



IEC 61784-3

Edition 4.0 2021-02

INTERNATIONAL STANDARD

NORME INTERNATIONALE



**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**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 25.040.40; 35.100.05

ISBN 978-2-8322-9268-6

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

CONTENTS

FOREWORD.....	7
0 Introduction	9
0.1 General.....	9
0.2 Use of extended assessment methods in Edition 4.....	11
0.3 Patent declaration.....	11
1 Scope.....	12
2 Normative references	12
3 Terms, definitions, symbols, abbreviated terms and conventions	14
3.1 Terms and definitions.....	14
3.2 Symbols and abbreviated terms	21
3.2.1 Abbreviated terms	21
3.2.2 Symbols	22
4 Conformance.....	22
5 Basics of safety-related fieldbus systems	23
5.1 Safety function decomposition	23
5.2 Communication system	23
5.2.1 General	23
5.2.2 IEC 61158 fieldbuses.....	24
5.2.3 Communication channel types	24
5.2.4 Safety function response time.....	25
5.3 Communication errors	25
5.3.1 General	25
5.3.2 Corruption	25
5.3.3 Unintended repetition	26
5.3.4 Incorrect sequence	26
5.3.5 Loss	26
5.3.6 Unacceptable delay	26
5.3.7 Insertion	26
5.3.8 Masquerade.....	26
5.3.9 Addressing	26
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	27
5.4.5 Connection authentication	27
5.4.6 Feedback message.....	27
5.4.7 Data integrity assurance	27
5.4.8 Redundancy with cross checking	28
5.4.9 Different data integrity assurance systems.....	28
5.5 Typical relationships between errors and safety measures.....	28
5.6 Communication phases	29
5.7 FSCP implementation aspects	30
5.8 Models for estimation of the total residual error rate	30
5.8.1 Applicability	30
5.8.2 General models for black channel communications.....	31

5.8.3	Identification of generic safety properties.....	31
5.8.4	Assumptions for residual error rate calculations.....	32
5.8.5	Residual error rates	33
5.8.6	Data integrity.....	35
5.8.7	Authenticity.....	36
5.8.8	Timeliness	38
5.8.9	Masquerade.....	41
5.8.10	Calculation of the total residual error rates	41
5.8.11	Total residual error rate and SIL	43
5.8.12	Configuration and parameterization for an FSCP	43
5.9	Relationship between functional safety and security	45
5.10	Boundary conditions and constraints.....	45
5.10.1	Electrical safety	45
5.10.2	Electromagnetic compatibility (EMC)	46
5.11	Installation guidelines	46
5.12	Safety manual.....	46
5.13	Safety policy	46
6	Communication Profile Family 1 (FOUNDATION™ Fieldbus) – Profiles for functional safety	47
7	Communication Profile Family 2 (CIP™) and Family 16 (SERCOS®) – Profiles for functional safety	47
8	Communication Profile Family 3 (PROFIBUS™, PROFINET™) – Profiles for functional safety	48
9	Communication Profile Family 6 (INTERBUS®) – Profiles for functional safety	48
10	Communication Profile Family 8 (CC-Link™) – Profiles for functional safety	49
10.1	Functional Safety Communication Profile 8/1	49
10.2	Functional Safety Communication Profile 8/2	49
11	Communication Profile Family 12 (EtherCAT™) – Profiles for functional safety.....	49
12	Communication Profile Family 13 (Ethernet POWERLINK™) – Profiles for functional safety	50
13	Communication Profile Family 14 (EPA®) – Profiles for functional safety.....	50
14	Communication Profile Family 17 (RAPIEnet™) – Profiles for functional safety.....	50
15	Communication Profile Family 18 (SafetyNET p™ Fieldbus) – Profiles for functional safety	51
Annex A (informative)	Example functional safety communication models	52
A.1	General.....	52
A.2	Model A (single message, channel and FAL, redundant SCLs).....	52
A.3	Model B (full redundancy)	52
A.4	Model C (redundant messages, FALs and SCLs, single channel).....	53
A.5	Model D (redundant messages and SCLs, single channel and FAL).....	53
Annex B (normative)	Safety communication channel model using CRC-based error checking	55
B.1	Overview.....	55
B.2	Channel model for calculations	55
B.3	Bit error probability P_e	56
B.4	Cyclic redundancy checking.....	57
B.4.1	General	57
B.4.2	Requirements for methods to calculate R_{CRC}	57
Annex C (informative)	Structure of technology-specific parts.....	59

Annex D (informative) Assessment guideline	62
D.1 Overview.....	62
D.2 Channel types.....	62
D.2.1 General	62
D.2.2 Black channel.....	62
D.2.3 White channel.....	62
D.3 Data integrity considerations for white channel approaches	63
D.3.1 General	63
D.3.2 Models B and C	63
D.3.3 Models A and D	64
D.4 Verification of safety measures	64
D.4.1 General	64
D.4.2 Implementation.....	65
D.4.3 Default safety action	65
D.4.4 Safe state	65
D.4.5 Transmission errors	65
D.4.6 Safety reaction and response times	65
D.4.7 Combination of measures	65
D.4.8 Absence of interference.....	66
D.4.9 Additional fault causes (white channel).....	66
D.4.10 Reference test beds and operational conditions.....	66
D.4.11 Conformance tester	66
Annex E (informative) Examples of implicit vs. explicit FSCP safety measures.....	67
E.1 General.....	67
E.2 Example fieldbus message with safety PDUs	67
E.3 Model with completely explicit safety measures	67
E.4 Model with explicit A-code and implicit T-code safety measures.....	68
E.5 Model with explicit T-code and implicit A-code safety measures.....	68
E.6 Model with split explicit and implicit safety measures	69
E.7 Model with completely implicit safety measures	70
E.8 Addition to Annex B – impact of implicit codes on properness	70
Annex F (informative) Legacy models for estimation of the total residual error rate	71
F.1 General.....	71
F.2 Calculation of the residual error rate	71
F.3 Total residual error rate and SIL	73
Annex G (informative) Implicit data safety mechanisms for IEC 61784-3 functional safety communication profiles (FSCPs).....	74
G.1 Overview.....	74
G.2 Basic principles.....	74
G.3 Problem statement: constant values for implicit data	75
G.4 RP for FSCPs with random, uniformly distributed err_{impl}	78
G.4.1 General	78
G.4.2 Uniform distribution within the interval $[0;2^i-1]$, $i \geq r$	79
G.4.3 Uniform distribution in the interval $[1;2^r-1]$, $i = r$	81
G.5 General case	83
G.6 Calculation of P_{ID}	83
Annex H (informative) Residual error probability for example CRC codes (tables for verification of calculation methods).....	85
H.1 Overview.....	85

