IEC 61784-3-1

Edition 2.0 2010-06

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

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

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

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

ICS 25.040.40; 35.100.05

ISBN 978-2-8322-9727-8

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

® 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 14
3.1.2 CPF 1: Additional terms and definitions 18
3.2 Symbols and abbreviated terms 19
3.2.1 Common symbols and abbreviated terms 19
3.2.2 CPF 1: Additional symbols and abbreviated terms 20
3.3 Conventions 20
3.3.1 State diagrams 20
3.3.2 Use of colors in figures 21
4 Overview of FSCP 1/1 (FOUNDATION Fieldbus™ SIS) 22
4.1 General 22
4.2 Key concepts of FSCP 1/1 23
4.2.1 Black channel 23
4.2.2 Connection key 23
4.2.3 Cross-check 23
4.2.4 FSCP 1/1 23
4.2.5 Programmable electronic system 23
4.2.6 Queuing delays 23
4.2.7 Redundancy 24
4.2.8 SIL environment 24
4.3 Key components of FSCP 1/1 24
4.3.1 Overview 24
4.3.2 Black channel 24
4.4 Relationship to the ISO OSI basic reference model 25
5 General 25
5.1 External documents providing specifications for the profile 25
5.2 Safety functional requirements 25
5.2.1 Requirements for functional safety 25
5.2.2 Functional constraints 26
5.2.3 Device manufacturer requirements 26
5.3 Safety measures 26
5.3.1 Sequence number 26
5.3.2 Time stamp 27
5.3.3 Time expectation 27
5.3.4 Connection authentication 27
5.3.5 Data integrity assurance 27
5.3.6 Redundancy with cross checking 27
5.3.7 Different data integrity assurance systems 27
5.3.8 Relationships between errors and safety measures 27

5.4 Safety communication layer structure 28
5.4.1 Network topology and device connectivity 28
5.4.2 Device architecture 28
5.5 Relationships with FAL (and DLL, PhL) 29
5.5.1 General 29
5.5.2 Data types 30
6 Safety communication layer services 30
6.1 Application Process (AP) 30
6.1.1 Overview 30
6.1.2 Network visible objects 31
6.1.3 Application layer interface 31
6.1.4 Object dictionary 31
6.1.5 Application program directory 31
6.2 Function block application processes 31
6.2.1 General 31
6.2.2 Function block model 31
6.2.3 Application process 34
6.3 Device to device communications 36
6.3.1 General 36
6.3.2 Client/server 36
6.3.3 Publisher/subscriber 37
6.3.4 Report distribution 37
6.3.5 FBAP operation in a linking device 37
6.3.6 System management kernel protocol (SMKP) communications 37
6.4 Profiles 37
6.4.1 General 37
6.4.2 FSCP 1/1 profile 37
6.5 Device descriptions 38
6.6 Common file formats 39
6.7 Configuration information 39
6.7.1 Overview 39
6.7.2 Level 1 configuration: manufacturer device definition 39
6.7.3 Level 2 configuration: network definition 39
6.7.4 Level 3 configuration: distributed application definition 39
6.7.5 Level 4 configuration: device configuration 39
7 Safety communication layer protocol 39
7.1 Safety PDU format 39
7.1.1 General 39
7.1.2 Safety communication layer CRC 40
7.1.3 Black channel time synchronization monitoring 40
7.1.4 Sequence number 40
7.1.5 Virtual header 41
7.1.6 Connection key 41
7.1.7 Redundancy and cross-check 42
7.2 Protocol extensions for use in safety-related systems 42
7.2.1 Overview 42
7.2.2 Publisher-subscriber interactions 42
7.2.3 Client-server interactions 48
7.2.4 Time synchronization 53

7.2.5 Device start-up 54
7.3 Communications entity 55
7.3.1 General 55
7.3.2 Network management 55
7.3.3 FMS 55
7.3.4 H1 stack 55
8 Safety communication layer management 55
8.1 Overview 55
8.2 SMK communications 55
8.3 FMS services 55
8.4 SMK services 55
8.4.1 General 55
8.4.2 Address assignment 56
8.4.3 Time synchronization 56
8.5 Safety communication layer configuration and start-up 56
8.5.1 H1 configuration and start-up 56
8.5.2 FSCP 1/1 FBAP 56
8.5.3 Testing 56
9 System requirements 56
9.1 Indicators and switches 56
9.2 Installation guidelines 56
9.3 Safety function response time 56
9.3.1 Overview 56
9.3.2 Safety Sensor 57
9.3.3 Input Function Block 57
9.3.4 Safe Transmission 57
9.3.5 Logic Solver 57
9.3.6 Discrete Output Function Block 57
9.3.7 Safety Actuator 57
9.4 Duration of demands 57
9.5 Constraints for calculation of system characteristics 57
9.5.1 System characteristics 57
9.5.2 Message rate 58
9.5.3 SIL level 58
9.5.4 Mixing FSCP 1/1 devices and CP 1/1 devices 58
9.5.5 Devices on a segment 58
9.5.6 Residual error rate calculations 58
9.6 Maintenance 59
9.7 Safety manual 59
10 Assessment 59
Annex A (informative) Additional information for functional safety communication profiles of CPF 1 60
A.1 Hash function calculation 60
A.2 Fault conditions arising from locations beyond the output function block 62
Annex B (informative) Information for assessment of the functional safety communication profiles of CPF 1 64
Bibliography 65

