 2: Application parameter 50
Table 19 – TIME encoding 52
Table 20 – Abort_Info: Connection abort in the event of an error detected by the SCLM 68
Table 21 – Abort_Info: Abort of all connections in the event of an error detected by the SCLS 69
Table 22 – Abort_Info: Abort of all connections in the event of an error detected by the SCLM 71
Table 23 – Set-Safety-Configuration service 72
Table 24 – Error_Info 72
Table 25 – Calculation of tIB 77
Table 26 – Calculation of tSRC 78
Table 27 – Calculation of tPST 78

Figure 1 – Relationships of IEC 61784-3 with other standards (machinery) 9
Figure 2 – Relationships of IEC 61784-3 with other standards (process) 10
Figure 3 – FSCP 6/7 communication preconditions 21
Figure 4 – Example of a safety function 25
Figure 5 – Decomposition of safety function into function blocks 26
Figure 6 – Overview of the results of the decomposition process 28
Figure 7 – Signal flow between the function blocks 28
Figure 8 – Interfaces between the safety devices within the safety communication system 29
Figure 9 – Signal flow and safe states 31
Figure 10 – Mapping of the Safe Transmission function block 33
Figure 11 – Relationship between SCL and the other layers of IEC 61158 Type 8 34
Figure 12 – Use of the AR-US service to initiate and parameterize 35
Figure 13 – Use of the AR-US service to transmit safety data 35
Figure 14 – Use of the AR-US service to abort 36
Figure 15 – Use of the AR-US service to abort 36
Figure 16 – Structure of the safety PDU 45
Figure 17 – Integration of safety data and deterministic remedial measures in the summation frame 46
Figure 18 – Write_Parameter_Byte_Req message 47
Figure 19 – Read_Parameter_Byte_Req message 47
Figure 20 – Parameter_Byte_Con message 47
Figure 21 – Set_Safety_Connection_ID_Req message 50
Figure 22 – Set_Safety_Connection_ID_Con message of safety slaves 50
Figure 23 – Parameter_Idle_Req 51
Figure 24 – Parameter_Idle_Con 51
Figure 25 – Parameter_Check_Con 51
Figure 26 – Parameter_Loc_ID_Changed_Con 51
Figure 27 – Transmit Safety Data Message 52
Figure 28 – Sync_a message of the SCLM 53
Figure 29 – Req_b message of the SCLM 53
Figure 30 – Req_c message of the SCLM 53
Figure 31 – Req_d message of the SCLM 54
Figure 32 – Abort_Connection message 54
Figure 33 – Safety-Slave_Error message 54
Figure 34 – SCLM state machine 55
Figure 35 – SCLS state machine 55
Figure 36 – Initiate sequence 56
Figure 37 – Send Application Parameter sequence 58
Figure 38 – Send Application Parameter ID sequence 59
Figure 39 – Parameterize device sequence 60
Figure 40 – Simultaneous transmission of safety data to the safety slaves 61
Figure 41 – Use of the sequence number in the SCLM and SCLS 62

Figure 42 – Startup and error-free operation 63
Figure 43 – Resynchronization during operation 64
Figure 44 – Invalid CRC 24 checksum detected by the SCLS 65
Figure 45 – Process data mode with diagnostic data transmission 66
Figure 46 – Process data mode with Acknowledgement-Data transmission 67
Figure 47 – Error when initiating a connection 68
Figure 48 – Error at an SCLS when aborting all connections 69
Figure 49 – Abort of all connections in the event of an error detected by the SCLM 70
Figure 50 – Overview of the shutdown time 75

INTERNATIONAL ELECTROTECHNICAL COMMISSION

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES –

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

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC 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 61784-3-6 has been prepared by subcommittee 65C: Industrial networks, of IEC technical committee 65: Industrial process measurement, control and automation.

This second edition cancels and replaces the first edition published in 2007. This edition constitutes a technical revision. The main changes with respect to the previous edition are listed below:

— updates in relation with changes in IEC 61784-3.

This bilingual version published in 2011-12, corresponds to the 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.