H.2	Example of a 32-bit CRC.....	85
H.3	Example of a 16-bit CRC.....	90
H.4	Conclusion.....	94
	Bibliography.....	96
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	– Transitions from Ed. 2 to Ed. 4 and future Ed. 5 assessment methods.....	11
Figure 4	– Safety communication as a part of a safety function.....	23
Figure 5	– Example model of a functional safety communication system.....	24
Figure 6	– Example of safety function response time components.....	25
Figure 7	– Conceptual FSCP protocol model.....	30
Figure 8	– FSCP implementation aspects.....	30
Figure 9	– Black channel from an FSCP perspective.....	31
Figure 10	– Model for authentication considerations.....	36
Figure 11	– Fieldbus and internal address errors.....	37
Figure 12	– Example of slowly increasing message latency.....	39
Figure 13	– Example of an active network element failure.....	40
Figure 14	– Example application 1 (m = 4).....	42
Figure 15	– Example application 2 (m = 2).....	42
Figure 16	– Example of configuration and parameterization procedures for FSCP.....	44
Figure A.1	– Model A.....	52
Figure A.2	– Model B.....	53
Figure A.3	– Model C.....	53
Figure A.4	– Model D.....	54
Figure B.1	– Binary symmetric channel (BSC).....	55
Figure B.2	– Block codes for error detection.....	56
Figure B.3	– Example of a block with a message part and a CRC signature.....	57
Figure B.4	– Proper and improper CRC polynomials.....	58
Figure D.1	– Basic Markov model.....	64
Figure E.1	– Example safety PDUs embedded in a fieldbus message.....	67
Figure E.2	– Model with completely explicit safety measures.....	67
Figure E.3	– Model with explicit A-code and implicit T-code safety measures.....	68
Figure E.4	– Model with explicit T-code and implicit A-code safety measures.....	69
Figure E.5	– Model with split explicit and implicit safety measures.....	69
Figure E.6	– Model with completely implicit safety measures.....	70
Figure F.1	– Example application 1 (m = 4).....	72
Figure F.2	– Example application 2 (m = 2).....	73
Figure G.1	– FSCP with implicit transmission of authenticity and/or timeliness codes.....	75
Figure G.2	– Example of an incorrect transmission with multiple error causes.....	76
Figure G.3	– Impact of errors in implicit data on the residual error probability.....	77
Figure H.1	– Residual error probabilities (example of a 32-bit CRC – result 1).....	87
Figure H.2	– Residual error probabilities (example of a 32-bit CRC – result 2).....	87

Figure H.3 – Residual error probabilities (example of a 32-bit CRC – result 3)	88
Figure H.4 – Residual error probabilities (example of a 32-bit CRC – result 4)	88
Figure H.5 – Residual error probabilities (example of a 32-bit CRC – result 5)	89
Figure H.6 – Residual error probabilities (example of a 32-bit CRC – result 6)	89
Figure H.7 – Residual error probabilities (example of a 16-bit CRC – result 1)	92
Figure H.8 – Residual error probabilities (example of a 16-bit CRC – result 2)	92
Figure H.9 – Residual error probabilities (example of a 16-bit CRC – result 3)	93
Figure H.10 – Residual error probabilities (example of a 16-bit CRC – result 4)	93
Figure H.11 – Residual error probabilities (example of a 16-bit CRC – result 5)	94
Figure H.12 – Example 1 of improper polynomial	94
Figure H.13 – Example 2 of improper polynomial	95
Table 1 – Overview of the effectiveness of the various measures on the possible errors	29
Table 2 – Typical relationship of residual error rate to SIL	43
Table 3 – Typical relationship of residual error on demand to SIL	43
Table 4 – Overview of profile identifier usable for FSCP 6/7	48
Table B.1 – Example dependency d_{\min} and block bit length n	56
Table C.1 – Common subclause structure for technology-specific parts	59
Table F.1 – Definition of items used for calculation of the residual error rates	72
Table F.2 – Typical relationship of residual error rate to SIL	73
Table F.3 – Typical relationship of residual error on demand to SIL	73
Table H.1 – Residual error probabilities (R_{CRC1}) for example CRC32 polynomial	86
Table H.2 – Residual error probabilities (R_{CRC2}) for example CRC16 polynomial	91

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

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 fourth edition cancels and replaces the third edition, published in 2016 and its Amendment 1, published in 2017. This edition constitutes a technical revision.

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

- Contents of previous Annex F were corrected based on feedback from peer review and subsequent analysis (in particular deletion of RP_U for data integrity, reduction of the Equation for RR_A , and clarifications on the values of RP_I and R_T).
- Additional assumptions for residual error rate calculations, clarification of assumption a).

- After correction, contents of previous Annex F were exchanged with the contents of previous Subclause 5.8.
- Contents of Subclause 5.9 on security replaced by a simple reference to IEC 62443 in accordance with Guide 120.
- Changes in Annex B: Dependency of this Annex B with the BSC model has been highlighted. First two paragraphs and figure in Clause B.2 have been deleted because of little relevance. The approximation Equation (B.4) has been deleted due to obsolescence, based on the observations that the CRC shall be anyway explicitly calculated in order to prove properness, and that it may produce optimistic results. Guidance for calculation of R_{CRC} in B.4.2 has been reviewed.
- Changes in Annex D: Formula D.1 was changed from an approximation to a proper Equation, with some adjustments, and contents of D.4.3 were clarified (default safety action).
- New informative Annex H, providing additional guidance for the calculation of RCRC.

