IEC 61784-3

Edition 3.0 2016-05

REDLINE VERSION

colour inside

Industrial communication networks – Profiles –
Part 3: Functional safety fieldbuses – General rules and profile definitions

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 25.040.40; 35.100.05

ISBN 978-2-8322-3372-6

Warning! Make sure that you obtained this publication from an authorized distributor.

® Registered trademark of the International Electrotechnical Commission

CONTENTS

FOREWORD 8
0 Introduction 10
0.1 General 10
0.2 Transition from Edition 2 to extended assessment methods in Edition 3 12
0.3 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 .....
3.1.2 CPF 1: Additional terms and definitions .....
3.1.3 CPF 2: Additional terms and definitions .....
3.1.4 CPF 3: Additional terms and definitions .....
3.1.5 CPF 6: Additional terms and definitions .....
3.1.6 CPF 8: Additional terms and definitions .....
3.1.7 CPF 12: Additional terms and definitions .....
3.1.8 CPF 13: Additional terms and definitions .....
3.1.9 CPF 14: Additional terms and definitions .....
3.2 Symbols and abbreviated terms 24
3.2.1 Common symbols and abbreviated terms .....
3.2.2 CPF 1: Additional symbols and abbreviated terms .....
3.2.3 CPF 2: Additional symbols and abbreviated terms .....
3.2.4 CPF 3: Additional symbols and abbreviated terms .....
3.2.5 CPF 6: Additional symbols and abbreviated terms .....
3.2.6 CPF 8: Additional symbols and abbreviated terms .....
3.2.7 CPF 12: Additional symbols and abbreviated terms .....
3.2.8 CPF 13: Additional symbols and abbreviated terms .....
3.2.9 CPF 14: Additional symbols and abbreviated terms .....
4 Conformance 26
5 Basics of safety-related fieldbus systems 26
5.1 Safety function decomposition 26
5.2 Communication system 27
5.2.1 General 27
5.2.2 IEC 61158 fieldbuses 27
5.2.3 Communication channel types 28
5.2.4 Safety function response time 28
5.3 Communication errors 29
5.3.1 General 29
5.3.2 Corruption 29
5.3.3 Unintended repetition 29
5.3.4 Incorrect sequence 30
5.3.5 Loss 30
5.3.6 Unacceptable delay 30
5.3.7 Insertion 30
5.3.8 Masquerade 30
5.3.9 Addressing 30

5.4 Deterministic remedial measures 31
5.4.1 General 31
5.4.2 Sequence number 31
5.4.3 Time stamp 31
5.4.4 Time expectation 31
5.4.5 Connection authentication 31
5.4.6 Feedback message 31
5.4.7 Data integrity assurance 32
5.4.8 Redundancy with cross checking 32
5.4.9 Different data integrity assurance systems 32
5.5 Typical relationships between errors and safety measures 32
5.6 Communication phases 33
5.7 FSCP implementation aspects 34
5.8 Data integrity considerations 34
5.8.1 Calculation of the residual error rate 34
5.8.2 Total residual error rate and SIL 37
5.9 Relationship between functional safety and security 38
5.10 Boundary conditions and constraints 39
5.10.1 Electrical safety 39
5.10.2 Electromagnetic compatibility (EMC) 39
5.11 Installation guidelines 40
5.12 Safety manual 40
5.13 Safety policy 40
6 Communication Profile Family 1 (FOUNDATION™ Fieldbus) – Profiles for functional safety 41
~~6.1 Functional Safety Communication Profile 1/1 .....~~
~~6.2 Technical overview .....~~
7 Communication Profile Family 2 (CIP™) and Family 16 (SERCOS®)– Profiles for functional safety 42
~~7.1 Functional Safety Communication Profile 2/1 .....~~
~~7.2 Technical overview .....~~
8 Communication Profile Family 3 (PROFIBUS™, PROFINET™) – Profiles for functional safety 44
~~8.1 Functional Safety Communication Profile 3/1 .....~~
~~8.2 Technical overview .....~~
9 Communication Profile Family 6 (INTERBUS®) – Profiles for functional safety 46
~~9.1 Functional Safety Communication Profile 6/7 .....~~
~~9.2 Technical overview .....~~
10 Communication Profile Family 8 (CC-Link™) – Profiles for functional safety 48
10.1 Functional Safety Communication Profile 8/1 48
10.2 ~~Technical overview~~ Functional Safety Communication Profile 8/2 48
11 Communication Profile Family 12 (EtherCAT™) – Profiles for functional safety 49
~~11.1 Functional Safety Communication Profile 12/1 .....~~
~~11.2 Technical overview .....~~
12 Communication Profile Family 13 (Ethernet POWERLINK™) – Profiles for functional safety 50
~~12.1 Functional Safety Communication Profile 13/1 .....~~
~~12.2 Technical overview .....~~

13 Communication Profile Family 14 (EPA®) – Profiles for functional safety 52
~~13.1 Functional Safety Communication Profile 14/1 .....~~
~~13.2 Technical overview.....~~
14 Communication Profile Family 17 (RAPIEnet™) – Profiles for functional safety 53
15 Communication Profile Family 18 (SafetyNET p™ Fieldbus) – Profiles for functional safety 53
Annex A (informative) Example functional safety communication models..... 54
A.1 General..... 54
A.2 Model A (single message, channel and FAL, redundant SCLs) 54
A.3 Model B (full redundancy)..... 54
A.4 Model C (redundant messages, FALs and SCLs, single channel)..... 55
A.5 Model D (redundant messages and SCLs, single channel and FAL)..... 55
Annex B (~~informative~~ normative) Safety communication channel model using CRC-based error checking 57
B.1 Overview..... 57
B.2 Channel model for calculations 57
B.3 Bit error probability Pe..... 58
B.4 Cyclic redundancy checking 59
B.4.1 General 59
B.4.2 Considerations concerning CRC polynomials 60
Annex C (informative) Structure of technology-specific parts..... 62
Annex D (informative) Assessment guideline 64
D.1 Overview..... 64
D.2 Channel types..... 64
D.2.1 General 64
D.2.2 Black channel 64
D.2.3 White channel..... 64
D.3 Data integrity considerations for white channel approaches..... 65
D.3.1 General 65
D.3.2 Models B and C 65
D.3.3 Models A and D 66
D.4 Verification of safety measures..... 67
D.4.1 General 67
D.4.2 Implementation 67
D.4.3 "De-energize to trip" principle..... 67
D.4.4 Safe state 67
D.4.5 Transmission errors 67
D.4.6 Safety reaction and response times..... 67
D.4.7 Combination of measures..... 68
D.4.8 Absence of interference 68
D.4.9 Additional fault causes (white channel)..... 68
D.4.10 Reference test beds and operational conditions..... 68
D.4.11 Conformance tester..... 69
Annex E (informative) Examples of implicit vs. explicit FSCP safety measures 70
E.1 General..... 70
E.2 Example fieldbus message with safety PDUs 70
E.3 Model with completely explicit safety measures 70
E.4 Model with explicit A-code and implicit T-code safety measures 71

E.5 Model with explicit T-code and implicit A-code safety measures 71
E.6 Model with split explicit and implicit safety measures 72
E.7 Model with completely implicit safety measures 73
E.8 Addition to Annex B – impact of implicit codes on properness 73
Annex F (informative) Extended models for estimation of the total residual error rate 74
F.1 Applicability 74
F.2 General models for black channel communications 74
F.3 Identification of generic safety properties 75
F.4 Assumptions for residual error rate calculations 75
F.5 Residual error rates 76
F.5.1 Explicit and implicit mechanisms 76
F.5.2 Residual error rate calculations 76
F.6 Data integrity 78
F.6.1 Probabilistic considerations 78
F.6.2 Deterministic considerations 78
F.7 Authenticity 79
F.7.1 General 79
F.7.2 Residual error rate for authenticity (RR_A) 80
F.8 Timeliness 81
F.8.1 General 81
F.8.2 Residual error rate for timeliness (RR_T) 83
F.9 Masquerade 84
F.9.1 General 84
F.9.2 Other terms used to calculate residual error rate for masquerade rejection (RR_M) 84
F.10 Calculation of the total residual error rates 84
F.10.1 Based on the summation of the residual error rates 84
F.10.2 Based on other quantitative proofs 85
F.11 Total residual error rate and SIL 85
F.12 Configuration and parameterization for an FSCP 86
F.12.1 General 86
F.12.2 Configuration and parameterization change rate 88
F.12.3 Residual error rate for configuration and parameterization 88
Bibliography 89

Figure 1 – Relationships of IEC 61784-3 with other standards (machinery) 10
Figure 2 – Relationships of IEC 61784-3 with other standards (process) 11
Figure 3 – Transition from Edition 2 to Edition 3 assessment methods 12
Figure 4 – Safety communication as a part of a safety function 27
Figure 5 – Example model of a functional safety communication system 28
Figure 6 – Example of safety function response time components 29
~~Figure 7 – Scope of FSCP 1/1 .....~~
Figure 7 – Conceptual FSCP protocol model 34
~~Figure 8 – Relationship of Safety Validators .....~~
Figure 8 – FSCP implementation aspects 34
~~Figure 9 – Basic communication preconditions for FSCP 3/1 .....~~

Figure 9 – Example application 1 (m=4) 36
~~Figure 10 – Structure of a FSCP 3/1 safety PDU~~ .....
Figure 10 – Example application 2 (m = 2) 37
~~Figure 11 – Safe communication modes~~ .....
Figure 11 – Zones and conduits concept for security according to IEC 62443 39
~~Figure 12 – FSCP 6/7 communication preconditions~~ .....
~~Figure 13 – Basic FSCP 12/1 system~~ .....
~~Figure 14 – Producer consumer example~~ .....
~~Figure 15 – Client server example~~ .....
~~Figure 16 – FSCP 14/1 safety communication architecture~~ .....
Figure A.1 – Model A 54
Figure A.2 – Model B 55
Figure A.3 – Model C 55
Figure A.4 – Model D 56
Figure B.1 – Communication channel with perturbation 57
Figure B.2 – Binary symmetric channel (BSC) 58
Figure B.3 – Example of a block with a message part and a CRC ~~bits (redundancy code)~~ signature 59
Figure B.4 – Block codes for error detection 60
Figure B.5 – Proper and improper CRC polynomials 61
Figure D.1 – Basic Markov model 66
Figure E.1 – Example safety PDUs embedded in a fieldbus message 70
Figure E.2 – Model with completely explicit safety measures 70
Figure E.3 – Model with explicit A-code and implicit T-code safety measures 71
Figure E.4 – Model with explicit T-code and implicit A-code safety measures 72
Figure E.5 – Model with split explicit and implicit safety measures 72
Figure E.6 – Model with completely implicit safety measures 73
Figure F.1 – Black channel from an FSCP perspective 74
Figure F.2 – Model for authentication considerations 79
Figure F.3 – Fieldbus and internal address errors 80
Figure F.4 – Example of slowly increasing message latency 82
Figure F.5 – Example of an active network element failure 83
Figure F.6 – Example application 1 (m = 4) 85
Figure F.7 – Example application 2 (m = 2) 85
Figure F.8 – Example of configuration and parameterization procedures for FSCP 87

Table 1 – Overview of the effectiveness of the various measures on the possible errors 33
Table 2 – Definition of items used for calculation of the residual error rates 36
Table 3 – Typical relationship of residual error rate to SIL ~~level~~ 37
Table 4 – Typical relationship of residual error on demand to SIL 37
Table 5 – Overview of profile identifier usable for FSCP 6/7 47
Table B.1 – Example dependency d_{min} and block bit length n 60
Table C.1 – Common subclause structure for technology-specific parts 62

Table F.1 – Typical relationship of residual error rate to SIL 86
Table F.2 – Typical relationship of residual error on demand to SIL.....86

INTERNATIONAL ELECTROTECHNICAL COMMISSION

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES –

Part 3: Functional safety fieldbuses – General rules and profile definitions

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.

