IEC 61784-3-8

Edition 3.0 2021-05

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Industrial communication networks – Profiles – Part 3-8: Functional safety fieldbuses – Additional specifications for CPF 8

Réseaux de communication industriels – Profils – Partie 3-8: Bus de terrain de sécurité fonctionnelle – Spécifications supplémentaires pour CPF 8

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

ICS 25.040.40; 35.100.05

ISBN 978-2-8322-9751-3

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 8: Additional terms and definitions 20
3.2 Symbols and abbreviated terms 21
3.2.1 Common symbols and abbreviated terms 21
3.2.2 CPF 8: Additional symbols and abbreviated terms 22
3.3 Conventions 22
4 Overview 22
5 General 22
6 Safety communication layer services 22
7 Safety communication layer protocol 23
8 Safety communication layer management 23
9 System requirements 23
10 Assessment 23
11 FSCP 8/1 23
11.1 Scope – FSCP 8/1 23
11.2 Normative references – FSCP 8/1 23
11.3 Terms, definitions, symbols, abbreviated terms and conventions – FSCP 8/1 23
11.4 Overview of FSCP 8/1 (CC-Link Safety™) 23
11.5 General – FSCP 8/1 24
11.5.1 External documents providing specifications for the profile 24
11.5.2 Safety functional requirements 24
11.5.3 Safety measures 24
11.5.4 Safety communication layer structure 26
11.5.5 Relationships with FAL (and DLL, PhL) 27
11.6 Safety communication layer services for FSCP 8/1 27
11.6.1 General 27
11.6.2 SASEs 27
11.6.3 SARs 28
11.6.4 Process data SAR ASEs 29
11.7 Safety communication layer protocol for FSCP 8/1 30
11.7.1 Safety PDU format 30
11.7.2 State description 38
11.8 Safety communication layer management for FSCP 8/1 43
11.8.1 General 43
11.8.2 Connection establishment and confirmation processing 43
11.8.3 Safety slave verification 43
11.9 System requirements for FSCP 8/1 44

11.9.1 Indicators and switches 44
11.9.2 Installation guidelines 45
11.9.3 Safety function response time 45
11.9.4 Duration of demands 47
11.9.5 Constraints for calculation of system characteristics 47
11.9.6 Maintenance 47
11.9.7 Safety manual 47
11.10 Assessment for FSCP 8/1 47
12 FSCP 8/2 48
12.1 Scope – FSCP 8/2 48
12.2 Normative references – FSCP 8/2 48
12.3 Terms, definitions, symbols, abbreviated terms and conventions – FSCP 8/2 48
12.4 Overview of FSCP 8/2 (CC-Link IE™ Safety communication function) 48
12.5 General – FSCP 8/2 48
12.5.1 External documents providing specifications for the profile 48
12.5.2 Safety functional requirements 49
12.5.3 Safety measures 49
12.5.4 Safety communication layer structure 54
12.5.5 Relationships with FAL (and DLL, PhL) 55
12.6 Safety communication layer services for FSCP 8/2 55
12.6.1 General 55
12.6.2 Connection reestablishment services 55
12.6.3 Data transmission services 56
12.6.4 Connection termination notification services 57
12.7 Safety communication layer protocol for FSCP 8/2 57
12.7.1 Safety PDU format 57
12.7.2 Safety FAL service protocol machine (SFSPM) 64
12.8 Safety communication layer management for FSCP 8/2 90
12.8.1 Parameter Definitions 90
12.8.2 Parameter Setup 94
12.8.3 Management Services 95
12.9 System requirements for FSCP 8/2 98
12.9.1 Indicators and switches 98
12.9.2 Installation guidelines 100
12.9.3 Safety function response time 100
12.9.4 Duration of demands 101
12.9.5 Constraints for calculation of system characteristics 101
12.9.6 Maintenance 102
12.9.7 Safety manual 102
12.10 Assessment for FSCP 8/2 103
Annex A (informative) Additional information for functional safety communication profiles of CPF 8 104
A.1 Hash function calculation for FSCP 8/1 104
A.2 Hash function calculation for FSCP 8/2 104
A.3 Meaning of response time calculation formula for FSCP 8/2 105
Annex B (informative) Information for assessment of the functional safety communication profiles of CPF 8 107
Bibliography 108

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 – Relationship between SCL and the other layers of IEC 61158 Type 18 27
Figure 4 – State diagram 39
Figure 5 – Detection of unintended repetition 51
Figure 6 – Detection of incorrect sequence 51
Figure 7 – Detection of loss 52
Figure 8 – Detection of unacceptable delay by time stamps 53
Figure 9 – Detection of unacceptable delay by timer 53
Figure 10 – Protocol Hierarchy 54
Figure 11 – Safety PDU Structure 58
Figure 12 – CTRL Configuration 59
Figure 13 – SASE-M and SASE-S TS 62
Figure 14 – S-Data during safety refresh 62
Figure 15 – S-Data not during safety refresh 63
Figure 16 – S-Data header configuration 63
Figure 17 – CRC calculation 64
Figure 18 – Communication models 64
Figure 19 – SFSPM state transition diagram 65
Figure 20 – Connection establishment sequence 67
Figure 21 – Optional sequence during connection establishment sequence 68
Figure 22 – Communication sequence during safety refresh communication 68
Figure 23 – Offset measurement and generation sequence during safety refresh communication 69
Figure 24 – SFSPM-M state transition diagram 70
Figure 25 – Sequence other than during safety refresh 74
Figure 26 – S-Connect-req 74
Figure 27 – S-InitConfirmNetPrm-req 75
Figure 28 – net_prm_list 75
Figure 29 – S-InitVerifyStnPrm-req 75
Figure 30 – stn_prm_list 76
Figure 31 – S-InvokeFunc-req 76
Figure 32 – S-WriteErrorInfo-req 77
Figure 33 – date_and_time_of_occurence 78
Figure 34 – SFSPM-S state transition diagram 79
Figure 35 – Sequence other than during safety refresh 84
Figure 36 – S-Connect-rsp 84
Figure 37 – S-InitConfirmNetPrm-rsp 85
Figure 38 – S-InitVerifyStnPrm-rsp 85
Figure 39 – S-InvokeFunc-rsp 86
Figure 40 – Offset calculation procedure of safety clock 87
Figure 41 – Relationship between transmission interval fluctuation and transmission_interval 91
Figure 42 – Calculation of allowable_refresh_interval 93