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

FDIS	Report on voting
65C/1067/FDIS	65C/1072/RVD

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

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

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

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

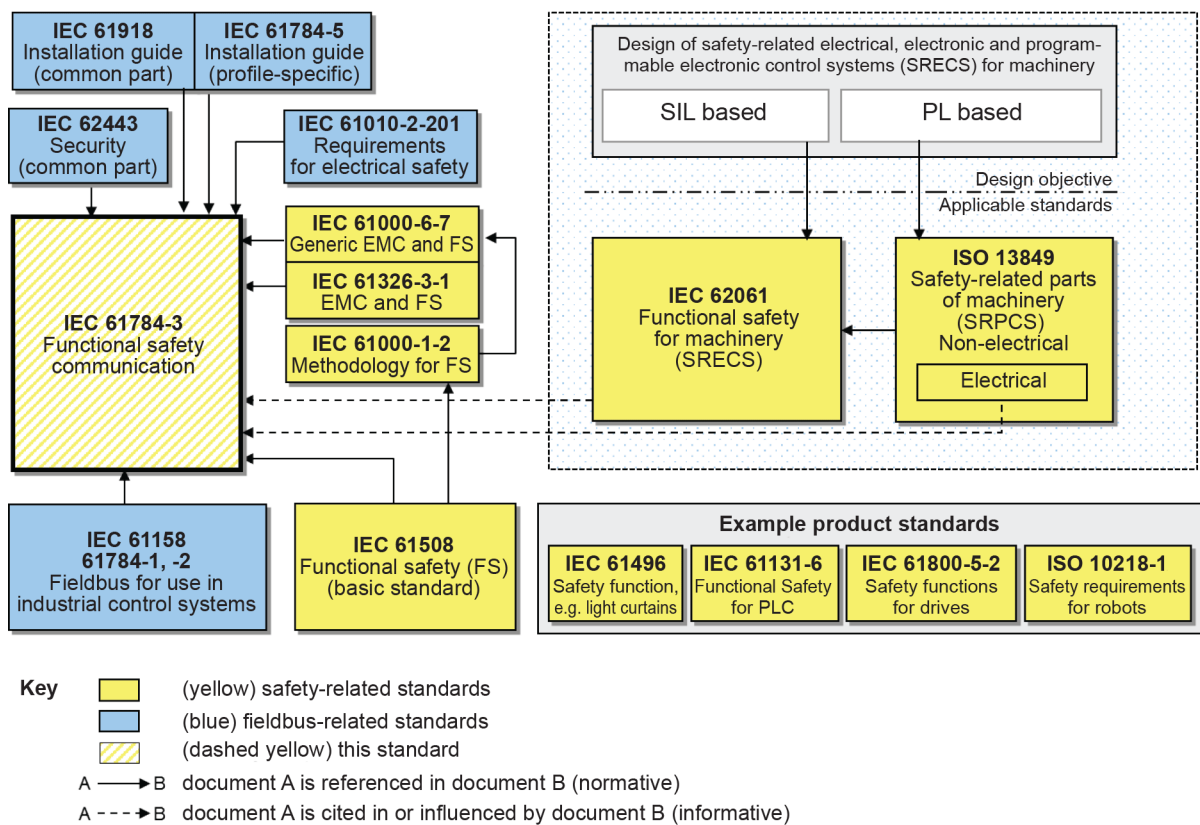
0 Introduction

0.1 General

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

IEC 61784-3 (all parts) explains the relevant principles for functional safety communications with reference to IEC 61508 (all parts) and specifies several safety communication layers (profiles and corresponding protocols) based on the communication profiles and protocol layers of IEC 61784-1, IEC 61784-2 and IEC 61158 (all parts). It does not cover electrical safety and intrinsic safety aspects. It also does not cover security aspects, nor does it provide any requirements for security.

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

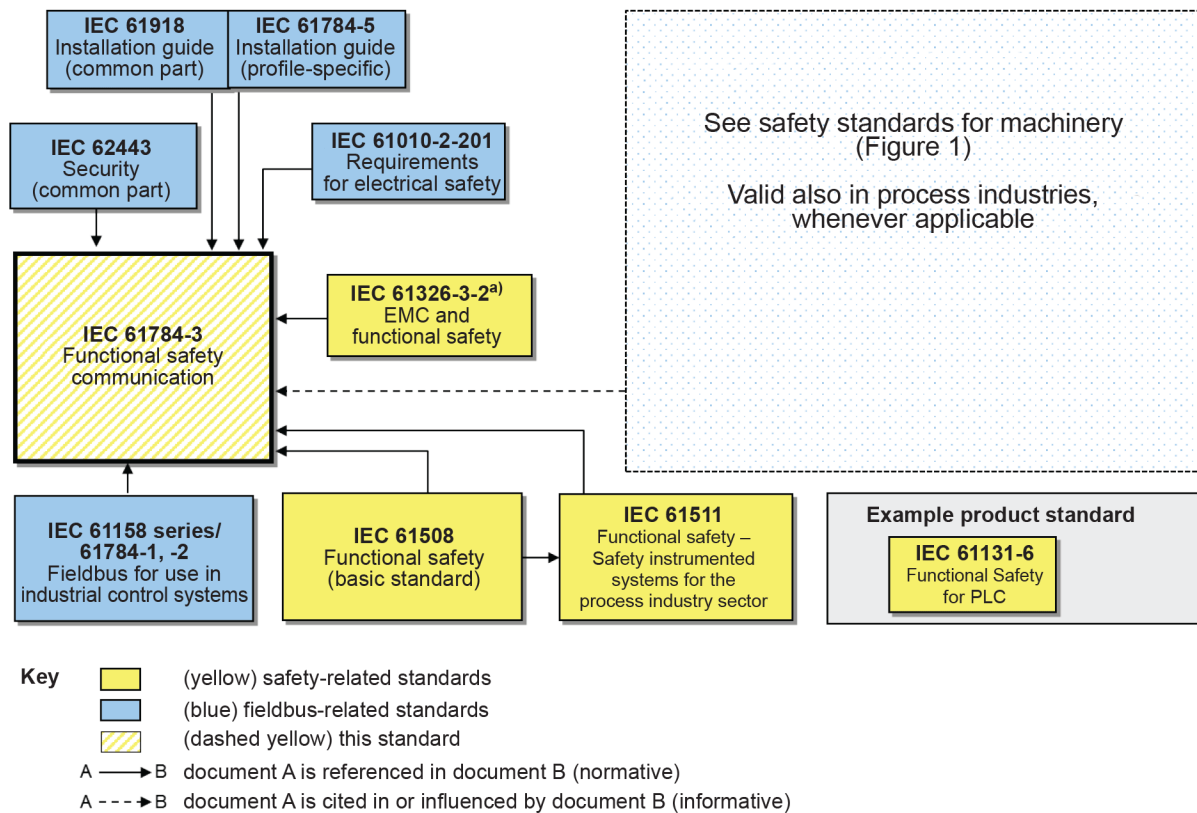


IEC

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

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

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



IEC

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

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

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

Safety communication layers specified in IEC 61784-3 (all parts) do this in such a way that a fieldbus can be used for applications requiring functional safety up to the Safety Integrity Level (SIL) specified by its corresponding functional safety communication profile.

The resulting SIL claim of a system depends on the implementation of the selected functional safety communication profile (FSCP) within this system – implementation of a functional safety communication profile in a standard device is not sufficient to qualify it as a safety device.