DISCLAIMER
This Redline version is not an official IEC Standard and is intended only to provide the user with an indication of what changes have been made to the previous version. Only the current version of the standard is to be considered the official document.

This Redline version provides you with a quick and easy way to compare all the changes between this standard and its previous edition. A vertical bar appears in the margin wherever a change has been made. Additions are in green text, deletions are in strikethrough red text.

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

This third edition cancels and replaces the second edition published in 2010. This edition constitutes a technical revision.

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

- clarifications and additional explanations for requirements, updated references;
- deletion of technical overviews of profiles (Clauses 6 to 13), and associated dedicated subclauses for terms, definitions, symbols and abbreviations;
- addition of profiles for Communication Profile Families 8, 17 and 18 (Clauses 10, 14, 15);
- clarifications of models in Annex A;
- Annex B changed from informative to normative;
- addition of a new informative Annex E describing models for explicit and implicit FSCP mechanisms;
- addition of a new informative Annex F introducing an extended model for estimation of the total residual error rate;
- updates in parts for CPF 1, CPF 2, CPF 3, CPF 8, CPF 13 (details provided in the parts);
- addition of a new part for CPF 17.

The text of this standard is based on the following documents:

FDIS	Report on voting
65C/840/FDIS	65C/848/RVD

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

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

A list of all parts of the IEC 61784-3 series, published under the general title *Industrial communication networks – Profiles – Functional safety fieldbuses*, can be found on the IEC website.

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC website under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

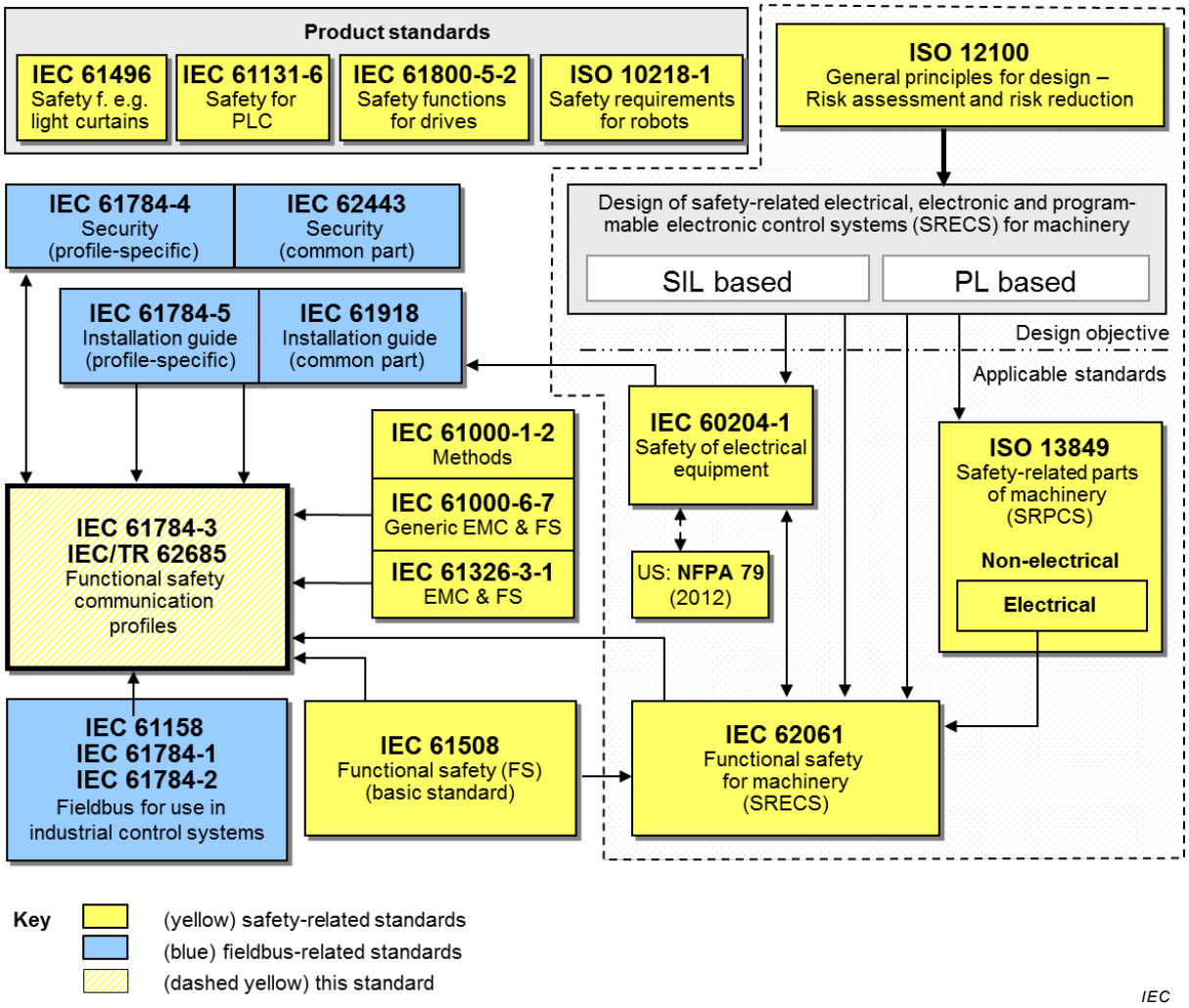
0 Introduction

0.1 General

The IEC 61158 fieldbus standard together with its companion standards IEC 61784-1 and IEC 61784-2 defines a set of communication protocols that enable distributed control of automation applications. Fieldbus technology is now considered well accepted and well proven. Thus ~~many~~ fieldbus enhancements ~~are emerging~~ continue to emerge, addressing ~~not yet standardized~~ applications for areas such as real time, safety-related and security-related applications.

This standard explains the relevant principles for functional safety communications with reference to IEC 61508 series and specifies several safety communication layers (profiles and corresponding protocols) based on the communication profiles and protocol layers of IEC 61784-1, IEC 61784-2 and the IEC 61158 series. It does not cover electrical safety and intrinsic safety aspects.

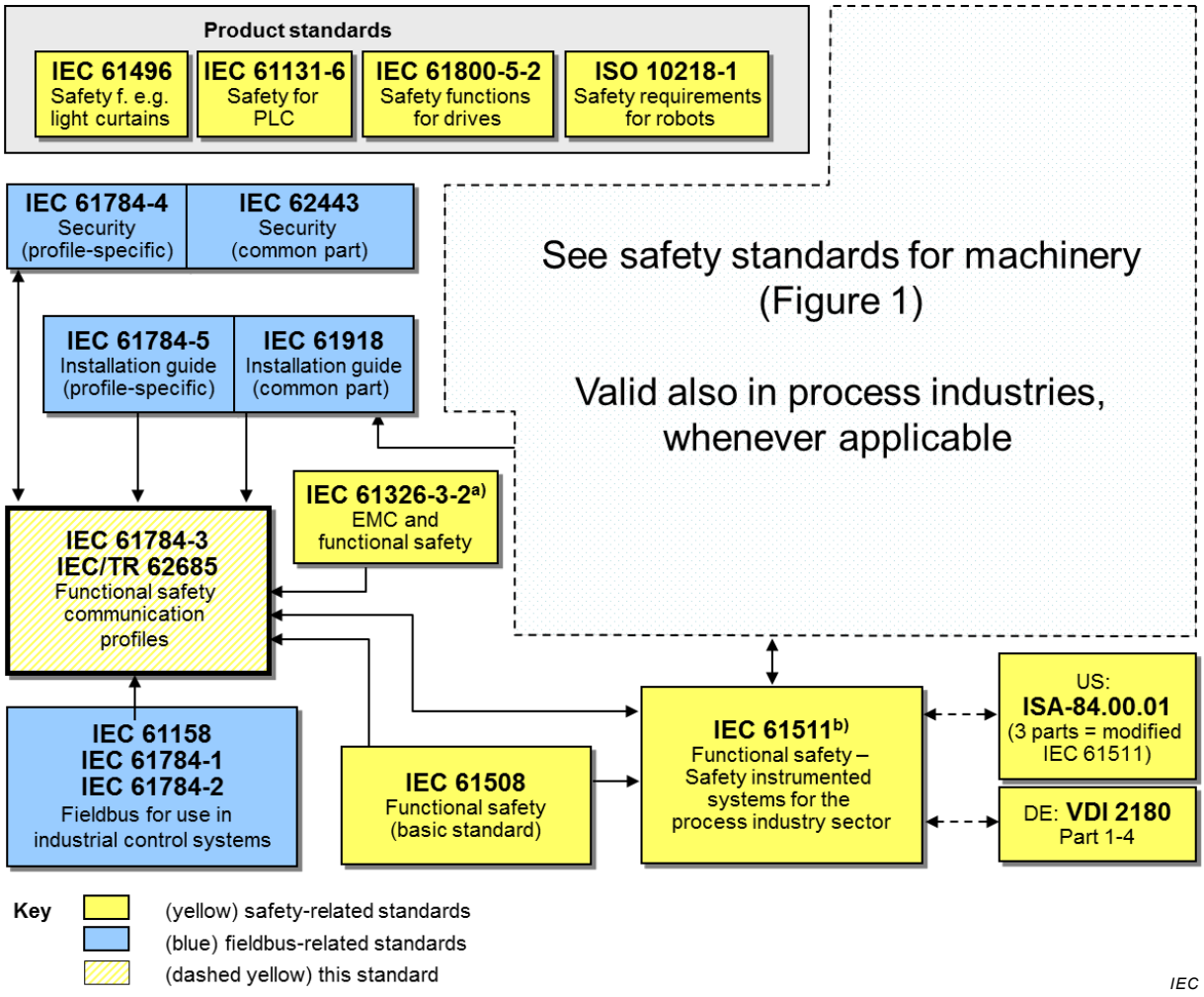
Figure 1 shows the relationships between this standard and relevant safety and fieldbus standards in a machinery environment.



NOTE Subclauses 6.7.6.4 (high complexity) and 6.7.8.1.6 (low complexity) of IEC 62061 specify the relationship between PL (Category) and SIL.

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

Figure 2 shows the relationships between this standard and relevant safety and fieldbus standards in a process environment.



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

[b] EN ratified.

Figure 2 – Relationships of IEC 61784-3 with other standards (process)

Safety communication layers which are implemented as parts of safety-related systems according to IEC 61508 series provide the necessary confidence in the transportation of messages (information) between two or more participants on a fieldbus in a safety-related system, or sufficient confidence of safe behaviour in the event of fieldbus errors or failures.

Safety communication layers specified in this standard do this in such a way that a fieldbus can be used for applications requiring functional safety up to the Safety Integrity Level (SIL) specified by its corresponding functional safety communication profile.

The resulting SIL claim of a system depends on the implementation of the selected functional safety communication profile (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.

This standard describes:

- basic principles for implementing the requirements of IEC 61508 series for safety-related data communications, including possible transmission faults, remedial measures and considerations affecting data integrity;
- ~~individual description of~~ functional safety 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 the IEC 61158 series.

