IEC 61784-3

Edition 3.1 2017-08

FINAL VERSION

VERSION FINALE

colour inside

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

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

IEC 61784-3:2016+AMD1:2017-08 CSV(en-fr)

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.

DISCLAIMER
This Consolidated version is not an official IEC Standard and has been prepared for user convenience. Only the current versions of the standard and its amendment(s) are to be considered the official documents.

This Consolidated version of IEC 61784-3 bears the edition number 3.1. It consists of the third edition (2016-05) [documents 65C/840/FDIS and 65C/848/RVD] and its amendment 1 (2017-08) [documents 65C/879/FDIS and 65C/886/RVD]. The technical content is identical to the base edition and its amendment.

This Final version does not show where the technical content is modified by amendment 1. A separate Redline version with all changes highlighted is available in this publication.

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

This third edition constitutes a technical revision.

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

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

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

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

The committee has decided that the contents of the base publication and its amendment will remain unchanged until the stability 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.

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

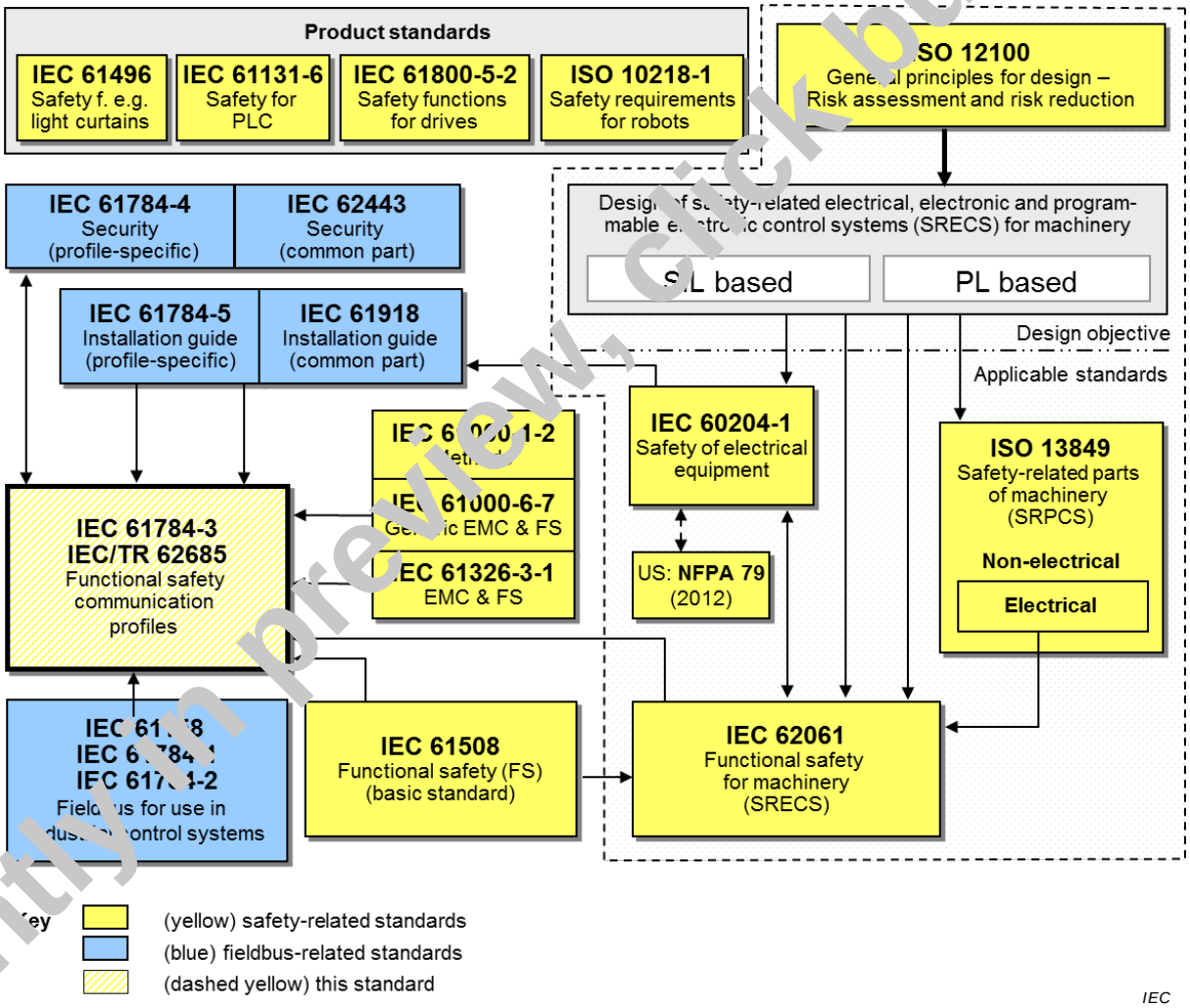
0 Introduction

0.1 General

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

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

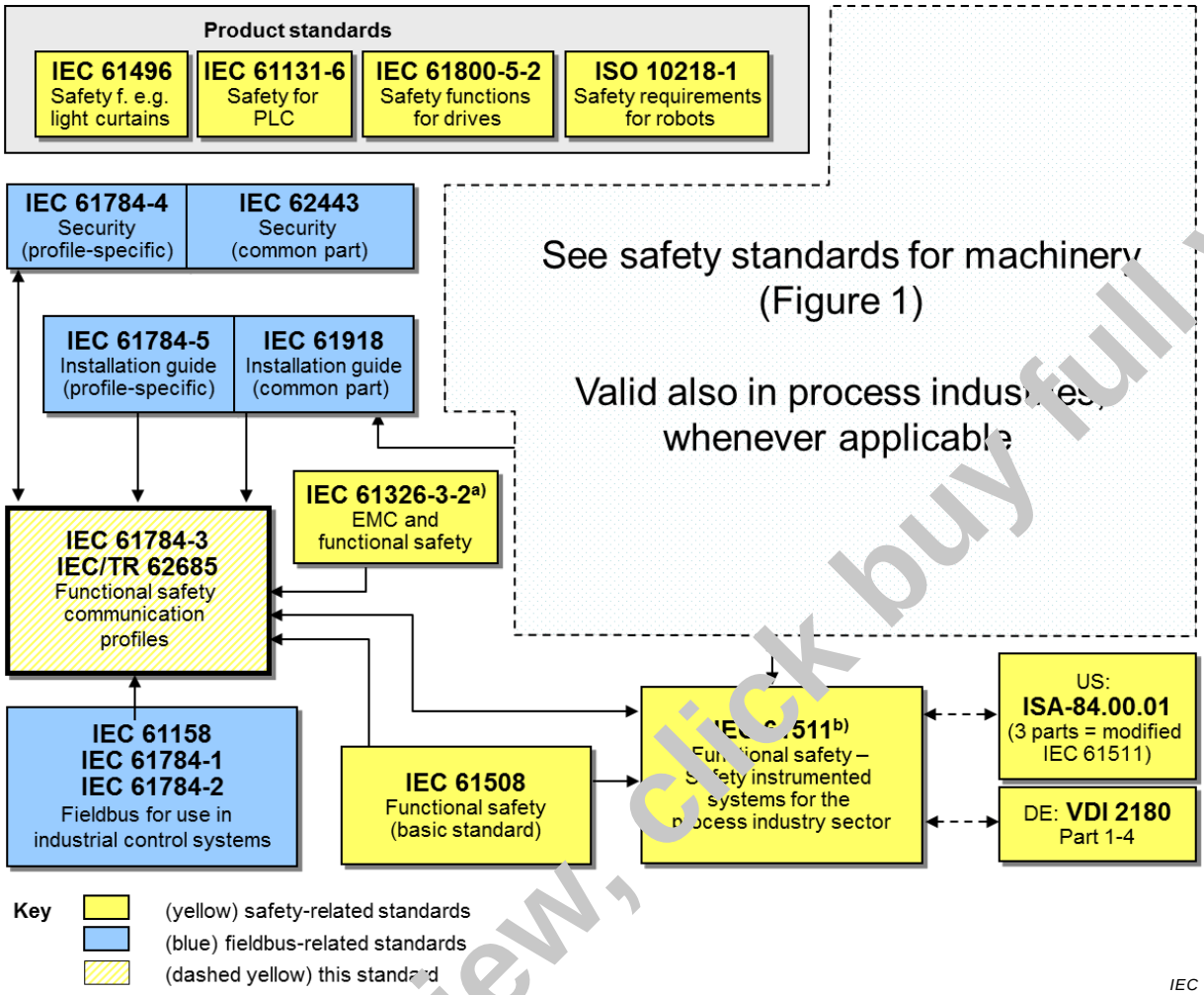
Figure 1 shows the relationships between this standard and relevant safety and fieldbus standards in a machinery environment.