Figure 43 – Calculation of allowable_delay 94
Figure 44 – Calculation of response time between safety PLCs 100
Figure 45 – Constraints on N_{SE} and m 102
Figure A.1 – Allowable_delay and offset calculation deviation 105

Table 1 – Selection of the various measures for possible errors 25
Table 2 – M1 safety device manager attribute format 31
Table 3 – S1 safety device manager attribute format 31
Table 4 – M1 safety connection manager attribute format 31
Table 5 – S1 safety connection manager attribute format 31
Table 6 – M1 safety cyclic transmission attribute format 32
Table 7 – S1 safety cyclic transmission attribute format 33
Table 8 – M1 safety device manager attribute encoding 33
Table 9 – S1 safety device manager attribute encoding 34
Table 10 – M1 safety connection manager attribute encoding 34
Table 11 – S1 safety connection manager attribute encoding 34
Table 12 – M1 safety cyclic transmission attribute encoding 35
Table 13 – S1 safety cyclic transmission attribute encoding 37
Table 14 – Safety master monitor timer operation 41
Table 15 – Safety slave monitor timer operation 41
Table 16 – Safety data monitor timer operation 41
Table 17 – Details of connection establishment and confirmation processing 43
Table 18 – Details of slave information verification processing 43
Table 19 – Details of safety slave parameter transmission processing 44
Table 20 – Monitor LEDs 45
Table 21 – Safety function response time calculation 46
Table 22 – Safety function response time definition of terms 46
Table 23 – Selection of the various measures for possible errors 50
Table 24 – SS-Start 55
Table 25 – SS-Restart 55
Table 26 – SS-InvokeFunc 56
Table 27 – SS-Read 56
Table 28 – SS-Write 57
Table 29 – SS-Terminate 57
Table 30 – Safety PDU elements 58
Table 31 – CTRL Elements 59
Table 32 – State list 65
Table 33 – SFSPM-M timers 70
Table 34 – SFSPM-M state transition table 71
Table 35 – support_functions 74
Table 36 – error_category 77
Table 37 – error_category for AL errors 77
Table 38 – error_code 78

Table 39 – SFSPM-S timers 79
Table 40 – SFSPM-S state transition table 80
Table 41 – Parameters used by safety communication layer 90
Table 42 – SM-SetSafetyStationInfo 95
Table 43 – Safety station information setting parameters of SM-SetSafetyStationInfo 95
Table 44 – SM-SetSafetyNetworkParameter 96
Table 45 – Safety network parameters of SM-SetSafetyNetworkParameter 96
Table 46 – SM-GetSafetyStationInfo 96
Table 47 – Safety station information parameters of SM-GetSafetyStationInfo (Request) 97
Table 48 – Safety station information parameters of SM-GetSafetyStationInfo (Response) 97
Table 49 – SM-GetSafetyNetworkParameter 97
Table 50 – Parameters of SM-GetSafetyNetworkParameter request 97
Table 51 – Parameters of SM-GetSafetyNetworkParameter response 98
Table 52 – Monitor LEDs 99
Table 53 – Communication port monitor LEDs 99
Table A.1 – Residual error probability for FSCP 8/1 CRC 104
Table A.2 – Residual error probability for FSCP 8/2 CRC 105

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES –

Part 3-8: Functional safety fieldbuses – Additional specifications for CPF 8

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.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

IEC 61784-3-8 has been prepared by subcommittee 65C: Industrial networks, of IEC technical committee 65: Industrial-process measurement, control and automation. It is an International Standard.

This third edition cancels and replaces the second edition published in 2016. This edition constitutes a technical revision.

This edition includes the following significant technical changes with respect to the previous edition:

- structured for compliance with IEC 61784-3 Ed.4;
- general editorial changes and clarifications;
- safety measures (11.5.3);

- safety application service elements (11.6.2);
- safety PDU format (11.7.1);
- constraints for calculations of system characteristics (11.9.5);
- safety measures (12.5.3);
- safety PDU format (12.7.1);
- behaviour (12.7.2);
- constraints for calculations of system characteristics (12.9.5);
- hash function calculations (Annex A).

The text of this International Standard is based on the following documents:

FDIS	Report on voting
65C/1083/FDIS	65C/1087/RVD

Full information on the voting for its approval can be found in the report on voting indicated in the above table.

The language used for the development of this International Standard is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/standardsdev/publications.

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 document will remain unchanged until the stability date indicated on the IEC website under "http://webstore.iec.ch" in the data related to the specific document. At this date, the document 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.