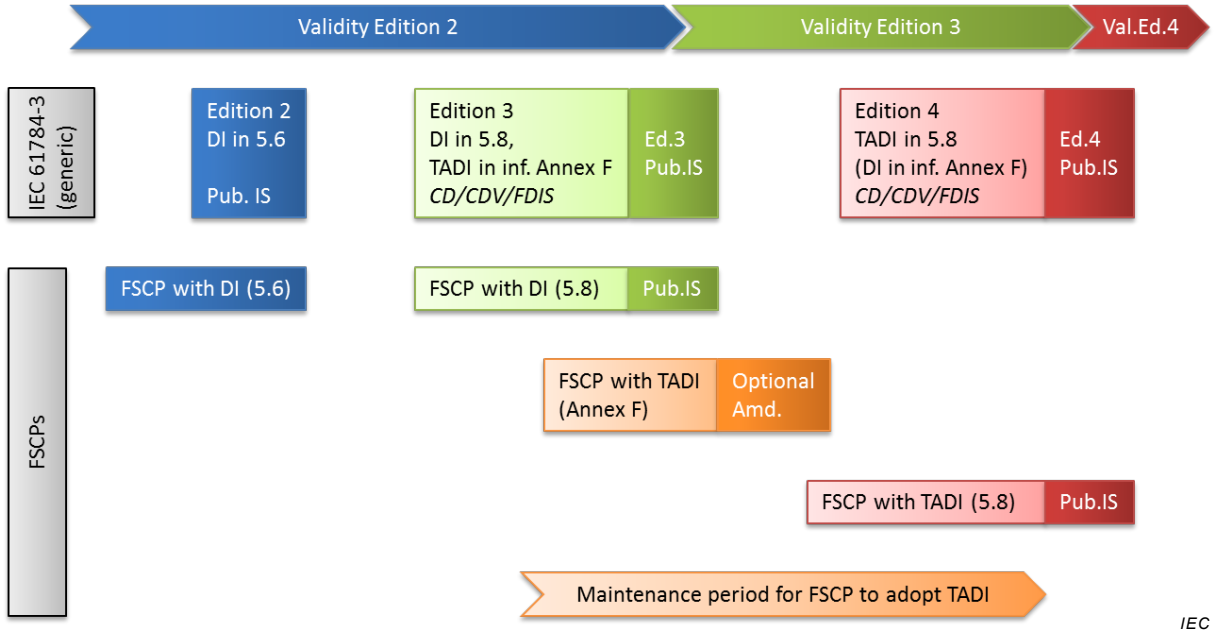
0.2 Transition from Edition 2 to extended assessment methods in Edition 3

This edition of the generic part of the standard includes additional extended models for future use when estimating the total residual error rate for an FSCP. This value can be used to determine if the FSCP meets the requirements of functional safety applications up to a given SIL. These extended models for qualitative and quantitative safety determination methods are detailed in Annex E and Annex F.

However, because of the typical duration of the assessment process, the FSCPs published prior to or concurrently with this new edition of the generic part can only be assessed using the methods from previous editions, based on data integrity considerations specified in 5.8.

The validity schema in Figure 3 shows how to handle the transition from original assessment methods of Edition 2 (specified in 5.8) to extended assessment methods in Edition 3 (currently specified in Annex F). According to this schema, the FSCPs are exempt from a new assessment according to Annex F until Edition 4, where the contents of current Annex F will replace the current 5.8.

NOTE However, a particular FSCP can achieve an earlier assessment and publish an adequate amendment.



Key

DI Data Integrity

TADI Timeliness, Authenticity, Data Integrity

Figure 3 – Transition from Edition 2 to Edition 3 assessment methods

0.3 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 functional safety communication profiles for families 1, 2, 3, 6, 8, 12, 13, 14, 17 and 18 given

in IEC 61784-3-1, IEC 61784-3-2, IEC 61784-3-3, IEC 61784-3-6, IEC 61784-3-8, IEC 61784-3-12, IEC 61784-3-13, IEC 61784-3-14, IEC 61784-3-17 and IEC 61784-3-18.

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

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

NOTE Patent details and corresponding contact information are provided in IEC 61784-3-1, IEC 61784-3-2, IEC 61784-3-3, IEC 61784-3-6, IEC 61784-3-8, IEC 61784-3-12, IEC 61784-3-13, IEC 61784-3-14, IEC 61784-3-17 and IEC 61784-3-18.

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

ISO (www.iso.org/patents) and IEC (http://patents.iec.ch) maintain on-line data bases of patents relevant to their standards. Users are encouraged to consult the data bases for the most up to date information concerning patents.

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES –

Part 3: Functional safety fieldbuses – General rules and profile definitions

1 Scope

This part of the IEC 61784-3 series explains some common principles that can be used in the transmission of safety-relevant messages among participants within a distributed network which use fieldbus technology in accordance with the requirements of IEC 61508 series[1] for functional safety. These principles are based on the black channel approach. They can be used in various industrial applications such as process control, manufacturing automation and machinery.

This part[2] and the IEC 61784-3-x parts specify several functional safety communication profiles based on the communication profiles and protocol layers of the fieldbus technologies in IEC 61784-1, IEC 61784-2 and the IEC 61158 series. These functional safety communication profiles use the black channel approach, as defined in IEC 61508. These functional safety communication profiles are intended for implementation in safety devices exclusively.

NOTE 1 Other safety-related communication systems meeting the requirements of IEC 61508 series ~~may~~ can exist that are not included in this standard.

NOTE 2 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.

All systems are exposed to unauthorized access at some point of their life cycle. Additional measures need to be considered in any safety-related application to protect fieldbus systems against unauthorized access. The IEC 62443 series will address many of these issues; the relationship with the IEC 62443 series is detailed in a dedicated subclause of this part.

NOTE 3 Additional profile specific requirements for security ~~may~~ can also be specified in IEC 61784-4[3] ~~[10]~~.

NOTE 4 Implementation of a functional safety communication profile according to this part in a device is not sufficient to qualify it as a safety device, as defined in IEC 61508 series.

NOTE 5 The resulting SIL claim of a system depends on the implementation of the selected functional safety communication profile within this system.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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*

---

1 In the following pages of this standard, “IEC 61508” will be used for “IEC 61508 series”.

2 In the following pages of this standard, “this part” will be used for “this part of the IEC 61784-3 series”.

3 Proposed new work item under consideration.

IEC 61010-2-201:2013, *Safety requirements for electrical equipment for measurement, control and laboratory use – Part 2-201: Particular requirements for control equipment*

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

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

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 61508-1:2010[4], *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements*

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

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

IEC 61784-3-1, *Industrial communication networks – Profiles – Part 3-1: Functional safety fieldbuses – Additional specifications for CPF 1*

IEC 61784-3-2, *Industrial communication networks – Profiles – Part 3-2: Functional safety fieldbuses – Additional specifications for CPF 2*

IEC 61784-3-3, *Industrial communication networks – Profiles – Part 3-3: Functional safety fieldbuses – Additional specifications for CPF 3*

IEC 61784-3-6, *Industrial communication networks – Profiles – Part 3-6: Functional safety fieldbuses – Additional specifications for CPF 6*

IEC 61784-3-8[5], *Industrial communication networks – Profiles – Part 3-8: Functional safety fieldbuses – Additional specifications for CPF 8*

IEC 61784-3-12[5], *Industrial communication networks – Profiles – Part 3-12: Functional safety fieldbuses – Additional specifications for CPF 12*

IEC 61784-3-13[5], *Industrial communication networks – Profiles – Part 3-13: Functional safety fieldbuses – Additional specifications for CPF 13*

~~4 To be published.~~

~~5 To be published.~~

IEC 61784-3-14~~5~~, *Industrial communication networks – Profiles – Part 3-14: Functional safety fieldbuses – Additional specifications for CPF 14*

IEC 61784-3-17[6], *Industrial communication networks – Profiles – Part 3-17: Functional safety fieldbuses – Additional specifications for CPF 17*

IEC 61784-3-18, *Industrial communication networks – Profiles – Part 3-18: Functional safety fieldbuses – Additional specifications for CPF 18*

IEC 61784-5 (all parts), *Industrial communication networks – Profiles – Part 5: Installation of fieldbuses ~~– Installation profiles for CPF x~~*

IEC 61918:2013, *Industrial communication networks – Installation of communication networks in industrial premises*

~~IEC 62280-1:2002, *Railway applications – Communication, signalling and processing systems – Part 1: Safety related communication in closed transmission systems*~~

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

6 To be published

IEC 61784-3

Edition 3.0 2016-05

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions

Réseaux de communication industriels – Profils – Partie 3: Bus de terrain de sécurité fonctionnelle – Règles générales et définitions de profils



IEC 61784-3:2016-05(en-fr)

CONTENTS

FOREWORD....7
0 Introduction....9
0.1 General....9
0.2 Transition from Edition 2 to extended assessment methods in Edition 3....11
0.3 Patent declaration....12
1 Scope....13
2 Normative references....13
3 Terms, definitions, symbols, abbreviated terms and conventions....15
3.1 Terms and definitions....15
3.2 Symbols and abbreviated terms....22
4 Conformance....23
5 Basics of safety-related fieldbus systems....23
5.1 Safety function decomposition....23
5.2 Communication system....24
5.2.1 General....24
5.2.2 IEC 61158 fieldbuses....24
5.2.3 Communication channel types....25
5.2.4 Safety function response time....25
5.3 Communication errors....26
5.3.1 General....26
5.3.2 Corruption....26
5.3.3 Unintended repetition....26
5.3.4 Incorrect sequence....26
5.3.5 Loss....27
5.3.6 Unacceptable delay....27
5.3.7 Insertion....27
5.3.8 Masquerade....27
5.3.9 Addressing....27
5.4 Deterministic remedial measures....27
5.4.1 General....27
5.4.2 Sequence number....27
5.4.3 Time stamp....27
5.4.4 Time expectation....28
5.4.5 Connection authentication....28
5.4.6 Feedback message....28
5.4.7 Data integrity assurance....28
5.4.8 Redundancy with cross checking....28
5.4.9 Different data integrity assurance systems....29
5.5 Typical relationships between errors and safety measures....29
5.6 Communication phases....30
5.7 FSCP implementation aspects....31
5.8 Data integrity considerations....31
5.8.1 Calculation of the residual error rate....31
5.8.2 Total residual error rate and SIL....33
5.9 Relationship between functional safety and security....34
5.10 Boundary conditions and constraints....35

5.10.1 Electrical safety 35
5.10.2 Electromagnetic compatibility (EMC) 35
5.11 Installation guidelines 36
5.12 Safety manual 36
5.13 Safety policy 36
6 Communication Profile Family 1 (FOUNDATION™ Fieldbus) – Profiles for functional safety 37
7 Communication Profile Family 2 (CIP™) and Family 16 (SERCOS®) – Profiles for functional safety 37
8 Communication Profile Family 3 (PROFIBUS™, PROFINET™) – Profiles for functional safety 37
9 Communication Profile Family 6 (INTERBUS®) – Profiles for functional safety 38
10 Communication Profile Family 8 (CC-Link™) – Profiles for functional safety 38
10.1 Functional Safety Communication Profile 8/1 38
10.2 Functional Safety Communication Profile 8/2 39
11 Communication Profile Family 12 (EtherCAT™) – Profiles for functional safety 39
12 Communication Profile Family 13 (Ethernet POWERLINK™) – Profiles for functional safety 40
13 Communication Profile Family 14 (EPA®) – Profiles for functional safety 40
14 Communication Profile Family 17 (RAPIEnet™) – Profiles for functional safety 40
15 Communication Profile Family 18 (SafetyNET p™ Fieldbus) – Profiles for functional safety 41
Annex A (informative) Example functional safety communication models 42
A.1 General 42
A.2 Model A (single message, channel and FAL, redundant SCLs) 42
A.3 Model B (full redundancy) 42
A.4 Model C (redundant messages, FALs and SCLs, single channel) 43
A.5 Model D (redundant messages and SCLs, single channel and FAL) 43
Annex B (normative) Safety communication channel model using CRC-based error checking 45
B.1 Overview 45
B.2 Channel model for calculations 45
B.3 Bit error probability Pe 46
B.4 Cyclic redundancy checking 47
B.4.1 General 47
B.4.2 Considerations concerning CRC polynomials 48
Annex C (informative) Structure of technology-specific parts 50
Annex D (informative) Assessment guideline 52
D.1 Overview 52
D.2 Channel types 52
D.2.1 General 52
D.2.2 Black channel 52
D.2.3 White channel 52
D.3 Data integrity considerations for white channel approaches 53
D.3.1 General 53
D.3.2 Models B and C 53
D.3.3 Models A and D 54
D.4 Verification of safety measures 55

