IEC 61784-3-8

Edition 1.0 2010-06

INTERNATIONAL STANDARD

colour inside

Industrial communication networks – Profiles – Part 3-8: Functional safety fieldbuses – Additional specifications for CPF 8

IEC 61784-3-8:2010(E)

IEC Central Office
3, rue de Varembé
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 It also gives information on projects, withdrawn and replaced publications.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 61784-3-8

Edition 1.0 2010-06

INTERNATIONAL STANDARD

Industrial communication networks – Profiles – Part 3-8: Functional safety fieldbuses – Additional specifications for CPF 8

INTERNATIONAL ELECTROTECHNICAL COMMISSION

PRICE CODE X

ICS 25.040.40; 35.100.05

ISBN 978-2-88910-980-7

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 8: Additional terms and definitions 16
3.2 Symbols and abbreviated terms 16
3.2.1 Common symbols and abbreviated terms 16
3.2.2 CPF 8: Additional symbols and abbreviated terms 17
3.3 Conventions 17
4 Overview of FSCP 8/1 (CC-Link Safety™) 17
5 General 18
5.1 External documents providing specifications for the profile 18
5.2 Safety functional requirements 18
5.3 Safety measures 18
5.3.1 General 18
5.3.2 Sequence number 19
5.3.3 Time expectation 19
5.3.4 Connection authentication 20
5.3.5 Feedback message 20
5.3.6 Different data integrity assurance system 20
5.4 Safety communication layer structure 20
5.5 Relationships with FAL (and DLL, PhL) 21
5.5.1 Overview 21
5.5.2 Data types 21
6 Safety communication layer services 21
6.1 General 21
6.2 SASEs 21
6.2.1 M1 safety device manager class specification 21
6.2.2 S1 safety device manager class specification 22
6.3 SARs 22
6.3.1 M1 safety connection manager class 22
6.3.2 S1 safety connection manager class 22
6.4 Process data SAR ASEs 23
6.4.1 M1 safety cyclic transmission class specification 23
6.4.2 S1 safety cyclic transmission class specification 23
7 Safety communication layer protocol 24
7.1 Safety PDU format 24
7.1.1 General 24
7.1.2 Abstract syntax 24
7.1.3 Transfer syntax 26
7.2 State description 30
7.2.1 Overview 30
7.2.2 Idle 31

7.2.3 FAL running 31
7.2.4 SCL running 32
7.2.5 Fail safe 32
7.2.6 Safety data transmission and processing 32
7.2.7 Forced termination 34

8 Safety communication layer management 34
8.1 General 34
8.2 Connection establishment and confirmation processing 35
8.3 Safety slave verification 35
8.3.1 General 35
8.3.2 Safety slave information verification process 35
8.3.3 Safety slave parameter transmission 35

9 System requirements 36
9.1 Indicators and switches 36
9.1.1 Switches 36
9.1.2 Indicators 36
9.2 Installation guidelines 37
9.3 Safety function response time 37
9.3.1 General 37
9.3.2 Time calculation 37
9.4 Duration of demands 39
9.5 Constraints for calculation of system characteristics 39
9.5.1 System characteristics 39
9.5.2 Residual error rate (Λ) 39
9.6 Maintenance 40
9.7 Safety manual 40

10 Assessment 41

Annex A (informative) Additional information for functional safety communication profiles of CPF 8 42

A.1 Hash function calculation 42

A.2 … 42

Annex B (informative) Information for assessment of the functional safety communication profiles of CPF 8 43