Table 1 – Example state transition table 21
Table 2 – Safety measures and possible communication errors 28
Table 3 – Data types used within FSCP 1/1 30
Table 4 – Fault state behaviour 33
Table 5 – Publisher states 44
Table 6 – Publisher state table - Received transitions 44
Table 7 – Publisher state table - Internal transitions 45
Table 8 – Subscriber states 46
Table 9 – Subscriber state table - Received transitions 47
Table 10 – Subscriber state table - Internal transitions 47
Table 11 – Server states during read operations 49
Table 12 – Received transitions for a FSCP 1/1 Server during read operations 49
Table 13 – States of a FSCP 1/1 server during write operations 51
Table 14 – Received transitions for a FSCP 1/1 Server during write operations 52
Table 15 – Values used for calculation of residual error rate 58
Table 16 – Values of R_{SL} (Pe) for different values of n 59
Table A.1 – Fault conditions arising from locations beyond the output function block 63

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 – Example state diagram 21
Figure 4 – Use of colors in figures 21
Figure 5 – Scope of FSCP 1/1 22
Figure 6 – FSCP 1/1 architecture (H1) 24
Figure 7 – Black channel 25
Figure 8 – FSCP 1/1 in system architecture 28
Figure 9 – FSCP 1/1 H1 device 29
Figure 10 – FSCP 1/1 protocol layers 29
Figure 11 – Relationship between FSCP 1/1 and the other layers of IEC 61158 Type 1 30
Figure 12 – Key write-lock 32
Figure 13 – Password write-lock 32
Figure 14 – Example of FSCP 1/1 communication 36
Figure 15 – Example of device description 38
Figure 16 – Safety PDU showing virtual content 43
Figure 17 – Safety PDU showing duplication of data and addition of CRC 43
Figure 18 – State transition diagram for a FSCP 1/1 Publisher 44
Figure 19 – Safety PDU showing duplication of data and addition of CRC 45
Figure 20 – Safety PDU showing virtual content 45
Figure 21 – State transition diagram for a FSCP 1/1 subscriber 46
Figure 22 – Safety PDU showing virtual content 48
Figure 23 – Safety PDU showing virtual content with sub index 48
Figure 24 – Safety PDU showing duplication of data, addition of sequence number and CRC 48

Figure 25 – State transition diagram for a FSCP 1/1 Server during read operations 49
Figure 26 – Safety PDU showing duplication of data and addition of sequence number and CRC 50
Figure 27 – Example of FSCP 1/1 write 51
Figure 28 – Example of FSCP 1/1 write with sub index 51
Figure 29 – State transition diagram for a FSCP 1/1 Server during write operations 51
Figure 30 – Safety PDU showing duplication of data and CRC 53
Figure 31 – Example of safety function response time components 57
Figure 32 – Example FSCP 1/1 network topology 58

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES –

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

FOREWORD

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

— adjustment of Figure 5;

— change of sequence number from two octets to four octets in 7.2.2 to match the final protocol from the consortium.

— addition of details for time synchronization in 7.2.4;

— addition of information for safety response time in 9.3;

— addition of information in constraints for calculation of system characteristics in 9.5.

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.

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.

