

INTERNATIONAL STANDARD

NORME INTERNATIONALE



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

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

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

PRICE CODE
CODE PRIX



ICS 35.100.05 25.040.40

ISBN 978-2-83220-535-8

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

CONTENTS

FOREWORD.....	5
INTRODUCTION.....	7
1 Scope.....	10
2 Normative references	10
3 Terms, definitions, symbols, abbreviated terms and conventions	11
3.1 Terms and definitions	11
3.1.1 Common terms and definitions	11
3.1.2 CPF 1: Additional terms and definitions	16
3.1.3 CPF 2: Additional terms and definitions	16
3.1.4 CPF 3: Additional terms and definitions	16
3.1.5 CPF 6: Additional terms and definitions	16
3.2 Symbols and abbreviated terms.....	17
3.2.1 Common symbols and abbreviated terms.....	17
3.2.2 CPF 1: Additional symbols and abbreviated terms.....	17
3.2.3 CPF 2: Additional symbols and abbreviated terms.....	17
3.2.4 CPF 3: Additional symbols and abbreviated terms.....	17
3.2.5 CPF 6: Additional symbols and abbreviated terms.....	17
4 Conformance.....	18
5 Basics of safety-related fieldbus systems	18
5.1 Safety function decomposition.....	18
5.2 Communication system.....	19
5.2.1 General.....	19
5.2.2 IEC 61158 fieldbuses.....	19
5.2.3 Communication channel types	20
5.2.4 Safety function response time.....	20
5.3 Communication errors	21
5.3.1 General.....	21
5.3.2 Corruption	21
5.3.3 Unintended repetition	21
5.3.4 Incorrect sequence	21
5.3.5 Loss	22
5.3.6 Unacceptable delay	22
5.3.7 Insertion	22
5.3.8 Masquerade	22
5.3.9 Addressing	22
5.4 Deterministic remedial measures.....	22
5.4.1 General	22
5.4.2 Sequence number	23
5.4.3 Time stamp	23
5.4.4 Time expectation	23
5.4.5 Connection authentication	23
5.4.6 Feedback message	23
5.4.7 Data integrity assurance.....	23
5.4.8 Redundancy with cross checking	23
5.4.9 Different data integrity assurance systems	24
5.5 Relationships between errors and safety measures	24

5.6	Data integrity considerations	25
5.6.1	Calculation of the residual error rate	25
5.6.2	Residual error rate and SIL	27
5.7	Relationship between functional safety and security	27
5.8	Boundary conditions and constraints	27
5.8.1	Electrical safety	27
5.8.2	Electromagnetic compatibility (EMC)	27
5.9	Installation guidelines	28
5.10	Safety manual	28
5.11	Safety policy	28
6	Communication Profile Family 1 (FOUNDATION™ Fieldbus) – Profiles for functional safety	29
6.1	Functional Safety Communication Profile 1/1	29
6.2	Technical overview	29
7	Communication Profile Family 2 (CIP™) – Profiles for functional safety	30
7.1	Functional Safety Communication Profile 2/1	30
7.2	Technical overview	30
8	Communication Profile Family 3 (PROFIBUS™, PROFINET™) – Profiles for functional safety	31
8.1	Functional Safety Communication Profile 3/1	31
8.2	Technical overview	31
9	Communication Profile Family 6 (INTERBUS®) – Profiles for functional safety	34
9.1	Functional Safety Communication Profile 6/7	34
9.2	Technical overview	34
Annex A (informative)	Example functional safety communication models	36
A.1	General	36
A.2	Model A	36
A.3	Model B	36
A.4	Model C	37
A.5	Model D	37
Annex B (informative)	A safety communication channel model using CRC-based error checking	39
B.1	Overview	39
B.2	Channel model for calculations	39
B.3	Cyclic redundancy checking	40
B.3.1	General	40
B.3.2	Considerations concerning CRC polynomials	42
Annex C (informative)	Structure of technology-specific parts	44
Bibliography		46
Table 1	– Overview of the effectiveness of the various measures on the possible errors	25
Table 2	– Definition of items used for calculation of the residual error rate	26
Table 3	– Relationship of residual error rate to SIL level	27
Table 4	– Overview of profile identifier usable for FSCP 6/7	34
Table B.1	– Example dependency d_{min} and block length n	42
Table C.1	– Common subclause structure for technology-specific parts	44