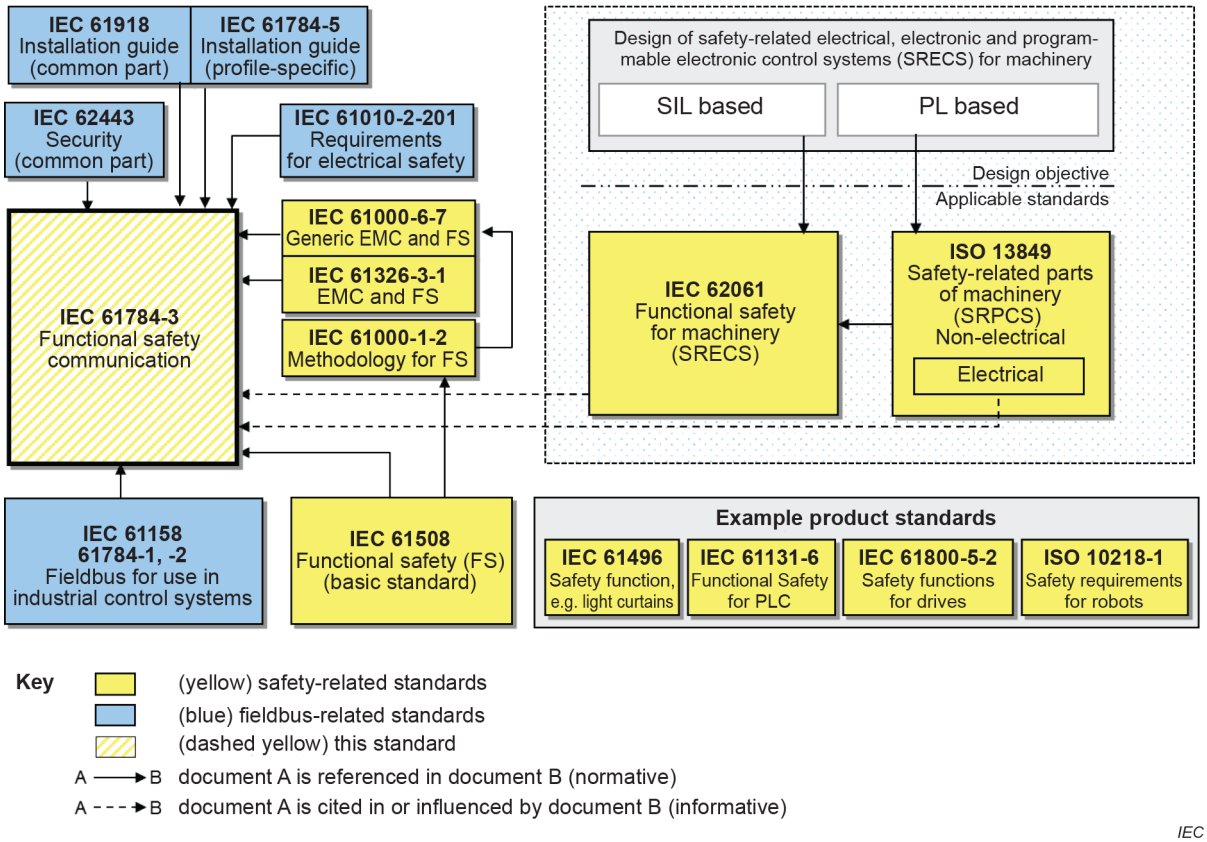
0 Introduction

0.1 General

The IEC 61158 (all parts) 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 fieldbus enhancements continue to emerge, addressing applications for areas such as real time and safety-related applications.

IEC 61784-3 (all parts) explains the relevant principles for functional safety communications with reference to IEC 61508 (all parts) 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 IEC 61158 (all parts). It does not cover electrical safety and intrinsic safety aspects. It also does not cover security aspects, nor does it provide any requirements for security.

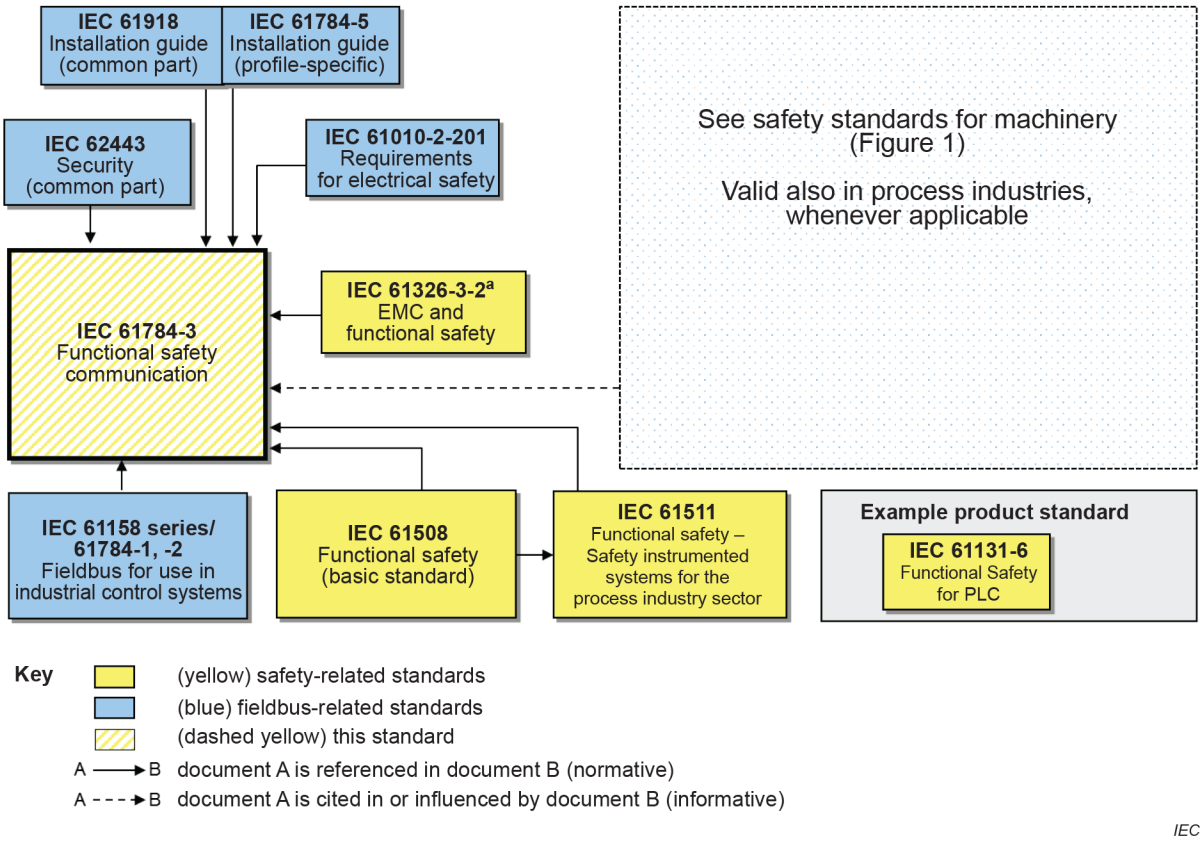
Figure 1 shows the relationships between IEC 61784-3 (all parts) and relevant safety and fieldbus standards in a machinery environment.



NOTE IEC 62061 specifies the relationship between PL (Category) and SIL.