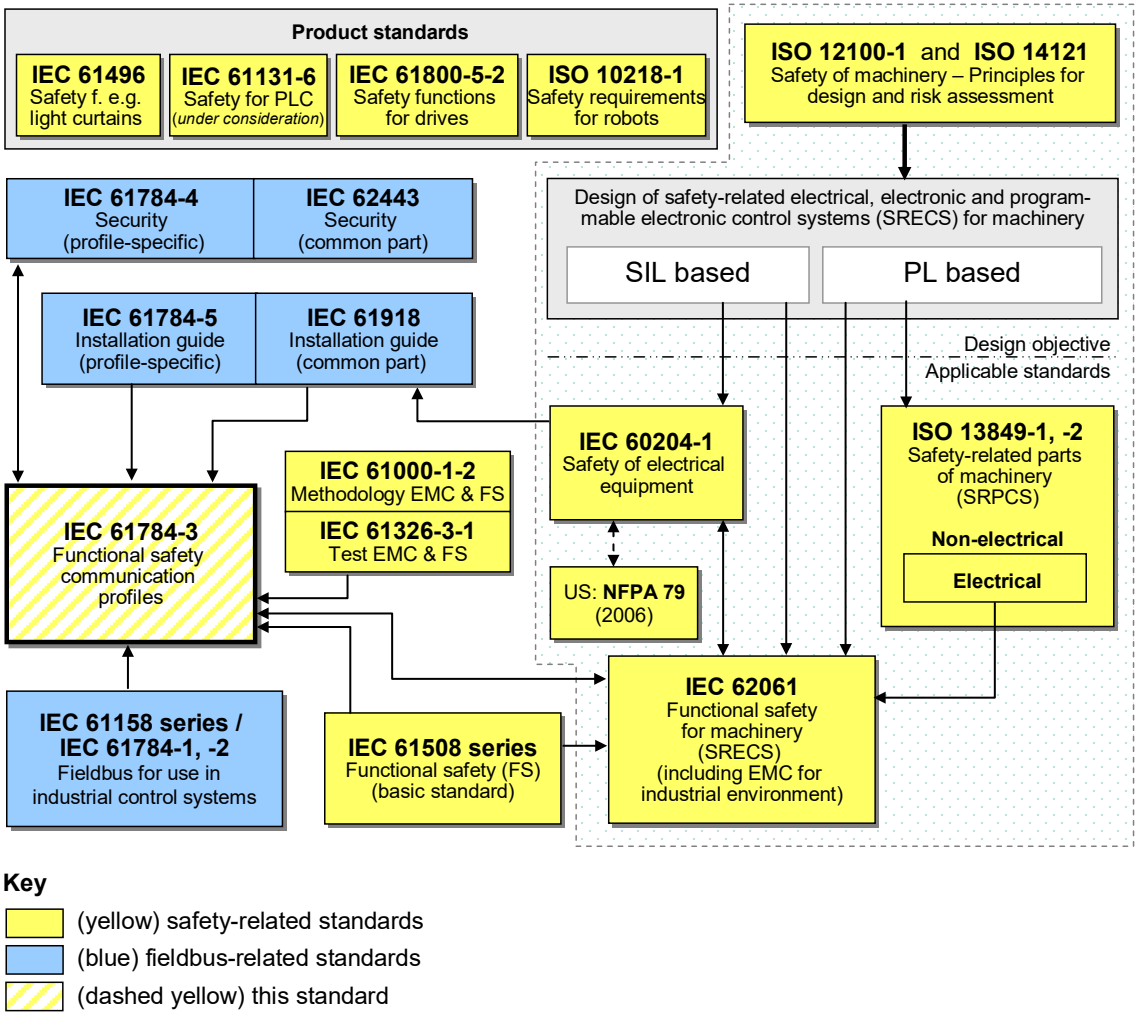
0 Introduction

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.

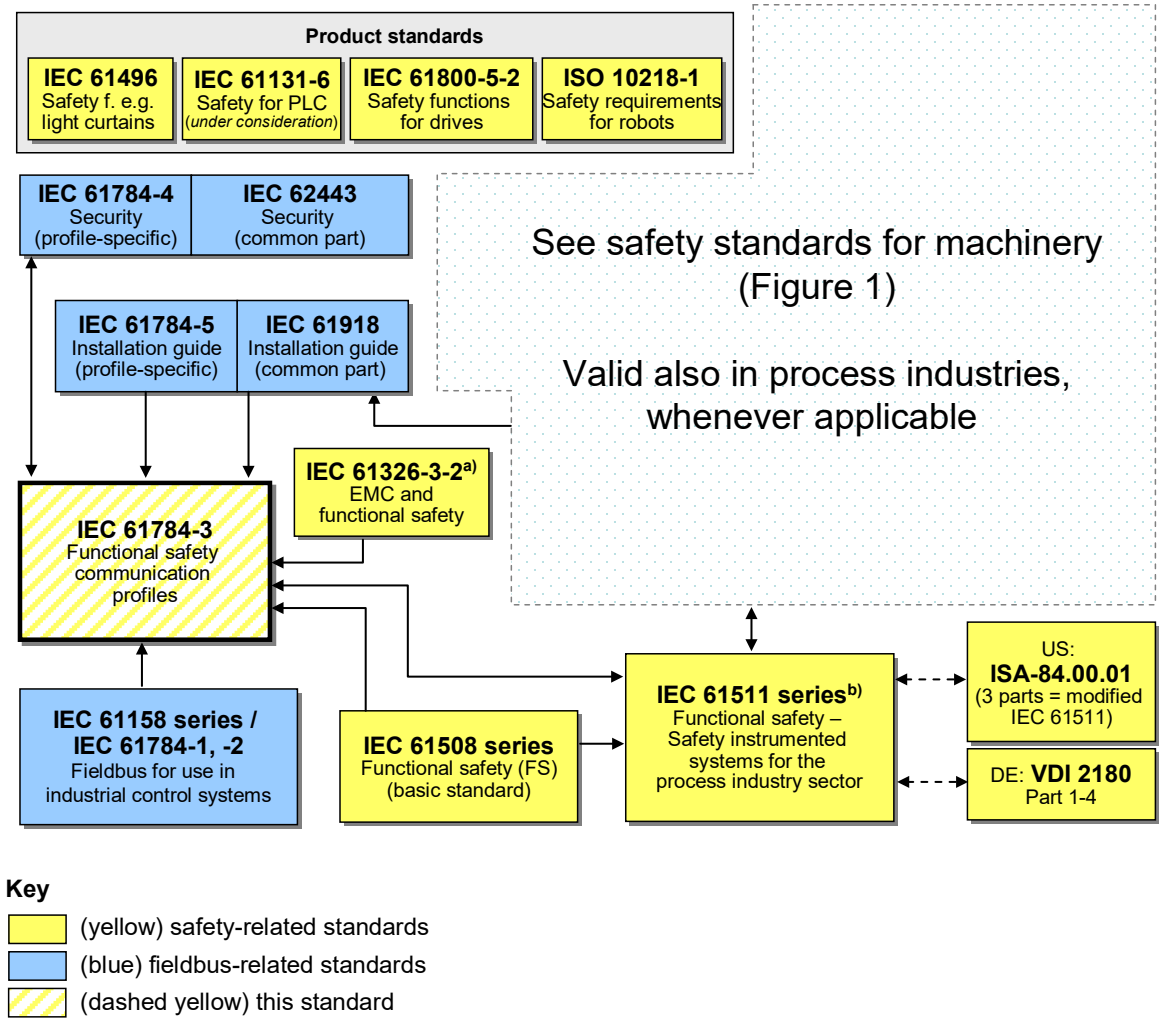
Figure 1 shows the relationships between this standard and relevant safety and fieldbus standards in a machinery environment.