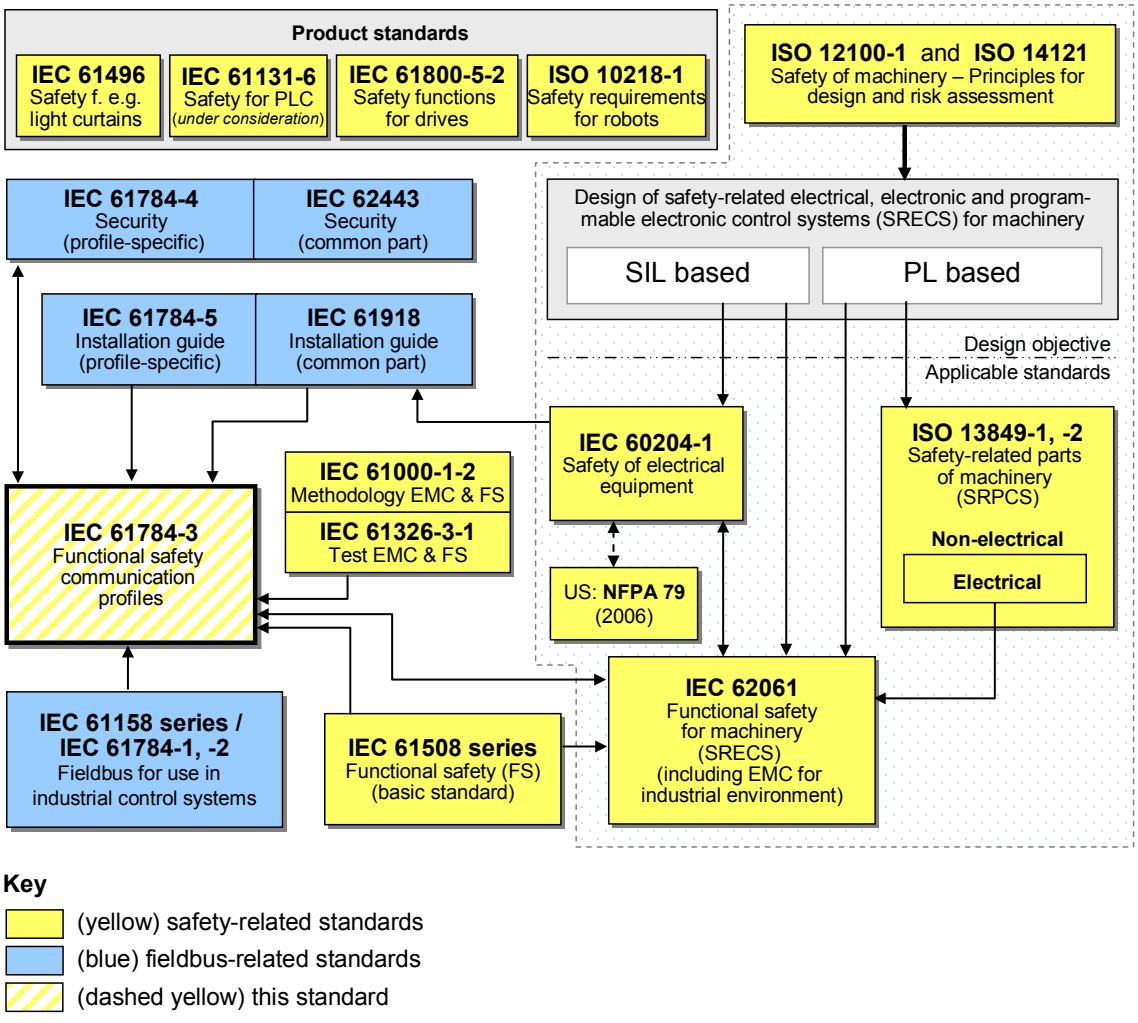
0 Introduction

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.