D.4.1 General 55
D.4.2 Implementation 55
D.4.3 "De-energize to trip" principle 55
D.4.4 Safe state 55
D.4.5 Transmission errors 55
D.4.6 Safety reaction and response times 55
D.4.7 Combination of measures 56
D.4.8 Absence of interference 56
D.4.9 Additional fault causes (white channel) 56
D.4.10 Reference test beds and operational conditions 56
D.4.11 Conformance tester 56
Annex E (informative) Examples of implicit vs. explicit FSCP safety measures 57
E.1 General 57
E.2 Example fieldbus message with safety PDUs 57
E.3 Model with completely explicit safety measures 57
E.4 Model with explicit A-code and implicit T-code safety measures 58
E.5 Model with explicit T-code and implicit A-code safety measures 58
E.6 Model with split explicit and implicit safety measures 59
E.7 Model with completely implicit safety measures 60
E.8 Addition to Annex B – impact of implicit codes on properness 60
Annex F (informative) Extended models for estimation of the total residual error rate 61
F.1 Applicability 61
F.2 General models for black channel communications 61
F.3 Identification of generic safety properties 62
F.4 Assumptions for residual error rate calculations 62
F.5 Residual error rates 63
F.5.1 Explicit and implicit mechanisms 63
F.5.2 Residual error rate calculations 63
F.6 Data integrity 65
F.6.1 Probabilistic considerations 65
F.6.2 Deterministic considerations 65
F.7 Authenticity 66
F.7.1 General 66
F.7.2 Residual error rate for authenticity (RR_A) 67
F.8 Timeliness 68
F.8.1 General 68
F.8.2 Residual error rate for timeliness (RR_T) 70
F.9 Masquerade 71
F.9.1 General 71
F.9.2 Other terms used to calculate residual error rate for masquerade rejection (RR_M) 71
F.10 Calculation of the total residual error rates 71
F.10.1 Based on the summation of the residual error rates 71
F.10.2 Based on other quantitative proofs 72
F.11 Total residual error rate and SIL 72
F.12 Configuration and parameterization for an FSCP 73
F.12.1 General 73
F.12.2 Configuration and parameterization change rate 75
F.12.3 Residual error rate for configuration and parameterization 75

Bibliography 76

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 – Transition from Edition 2 to Edition 3 assessment methods 11
Figure 4 – Safety communication as a part of a safety function 24
Figure 5 – Example model of a functional safety communication system 25
Figure 6 – Example of safety function response time components 26
Figure 7 – Conceptual FSCP protocol model 31
Figure 8 – FSCP implementation aspects 31
Figure 9 – Example application 1 (m=4) 33
Figure 10 – Example application 2 (m = 2) 33
Figure 11 – Zones and conduits concept for security according to IEC 62443 35
Figure A.1 – Model A 42
Figure A.2 – Model B 43
Figure A.3 – Model C 43
Figure A.4 – Model D 44
Figure B.1 – Communication channel with perturbation 45
Figure B.2 – Binary symmetric channel (BSC) 46
Figure B.3 – Example of a block with a message part and a CRC signature 47
Figure B.4 – Block codes for error detection 48
Figure B.5 – Proper and improper CRC polynomials 49
Figure D.1 – Basic Markov model 54
Figure E.1 – Example safety PDUs embedded in a fieldbus message 57
Figure E.2 – Model with completely explicit safety measures 57
Figure E.3 – Model with explicit A-code and implicit T-code safety measures 58
Figure E.4 – Model with explicit T-code and implicit A-code safety measures 59
Figure E.5 – Model with split explicit and implicit safety measures 59
Figure E.6 – Model with completely implicit safety measures 60
Figure F.1 – Black channel from an FSCP perspective 61
Figure F.2 – Model for authentication considerations 66
Figure F.3 – Fieldbus and internal address errors 67
Figure F.4 – Example of slowly increasing message latency 69
Figure F.5 – Example of an active network element failure 70
Figure F.6 – Example application 1 (m = 4) 72
Figure F.7 – Example application 2 (m = 2) 72
Figure F.8 – Example of configuration and parameterization procedures for FSCP 74

Table 1 – Overview of the effectiveness of the various measures on the possible errors 30
Table 2 – Definition of items used for calculation of the residual error rates 32
Table 3 – Typical relationship of residual error rate to SIL 34
Table 4 – Typical relationship of residual error on demand to SIL 34
Table 5 – Overview of profile identifier usable for FSCP 6/7 38

Table B.1 – Example dependency d_{min} and block bit length n 48
Table C.1 – Common subclause structure for technology-specific parts.....50
Table F.1 – Typical relationship of residual error rate to SIL 73
Table F.2 – Typical relationship of residual error on demand to SIL.....73

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES –

Part 3: Functional safety fieldbuses – General rules and profile definitions

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.

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

This third edition cancels and replaces the second edition published in 2010. This edition constitutes a technical revision.

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

- clarifications and additional explanations for requirements, updated references;
- deletion of technical overviews of profiles (Clauses 6 to 13), and associated dedicated subclauses for terms, definitions, symbols and abbreviations;
- addition of profiles for Communication Profile Families 8, 17 and 18 (Clauses 10, 14, 15);
- clarifications of models in Annex A;

- Annex B changed from informative to normative;
- addition of a new informative Annex E describing models for explicit and implicit FSCP mechanisms;
- addition of a new informative Annex F introducing an extended model for estimation of the total residual error rate;
- updates in parts for CPF 1, CPF 2, CPF 3, CPF 8, CPF 13 (details provided in the parts);
- addition of a new part for CPF 17.

The text of this standard is based on the following documents:

FDIS	Report on voting
65C/840/FDIS	65C/848/RVD

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

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

A list of all parts of the IEC 61784-3 series, published under the general title *Industrial communication networks – Profiles – Functional safety fieldbuses*, can be found on the IEC website.

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC website under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

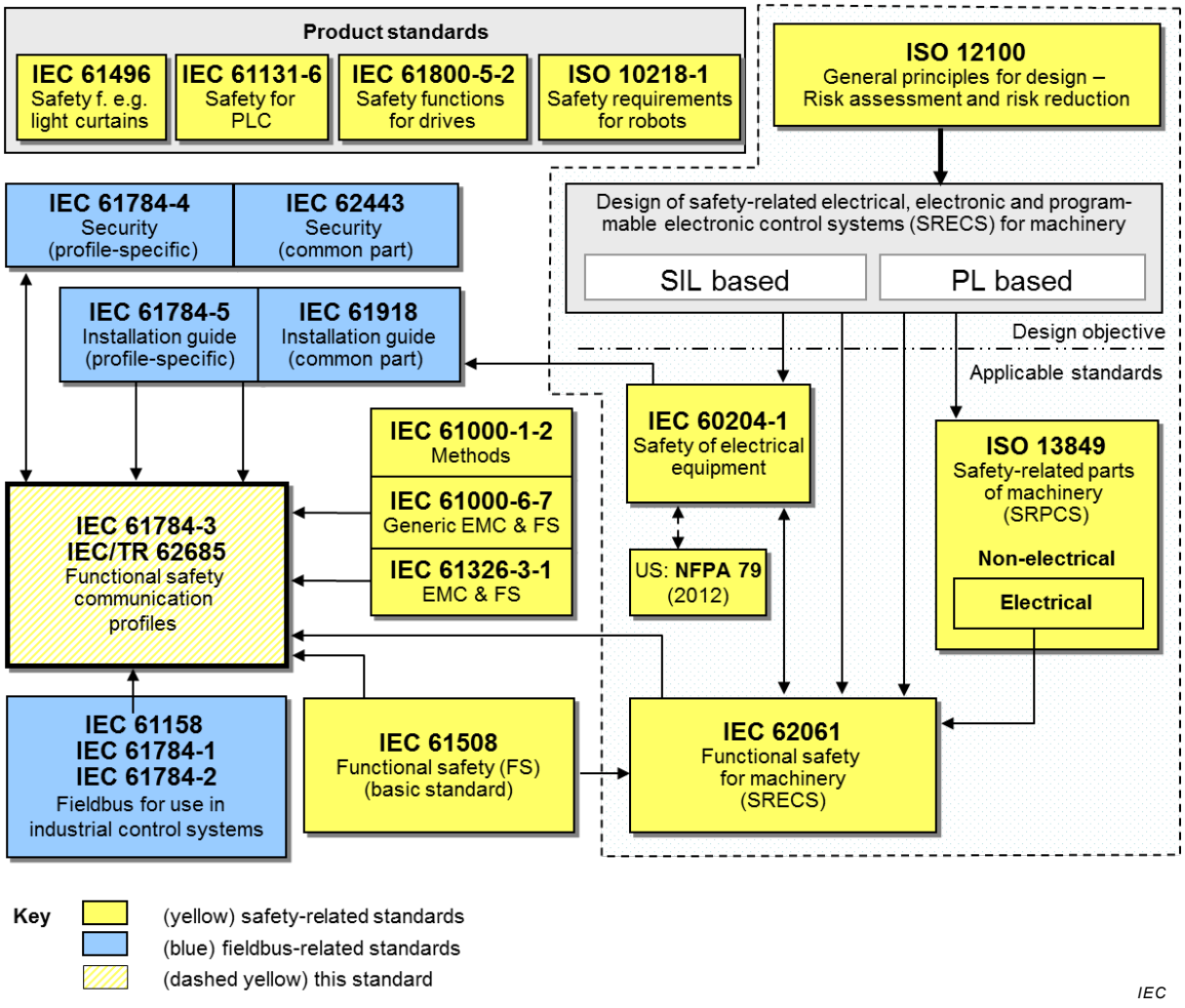
0 Introduction

0.1 General

The IEC 61158 fieldbus standard together with its companion standards IEC 61784-1 and IEC 61784-2 defines a set of communication protocols that enable distributed control of automation applications. Fieldbus technology is now considered well accepted and well proven. Thus fieldbus enhancements continue to emerge, addressing applications for areas such as real time, safety-related and security-related applications.

This standard explains the relevant principles for functional safety communications with reference to IEC 61508 series and specifies several safety communication layers (profiles and corresponding protocols) based on the communication profiles and protocol layers of IEC 61784-1, IEC 61784-2 and the IEC 61158 series. It does not cover electrical safety and intrinsic safety aspects.

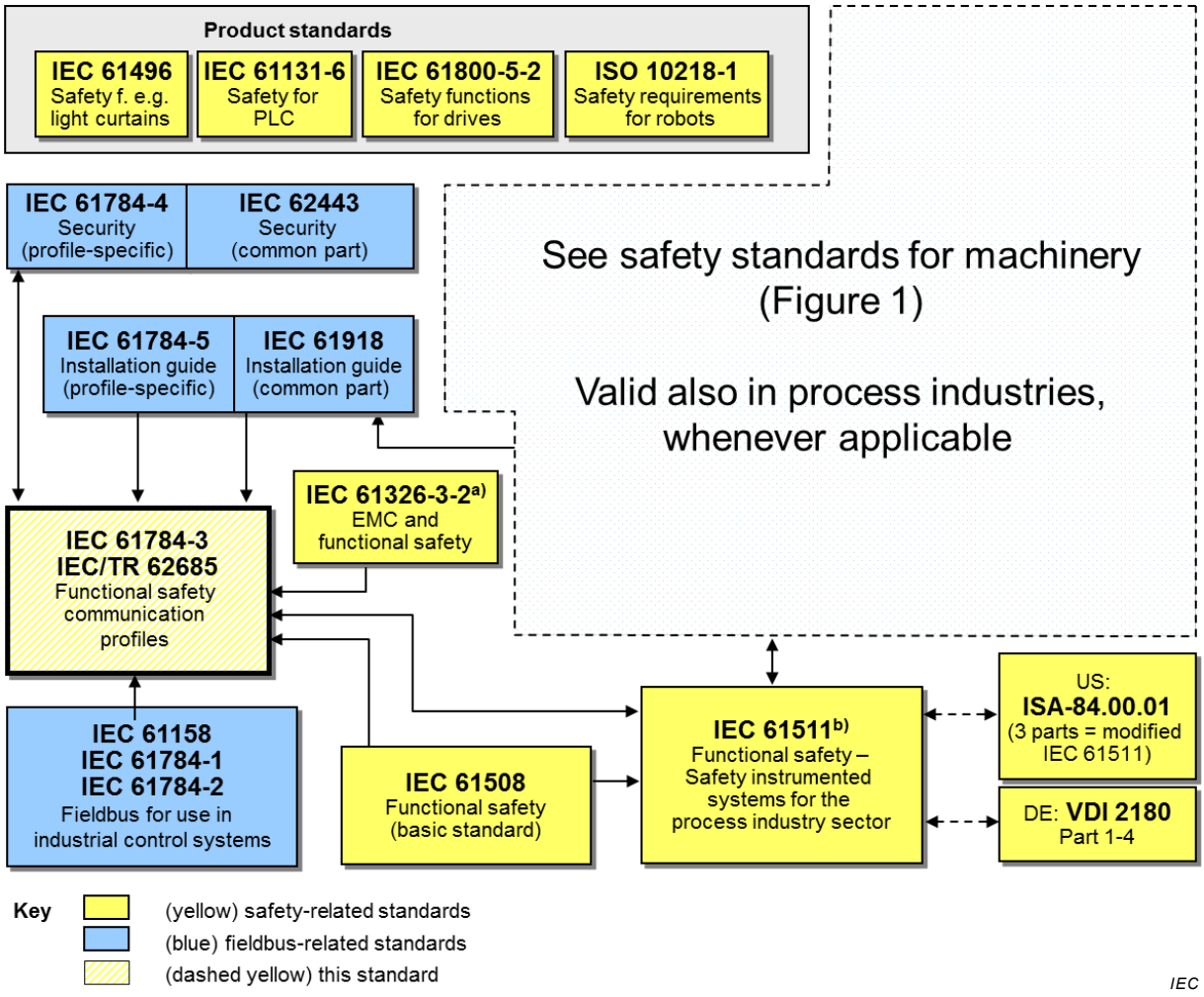
Figure 1 shows the relationships between this standard and relevant safety and fieldbus standards in a machinery environment.