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

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

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

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

Information may be obtained from:

[FF] Fieldbus Foundation

9005 Mountain Ridge Drive
Bowie Bldg. - Suite 190
Austin, TX 78759-5316
USA
Tel: +1 512 794 8890

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

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES –

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

1 Scope

This part of the IEC 61784-3 series specifies a safety communication layer (services and protocol) based on CPF 1 of IEC 61784-1 and IEC 61158 Types 1 and 9. It identifies the principles for functional safety communications defined in IEC 61784-3 that are relevant for this safety communication layer.

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

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

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

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

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

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

---

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

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

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

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

IEC 61508-1:2010[3], *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements*

IEC 61508-2:2010[3], *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*

IEC 61508-3:2010[3], *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements*

IEC 61508-4:2010[3], *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations*

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

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

IEC 61784-3:2010[4], *Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions*

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

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

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 To be published.

4 To be published.

SOMMAIRE

AVANT-PROPOS 73
0 Introduction 75
0.1 Généralités 75
0.2 Déclaration de brevets 79
1 Domaine d'application 80
2 Références normatives 80
3 Termes, définitions, symboles, abréviations et conventions 82
3.1 Termes et définitions 82
3.1.1 Termes et définitions communs 82
3.1.2 CPF 1: Termes et définitions supplémentaires 86
3.2 Symboles et abréviations 87
3.2.1 Symboles et abréviations communs 87
3.2.2 CPF 1: Symboles et abréviations supplémentaires 88
3.3 Conventions 89
3.3.1 Diagrammes d'états 89
3.3.2 Utilisation de couleurs dans les figures 90
4 Présentation générale de FSCP 1/1 (FOUNDATION Fieldbus™ SIS) 91
4.1 Généralités 91
4.2 Concepts clés du FSCP 1/1 92
4.2.1 Canal noir 92
4.2.2 Clé de connexion 92
4.2.3 Contre-vérification 92
4.2.4 FSCP 1/1 92
4.2.5 Système électronique programmable 92
4.2.6 Retards de mise en file d'attente 93
4.2.7 Redondance 93
4.2.8 environnement SIL 93
4.3 Composantes clés du FSCP 1/1 93
4.3.1 Présentation générale 93
4.3.2 Canal noir 95
4.4 Relation avec le modèle de référence de base OSI de l'ISO 95
5 Généralités 96
5.1 Documents externes de spécifications applicables au profil 96
5.2 Exigences de sécurité fonctionnelle 96
5.2.1 Exigences relatives à la sécurité fonctionnelle 96
5.2.2 Contraintes de fonctionnement 97
5.2.3 Exigences du fabricant d'appareils 97
5.3 Mesures de sécurité 97
5.3.1 Numéro de séquence 97
5.3.2 Horodatage 97
5.3.3 Délai 97
5.3.4 Authentification de connexion 97
5.3.5 Assurance d'intégrité des données 97
5.3.6 Redondance avec contre-vérification 97
5.3.7 Différents systèmes d'assurance d'intégrité des données 98
5.3.8 Relations entre les erreurs et les mesures de sécurité 98

5.4 Structure de la couche de communication de sécurité 98
5.4.1 Topologie de réseau et connectivité des appareils 98
5.4.2 Architecture des appareils 99
5.5 Relations avec la FAL (et DLL, PhL) 100
5.5.1 Généralités 100
5.5.2 Types de données 100
6 Services de la couche de communication de sécurité 101
6.1 Processus d'Application (AP) 101
6.1.1 Présentation générale 101
6.1.2 Objets visibles de réseau 101
6.1.3 Interface de couche application 101
6.1.4 Dictionnaire d'objets 101
6.1.5 Répertoire de programmes d'application 102
6.2 Processus d'application de blocs de fonctions 102
6.2.1 Généralités 102
6.2.2 Modèle de blocs de fonctions 102
6.2.3 Processus d'application 105
6.3 Communications entre appareils 108
6.3.1 Généralités 108
6.3.2 Client/serveur 109
6.3.3 Editeur/abonné 109
6.3.4 Diffusion de rapports 109
6.3.5 Opération FBAP dans un appareil de liaison 109
6.3.6 Communications de protocole de noyau de gestion de système (SMKP) .. 109
6.4 Profils 110
6.4.1 Généralités 110
6.4.2 Profil FSCP 1/1 110
6.5 Descriptions d'appareils 111
6.6 Formats de fichiers communs 111
6.7 Informations de configuration 112
6.7.1 Présentation générale 112
6.7.2 Configuration de niveau 1: définition d'appareil du fabricant 112
6.7.3 Configuration de niveau 2: définition du réseau 112
6.7.4 Configuration de niveau 3: définition d'application distribuée 112
6.7.5 Configuration de niveau 4: configuration d'appareil 112
7 Protocole de couche de communication de sécurité 112
7.1 Format PDU de sécurité 112
7.1.1 Généralités 112
7.1.2 CRC de couche de communication de sécurité 112
7.1.3 Contrôle de la synchronisation temporelle par le canal noir 113
7.1.4 Numéro de séquence 113
7.1.5 En-tête virtuel 114
7.1.6 Clé de connexion 115
7.1.7 Redondance et contre-vérification 115
7.2 Extensions de protocole pour utilisation dans des systèmes relatifs à la sécurité 115
7.2.1 Présentation générale 115
7.2.2 Interactions éditeur-abonné 115
7.2.3 Interactions client-serveur 121
7.2.4 Synchronisation temporelle 128

