SLOVENSKI STANDARD
oSIST prEN IEC 61784-3:2020

01-april-2020

Industrijska komunikacijska omrežja - Profili - 3. del: Funkcionalno varna procesna vodila - Splošna pravila in definicije profilov

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

Ta slovenski standard je istoveten z: prEN IEC 61784-3:2020

ICS:

25.040.40	Merjenje in krmiljenje industrijskih postopkov	Industrial process measurement and control
35.100.05	Večslojne uporabniške rešitve	Multilayer applications

oSIST prEN IEC 61784-3:2020 **en,fr,de**

65C/991/CDV

COMMITTEE DRAFT FOR VOTE (CDV)

PROJECT NUMBER: **IEC 61784-3 ED4**	
DATE OF CIRCULATION: **2020-01-24**	CLOSING DATE FOR VOTING: **2020-04-17**
SUPERSEDES DOCUMENTS: **65C/962/CD,65C/978A/CC**	

IEC SC 65C : INDUSTRIAL NETWORKS

SECRETARIAT: France	SECRETARY: Ms Valérie DEMASSIEUX
OF INTEREST TO THE FOLLOWING COMMITTEES: SC 22G,TC 44,TC 57,SC 65A,TC 66	PROPOSED HORIZONTAL STANDARD: ☐ Other TC/SCs are requested to indicate their interest, if any, in this CDV to the secretary.

FUNCTIONS CONCERNED:

☐ EMC ☐ ENVIRONMENT ☐ QUALITY ASSURANCE ☐ SAFETY

☒ SUBMITTED FOR CENELEC PARALLEL VOTING	☐ NOT SUBMITTED FOR CENELEC PARALLEL VOTING

Attention IEC-CENELEC parallel voting

The attention of IEC National Committees, members of CENELEC, is drawn to the fact that this Committee Draft for Vote (CDV) is submitted for parallel voting.

The CENELEC members are invited to vote through the CENELEC online voting system.

This document is still under study and subject to change. It should not be used for reference purposes.

Recipients of this document are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

TITLE:

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

PROPOSED STABILITY DATE: 2024

NOTE FROM TC/SC OFFICERS:

In order to facilitate analysis by National Committees, changes with respect to the CDV have been highlighted in yellow in this document.

CONTENTS

FOREWORD 7
0 Introduction 10
0.1 General 10
0.2 Use of extended assessment methods in Edition 4 12
0.3 Patent declaration 12
1 Scope 14
2 Normative references 14
3 Terms, definitions, symbols, abbreviated terms and conventions 16
3.1 Terms and definitions 16
3.2 Symbols and abbreviated terms 23
3.2.1 Abbreviated terms 23
3.2.2 Symbols 24
4 Conformance 25
5 Basics of safety-related fieldbus systems 25
5.1 Safety function decomposition 25
5.2 Communication system 26
5.2.1 General 26
5.2.2 IEC 61158 fieldbuses 26
5.2.3 Communication channel types 27
5.2.4 Safety function response time 27
5.3 Communication errors 28
5.3.1 General 28
5.3.2 Corruption 28
5.3.3 Unintended repetition 28
5.3.4 Incorrect sequence 28
5.3.5 Loss 29
5.3.6 Unacceptable delay 29
5.3.7 Insertion 29
5.3.8 Masquerade 29
5.3.9 Addressing 29
5.4 Deterministic remedial measures 29
5.4.1 General 29
5.4.2 Sequence number 29
5.4.3 Time stamp 29
5.4.4 Time expectation 30
5.4.5 Connection authentication 30
5.4.6 Feedback message 30
5.4.7 Data integrity assurance 30
5.4.8 Redundancy with cross checking 30
5.4.9 Different data integrity assurance systems 30
5.5 Typical relationships between errors and safety measures 31
5.6 Communication phases 32
5.7 FSCP implementation aspects 32
5.8 Models for estimation of the total residual error rate 33
5.8.1 Applicability 33

