Edition 2.0 2010-06

INTERNATIONAL STANDARD

colour inside

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

INTERNATIONAL ELECTROTECHNICAL COMMISSION

PRICE CODE XA

ICS 25.040.40; 35.100.05

ISBN 978-2-88910-948-7

CONTENTS

FOREWORD 6
0 Introduction 8
0.1 General 8
0.2 Patent declaration 10
1 Scope 11
2 Normative references 11
3 Terms, definitions, symbols, abbreviated terms and conventions 13
3.1 Terms and definitions 13
3.1.1 Common terms and definitions 13
3.1.2 CPF 1: Additional terms and definitions 18
3.1.3 CPF 2: Additional terms and definitions 18
3.1.4 CPF 3: Additional terms and definitions 18
3.1.5 CPF 6: Additional terms and definitions 18
3.1.6 CPF 8: Additional terms and definitions 18
3.1.7 CPF 12: Additional terms and definitions 18
3.1.8 CPF 13: Additional terms and definitions 18
3.1.9 CPF 14: Additional terms and definitions 18
3.2 Symbols and abbreviated terms 19
3.2.1 Common symbols and abbreviated terms 19
3.2.2 CPF 1: Additional symbols and abbreviated terms 19
3.2.3 CPF 2: Additional symbols and abbreviated terms 19
3.2.4 CPF 3: Additional symbols and abbreviated terms 19
3.2.5 CPF 6: Additional symbols and abbreviated terms 20
3.2.6 CPF 8: Additional symbols and abbreviated terms 20
3.2.7 CPF 12: Additional symbols and abbreviated terms 20
3.2.8 CPF 13: Additional symbols and abbreviated terms 20
3.2.9 CPF 14: Additional symbols and abbreviated terms 20
4 Conformance 20
5 Basics of safety-related fieldbus systems 21
5.1 Safety function decomposition 21
5.2 Communication system 21
5.2.1 General 21
5.2.2 IEC 61158 fieldbuses 21
5.2.3 Communication channel types 22
5.2.4 Safety function response time 22
5.3 Communication errors 23
5.3.1 General 23
5.3.2 Corruption 23
5.3.3 Unintended repetition 23
5.3.4 Incorrect sequence 23
5.3.5 Loss 24
5.3.6 Unacceptable delay 24
5.3.7 Insertion 24
5.3.8 Masquerade 24
5.3.9 Addressing 24
5.4 Deterministic remedial measures 24

5.4.1 General 24
5.4.2 Sequence number 25
5.4.3 Time stamp 25
5.4.4 Time expectation 25
5.4.5 Connection authentication 25
5.4.6 Feedback message 25
5.4.7 Data integrity assurance 25
5.4.8 Redundancy with cross checking 25
5.4.9 Different data integrity assurance systems 26
5.5 Relationships between errors and safety measures 26
5.6 Data integrity considerations 27
5.6.1 Calculation of the residual error rate 27
5.6.2 Residual error rate and SIL 29
5.7 Relationship between functional safety and security 29
5.8 Boundary conditions and constraints 30
5.8.1 Electrical safety 30
5.8.2 Electromagnetic compatibility (EMC) 30
5.9 Installation guidelines 30
5.10 Safety manual 30
5.11 Safety policy 30
6 Communication Profile Family 1 (FOUNDATION™ Fieldbus) – Profiles for functional safety 31
6.1 Functional Safety Communication Profile 1/1 31
6.2 Technical overview 31
7 Communication Profile Family 2 (CIP™) – Profiles for functional safety 32
7.1 Functional Safety Communication Profile 2/1 32
7.2 Technical overview 32
8 Communication Profile Family 3 (PROFIBUS™, PROFINET™) – Profiles for functional safety 34
8.1 Functional Safety Communication Profile 3/1 34
8.2 Technical overview 34
9 Communication Profile Family 6 (INTERBUS®) – Profiles for functional safety 36
9.1 Functional Safety Communication Profile 6/7 36
9.2 Technical overview 37
10 Communication Profile Family 8 (CC-Link™) – Profiles for functional safety 38
10.1 Functional Safety Communication Profile 8/1 38
10.2 Technical overview 38
11 Communication Profile Family 12 (EtherCAT™) – Profiles for functional safety 39
11.1 Functional Safety Communication Profile 12/1 39
11.2 Technical overview 39
12 Communication Profile Family 13 (Ethernet POWERLINK™) – Profiles for functional safety 40
12.1 Functional Safety Communication Profile 13/1 40
12.2 Technical overview 40
13 Communication Profile Family 14 (EPA®) – Profiles for functional safety 41
13.1 Functional Safety Communication Profile 14/1 41
13.2 Technical overview 42
Annex A (informative) Example functional safety communication models 43