7.2.5 Démarrage de l'appareil 129
7.3 Entité de communications 129
7.3.1 Généralités 129
7.3.2 Gestion de réseau 129
7.3.3 FMS 130
7.3.4 Pile H1 130
8 Gestion de la couche de communication de sécurité 130
8.1 Présentation générale 130
8.2 Communications SMK 130
8.3 Services FMS 130
8.4 Services SMK 130
8.4.1 Généralités 130
8.4.2 Attribution d'adresse 130
8.4.3 Synchronisation temporelle 131
8.5 Configuration de la couche de communication de sécurité et démarrage 131
8.5.1 Configuration H1 et démarrage 131
8.5.2 FBAP FSCP 1/1 131
8.5.3 Essais 131
9 Exigences système 131
9.1 Voyants et commutateurs 131
9.2 Lignes directrices d'installation 131
9.3 Temps de réponse de la fonction de sécurité 131
9.3.1 Présentation générale 131
9.3.2 Capteur de sécurité 132
9.3.3 Bloc de fonctions d'entrée 132
9.3.4 Transmission de sécurité 132
9.3.5 Résolveur logique 132
9.3.6 Blocs de fonctions de sortie discrète 132
9.3.7 Actionneur de sécurité 132
9.4 Durée des demandes 133
9.5 Contraintes liées au calcul des caractéristiques des systèmes 133
9.5.1 Caractéristiques du système 133
9.5.2 Taux de messages 133
9.5.3 Niveau SIL 133
9.5.4 Mélange d'appareils FSCP 1/1 et d'appareils CP 1/1 134
9.5.5 Appareils sur un segment 134
9.5.6 Calcul du taux d'erreur différentiel résiduel 134
9.6 Maintenance 135
9.7 Manuel de sécurité 135
10 Evaluation 135
Annexe A (informative) Informations supplémentaires pour les profils de communication de sécurité fonctionnelle de CPF 1 136
A.1 Calcul de la fonction de hachage 136
A.2 Conditions de panne issues d'emplacements situés au-delà du bloc de fonctions de sortie 139
Annexe B (informative) Informations pour l'évaluation des profils de communication de sécurité fonctionnelle de le CPF 1 140
Bibliographie 141

Tableau 1 – Exemple de tableau de transitions d'état 90
Tableau 2 – Mesures de sécurité et erreurs de communication possibles 98
Tableau 3 – Types de données utilisés dans le protocole FSCP 1/1 101
Tableau 4 – Comportement d'états d'anomalie 104
Tableau 5 – Etats de l'éditeur 117
Tableau 6 – Tableau d'états de l'éditeur – Transitions reçues 117
Tableau 7 – Tableau d'états de l'éditeur – Transitions internes 118
Tableau 8 – Etats de l'abonné 119
Tableau 9 – Tableau d'états de l'abonné – Transitions reçues 120
Tableau 10 – Tableau d'états de l'abonné – Transitions internes 121
Tableau 11 – Etats du serveur pendant les opérations de lecture 123
Tableau 12 – Transitions reçues pour un serveur FSCP 1/1 pendant les opérations de lecture 124
Tableau 13 – Etats d'un serveur FSCP 1/1 au cours des opérations d'écriture 125
Tableau 14 – Transitions reçues pour un serveur FSCP 1/1 pendant les opérations d'écriture 126
Tableau 15 – Valeurs utilisées pour le calcul du taux d'erreurs résiduelles 134
Tableau 16 – Valeurs de R_{SL} (Pe) pour différentes valeurs de n 134
Tableau A.1 – Conditions de panne issues d'emplacements situés au-delà du bloc de fonctions de sortie 139

Figure 1 – Relation entre l'IEC 61784-3 et d'autres normes (machines) 76
Figure 2 – Relations entre l'IEC 61784-3 et d'autres normes (processus) 78
Figure 3 – Exemple de diagramme d'états 89
Figure 4 – Utilisation de couleurs dans les figures 90
Figure 5 – Domaine d'application du FSCP 1/1 91
Figure 6 – Architecture du protocole FSCP 1/1 (H1) 94
Figure 7 – Canal noir 95
Figure 8 – Protocole FSCP 1/1 dans l'architecture de système 98
Figure 9 – Appareil H1 FSCP 1/1 99
Figure 10 – Couches de protocole FSCP 1/1 100
Figure 11 – Relation entre le FSCP 1/1 et les autres couches du type 1 de l'IEC 61158 100
Figure 12 – Système d'interdiction d'écriture à clé 103
Figure 13 – Système d'interdiction d'écriture à mots de passe 103
Figure 14 – Exemple de communication FSCP 1/1 108
Figure 15 – Exemple de description d'appareils 111
Figure 16 – Représentation du contenu virtuel d'un PDU de sécurité 116
Figure 17 – PDU de sécurité représentant la duplication des données et l'ajout du CRC 116
Figure 18 – Diagramme de transition d'états pour un éditeur FSCP 1/1 117
Figure 19 – PDU de sécurité représentant la duplication des données et l'ajout du CRC 118
Figure 20 – Représentation du contenu virtuel d'un PDU de sécurité 118
Figure 21 – Diagramme de transition d'états pour un abonné FSCP 1/1 120
Figure 22 – Représentation du contenu virtuel d'un PDU de sécurité 122