Bibliography 44

Table 1 – Selection of the various measures for possible errors 19

Table 2 – M1 safety device manager attribute format 24

Table 3 – S1 safety device manager attribute format 24

Table 4 – M1 safety connection manager attribute format 24

Table 5 – S1 safety connection manager attribute format 25

Table 6 – M1 safety cyclic transmission attribute format 25

Table 7 – S1 safety cyclic transmission attribute format 26

Table 8 – M1 safety device manager attribute encoding 26

Table 9 – S1 safety device manager attribute encoding 27

Table 10 – M1 safety connection manager attribute encoding 27

Table 11 – S1 safety connection manager attribute encoding 27

Table 12 – M1 safety cyclic transmission attribute encoding 28
Table 13 – S1 safety cyclic transmission attribute encoding 29
Table 14 – Safety master monitor timer operation 33
Table 15 – Safety slave monitor timer operation 33
Table 16 – Safety data monitor timer operation 33
Table 17 – Details of connection establishment and confirmation processing 35
Table 18 – Details of slave information verification processing 35
Table 19 – Details of safety slave parameter transmission processing 36
Table 20 – Monitor LEDs 36
Table 21 – Safety function response time calculation 38
Table 22 – Safety function response time definition of terms 38
Table 23 – Number of occupied slots and safety data 39
Table 24 – Residual error rate Λ (occupied slots = 1) 40
Table 25 – Residual error rate Λ (occupied slots = 2) 40

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 – Relationship between SCL and the other layers of IEC 61158 Type 18 21
Figure 4 – State diagram 31

INTERNATIONAL ELECTROTECHNICAL COMMISSION

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES –

Part 3-8: Functional safety fieldbuses – Additional specifications for CPF 8

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 61784-3-8 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/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.

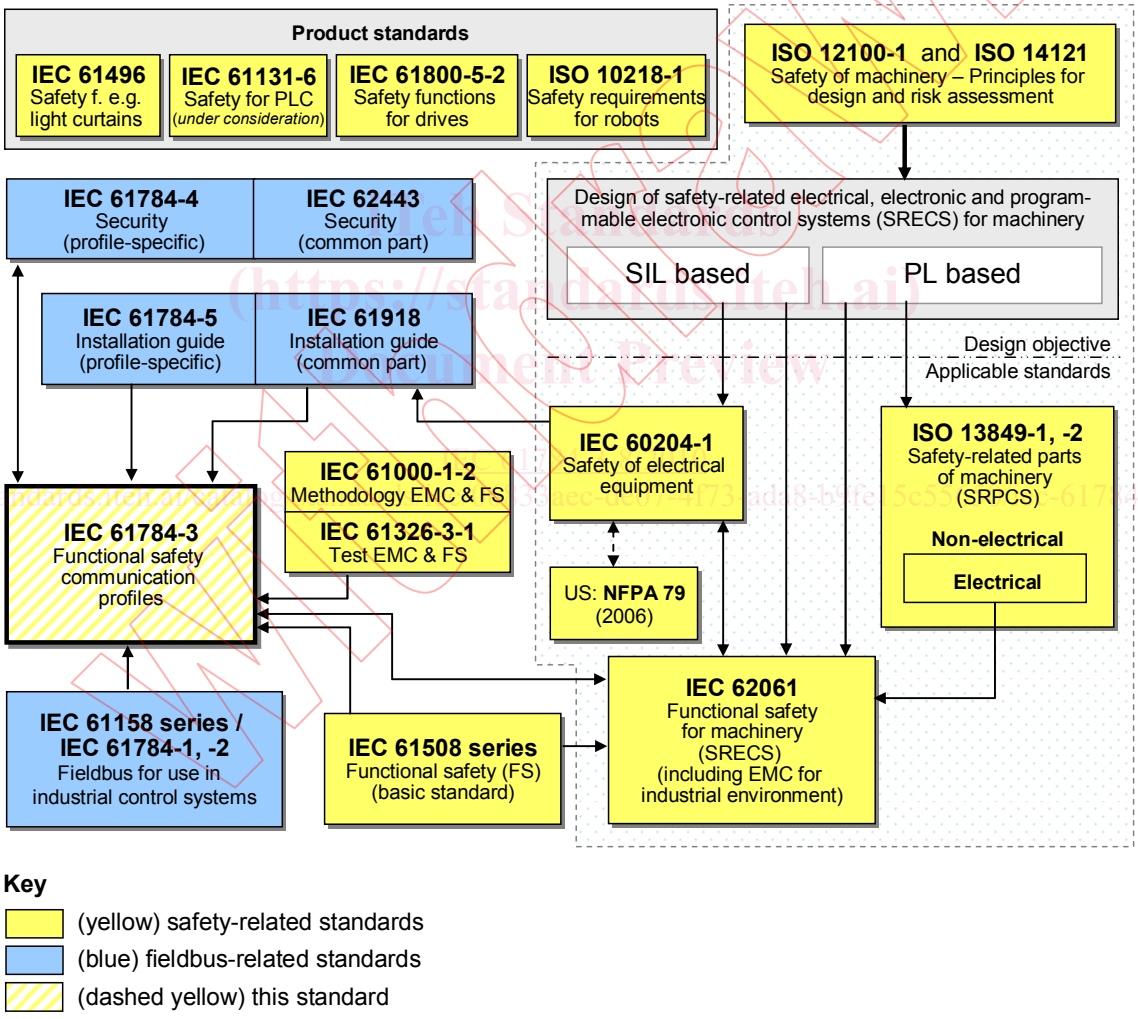
IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