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

Figure 2 shows the relationships between IEC 61784-3 (all parts) and relevant safety and fieldbus standards in a process environment.



[a] For specified electromagnetic environments; otherwise IEC 61326-3-1 or IEC 61000-6-7.

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 (all parts) 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 IEC 61784-3 (all parts) 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 (FSCP) within this system – implementation of a functional safety communication profile in a standard device is not sufficient to qualify it as a safety device.

IEC 61784-3 (all parts) describes:

- basic principles for implementing the requirements of IEC 61508 (all parts) for safety-related data communications, including possible transmission faults, remedial measures and considerations affecting data integrity;
- functional safety communication profiles for several communication profile families in IEC 61784-1 and IEC 61784-2, including safety layer extensions to the communication service and protocols sections of IEC 61158 (all parts).

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 a patent concerning the functional safety communication profiles for family 8. IEC takes no position concerning the evidence, validity, and scope of this patent right.

The holder of this patent right has assured IEC that s/he is willing to negotiate licences under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statement of the holder of this patent right is registered with IEC. Information may be obtained from the patent database available at http://patents.iec.ch.

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

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES –

Part 3-8: Functional safety fieldbuses – Additional specifications for CPF 8

1 Scope

This part of IEC 61784-3 (all parts) specifies a safety communication layer (services and protocol) based on CPF 8 of IEC 61784-1, IEC 61784-2 and IEC 61158 Type 18 and Type 23. It identifies the principles for functional safety communications defined in IEC 61784-3 that are relevant for this safety communication layer. This safety communication layer is intended for implementation in safety devices only.

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 document 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 (all parts)[1] for functional safety. These mechanisms may be used in various industrial applications such as process control, manufacturing automation and machinery.

This document 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 document in a standard device is not sufficient to qualify it as a safety device.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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, *Industrial-process measurement and control – Programmable controllers – Part 2: Equipment requirements and tests*

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 61158-3-18, *Industrial communication networks – Fieldbus specifications – Part 3-18: Data-link layer service definition – Type 18 elements*

IEC 61158-4-18, *Industrial communication networks – Fieldbus specifications – Part 4-18: Data-link layer protocol specification – Type 18 elements*

---

1 In the following pages of this document, "IEC 61508" will be used for "IEC 61508 (all parts)".

IEC 61158-5-18, *Industrial communication networks – Fieldbus specifications – Part 5-18: Application layer service definition – Type 18 elements*

IEC 61158-5-23, *Industrial communication networks – Fieldbus specifications – Part 5-23: Application layer service definition – Type 23 elements*

IEC 61158-6-18, *Industrial communication networks – Fieldbus specifications – Part 6-18: Application layer protocol specification – Type 18 elements*

IEC 61158-6-23, *Industrial communication networks – Fieldbus specifications – Part 6-23: Application layer protocol specification – Type 23 elements*

IEC 61326-3-1, *Electrical equipment for measurement, control and laboratory use – EMC requirements – Part 3-1: Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety) – General industrial applications*

IEC 61326-3-2, *Electrical equipment for measurement, control and laboratory use – EMC requirements – Part 3-2: Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety) – Industrial applications with specified electromagnetic environment*

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

IEC 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/IEEE 8802-3*

IEC 61784-3:2021, *Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions*

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

ISO/IEC/IEEE 8802-3, *Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 3: Standard for Ethernet*

SOMMAIRE

AVANT-PROPOS 115
0 Introduction 117
0.1 Généralités 117
0.2 Déclaration de brevets 119
1 Domaine d'application 120
2 Références normatives 120
3 Termes, définitions, symboles, abréviations et conventions 121
3.1 Termes et définitions 121
3.1.1 Termes et définitions communs 122
3.1.2 CPF 8: Termes et définitions supplémentaires 128
3.2 Symboles et abréviations 130
3.2.1 Symboles et abréviations communs 130
3.2.2 CPF 8: Symboles et abréviations supplémentaires 131
3.3 Conventions 131
4 Présentation générale 131
5 Généralités 131
6 Services de la couche de communication de sécurité 131
7 Protocole de couche de communication de sécurité 132
8 Gestion de la couche de communication de sécurité 132
9 Exigences système 132
10 Evaluation 132
11 FSCP 8/1 132
11.1 Domaine d'application – FSCP 8/1 132
11.2 Références normatives – FSCP 8/1 132
11.3 Termes, définitions, symboles, abréviations et conventions – FSCP 8/1 132
11.4 Aperçu de FSCP 8/1 (CC-Link Safety™) 132
11.5 Généralités – FSCP 8/1 133
11.5.1 Documents externes de spécifications applicables au profil 133
11.5.2 Exigences fonctionnelles de sécurité 133
11.5.3 Mesures de sécurité 133
11.5.4 Structure de la couche de communication de sécurité 135
11.5.5 Relations avec la FAL (et DLL PhL) 136
11.6 Services de la couche de communication de sécurité pour FSCP 8/1 136
11.6.1 Généralités 136
11.6.2 SASE 136
11.6.3 SAR 137
11.6.4 ASE SAR des données de processus 138
11.7 Protocole de couche de communication de sécurité pour FSCP 8/1 139
11.7.1 Format PDU de sécurité 139
11.7.2 Description d'état 148
11.8 Gestion de la couche de communication de sécurité pour FSCP 8/1 153
11.8.1 Généralités 153
11.8.2 Etablissement de connexion et processus de confirmation 153
11.8.3 Vérification des esclaves de sécurité 154
11.9 Exigences système pour FSCP 8/1 154