Figure 23 – Représentation du contenu virtuel d'un PDU de sécurité avec sous-index 122
Figure 24 – PDU de sécurité représentant la duplication des données et l'ajout du numéro de séquence et du CRC 122
Figure 25 – Diagramme de transition d'états pour un serveur FSCP 1/1 pendant les opérations de lecture 123
Figure 26 – PDU de sécurité représentant la duplication des données et l'ajout du numéro de séquence et du CRC 124
Figure 27 – Exemple d'écriture FSCP 1/1 125
Figure 28 – Exemple d'écriture FSCP 1/1 avec sous-index 125
Figure 29 – Diagramme de transition d'états pour un serveur FSCP 1/1 pendant les opérations d'écriture 126
Figure 30 – PDU de sécurité représentant la duplication des données et le CRC 127
Figure 31 – Exemple des composantes du temps de réponse de la fonction de sécurité 132
Figure 32 – Exemple de topologie de réseau FSCP 1/1 133

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

RÉSEAUX DE COMMUNICATION INDUSTRIELS – PROFILS –

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

AVANT-PROPOS

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

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

Cette deuxième édition annule et remplace la première édition parue en 2007. Cette édition constitue une révision technique. Cette édition inclut les modifications techniques majeures suivantes par rapport à l'édition précédente:

— mises à jour en relation avec les modifications apportées à l'IEC 61784-3;

— ajustement de la Figure 5;

— changement de numéro de séquence de deux octets à quatre octets en 7.2.2 pour coïncider avec le protocole final du consortium.

— ajout de détails pour la synchronisation temporelle en 7.2.4;

— ajout d'informations relatives au temps de réponse de sécurité en 9.3;

— ajout d'informations sous forme de contraintes pour le calcul des caractéristiques d'un système en 9.5.

La présente version bilingue (2021-04) correspond à la version anglaise monolingue publiée en 2010-06.

La version française de cette norme n'a pas été soumise au vote.

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

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

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous "http://webstore.iec.ch" dans les données relatives à la publication recherchée. 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.

