IEC 61784-3

Edition 4.0 2021-02

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

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

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

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

ICS 25.040.40; 35.100.05

ISBN 978-2-8322-9268-6

CONTENTS

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.

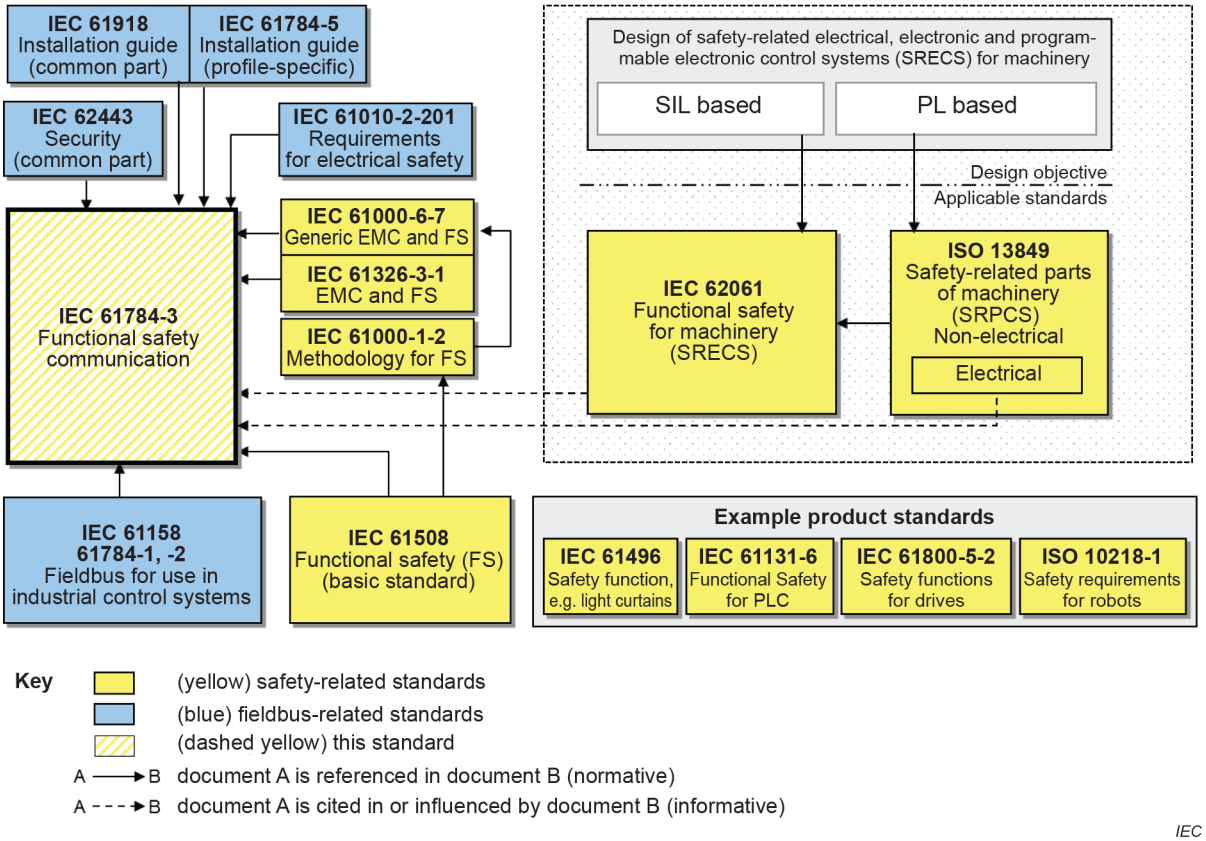
0 Introduction

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.