11.9.1 Voyants et commutateurs 154
11.9.2 Lignes directrices d'installation 156
11.9.3 Temps de réponse de la fonction de sécurité 156
11.9.4 Durée des demandes (ou sollicitations) 157
11.9.5 Contraintes liées au calcul des caractéristiques du système 157
11.9.6 Maintenance 157
11.9.7 Manuel de sécurité 158
11.10 Evaluation de FSCP 8/1 158
12 FSCP 8/2 158
12.1 Domaine d'application – FSCP 8/2 158
12.2 Références normatives – FSCP 8/2 158
12.3 Termes, définitions, symboles, abréviations et conventions – FSCP 8/2 158
12.4 Présentation de FSCP 8/2 (fonction de communication de sécurité CC-Link IE™) 159
12.5 Généralités – FSCP 8/2 159
12.5.1 Documents externes de spécifications applicables au profil 159
12.5.2 Exigences fonctionnelles de sécurité 159
12.5.3 Mesures de sécurité 160
12.5.4 Structure de la couche de communication de sécurité 165
12.5.5 Relations avec la FAL (et DLL PhL) 166
12.6 Services de la couche de communication de sécurité pour FSCP 8/2 166
12.6.1 Généralités 166
12.6.2 Services de rétablissement de la connexion 166
12.6.3 Services de transmission de données 167
12.6.4 Service de notification de fin de connexion 168
12.7 Protocole de couche de communication de sécurité pour FSCP 8/2 169
12.7.1 Format PDU de sécurité 169
12.7.2 Machine de protocole de service FAL de sécurité (SFSPM) 175
12.8 Gestion de la couche de communication de sécurité pour FSCP 8/2 201
12.8.1 Définitions de paramètre 201
12.8.2 Configuration de paramètre 206
12.8.3 Services de gestion 206
12.9 Exigences système pour FSCP 8/2 209
12.9.1 Voyants et commutateurs 209
12.9.2 Lignes directrices d'installation 211
12.9.3 Temps de réponse de la fonction de sécurité 211
12.9.4 Durée des demandes (ou sollicitations) 212
12.9.5 Contraintes liées au calcul des caractéristiques du système 212
12.9.6 Maintenance 213
12.9.7 Manuel de sécurité 214
12.10 Evaluation de FSCP 8/2 214
Annexe A (informative) Informations supplémentaires pour les profils de communication de sécurité fonctionnelle de la CPF 8 215
A.1 Calcul de la fonction de hachage pour FSCP 8/1 215
A.2 Calcul de la fonction de hachage pour FSCP 8/2 215
A.3 Signification de la formule de calcul du temps de réponse pour FSCP 8/2 216
Annexe B (informative) Informations pour l'évaluation des profils de communication de sécurité fonctionnelle de la CPF 8 218
Bibliographie 219

Figure 1 – Relations entre l'IEC 61784-3 et d'autres normes (machines) 117
Figure 2 – Relations entre l'IEC 61784-3 et d'autres normes (transformation) 118
Figure 3 – Relation entre la SCL et les autres couches du Type 18 de l'IEC 61158 136
Figure 4 – Diagramme d'états 149
Figure 5 – Détection d'une répétition non prévue 162
Figure 6 – Détection d'une séquence incorrecte 162
Figure 7 – Détection d'une perte 163
Figure 8 – Détection d'un retard inacceptable par les horodatages 164
Figure 9 – Détection d'un retard inacceptable par le temporisateur 164
Figure 10 – Hiérarchie de protocole 166
Figure 11 – Structure du PDU de sécurité 169
Figure 12 – Configuration CTRL 170
Figure 13 – TS du SASE-M et du SASE-S 173
Figure 14 – S-Data lors du rafraîchissement de sécurité 173
Figure 15 – S-Data hors du rafraîchissement de sécurité 174
Figure 16 – Configuration d'en-tête S-Data 174
Figure 17 – Calcul de CRC 175
Figure 18 – Modèle de communication 176
Figure 19 – Diagramme de transition d'état SFSPM 176
Figure 20 – Séquence d'établissement d'une connexion 178
Figure 21 – Séquence facultative au cours de la séquence d'établissement de la connexion 179
Figure 22 – Séquence de communication lors de la communication de rafraîchissement de sécurité 180
Figure 23 – Séquence de mesure et de génération du décalage lors de la communication de rafraîchissement de sécurité 180
Figure 24 – Diagramme de transition d'état SFSPM-M 181
Figure 25 – Séquence autre que celle réalisée lors du rafraîchissement de sécurité 185
Figure 26 – S-Connect-req 185
Figure 27 – S-InitConfirmNetPrm-req 186
Figure 28 – net_prm_list 186
Figure 29 – S-InitVerifyStnPrm-req 187
Figure 30 – stn_prm_list 187
Figure 31 – S-InvokeFunc-req 187
Figure 32 – S-WriteErrorInfo-req 188
Figure 33 – date_and_time_of_occurence 189
Figure 34 – Diagramme de transition d'état SFSPM-S 190
Figure 35 – Séquence autre que celle réalisée lors du rafraîchissement de sécurité 195
Figure 36 – S-Connect-rsp 195
Figure 37 – S-InitConfirmNetPrm-rsp 196
Figure 38 – S-InitVerifyStnPrm-rsp 196
Figure 39 – S-InvokeFunc-rsp 197
Figure 40 – Procédure de calcul du décalage de l'horloge de sécurité 198

Figure 41 – Relation entre la variation de l'intervalle de transmission et transmission_interval 202
Figure 42 – Calcul d'allowable_refresh_interval 204
Figure 43 – Calcul d'allowable_delay 205
Figure 44 – Calcul du temps de réponse entre des PLC de sécurité 211
Figure 45 – Contraintes sur N_{SE} et m 213
Figure A.1 – allowable_delay et écart de calcul de décalage 216