NOTE Subclauses 6.7.6.4 (high complexity) and 6.7.8.1.6 (low complexity) of IEC 62061 specify the relationship between PL (Category) and SIL.

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

Figure 2 shows the relationships between this standard and relevant safety and fieldbus standards in a process environment.



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

[b] EN ratified.

Figure 2 – Relationships of IEC 61784-3 with other standards (process)

Safety communication layers which are implemented as parts of safety-related systems according to IEC 61508 series provide the necessary confidence in the transportation of messages (information) between two or more participants on a fieldbus in a safety-related system, or sufficient confidence of safe behaviour in the event of fieldbus errors or failures.

Safety communication layers specified in this standard do this in such a way that a fieldbus can be used for applications requiring functional safety up to the Safety Integrity Level (SIL) specified by its corresponding functional safety communication profile.

The resulting SIL claim of a system depends on the implementation of the selected functional safety communication profile (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.

This standard describes:

- basic principles for implementing the requirements of IEC 61508 series for safety-related data communications, including possible transmission faults, remedial measures and considerations affecting data integrity;
- 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 the IEC 61158 series.

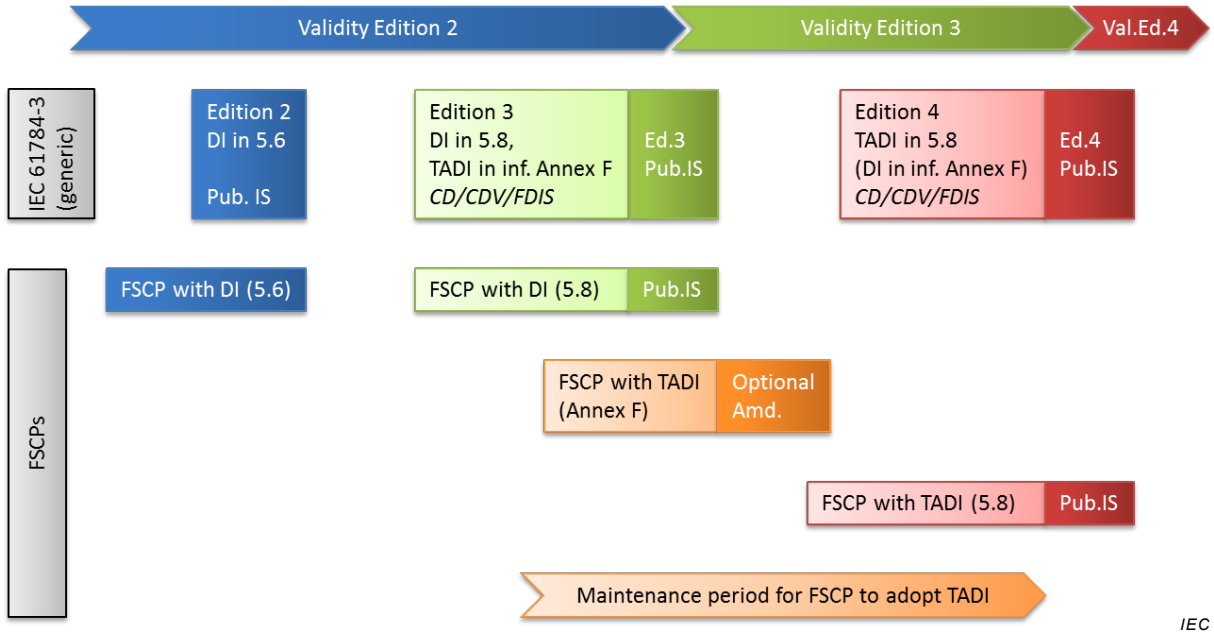
0.2 Transition from Edition 2 to extended assessment methods in Edition 3

This edition of the generic part of the standard includes additional extended models for future use when estimating the total residual error rate for an FSCP. This value can be used to determine if the FSCP meets the requirements of functional safety applications up to a given SIL. These extended models for qualitative and quantitative safety determination methods are detailed in Annex E and Annex F.

However, because of the typical duration of the assessment process, the FSCPs published prior to or concurrently with this new edition of the generic part can only be assessed using the methods from previous editions, based on data integrity considerations specified in 5.8.

The validity schema in Figure 3 shows how to handle the transition from original assessment methods of Edition 2 (specified in 5.8) to extended assessment methods in Edition 3 (currently specified in Annex F). According to this schema, the FSCPs are exempt from a new assessment according to Annex F until Edition 4, where the contents of current Annex F will replace the current 5.8.

NOTE However, a particular FSCP can achieve an earlier assessment and publish an adequate amendment.



Key

DI Data Integrity

TADI Timeliness, Authenticity, Data Integrity

Figure 3 – Transition from Edition 2 to Edition 3 assessment methods

0.3 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 functional safety communication profiles for families 1, 2, 3, 6, 8, 12, 13, 14, 17 and 18 given in IEC 61784-3-1, IEC 61784-3-2, IEC 61784-3-3, IEC 61784-3-6, IEC 61784-3-8, IEC 61784-3-12, IEC 61784-3-13, IEC 61784-3-14, IEC 61784-3-17 and IEC 61784-3-18.

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

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

NOTE Patent details and corresponding contact information are provided in IEC 61784-3-1, IEC 61784-3-2, IEC 61784-3-3, IEC 61784-3-6, IEC 61784-3-8, IEC 61784-3-12, IEC 61784-3-13, IEC 61784-3-14, IEC 61784-3-17 and IEC 61784-3-18.

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

ISO (www.iso.org/patents) and IEC (http://patents.iec.ch) maintain on-line data bases of patents relevant to their standards. Users are encouraged to consult the data bases for the most up to date information concerning patents.

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES –

Part 3: Functional safety fieldbuses – General rules and profile definitions

1 Scope

This part of the IEC 61784-3 series explains some common principles that can be used in the transmission of safety-relevant messages among participants within a distributed network which use fieldbus technology in accordance with the requirements of IEC 61508 series[1] for functional safety. These principles are based on the black channel approach. They can be used in various industrial applications such as process control, manufacturing automation and machinery.

This part[2] and the IEC 61784-3-x parts specify several functional safety communication profiles based on the communication profiles and protocol layers of the fieldbus technologies in IEC 61784-1, IEC 61784-2 and the IEC 61158 series. These functional safety communication profiles use the black channel approach, as defined in IEC 61508. These functional safety communication profiles are intended for implementation in safety devices exclusively.

NOTE 1 Other safety-related communication systems meeting the requirements of IEC 61508 series can exist that are not included in this standard.

NOTE 2 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.

All systems are exposed to unauthorized access at some point of their life cycle. Additional measures need to be considered in any safety-related application to protect fieldbus systems against unauthorized access. The IEC 62443 series will address many of these issues; the relationship with the IEC 62443 series is detailed in a dedicated subclause of this part.

NOTE 3 Additional profile specific requirements for security can also be specified in IEC 61784-4[3].

NOTE 4 Implementation of a functional safety communication profile according to this part in a device is not sufficient to qualify it as a safety device, as defined in IEC 61508 series.

NOTE 5 The resulting SIL claim of a system depends on the implementation of the selected functional safety communication profile within this system.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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*

---

1 In the following pages of this standard, “IEC 61508” will be used for “IEC 61508 series”.

2 In the following pages of this standard, “this part” will be used for “this part of the IEC 61784-3 series”.

3 Proposed new work item under consideration.

IEC 61010-2-201:2013, *Safety requirements for electrical equipment for measurement, control and laboratory use – Part 2-201: Particular requirements for control equipment*

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

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

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

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

IEC 61784-3-1, *Industrial communication networks – Profiles – Part 3-1: Functional safety fieldbuses – Additional specifications for CPF 1*

IEC 61784-3-2, *Industrial communication networks – Profiles – Part 3-2: Functional safety fieldbuses – Additional specifications for CPF 2*

IEC 61784-3-3, *Industrial communication networks – Profiles – Part 3-3: Functional safety fieldbuses – Additional specifications for CPF 3*

IEC 61784-3-6, *Industrial communication networks – Profiles – Part 3-6: Functional safety fieldbuses – Additional specifications for CPF 6*

IEC 61784-3-8, *Industrial communication networks – Profiles – Part 3-8: Functional safety fieldbuses – Additional specifications for CPF 8*

IEC 61784-3-12, *Industrial communication networks – Profiles – Part 3-12: Functional safety fieldbuses – Additional specifications for CPF 12*

IEC 61784-3-13, *Industrial communication networks – Profiles – Part 3-13: Functional safety fieldbuses – Additional specifications for CPF 13*

IEC 61784-3-14, *Industrial communication networks – Profiles – Part 3-14: Functional safety fieldbuses – Additional specifications for CPF 14*

IEC 61784-3-17[4], *Industrial communication networks – Profiles – Part 3-17: Functional safety fieldbuses – Additional specifications for CPF 17*

IEC 61784-3-18, *Industrial communication networks – Profiles – Part 3-18: Functional safety fieldbuses – Additional specifications for CPF 18*

IEC 61784-5 (all parts), *Industrial communication networks – Profiles – Part 5: Installation of fieldbuses*

IEC 61918:2013, *Industrial communication networks – Installation of communication networks in industrial premises*