IEC 61784-3 (all parts) describes:

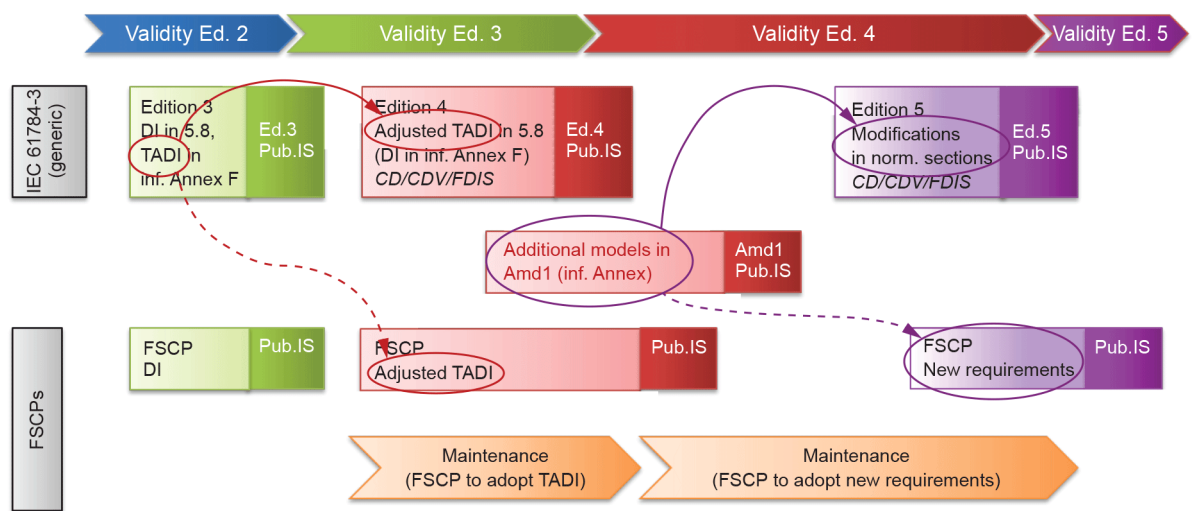
- basic principles for implementing the requirements of IEC 61508 (all parts) for safety-related data communications, including possible transmission faults, remedial measures and considerations affecting data integrity;
- functional safety communication profiles for several communication profile families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

0.2 Use of extended assessment methods in Edition 4

This edition of the generic part of IEC 61784-3 (all parts) includes extended models for 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 5.8.

Upon publication of this new edition of the generic part, FSCPs shall be assessed using the methods from this Edition 4, based on the extended models specified in 5.8 (derived from a modified version of Annex F of Edition 3). The informative Annex F contains the legacy models for reference purpose only.

Figure 3 shows the transitions from original assessment methods of Edition 2 to extended assessment methods in this Edition 4 and the future Edition 5.



IEC

Key

DI Data Integrity

TADI Timeliness, Authenticity, Data Integrity

Figure 3 – Transitions from Ed. 2 to Ed. 4 and future Ed. 5 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 IEC that they are willing to negotiate licences under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statements of the holders of these patent rights are registered with IEC. Information may be obtained from the patent database available at <http://patents.iec.ch>.

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

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES –

Part 3: 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 (all parts)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 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 IEC 61158 (all parts). 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 (all parts) can exist that are not included in IEC 61784-3 (all parts).

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. IEC 62443 (all parts) will address many of these issues; the relationship with IEC 62443 (all parts) is detailed in a dedicated subclause of this document.

NOTE 3 Implementation of a functional safety communication profile according to this document in a device is not sufficient to qualify it as a safety device, as defined in IEC 61508 (all parts).

NOTE 4 The resulting SIL claim of a system depends on the implementation of the selected functional safety communication profile within this system.

NOTE 5 Annex C explains the numbering scheme used for the technology-specific parts (IEC 61784-3-x) as well as their common general structure.

NOTE 6 Annex D provides a guideline for the assessment and test of safety communication profiles as well as safety-related devices using these profiles.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 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 document, “IEC 61508” will be used for “IEC 61508 (all parts)”.

IEC 61010-2-201, *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/IEEE 8802-3*

IEC 61784-3 (all parts), *Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses*

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

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

SOMMAIRE

AVANT-PROPOS	108
0 Introduction	110
0.1 Généralités	110
0.2 Utilisation des méthodes d'évaluation étendue de l'édition 4	112
0.3 Déclaration de brevet.....	113
1 Domaine d'application	114
2 Références normatives	115
3 Termes, définitions, symboles, abréviations et conventions	116
3.1 Termes et définitions	116
3.2 Symboles et termes abrégés.....	124
3.2.1 Termes abrégés.....	124
3.2.2 Symboles.....	125
4 Conformité.....	126
5 Principes des systèmes de bus de terrain relatifs à la sécurité	126
5.1 Décomposition d'une fonction de sécurité	126
5.2 Système de communication	127
5.2.1 Généralités	127
5.2.2 Bus de terrain définis dans l'IEC 61158	127
5.2.3 Types de canaux de communication	128
5.2.4 Temps de réponse de la fonction de sécurité	128
5.3 Erreurs de communication	129
5.3.1 Généralités	129
5.3.2 Corruption	129
5.3.3 Répétition non prévue.....	129
5.3.4 Séquence incorrecte.....	130
5.3.5 Perte	130
5.3.6 Retard inacceptable.....	130
5.3.7 Insertion	130
5.3.8 Déguisement	130
5.3.9 Adressage	130
5.4 Mesures correctives déterministes	130
5.4.1 Généralités	130
5.4.2 Numéro de séquence.....	131
5.4.3 Horodatage.....	131
5.4.4 Délai.....	131
5.4.5 Authentification de connexion	131
5.4.6 Message en retour.....	131
5.4.7 Assurance d'intégrité des données	131
5.4.8 Redondance avec contre-vérification	132
5.4.9 Différents systèmes d'assurance d'intégrité des données	132
5.5 Relations types entre les erreurs et les mesures de sécurité.....	132
5.6 Phases de communication	133
5.7 Aspects relatifs à la mise en œuvre du FSCP	134
5.8 Modèles pour l'estimation du taux total d'erreurs résiduelles	135
5.8.1 Applicabilité.....	135
5.8.2 Modèles généraux pour les communications du canal noir.....	135