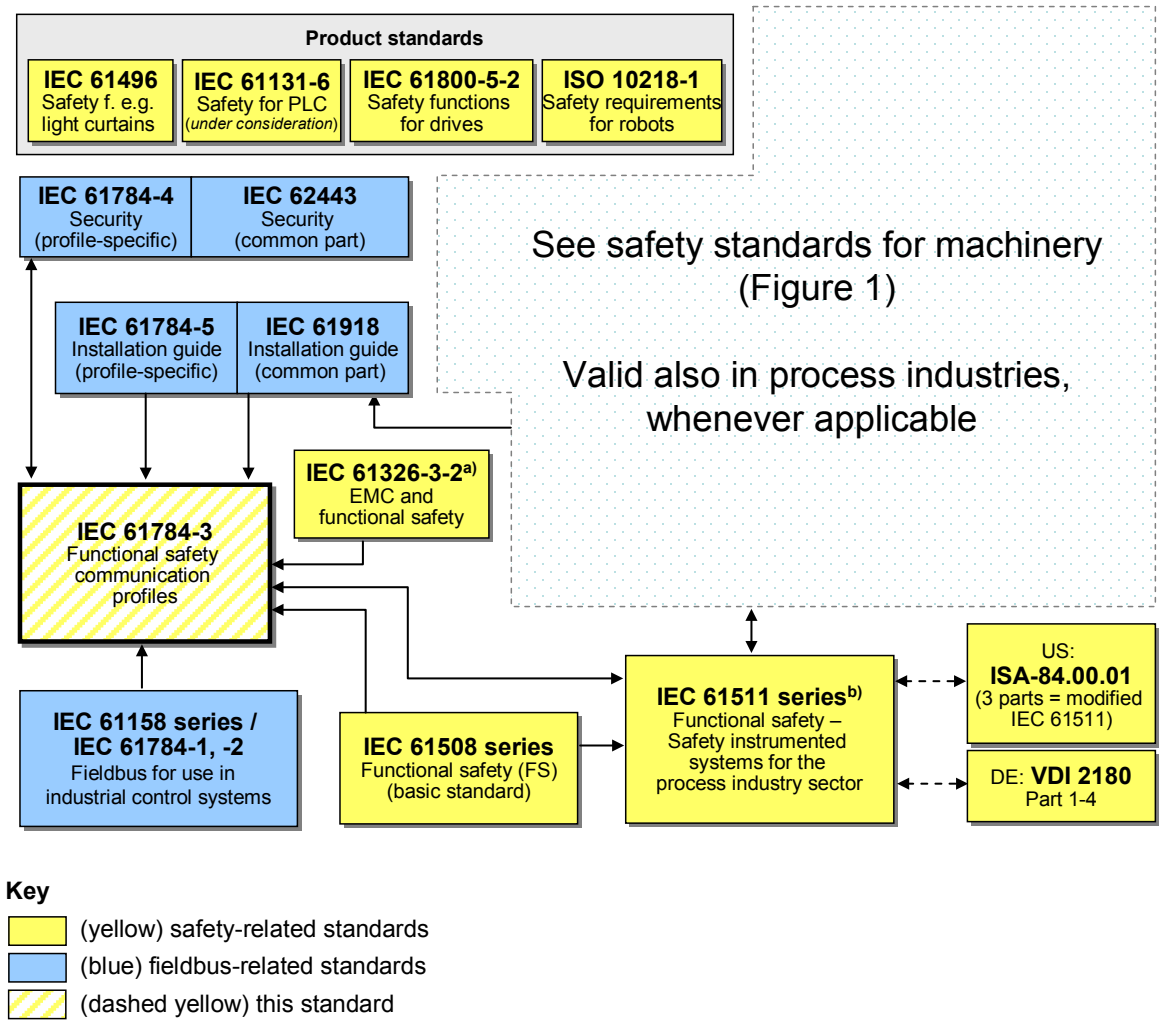
Figure 1 shows the relationships between this standard and relevant safety and fieldbus standards in a machinery environment.



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

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

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

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

Information may be obtained from:

[PxC] Phoenix Contact GmbH & Co. KG
Intellectual Property Licenses & Standards
Flachsmarktstr. 8
D-32825 Blomberg,
GERMANY

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights other than those identified above. IEC shall not be held responsible for identifying any or all such patent rights.

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES –

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

1 Scope

This part of the IEC 61784-3 series specifies a safety communication layer (services and protocol) based on CPF 6 of IEC 61784-1, IEC 61784-2 and IEC 61158 Type 8. It identifies the principles for functional safety communications defined in IEC 61784-3 that are relevant for this safety communication layer.

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

This 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 60204-1, *Safety of machinery – Electrical equipment of machines – Part 1: General requirements*

IEC 61131-3, *Programmable controllers – Part 3: Programming languages*

IEC 61158 (all parts), *Industrial communication networks – Fieldbus specifications*

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

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

IEC 61158-4-8, *Industrial communication networks – Fieldbus specifications – Part 4-8: Data-link layer protocol specification – Type 8 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 61158-5-8:2007, *Industrial communication networks – Fieldbus specifications – Part 5-8: Application layer service definition – Type 8 elements*

IEC 61158-6-8, *Industrial communication networks – Fieldbus specifications – Part 6-8: Application layer protocol specification – Type 8 elements*

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

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

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

IEC 61784-2, *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*

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

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

IEC 62061, *Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems*

ISO 12100-1, *Safety of machinery – Basic concepts, general principles for design – Part 1: Basic terminology, methodology*

ISO 13849-1, *Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design*

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
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] In preparation.