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

4 To be published

SOMMAIRE

AVANT-PROPOS 83
0 Introduction 85
0.1 Généralités 85
0.2 Transition de l'édition 2 aux méthodes d'évaluation étendue de l'édition 3 88
0.3 Déclaration de brevet 89
1 Domaine d'application 91
2 Références normatives 91
3 Termes, définitions, symboles, abréviations et conventions 93
3.1 Termes et définitions 93
3.2 Symboles et abréviations 100
4 Conformité 102
5 Principes des systèmes de bus de terrain relatifs à la sécurité 102
5.1 Décomposition d'une fonction de sécurité 102
5.2 Système de communication 103
5.2.1 Généralités 103
5.2.2 Bus de terrain définis dans l'IEC 61158 103
5.2.3 Types de canaux de communication 104
5.2.4 Temps de réponse de la fonction de sécurité 105
5.3 Erreurs de communication 105
5.3.1 Généralités 105
5.3.2 Corruption 105
5.3.3 Répétition non prévue 106
5.3.4 Séquence incorrecte 106
5.3.5 Perte 106
5.3.6 Retard inacceptable 106
5.3.7 Insertion 106
5.3.8 Déguisement 106
5.3.9 Adressage 107
5.4 Mesures correctives déterministes 107
5.4.1 Généralités 107
5.4.2 Numéro de séquence 107
5.4.3 Horodatage 107
5.4.4 Délai 107
5.4.5 Authentification de connexion 107
5.4.6 Message en retour 108
5.4.7 Assurance d'intégrité des données 108
5.4.8 Redondance avec contre-vérification 108
5.4.9 Différents systèmes d'assurance d'intégrité des données 108
5.5 Relations typiques entre les erreurs et les mesures de sécurité 108
5.6 Phases de communication 109
5.7 Aspects relatifs à la mise en œuvre du FSCP 110
5.8 Considérations relatives à l'intégrité des données 111
5.8.1 Calcul du taux d'erreurs résiduelles 111
5.8.2 Taux total d'erreurs résiduelles et SIL 114
5.9 Relation entre sécurité fonctionnelle et sûreté 114
5.10 Conditions aux limites et contraintes 115

5.10.1 Sécurité électrique 115
5.10.2 Compatibilité électromagnétique (CEM) 116
5.11 Guide d'installation 116
5.12 Manuel de sécurité 116
5.13 Politique de sécurité 116
6 Famille de profils de communication 1 (Fieldbus FOUNDATION™) – Profils de sécurité fonctionnelle 117
7 Famille de profils de communication 2 (CIP™) et Famille 16 (SERCOS®) – Profils de sécurité fonctionnelle 118
8 Famille de profils de communication 3 (PROFIBUS™, PROFINET™) – Profils de sécurité fonctionnelle 118
9 Famille de profils de communication 6 (INTERBUS®) – Profils de sécurité fonctionnelle 119
10 Famille de profils de communication 8 (CC-Link™) – Profils de sécurité fonctionnelle 119
10.1 Profil de communication de sécurité fonctionnelle 8/1 119
10.2 Profil de communication de sécurité fonctionnelle 8/2 120
11 Famille de profils de communication 12 (EtherCAT™) – Profils de sécurité fonctionnelle 120
12 Famille de profils de communication 13 (Ethernet POWERLINK™) – Profils de sécurité fonctionnelle 120
13 Famille de profils de communication 14 (EPA®) – Profils de sécurité fonctionnelle 121
14 Famille de profils de communication 17 (RAPIEnet™) – Profils de sécurité fonctionnelle 121
15 Famille de profils de communication 18 (Fieldbus SafetyNET p™) – Profils de sécurité fonctionnelle 121
Annexe A (informative) Exemple de modèles de communication de sécurité fonctionnelle 122
A.1 Généralités 122
A.2 Modèle A (message unique, canal et FAL, SCL redondantes) 122
A.3 Modèle B (redondance complète) 122
A.4 Modèle C (messages redondants, FAL et SCL, canal unique) 123
A.5 Modèle D (messages redondants et SCL, canal unique et FAL) 123
Annexe B (normative) Modèle de canal de communication de sécurité qui utilise le contrôle d'erreurs CRC 125
B.1 Vue d'ensemble 125
B.2 Modèle de canal pour calculs 125
B.3 Probabilité d'erreurs sur les éléments binaires Pe 126
B.4 Contrôle de redondance cyclique 127
B.4.1 Généralités 127
B.4.2 Considérations relatives aux polynômes CRC 129
Annexe C (informative) Structure des parties spécifiques à la technologie 131
Annexe D (informative) Lignes directrices pour l'évaluation 134
D.1 Vue d'ensemble 134
D.2 Types de canaux 134
D.2.1 Généralités 134
D.2.2 Canal noir 134
D.2.3 Canal blanc 135
D.3 Considérations relatives à l'intégrité des données pour les méthodes du canal blanc 135

D.3.1 Généralités 135
D.3.2 Modèles B et C 135
D.3.3 Modèles A et D 136
D.4 Vérification des mesures de sécurité 137
D.4.1 Généralités 137
D.4.2 Mise en œuvre 137
D.4.3 Principe de "mise hors tension pour déclenchement" 137
D.4.4 Etat de sécurité 138
D.4.5 Erreurs de transmission 138
D.4.6 Réaction de sécurité et temps de réponse 138
D.4.7 Combinaison des mesures 138
D.4.8 Absence de perturbations 138
D.4.9 Causes d'anomalies supplémentaires (canal blanc) 138
D.4.10 Bancs d'essai de référence et conditions de fonctionnement 139
D.4.11 Appareil de vérification de conformité 139
Annexe E (informative) Exemples de mesures de sécurité de FSCP implicites et explicites 140
E.1 Généralités 140
E.2 Exemple de message de bus de terrain avec PDU de sécurité 140
E.3 Modèle avec mesures de sécurité totalement explicites 140
E.4 Modèle avec mesures de sécurité explicites de code A et implicites de code T 142
E.5 Modèle avec mesures de sécurité explicites de code T et implicites de code A 143
E.6 Modèle avec mesures de sécurité explicites et implicites divisées 144
E.7 Modèle avec mesures de sécurité totalement implicites 145
E.8 Ajout à l'Annexe B – Influence des codes implicites sur l'exactitude 145
Annexe F (informative) Modèles étendus pour l'estimation du taux total d'erreurs résiduelles 146
F.1 Applicabilité 146
F.2 Modèles généraux pour les communications du canal noir 146
F.3 Identification des propriétés de sécurité générique 148
F.4 Hypothèses pour les calculs de taux d'erreurs résiduelles 148
F.5 Taux d'erreurs résiduelles 149
F.5.1 Mécanismes explicites et implicites 149
F.5.2 Calculs de taux d'erreurs résiduelles 149
F.6 Intégrité des données 151
F.6.1 Considérations probabilistes 151
F.6.2 Considérations déterministes 152
F.7 Authenticité 152
F.7.1 Généralités 152
F.7.2 Taux d'erreurs résiduelles pour l'authenticité (RR_A) 155
F.8 Opportunité 155
F.8.1 Généralités 155
F.8.2 Taux d'erreurs résiduelles pour l'opportunité (RR_T) 158
F.9 Déguisement 158
F.9.1 Généralités 158
F.9.2 Autres termes utilisés pour calculer le taux d'erreurs résiduelles pour le rejet de déguisement (RR_M) 158
F.10 Calcul du taux total d'erreurs résiduelles 158

F.10.1 Sur la base de la somme des taux d'erreurs résiduelles 158
F.10.2 Sur la base d'autres preuves quantitatives 160
F.11 Taux total d'erreurs résiduelles et SIL 160
F.12 Configuration et paramétrage pour un FSCP 161
F.12.1 Généralités 161
F.12.2 Fréquence de modification de la configuration et du paramétrage 163
F.12.3 Taux d'erreurs résiduelles pour la configuration et le paramétrage 163
Bibliographie 164

Figure 1 – Relations entre l'IEC 61784-3 et d'autres normes (machines) 86
Figure 2 – Relations entre l'IEC 61784-3 et d'autres normes (transformation) 88
Figure 3 – Transition de l'édition 2 aux méthodes d'évaluation de l'édition 3 89
Figure 4 – Communication de sécurité comme partie intégrante d'une fonction de sécurité 103
Figure 5 – Exemple de modèle d'un système de communication de sécurité fonctionnelle 104
Figure 6 – Exemple des composantes du temps de réponse de la fonction de sécurité 105
Figure 7 – Modèle de protocole FSCP conceptuel 110
Figure 8 – Aspects relatifs à la mise en œuvre du FSCP 111
Figure 9 – Exemple d'application 1 (m = 4) 113
Figure 10 – Exemple d'application 2 (m = 2) 113
Figure 11 – Concept de zones et conduits pour la sûreté conformément à l'IEC 62443 115
Figure A.1 – Modèle A 122
Figure A.2 – Modèle B 123
Figure A.3 – Modèle C 123
Figure A.4 – Modèle D 124
Figure B.1 – Canal de communication avec perturbation 126
Figure B.2 – Canal symétrique binaire (BSC) 126
Figure B.3 – Exemple de bloc avec une partie message et une signature CRC 128
Figure B.4 – Codes de blocs pour la détection d'erreurs 128
Figure B.5 – Polynômes CRC appropriés et inappropriés 130
Figure D.1 – Modèle de Markov de base 136
Figure E.1 – Exemple de PDU de sécurité intégrés à un message de bus de terrain 140
Figure E.2 – Modèle avec mesures de sécurité totalement explicites 141
Figure E.3 – Modèle avec mesures de sécurité explicites de code A et mesures de sécurité implicites de code T 142
Figure E.4 – Modèle avec mesures de sécurité explicites de code T et mesures de sécurité implicites de code A 143
Figure E.5 – Modèle avec mesures de sécurité explicites et implicites divisées 144
Figure E.6 – Modèle avec mesures de sécurité totalement implicites 145
Figure F.1 – Canal noir du point de vue d'un FSCP 147
Figure F.2 – Modèle pour la prise en compte de l'authentification 153
Figure F.3 – Bus de terrain et erreurs d'adresse internes 154
Figure F.4 – Exemple de latence de message en croissance progressive 156
Figure F.5 – Exemple de défaillance d'un élément de réseau actif 157

Figure F.6 – Exemple d'application 1 (m = 4) 159
Figure F.7 – Exemple d'application 2 (m = 2) 160
Figure F.8 – Exemple de procédures de configuration et de paramétrage pour FSCP 162

Tableau 1 – Présentation générale de l'efficacité des différentes mesures sur les erreurs possibles 109
Tableau 2 – Définition des éléments utilisés pour le calcul des taux d'erreurs résiduelles 112
Tableau 3 – Relation typique entre le taux d'erreurs résiduelles et le SIL 114
Tableau 4 – Relation typique entre l'erreur résiduelle et le SIL 114
Tableau 5 – Présentation générale de l'identifiant de profil applicable au protocole FSCP 6/7 119
Tableau B.1 – Exemple de dépendance d_{min} et de longueur binaire de bloc n 129
Tableau C.1 – Structure commune des paragraphes pour les parties spécifiques à la technologie 131
Tableau F.1 – Relation typique entre le taux d'erreurs résiduelles et le SIL 161
Tableau F.2 – Relation typique entre l'erreur résiduelle et le SIL 161

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

RÉSEAUX DE COMMUNICATION INDUSTRIELS – PROFILS –

Partie 3: Bus de terrain de sécurité fonctionnelle – Règles générales et définitions de profils

AVANT-PROPOS

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

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

Cette troisième édition annule et remplace la deuxième édition parue en 2010. Cette édition constitue une révision technique.

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

- clarifications et explications complémentaires des exigences, références actualisées;
- suppression des présentations techniques de profils (Articles 6 à 13) et paragraphes dédiés associés à des termes, définitions, symboles et abréviations;

- ajout de profils pour les familles de profils de communication 8, 17 et 18 (Articles 10, 14, 15);
- clarifications des modèles de l'Annexe A;
- modification de l'Annexe B informative qui devient normative;
- ajout d'une nouvelle Annexe E informative pour décrire les modèles des mécanismes FSCP explicites et implicites;
- ajout d'une nouvelle Annexe F informative qui introduit un modèle étendu pour l'estimation du taux total d'erreurs résiduelles;
- actualisations des parties pour les CPF 1, CPF 2, CPF 3, CPF 8, CPF 13 (détails fournis dans les parties);
- ajout d'une nouvelle partie pour CPF 17.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
65C/840/FDIS	65C/848/RVD

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

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

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

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

- reconduite,
- supprimée,
- remplacée par une édition révisée, ou
- amendée.

