IEC 61784-3-3

Edition 4.0 2021-05

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

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

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

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

ICS 25.040.40; 35.100.05

ISBN 978-2-8322-9749-0

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 9
0 Introduction 11
0.1 General 11
0.2 Patent declaration 12
1 Scope 14
2 Normative references 14
3 Terms, definitions, symbols, abbreviated terms and conventions 16
3.1 Terms and definitions 16
3.1.1 Common terms and definitions 16
3.1.2 CPF 3: Additional terms and definitions 22
3.2 Symbols and abbreviated terms 27
3.2.1 Common symbols and abbreviated terms 27
3.2.2 CPF 3: Additional symbols and abbreviated terms 28
3.3 Conventions 29
4 Overview of FSCP 3/1 (PROFIsafe™) 29
5 General 32
5.1 External documents providing specifications for the profile 32
5.2 Safety functional requirements 32
5.3 Safety measures 32
5.4 Safety communication layer structure 33
5.4.1 Principle of FSCP 3/1 safety communications 33
5.4.2 CPF 3 communication structures 35
5.5 Relationships with FAL (and DLL, PhL) 37
5.5.1 Device model 37
5.5.2 Application and communication relationships 38
5.5.3 Data types 38
6 Safety communication layer services 39
6.1 F-Host driver services 39
6.2 F-Device driver services 43
6.3 Diagnosis 45
6.3.1 Safety alarm generation 45
6.3.2 F-(Sub)Module safety layer diagnosis 45
7 Safety communication layer protocol 46
7.1 Safety PDU format 46
7.1.1 Safety PDU structure 46
7.1.2 Safety IO data 47
7.1.3 Status and Control Byte 47
7.1.4 (Virtual) MonitoringNumber 49
7.1.5 (Virtual) MNR mechanism (F_CRC_Seed=0) 50
7.1.6 (Virtual) MNR mechanism (F_CRC_Seed=1) 50
7.1.7 CRC2 Signature (F_CRC_Seed=0) 52
7.1.8 CRC2 Signature (F_CRC_Seed=1) 53
7.1.9 Non-safety IO data 54
7.2 FSCP 3/1 behavior 54
7.2.1 General 54

7.2.2 F-Host driver state diagram 55
7.2.3 F-Device driver state diagram 58
7.2.4 F-Device driver restart 62
7.2.5 Sequence diagrams 62
7.2.6 Timing diagram for a MonitoringNumber reset 69
7.2.7 Monitoring of safety times 69
7.3 Reaction in the event of a malfunction 72
7.3.1 Corruption of safety data 72
7.3.2 Unintended repetition 72
7.3.3 Incorrect sequence 73
7.3.4 Loss 73
7.3.5 Unacceptable delay 73
7.3.6 Insertion 73
7.3.7 Masquerade 73
7.3.8 Addressing 73
7.3.9 Out-of-sequence 74
7.3.10 Loop-back 74
7.3.11 Network boundaries and router 74
7.4 F-Startup and parameter change at runtime 75
7.4.1 Standard startup procedure 75
8 Safety communication layer management 75
8.1 F-Parameter 75
8.1.1 Summary 75
8.1.2 F_Source/Destination_Address (Codename) 76
8.1.3 F_WD_Time (F-Watchdog time) 77
8.1.4 F_WD_Time_2 (secondary F-Watchdog time) 77
8.1.5 F_Prm_Flag1 (Parameters for the safety layer management) 77
8.1.6 F_Prm_Flag2 (Parameters for the safety layer management) 80
8.1.7 F_iPar_CRC (value of iPar_CRC across iParameters) 81
8.1.8 F_Par_CRC calculation (across F-Parameters) 81
8.1.9 Structure of the F-Parameter record data object 82
8.2 iParameter and iPar_CRC 82
8.3 Safety parameterization 83
8.3.1 Objectives 83
8.3.2 GSDL and GSDML safety extensions 84
8.3.3 Securing safety parameters and GSD data 86
8.4 Safety configuration 90
8.4.1 Order of IO data types 90
8.4.2 Securing the safety IO data description 90
8.4.3 DataItem data type section examples 91
8.5 Data type information usage 95
8.5.1 F-Host Channel driver 95
8.5.2 Rules for standard F-Host Channel drivers 96
8.5.3 Recommendations for the use of F-Host Channel drivers 97
8.6 Safety parameter assignment mechanisms 98
8.6.1 F-Parameter assignment 98
8.6.2 General iParameter assignment 98
8.6.3 System integration requirements for iParameterization tools 98
8.6.4 iPar-Server 100

9 System requirements 111
9.1 Indicators and switches 111
9.2 Installation guidelines 111
9.3 Safety function response time 111
9.3.1 Model 111
9.3.2 Calculation and optimization 113
9.3.3 Adjustment of watchdog times for FSCP 3/1 115
9.3.4 Engineering tool support 116
9.3.5 Retries (repetition of messages) 116
9.4 Duration of demands 117
9.5 Constraints for the calculation of system characteristics 117
9.5.1 Probabilistic considerations 117
9.5.2 Safety related assumptions 119
9.5.3 Non safety related constraints (availability) 120
9.6 Maintenance 120
9.6.1 F-(Sub)Module commissioning / replacement 120
9.6.2 Identification and maintenance functions 120
9.7 Safety manual 121
9.8 Wireless transmission channels 122
9.8.1 Black channel approach 122
9.8.2 Availability 122
9.8.3 Security measures 122
9.8.4 Stationary and mobile applications 122
9.9 Relationship between functional safety and security 123
9.10 Conformance classes 123
10 Assessment 125
10.1 Safety policy 125
10.2 Obligations 125
Annex A (informative) Additional information for functional safety communication profiles of CPF 3 126
A.1 Hash function calculation 126
A.2 Example values for MonitoringNumbers (MNR) 130
Annex B (informative) Information for assessment of the functional safety communication profiles of CPF 3 131
Annex C (normative) Optional features 132
C.1 Reaction on Device_Fault in F-Host 132
C.1.1 Situation 132
C.1.2 Documentation for the user 132
C.1.3 Optional extensions of F-Host driver Transition Table 132
C.1.4 Recommendation for the case without Extensions of F-Host driver Transitions 135
C.2 Optional extensions of F-Host driver to "Disable F-(Sub)Module" 135
C.3 Combination of "Disable F-(Sub)Module" and "reaction on Device_Fault" 139
C.4 FSCP 3/1 and PROFIenergy 141
C.4.1 Use of FSCP 3/1-Devices with PROFIenergy 141
C.4.2 Sequence in case of PROFIenergy power off on 141
C.5 Requirement multiple F-Hosts communicate with single F-(Sub)Module 141
C.6 FSCP 3/1 PiR 142
Bibliography 143

