

INTERNATIONAL STANDARD

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

(<https://standards.iteh.ai/>)
Document Preview

IEC 61784-3:2007

<https://standards.iteh.ai/catalog/standards/iec/179847db-72ce-47d7-8ed0-62589ec547c9/iec-61784-3-2007>

Withhold



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2007 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester.

If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

IEC Central Office
3, rue de Varembe
CH-1211 Geneva 20
Switzerland
Email: inmail@iec.ch
Web: www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

- Catalogue of IEC publications: www.iec.ch/searchpub

The IEC on-line Catalogue enables you to search by a variety of criteria (reference number, text, technical committee,...). It also gives information on projects, withdrawn and replaced publications.

- IEC Just Published: www.iec.ch/online_news/justpub

Stay up to date on all new IEC publications. Just Published details twice a month all new publications released. Available on-line and also by email.

- Electropedia: www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 20 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary online.

- Customer Service Centre: www.iec.ch/webstore/custserv

If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us:

Email: csc@iec.ch

Tel.: +41 22 919 02 11

Fax: +41 22 919 03 00

IEC 61784-3:2007

<https://standards.iec.org/standards/iec/179847db-72ce-47d7-8ed0-62589ec547c9/iec-61784-3-2007>

INTERNATIONAL STANDARD

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

<https://standards.iteh.ai/standards/iec/61784-3-2007>
<https://standards.iteh.ai/catalog/standards/iec/179847db-72ce-47d7-8ed0-62589ec547c9/iec-61784-3-2007>

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

PRICE CODE



CONTENTS

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

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

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

INTERNATIONAL ELECTROTECHNICAL COMMISSION

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES

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

FOREWORD

- 1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
- 2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
- 3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
- 4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
- 5) IEC provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with an IEC Publication.
- 6) All users should ensure that they have the latest edition of this publication.
- 7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
- 8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
- 9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

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

IEC takes no position concerning the evidence, validity and scope of these patent rights. The holders of these patent rights have assured the IEC that they are willing to negotiate licences under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statements of the holders of these patent rights are registered with IEC.

NOTE Patent details and corresponding contact information are provided in IEC 61784-3-1, IEC 61784-3-2, IEC 61784-3-3 and IEC 61784-3-6.

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

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

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

Full information on the voting for the approval of this standard can be found in the report on voting indicated in the above table.

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

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

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

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

iTeh Standards
(<https://standards.itih.ai>)
Document Preview

IEC 61784-3:2007

<https://standards.itih.ai/catalog/standards/iec/179847db-72ce-47d7-8ed0-62589ec547c9/iec-61784-3-2007>