5.8.3	Identification des propriétés de sécurité générique	136
5.8.4	Hypothèses pour les calculs de taux d'erreurs résiduelles	136
5.8.5	Taux d'erreurs résiduelles.....	137
5.8.6	Intégrité des données	139
5.8.7	Authenticité	140
5.8.8	Opportunité	143
5.8.9	Déguisement	146
5.8.10	Calcul des taux totaux d'erreurs résiduelles.....	146
5.8.11	Taux total d'erreurs résiduelles et SIL.....	148
5.8.12	Configuration et paramétrage pour un FSCP	149
5.9	Relation entre sécurité fonctionnelle et sûreté.....	150
5.10	Conditions aux limites et contraintes	151
5.10.1	Sécurité électrique.....	151
5.10.2	Compatibilité électromagnétique (CEM).....	151
5.11	Guides d'installation.....	151
5.12	Manuel de sécurité.....	151
5.13	Politique de sécurité	151
6	Famille de profils de communication 1 (Fieldbus FOUNDATION™) – Profils de sécurité fonctionnelle.....	152
7	Famille de profils de communication 2 (CIP™) et Famille 16 (SERCOS®) – Profils de sécurité fonctionnelle.....	153
8	Famille de profils de communication 3 (PROFIBUS™, PROFINET™) – Profils de sécurité fonctionnelle.....	153
9	Famille de profils de communication 6 (INTERBUS®) – Profils de sécurité fonctionnelle.....	154
10	Famille de profils de communication 8 (CC-Link™) – Profils de sécurité fonctionnelle.....	154
10.1	Profil de communication de sécurité fonctionnelle 8/1	154
10.2	Profil de communication de sécurité fonctionnelle 8/2	155
11	Famille de profils de communication 12 (EtherCAT™) – Profils de sécurité fonctionnelle.....	155
12	Famille de profils de communication 13 (Ethernet POWERLINK™) – Profils de sécurité fonctionnelle.....	155
13	Famille de profils de communication 14 (EPA®) – Profils de sécurité fonctionnelle.....	156
14	Famille de profils de communication 17 (RAPIenet™) – Profils de sécurité fonctionnelle.....	156
15	Famille de profils de communication 18 (Fieldbus SafetyNET p™) – Profils de sécurité fonctionnelle.....	156
Annexe A (informative) Exemple de modèles de communication de sécurité fonctionnelle		157
A.1	Généralités	157
A.2	Modèle A (message unique, canal et FAL, SCL redondantes)	157
A.3	Modèle B (redondance complète).....	157
A.4	Modèle C (messages redondants, FAL et SCL, canal unique)	158
A.5	Modèle D (messages redondants et SCL, canal unique et FAL)	158
Annexe B (normative) Modèle de canal de communication de sécurité qui utilise le contrôle d'erreurs CRC		160
B.1	Vue d'ensemble	160
B.2	Modèle de canal pour calculs.....	160
B.3	Probabilité d'erreurs sur les éléments binaires P_e	162

B.4	Contrôle de redondance cyclique	162
B.4.1	Généralités	162
B.4.2	Exigences relatives aux méthodes de calcul de R_{CRC}	163
Annexe C (informative) Structure des parties spécifiques à la technologie		165
Annexe D (informative) Lignes directrices pour l'évaluation		168
D.1	Vue d'ensemble	168
D.2	Types de canaux.....	168
D.2.1	Généralités	168
D.2.2	Canal noir.....	168
D.2.3	Canal blanc	169
D.3	Considérations relatives à l'intégrité des données pour les méthodes du canal blanc	169
D.3.1	Généralités	169
D.3.2	Modèles B et C	169
D.3.3	Modèles A et D	170
D.4	Vérification des mesures de sécurité.....	171
D.4.1	Généralités	171
D.4.2	Mise en œuvre.....	171
D.4.3	Action de sécurité par défaut	171
D.4.4	Etat de sécurité	171
D.4.5	Erreurs de transmission.....	171
D.4.6	Réaction de sécurité et temps de réponse	172
D.4.7	Combinaison des mesures.....	172
D.4.8	Absence de perturbations	172
D.4.9	Causes d'anomalies supplémentaires (canal blanc)	172
D.4.10	Bancs d'essai de référence et conditions de fonctionnement	172
D.4.11	Appareil de vérification de conformité	173
Annexe E (informative) Exemples de mesures de sécurité de FSCP implicites et explicites		174
E.1	Généralités	174
E.2	Exemple de message de bus de terrain avec PDU de sécurité.....	174
E.3	Modèle avec mesures de sécurité totalement explicites	174
E.4	Modèle avec mesures de sécurité explicites de code A et implicites de code T	175
E.5	Modèle avec mesures de sécurité explicites de code T et implicites de code A	176
E.6	Modèle avec mesures de sécurité explicites et implicites divisées	176
E.7	Modèle avec mesures de sécurité totalement implicites	177
E.8	Ajout à l'Annexe B – Influence des codes implicites sur l'exactitude.....	178
Annexe F (informative) Anciens modèles pour l'estimation du taux total d'erreurs résiduelles		179
F.1	Généralités	179
F.2	Calcul du taux d'erreurs résiduelles	179
F.3	Taux total d'erreurs résiduelles et SIL	181
Annexe G (informative) Mécanismes de sécurité qui reposent sur des données implicites pour les profils de communication de sécurité fonctionnelle (FSCP) définis dans l'IEC 617843.....		182
G.1	Vue d'ensemble	182
G.2	Principes de base	182
G.3	Enoncé du problème: valeurs constantes pour les données implicites	184

G.4	RP pour les FSCP avec une variable err_{impl} aléatoire et uniformément répartie	186
G.4.1	Généralités	186
G.4.2	Répartition uniforme dans l'intervalle $[0;2^i-1]$, $i \geq r$	187
G.4.3	Répartition uniforme dans l'intervalle $[1;2^r-1]$, $i = r$	189
G.5	Cas général	191
G.6	Calcul de P_{ID}	192
Annexe H (informative) Probabilité d'erreurs résiduelles pour des exemples de codes CRC (tableaux de vérification des méthodes de calcul)		194
H.1	Vue d'ensemble	194
H.2	Exemple de CRC de 32 bits	194
H.3	Exemple de CRC de 16 bits	199
H.4	Conclusion	203
Bibliographie		205
Figure 1	– Relations entre l'IEC 61784-3 et d'autres normes (machines)	110
Figure 2	– Relations entre l'IEC 61784-3 et d'autres normes (transformation)	111
Figure 3	– Transitions des méthodes d'évaluation de l'édition 2 à l'édition 4 puis à la future édition 5	112
Figure 4	– Communication de sécurité comme partie intégrante d'une fonction de sécurité	127
Figure 5	– Exemple de modèle d'un système de communication de sécurité fonctionnelle	128
Figure 6	– Exemple des composantes du temps de réponse de la fonction de sécurité	129
Figure 7	– Modèle de protocole FSCP conceptuel	134
Figure 8	– Aspects relatifs à la mise en œuvre du FSCP	134
Figure 9	– Canal noir du point de vue d'un FSCP	135
Figure 10	– Modèle pour la prise en compte de l'authentification	141
Figure 11	– Bus de terrain et erreurs d'adresse internes	142
Figure 12	– Exemple de latence de message en croissance progressive	144
Figure 13	– Exemple de défaillance d'un élément de réseau actif	145
Figure 14	– Exemple d'application 1 ($m = 4$)	147
Figure 15	– Exemple d'application 2 ($m = 2$)	147
Figure 16	– Exemple de procédures de configuration et de paramétrage pour FSCP	149
Figure A.1	– Modèle A	157
Figure A.2	– Modèle B	158
Figure A.3	– Modèle C	158
Figure A.4	– Modèle D	159
Figure B.1	– Canal symétrique binaire (BSC)	160
Figure B.2	– Codes de blocs pour la détection d'erreurs	161
Figure B.3	– Exemple de bloc avec une partie message et une signature CRC	163
Figure B.4	– Polynômes CRC appropriés et inappropriés	164
Figure D.1	– Modèle de Markov de base	170
Figure E.1	– Exemple de PDU de sécurité intégrés à un message de bus de terrain	174
Figure E.2	– Modèle avec mesures de sécurité totalement explicites	174