Figure 1 – Relationships of IEC 61784-3 with other standards (machinery) 11
Figure 2 – Relationships of IEC 61784-3 with other standards (process) 12
Figure 3 – Basic communication preconditions for FSCP 3/1 30
Figure 4 – Structure of an FSCP 3/1 safety PDU 30
Figure 5 – Safety communication on CPF 3 31
Figure 6 – Standard CPF 3 transmission system 34
Figure 7 – Safety layer architecture 35
Figure 8 – Basic communication layers 35
Figure 9 – Crossing network borders with routers 36
Figure 10 – Complete safety transmission paths 37
Figure 11 – IO Device model 38
Figure 12 – FSCP 3/1 communication structure 39
Figure 13 – F application interface of F-Host driver instances 40
Figure 14 – Motivation for "Channel-related Passivation" 41
Figure 15 – F-Device driver interfaces 43
Figure 16 – Safety PDU for CPF 3 47
Figure 17 – Status Byte 47
Figure 18 – Control Byte 48
Figure 19 – The Toggle Bit function 49
Figure 20 – MonitoringNumber integration 50
Figure 21 – F-Host driver CRC2 signature generation (F_CRC_Seed=0) 52
Figure 22 – Details of the CRC2 signature calculation (F_CRC_Seed=0) 53
Figure 23 – CRC2 signature calculation (F_CRC_Seed=1) 53
Figure 24 – Details of the CRC2 signature calculation (F_CRC_Seed=1) 54
Figure 25 – Safety layer communication relationship 54
Figure 26 – F-Host driver state diagram 55
Figure 27 – F-Device driver state diagram 59
Figure 28 – Interaction F-Host driver / F-Device driver during start-up 63
Figure 29 – Interaction F-Host driver / F-Device driver during F-Host power off > on 64
Figure 30 – Interaction F-Host driver / F-Device driver with delayed power on 65
Figure 31 – Interaction F-Host driver / F-Device driver during power off → on 66
Figure 32 – Interaction while F-Host driver recognizes CRC error 67
Figure 33 – Interaction while F-Device driver recognizes CRC error 68
Figure 34 – Impact of the MNR reset signal 69
Figure 35 – Monitoring the message transit time F-Host ↔ F-(Sub)Module 70
Figure 36 – Extended watchdog time on request 72
Figure 37 – Effect of F_WD_Time_2 77
Figure 38 – F_Prm_Flag1 78
Figure 39 – F_Check_iPar 78
Figure 40 – F_SIL 78
Figure 41 – F_CRC_Length 79
Figure 42 – F_CRC_Seed 79

Figure 43 – F_Prm_Flag2 80
Figure 44 – F_Passivation 80
Figure 45 – F_Block_ID 80
Figure 46 – F_Par_Version 81
Figure 47 – F-Parameter 82
Figure 48 – iParameter block 83
Figure 49 – F-Parameter extension within the GSDML specification 85
Figure 50 – F_Par_CRC signature including iPar_CRC 86
Figure 51 – F-Host Channel driver as "glue" between F-(Sub)Module and application program 96
Figure 52 – Layout example of an F-Host Channel driver 97
Figure 53 – F-Parameter assignment for F-(Sub)Modules 98
Figure 54 – System integration of CPD-Tools 99
Figure 55 – iPar-Server mechanism (commissioning) 100
Figure 56 – iPar-Server mechanism (for example F-(Sub)Module replacement) 102
Figure 57 – iPar-Server request coding ("status model") 103
Figure 58 – Coding of SR_Type 104
Figure 59 – iPar-Server request coding ("alarm model") 105
Figure 60 – iPar-Server state diagram 108
Figure 61 – Example safety function with a critical response time path 112
Figure 62 – Simplified typical response time model 112
Figure 63 – Frequency distributions of typical response times of the model 113
Figure 64 – Context of delay times and watchdog times 114
Figure 65 – Timing sections forming the FSCP 3/1 F_WD_Time 115
Figure 66 – Frequency distribution of response times with message retries 116
Figure 67 – Residual error probabilities for the 24-bit CRC polynomial 117
Figure 68 – Residual error probabilities for the 32-bit CRC polynomial 118
Figure 69 – Monitoring of corrupted messages 119
Figure A.1 – Typical "C" procedure of a cyclic redundancy check 126
Figure C.1 – F-Host driver application interface with feature Reaction on Device_Fault 132
Figure C.2 – F-Host driver application interface with feature Disable F-(Sub)Module 136
Figure C.3 – Timing diagram to use Disable F-(Sub)Module 136

Table 1 – Deployed measures to master errors 33
Table 2 – Data types for FSCP 3/1 38
Table 3 – F_MessageTrailer for FSCP 3/1 38
Table 4 – Safety layer diagnosis messages 45
Table 5 – Buffer entry on CRC2 error 46
Table 6 – MonitoringNumber of an F-Host driver SPDU 50
Table 7 – MonitoringNumber of an F-Device driver SPDU 50
Table 8 – MonitoringNumber of an F-Host driver SPDU 51
Table 9 – MonitoringNumber of an F-Device driver SPDU 51
Table 10 – Definition of terms used in F-Host driver state diagram 55

Table 11 – F-Host driver states and transitions 56
Table 12 – Definition of terms used in Figure 27 59
Table 13 – F-Device driver states and transitions 60
Table 14 – SIL monitor times 71
Table 15 – Safety network boundaries 75
Table 16 – Codename octet order 76
Table 17 – Allowed combinations of F_CRC_Seed and F_Passivation 79
Table 18 – GSDL keywords for F-Parameters and F-IO structures 84
Table 19 – Algorithm to build CRC0 87
Table 20 – GSD example in GSDL notation 88
Table 21 – GSD example in GSDML notation 89
Table 22 – Serialized octet stream for the examples 89
Table 23 – Order of IO data types 90
Table 24 – IO data structure items 91
Table 25 – DataItem section for F_IN_OUT_1 92
Table 26 – DATA_STRUCTURE_CRC for F_IN_OUT_1 92
Table 27 – DataItem section for F_IN_OUT_2 93
Table 28 – DATA_STRUCTURE_CRC for F_IN_OUT_2 93
Table 29 – DataItem section for F_IN_OUT_5 94
Table 30 – DATA_STRUCTURE_CRC for F_IN_OUT_5 94
Table 31 – DataItem section for F_IN_OUT_6 95
Table 32 – DATA_STRUCTURE_CRC for F_IN_OUT_6 95
Table 33 – Sample F-Host Channel drivers 96
Table 34 – Requirements for iParameterization 99
Table 35 – Specifier for the iPar-Server Request 104
Table 36 – Structure of the Read_RES_PDU ("read record") 106
Table 37 – Structure of the Write_REQ_PDU ("write record") 106
Table 38 – Structure of the Pull_RES_PDU ("Pull") 106
Table 39 – Structure of the Push_REQ_PDU ("Push") 107
Table 40 – iPar-Server states and transitions 109
Table 41 – iPar-Server management measures 110
Table 42 – Definition of terms in Figure 69 119
Table 43 – Information to be included in the safety manual 121
Table 44 – F-Host conformance class requirements 123
Table 45 – Main characteristics of protocol versions 124
Table 46 – F-Host driver / F-Device driver conformance matrix 124
Table A.1 – The table "Crctab24" for 24 bit CRC signature calculations 127
Table A.2 – The table "Crctab32" for 32 bit CRC signature calculations 128
Table A.3 – The table "Crctab16" for 16 bit CRC signature calculations 129
Table A.4 – Values of CN_incrNR_64 and MNR for F-Host PDU 130
Table C.1 – Definition of additional terms used in driver transitions 133
Table C.2 – F-Host driver transitions – added with reaction on Device_Fault 133
Table C.3 – Prevent unintentional restart by application measures 135

