

**Industrial communication networks - Profiles - Part 3-18:
Functional safety fieldbuses - Additional specifications
for CPF 18**

EESTI STANDARDI EESSÕNA

NATIONAL FOREWORD

<p>Käesolev Eesti standard EVS-EN 61784-3-18:2011 sisaldab Euroopa standardi EN 61784-3-18:2011 ingliskeelset teksti.</p> <p>Standard on kinnitatud Eesti Standardikeskuse 29.07.2011 käskkirjaga ja jõustub sellekohase teate avaldamisel EVS Teatajas.</p> <p>Euroopa standardimisorganisatsioonide poolt rahvuslikele liikmetele Euroopa standardi teksti kättesaadavaks tegemise kuupäev on 01.07.2011.</p> <p>Standard on kättesaadav Eesti standardiorganisatsioonist.</p>	<p>This Estonian standard EVS-EN 61784-3-18:2011 consists of the English text of the European standard EN 61784-3-18:2011.</p> <p>This standard is ratified with the order of Estonian Centre for Standardisation dated 29.07.2011 and is endorsed with the notification published in the official bulletin of the Estonian national standardisation organisation.</p> <p>Date of Availability of the European standard text 01.07.2011.</p> <p>The standard is available from Estonian standardisation organisation.</p>
--	---

ICS 13.110, 25.040.40, 35.100.05

Standardite reprodutseerimis- ja levitamiseõigus kuulub Eesti Standardikeskusele

Andmete paljundamine, taastekitamine, kopeerimine, salvestamine elektroonilisse süsteemi või edastamine ükskõik millises vormis või millisel teel on keelatud ilma Eesti Standardikeskuse poolt antud kirjaliku loata.

Kui Teil on küsimusi standardite autorikaitse kohta, palun võtke ühendust Eesti Standardikeskusega:
Aru 10 Tallinn 10317 Eesti; www.evs.ee; Telefon: 605 5050; E-post: info@evs.ee

Right to reproduce and distribute belongs to the Estonian Centre for Standardisation

No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying, without permission in writing from Estonian Centre for Standardisation.

If you have any questions about standards copyright, please contact Estonian Centre for Standardisation:
Aru str 10 Tallinn 10317 Estonia; www.evs.ee; Phone: 605 5050; E-mail: info@evs.ee

**Industrial communication networks -
Profiles -
Part 3-18: Functional safety fieldbuses -
Additional specifications for CPF 18
(IEC 61784-3-18:2011)**

Réseaux de communication industriels -
Profils -
Partie 3-18: Bus de terrain à sécurité
fonctionnelle -
Spécifications supplémentaires pour le
CPF 18
(CEI 61784-3-18:2011)

Industrielle Kommunikationsnetze -
Profile -
Teil 3-18: Funktional sichere Übertragung
bei Feldbussen -
Zusätzliche Festlegungen für die
Kommunikationsprofilfamilie 18
(IEC 61784-3-18:2011)

This European Standard was approved by CENELEC on 2011-05-25. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the Central Secretariat or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the Central Secretariat has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and the United Kingdom.

CENELEC

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

Management Centre: Avenue Marnix 17, B - 1000 Brussels

Foreword

The text of document 65C/639/FDIS, future edition 1 of IEC 61784-3-18, prepared by SC 65C, Industrial networks, of IEC TC 65, Industrial-process measurement, control and automation, was submitted to the IEC-CENELEC parallel vote and was approved by CENELEC as EN 61784-3-18 on 2011-05-25.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN and CENELEC shall not be held responsible for identifying any or all such patent rights.

The following dates were fixed:

- latest date by which the EN has to be implemented
at national level by publication of an identical
national standard or by endorsement (dop) 2012-02-25
- latest date by which the national standards conflicting
with the EN have to be withdrawn (dow) 2014-05-25

Annex ZA has been added by CENELEC.