Figure 1 – Relationships of IEC 61784-3 with other standards (machinery)	7
Figure 2 – Relationships of IEC 61784-3 with other standards (process)	8
Figure 3 – Safety communication as a part of a safety function	19
Figure 4 – Example model of a functional safety communication system	20
Figure 5 – Example of safety function response time components	21
Figure 6 – Example application	26
Figure 7 – Scope of FSCP 1/1	29
Figure 8 – Relationship of Safety Validators	30
Figure 9 – Basic communication preconditions for FSCP 3/1	32
Figure 10 – Structure of a FSCP 3/1 safety PDU	33
Figure 11 – Safe communication modes	33
Figure 12 – FSCP 6/7 communication preconditions	35
Figure A.1 – Model A	36
Figure A.2 – Model B	37
Figure A.3 – Model C	37
Figure A.4 – Model D	38
Figure B.1 – Communication channel with perturbation	39
Figure B.2 – Binary symmetric channel (BSC)	40
Figure B.3 – Example of a block with message and CRC bits (redundancy code)	41
Figure B.4 – Block codes for error detection	41
Figure B.5 – Proper and improper CRC polynomials	42

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 provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with an IEC Publication.
- 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.

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 and 6 given in IEC 61784-3-1, IEC 61784-3-2, IEC 61784-3-3 and IEC 61784-3-6.

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 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 and IEC 61784-3-6.

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 bilingual version (2012-12) corresponds to the monolingual English version, published in 2007-12.

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

FDIS	Report on voting
65C/470/FDIS	65C/481/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.

The French version of this standard has not been voted upon.

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

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

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

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

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.