Table C.4 – F-Host driver transitions – with feature Disable F-(Sub)Module 137
Table C.5 – F-Host driver transitions – added with "reaction on Device_Fault" and "Disable F-(Sub)Module" 139

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES –

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

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 61784-3-3 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 fourth edition cancels and replaces the third edition published in 2016. This edition constitutes a technical revision.

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

- editorial changes regarding timeliness, transformation of comments in the chart into instructions;
- use abbreviations of PROFINET;
- information added about checks and safety manual for PROFIsafe Address Type 1 and 2;
- information added about PFDavg, support of automatic test, add diagnosis messages;

- explanation and specification of optional statemachines for reaction on device fault;
- new optional variable "OAD_Nec_C" for optional feature "Reaction of Device_Fault in F_Host";
- specification of the optional F-Host feature for "Disable F-(Sub)Module";
- specify requirements for FSCP 3/1 and PROFIenergy;
- specify requirement for multiple F-Hosts communicating with a single F-(Sub)Module; Update of the Safety Manual;
- diverse error corrections, fixes of typos, and reference updates;
- updated bibliography.

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.

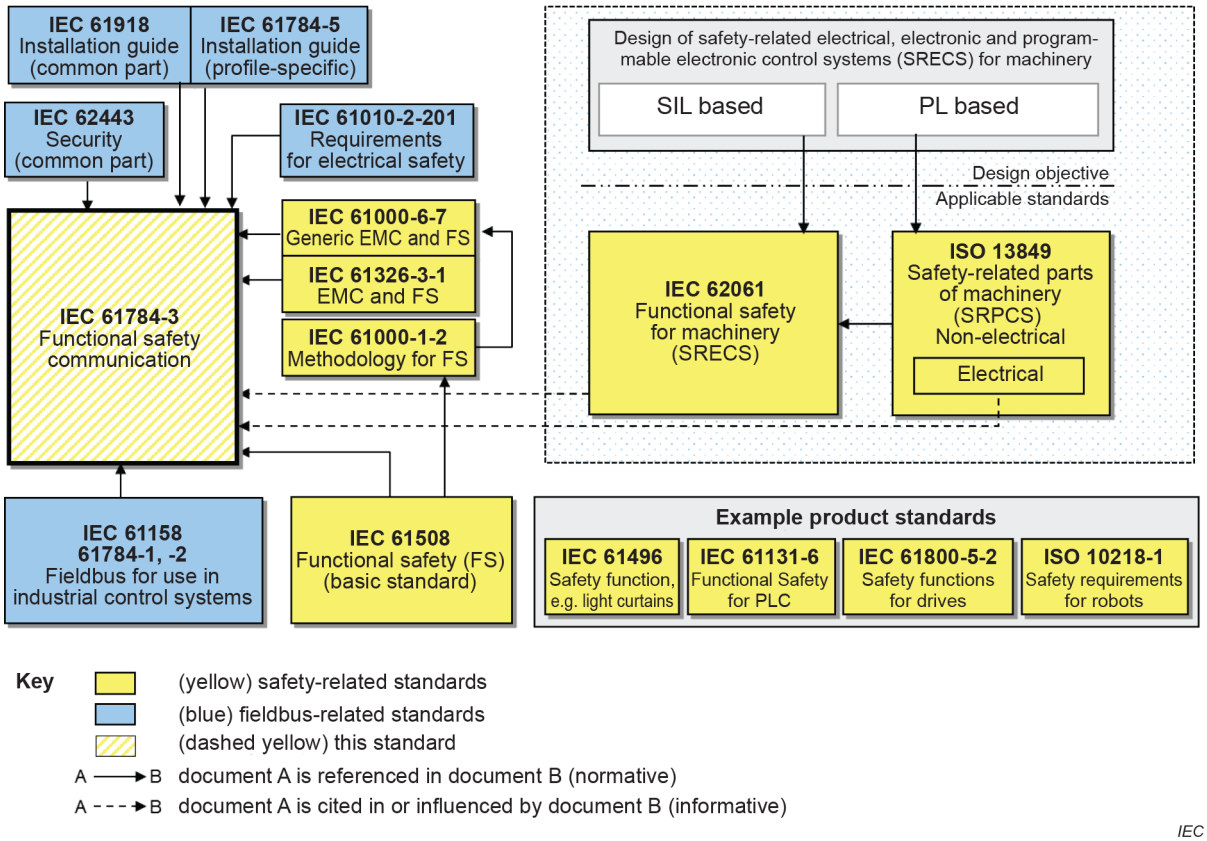
0 Introduction

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.