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.

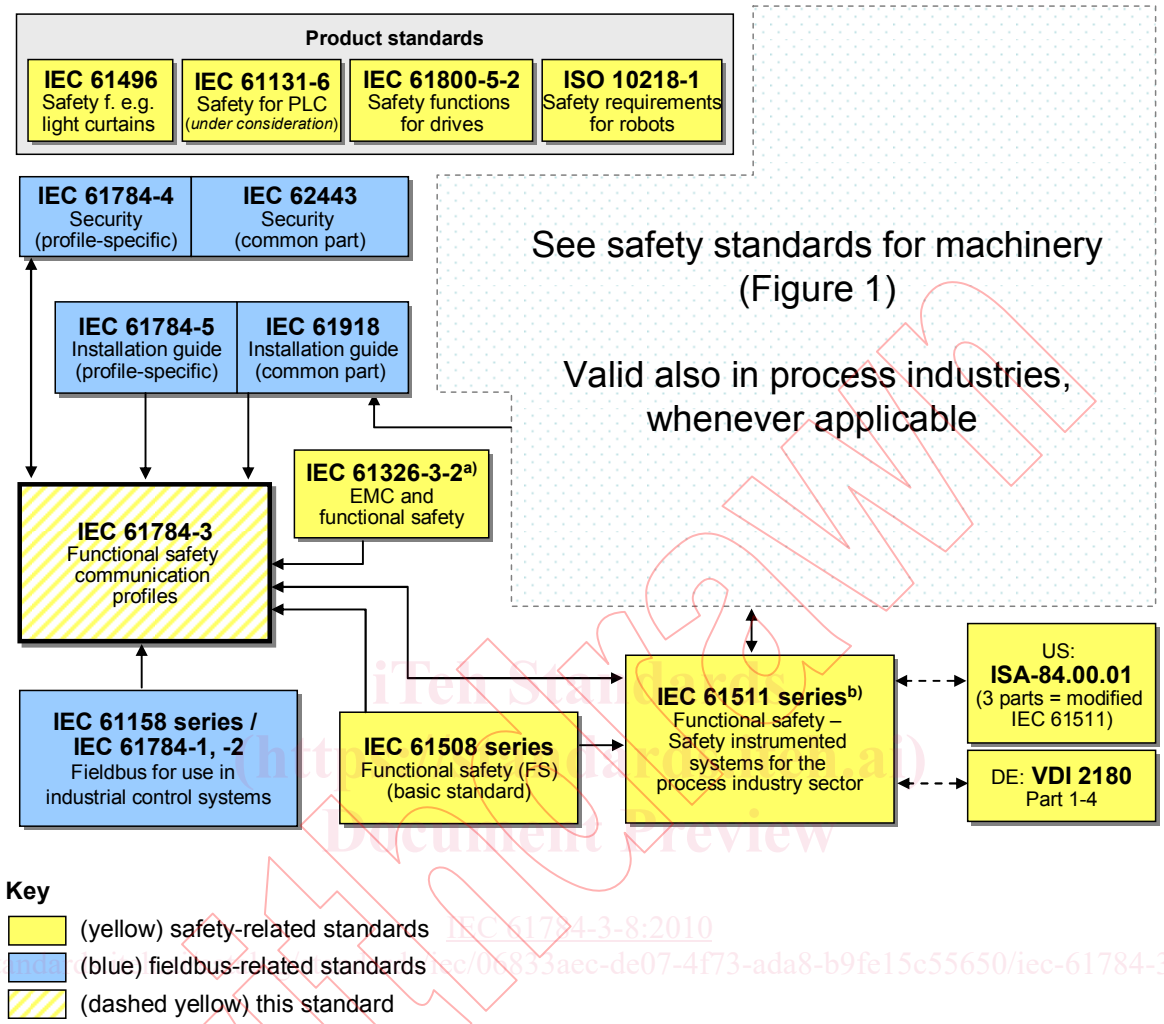
Figure 1 shows the relationships between this standard and relevant safety and fieldbus standards in a machinery environment.