INTRODUCTION

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

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

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

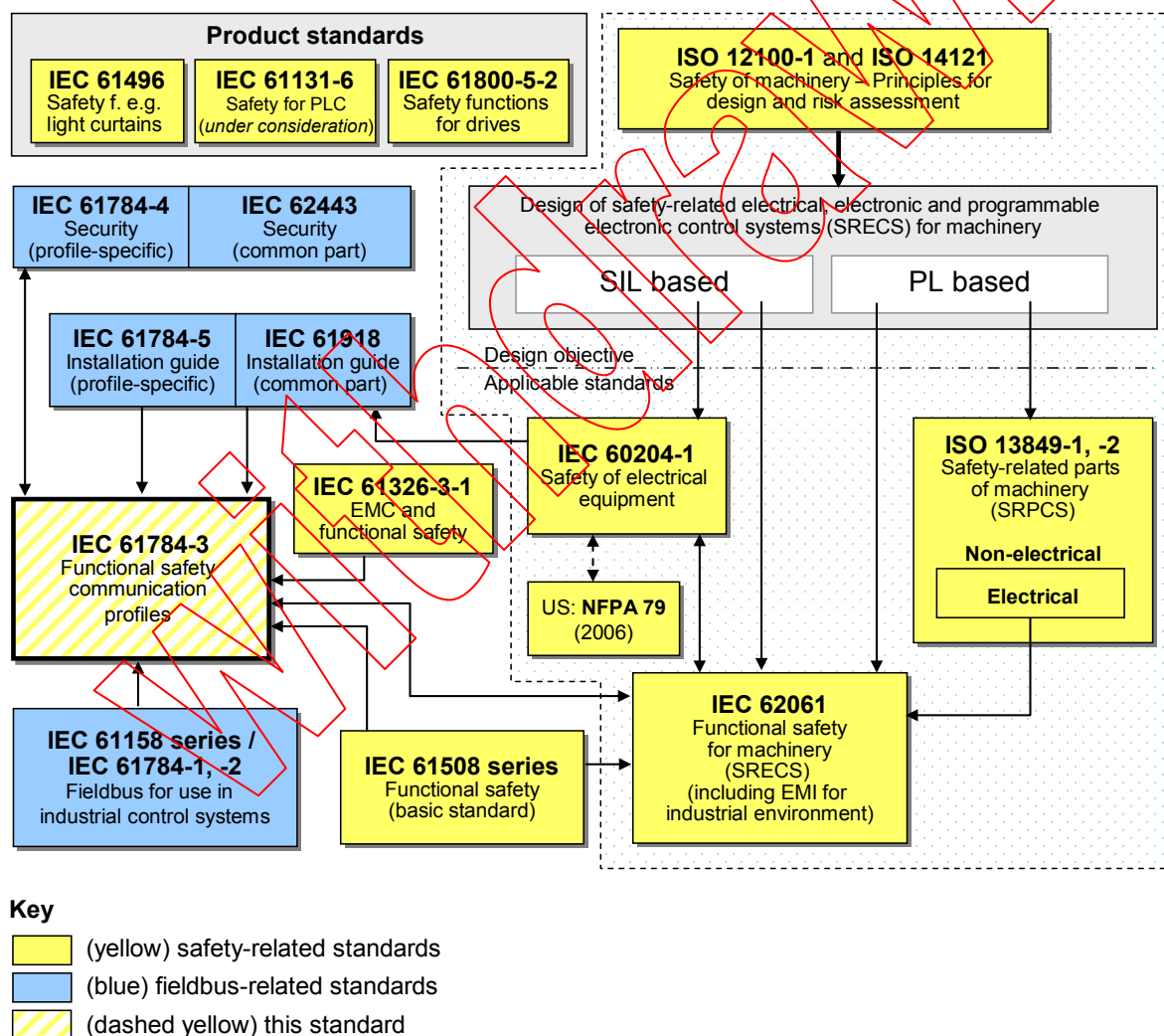
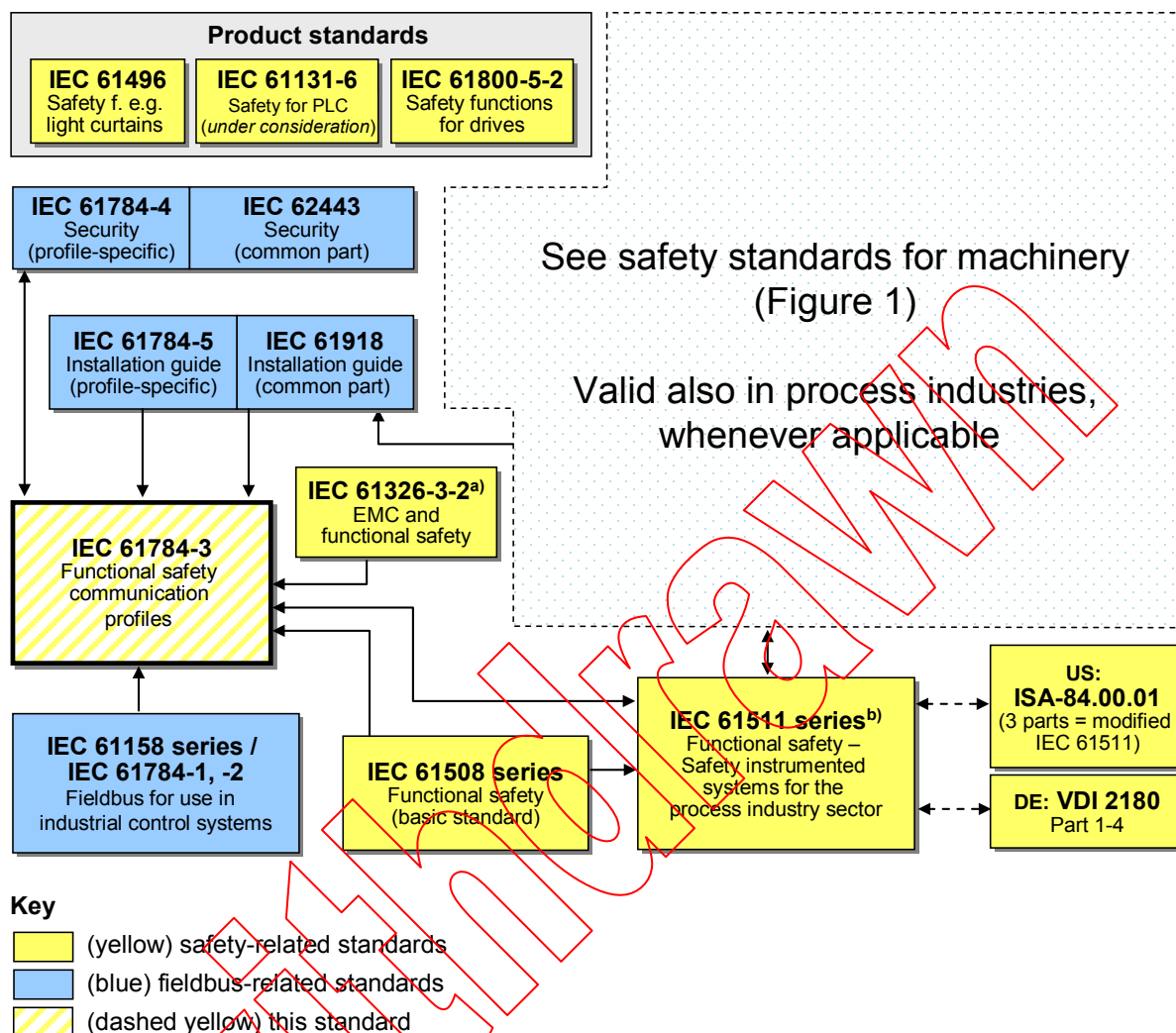


Figure 1 – Relationships of IEC 61784-3 with other standards (machinery)

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



^a For specified electromagnetic environments; otherwise IEC 61326-3-1.

^b EN ratified.

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

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

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

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

This standard describes:

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

Withdrawn

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 than can be used in the transmission of safety-relevant messages among participants within a distributed network using fieldbus technology in accordance with the requirements of IEC 61508 series for functional safety. These principles can be used in various industrial applications such as process control, manufacturing automation and machinery.

This part¹ 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.

NOTE 1 Other safety-related communication systems meeting the requirements of IEC 61508 series may 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. IEC 62443 will address many of these issues; the relationship with IEC 62443 is detailed in a dedicated subclause of this part.