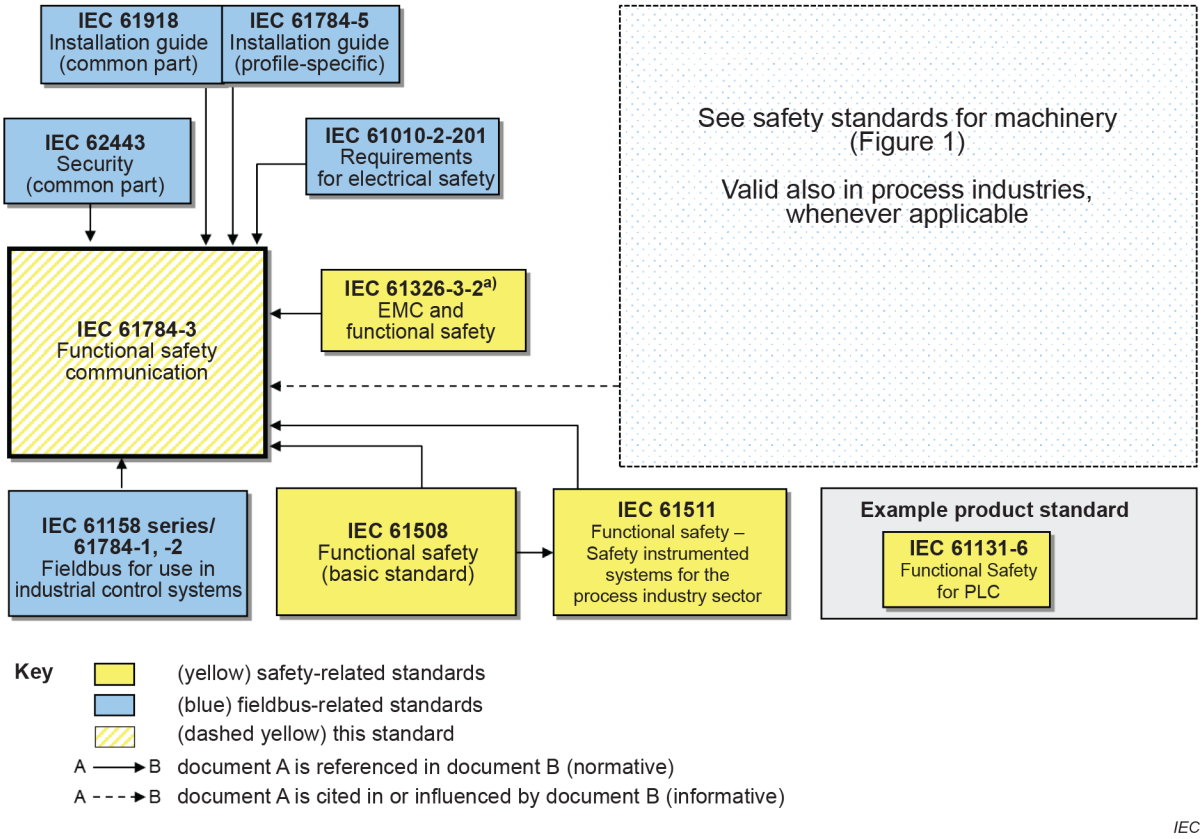
Figure 1 shows the relationships between IEC 61784-3 (all parts) and relevant safety and fieldbus standards in a machinery environment.



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

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

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



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

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

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

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

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

IEC 61784-3 (all parts) describes:

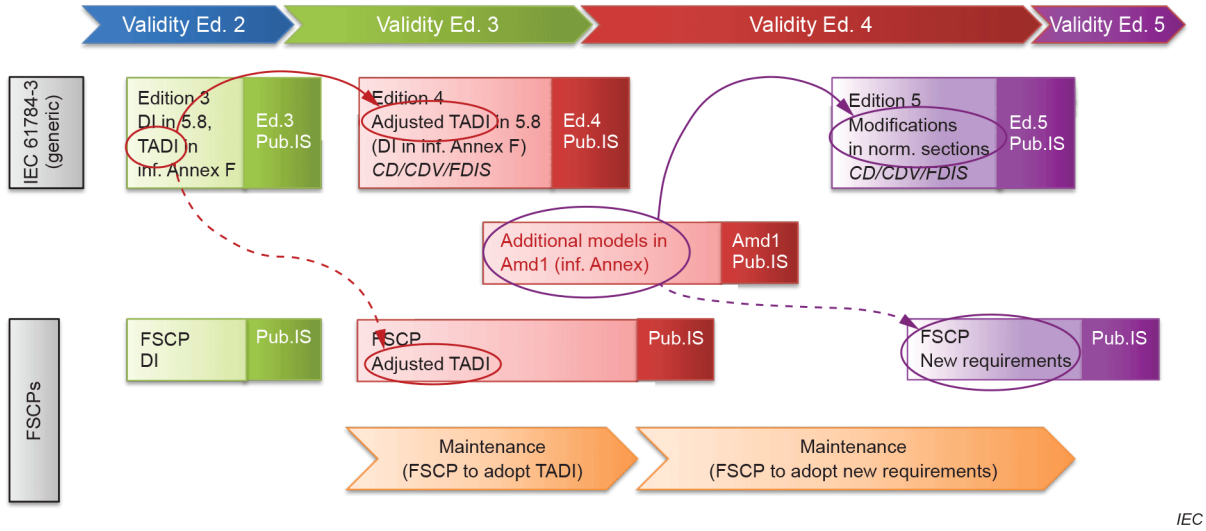
- basic principles for implementing the requirements of IEC 61508 (all parts) for safety-related data communications, including possible transmission faults, remedial measures and considerations affecting data integrity;
- functional safety communication profiles for several communication profile families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

0.2 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.