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.

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES –

Part 3-8: Functional safety fieldbuses – Additional specifications for CPF 8

1 Scope

This part of the IEC 61784-3 series specifies a safety communication layer (services and protocol) based on CPF 8 of IEC 61784-1 and IEC 61158 Type 18. It identifies the principles for functional safety communications defined in IEC 61784-3 that are relevant for this safety communication layer.

NOTE 1 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.

This part[1] defines mechanisms for the transmission of safety-relevant messages among participants within a distributed network using fieldbus technology in accordance with the requirements of IEC 61508 series[2] for functional safety. These mechanisms may be used in various industrial applications such as process control, manufacturing automation and machinery.

This part provides guidelines for both developers and assessors of compliant devices and systems.

NOTE 2 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 according to this part in a standard device is not sufficient to qualify it as a safety device.

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 60204-1, *Safety of machinery – Electrical equipment of machines – Part 1: General requirements*

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

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

IEC 61158-2, *Industrial communication networks – Fieldbus specifications – Part 2: Physical layer specification and service definition*

IEC 61158-3-18, *Industrial communication networks – Fieldbus specifications – Part 3-18: Data-link layer service definition – Type 18 elements*

IEC 61158-4-18, *Industrial communication networks – Fieldbus specifications – Part 4-18: Data-link layer protocol specification – Type 18 elements*

---

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

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

IEC 61158-5-18, *Industrial communication networks – Fieldbus specifications – Part 5-18: Application layer service definition – Type 18 elements*

IEC 61158-6-18, *Industrial communication networks – Fieldbus specifications – Part 6-18: Application layer protocol specification – Type 18 elements*

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 61511 (all parts), *Functional safety – Safety instrumented systems for the process industry sector*

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

IEC 61784-3: 2010[3] *Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions*

IEC 62061, *Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control 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
availability
probability for an automated system that for a given period of time there are no unsatisfactory system conditions such as loss of production

3.1.1.2
black channel
communication channel without available evidence of design or validation according to IEC 61508

3.1.1.3
communication channel
logical connection between two end-points within a *communication system*

[3] In preparation.

3.1.1.4
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

3.1.1.5
connection
logical binding between two application objects within the same or different devices

3.1.1.6
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 [32], [33][4].

3.1.1.7
error
discrepancy between a computed, observed or measured value or condition and the true, specified or theoretically correct value or condition

[IEC 61508-4:2010[5]], [IEC 61158]

NOTE 1 Errors may be due to design mistakes within hardware/software and/or corrupted information due to electromagnetic interference and/or other effects.

NOTE 2 Errors do not necessarily result in a *failure* or a *fault*.

3.1.1.8
failure
termination of the ability of a functional unit to perform a required function or operation of a functional unit in any way other than as required

NOTE 1 The definition in IEC 61508-4 is the same, with additional notes.

[IEC 61508-4:2010, modified], [ISO/IEC 2382-14.01.11, modified]

NOTE 2 Failure may be due to an *error* (for example, problem with hardware/software design or message disruption).

3.1.1.9
fault
abnormal condition that may cause a reduction in, or loss of, the capability of a functional unit to perform a required function

NOTE IEV 191-05-01 defines “fault” as a state characterized by the inability to perform a required function, excluding the inability during preventive maintenance or other planned actions, or due to lack of external resources.

[IEC 61508-4:2010, modified], [ISO/IEC 2382-14.01.10, modified]

3.1.1.10
fieldbus
communication system based on serial data transfer and used in industrial automation or process control applications

---

4 Figures in square brackets refer to the bibliography.

5 To be published.