NOTE 3 Additional profile specific requirements for security may also be specified in the future IEC 61784-4.

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 referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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

IEC 61158 (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*²

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 EM environment*²

¹ In the following pages of this standard, “this part” will be used for “this part of the IEC 61784-3 series”.

² To be published.

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

IEC 61508-1, *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 61784-5 (all parts), *Industrial communication networks – Profiles – Part 5: Installation of fieldbuses – Installation profiles for CPF x*

IEC 61918, *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*

SOMMAIRE

AVANT-PROPOS	51
INTRODUCTION	53
1 Domaine d'application	57
2 Références normatives	57
3 Termes, définitions, symboles, abréviations et conventions	58
3.1 Termes et définitions	58
3.1.1 Termes et définitions communs	59
3.1.2 CPF 1: Termes et définitions supplémentaires	64
3.1.3 CPF 2: Termes et définitions supplémentaires	64
3.1.4 CPF 3: Termes et définitions supplémentaires	64
3.1.5 CPF 6: Termes et définitions supplémentaires	64
3.2 Symboles et abréviations	64
3.2.1 Symboles et abréviations communs	64
3.2.2 CPF 1: Symboles et abréviations supplémentaires	65
3.2.3 CPF 2: Symboles et abréviations supplémentaires	65
3.2.4 CPF 3: Symboles et abréviations supplémentaires	65
3.2.5 CPF 6: Symboles et abréviations supplémentaires	65
4 Conformité	65
5 Principes des systèmes de bus de terrain relatifs à la sécurité	66
5.1 Décomposition des fonctions de sécurité	66
5.2 Système de communication	67
5.2.1 Généralités	67
5.2.2 Bus de terrain définis dans la CEI 61158	67
5.2.3 Types de canaux de communication	68
5.2.4 Temps de réponse de la fonction de sécurité	69
5.3 Erreurs de communication	69
5.3.1 Généralités	69
5.3.2 Corruption	69
5.3.3 Répétition non prévue	70
5.3.4 Séquence incorrecte	70
5.3.5 Perte	70
5.3.6 Retard inacceptable	70
5.3.7 Insertion	71
5.3.8 Mascarade	71
5.3.9 Adressage	71
5.4 Mesures correctives déterministes	71
5.4.1 Généralités	71
5.4.2 Numéro de séquence	71
5.4.3 Datation (horodatage)	71
5.4.4 Délai	72
5.4.5 Authentification de connexion	72
5.4.6 Message de réaction	72
5.4.7 Assurance d'intégrité des données	72
5.4.8 Redondance avec contre-vérification	72
5.4.9 Différents systèmes d'assurance d'intégrité des données	73

5.5	Relations entre les erreurs et les mesures de sécurité.....	73
5.6	Considérations concernant l'intégrité des données	74
5.6.1	Calcul du taux d'erreurs résiduelles	74
5.6.2	Taux d'erreurs résiduelles et SIL	76
5.7	Relation entre sécurité fonctionnelle et sûreté	77
5.8	Conditions aux limites et contraintes	77
5.8.1	Sécurité électrique.....	77
5.8.2	Compatibilité électromagnétique (CEM).....	77
5.9	Lignes directrices d'installation.....	78
5.10	Manuel de sécurité	78
5.11	Politique de sécurité.....	78
6	Famille de profils de communication 1 (FOUNDATION™ Fieldbus) - Profils de sécurité fonctionnelle.....	79
6.1	Profil de communication de sécurité fonctionnelle 1/1.....	79
6.2	Présentation générale d'ordre technique	79
7	Famille de profils de communication 2 (CIP™) – Profils de sécurité fonctionnelle.....	80
7.1	Profil de communication de sécurité fonctionnelle 2/1.....	80
7.2	Présentation générale d'ordre technique	81
8	Famille de profils de communication 3 (PROFIBUS™, PROFINET™) – Profils de sécurité fonctionnelle.....	82
8.1	Profil de communication de sécurité fonctionnelle 3/1.....	82
8.2	Présentation générale d'ordre technique	82
9	Famille de profils de communication 6 (INTERBUS®) – Profils de sécurité fonctionnelle.....	85
9.1	Profil de communication de sécurité fonctionnelle 6/7.....	85
9.2	Présentation générale d'ordre technique	86
	Annexe A (informative) Exemple de modèles de communication de sécurité fonctionnelle	88
A.1	Généralités	88
A.2	Modèle A	88
A.3	Modèle B	89
A.4	Modèle C	89
A.5	Modèle D	90
	Annexe B (informative) Modèle de canal de communication de sécurité utilisant le contrôle d'erreurs CRC	92
B.1	Présentation générale	92
B.2	Modèle de canal pour calculs	92
B.3	Contrôle de redondance cyclique	94
B.3.1	Généralités	94
B.3.2	Considérations concernant les polynômes CRC	96
	Annexe C (informative) Structure des parties spécifiques à la technologie	98
	Bibliographie.....	100
	Tableau 1 – Présentation générale de l'efficacité des diverses mesures sur les erreurs possibles	74
	Tableau 2 – Définition des éléments utilisés pour le calcul du taux d'erreurs résiduelles.....	76
	Tableau 3 – Relation entre le taux d'erreurs résiduelles et le niveau SIL.....	77
	Tableau 4 – Présentation générale de l'identificateur de profil applicable au protocole FSCP 6/7	86