5.8.2 General models for black channel communications 33
5.8.3 Identification of generic safety properties 34
5.8.4 Assumptions for residual error rate calculations 35
5.8.5 Residual error rates 35
5.8.6 Data integrity 37
5.8.7 Authenticity 38
5.8.8 Timeliness 41
5.8.9 Masquerade 44
5.8.10 Calculation of the total residual error rates 44
5.8.11 Total residual error rate and SIL 46
5.8.12 Configuration and parameterization for an FSCP 46
5.9 Relationship between functional safety and security 48
5.10 Boundary conditions and constraints 48
5.10.1 Electrical safety 48
5.10.2 Electromagnetic compatibility (EMC) 49
5.11 Installation guidelines 49
5.12 Safety manual 49
5.13 Safety policy 49
6 Communication Profile Family 1 (FOUNDATION™ Fieldbus) – Profiles for functional safety 50
7 Communication Profile Family 2 (CIP™) and Family 16 (SERCOS®) – Profiles for functional safety 50
8 Communication Profile Family 3 (PROFIBUS™, PROFINET™) – Profiles for functional safety 51
9 Communication Profile Family 6 (INTERBUS®) – Profiles for functional safety 51
10 Communication Profile Family 8 (CC-Link™) – Profiles for functional safety 52
10.1 Functional Safety Communication Profile 8/1 52
10.2 Functional Safety Communication Profile 8/2 52
11 Communication Profile Family 12 (EtherCAT™) – Profiles for functional safety 52
12 Communication Profile Family 13 (Ethernet POWERLINK™) – Profiles for functional safety 53
13 Communication Profile Family 14 (EPA®) – Profiles for functional safety 53
14 Communication Profile Family 17 (RAPIEnet™) – Profiles for functional safety 53
15 Communication Profile Family 18 (SafetyNET p™ Fieldbus) – Profiles for functional safety 54
Annex A (informative) Example functional safety communication models 55
A.1 General 55
A.2 Model A (single message, channel and FAL, redundant SCLs) 55
A.3 Model B (full redundancy) 55
A.4 Model C (redundant messages, FALs and SCLs, single channel) 56
A.5 Model D (redundant messages and SCLs, single channel and FAL) 56
Annex B (normative) Safety communication channel model using CRC-based error checking 58
B.1 Overview 58
B.2 Channel model for calculations 58
B.3 Bit error probability Pe 59
B.4 Cyclic redundancy checking 60
B.4.1 General 60
B.4.2 Requirements for methods to calculate R_{CRC} 60

Annex C (informative) Structure of technology-specific parts 62
Annex D (informative) Assessment guideline 65
D.1 Overview 65
D.2 Channel types 65
D.2.1 General 65
D.2.2 Black channel 65
D.2.3 White channel 65
D.3 Data integrity considerations for white channel approaches 66
D.3.1 General 66
D.3.2 Models B and C 66
D.3.3 Models A and D 67
D.4 Verification of safety measures 67
D.4.1 General 67
D.4.2 Implementation 68
D.4.3 Default safety action 68
D.4.4 Safe state 68
D.4.5 Transmission errors 68
D.4.6 Safety reaction and response times 68
D.4.7 Combination of measures 68
D.4.8 Absence of interference 69
D.4.9 Additional fault causes (white channel) 69
D.4.10 Reference test beds and operational conditions 69
D.4.11 Conformance tester 69
Annex E (informative) Examples of implicit vs. explicit FSCP safety measures 70
E.1 General 70
E.2 Example fieldbus message with safety PDUs 70
E.3 Model with completely explicit safety measures 70
E.4 Model with explicit A-code and implicit T-code safety measures 71
E.5 Model with explicit T-code and implicit A-code safety measures 71
E.6 Model with split explicit and implicit safety measures 72
E.7 Model with completely implicit safety measures 73
E.8 Addition to Annex B – impact of implicit codes on properness 73
Annex F (informative) Legacy models for estimation of the total residual error rate 74
F.1 General 74
F.2 Calculation of the residual error rate 74
F.3 Total residual error rate and SIL 76
Annex G (informative) Implicit data safety mechanisms for IEC 61784-3 functional safety communication profiles (FSCPs) 77
G.1 Overview 77
G.2 Basic principles 77
G.3 Problem statement: constant values for implicit data 78
G.4 RP for FSCPs with random, uniformly distributed err_{impl} 81
G.4.1 General 81
G.4.2 Uniform distribution within the interval $[0;2^{i}-1]$, $i \geq r$ 82
G.4.3 Uniform distribution in the interval $[1;2^{r}-1]$, $i = r$ 84
G.5 General case 86
G.6 Calculation of P_{ID} 86
Annex H (informative) Residual error probability for example CRC codes (tables for verification of calculation methods) 88