IMPORTANT – Le logo *"colour inside"* qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

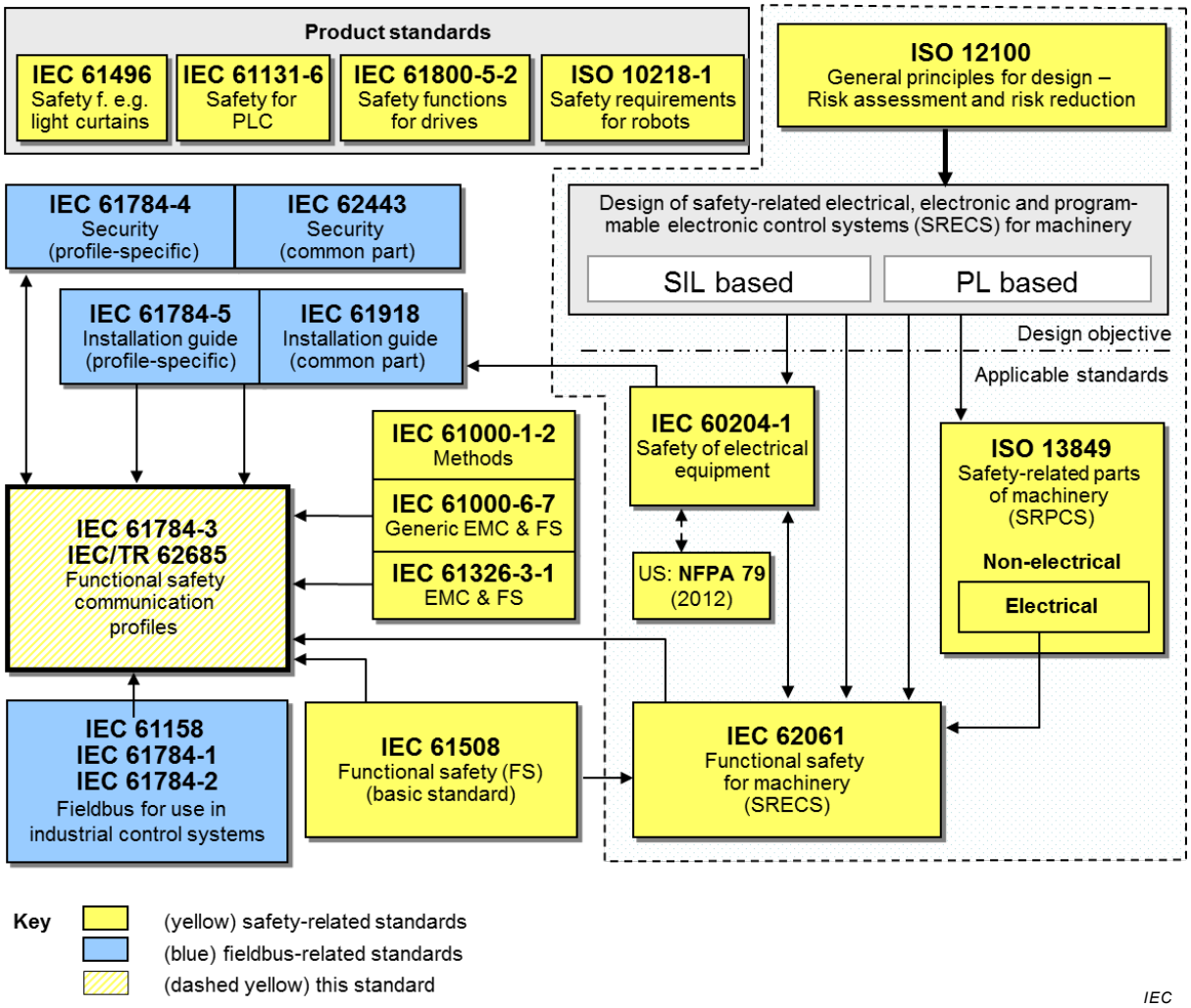
0 Introduction

0.1 Généralités

L'IEC 61158, relative aux bus de terrain, ainsi que ses normes associées IEC 61784-1 et IEC 61784-2, définit un ensemble de protocoles de communication qui assurent la commande répartie d'applications automatisées. La technologie de bus de terrain est désormais reconnue et bien éprouvée. 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 et à la sûreté.

Cette norme définit les principes applicables aux communications de sécurité fonctionnelle en référence à la série IEC 61508; elle spécifie plusieurs couches de communication de sécurité (profils et protocoles correspondants) en fonction des profils de communication et des couches de protocole de l'IEC 61784-1, l'IEC 61784-2 et de la série IEC 61158. Elle ne couvre pas les aspects relatifs à la sécurité électrique et à la sécurité intrinsèque.

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

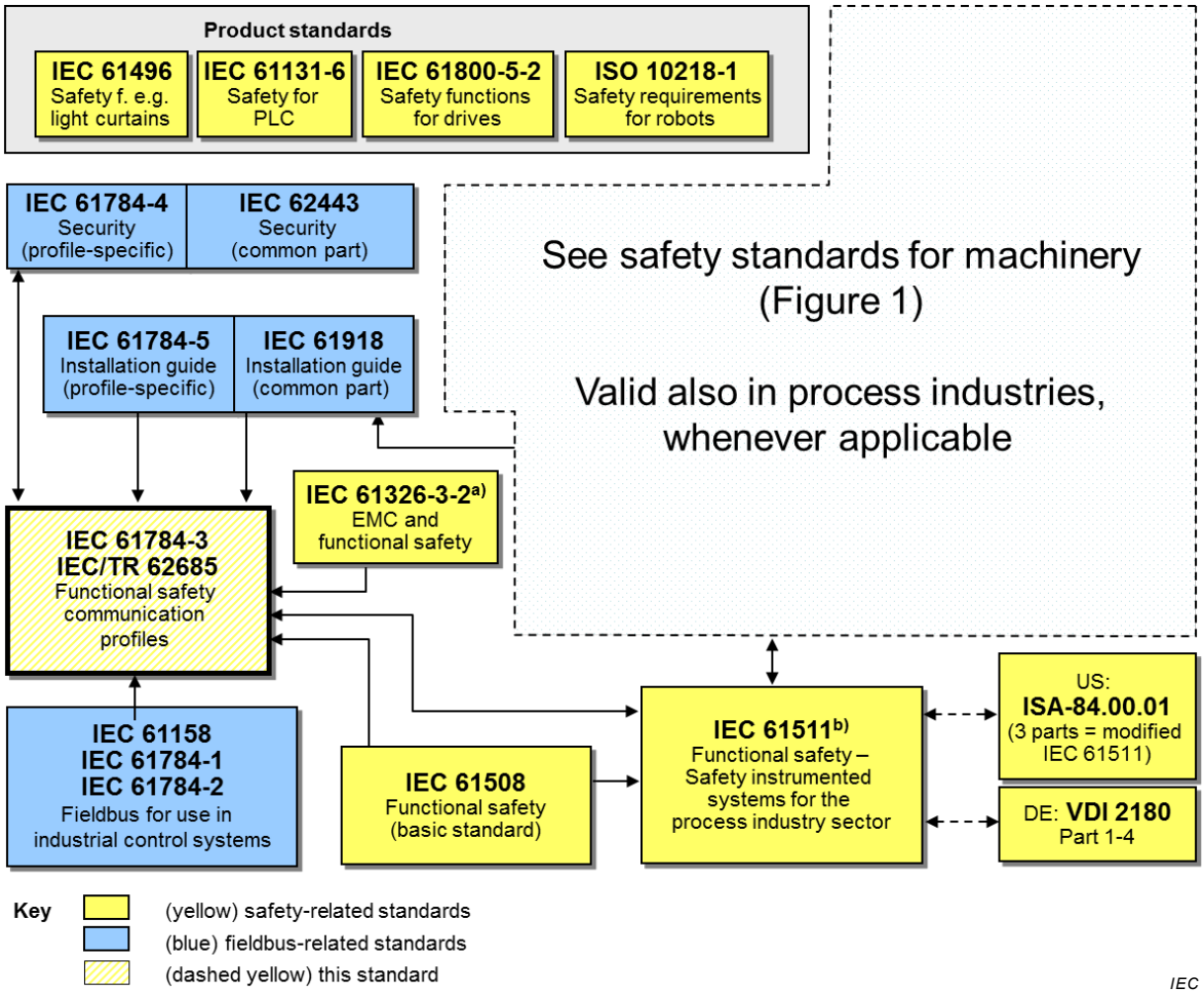


Anglais	Français
Product standards	Normes de produits
Safety function, e.g. light curtains	Fonction de sécurité, par exemple rideaux de lumière
Safety for PLC	Sécurité relative aux automates programmables
Safety functions for drives	Fonctions de sécurité applicables aux entraînements
Safety requirements for robots	Exigences de sécurité applicables aux robots
General principles for design – Risk assessment and risk reduction	Principes généraux de conception – Appréciation du risque et réduction du risque
Security (profile-specific)	Sécurité (spécifique au profil)
Security (common part)	Sécurité (partie commune)
Design of safety-related electrical, electronic and programmable electronic control systems (SRECS) for machinery	Conception des systèmes de commande électriques, électroniques et électroniques programmables relatifs à la sécurité pour les machines
SIL based	Basé sur SIL
PL based	Basé sur PL
Installation guide (profile-specific)	Guide d'installation (spécifique au profil)
Installation guide (common part)	Guide d'installation (partie commune)
Design objective	Objectif de conception
Applicable standards	Normes applicables
Methods	Méthodes
Generic EMC & FS	CEM & FS génériques
EMC & FS	CEM & FS
Safety of electrical equipment	Sécurité des équipements électriques
Safety-related parts of machinery	Sécurité des machines – Parties des systèmes de commande relatives à la sécurité
Non-electrical	Non électrique
Electrical	Electrique
Functional safety communication profiles	Profils de communication de sécurité fonctionnelle
Fieldbus for use in industrial control systems	Bus de terrain pour utilisation dans des systèmes de commande industriels
Functional safety (FS) (basic standard)	Sécurité fonctionnelle (FS) (norme de base)
Functional safety for machinery	Sécurité fonctionnelle des machines
Key	Légende
(yellow) safety-related standards	(jaune) normes relatives à la sécurité
(blue) fieldbus-related standards	(bleu) normes relatives au bus de terrain
(dashed yellow) this standard	(jaune pointillé) la présente norme

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

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

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



Anglais	Français
Product standards	Normes de produits
Safety function, e.g. light curtains	Fonction de sécurité, par exemple rideaux de lumière
Safety for PLC	Sécurité relative aux automates programmables
Safety functions for drives	Fonctions de sécurité applicables aux entraînements
Safety requirements for robots	Exigences de sécurité applicables aux robots
Security (profile-specific)	Sûreté (spécifique au profil)
Security (common part)	Sûreté (partie commune)
Installation guide (profile-specific)	Guide d'installation (spécifique au profil)
Installation guide (common part)	Guide d'installation (partie commune)
See safety standards for machinery (Figure 1)	Voir normes de sécurité pour les machines (Figure 1)
Valid also in process industries, whenever applicable	Valable également dans les industries de transformation, le cas échéant
Functional safety communication profiles	Profils de communication de sécurité fonctionnelle
EMC and functional safety	CEM et sécurité fonctionnelle
Fieldbus for use in industrial control systems	Bus de terrain pour utilisation dans des systèmes de commande industriels
Functional safety (basic standard)	Sécurité fonctionnelle (norme de base)

Anglais	Français
Functional safety–safety instrumented systems for the process industry sector	Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur des industries de transformation
3 parts = modified IEC 61511	3 parties = IEC 61511 modifiée
Part 1 – 4	Parties 1 à 4
Key	Légende
(yellow) safety-related standards	(jaune) normes relatives à la sécurité
(blue) fieldbus-related standards	(bleu) normes relatives au bus de terrain
(dashed yellow) this standard	(jaune pointillé) la présente norme

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

[b] EN ratifiée.

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 la série IEC 61508 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 la présente norme permettent de garantir cette assurance de sorte qu'un bus de terrain puisse 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.

La présente norme décrit:

- les principes de base de la mise en œuvre des exigences de la série IEC 61508 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 les IEC 61784-1 et IEC 61784-2, y compris les extensions de la couche de sécurité aux sections relatives au service et aux protocoles de communication de la série IEC 61158.