Tableau B.1 – Exemple de dépendance $d_{\min}$ et de longueur de bloc n	96
Tableau C.1 – Structure des paragraphes communs pour les parties spécifiques à la technologie	98
Figure 1 – Relation entre la CEI 61784–3 et d’autres normes (machines)	54
Figure 2 – Relations entre la CEI 61784–3 et d’autres normes (procédés industriels)	56
Figure 3 – Communication de sécurité comme partie intégrante d’une fonction de sécurité.....	67
Figure 4 – Exemple de modèle d’un système de communication de sécurité fonctionnelle	68
Figure 5 – Exemple des composantes du temps de réponse de la fonction de sécurité	69
Figure 6 – Exemple d’application	76
Figure 7 – Domaine d’application du FSCP 1/1	80
Figure 8 – Relation des objets de validation de sécurité.....	81
Figure 9 – Conditions préalables de communication de base pour le protocole FSCP 3/1	83
Figure 10 – Structure d’un PDU de sécurité FSCP 3/1.....	84
Figure 11 – Modes de communication sécurisée	85
Figure 12 – Conditions préalables de communication FSCP 6/7.....	86
Figure A.1 – Modèle A	88
Figure A.2 – Modèle B	89
Figure A.3 – Modèle C	90
Figure A.4 – Modèle D	91
Figure B.1 – Canal de communication avec perturbation.....	93
Figure B.2 – Canal symétrique binaire (BSC).....	93
Figure B.3 – Exemple de bloc comportant un message et des bits CRC (code de redondance)	95
Figure B.4 – Codes de blocs pour la détection d’erreurs	95
Figure B.5 – Polynômes CRC appropriés et inappropriés	97

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

**RÉSEAUX DE COMMUNICATIONS INDUSTRIELS –
PROFILS –****Partie 3: Bus de terrain de sécurité fonctionnelle –
Règles générales et définitions de profils**

AVANT-PROPOS

- 1) La Commission Electrotechnique Internationale (CEI) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de la CEI). La CEI 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, la CEI – 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 la CEI"). 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 la CEI, participent également aux travaux. La CEI 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 la CEI concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de la CEI intéressés sont représentés dans chaque comité d'études.
- 3) Les Publications de la CEI se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de la CEI. Tous les efforts raisonnables sont entrepris afin que la CEI s'assure de l'exactitude du contenu technique de ses publications; la CEI 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 la CEI s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de la CEI dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de la CEI et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
- 5) La CEI 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 la CEI. La CEI 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 la CEI, 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 la CEI, 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 la CEI ou de toute autre Publication de la CEI, 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 la CEI peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. La CEI ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et de ne pas avoir signalé leur existence.

La commission électrotechnique internationale (CEI) attire l'attention sur le fait qu'il est déclaré que la conformité avec le présent document peut impliquer l'utilisation de brevets concernant les profils de communication de sécurité fonctionnelle pour les familles 1, 2, 3, et 6 donnés dans la CEI 61784-3-1, la CEI 61784-3-2, la CEI 61784-3-3 et la CEI 61784-3-6.

La CEI ne prend pas position quant à la preuve, à la validité et à la portée de ces droits de propriété. Le détenteur de ces droits de propriété a donné l'assurance à la CEI qu'il consent à négocier des licences avec des demandeurs du monde entier, à des termes et conditions raisonnables et non discriminatoires. A ce propos, la déclaration du détenteur des droits de propriété est enregistrée à la CEI.

NOTE Les détails relatifs aux brevets et l'information personne-ressource correspondante sont fournis dans la CEI 61784-3-1, la CEI 61784-3-2, la CEI 61784-3-3 et la CEI 61784-3-6.

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

La présente version bilingue (2012-12) correspond à la version anglaise monolingue publiée en 2007-12.

Le texte anglais de cette norme est issu des documents 65C/470/FDIS et 65C/481/RVD.

Le rapport de vote 65C/481/RVD donne toute information sur le vote ayant abouti à l'approbation de cette norme.

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

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

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 la CEI 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.

La liste de toutes les parties de la série CEI 61784-3, publiées sous le titre général *Réseaux de communications industriels – Profils – Bus de terrain de sécurité fonctionnelle*, est disponible sur le site Web de la CEI.