Tableau 1 – Choix des différentes mesures qui correspondent aux erreurs possibles 134
Tableau 2 – Format d'attributs de gestionnaire d'appareil de sécurité M1 140
Tableau 3 – Format d'attributs de gestionnaire d'appareil de sécurité S1 140
Tableau 4 – Format d'attributs de gestionnaire de connexion de sécurité M1 140
Tableau 5 – Format d'attributs de gestionnaire de connexion de sécurité S1 141
Tableau 6 – Format d'attributs de transmission cyclique de sécurité M1 141
Tableau 7 – Format d'attributs de transmission cyclique de sécurité S1 142
Tableau 8 – Codage d'attributs de gestionnaire d'appareil de sécurité M1 143
Tableau 9 – Codage d'attributs de gestionnaire d'appareil de sécurité S1 143
Tableau 10 – Codage d'attributs de gestionnaire de connexion de sécurité M1 144
Tableau 11 – Codage d'attributs de gestionnaire de connexion de sécurité S1 144
Tableau 12 – Codage d'attributs de transmission cyclique de sécurité M1 145
Tableau 13 – Codage d'attributs de transmission cyclique de sécurité S1 147
Tableau 14 – Fonctionnement du temporisateur de contrôle des appareils maîtres de sécurité 151
Tableau 15 – Fonctionnement du temporisateur de contrôle des appareils esclaves de sécurité 151
Tableau 16 – Fonctionnement du temporisateur de contrôle des données de sécurité 152
Tableau 17 – Détails de l'établissement de connexion et du processus de confirmation 153
Tableau 18 – Détails du processus de vérification des informations sur les esclaves 154
Tableau 19 – Détails du processus de transmission des paramètres des esclaves de sécurité 154
Tableau 20 – LED du moniteur 155
Tableau 21 – Calcul du temps de réponse de la fonction de sécurité 156
Tableau 22 – Définitions des termes relatifs au temps de réponse de la fonction de sécurité 157
Tableau 23 – Choix des différentes mesures qui correspondent aux erreurs possibles 161
Tableau 24 – SS-Start 166
Tableau 25 – SS-Restart 167
Tableau 26 – SS-InvokeFunc 167
Tableau 27 – SS-Read 168
Tableau 28 – SS-Write 168
Tableau 29 – SS-Terminate 168
Tableau 30 – Eléments du PDU de sécurité 169
Tableau 31 – Eléments de CTRL 170
Tableau 32 – Liste des états 177

Tableau 33 – Temporisateurs SFSPM-M 182
Tableau 34 – Table des transitions d'état SFSPM-M 182
Tableau 35 – support_functions 186
Tableau 36 – error_category 188
Tableau 37 – error_category correspondant aux erreurs AL 189
Tableau 38 – error_code 189
Tableau 39 – Temporisateurs SFSPM-S 191
Tableau 40 – Table des transitions d'état SFSPM-S 191
Tableau 41 – Paramètres utilisés par la couche de communication de sécurité 201
Tableau 42 – SM-SetSafetyStationInfo 206
Tableau 43 – Paramètres de configuration des informations relatives au poste de sécurité de SM-SetSafetyStationInfo 206
Tableau 44 – SM-SetSafetyNetworkParameter 207
Tableau 45 – Paramètres de réseau de sécurité de SM-SetSafetyNetworkParameter 207
Tableau 46 – SM-GetSafetyStationInfo 207
Tableau 47 – Paramètres des informations relatives au poste de sécurité de SM-GetSafetyStationInfo (Demande) 208
Tableau 48 – Paramètres des informations relatives au poste de sécurité de SM-GetSafetyStationInfo (Réponse) 208
Tableau 49 – SM-GetSafetyNetworkParameter 208
Tableau 50 – Paramètres de la demande SM-GetSafetyNetworkParameter 209
Tableau 51 – Paramètres de la réponse SM-GetSafetyNetworkParameter 209
Tableau 52 – LED du moniteur 210
Tableau 53 – LED du moniteur de port de communication 211
Tableau A.1 – Probabilité d'erreurs résiduelles du CRC pour FSCP 8/1 215
Tableau A.2 – Probabilité d'erreurs résiduelles du CRC pour FSCP 8/2 216

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

RÉSEAUX DE COMMUNICATION INDUSTRIELS – PROFILS –

Partie 3-8: Bus de terrain de sécurité fonctionnelle – Spécifications supplémentaires pour CPF 8

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.
9) L'attention est attirée sur le fait que certains des éléments du présent document de l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets.

L'IEC 61784-3-8 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. Il s'agit d'une Norme internationale.

Cette troisième édition annule et remplace la deuxième édition parue en 2016. Cette édition constitue une révision technique.

Cette édition inclut les modifications techniques majeures suivantes par rapport à l'édition précédente:

- structuration à des fins de conformité à l'IEC 61784-3 Ed.4;
- modifications et clarifications rédactionnelles d'ordre général;

- mesures de sécurité (11.5.3);
- élément de service d'application de sécurité (11.6.2);
- format PDU de sécurité (11.7.1);
- contraintes liées au calcul des caractéristiques du système (11.9.5);
- mesures de sécurité (12.5.3);
- format PDU de sécurité (12.7.1);
- comportement (12.7.2);
- contraintes liées au calcul des caractéristiques du système (12.9.5);
- calcul de la fonction de hachage (Annexe A).

Le texte de cette Norme internationale est issu des documents suivants:

FDIS	Rapport de vote
65C/1083/FDIS	65C/1087/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à son approbation.

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

La langue employée pour l'élaboration de cette Norme internationale est l'anglais.

Le présent document a été rédigé selon les Directives ISO/IEC, Partie 2, il a été développé selon les Directives ISO/IEC, Partie 1 et les Directives ISO/IEC, Supplément IEC, disponibles sous www.iec.ch/members_experts/refdocs. Les principaux types de documents développés par l'IEC sont décrits plus en détail sous www.iec.ch/standardsdev/publications.

Une liste de toutes les parties de la série IEC 61784-3, publiées sous le titre général *Réseaux de communication industriels – Profils – Bus de terrain de sécurité fonctionnelle*, se trouve sur le site web de l'IEC.

Le comité a décidé que le contenu du présent document ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous webstore.iec.ch dans les données relatives au document recherché. A cette date, le document sera

- reconduit,
- supprimé,
- remplacé par une édition révisée, ou
- amendé.

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.