Figure E.3 – Modèle avec mesures de sécurité explicites de code A et mesures de sécurité implicites de code T	175
Figure E.4 – Modèle avec mesures de sécurité explicites de code T et mesures de sécurité implicites de code A	176
Figure E.5 – Modèle avec mesures de sécurité explicites et implicites divisées	177
Figure E.6 – Modèle avec mesures de sécurité totalement implicites	177
Figure F.1 – Exemple d'application 1 (m = 4)	180
Figure F.2 – Exemple d'application 2 (m = 2)	181
Figure G.1 – FSCP à transmission implicite de codes d'authenticité et/ou d'opportunité.....	183
Figure G.2 – Exemple de transmission incorrecte due à des causes d'erreur multiples	184
Figure G.3 – Influence des erreurs dans les données implicites sur la probabilité d'erreurs résiduelles	185
Figure H.1 – Probabilités d'erreurs résiduelles (exemple de CRC de 32 bits – résultat 1)	196
Figure H.2 – Probabilités d'erreurs résiduelles (exemple de CRC de 32 bits – résultat 2)	196
Figure H.3 – Probabilités d'erreurs résiduelles (exemple de CRC de 32 bits – résultat 3)	197
Figure H.4 – Probabilités d'erreurs résiduelles (exemple de CRC de 32 bits – résultat 4)	197
Figure H.5 – Probabilités d'erreurs résiduelles (exemple de CRC de 32 bits – résultat 5)	198
Figure H.6 – Probabilités d'erreurs résiduelles (exemple de CRC de 32 bits – résultat 6)	198
Figure H.7 – Probabilités d'erreurs résiduelles (exemple de CRC de 16 bits – résultat 1)	201
Figure H.8 – Probabilités d'erreurs résiduelles (exemple de CRC de 16 bits – résultat 2)	201
Figure H.9 – Probabilités d'erreurs résiduelles (exemple de CRC de 16 bits – résultat 3)	202
Figure H.10 – Probabilités d'erreurs résiduelles (exemple de CRC de 16 bits – résultat 4)	202
Figure H.11 – Probabilités d'erreurs résiduelles (exemple de CRC de 16 bits – résultat 5)	203
Figure H.12 – Exemple 1 de polynôme inapproprié	204
Figure H.13 – Exemple 2 de polynôme inapproprié	204
Tableau 1 – Présentation générale de l'efficacité des différentes mesures sur les erreurs possibles	133
Tableau 2 – Relation type entre le taux d'erreurs résiduelles et le SIL	148
Tableau 3 – Relation type entre l'erreur résiduelle et le SIL	148
Tableau 4 – Présentation générale de l'identifiant de profil applicable au protocole FSCP 6/7	154
Tableau B.1 – Exemple de dépendance d_{min} et longueur binaire de bloc n	161
Tableau C.1 – Structure commune des paragraphes pour les parties spécifiques à la technologie	165

Tableau F.1 – Définition des éléments utilisés pour le calcul des taux d'erreurs résiduelles	180
Tableau F.2 – Relation type entre le taux d'erreurs résiduelles et le SIL	181
Tableau F.3 – Relation type entre l'erreur résiduelle et le SIL	181
Tableau H.1 – Probabilités d'erreurs résiduelles (R_{CRC1}) pour l'exemple de polynôme CRC32.....	195
Tableau H.2 – Probabilités d'erreurs résiduelles (R_{CRC2}) pour l'exemple de polynôme CRC16.....	200

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.
- 9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

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 quatrième édition annule et remplace la troisième édition parue en 2016 et son Amendement 1 paru en 2017. Cette édition constitue une révision technique.

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

- rectification du contenu de la précédente Annexe F sur la base des commentaires reçus après examen des pairs et des analyses ultérieures (en particulier, suppression de RP_U pour l'intégrité des données, réduction de l'équation pour RR_A , et clarifications concernant les valeurs de RP_I et R_T);
- hypothèses supplémentaires pour les calculs de taux d'erreurs résiduelles, clarification de l'hypothèse a);
- après rectification, échange du contenu de la précédente Annexe F avec le contenu du précédent Paragraphe 5.8;
- remplacement du contenu du Paragraphe 5.9 relatif à la sûreté par une simple référence à l'IEC 62443, conformément au Guide 120;
- modifications de l'Annexe B: mise en évidence de la dépendance de cette Annexe B au modèle BSC; suppression des deux premiers alinéas et de la figure à l'Article B.2 en raison de leur manque de pertinence; suppression de l'approximation de l'Equation B.4 en raison de son obsolescence, sur la base des observations qui indiquent que le CRC doit dans tous les cas être explicitement calculé afin de démontrer son exactitude, et qu'il peut produire des résultats optimistes; révision des recommandations pour le calcul de R_{CRC} en B.4.2;
- modifications de l'Annexe D: remplacement de l'approximation de la Formule D.1 par une équation appropriée, avec quelques ajustements, et clarification du contenu du D.4.3 (action de sécurité par défaut);
- nouvelle Annexe H informative, qui fournit des recommandations supplémentaires pour le calcul de R_{CRC} .

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

FDIS	Rapport de vote
65C/1067/FDIS	65C/1072/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 internationale.