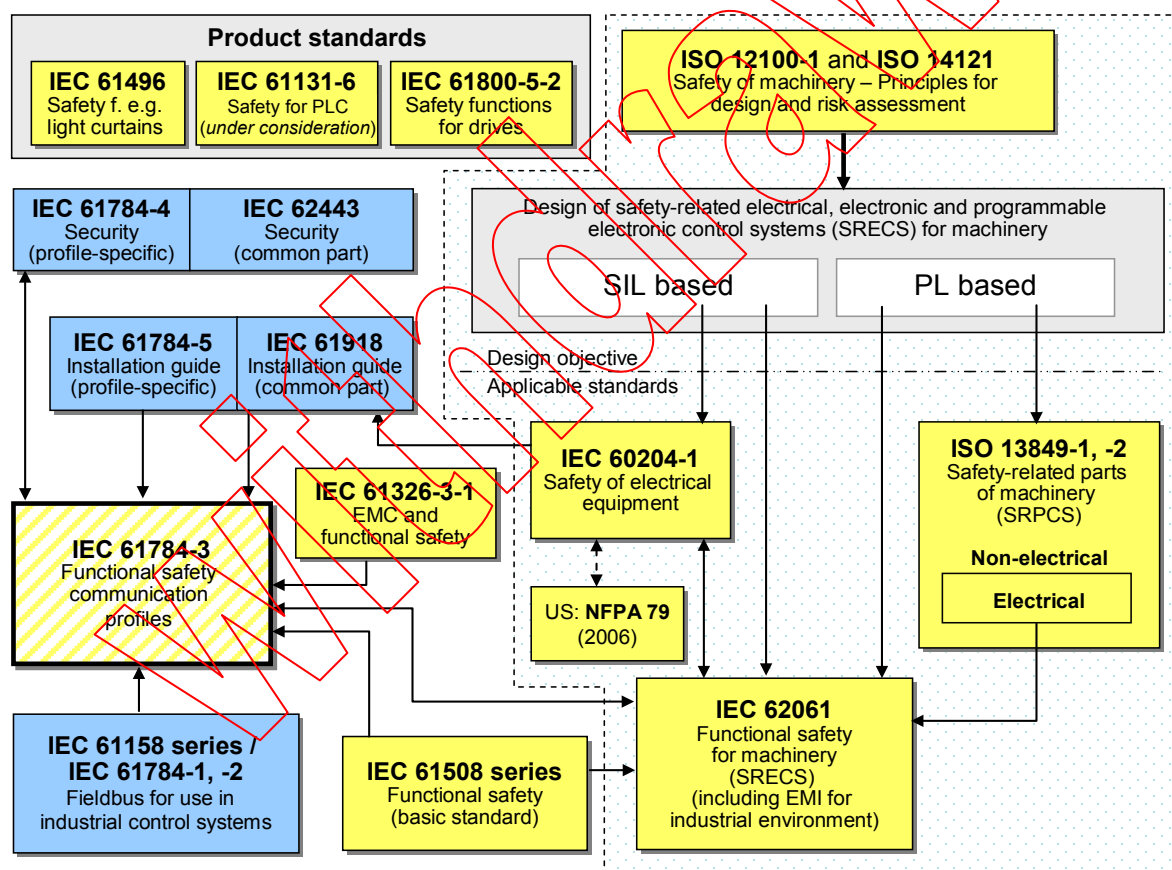
IMPORTANT – Le logo "colour inside" qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante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

INTRODUCTION

La CEI 61158 relative aux bus de terrain, ainsi que ses normes associées CEI 61784-1 et CEI 61784-2, définit un ensemble de protocoles de communication qui assurent la commande répartie d'applications automatisées. La technologie de bus de terrain est désormais reconnue et bien éprouvée. Ainsi de nombreuses améliorations des bus de terrain se développent pour traiter de domaines non encore normalisés tels que les applications temps réel relatives à la sécurité et à la sûreté.

La présente norme définit les principes pertinents applicables aux communications en termes de sécurité fonctionnelle en référence à la série CEI 61508, et spécifie plusieurs couches de communication de sécurité (profils et protocoles correspondants) basées sur les profils de communication et les couches de protocole de la CEI 61784-1, la CEI 61784-2 et la série CEI 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 machines.