A.1 General 43
A.2 Model A 43
A.3 Model B 43
A.4 Model C 44
A.5 Model D 44
Annex B (informative) A safety communication channel model using CRC-based error checking 46
B.1 Overview 46
B.2 Channel model for calculations 46
B.3 Cyclic redundancy checking 47
B.3.1 General 47
B.3.2 Considerations concerning CRC polynomials 49
Annex C (informative) Structure of technology-specific parts 51
Annex D (informative) Assessment guideline 53
D.1 Overview 53
D.2 Channel types 53
D.2.1 General 53
D.2.2 Black channel 53
D.2.3 White channel 53
D.3 Data integrity considerations for white channel approaches 54
D.3.1 General 54
D.3.2 Model B and C 54
D.3.3 Model A and D 55
D.4 Verification of safety measures 55
D.4.1 General 55
D.4.2 Implementation 56
D.4.3 "De-energize to trip" principle 56
D.4.4 Safe state 56
D.4.5 Transmission errors 56
D.4.6 Safety reaction and response times 56
D.4.7 Combination of measures 56
D.4.8 Absence of interference 57
D.4.9 Additional fault causes (white channel) 57
D.4.10 Reference test beds and operational conditions 57
D.4.11 Conformance tester 57
Bibliography 58

Table 1 – Overview of the effectiveness of the various measures on the possible errors 27
Table 2 – Definition of items used for calculation of the residual error rate 28
Table 3 – Relationship of residual error rate to SIL level 29
Table 4 – Overview of profile identifier usable for FSCP 6/7 37
Table B.1 – Example dependency d_{min} and block length n 49
Table C.1 – Common subclause structure for technology-specific parts 51

Figure 1 – Relationships of IEC 61784-3 with other standards (machinery) 8
Figure 2 – Relationships of IEC 61784-3 with other standards (process) 9
Figure 3 – Safety communication as a part of a safety function 21
Figure 4 – Example model of a functional safety communication system 22
Figure 5 – Example of safety function response time components 23
Figure 6 – Example application 29
Figure 7 – Scope of FSCP 1/1 32
Figure 8 – Relationship of Safety Validators 33
Figure 9 – Basic communication preconditions for FSCP 3/1 35
Figure 10 – Structure of a FSCP 3/1 safety PDU 35
Figure 11 – Safe communication modes 36
Figure 12 – FSCP 6/7 communication preconditions 37
Figure 13 – Basic FSCP 12/1 system 39
Figure 14 – Producer consumer example 41
Figure 15 – Client server example 41
Figure 16 – FSCP 14/1 safety communication architecture 42
Figure A.1 – Model A 43
Figure A.2 – Model B 44
Figure A.3 – Model C 44
Figure A.4 – Model D 45
Figure B.1 – Communication channel with perturbation 46
Figure B.2 – Binary symmetric channel (BSC) 47
Figure B.3 – Example of a block with message and CRC bits (redundancy code) 48
Figure B.4 – Block codes for error detection 48
Figure B.5 – Proper and improper CRC polynomials 49
Figure D.1 – Basic Markov model 55

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 second edition cancels and replaces the first edition published in 2007. This edition constitutes a technical revision. The main changes with respect to the previous edition are listed below:

- clarifications and additional explanations for requirements, updated references;
- updates of definitions and requirements in relation with the new edition of IEC 61508;
- addition of a new informative Annex D providing an assessment guideline;
- updates in parts for CPF 1, CPF 2, CPF 3, CPF 6 (details provided in the parts);
- addition of new parts for CPF 8, CPF 12, CPF 13, CPF 14;
- in CPF parts, addition of an annex to provide information about test laboratories for testing and validating conformance of FSCP products.

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

FDIS	Report on voting
65C/591A/FDIS	65C/603/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.

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 this publication 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.