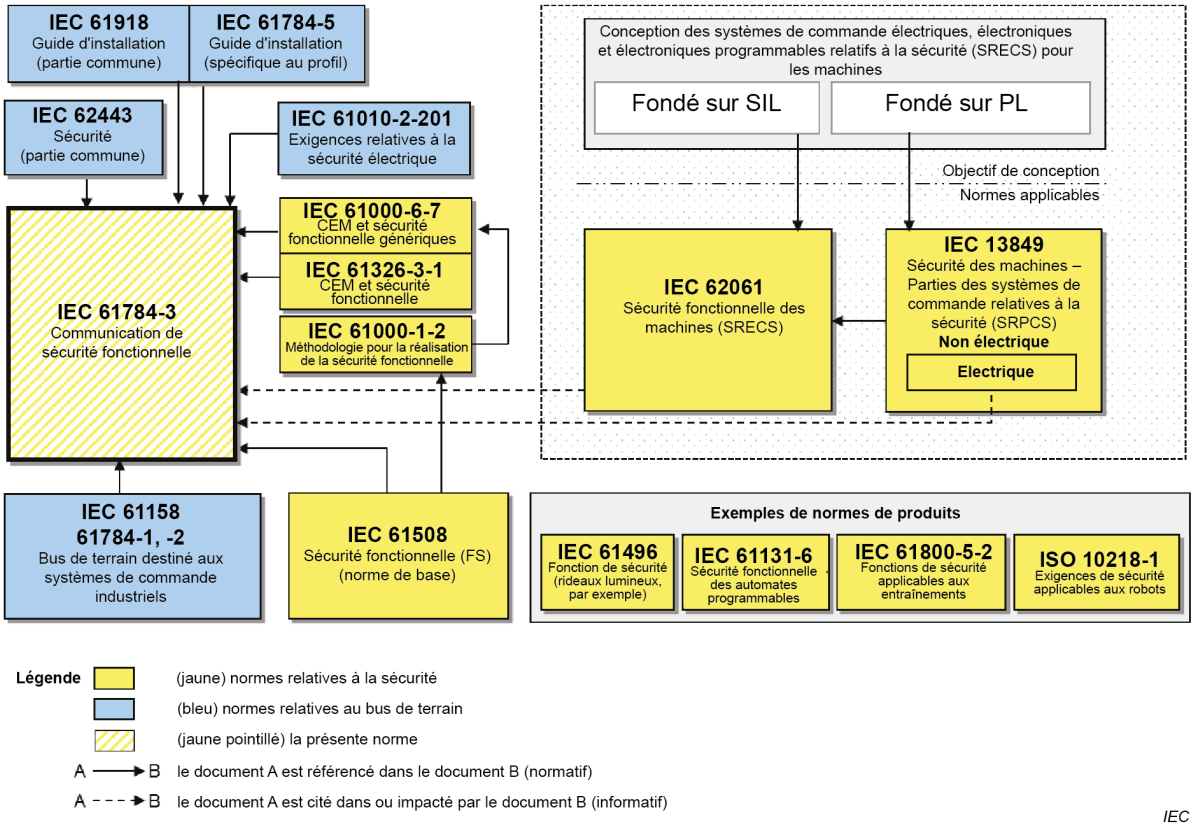
0 Introduction

0.1 Généralités

L'IEC 61158 (toutes les parties), relative aux bus de terrain, ainsi que ses normes associées IEC 61784-1 et IEC 61784-2, définissent 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. Les améliorations des bus de terrain se poursuivent; elles couvrent des applications pour des domaines comme les applications en temps réel relatives à la sécurité.

La série IEC 61784-3 (toutes les parties) explique les principes pertinents pour les communications de sécurité fonctionnelle en référence à l'IEC 61508 (toutes les parties) et spécifie plusieurs couches de communication de sécurité (profils et protocoles correspondants) qui reposent sur les profils de communication et les couches de protocole de l'IEC 61784-1, l'IEC 61784-2 et l'IEC 61158 (toutes les parties). Elle ne couvre pas les aspects relatifs à la sécurité électrique et à la sécurité intrinsèque. Elle ne couvre pas non plus les aspects relatifs à la sûreté et ne prévoit aucune exigence en matière de sûreté.

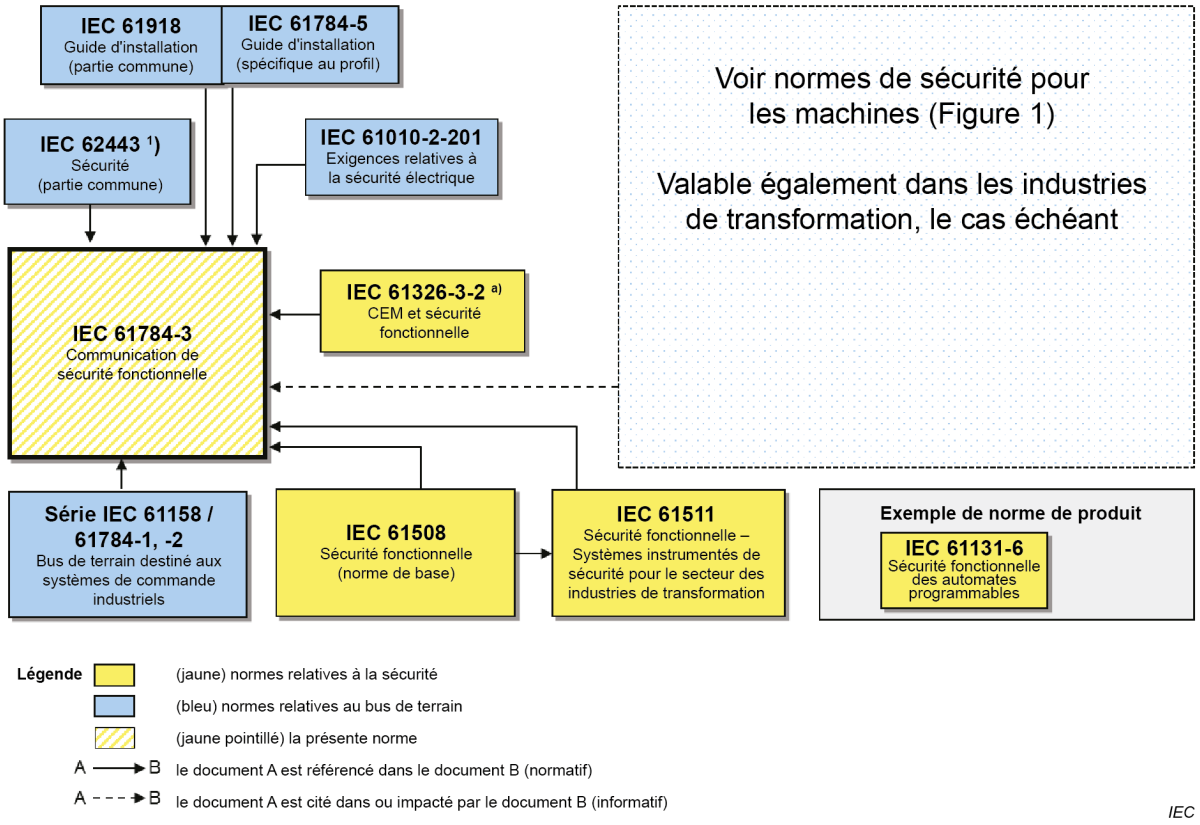
La Figure 1 représente les relations entre l'IEC 61784-3 (toutes les parties) et les normes pertinentes relatives à la sécurité et aux bus de terrain dans un environnement de machines.