SOMMAIRE

AVANT-PROPOS 91
0 Introduction 93
0.1 Généralités 93
0.2 Déclaration de droits de propriété 97
1 Domaine d'application 99
2 Références normatives 99
3 Termes, définitions, symboles, abréviations et conventions 100
3.1 Termes et définitions 100
3.1.1 Termes et définitions communs 101
3.1.2 CPF 6: Termes et définitions supplémentaires 105
3.2 Symboles et abréviations 106
3.2.1 Symboles et abréviations communs 106
3.2.2 CPF 6: Symboles et abréviations supplémentaires 106
3.3 Conventions 107
4 Présentation de FSCP 6/7 (INTERBUS™ Safety) 108
4.1 Généralités 108
4.2 Présentation générale d'ordre technique 108
4.3 Profil de communication de sécurité fonctionnelle 6/7 109
5 Généralités 110
5.1 Documents externes de spécifications applicables au profil 110
5.2 Exigences fonctionnelles de sécurité 110
5.3 Mesures de sécurité 110
5.3.1 Généralités 110
5.3.2 Numéro de séquence 111
5.3.3 Datation 111
5.3.4 Délai 111
5.3.5 Acquittement 111
5.3.6 Authentification de connexion 111
5.3.7 Distinction entre les messages relatifs et non relatifs à la sécurité – différents systèmes d'assurance d'intégrité des données 112
5.3.8 Temps d'arrêt paramétré 112
5.4 Structure de la couche de communication de sécurité 112
5.4.1 Processus de décomposition 112
5.4.2 Définition de la fonction de sécurité du système de communication de sécurité 113
5.4.3 Décomposition de la fonction de sécurité d'un système de communication de sécurité en blocs de fonctions 114
5.4.4 Attribution des blocs de fonctions aux sous-systèmes 116
5.4.5 Exigences de sécurité et exigences d'intégrité de sécurité 120
5.4.6 Spécification de l'état de sécurité 121
5.4.7 Réponse à une anomalie 123
5.4.8 Catégorie d'arrêt 124
5.4.9 Transmission sécurisée 124
5.5 Relations avec la FAL (et DLL, PhL) 125
5.5.1 Présentation 125
5.5.2 Utilisation du service AR-US pour le démarrage et le paramétrage 126

5.5.3 Utilisation du service AR-US pour la transmission des données de sécurité 127
5.5.4 Utilisation du service AR-US pour l'abandon 128
5.5.5 Types de données 128
6 Services de la couche de communication de sécurité 128
6.1 Généralités 128
6.2 Principe de transmission des messages de sécurité entre le SCLM et le SCLS 128
6.3 Exigences relatives au bloc de fonctions 129
6.3.1 Bloc de fonctions Données d'entrée sécurisées 129
6.3.2 Bloc de fonctions Données de sortie sécurisées 129
6.3.3 Bloc de fonctions Calcul sécurisé 129
6.4 Gestion de contexte 130
6.4.1 Service Initiate 130
6.4.2 Service Abort 131
6.5 Paramétrage du bloc de fonctions 132
6.5.1 Service Send Application Parameter (Envoi du paramètre d'application) 132
6.5.2 Service Send Application Parameter ID (Envoi de l'ID du paramètre d'application) 133
6.5.3 Service « Parameterize Device » 133
6.6 Mode de données de processus sécurisé 134
6.6.1 Transmit-Safety-Data (Transmission de données de sécurité) 134
6.6.2 Service Set-Diagnostic-Data (Définition des données de diagnostic) 136
6.6.3 Service Set-Acknowledgement-Data (Définition des données d'acquittement) 136
7 Protocole de couche de communication de sécurité 137
7.1 Format PDU de sécurité 137
7.1.1 Structure des messages de sécurité 137
7.1.2 Description du polynôme utilisé 138
7.1.3 Structure des messages de sécurité du paramétrage sécurisé et de l'état de repos 138
7.1.4 Structure des messages de sécurité pour la transmission des données de sécurité 144
7.1.5 Messages de synchronisation 145
7.1.6 Structure des messages de sécurité d'abandon des connexions 146
7.2 Description d'état 146
7.2.1 Diagrammes d'états du SCLM et du SCLS 146
7.2.2 Initiate (Lancement) 149
7.2.3 Paramétrage 150
7.2.4 Mode de données de processus 157
7.2.5 Mode de données de processus avec transmission de données de diagnostic 162
7.2.6 Mode de données de processus avec transmission de données d'acquittement 162
7.2.7 Connexion abandonnée 163
7.3 Abort (Abandon) 163
7.3.1 Abandon de connexion en cas d'erreur détectée par le SCLM 163
7.3.2 Abandon de toutes les connexions en cas d'erreur détectée par le SCLS 164