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

Ce document a été rédigé 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 ce document ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous "<http://webstore.iec.ch>" dans les données relatives au document recherché. A cette date, le document sera

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

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

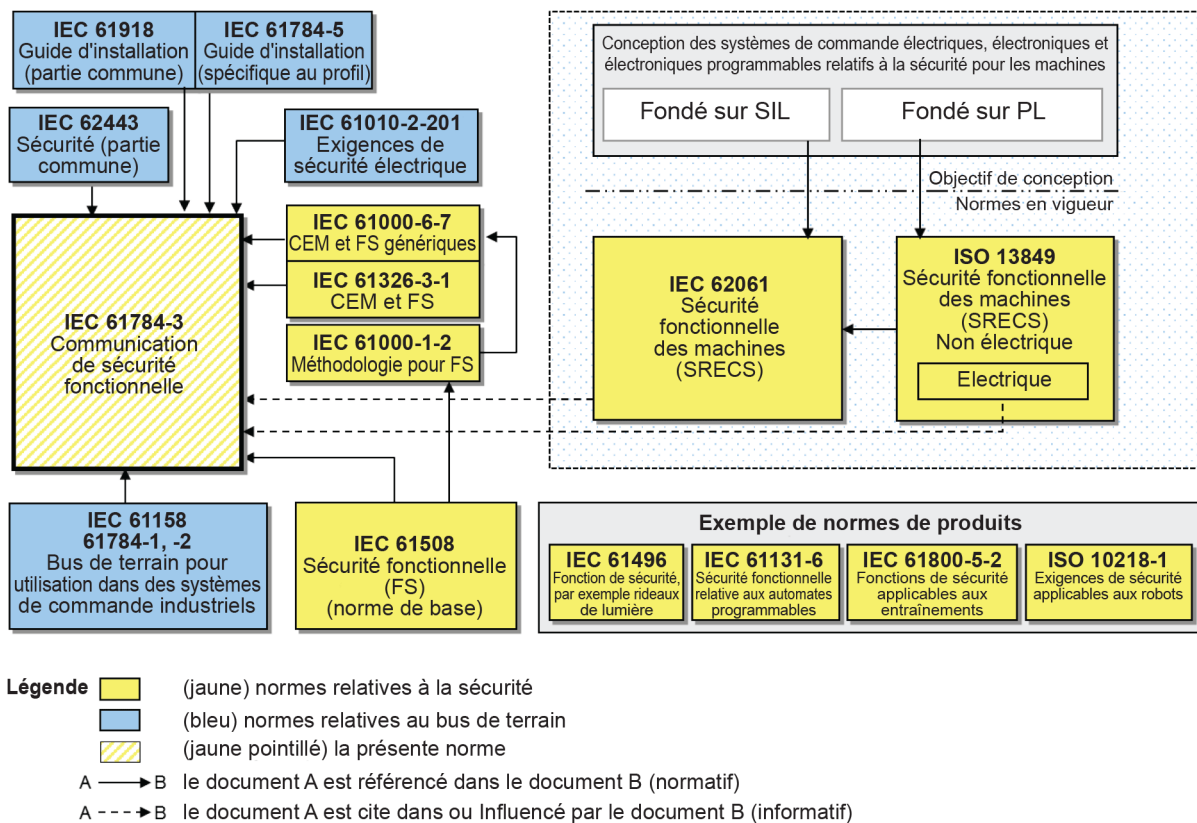
0 Introduction

0.1 Généralités

L'IEC 61158 (toutes les parties), relative aux bus de terrain, ainsi que ses normes associées IEC 61784-1 et IEC 61784-2, définissent un ensemble de protocoles de communication qui assurent la commande répartie d'applications automatisées. La technologie de bus de terrain est désormais reconnue et bien éprouvée. Les améliorations des bus de terrain se poursuivent; elles couvrent des applications pour des domaines comme les applications en temps réel relatives à la sécurité.

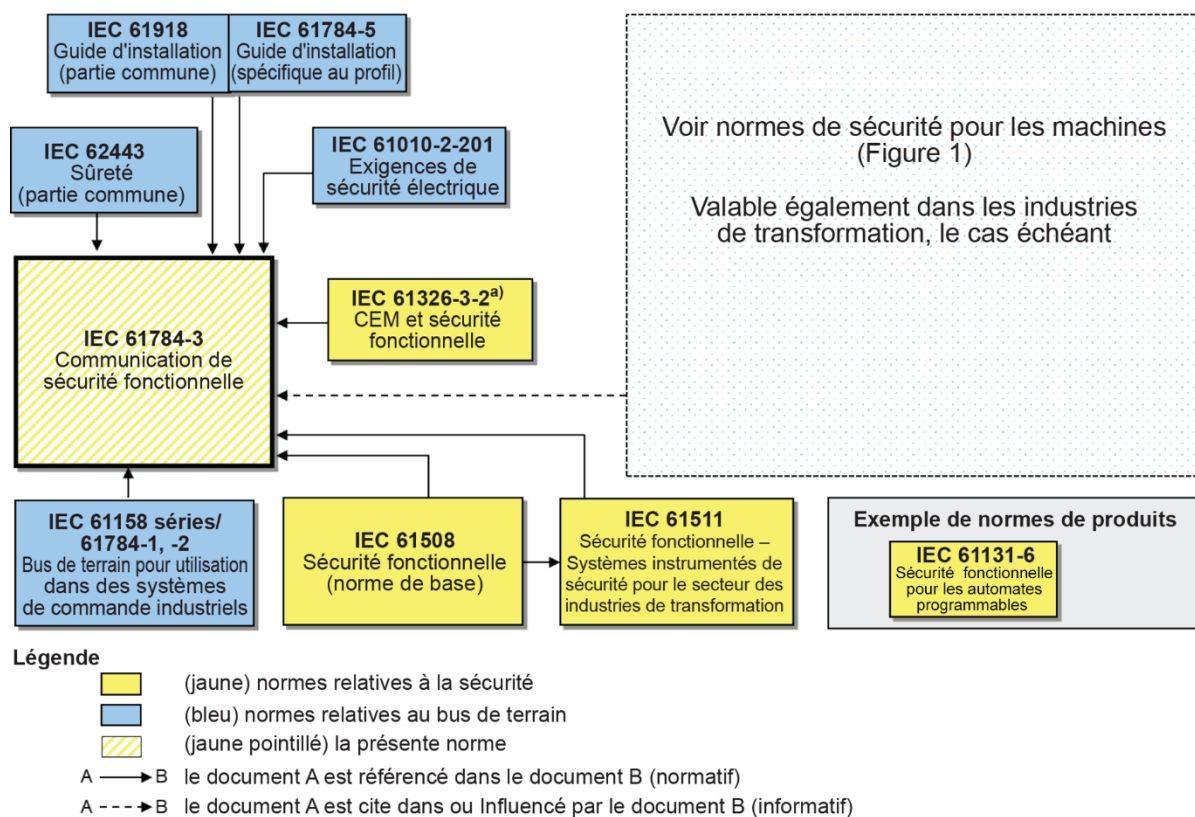
L'IEC 61784-3 (toutes les parties) définit les principes applicables aux communications de sécurité fonctionnelle en référence à l'IEC 61508 (toutes les parties); elle spécifie plusieurs couches de communication de sécurité (profils et protocoles correspondants) en fonction des profils de communication et des couches de protocole de l'IEC 61784-1, l'IEC 61784-2 et l'IEC 61158 (toutes les parties). Elle ne couvre pas les aspects relatifs à la sécurité électrique et à la sécurité intrinsèque. Elle ne couvre pas non plus les aspects relatifs à la sûreté et ne prévoit aucune exigence en matière de sûreté.