Endorsement notice

The text of the International Standard IEC 61784-3-18:2011 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following notes have to be added for the standards indicated:

IEC 60204-1	NOTE	Harmonized as EN 60204-1.
IEC 61131-6	NOTE	Harmonized as EN 61131-6 ¹⁾ .
IEC 61158 series	NOTE	Harmonized in EN 61158 series.
IEC 61326-3-1	NOTE	Harmonized as EN 61326-3-1.
IEC 61326-3-2	NOTE	Harmonized as EN 61326-3-2.
IEC 61496 series	NOTE	Harmonized in EN 61496 series.
IEC 61508-1:2010	NOTE	Harmonized as EN 61508-1:2010.
IEC 61508-4:2010	NOTE	Harmonized as EN 61508-4:2010.
IEC 61508-5:2010	NOTE	Harmonized as EN 61508-5:2010.
IEC 61511 series	NOTE	Harmonized in EN 61511 series.
IEC 61784-1	NOTE	Harmonized as EN 61784-1.
IEC 61784-5 series	NOTE	Harmonized in EN 61784-5 series.
IEC 61800-5-2	NOTE	Harmonized as EN 61800-5-2.
IEC 62061	NOTE	Harmonized as EN 62061.
ISO 10218-1	NOTE	Harmonized as EN ISO 10218-1.
ISO 12100-1	NOTE	Harmonized as EN ISO 12100-1.
ISO 13849-1	NOTE	Harmonized as EN ISO 13849-1.

¹⁾ At draft stage.

ISO 13849-2 NOTE Harmonized as EN ISO 13849-2.

ISO 14121 NOTE Harmonized as EN ISO 14121.

This document is a preview generated by EVS

Annex ZA (normative)

Normative references to international publications with their corresponding European publications

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.

NOTE When an international publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
IEC 61158-3-22	-	Industrial communication networks - Fieldbus - specifications - Part 3-22: Data-link layer service definition - Type 22 elements	-	-
IEC 61158-4-22	-	Industrial communication networks - Fieldbus - specifications - Part 4-22: Data-link layer protocol specification - Type 22 elements	-	-
IEC 61158-5-22	-	Industrial communication networks - Fieldbus - specifications - Part 5-22: Application layer service definition - Type 22 elements	-	-
IEC 61158-6-22	-	Industrial communication networks - Fieldbus - specifications - Part 6-22: Application layer protocol specification - Type 22 elements	-	-
IEC 61508	Series	Functional safety of electrical/electronic/programmable electronic safety-related systems	EN 61508	Series
IEC 61508-2	2010	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems	EN 61508-2	2010
IEC 61784-2	2010	Industrial communication networks - Profiles - Part 2: Additional fieldbus profiles for real-time networks based on ISO/IEC 8802-3	EN 61784-2	2010
IEC 61784-3	2010	Industrial communication networks - Profiles - Part 3: Functional safety fieldbuses - General rules and profile definitions	EN 61784-3	2010
IEC 61918	-	Industrial communication networks - Installation of communication networks in industrial premises	EN 61918	-
ISO/IEC 10731	-	Information technology - Open Systems Interconnection - Basic reference model - Conventions for the definition of OSI services	-	-

CONTENTS

FOREWORD.....	5
0 Introduction	7
0.1 General	7
0.2 Patent declaration	9
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 18: Additional terms and definitions	15
3.2 Symbols and abbreviated terms.....	16
3.2.1 Common symbols and abbreviated terms	16
3.2.2 CPF 18: Additional symbols and abbreviated terms	17
3.3 Conventions	17
4 Overview of FSCP 18/1 (SafetyNET p™).....	19
4.1 General	19
4.2 FSCP 18/1	19
5 General	20
5.1 External documents providing specifications for the profile	20
5.2 Safety functional requirements	20
5.3 Safety measures	20
5.4 Safety communication layer structure	21
5.5 Relationships with FAL (and DLL, PhL)	22
5.5.1 General	22
5.5.2 Data Types	22
6 Safety communication layer services	22
6.1 General elements	22
6.1.1 General	22
6.1.2 Safety object dictionary	22
6.1.3 Safety process data object (SPDO)	22
6.1.4 Safety heartbeat (SHB).....	22
6.1.5 Safety delay monitoring (SDM)	23
6.2 Communication relation	23
7 Safety communication layer protocol	24
7.1 Safety PDU format	24
7.1.1 General	24
7.1.2 Safety process data objects (SPDO).....	24
7.1.3 Safety heartbeat (SHB).....	26
7.1.4 Safety PDUs embedded in a Type 22 PDU	28
7.2 Safety communication layer management (SALMT).....	28
7.3 Safety process data communication	30
7.4 Safety heartbeat.....	32
7.5 Delay monitoring	33
8 Safety communication layer management.....	34
8.1 Parameter handling	34
8.2 Safety object dictionary	34