NOTE L'IEC 62061 spécifie la relation entre PL (Catégorie) et SIL.

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

La Figure 2 représente les relations entre l'IEC 61784-3 (toutes les parties) et les normes pertinentes relatives à la sécurité et aux bus de terrain dans un environnement de processus.



[a] Pour les environnements électromagnétiques spécifiés; sinon, l'IEC 61326-3-1 ou l'IEC 61000-6-7 s'applique.

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

Les couches de communication de sécurité mises en œuvre dans le cadre de systèmes relatifs à la sécurité conformément à l'IEC 61508 (toutes les parties) assurent la confiance nécessaire à accorder à la transmission de messages (informations) entre plusieurs participants 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 l'IEC 61784-3 (toutes les parties) permettent de s'assurer qu'un bus de terrain peut être utilisé dans des applications qui nécessitent 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 (FSCP) 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).

L'IEC 61784-3 (toutes les parties) décrit:

- les principes de base de la mise en œuvre des exigences de l'IEC 61508 (toutes les parties) pour les communications de données relatives à la sécurité, y compris les anomalies de transmission potentielles, les mesures correctives et des considérations relatives à l'intégrité des données;
- les profils de communication de sécurité fonctionnelle pour plusieurs familles de profils de communication dans l'IEC 61784-1 et l'IEC 61784-2, y compris les extensions de la couche de sécurité aux sections relatives au service et aux protocoles de communication de l'IEC 61158 (toutes les parties).

0.2 Déclaration de brevets

La Commission Electrotechnique Internationale (IEC) attire l'attention sur le fait qu'il est déclaré que la conformité avec les dispositions du présent document peut impliquer l'utilisation de brevets intéressant les profils de communication de sécurité fonctionnelle pour la famille 8. L'IEC ne prend pas position quant à la preuve, à la validité et à la portée de ces droits de propriété.

Le détenteur de ces droits de propriété a donné l'assurance à l'IEC qu'il consent à négocier des licences avec des demandeurs du monde entier à des termes et conditions raisonnables et non discriminatoires. A ce propos, la déclaration du détenteur des droits de propriété est enregistrée à l'IEC. Des informations peuvent être obtenues dans la base de données des droits de propriété, disponible à l'adresse suivante: http://patents.iec.ch.

L'attention est d'autre part attirée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété autres que ceux qui ont été enregistrés dans la base de données des droits de propriété. L'IEC ne saurait être tenue pour responsable de l'identification de ces droits de propriété en tout ou partie.

RÉSEAUX DE COMMUNICATION INDUSTRIELS – PROFILS –

Partie 3-8: Bus de terrain de sécurité fonctionnelle – Spécifications supplémentaires pour CPF 8

1 Domaine d'application

La présente partie de l'IEC 61784-3 (toutes les parties) spécifie une couche de communication de sécurité (services et protocole) qui repose sur la CPF 8 de l'IEC 61784-1, de l'IEC 61784-2 et de l'IEC 61158 Type 18 et Type 23. Elle identifie les principes applicables aux communications de sécurité fonctionnelle définies dans l'IEC 61784-3, qui correspondent à cette couche de communication de sécurité. Cette couche de communication de sécurité est destinée à être mise en œuvre uniquement sur les appareils 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.

Le présent document définit les mécanismes de transmission des messages relatifs 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 (toutes les parties)[1] concernant la sécurité fonctionnelle. Ces mécanismes peuvent être utilisés dans différentes applications industrielles, par exemple la commande de processus, l'usinage automatique et les machines.

Le présent document fournit des lignes directrices aux développeurs, ainsi qu'aux évaluateurs d'appareils et de 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 d'un profil de communication de sécurité fonctionnelle conforme au présent document dans un appareil normal ne suffit pas à le qualifier d'appareil de sécurité).

2 Références normatives

Les documents suivants sont cités dans le texte de sorte qu'ils constituent, pour tout ou partie de leur contenu, des exigences 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, *Mesurage et contrôle des processus industriels – Automates programmables – Partie 2: Exigences et essais des équipements*

IEC 61158 (toutes les parties), *Réseaux de communication industriels – Spécifications des bus de terrain*

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

IEC 61158-3-18, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 3-18: Définition des services de couche liaison de données – Eléments de type 18*

---

[1] Dans les pages suivantes du présent document, "IEC 61508" remplace "IEC 61508 (toutes les parties)".

IEC 61158-4-18, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 4-18: Spécification du protocole de la couche de liaison de données – Eléments de type 18*

IEC 61158-5-18, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 5-18: Définition des services des couches d'application – Eléments de type 18*

IEC 61158-5-23, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 5-23: Définition des services des couches d'application – Eléments de type 23*

IEC 61158-6-18, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 6-18: Spécification de protocole de la couche application – Eléments de type 18*

IEC 61158-6-23, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 6-23: Spécification de protocole de la couche application – Eléments de type 23*

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

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

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

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

IEC 61784-3:2021, *Réseaux de communication industriels – Profils – Partie 3: Bus de terrain de sécurité fonctionnelle – Règles générales et définitions de profils*

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

ISO/IEC/IEEE 8802-3, *Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 3: Standard for Ethernet* (disponible en anglais seulement)