7.3.3 Abandon de toutes les connexions en cas d'erreur détectée par le SCLM 166
8 Gestion de la couche de communication de sécurité 168
8.1 Généralités 168
8.2 Exigences en matière de gestion de la couche de communication de sécurité 168
8.3 Service Set-Safety-Configuration 168
8.4 Service Start IEC 61158 Type 8 169
9 Exigences système 169
9.1 Voyants et commutateurs 169
9.2 Lignes directrices d'installation 169
9.3 Temps de réponse de la fonction de sécurité 170
9.3.1 Généralités 170
9.3.2 Calcul du temps d'arrêt paramétré 170
9.4 Durée des demandes 175
9.5 Contraintes liées au calcul des caractéristiques du système 175
9.5.1 Caractéristiques du système 175
9.5.2 Calcul du nombre de messages par seconde 175
9.6 Maintenance 176
9.7 Manuel de sécurité 176
10 Évaluation 176
Annexe A (informative) Informations supplémentaires pour les profils de communication de sécurité fonctionnelle de CPF 6 178
Annexe B (informative) Informations pour l'évaluation des profils de communication de sécurité fonctionnelle de CPF 6 179
Bibliographie 180

Tableau 1 – Présentation générale de l'identifiant de profil applicable au protocole FSCP 6/7 109
Tableau 2 – Sélection des différentes mesures correspondant aux erreurs possibles 111
Tableau 3 – Liste des blocs de fonctions et des sous-systèmes 116
Tableau 4 – Flux de signal entre les blocs de fonctions 119
Tableau 5 – Paramètres du service Initiate 130
Tableau 6 – Mode de paramétrage et services connexes 131
Tableau 7 – Paramètres du service Abort 131
Tableau 8 – Abandon d'une connexion point à point par le SRP ou le SRC 132
Tableau 9 – Service Send Application Parameter 132
Tableau 10 – Service Send Application Parameter ID 133
Tableau 11 – Paramètres du service Parameterize Device 134
Tableau 12 – Paramètres du service Transmit-Safety-Data 135
Tableau 13 – Paramètres du service Set-Diagnostic-Data 136
Tableau 14 – Paramètres du service Set-Acknowledgement-Data 137
Tableau 15 – ID de paramètre 140
Tableau 16 – Bloc 0: ID de dispositif 140
Tableau 17 – Bloc 1: ID d'enregistrement de paramètre 141
Tableau 18 – Bloc 2: Paramètre d'application 142
Tableau 19 – Codage TIME 144

Tableau 20 – Abort_Info: Abandon de connexion en cas d'erreur détectée par le SCLM 164
Tableau 21 – Abort_Info: Abandon de toutes les connexions en cas d'erreur détectée par le SCLS 166
Tableau 22 – Abort_Info: Abandon de toutes les connexions en cas d'erreur détectée par le SCLM 167
Tableau 23 – Service Set-Safety-Configuration 168
Tableau 24 – Error_Info 169
Tableau 25 – Calcul de tIB 174
Tableau 26 – Calcul de tSRC 174
Tableau 27 – Calcul de tPST 174