8.2.1	General	34
8.2.2	Communication profile section	35
8.2.3	Standardized device profile section	51
9	System requirements	51
9.1	Indicators and switches	51
9.1.1	Indicator states and flash rates	51
9.1.2	Indicators	51
9.1.3	Switches	52
9.2	Installation guidelines	52
9.3	Safety function response time	52
9.3.1	General	52
9.3.2	Determination of FSCP 18/1 time expectation behavior	53
9.3.3	Calculation of the worst case safety function response time	53
9.4	Duration of demands	53
9.5	Constraints for calculation of system characteristics	53
9.5.1	Safety related constraints	53
9.5.2	Probabilistic considerations	55
9.6	Maintenance	55
9.7	Safety manual	55
10	Assessment	55
Annex A (informative) Additional information for functional safety communication profiles of CPF 18		57
Annex B (informative) Information for assessment of the functional safety communication profiles of CPF 18		58
Bibliography		59
Table 1 – Object definition		18
Table 2 – Safety PDU element definition		18
Table 3 – Communication errors and detection measures		21
Table 4 – SPDO PDU structure		25
Table 5 – SHB request PDU structure		26
Table 6 – SHB response PDU structure		27
Table 7 – SHB safety communication layer state encoding		27
Table 8 – SALMT commands		28
Table 9 – System states of SALMT state machine		29
Table 10 – State transitions SALMT state machine		30
Table 11 – System states of RxSPDO state machine		31
Table 12 – State transitions RxSPDO state machine		31
Table 13 – Timeouts		32
Table 14 – Safety object dictionary structure		34
Table 15 – Objects of communication section		35
Table 16 – Device type		36
Table 17 – Safety ID		37
Table 18 – Safety consumer heartbeat entry		37
Table 19 – Safety consumer heartbeat		38

Table 20 – Safety producer heartbeat parameter	39
Table 21 – Safety bus cycle times	42
Table 22 – SPDO timeout tolerance	43
Table 23 – Receive SPDO communication parameter	43
Table 24 – Transmit SPDO communication parameter	46
Table 25 – Mapping format	49
Table 26 – Receive SPDO mapping parameter	49
Table 27 – Transmit SPDO mapping parameter	50
Table 28 – Indicator states definiton	51
Table 29 – STATUS indicator states	51
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 – FSCP 18/1 system	19
Figure 4 – FSCP 18/1 software architecture	21
Figure 5 – SPDO interaction model	23
Figure 6 – SHB interaction model	23
Figure 7 – Safety process data object structure	24
Figure 8 – Safety heartbeat request structure	26
Figure 9 – Safety heartbeat response structure	26
Figure 10 – Safety PDU for FSCP 18/1 embedded in a Type 22 CDC data section	28
Figure 11 – SALMT state machine	29
Figure 12 – RxSPDO state machine	31
Figure 13 – Heartbeat procedure	32
Figure 14 – Delay measurement principle	33
Figure 15 – Parameter handling	34
Figure 16 – Safety response time components	52
Figure 17 – Considered data fields for message size calculation	54
Figure 18 – Residual error rate	55