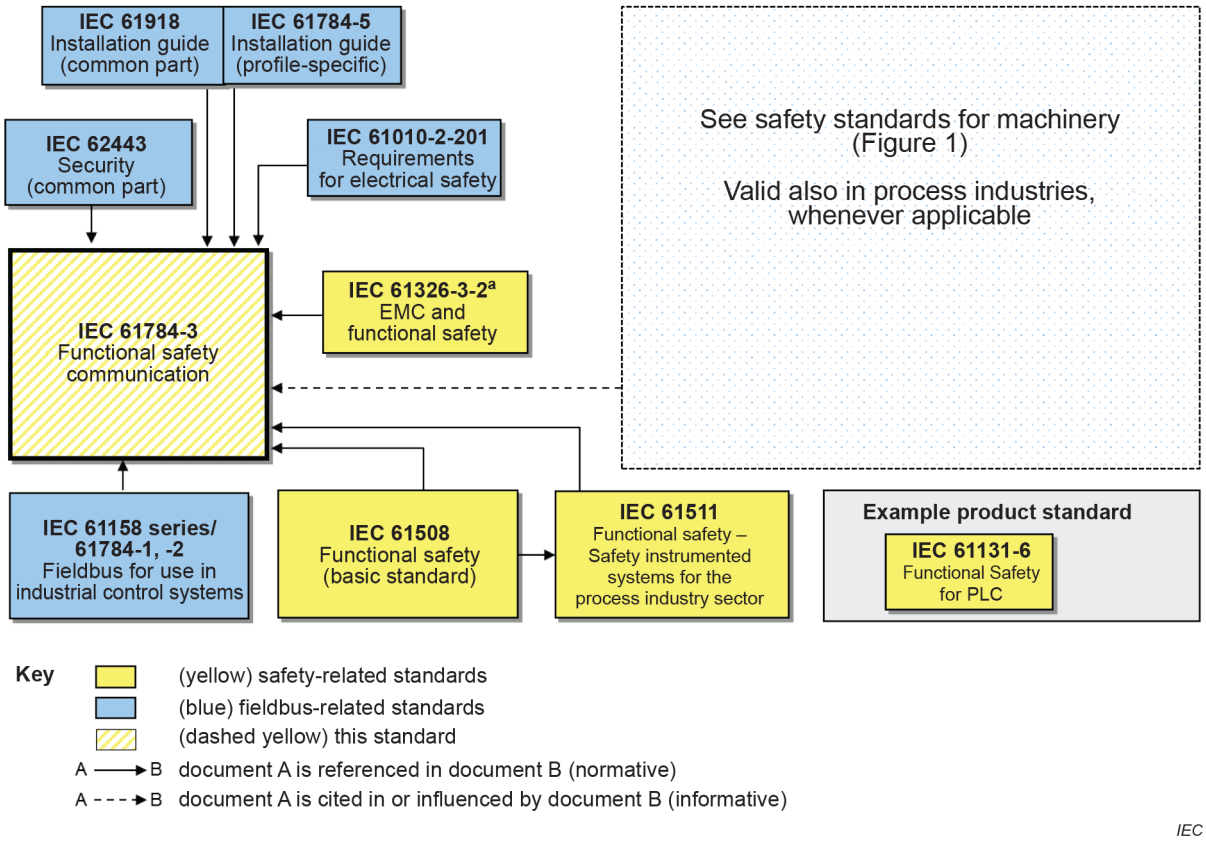
Figure 1 shows the relationships between IEC 61784-3 (all parts) and relevant safety and fieldbus standards in a machinery environment.



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 patents concerning the functional safety communication profiles for family 3. IEC takes no position concerning the evidence, validity, and scope of these patent rights.

The holder of these patent rights 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 these patent rights 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 3-3: Functional safety fieldbuses – Additional specifications for CPF 3

1 Scope

This part of IEC 61784-3 (all parts) specifies a safety communication layer (services and protocol) based on CPF 3 of IEC 61784-1, IEC 61784-2 (CP 3/1, CP 3/2, CP 3/4, CP 3/5 and CP 3/6) and IEC 61158 Types 3 and 10. 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 60204-1, *Safety of machinery – Electrical equipment of machines – Part 1: General requirements*

IEC 61000-6-7, *Electromagnetic compatibility (EMC) – Part 6-7: Generic standards – Immunity requirements for equipment intended to perform functions in a safety-related system (functional safety) in industrial locations*

IEC 61010-2-201:2017, *Safety requirements for electrical equipment for measurement, control and laboratory use – Part 2-201: Particular requirements for control equipment*

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

---

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

IEC 61158-5-3, *Industrial communication networks – Fieldbus specifications – Part 5-3: Application layer service definition –Type 3 elements*

IEC 61158-5-10, *Industrial communication networks – Fieldbus specifications – Part 5-10: Application layer service definition – Type 10 elements*

IEC 61158-6-3, *Industrial communication networks – Fieldbus specifications – Part 6-3: Application layer protocol specification – Type 3 elements*

IEC 61158-6-10, *Industrial communication networks – Fieldbus specifications – Part 6-10: Application layer protocol specification – Type 10 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 61508-2, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for 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 61784-5-3, *Industrial communication networks – Profiles – Part 5-3: Installation of fieldbuses – Installation profiles for CPF 3*

IEC 61918:2018, *Industrial communication networks – Installation of communication networks in industrial premises*

IEC 62061, *Safety of machinery – Functional safety of safety-related control systems*

IEC 62280:2014, *Railway applications – Communication, signalling and processing systems – Safety related communication in transmission systems*

IEC 62443 (all parts), *Industrial communication networks – Network and system security*

ISO 13849-1:2015, *Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design*

ISO 13849-2:2012, *Safety of machinery – Safety-related parts of control systems – Part 2: Validation*

SOMMAIRE

AVANT-PROPOS 155
0 Introduction 157
0.1 Généralités 157
0.2 Déclaration de brevets 159
1 Domaine d'application 160
2 Références normatives 160
3 Termes, définitions, symboles, abréviations et conventions 162
3.1 Termes et définitions 162
3.1.1 Termes et définitions communs 162
3.1.2 CPF 3: Termes et définitions supplémentaires 169
3.2 Symboles et abréviations 174
3.2.1 Symboles et abréviations communs 174
3.2.2 CPF 3: Symboles et abréviations supplémentaires 175
3.3 Conventions 176
4 Présentation générale de FSCP 3/1 (PROFIsafe™) 176
5 Généralités 179
5.1 Documents externes de spécifications applicables au profil 179
5.2 Exigences fonctionnelles de sécurité 179
5.3 Mesures de sécurité 180
5.4 Structure de la couche de communication de sécurité 181
5.4.1 Principe des communications de sécurité FSCP 3/1 181
5.4.2 Structures de communication CPF 3 182
5.5 Relations avec la FAL (et DLL, PhL) 184
5.5.1 Modèle d'appareil 184
5.5.2 Relations d'application et de communication 185
5.5.3 Types de données 185
6 Services de la couche de communication de sécurité 186
6.1 Services du pilote de l'hôte F 186
6.2 Services du pilote de l'appareil F 190
6.3 Diagnostic 192
6.3.1 Génération d'alarme de sécurité 192
6.3.2 Diagnostic de la couche de sécurité du (Sous-)Module F 192
7 Protocole de couche de communication de sécurité 194
7.1 Format PDU de sécurité 194
7.1.1 Structure PDU de sécurité 194
7.1.2 Données d'entrée-sortie de sécurité 195
7.1.3 Octet d'état et de contrôle 195
7.1.4 MonitoringNumber (virtuel) 197
7.1.5 Mécanisme du MNR (virtuel) (F_CRC_Seed=0) 198
7.1.6 Mécanisme du MNR (virtuel) (F_CRC_Seed=1) 198
7.1.7 Signature CRC2 (F_CRC_Seed=0) 200
7.1.8 Signature CRC2 (F_CRC_Seed=1) 201
7.1.9 Données d'entrée-sortie autres que de sécurité 202
7.2 Comportement FSCP 3/1 202
7.2.1 Généralités 202