Figure 1 - Relation entre la CEI 61784–3 et d'autres normes (machines) 95
Figure 2 - Relations entre la CEI 61784–3 et d'autres normes (transformation) 97
Figure 3 – Conditions préalables de communication FSCP 6/7 108
Figure 4 – Exemple de fonction de sécurité 114
Figure 5 – Décomposition de la fonction de sécurité en blocs de fonctions 115
Figure 6 – Présentation des résultats du processus de décomposition 117
Figure 7 – Flux de signal entre les blocs de fonctions 118
Figure 8 – Interfaces entre les dispositifs de sécurité au sein du système de communication de sécurité 120
Figure 9 – Flux de signal et états de sécurité 122
Figure 10 – Mise en correspondance du bloc de fonctions Transmission sécurisée 125
Figure 11 – Relation entre la SCL et les autres couches du Type 8 de la CEI 61158 126
Figure 12 – Utilisation du service AR-US pour le démarrage et le paramétrage 127
Figure 13 – Utilisation du service AR-US pour la transmission des données de sécurité 127
Figure 14 – Utilisation du service AR-US pour l'abandon 128
Figure 15 – Utilisation du service AR-US pour l'abandon 128
Figure 16 – Structure du PDU de sécurité 137
Figure 17 – Intégration des données de sécurité et des mesures correctives déterministes dans le cadre de sommation 138
Figure 18 – Message Write_Parameter_Byte_Req 139
Figure 19 – Message Read_Parameter_Byte_Req 139
Figure 20 – Message Parameter_Byte_Con 139
Figure 21 – Message Set_Safety_Connection_ID_Req 142
Figure 22 – Message Set_Safety_Connection_ID_Con des esclaves de sécurité 142
Figure 23 – Parameter_Idle_Req 143
Figure 24 – Parameter_Idle_Con 143
Figure 25 – Parameter_Check_Con 143
Figure 26 – Parameter_Loc_ID_Changed_Con 143
Figure 27 – Message de transmission des données de sécurité 144
Figure 28 – Message Sync_a du SCLM 145
Figure 29 – Message Req_b du SCLM 145
Figure 30 – Message Req_c du SCLM 145
Figure 31 – Message Req_d du SCLM 146

Figure 32 – Message Abort_Connection 146
Figure 33 – Message Safety-Slave_Error 146
Figure 34 – Diagramme d'états du SCLM 147
Figure 35 – Diagramme d'états du SCLS 148
Figure 36 – Séquence de lancement 149
Figure 37 – Séquence d'envoi du paramètre d'application 152
Figure 38 – Séquence d'envoi de l'ID du paramètre d'application 154
Figure 39 – Séquence de paramétrage du dispositif 156
Figure 40 – Transmission simultanée des données de sécurité aux esclaves de sécurité 157
Figure 41 – Utilisation du numéro de séquence dans le SCLM et le SCLS 158
Figure 42 – Démarrage et fonctionnement exempt d'erreurs 159
Figure 43 – Resynchronisation pendant le fonctionnement 160
Figure 44 – Somme de contrôle CRC 24 non valide détectée par le SCLS 161
Figure 45 – Mode de données de processus avec transmission de données de diagnostic 162
Figure 46 – Mode de données de processus avec transmission de données d'acquittement 163
Figure 47 – Erreur lors de l'établissement d'une connexion 164
Figure 48 – Erreur au niveau d'un SCLS lors de l'abandon de toutes les connexions 165
Figure 49 – Abandon de toutes les connexions en cas d'erreur détectée par le SCLM 167
Figure 50 – Présentation de l'arrêt de sécurité 171

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

RÉSEAUX DE COMMUNICATION INDUSTRIELS – PROFILS –

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

AVANT-PROPOS

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

La Norme internationale CEI 61784-3-6 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.

Cette seconde édition annule et remplace la première édition publiée en 2007. Cette édition constitue une révision technique. Les principales modifications par rapport à l'édition précédente sont énumérées ci-dessous:

— mises à jour par rapport aux changements apportés à la CEI 61784-3.

La présente version bilingue, 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*, peut être consultée 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 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.