0.2 Transition de l'édition 2 aux méthodes d'évaluation étendue de l'édition 3

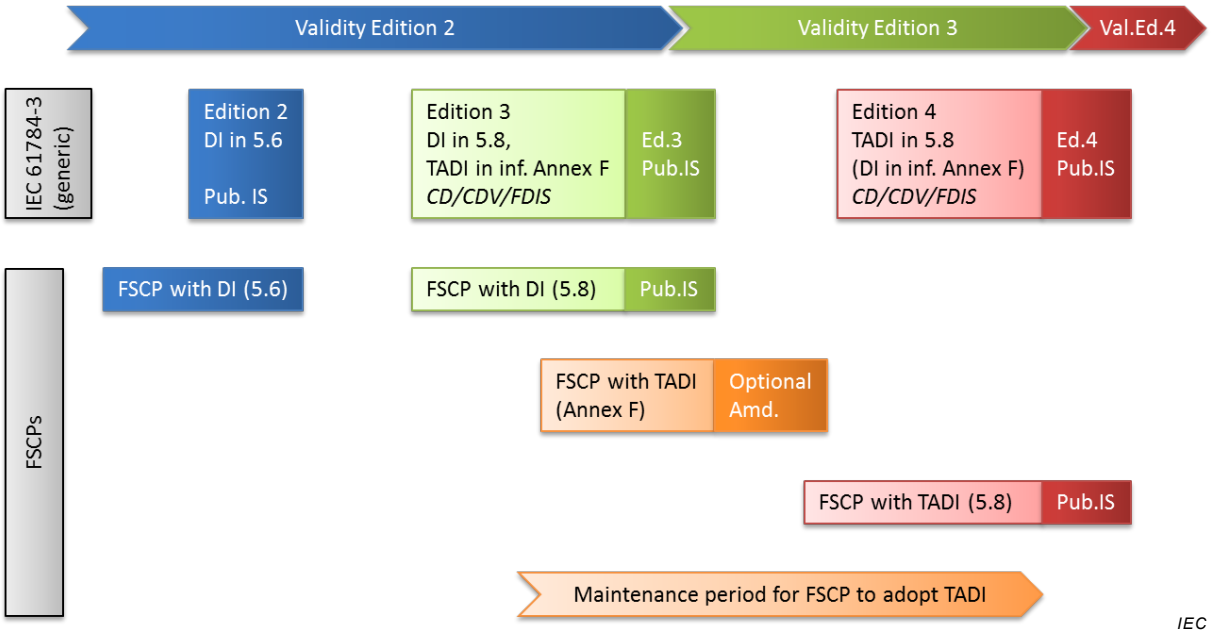
Cette édition de la partie générique de la norme comprend des modèles étendus supplémentaires pour une utilisation ultérieure lors de l'estimation du taux total d'erreurs résiduelles pour un FSCP. Cette valeur peut être utilisée pour déterminer si le FSCP satisfait aux exigences des applications de sécurité fonctionnelle jusqu'à un SIL donné. Ces modèles étendus pour les méthodes qualitatives et quantitatives de détermination de sécurité sont détaillés à l'Annexe E et à l'Annexe F.

Toutefois, en raison de la durée typique du processus d'évaluation, les Profils de Communication de Sécurité Fonctionnelle publiés avant ou en même temps que cette nouvelle édition de la partie générique ne peuvent être évalués qu'en fonction des méthodes

des éditions précédentes, sur la base des considérations relatives à l'intégrité des données détaillées en 5.8.

Le schéma de validité de la Figure 3 présente le procédé de gestion de la transition des méthodes d'évaluation d'origine de l'édition 2 (détaillé en 5.8) aux méthodes d'évaluation étendue de l'édition 3 (actuellement spécifiées à l'Annexe F). Conformément à ce schéma, les Profils de Communication de Sécurité Fonctionnelle sont exemptés d'une nouvelle évaluation conformément à l'Annexe F jusqu'à l'édition 4, lorsque le contenu de l'Annexe F actuelle remplacera le 5.8 actuel.

NOTE Un FSCP peut cependant réaliser une évaluation antérieure et publier un amendement approprié.



Anglais	Français
Validity edition	Edition de validité
(generic)	(générique)
DI in …	DI en …
… in inf. Annex F	… à l'Annexe F inf.
… with DI	… avec DI
… with TADI	… avec TADI
Optional amd.	Amd. facultatif
Maintenance period for FSCP to adopt TADI	Période de maintenance permettant au FSCP d'adopter TADI

Légende

DI Data Integrity (Intégrité des données)

TADI Timeliness, Authenticity, Data Integrity (Opportunité, Authenticité, Intégrité des données)

Figure 3 – Transition de l'édition 2 aux méthodes d'évaluation de l'édition 3

0.3 Déclaration de brevet

La commission électrotechnique internationale (IEC) attire l'attention sur le fait qu'il est déclaré que la conformité aux dispositions du présent document peut impliquer l'utilisation de brevets qui intéressent les profils de communication de sécurité fonctionnelle pour les familles 1, 2, 3, 6, 8, 12, 13, 14, 17 et 18 de l'IEC 61784-3-1, l'IEC 61784-3-2,

l'IEC 61784-3-3, l'IEC 61784-3-6, l'IEC 61784-3-8, l'IEC 61784-3-12, l'IEC 61784-3-13, l'IEC 61784-3-14, l'IEC 61784-3-17 et l'IEC 61784-3-18.

L'IEC ne prend pas position quant à la preuve, à la validité et à la portée de ces droits de propriété.

Les détenteurs de ces droits de propriété ont donné l'assurance à l'IEC qu'ils consentent à négocier des licences avec des demandeurs du monde entier, sans frais ou à des termes et conditions raisonnables et non discriminatoires. A ce propos, les énoncés des détenteurs de ces droits de propriété sont enregistrés à l'IEC.

NOTE Les détails relatifs aux brevets et les informations relatives aux coordonnées correspondantes sont fournis dans l'IEC 61784-3-1, l'IEC 61784-3-2, l'IEC 61784-3-3, l'IEC 61784-3-6, l'IEC 61784-3-8, l'IEC 61784-3-12, l'IEC 61784-3-13, l'IEC 61784-3-14, l'IEC 61784-3-17 et l'IEC 61784-3-18.

L'attention est attirée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété intellectuelle autres que ceux identifiés ci-dessus. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et de ne pas avoir signalé leur existence.

L'ISO (www.iso.org/patents) et l'IEC (http://patents.iec.ch) maintiennent à disposition des bases de données en ligne des droits de propriété relatifs à leurs normes. Les utilisateurs sont encouragés à consulter ces bases de données pour obtenir les informations les plus récentes concernant les droits de propriété.

RÉSEAUX DE COMMUNICATION INDUSTRIELS – PROFILS –

Partie 3: Bus de terrain de sécurité fonctionnelle – Règles générales et définitions de profils

1 Domaine d'application

La présente partie de la série IEC 61784-3 définit des principes communs qui peuvent être appliqués pour la transmission des messages relatifs à la sécurité entre les participants d'un réseau réparti, à l'aide de la technologie de bus de terrain conformément aux exigences de la série IEC 61508[1] sur la sécurité fonctionnelle. Ces principes peuvent s'appuyer sur le principe de canal noir. Ils peuvent être utilisés dans différentes applications industrielles, par exemple la commande de processus, l'usinage automatique et les machines.

La présente partie[2] et les parties IEC 61784-3-x spécifient plusieurs profils de communication de sécurité fonctionnelle basés sur les profils de communication et les couches de protocole des technologies des bus de terrain de l'IEC 61784-1, de l'IEC 61784-2 et de la série IEC 61158. Ces profils de communication de sécurité fonctionnelle utilisent le principe de canal noir, comme défini dans l'IEC 61508. Ces profils de communication de sécurité fonctionnelle sont destinés à être exclusivement mis en œuvre dans des appareils de sécurité.

NOTE 1 Il peut exister d'autres systèmes de communication relatifs à la sécurité qui satisfont aux exigences de la série IEC 61508 et ne sont pas inclus dans la présente norme.

NOTE 2 Elle ne couvre pas les aspects relatifs à la sécurité électrique et à la sécurité intrinsèque. La sécurité électrique concerne les dangers comme les chocs électriques. La sécurité intrinsèque concerne les dangers associés aux atmosphères explosibles.

Tous les systèmes sont exposés à un accès non autorisé à un certain moment de leur cycle de vie. Des mesures supplémentaires doivent être prises en compte dans une application relative à la sécurité afin de protéger les systèmes qui disposent de bus de terrain contre tout accès non autorisé. La série IEC 62443 traite bon nombre de ces questions; la relation avec la série IEC 62443 est détaillée dans un paragraphe dédié de la présente partie.

NOTE 3 Des exigences spécifiques au profil peuvent également être spécifiées dans l'IEC 61784-4[3].

NOTE 4 La mise en œuvre du profil de communication de sécurité fonctionnelle, conforme à la présente partie, dans un appareil normal ne suffit pas à le qualifier d'appareil de sécurité, comme défini dans la série IEC 61508.

NOTE 5 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.

2 Références normatives

Les documents suivants sont cités en référence de manière normative, en intégralité ou en partie, dans le présent document et sont indispensables pour son application. 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).

_____

1 Dans les pages suivantes de la présente norme, "IEC 61508" remplace "série IEC 61508".

2 Dans les pages suivantes de la présente norme, "la présente partie" remplace "cette partie de la série IEC 61784-3".

3 Proposition d'un nouveau sujet de travail à l'étude.

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 61010-2-201:2013, *Règles de sécurité pour appareils électriques de mesurage, de régulation et de laboratoire – Partie 2-201: Exigences particulières pour les équipements de commande*

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

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 61508-1:2010, *Sécurité fonctionnelle des systèmes électriques/électroniques/ électroniques programmables relatifs à la sécurité – Partie 1: Exigences générales*

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

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

IEC 61784-3-1, *Industrial communication networks – Profiles – Part 3-1: Functional safety fieldbuses – Additional specifications for CPF* (disponible en anglais seulement)

IEC 61784-3-2, *Réseaux de communication industriels – Profils – Partie 3-2: Bus de terrain de sécurité fonctionnelle – Spécifications supplémentaires pour CPF 2*

IEC 61784-3-3, *Réseaux de communication industriels – Profils – Partie 3-3: Bus de terrain de sécurité fonctionnelle – Spécifications supplémentaires pour CPF 3*

IEC 61784-3-6, *Réseaux de communication industriels – Profils – Partie 3-6: Bus de terrain de sécurité fonctionnelle – Spécifications supplémentaires pour CPF 6*

IEC 61784-3-8, *Industrial communication networks – Profiles – Part 3-8: Functional safety fieldbuses – Additional specifications for CPF 8* (disponible en anglais seulement)

IEC 61784-3-12, *Réseaux de communication industriels – Profils – Partie 3-12: Bus de terrain de sécurité fonctionnelle – Spécifications supplémentaires pour CPF 12*

IEC 61784-3-13, *Réseaux de communication industriels – Profils – Partie 3-13: Bus de terrain de sécurité fonctionnelle – Spécifications supplémentaires pour CPF 13*

IEC 61784-3-14, *Réseaux de communication industriels – Profils – Partie 3-14: Bus de terrain de sécurité fonctionnelle – Spécifications supplémentaires pour CPF 14*

IEC 61784-3-17[4], *Réseaux de communication industriels – Profils – Partie 3-17: Bus de terrain de sécurité fonctionnelle – Spécifications supplémentaires pour CPF 17*

IEC 61784-3-18, *Réseaux de communication industriels – Profils – Partie 3-18: Bus de terrain de sécurité fonctionnelle – Spécifications supplémentaires pour CPF 18*

IEC 61784-5 (toutes les parties), *Réseaux de communication industriels – Profils – Partie 5: Installation des bus de terrain*

IEC 61918:2013, *Réseaux de communication industriels – Installation de réseaux de communication dans des locaux industriels*

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

4 A publier