INTRODUCTION

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

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

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

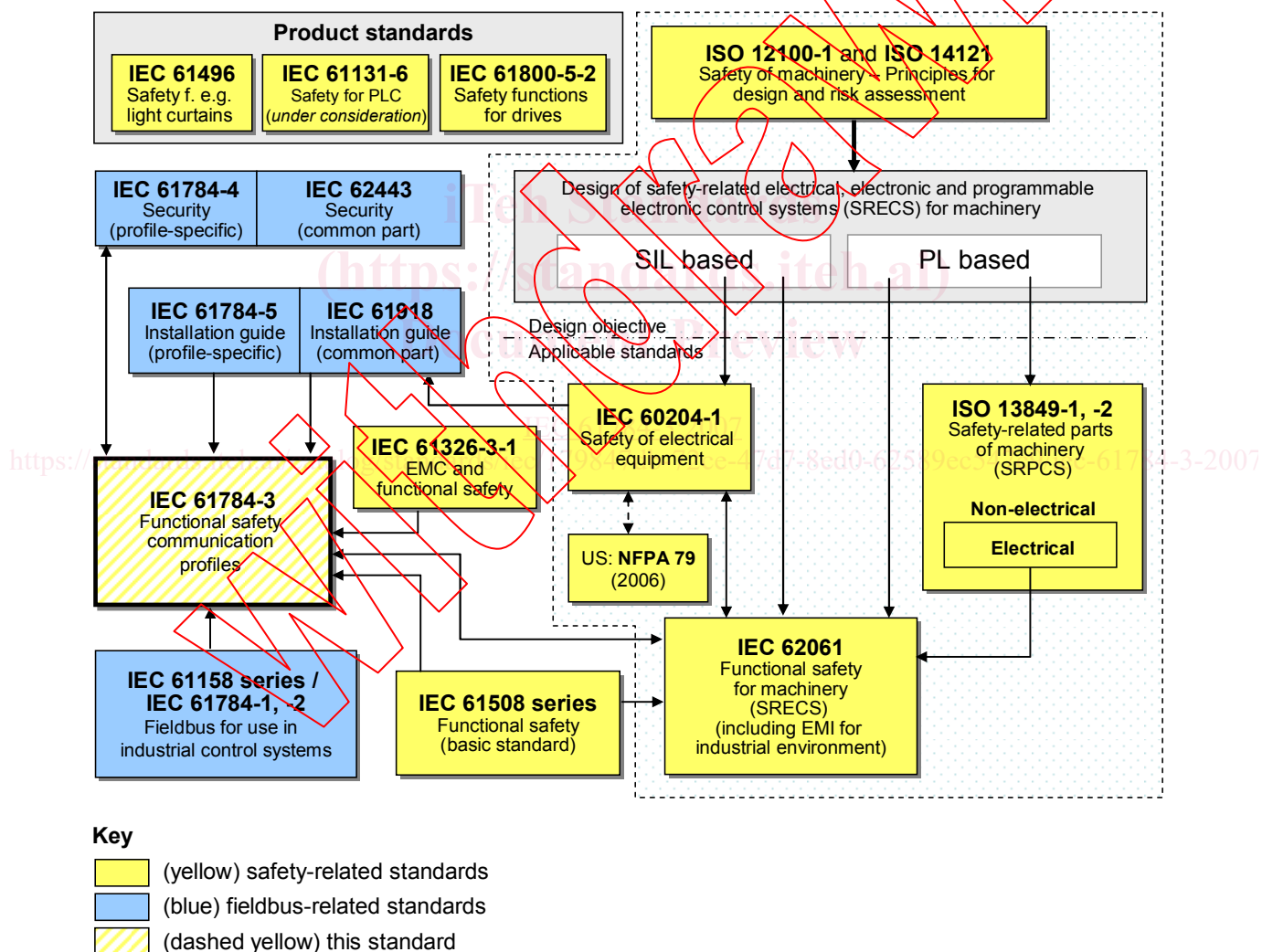


Figure 1 – Relationships of IEC 61784-3 with other standards (machinery)