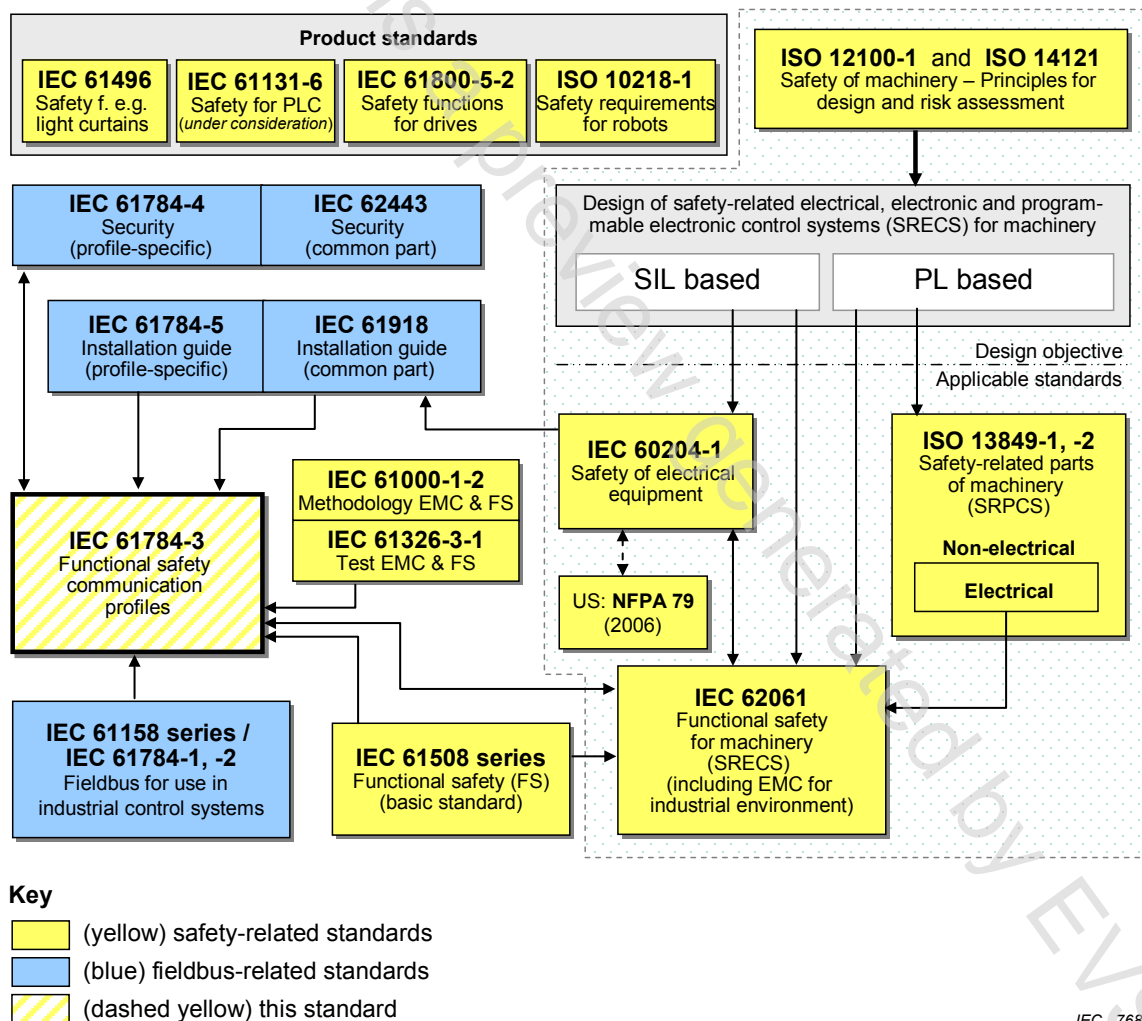
0 Introduction

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.