7.2.2 Diagramme d'états du pilote de l'hôte F 203
7.2.3 Diagramme d'états du pilote de l'appareil F 208
7.2.4 Redémarrage du pilote de l'appareil F 211
7.2.5 Diagrammes séquentiels 212
7.2.6 Chronogramme de réinitialisation d'un MonitoringNumber 218
7.2.7 Surveillance des temps de sécurité 219
7.3 Réaction en cas de dysfonctionnement 221
7.3.1 Corruption des données de sécurité 221
7.3.2 Répétition non prévue 222
7.3.3 Séquence incorrecte 222
7.3.4 Perte 222
7.3.5 Retard inacceptable 222
7.3.6 Insertion 222
7.3.7 Déguisement 222
7.3.8 Adressage 223
7.3.9 Hors séquence 223
7.3.10 Bouclage 223
7.3.11 Limites du réseau et routeur 224
7.4 Démarrage F et modification des paramètres lors de l'exécution 224
7.4.1 Procédure de démarrage normalisée 224
8 Gestion de la couche de communication de sécurité 225
8.1 Paramètre F 225
8.1.1 Récapitulatif 225
8.1.2 F_Source/Destination_Address (Nom de code) 226
8.1.3 F_WD_Time (temps de fonctionnement du chien de garde F) 226
8.1.4 F_WD_Time_2 (temps de fonctionnement du chien de garde F secondaire) 226
8.1.5 F_Prm_Flag1 (Paramètres de gestion de la couche de sécurité) 227
8.1.6 F_Prm_Flag2 (Paramètres de gestion de la couche de sécurité) 229
8.1.7 F_iPar_CRC (valeur d'iPar_CRC dans les iParamètres) 230
8.1.8 Calcul de F_Par_CRC (dans les paramètres F) 231
8.1.9 Structure de l'objet de données d'enregistrement du paramètre F 231
8.2 iParamètre et iPar_CRC 232
8.3 Paramétrage de sécurité 233
8.3.1 Objectifs 233
8.3.2 Extensions de sécurité GSDL et GSDML 234
8.3.3 Protection des paramètres de sécurité et des données GSD 236
8.4 Configuration de la sécurité 240
8.4.1 Ordre des types de données d'entrée-sortie 240
8.4.2 Protection de la description des données d'entrée-sortie de sécurité 241
8.4.3 Exemples de sections de type de données DataItem 242
8.5 Utilisation des informations de type de données 246
8.5.1 Pilote de canal de l'hôte F 246
8.5.2 Règles pour les pilotes de canal de l'hôte F normalisés 247
8.5.3 Recommandations relatives à l'utilisation des pilotes de canal de l'hôte F 248
8.6 Mécanismes d'attribution de paramètres de sécurité 250
8.6.1 Attribution du paramètre F 250
8.6.2 Attribution générale d'iParamètres 250

8.6.3 Exigences d'intégration système des outils d'iParamétrage 250
8.6.4 Serveur d'iParamètres 252
9 Exigences système 263
9.1 Voyants et commutateurs 263
9.2 Lignes directrices d'installation 264
9.3 Temps de réponse de la fonction de sécurité 264
9.3.1 Modèle 264
9.3.2 Calcul et optimisation 266
9.3.3 Ajustement des temps de fonctionnement du chien de garde pour FSCP 3/1 268
9.3.4 Prise en charge de l'outil de développement 269
9.3.5 Relances (répétition des messages) 269
9.4 Durée des sollicitations 270
9.5 Contraintes liées au calcul des caractéristiques des systèmes 270
9.5.1 Considérations probabilistes 270
9.5.2 Hypothèses relatives à la sécurité 273
9.5.3 Contraintes non relatives à la sécurité (disponibilité) 273
9.6 Maintenance 273
9.6.1 Mise en service/remplacement du (Sous-)Module F 273
9.6.2 Fonctions d'identification et de maintenance 274
9.7 Manuel de sécurité 274
9.8 Canaux de transmission sans fil 276
9.8.1 Approche du canal noir 276
9.8.2 Disponibilité 276
9.8.3 Mesures de sécurité 276
9.8.4 Applications fixes et mobiles 276
9.9 Relation entre sécurité fonctionnelle et sûreté 276
9.10 Classes de conformité 276
10 Evaluation 278
10.1 Politique de sécurité 278
10.2 Obligations 279
Annexe A (informative) Informations supplémentaires pour les profils de communication de sécurité fonctionnelle de la CPF 3 280
A.1 Calcul de la fonction de hachage 280
A.2 Exemples de valeurs pour les MonitoringNumbers (MNR) 284
Annexe B (informative) Informations pour l'évaluation des profils de communication de sécurité fonctionnelle de la CPF 3 285
Annexe C (normative) Fonctions facultatives 286
C.1 Réaction à Device_Fault dans l'hôte F 286
C.1.1 Situation 286
C.1.2 Documentation destinée à l'utilisateur 286
C.1.3 Extensions facultatives du tableau de transitions du pilote de l'hôte F 286
C.1.4 Recommandation concernant le cas sans extensions des transitions de pilote de l'hôte F 289
C.2 Extensions facultatives du pilote de l'hôte F pour "Désactiver le (Sous-)Module F" 290
C.3 Combinaison de "Désactiver le (Sous-)Module F" et de "réaction à Device_Fault" 293
C.4 FSCP 3/1 et PROFIenergy 295
C.4.1 Utilisation d'appareils FSCP 3/1 avec PROFIenergy 295

C.4.2 Séquence en cas d'activation de la mise hors tension par PROFIenergy 295
C.5 Exigence "Plusieurs hôtes F communiquent avec un (Sous-)Module F unique" 296
C.6 PiR FSCP 3/1 296
Bibliographie 297