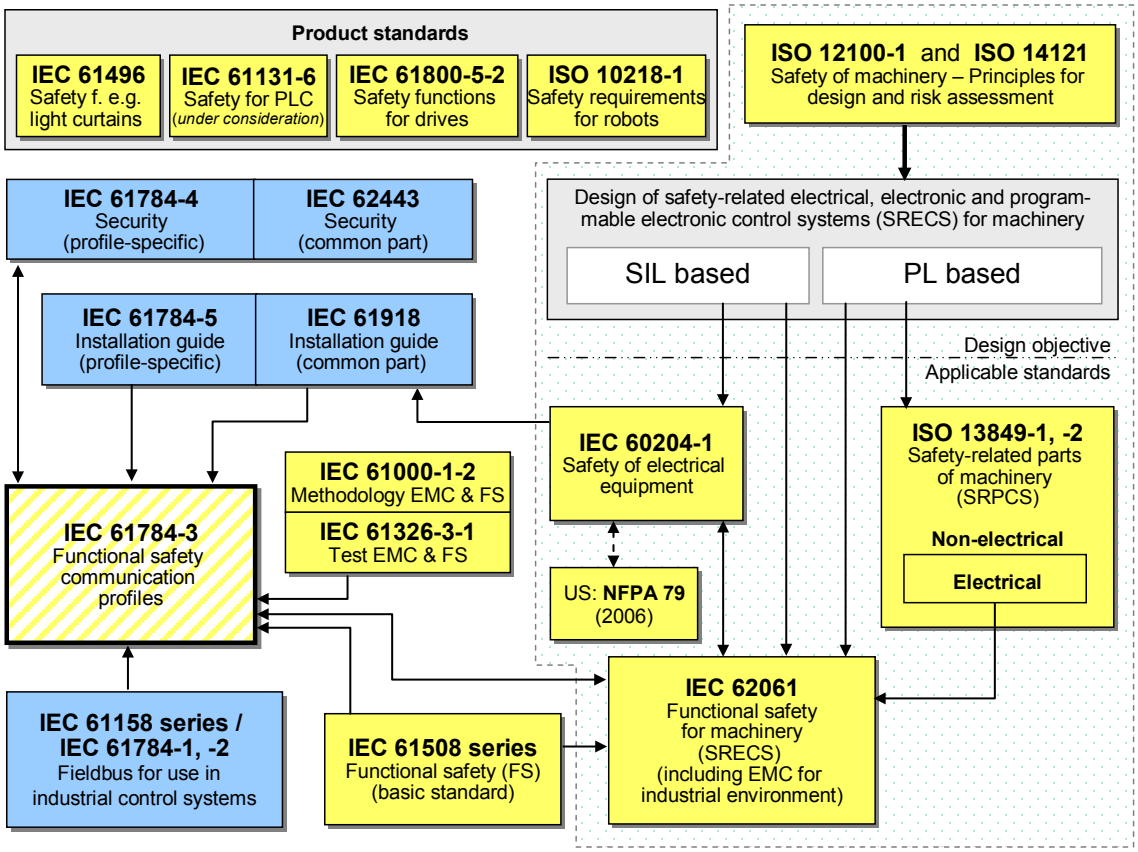
0 Introduction

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 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

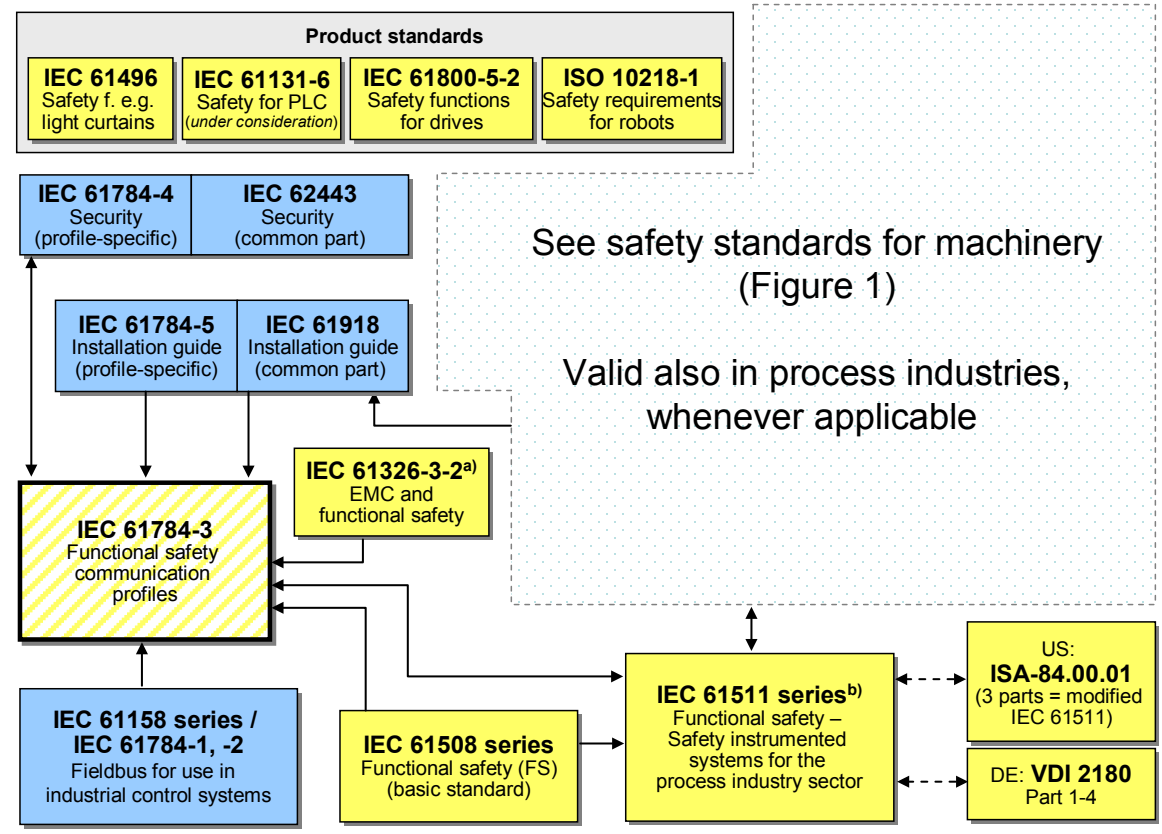
Anglais	Français
Product standards	Normes de produits
Safety function, e.g. light curtains	Fonction de sécurité, par exemple barrières photo électriques
Safety for PLC (under consideration)	Sécurité relative aux automates programmables (à l'étude)
Safety functions for drives	Fonctions de sécurité applicables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