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

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

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



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

[b] EN ratified.

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

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

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

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

This standard describes:

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

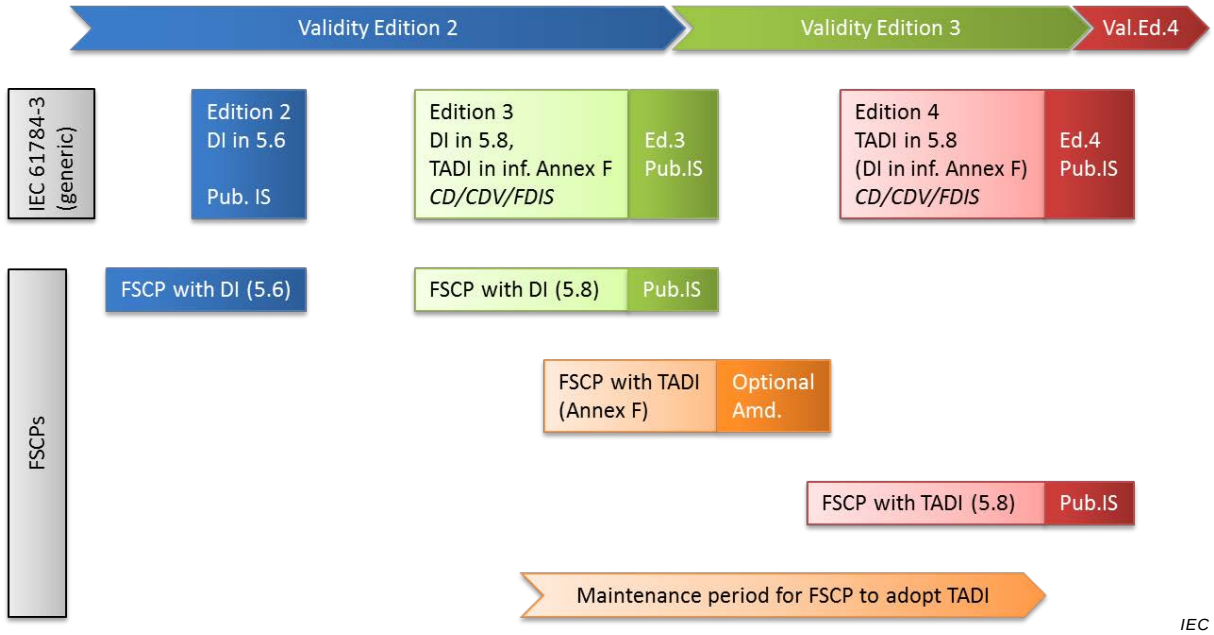
0.2 Transition from Edition 2 to extended assessment methods in Edition 3

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

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

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

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



Key

DI Data Integrity

TADI Timeliness, Authenticity, Data Integrity

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

0.3 Patent declaration

The International Electrotechnical Commission (IEC) draws attention to the fact that it is claimed that compliance with this document may involve the use of patents concerning functional safety communication profiles for families 1, 2, 3, 6, 8, 12, 13, 14, 17 and 18 given in IEC 61784-3-1, IEC 61784-3-2, IEC 61784-3-3, IEC 61784-3-6, IEC 61784-3-8, IEC 61784-3-12, IEC 61784-3-13, IEC 61784-3-14, IEC 61784-3-17 and IEC 61784-3-18.

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

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

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

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

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

INTRODUCTION to the Amendment

This Amendment 1 discusses the concepts of implicit data safety mechanisms for use in functional safety communications protocols (FSCPs) as specified in IEC 61784-3:2016.

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES –

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

1 Scope

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

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

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

NOTE 2 It does not cover electrical safety and intrinsic safety aspects. Electrical safety relates to hazards such as electrical shock. Intrinsic safety relates to hazards associated with potentially explosive atmospheres.

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

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

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

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

2 Normative references

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

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

---

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

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

3 Proposed new work item under consideration.