Key

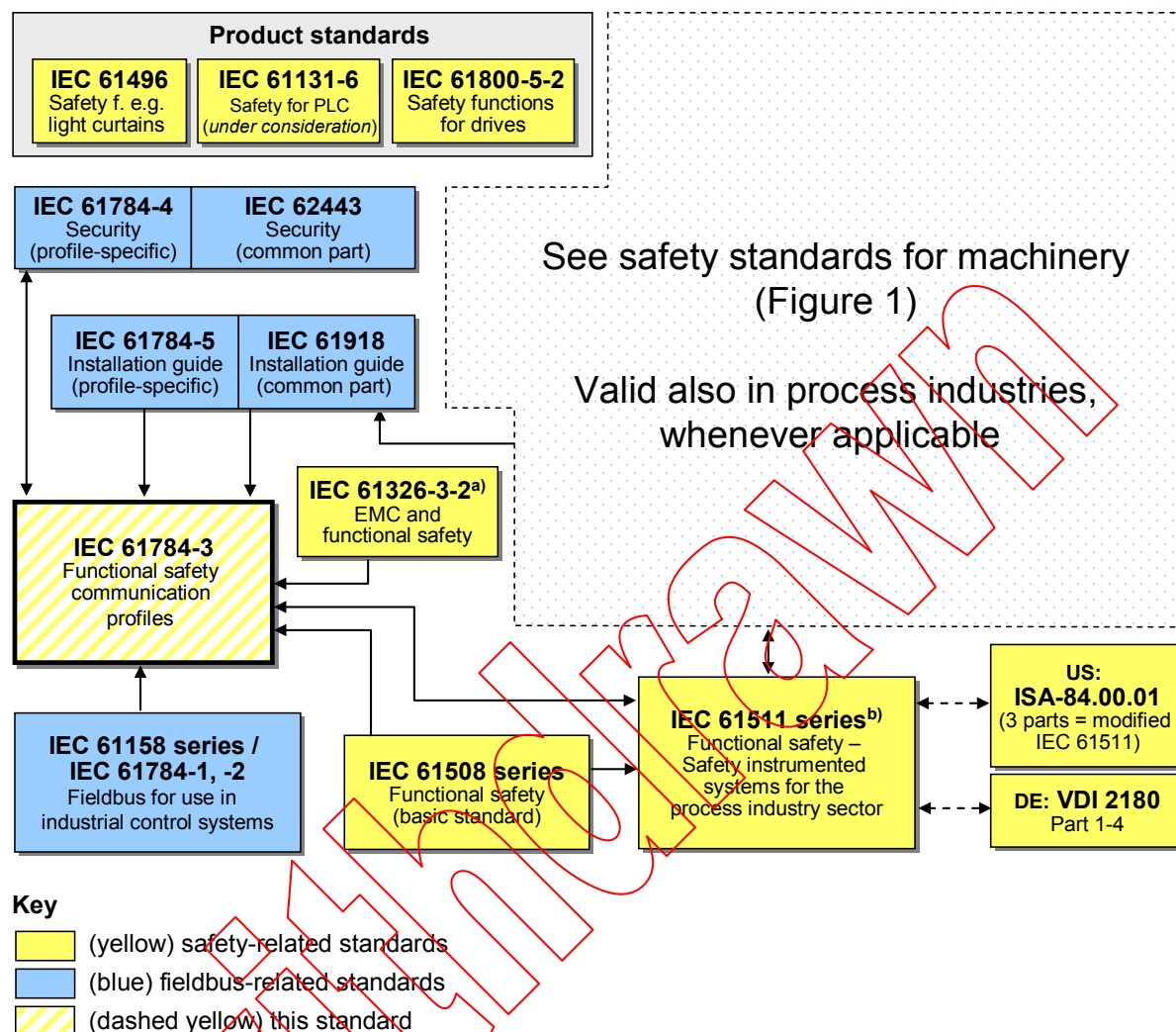
- (yellow) safety-related standards
- (blue) fieldbus-related standards
- (dashed yellow) this standard

Anglais	Français
Product standards	Normes de produits
Safety function, e.g. light curtains	Fonction de sécurité, par exemple barrières photo électriques

Anglais	Français
Safety for PLC (under consideration)	Sécurité relative aux automates programmables (à l'étude)
Safety functions for drives	Fonctions de sécurité applicables aux entraînements
Safety requirements for robots	Exigences de sécurité applicables aux robots
Safety of machinery - ... assessment	Sécurité des machines – Principes généraux de conception et d'appréciation du risque
Security (profile-specific)	Sûreté (spécifique au profil)
Security (common part)	Sûreté (partie commune)
Design of safety-related electrical, electronic and programmable electronic control system (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
Safety of electrical equipment	Sécurité des équipements électriques
Safety-related parts of machinery	Parties des systèmes de commande relatives à la sécurité
Non-electrical	Non électrique
Electrical	Électrique
EMC and functional safety	Compatibilité électromagnétique et sécurité fonctionnelle
Functional safety communication profiles	Profils de communication de sécurité fonctionnelle
IEC 61158 series / Fieldbus for use in industrial control systems	Série CEI 61158 / Bus de terrain pour utilisation dans des systèmes de commande industriels
IEC 61508 series, Functional safety (basic standard)	Série CEI 61508, Sécurité fonctionnelle (norme de base)
Functional safety for machinery (SRECS) (including EMI for industrial environment)	Sécurité fonctionnelle des systèmes de commande électriques, électroniques et électroniques programmables (y compris les interférences électromagnétiques dans l'environnement industriel)
Key	Légende
(yellow) safety-related standards	(jaune) normes relatives à la sécurité
(blue) fieldbus-related standards	(bleu) normes relatives au bus de terrain
(dashed) yellow) this standard	(jaune pointillé) la présente norme
IEC	CEI