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

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 RCRC.

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.

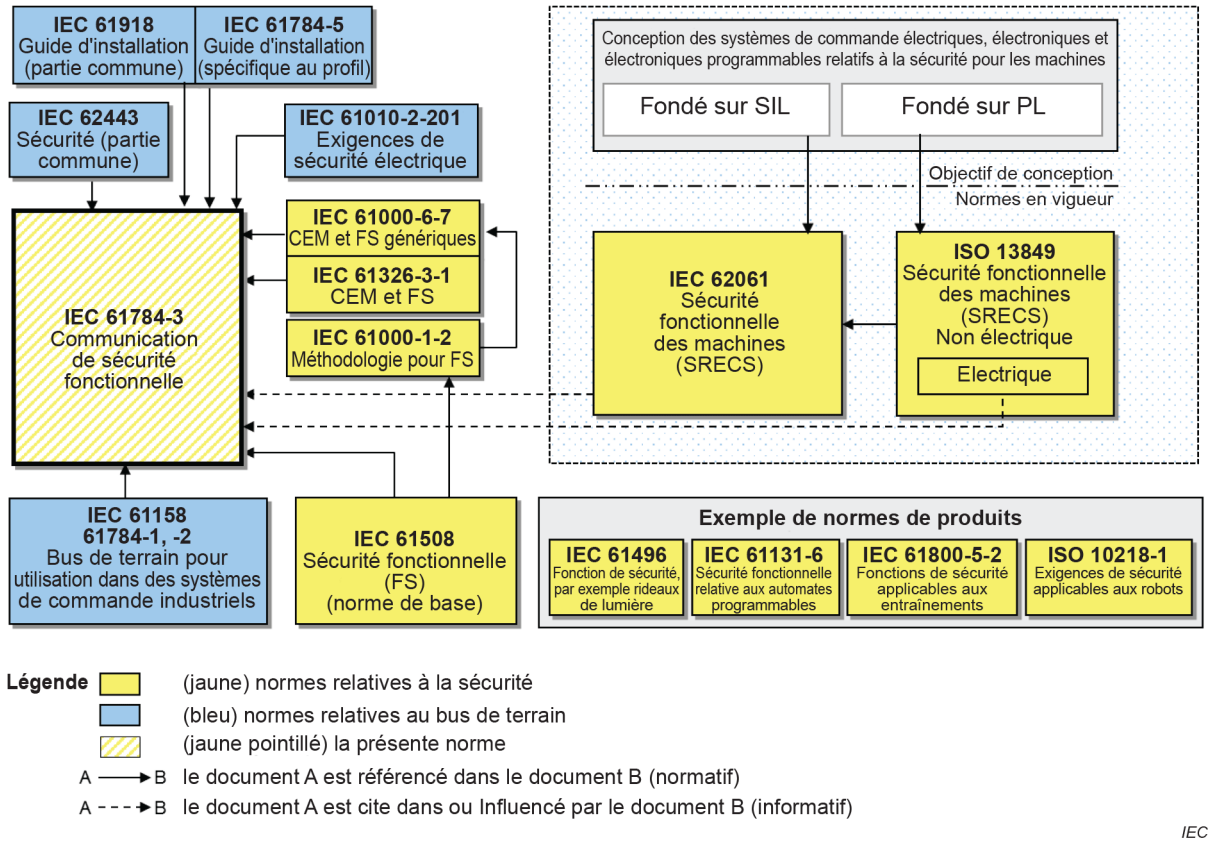
0 Introduction

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.