H.1 Overview 88
H.2 Example of a 32 bit CRC 88
H.3 Example of a 16 bit CRC 93
H.4 Conclusion 97
Bibliography 99

Figure 1 – Relationships of IEC 61784-3 with other standards (machinery) 10
Figure 2 – Relationships of IEC 61784-3 with other standards (process) 11
Figure 3 – Transitions from Edition 2 to Edition 4 and future Edition 5 assessment methods 12
Figure 4 – Safety communication as a part of a safety function 26
Figure 5 – Example model of a functional safety communication system 27
Figure 6 – Example of safety function response time components 28
Figure 7 – Conceptual FSCP protocol model 32
Figure 8 – FSCP implementation aspects 33
Figure 9 – Black channel from an FSCP perspective 34
Figure 10 – Model for authentication considerations 39
Figure 11 – Fieldbus and internal address errors 40
Figure 12 – Example of slowly increasing message latency 42
Figure 13 – Example of an active network element failure 43
Figure 14 – Example application 1 (m = 4) 45
Figure 15 – Example application 2 (m = 2) 45
Figure 16 – Example of configuration and parameterization procedures for FSCP 47
Figure A.1 – Model A 55
Figure A.2 – Model B 56
Figure A.3 – Model C 56
Figure A.4 – Model D 57
Figure B.1 – Binary symmetric channel (BSC) 58
Figure B.2 – Block codes for error detection 59
Figure B.3 – Example of a block with a message part and a CRC signature 60
Figure B.4 – Proper and improper CRC polynomials 61
Figure D.1 – Basic Markov model 67
Figure E.1 – Example safety PDUs embedded in a fieldbus message 70
Figure E.2 – Model with completely explicit safety measures 70
Figure E.3 – Model with explicit A-code and implicit T-code safety measures 71
Figure E.4 – Model with explicit T-code and implicit A-code safety measures 72
Figure E.5 – Model with split explicit and implicit safety measures 72
Figure E.6 – Model with completely implicit safety measures 73
Figure F.1 – Example application 1 (m=4) 75
Figure F.2 – Example application 2 (m = 2) 76
Figure G.1 – FSCP with implicit transmission of authenticity and/or timeliness codes 78
Figure G.2 – Example of an incorrect transmission with multiple error causes 79
Figure G.3 – Impact of errors in implicit data on the residual error probability 80
Figure H.1 – Residual error probabilities (example of a 32 bit CRC – result 1) 90