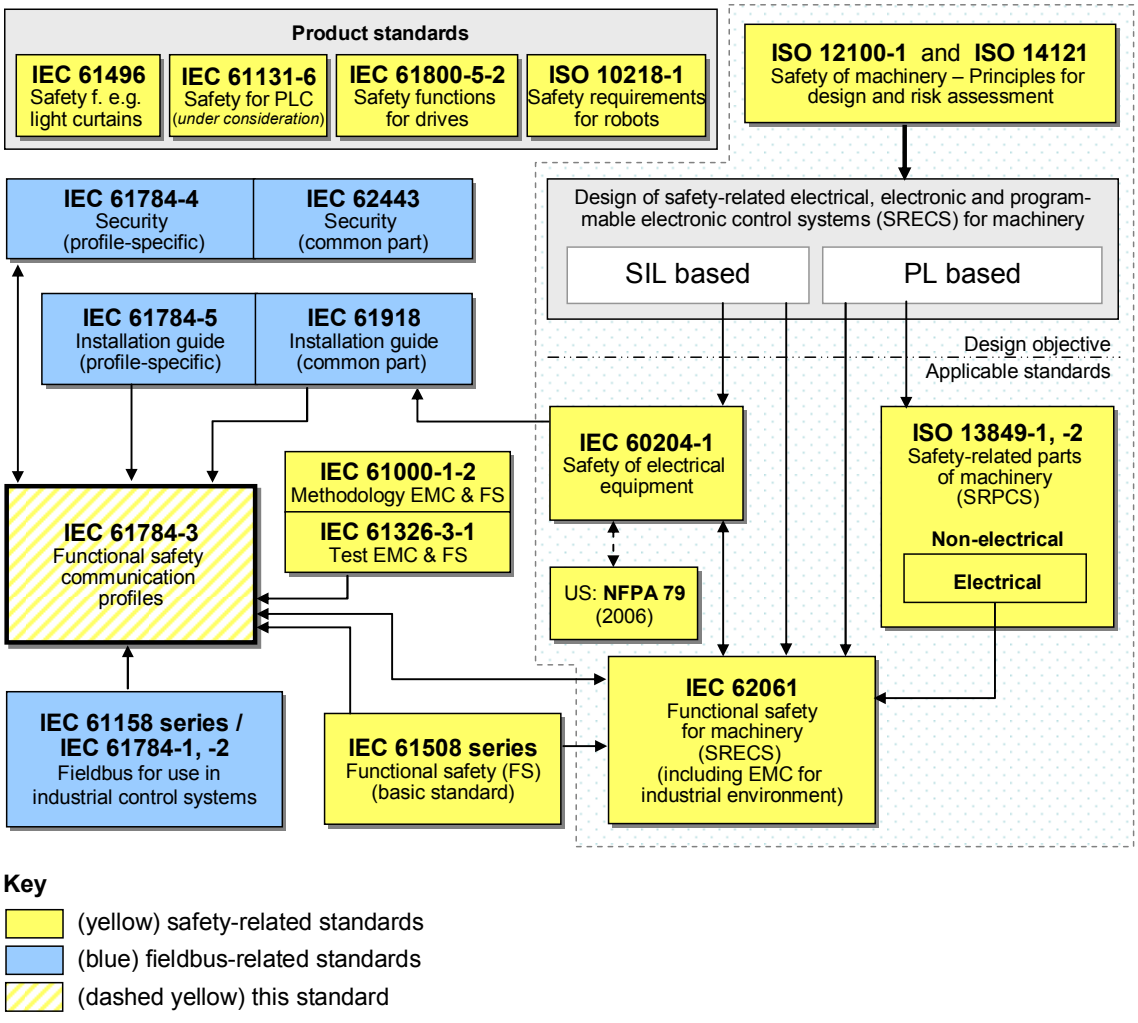
0 Introduction

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 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.