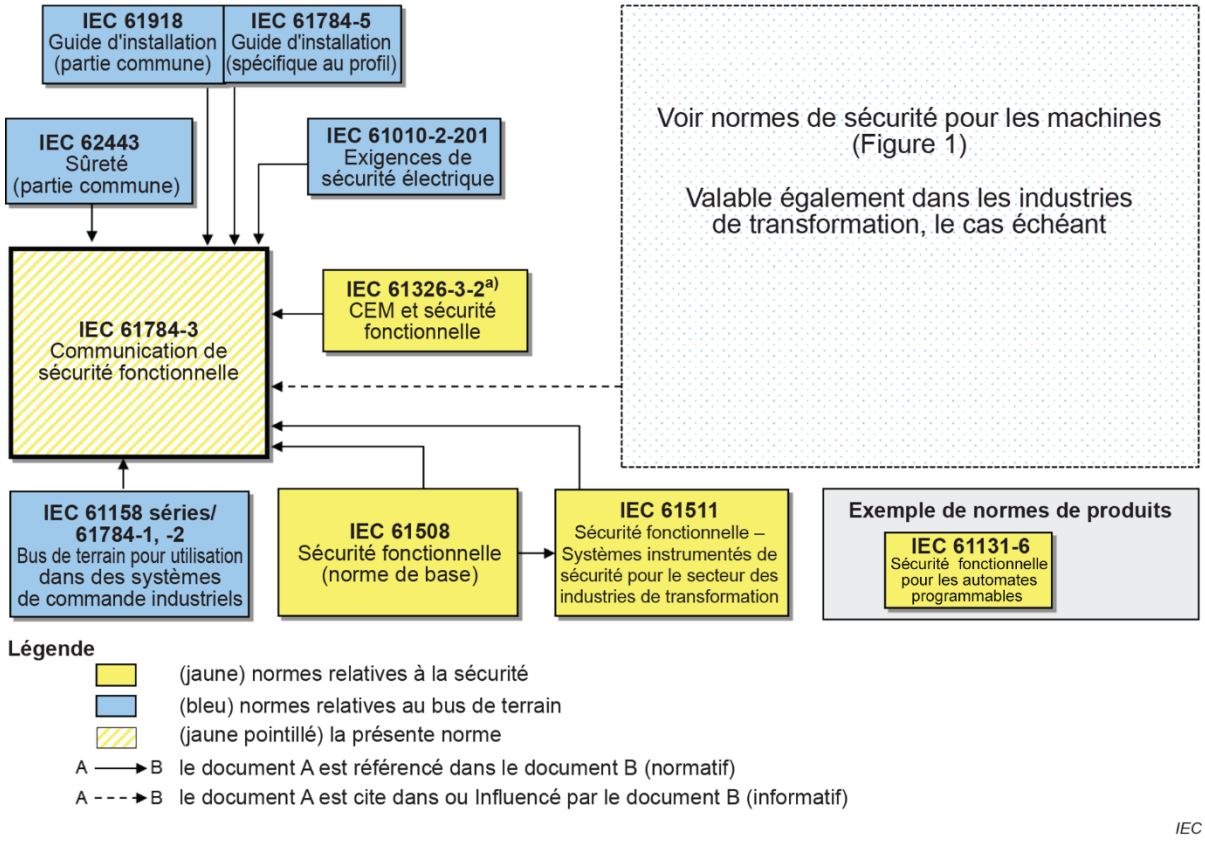
La Figure 1 représente les relations entre l'IEC 61784-3 (toutes les parties) et les normes pertinentes relatives à la sécurité et aux bus de terrain dans un environnement de machines



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

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

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



[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:

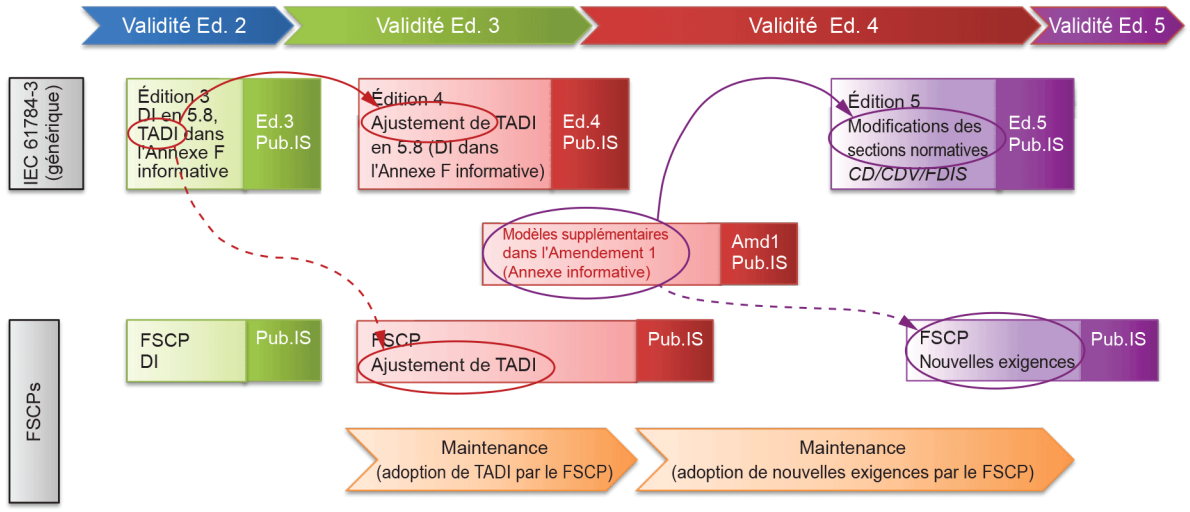
- les principes de base de la mise en œuvre des exigences de l'IEC 61508 (toutes les parties) pour les communications de données relatives à la sécurité, y compris les anomalies de transmission potentielles, les mesures correctives et des considérations relatives à l'intégrité des données;
- les profils 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.



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*