Figure 1 – Relations entre l'IEC 61784-3 et d'autres normes (machines) 157
Figure 2 – Relations entre l'IEC 61784-3 et d'autres normes (processus) 158
Figure 3 – Conditions préalables de communication de base pour le protocole FSCP 3/1 177
Figure 4 – Structure d'un PDU de sécurité FSCP 3/1 178
Figure 5 – Communication de sécurité avec CPF 3 178
Figure 6 – Système de transmission CPF 3 normalisé 181
Figure 7 – Architecture de la couche de sécurité 182
Figure 8 – Couches de communication de base 182
Figure 9 – Croisement des limites du réseau avec les routeurs 183
Figure 10 – Voies de transmission de sécurité complètes 184
Figure 11 – Modèle d'appareil entrée-sortie 185
Figure 12 – Structure de communication FSCP 3/1 186
Figure 13 – Interface d'application F des instances du pilote de l'hôte F 187
Figure 14 – Motivation pour l'option "Passivation relative aux canaux" 188
Figure 15 – Interfaces du pilote de l'appareil F 191
Figure 16 – PDU de sécurité pour CPF 3 194
Figure 17 – Octet d'état 195
Figure 18 – Octet de contrôle 196
Figure 19 – Fonction du bit de bascule 197
Figure 20 – Intégration du MonitoringNumber 198
Figure 21 – Génération de signature CRC2 du pilote de l'hôte F (F_CRC_Seed=0) 200
Figure 22 – Détails du calcul de la signature CRC2 (F_CRC_Seed=0) 201
Figure 23 – Calcul de signature CRC2 (F_CRC_Seed=1) 201
Figure 24 – Détails du calcul de la signature CRC2 (F_CRC_Seed=1) 202
Figure 25 – Relation de communication de la couche de sécurité 203
Figure 26 – Diagramme d'états du pilote de l'hôte F 203
Figure 27 – Diagramme d'états du pilote de l'appareil F 208
Figure 28 – Interaction du pilote de l'hôte F et du pilote de l'appareil F pendant le démarrage 212
Figure 29 – Interaction du pilote de l'hôte F et du pilote de l'appareil F pendant la mise hors tension > sous tension de l'hôte F 213
Figure 30 – Interaction du pilote de l'hôte F et du pilote de l'appareil F pendant un report de mise sous tension 214
Figure 31 – Interaction du pilote de l'hôte F et du pilote de l'appareil F pendant la mise hors tension → sous tension 215
Figure 32 – Interaction lorsque le pilote de l'hôte F reconnaît une erreur CRC 216
Figure 33 – Interaction lorsque le pilote de l'appareil F reconnaît une erreur CRC 217
Figure 34 – Impact du signal de réinitialisation du MNR 218

Figure 35 – Surveillance de la durée d'acheminement du message hôte F ↔ (Sous-)Module F 219
Figure 36 – Temps de fonctionnement étendu du chien de garde à la demande 221
Figure 37 – Effet de F_WD_Time_2 227
Figure 38 – F_Prm_Flag1 227
Figure 39 – F_Check_iPar 228
Figure 40 – F_SIL 228
Figure 41 – F_CRC_Length 228
Figure 42 – F_CRC_Seed 229
Figure 43 – F_Prm_Flag2 229
Figure 44 – F_Passivation 230
Figure 45 – F_Block_ID 230
Figure 46 – F_Par_Version 230
Figure 47 – Paramètre F 231
Figure 48 – Bloc iParamètre 233
Figure 49 – Extension du paramètre F dans la spécification GSDML 235
Figure 50 – Signature F_Par_CRC incluant iPar_CRC 236
Figure 51 – Pilote de canal de l'hôte F en tant que "colle" entre le (Sous-)Module F et le programme d'application 247
Figure 52 – Exemple de présentation d'un pilote de canal de l'hôte F 248
Figure 53 – Attribution du paramètre F pour (Sous-)Modules F 250
Figure 54 – Intégration système des outils CPD 252
Figure 55 –Mécanisme de serveur d'iParamètres (mise en service) 253
Figure 56 – Mécanisme du serveur d'iParamètres (remplacement du (Sous-)Module F, par exemple) 254
Figure 57 – Codage de la demande de serveur d'iParamètres ("modèle d'état") 255
Figure 58 – Codage de SR_Type 257
Figure 59 – Codage de la demande de serveur d'iParamètres ("modèle d'alarme") 257
Figure 60 – Diagramme d'états du serveur d'iParamètres 260
Figure 61 – Exemple de fonction de sécurité avec chemin de temps de réponse critique 264
Figure 62 – Modèle simplifié de temps de réponse classique 265
Figure 63 – Distributions de fréquence des temps de réponse classiques du modèle 266
Figure 64 – Contexte de délais et de temps de fonctionnement du chien de garde 267
Figure 65 – Sections de temporisation formant le F_WD_Time de FSCP 3/1 268
Figure 66 – Distribution de fréquence des temps de réponse avec relances de message 270
Figure 67 – Probabilités d'erreurs résiduelles du polynôme CRC 24 bits 271
Figure 68 – Probabilités d'erreurs résiduelles du polynôme CRC 32 bits 271
Figure 69 – Surveillance des messages corrompus 272
Figure A.1 – Procédure "C" classique de contrôle de redondance cyclique 280
Figure C.1 – Interface d'application du pilote de l'hôte F avec la fonction Réaction à Device_Fault 286
Figure C.2 – Interface d'application du pilote de l'hôte F avec la fonction Désactiver le (Sous-)Module F 290
Figure C.3 – Diagramme de temporisation pour utiliser Désactiver le (Sous-)Module F 291