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

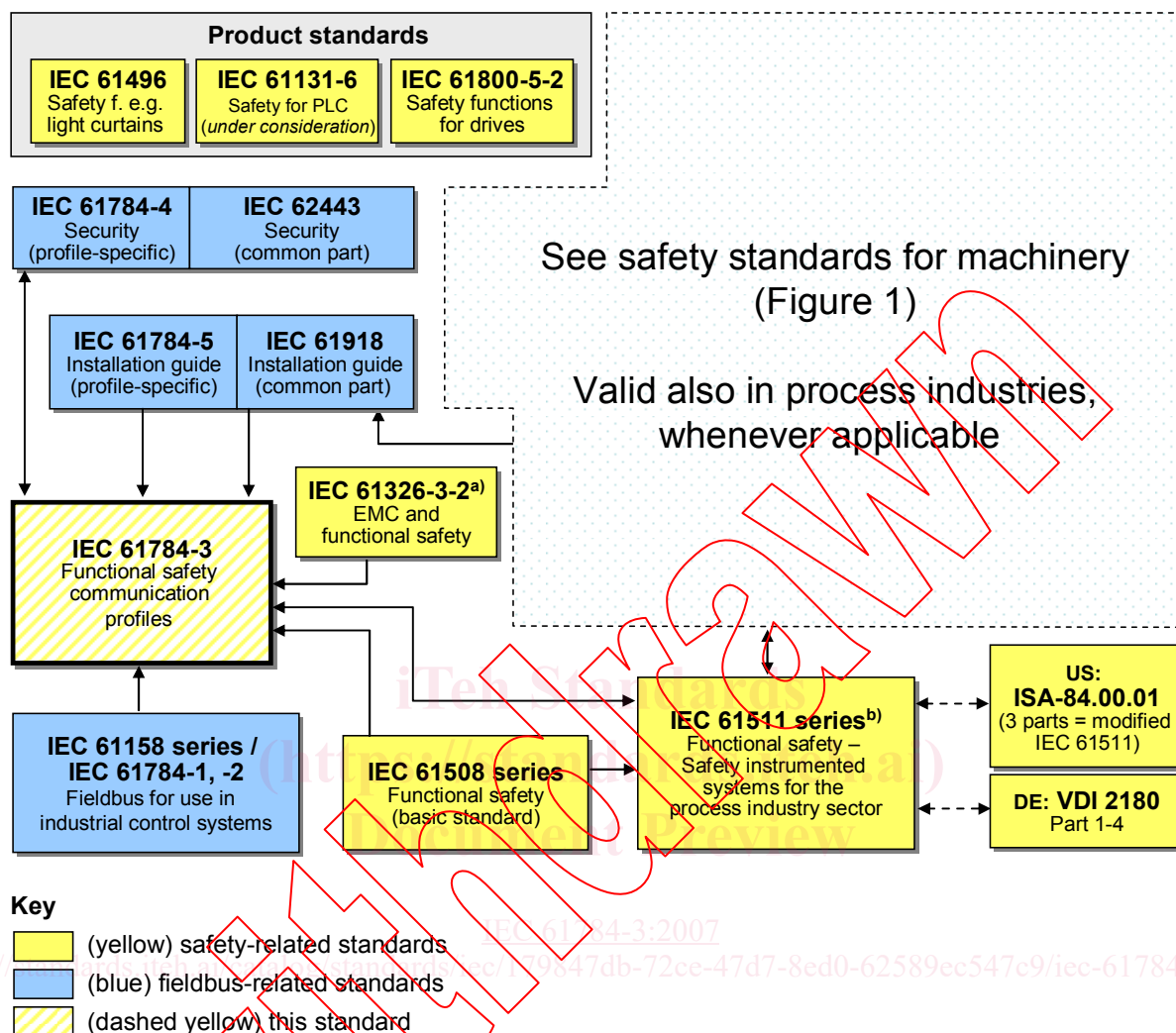


Figure 2 – Relationships of IEC 61784-3 with other standards (process)

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

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

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

This standard describes:

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

Withdrawing

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

IEC 61784-3:2007
<https://standards.iteh.ai/catalog/standards/iec/179847db-72ce-47d7-8ed0-62589ec547c9/iec-61784-3-2007>

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES

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

1 Scope

This part of the IEC 61784-3 series explains some common principles than can be used in the transmission of safety-relevant messages among participants within a distributed network using fieldbus technology in accordance with the requirements of IEC 61508 series for functional safety. These principles can be used in various industrial applications such as process control, manufacturing automation and machinery.

This part¹ and the IEC 61784-3-x parts specify several functional safety communication profiles based on the communication profiles and protocol layers of the fieldbus technologies in IEC 61784-1, IEC 61784-2 and the IEC 61158 series.

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

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

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

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

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

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

2 Normative references

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

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

IEC 61158 (all parts), *Industrial communication networks – Fieldbus specifications*

IEC 61326-3-1, *Electrical equipment for measurement, control and laboratory use – EMC requirements – Part 3-1: Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety) – General industrial applications*²

IEC 61326-3-2, *Electrical equipment for measurement, control and laboratory use – EMC requirements – Part 3-2: Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety) – Industrial applications with specified EM environment*²

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

² To be published.

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

IEC 61508-1, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements*

IEC 61508-2, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*

IEC 61784-1, *Industrial communication networks – Profiles – Part 1: Fieldbus profiles*

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

IEC 61784-3-1, *Industrial communication networks – Profiles – Part 3-1: Functional safety fieldbuses – Additional specifications for CPF 1*

IEC 61784-3-2, *Industrial communication networks – Profiles – Part 3-2: Functional safety fieldbuses – Additional specifications for CPF 2*

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

IEC 61784-3-6, *Industrial communication networks – Profiles – Part 3-6: Functional safety fieldbuses – Additional specifications for CPF 6*

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

IEC 61918, *Industrial communication networks – Installation of communication networks in industrial premises*

IEC 62280-1:2002, *Railway applications – Communication, signalling and processing systems – Part 1: Safety-related communication in closed transmission systems*

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

NOTE Availability depends on MTBF (mean time between failure) and MDT (mean down time):
Availability = $MTBF / (MTBF + MDT)$.

3.1.1.3

black channel

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

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 [26], [27]³

3.1.1.9

diversity

different means of performing a required function

EXAMPLE Diversity may be achieved by different physical methods or different design approaches.

[IEC 61508-4:1998]

3.1.1.10

error

discrepancy between a computed, observed or measured value or condition and the true, specified or theoretically correct value or condition

NOTE 1 An error can be caused by a faulty item, e.g. a computing error made by faulty computer equipment.

[IEV 191-05-24], [IEC 61508-4:1998], [IEC 61158]

NOTE 2 Errors may be due to design mistakes within hardware/software and/or corrupted information due to electromagnetic interference and/or other effects.

NOTE 3 Errors do not necessarily result in a *failure* or a *fault*.

3.1.1.11

failure

termination of the ability of a functional unit to perform a required function

³ Figures in square brackets refer to the bibliography.