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

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



Anglais	Français
Product standards	Normes de produits
Safety function, e.g. light curtains	Fonction de sécurité, par exemple barrières photo électriques
Safety for PLC (under consideration)	Sécurité relative aux automates programmables (à l'étude)
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

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

^a Pour des environnements électromagnétiques spécifiés, sinon CEI 61326-3-1.

^b EN ratifiée.

Figure 2 – Relations entre la CEI 61784-3 et d'autres normes (procédés industriels)

Les couches de communication de sécurité mises en œuvre dans le cadre de systèmes relatifs à la sécurité conformément à la série CEI 61508, assurent la confiance nécessaire lors de la transmission des messages (information) sur un bus de terrain dans un système relatif à la sécurité entre deux participants ou plus, ou une fiabilité suffisante quant au 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 garantissent qu'un bus de terrain peut être utilisé dans des applications nécessitant une sécurité fonctionnelle jusqu'au niveau d'intégrité de sécurité (SIL) spécifié par son profil de communication correspondant.

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

La présente norme décrit:

- les principes de base de la mise en œuvre des exigences de la CEI 61508 pour les communications de données relatives à la sécurité, y compris les défauts de transmission potentiels, les mesures correctives et ce qui concerne l'intégrité des données;
- la description individuelle des profils de sécurité fonctionnelle pour plusieurs familles de profils de communication dans la CEI 61784-1 et la CEI 61784-2;
- les extensions de la couche de sécurité aux sections relatives au service et aux protocoles de communication de la série CEI 61158.

RÉSEAUX DE COMMUNICATIONS 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 CEI 61784-3 définit des principes communs pouvant être appliqués pour la transmission des messages propres à la sécurité entre les participants d'un réseau réparti, en utilisant la technologie de bus de terrain conformément aux exigences de la série CEI 61508 concernant la sécurité fonctionnelle. Ces principes peuvent être utilisés dans diverses applications industrielles, telles que la commande de processus, l'usinage automatique et les machines.

La présente partie¹ et les parties CEI 61784-3-x spécifient plusieurs profils de communication de sécurité fonctionnelle basés sur les profils de communication et les couches de protocole des technologies de bus de terrain de la CEI 61784-1, la CEI 61784-2 et la série CEI 61158.

NOTE 1 Il peut exister d'autres systèmes de communication relatifs à la sécurité qui satisfont aux exigences de la série CEI 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 tels que 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 nécessitent d'être prises en compte dans toute application nécessitant un niveau de sécurité afin de protéger les systèmes ayant des bus de terrain contre tout accès non autorisé. La CEI 62443 traite bon nombre de ces questions; la relation avec la CEI 62443 est détaillée dans un paragraphe dédié de la présente partie.

NOTE 3 Des exigences supplémentaires spécifiques au profil et concernant la sécurité peuvent également être spécifiées dans la future CEI 61784-4.

NOTE 4 La mise en œuvre du profil de communication de sécurité fonctionnelle, conforme à la présente partie, dans un dispositif normal ne suffit pas à le qualifier de dispositif de sécurité, tel que défini dans la série CEI 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 de référence suivants sont indispensables pour l'application du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

IEC 61131-2, *Programmable controllers – Part 2 Equipment requirements and tests* (disponible uniquement en anglais)

IEC 61158 (all parts), *Industrial communication networks – Fieldbus specifications* (disponible uniquement en anglais)

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

CEI 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*²

CEI 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*²

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

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

CEI 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 uniquement en anglais)

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

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

IEC 61784-3-2, *Industrial communication networks – Profiles – Part 3-2: Functional safety fieldbuses – Additional specifications for CPF 2* (disponible uniquement en anglais)

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

IEC 61784-3-6, *Industrial communication networks – Profiles – Part 3-6: Functional safety fieldbuses – Additional specifications for CPF 6* (disponible uniquement en anglais)

IEC 61784-5 (toutes les parties), *Industrial communication networks – Profiles – Part 5: Installation of fieldbuses – Installation profiles for CPF x* (disponible uniquement en anglais)

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

CEI 62280-1:2002, *Applications ferroviaires – Systèmes de signalisation, de télécommunication et de traitement – Partie 1: Communication de sécurité sur des systèmes de transmission fermés*

² A publier.