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

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



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 series[b)] Functional safety–safety instrumented systems for the process industry sector	Série CEI 61511[b)] 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 - Relations entre la CEI 61784–3 et d'autres normes (transformation)

Les couches de communication de sécurité mises en œuvre dans la trame de systèmes relatifs à la sécurité conformément à la série CEI 61508, assurent la confiance nécessaire à accorder à la transmission de messages (information) entre deux participants ou plus sur un bus de terrain dans un système relatif à la sécurité, ou une fiabilité suffisante dans le comportement de sécurité en cas d'erreurs ou de défaillances du bus de terrain.

Les couches de communication de sécurité spécifiées dans la présente norme permettent de garantir cette assurance en utilisant un bus de terrain dans des applications nécessitant une sécurité fonctionnelle jusqu'au niveau d'intégrité de sécurité (SIL) spécifié par son profil de communication de sécurité fonctionnelle correspondant.

La revendication du SIL qui en résulte pour un système dépend de la mise en œuvre du profil de communication de sécurité fonctionnelle retenu au sein du système – la mise en œuvre du profil de communication de sécurité fonctionnelle dans un 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 6, où la notation [xx] désigne le détenteur des droits de propriété.

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

La CEI ne prend pas position 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:

[PxC] Phoenix Contact GmbH & Co. KG
Intellectual Property Licenses & Standards
Flachsmarktstr. 8
D-32825 Blomberg,
ALLEMAGNE

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

RÉSEAUX DE COMMUNICATION INDUSTRIELS – PROFILS –

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

1 Domaine d'application

La présente partie de la série CEI 61784-3 spécifie une couche de communication relative à la sécurité (services et protocole) fondée sur la CPF 6 de la CEI 61784-1, de la CEI 61784-2 et le Type 8 de la CEI 61158. Elle identifie les principes applicables aux communications de sécurité fonctionnelle définies dans la CEI 61784-3, et appropriés à cette couche de communication de sécurité.

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

La présente 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).

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

IEC 61131-3, *Programmable controllers – Part 3: Programming languages* (disponible en anglais uniquement)

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

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

---

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".

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

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

IEC 61158-5–8 :2007, *Industrial communication networks – Fieldbus specifications – Part 5-8: Application layer service definition – Type 8 elements* (disponible uniquement en anglais)

IEC 61158-6–8, *Industrial communication networks – Fieldbus specifications – Part 6-8: Application layer protocol specification – Type 8 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*

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

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

CEI 61784-3:2010[3], *Réseaux de communication industriels – Profils – Partie 3 : Bus de terrain de sécurité fonctionnelle – Règles générales et définitions de profil*

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

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

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

ISO 12100-1, *Sécurité des machines – Notions fondamentales, principes généraux de conception – Partie 1: Terminologie de base, méthodologie*

ISO 13849-1, *Sécurité des machines – Parties des systèmes de commande relatives à la sécurité – Partie 1 : Principes généraux de conception*

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 En cours d'élaboration.