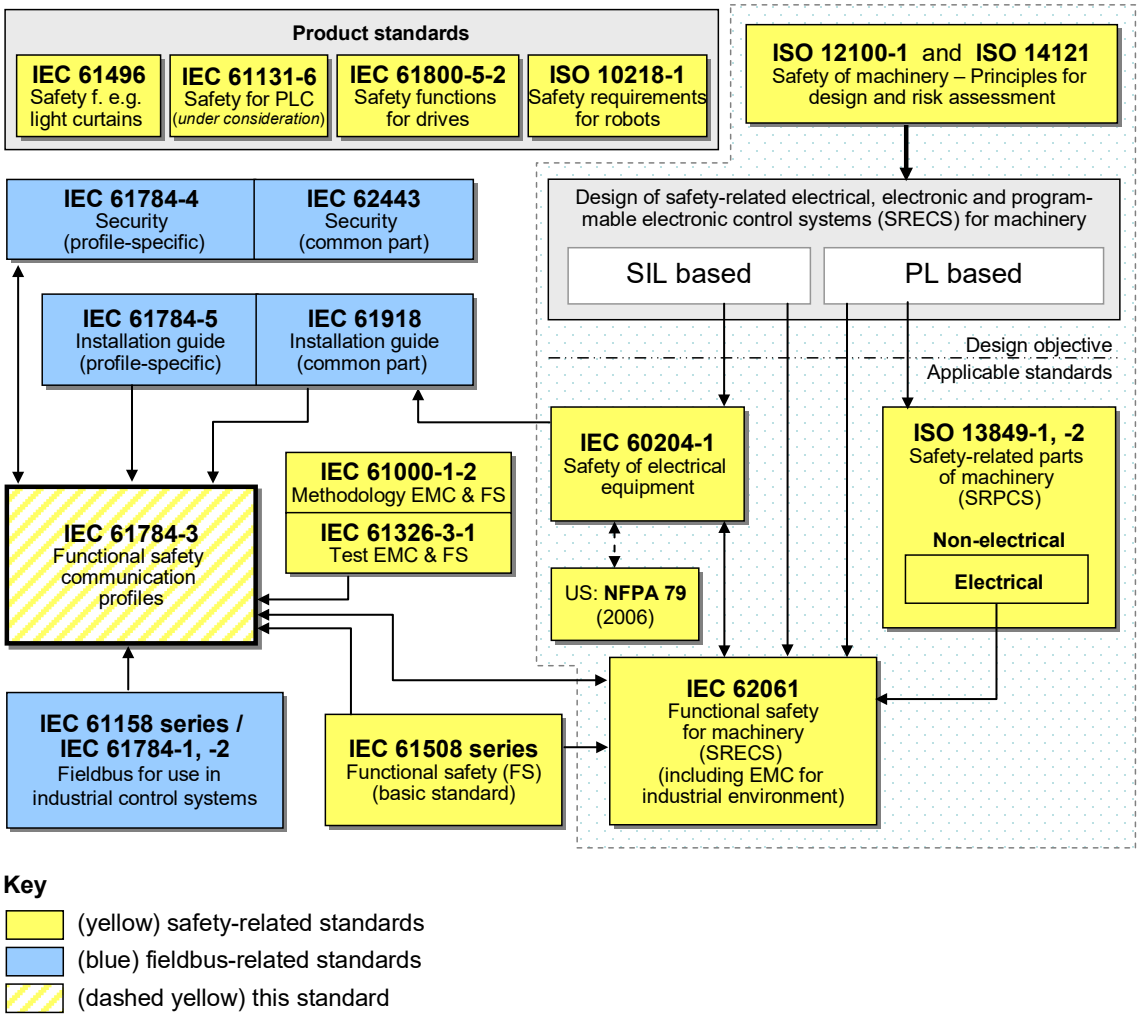
0 Introduction

0.1 Généralités

L'IEC 61158 relative aux bus de terrain, ainsi que ses normes associées IEC 61784-1 et IEC 61784-2, définit un ensemble de protocoles de communication qui assurent la commande répartie d'applications automatisées. La technologie de bus de terrain est désormais reconnue et bien éprouvée. Ainsi 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 de sécurité fonctionnelle en référence à la série IEC 61508, et spécifie plusieurs couches de communication de sécurité (profils et protocoles correspondants) basées sur les profils de communication et les couches de protocole de l'IEC 61784-1, l'IEC 61784-2 et de la série IEC 61158. Elle ne couvre pas les aspects relatifs à la sécurité électrique et à la sécurité intrinsèque.