Tableau 1 – Mesures déployées pour maîtriser les erreurs 180
Tableau 2 – Types de données pour FSCP 3/1 185
Tableau 3 – F_MessageTrailer pour FSCP 3/1 185
Tableau 4 – Messages de diagnostic de la couche de sécurité 193
Tableau 5 – Entrée de mémoire tampon sur erreur CRC2 194
Tableau 6 – MonitoringNumber du SPDU d'un pilote de l'hôte F 198
Tableau 7 – MonitoringNumber du SPDU d'un pilote de l'appareil F 198
Tableau 8 – MonitoringNumber du SPDU d'un pilote de l'hôte F 199
Tableau 9 – MonitoringNumber du SPDU d'un pilote de l'appareil F 199
Tableau 10 – Définition des termes utilisés dans le diagramme d'états du pilote de l'hôte F 204
Tableau 11 – Etats et transitions du pilote de l'hôte F 205
Tableau 12 – Définition des termes utilisés dans la Figure 27 208
Tableau 13 – Etats et transitions du pilote de l'appareil F 209
Tableau 14 – Temps de l'appareil de surveillance SIL 220
Tableau 15 – Limites du réseau de sécurité 224
Tableau 16 – Ordre des octets de nom de code 226
Tableau 17 – Combinaisons admises de F_CRC_Seed et de F_Passivation 229
Tableau 18 – Mots clés GSDL des paramètres F et des structures d'entrée-sortie F 234
Tableau 19 – Algorithme de génération de CRC0 237
Tableau 20 – Exemple de GSD dans la notation GSDL 238
Tableau 21 – Exemple de GSD dans la notation GSDML 239
Tableau 22 – Flux d'octets sérialisé pour les exemples 240
Tableau 23 – Ordre des types de données d'entrée-sortie 241
Tableau 24 – Eléments de structure de données d'entrée-sortie 242
Tableau 25 – Section DataItem de F_IN_OUT_1 243
Tableau 26 – DATA_STRUCTURE_CRC de F_IN_OUT_1 243
Tableau 27 – Section DataItem de F_IN_OUT_2 244
Tableau 28 – DATA_STRUCTURE_CRC de F_IN_OUT_2 244
Tableau 29 – Section DataItem de F_IN_OUT_5 245
Tableau 30 – DATA_STRUCTURE_CRC de F_IN_OUT_5 245
Tableau 31 – Section DataItem de F_IN_OUT_6 246
Tableau 32 – DATA_STRUCTURE_CRC de F_IN_OUT_6 246
Tableau 33 – Modèles de pilotes de canal de l'hôte F 248
Tableau 34 – Exigences pour l'iParamétrage 251
Tableau 35 – Spécificateur de la demande de serveur d'iParamètres 256
Tableau 36 – Structure de Read_RES_PDU ("read record") 258
Tableau 37 – Structure de Write_REQ_PDU ("write record") 258
Tableau 38 – Structure de Pull_RES_PDU ("Pull") 259
Tableau 39 – Structure de Push_REQ_PDU ("Push") 259
Tableau 40 – Etats et transitions du serveur d'iParamètres 261
Tableau 41 – Mesures de gestion du serveur d'iParamètres 262

Tableau 42 – Définition des termes utilisés dans la Figure 69 272
Tableau 43 – Informations à inclure dans le manuel de sécurité 274
Tableau 44 – Exigences de classe de conformité de l'hôte F 277
Tableau 45 – Principales caractéristiques des versions de protocole 278
Tableau 46 – Matrice de conformité du pilote de l'hôte F/du pilote de l'appareil F 278
Tableau A.1 – Tableau "Crctab24" de calculs de la signature CRC 24 bits 281
Tableau A.2 – Tableau "Crctab32" de calculs de la signature CRC 32 bits 282
Tableau A.3 – Tableau "Crctab16" de calculs de la signature CRC 16 bits 283
Tableau A.4 – Valeurs de CN_incrNR_64 et de MNR pour le PDU de l'hôte F 284
Tableau C.1 – Définition de termes supplémentaires utilisés dans les transitions de pilote 287
Tableau C.2 – Transitions de pilote de l'hôte F – ajoutées avec la réaction à Device_Fault 287
Tableau C.3 – Empêcher un redémarrage involontaire par des mesures d'application 289
Tableau C.4 – Transitions du pilote de l'hôte F – avec la fonction Désactiver le (Sous-)Module F 291
Tableau C.5 – Transitions du pilote de l'hôte F – ajoutées avec "réaction à Device_Fault" et "Désactiver le (Sous-)Module F" 293

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

RÉSEAUX DE COMMUNICATION INDUSTRIELS – PROFILS –

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

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 de la présente Publication 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 61784-3-3 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 quatrième édition annule et remplace la troisième édition parue en 2016. Cette édition constitue une révision technique.

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

- modifications rédactionnelles concernant l'opportunité, transformation des commentaires dans le diagramme en instructions;

- utilisation des abréviations de PROFINET;
- informations supplémentaires concernant les contrôles et le manuel de sécurité pour les types d'adresses PROFIsafe 1 et 2;
- informations supplémentaires concernant PFDavg, prise en charge de l'essai automatique, ajout de messages de diagnostic;
- explication et spécification de diagrammes d'états facultatifs concernant la réaction en cas d'anomalie de l'appareil;
- nouvelle variable facultative "OAD_Nec_C" pour la fonction facultative "Réaction à Device_Fault dans F_Host";
- spécification de la fonction facultative de l'hôte F pour "Désactiver le (Sous-)Module F";
- spécification des exigences concernant FSCP 3/1 et PROFIenergy;
- spécification des exigences concernant la communication de plusieurs hôtes F avec un (Sous-)Module F unique; mise à jour du manuel de sécurité;
- corrections d'erreurs diverses, de fautes de frappe, et mises à jour des références;
- mise à jour de la bibliographie.

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 "http://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.