Figure H.2 – Residual error probabilities (example of a 32 bit CRC – result 2) 90
Figure H.3 – Residual error probabilities (example of a 32 bit CRC – result 3) 91
Figure H.4 – Residual error probabilities (example of a 32 bit CRC – result 4) 91
Figure H.5 – Residual error probabilities (example of a 32 bit CRC – result 5) 92
Figure H.6 – Residual error probabilities (example of a 32 bit CRC – result 6) 92
Figure H.7 – Residual error probabilities (example of a 16 bit CRC – result 1) 95
Figure H.8 – Residual error probabilities (example of a 16 bit CRC – result 2) 95
Figure H.9 – Residual error probabilities (example of a 16 bit CRC – result 3) 96
Figure H.10 – Residual error probabilities (example of a 16 bit CRC – result 4) 96
Figure H.11 – Residual error probabilities (example of a 16 bit CRC – result 5) 97
Figure H.12 – Example 1 of improper polynomial 97
Figure H.13 – Example 2 of improper polynomial 98

Table 1 – Overview of the effectiveness of the various measures on the possible errors 31
Table 2 – Typical relationship of residual error rate to SIL 46
Table 3 – Typical relationship of residual error on demand to SIL 46
Table 4 – Overview of profile identifier usable for FSCP 6/7 51
Table B.1 – Example dependency d_{min} and block bit length n 59
Table C.1 – Common subclause structure for technology-specific parts 62
Table F.1 – Definition of items used for calculation of the residual error rates 75
Table F.2 – Typical relationship of residual error rate to SIL 76
Table F.3 – Typical relationship of residual error on demand to SIL 76
Table H.1 – Residual error probabilities (R_{CRC1}) for example CRC32 polynomial 89
Table H.2 – Residual error probabilities (R_{CRC2}) for example CRC16 polynomial 94

INTERNATIONAL ELECTROTECHNICAL COMMISSION

____

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES –

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

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.

2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.

3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.

4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.

5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.

6) All users should ensure that they have the latest edition of this publication.

7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.

8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.

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

This 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.

- 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 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.
- New informative Annex H, providing additional guidance for the calculation of R_{CRC}.

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

FDIS	Report on voting
65C/XX/FDIS	65C/XX/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.

The National Committees are requested to note that for this document the stability date is 2024.

THIS TEXT IS INCLUDED FOR THE INFORMATION OF THE NATIONAL COMMITTEES AND WILL BE DELETED AT THE PUBLICATION STAGE.

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.

90

91

Changes with respect to the second CD for this edition have been highlighted in yellow in this document. Note that the new draft Annex I introduced in the second CD and all corresponding references have been deleted from this document, instead Annex I contents will be further developed in a follow up Amendment. All references to IEC TR 62685:2010 (Assessment guideline for safety devices using IEC 61784-3FSCPs) have also been deleted, since the document is now withdrawn.

THIS TEXT IS INCLUDED FOR THE INFORMATION OF THE NATIONAL COMMITTEES AND WILL BE DELETED AT THE PUBLICATION STAGE.