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

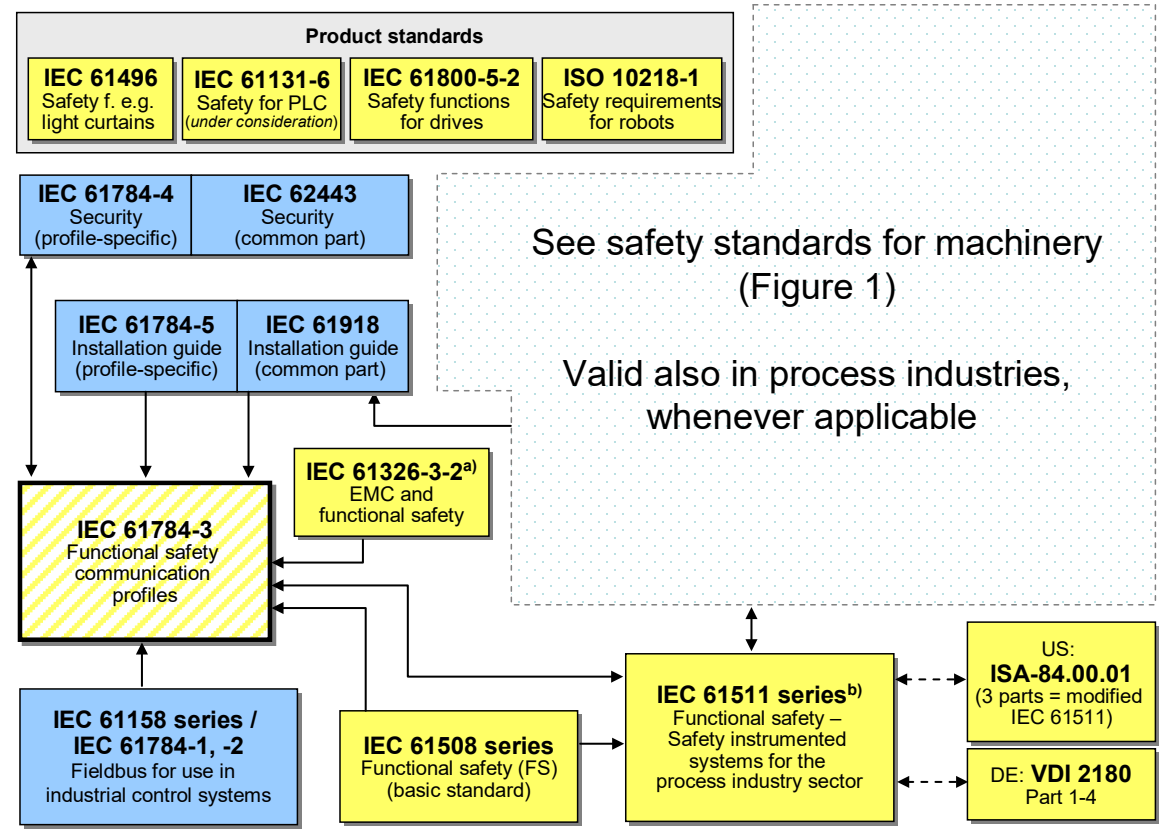


Anglais	Français
Product standards	Normes de produits
Safety function, e.g. light curtains	Fonction de sécurité, par exemple rideaux de lumière
Safety for PLC (under consideration)	Sécurité relative aux automates programmables (à l'étude)
Safety functions for drives	Fonctions de sécurité applicables aux entraînements
Safety of machinery – ... assessment	Sécurité des machines – principes généraux de conception et appréciation du risque
Security (profile-specific)	Sûreté (spécifique au profil)
Security (common part)	Sûreté (partie commune)
Design of safety-related .... for machinery	Conception des systèmes de commande électriques, électroniques et électroniques programmables relatifs à la sécurité pour les machines
SIL based	Basé sur SIL
PL based	Basé sur PL
Installation guide (profile-specific)	Guide d'installation (spécifique au profil)
Installation guide (common part)	Guide d'installation (partie commune)
Design objective	Objectif de conception
Applicable standards	Normes applicables
Safety of electrical equipment	Sécurité des équipements électriques
Safety-related parts of machinery	Parties des systèmes de commande relatives à la sécurité
Non-electrical	Non électrique
Electrical	Electrique
EMC & functional safety	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 aux bus de terrain
(dashed) yellow) this standard	(jaune pointillé) la présente norme
IEC	CEI

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

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

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



[a] Pour des environnements électromagnétiques spécifiés, sinon IEC 61326-3-1.

[b] EN ratifiée.

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

Anglais	Français
EMC and functional safety	CEM & sécurité fonctionnelle
IEC 61158 series Fieldbus for use in industrial control systems	Série CEI 61158 Bus de terrain pour utilisation dans des systèmes de commande industriels
IEC 61508 series, Functional safety (basic standard)	Série CEI 61508 Sécurité fonctionnelle (norme de base)
IEC 61511 series Functional safety … sector	Série CEI 61511 sécurité fonctionnelle – systèmes instrumentés de sécurité pour le secteur des industries de transformation
(3 parts = modified IEC 61511)	(3 parties = CEI 61511 modifiée)
Part 1 –4	Parties 1 à 4
Key	Légende
(yellow) safety-related standards	(jaune) normes relatives à la sécurité
(blue) fieldbus-related standards	(bleu) normes relatives aux bus de terrain
(dashed) yellow) this standard	(jaune pointillé) la présente norme
IEC	CEI

Figure 2 – Relations entre l'IEC 61784-3 et d'autres normes (processus)

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

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

La revendication du SIL qui en résulte pour un système dépend de la mise en œuvre du profil de communication de sécurité fonctionnelle retenu au sein du système – la mise en œuvre du profil de communication de sécurité fonctionnelle dans un appareil normal ne suffit pas à le qualifier d'appareil de sécurité.

La présente norme décrit:

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

— la description individuelle des profils de sécurité fonctionnelle pour plusieurs familles de profils de communication dans l'IEC 61784-1 et l'IEC 61784-2;

— les extensions de la couche de sécurité aux sections relatives au service et aux protocoles de communication de la série IEC 61158.

0.2 Déclaration de brevets

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

US 6,999,824	[FF]	Système et méthode de mise en œuvre des systèmes instrumentés de sécurité dans une architecture de bus de terrain

La IEC 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 l'IEC 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 l'IEC.

Des informations peuvent être obtenues auprès de:

[FF] Fieldbus Foundation

9005 Mountain Ridge Drive
Bowie Bldg. – Suite 190
Austin, TX 78759-5316
USA
Tél: +1 512 794 8890

L'attention est attirée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété autres que ceux mentionnés ci-dessus. La IEC 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 3-1: Bus de terrain à sécurité fonctionnelle – Spécifications complémentaires pour le CPF 1

1 Domaine d'application

La présente partie de la série IEC 61784-3 spécifie une couche de communication de sécurité (services et protocole) basée sur la CPF 1 de l'IEC 61784-1 et l'IEC 61158 Types 1 et 9. Elle identifie les principes de communication de sécurité fonctionnelle définis dans l'IEC 61784-3 qui sont pertinents pour 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 IEC 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 d'appareils et systèmes conformes.

NOTE 2 La revendication du SIL qui en résulte pour un système dépend de la mise en œuvre du profil de communication de sécurité fonctionnelle retenu au sein du système – la mise en œuvre du profil de communication de sécurité fonctionnelle, conforme à la présente partie, dans un appareil normal ne suffit pas à le qualifier d'appareil de sécurité.

2 Références normatives

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

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

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

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

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

---

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

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

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

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

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

IEC 61158-6-9, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 6-9: Spécification du protocole de la couche application – Eléments de type 9*

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

IEC 61508-1:2010[3], *Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité – Partie 1: Règles générales*

IEC 61508-2:2010[3], *Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité – Partie 2: Exigences pour les systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité*

IEC 61508-3:2010[3], *Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité – Partie 3: Exigences relatives au logiciel*

IEC 61508-4:2010[3], *Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité – Partie 4: Définitions et abréviations*

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

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

IEC 61784-3:2010[4], *Réseaux de communication industriels – Profils – Partie 3: Bus de terrain de sécurité fonctionnelle – Règles générales et définitions de profil*

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

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

ISO/IEC 8802-3, *Technologies de l'information – Télécommunications et échange d'information entre systèmes – Réseaux locaux et métropolitains – Prescriptions spécifiques – Partie 3: Accès multiple par surveillance du signal et détection de collision (CSMA/CD) et spécifications pour la couche physique*

---

[3] A publier.

[4] A publier.