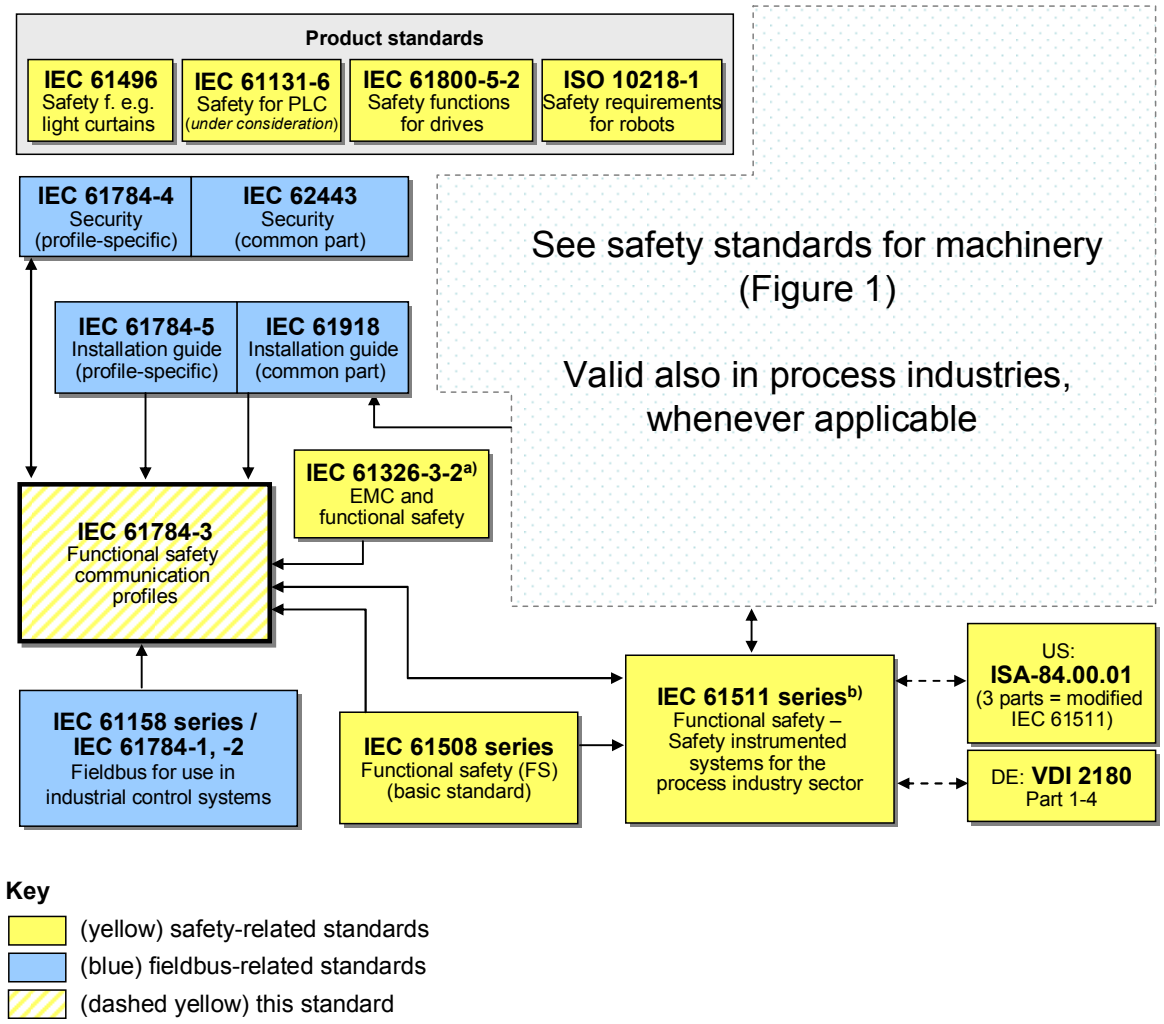
Figure 1 shows the relationships between this standard and relevant safety and fieldbus standards in a machinery environment.



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.

[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 series 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.

0.2 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, 12, 13 and 14 given in IEC 61784-3-1, IEC 61784-3-2, IEC 61784-3-3, IEC 61784-3-6, IEC 61784-3-12, IEC 61784-3-13 and IEC 61784-3-14.

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.

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 61784-3-12, IEC 61784-3-13 and IEC 61784-3-14.

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[1] for functional safety. These principles 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.

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. 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 may also be specified in IEC 61784-4[3] [10].

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*

---

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.

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[4], *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 61784-3-8[5], *Industrial communication networks – Profiles – Part 3-8: Functional safety fieldbuses – Additional specifications for CPF 8*

IEC 61784-3-12[5], *Industrial communication networks – Profiles – Part 3-12: Functional safety fieldbuses – Additional specifications for CPF 12*

IEC 61784-3-13[5], *Industrial communication networks – Profiles – Part 3-13: Functional safety fieldbuses – Additional specifications for CPF 13*

IEC 61784-3-14[5], *Industrial communication networks – Profiles – Part 3-14: Functional safety fieldbuses – Additional specifications for CPF 14*

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*

---

4 To be published.

5 To be published.

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

3 Terms, definitions, symbols, abbreviated terms and conventions

3.1 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1.1 Common terms and definitions

3.1.1.1
absolute time stamp
time stamp referenced to a global time which is common for a group of devices using a *fieldbus*
[IEC 62280-2, modified]

3.1.1.2
availability
probability for an automated system that for a given period of time there are no unsatisfactory system conditions such as loss of production

3.1.1.3
black channel
communication channel without available evidence of design or validation according to IEC 61508

3.1.1.4
bridge
abstract device that connects multiple network segments along the data link layer

3.1.1.5
communication channel
logical connection between two end-points within a *communication system*

3.1.1.6
communication system
arrangement of hardware, software and propagation media to allow the transfer of *messages* (ISO/IEC 7498 application layer) from one application to another

3.1.1.7
connection
logical binding between two application objects within the same or different devices

3.1.1.8
Cyclic Redundancy Check (CRC)
<value> redundant data derived from, and stored or transmitted together with, a block of data in order to detect data corruption

<method> procedure used to calculate the redundant data

NOTE 1 Terms “CRC code” and "CRC signature", and labels such as CRC1, CRC2, may also be used in this standard to refer to the redundant data.

NOTE 2 See also [29], [30][6].

---

6 Figures in square brackets refer to the bibliography.