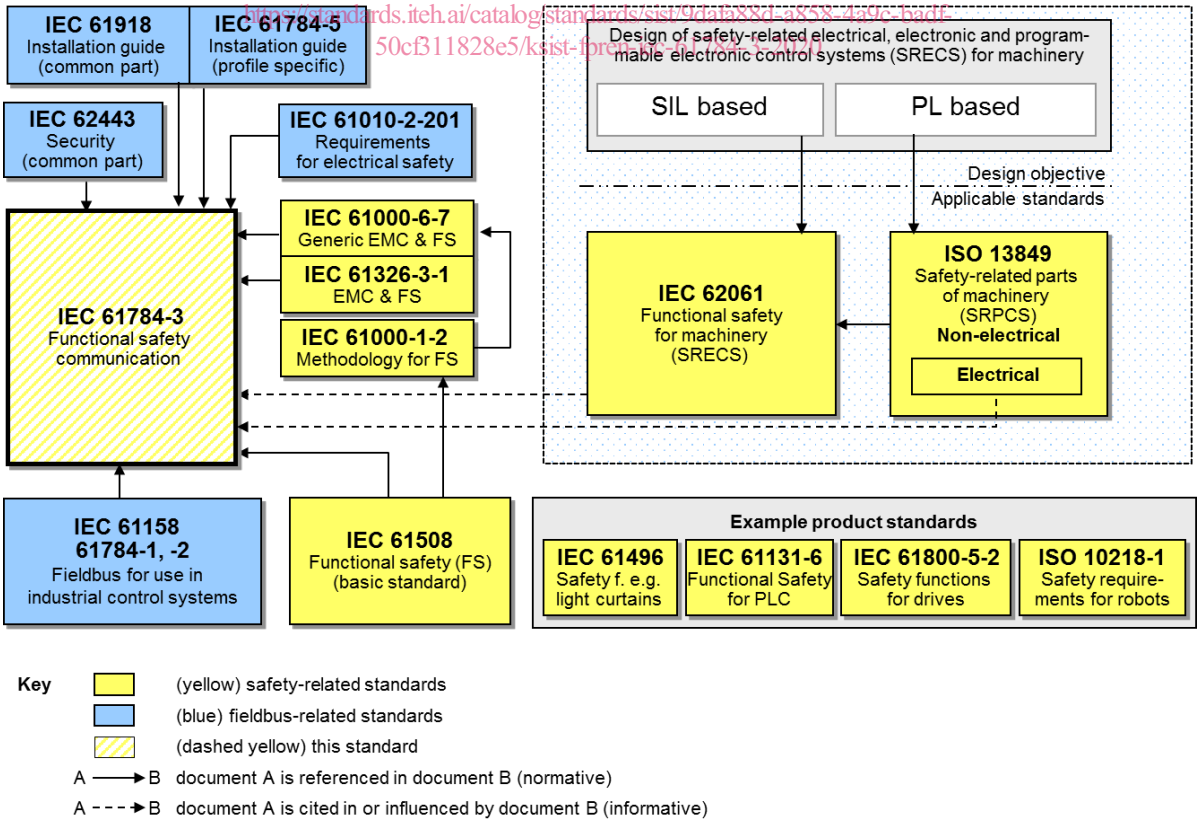
0 Introduction

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.

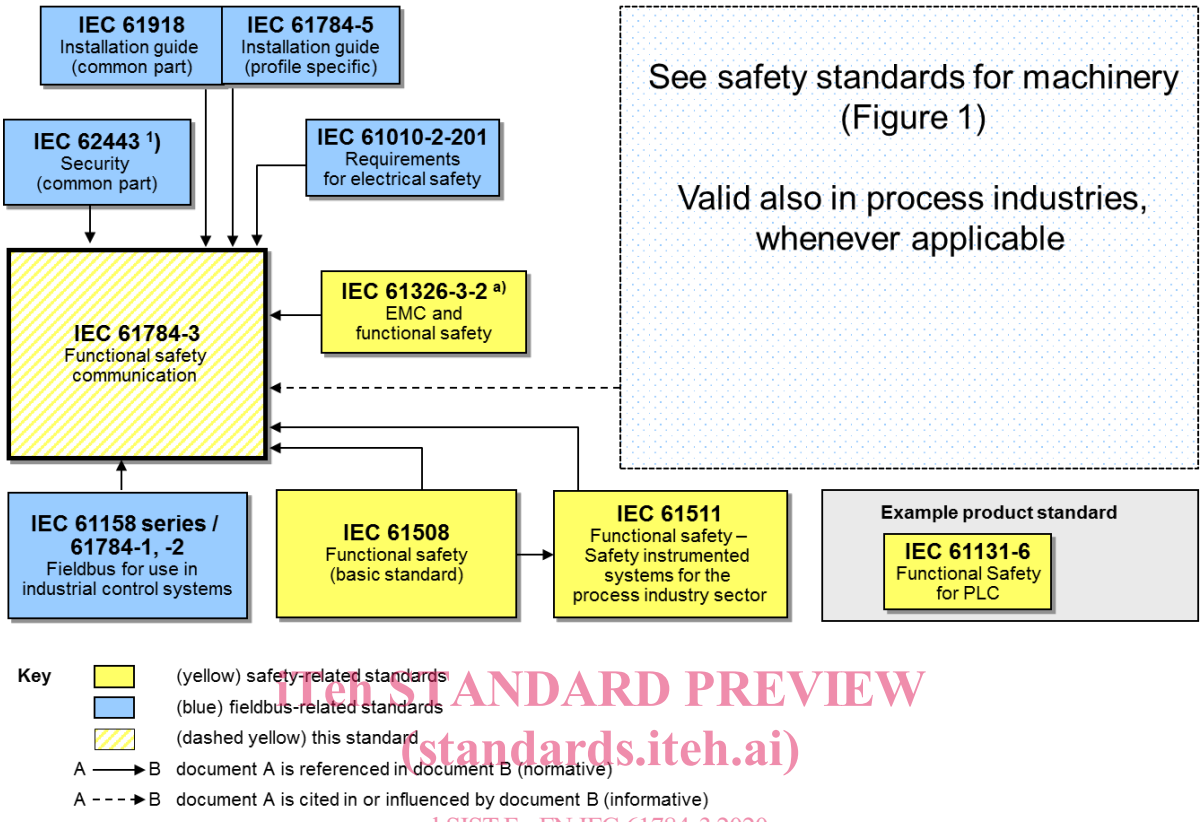
Figure 1 shows the relationships between IEC 61784-3 (all parts) and relevant safety and fieldbus standards in a machinery environment.