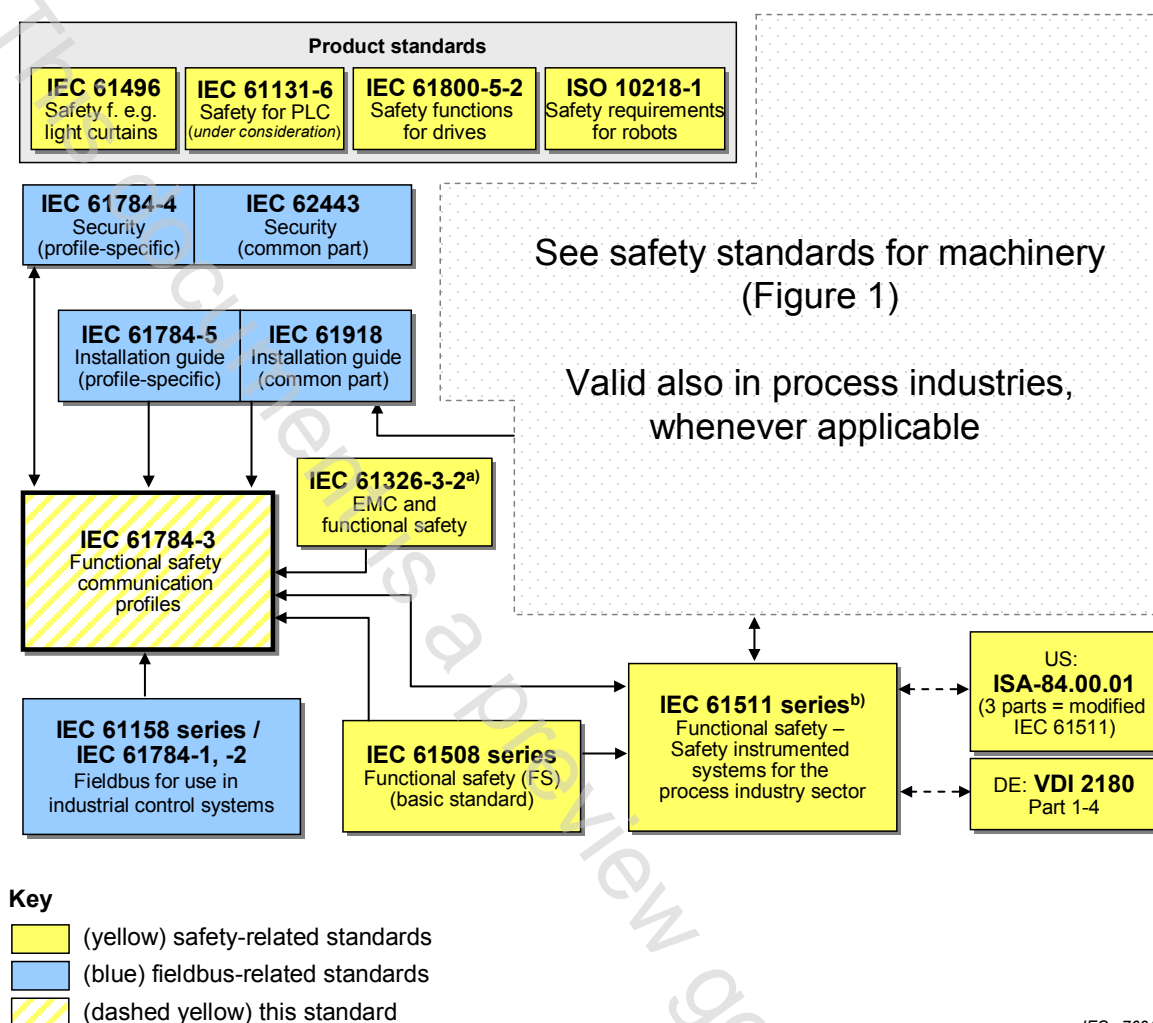
Figure 1 shows the relationships between this standard and relevant safety and fieldbus standards in a machinery environment.



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 a patent concerning the functional safety communication profiles for family 18 as follows, where the [xx] notation indicates the holder of the patent right:

DE 10 2008 007 672.4-31 [PI] Verfahren und Vorrichtung zum Übertragen von Daten in einem Netzwerk

IEC takes no position concerning the evidence, validity and scope of this patent right.

The holder of this patent right has assured the IEC that he/she is 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 statement of the holder of this patent right is registered with IEC. Information may be obtained from:

Information may be obtained from:

[PI] Pilz GmbH & Co. KG
Felix-Wankel-Str. 2
73760 Ostfildern
GERMANY

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

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

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES

Part 3-18: Functional safety fieldbuses – Additional specifications for CPF 18

1 Scope

This part of the IEC 61784-3 series specifies a safety communication layer (services and protocol) based on CPF 18 of IEC 61784-2 and IEC 61158 Type 22. 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 part¹ 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 series² 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 61158-3-22, *Industrial communication networks – Fieldbus specifications – Part 3-22: Data-link layer service definition – Type 22 elements*

IEC 61158-4-22, *Industrial communication networks – Fieldbus specifications – Part 4-22: Data-link layer protocol specification – Type 22 elements*

IEC 61158-5-22, *Industrial communication networks – Fieldbus specifications – Part 5-22: Application layer service definition – Type 22 elements*

IEC 61158-6-22, *Industrial communication networks – Fieldbus specifications – Part 6-22: Application layer protocol specification – Type 22 elements*

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

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 61508-2:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*

IEC 61784-2:2010, *Industrial communication networks – Profiles – Part 2: Additional fieldbus profiles for real-time networks based on ISO/IEC 8802-3*

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

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

ISO/IEC 10731, *Information technology – Open system interconnection – Basic reference model – Conventions for the definition of OSI services*

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*

3.1.1.4

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.