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



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

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



IEC

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

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

Les couches de communication de sécurité mises en œuvre dans le cadre de systèmes relatifs à la sécurité conformément à l'IEC 61508 (toutes les parties) assurent la confiance nécessaire à accorder à la transmission de messages (informations) entre plusieurs participants sur un bus de terrain dans un système relatif à la sécurité ou une fiabilité suffisante dans le comportement de sécurité en cas d'erreurs ou de défaillances du bus de terrain.

Les couches de communication de sécurité spécifiées dans l'IEC 61784-3 (toutes les parties) permettent de 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).

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

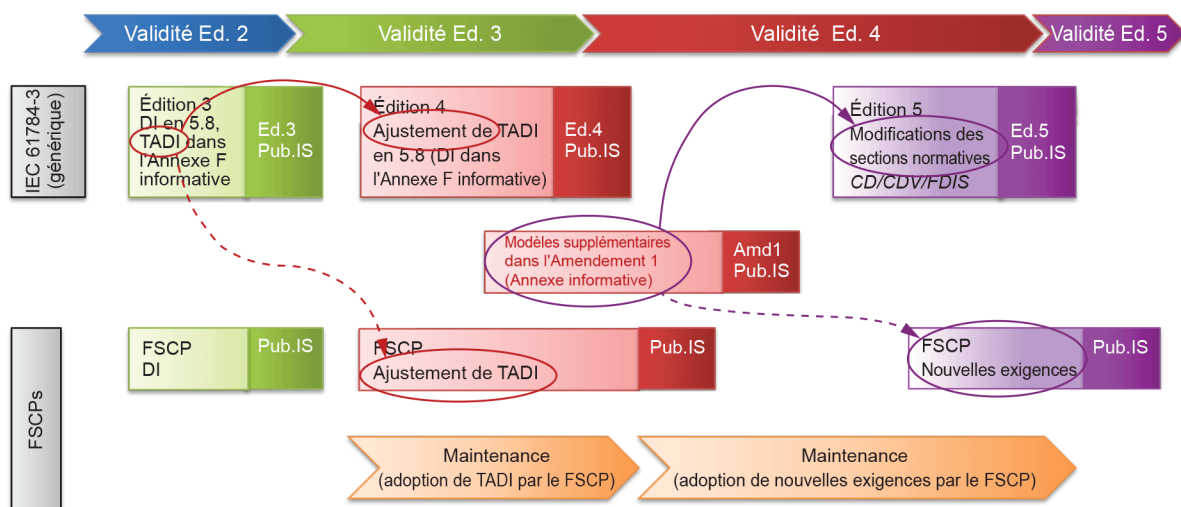
- les principes de base de la mise en œuvre des exigences de l'IEC 61508 (toutes les parties) pour les communications de données relatives à la sécurité, y compris les anomalies de transmission potentielles, les mesures correctives et des considérations relatives à l'intégrité des données;
- les profils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

0.2 Utilisation des méthodes d'évaluation étendue de l'édition 4

Cette édition de la partie générique de l'IEC 61784-3 (toutes les parties) 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 décrits à l'Annexe E et en 5.8.

Au moment de la publication de cette nouvelle édition de la partie générique, les FSCP doivent être évalués en fonction des méthodes de la présente édition 4, sur la base des modèles étendus spécifiés en 5.8 (extraits d'une version modifiée de l'Annexe F de l'édition 3). L'Annexe F informative présente les anciens modèles à des fins de référence uniquement.

La Figure 3 représente les transitions des méthodes d'évaluation d'origine de l'édition 2 aux méthodes d'évaluation étendue de la présente édition 4 puis à celles de la future édition 5.



IEC

Légende

DI Data Integrity (Intégrité des données)

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

Figure 3 – Transitions des méthodes d'évaluation de l'édition 2 à l'édition 4 puis à la future édition 5

0.3 Déclaration de brevet

La commission électrotechnique internationale (IEC) attire l'attention sur le fait qu'il est déclaré que la conformité avec les dispositions du présent document peut impliquer l'utilisation de brevets 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, à des termes et conditions raisonnables et non discriminatoires. A ce propos, les déclarations des détenteurs de ces droits de propriété sont enregistrés à l'IEC. Des informations peuvent être obtenues à partir de la base de données des brevets disponible à l'adresse <http://patents.iec.ch>.

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

RÉSEAUX DE COMMUNICATION INDUSTRIELS – PROFILS –

Partie 3: 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 l'IEC 61508 (toutes les parties)¹ sur la sécurité fonctionnelle. Ces principes s'appuient 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 et les parties IEC 61784-3-x spécifient plusieurs profils de communication de sécurité fonctionnelle fondés 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 l'IEC 61158 (toutes les parties). 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 l'IEC 61508 (toutes les parties) et ne sont pas inclus dans l'IEC 61784-3 (toutes les parties).

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. Il est nécessaire de prendre en compte des mesures supplémentaires dans une application relative à la sécurité afin de protéger les systèmes qui disposent de bus de terrain contre tout accès non autorisé. L'IEC 62443 (toutes les parties) traite bon nombre de ces questions; la relation avec l'IEC 62443 (toutes les parties) est décrite dans un paragraphe dédié du présent document.

NOTE 3 La mise en œuvre du profil de communication de sécurité fonctionnelle, conforme au présent document, dans un appareil normal ne suffit pas à le qualifier d'appareil de sécurité, comme défini dans l'IEC 61508 (toutes les parties).

NOTE 4 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.

NOTE 5 L'Annexe C explique le système de numérotation utilisé pour les parties spécifiques à la technologie (IEC 61784-3-x) ainsi que leur structure générale commune.

NOTE 6 L'Annexe D fournit des lignes directrices pour l'évaluation et les essais des profils de communication de sécurité et des appareils relatifs à la sécurité qui utilisent ces profils.

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

2 Références normatives

Les documents suivants sont cités dans le texte de sorte qu'ils constituent, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

IEC 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, *Exigences 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, *Industrial communication networks – Profiles – Part 1: Fieldbus profiles* (disponible en anglais seulement)

IEC 61784-2, *Industrial communication networks – Profiles – Part 2: Additional fieldbus profiles for real-time networks based on ISO/IEC/IEEE 8802-3* (disponible en anglais seulement)

IEC 61784-3 (toutes les parties), *Réseaux de communication industriels – Profils – Partie 3: Bus de terrain de sécurité fonctionnelle*

IEC 61784-3-1, *Industrial communication networks – Profiles – Part 3-1: Functional safety fieldbuses – Additional specifications for CPF 1* (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, *Réseaux de communication industriels – Profils – Partie 3-8: Bus de terrain de sécurité fonctionnelle – Spécifications supplémentaires pour CPF 8*

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, *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 61918:2018, *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*