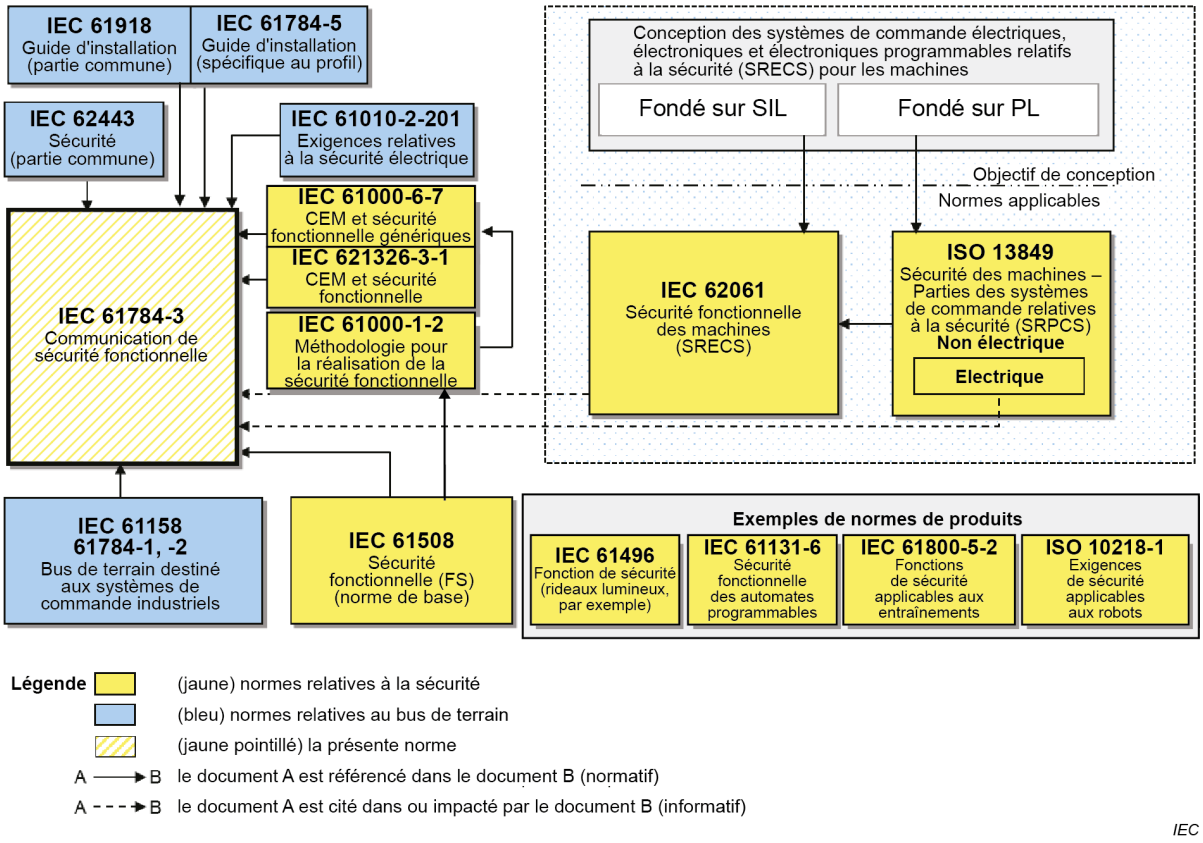
0 Introduction

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.

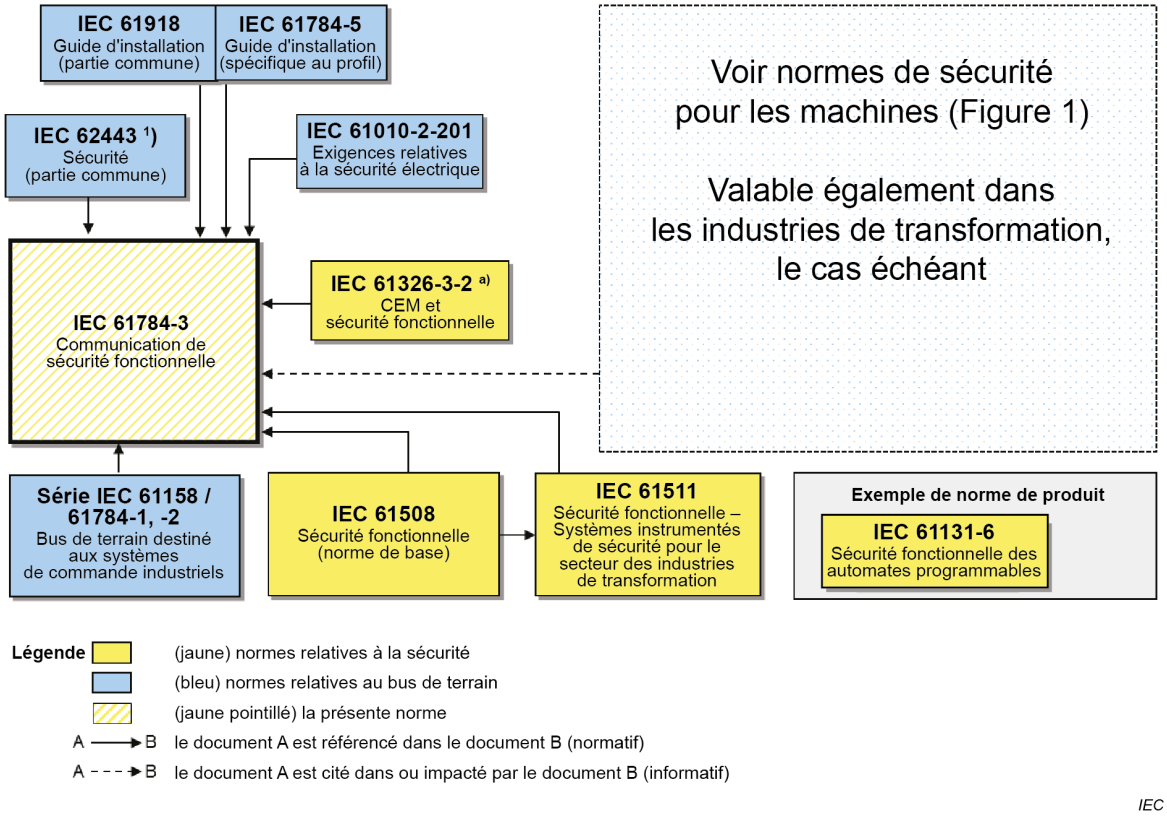
La Figure 1 représente les relations entre l'IEC 61784-3 (toutes les parties) et les normes pertinentes relatives à la sécurité et aux bus de terrain dans un environnement de machines.



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 (processus)

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

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 3 de l'IEC 61784-1 et les Types 3 et 10 de l'IEC 61784-2 (CP 3/1, CP 3/2, CP 3/4, CP 3/5 et CP 3/6) et de l'IEC 61158. 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 60204-1, *Sécurité des machines – Equipement électrique des machines – Partie 1: Exigences générales*

IEC 61000-6-7, *Compatibilité électromagnétique (CEM) – Partie 6-7: Normes génériques – Exigences d'immunité pour les équipements visant à exercer des fonctions dans un système lié à la sécurité (sécurité fonctionnelle) dans des sites industriels*

IEC 61010-2-201:2017, *Règles de sécurité pour appareils électriques de mesurage, de régulation et de laboratoire – Partie 2-201: Exigences particulières relatives aux équipements de commande*

---

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

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

IEC 61158-5-3, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 5-3: Définition des services de la couche application – Eléments de type 3*

IEC 61158-5-10, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 5-10: Définition des services de la couche application – Eléments de type 10*

IEC 61158-6-3, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 6-3: Spécification du protocole de couche application – Eléments de type 3*

IEC 61158-6-10, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 6-10: Spécification du protocole de couche application – Eléments de type 10*

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 61508-2, *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 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 basés 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 61784-5-3, *Réseaux de communication industriels – Profils – Partie 5-3: Installation des bus de terrain – Profils d'installation pour CPF 3*

IEC 61918:2018, *Réseaux de communication industriels – Installation de réseaux de communication dans des locaux industriels*

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

IEC 62280:2014, *Applications ferroviaires – Systèmes de signalisation, de télécommunication et de traitement – Communication de sécurité dans les systèmes de transmission*

IEC 62443 (toutes les parties), *Réseaux industriels de communication – Sécurité dans les réseaux et les systèmes*

ISO 13849-1:2015, *Sécurité des machines - Parties des systèmes de commande relatives à la sécurité - Partie 1: Principes généraux de conception*

ISO 13849-2:2012, *Sécurité des machines - Parties des systèmes de commande relatives à la sécurité - Partie 2: Validation*