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:

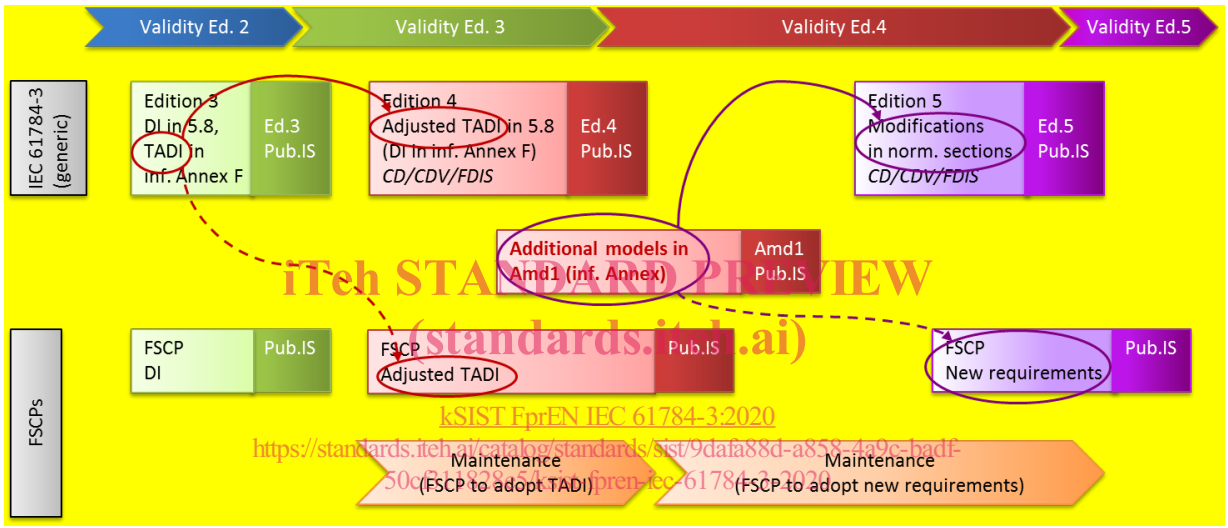
- basic principles for implementing the requirements of IEC 61508 (all parts) for safety-related data communications, including possible transmission faults, remedial measures and considerations affecting data integrity;
- functional safety communication profiles for several communication profile families 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 Edition 2 to Edition 4 and future Edition 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 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.

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

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

180

181