

**Industrial communication networks - Profiles - Part 3-12:
Functional safety fieldbuses - Additional specifications
for CPF 12**

EESTI STANDARDI EESSÕNA

NATIONAL FOREWORD

Käesolev Eesti standard EVS-EN 61784-3-12:2011 sisaldab Euroopa standardi EN 61784-3-12:2010 ingliskeelset teksti.

Standard on kinnitatud Eesti Standardikeskuse 31.01.2011 käskkirjaga ja jõustub sellekohase teate avaldamisel EVS Teatajas.

Euroopa standardimisorganisatsioonide poolt rahvuslikele liikmetele Euroopa standardi teksti kättesaadavaks tegemise kuupäev on 13.08.2010.

Standard on kättesaadav Eesti standardiorganisatsioonist.

This Estonian standard EVS-EN 61784-3-12:2011 consists of the English text of the European standard EN 61784-3-12:2010.

This standard is ratified with the order of Estonian Centre for Standardisation dated 31.01.2011 and is endorsed with the notification published in the official bulletin of the Estonian national standardisation organisation.

Date of Availability of the European standard text 13.08.2010.

The standard is available from Estonian standardisation organisation.

ICS 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 3-12: Functional safety fieldbuses -
Additional specifications for CPF 12
(IEC 61784-3-12:2010)**

Réseaux de communication industriels -
Partie 3-12: Bus de terrain à sécurité
fonctionnelle -
Spécifications complémentaires
pour le CPF 12
(CEI 61784-3-12:2010)

Industrielle Kommunikationsnetze -
Profile -
Teil 3-12: Funktional sichere Übertragung
bei Feldbussen -
Zusätzliche Festlegungen
für die Kommunikationsprofilfamilie 12
(IEC 61784-3-12:2010)

This European Standard was approved by CENELEC on 2010-07-01. 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/591A/FDIS, future edition 1 of IEC 61784-3-12, 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 61784-3-12 on 2010-07-01.

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) 2011-04-01
- latest date by which the national standards conflicting with the EN have to be withdrawn (dow) 2013-07-01

Annex ZA has been added by CENELEC.

Endorsement notice

The text of the International Standard IEC 61784-3-12:2010 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 61158 series	NOTE	Harmonized in EN 61158 series (not modified).
IEC 61496 series	NOTE	Harmonized in EN 61496 series (partially modified).
IEC 61508-1:2010	NOTE	Harmonized as EN 61508-1:2010 (not modified).
IEC 61508-4:2010	NOTE	Harmonized as EN 61508-4:2010 (not modified).
IEC 61508-5:2010	NOTE	Harmonized as EN 61508-5:2010 (not modified).
IEC 61511 series	NOTE	Harmonized in EN 61511 series (not modified).
IEC 61784-1	NOTE	Harmonized as EN 61784-1.
IEC 61784-5 series	NOTE	Harmonized in EN 61784-5 series (not modified).
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.
ISO 13849-2	NOTE	Harmonized as EN ISO 13849-2.

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 60204-1	-	Safety of machinery - Electrical equipment of machines - Part 1: General requirements	EN 60204-1	-
IEC 61000-6-2	-	Electromagnetic compatibility (EMC) - Part 6-2: Generic standards - Immunity for industrial environments	EN 61000-6-2	-
IEC 61131-2	-	Programmable controllers - Part 2: Equipment requirements and tests	EN 61131-2	-
IEC 61158-2	-	Industrial communication networks - Fieldbus specifications - Part 2: Physical layer specification and service definition	EN 61158-2	-
IEC 61158-3-12	-	Industrial communication networks - Fieldbus specifications - Part 3-12: Data-link layer service definition - Type 12 elements	EN 61158-3-12	-
IEC 61158-4-12	-	Industrial communication networks - Fieldbus specifications - Part 4-12: Data-link layer protocol specification - Type 12 elements	EN 61158-4-12	-
IEC 61158-5-12	-	Industrial communication networks - Fieldbus specifications - Part 5-12: Application layer service definition - Type 12 elements	EN 61158-5-12	-
IEC 61158-6-12	-	Industrial communication networks - Fieldbus specifications - Part 6-12: Application layer protocol specification - Type 12 elements	EN 61158-6-12	-
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	EN 61326-3-1	-

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
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	EN 61326-3-2	-
IEC 61508	Series	Functional safety of electrical/electronic/programmable electronic safety-related systems	EN 61508	Series
IEC 61784-2		Industrial communication networks - Profiles - Part 2: Additional fieldbus profiles for real-time networks based on ISO/IEC 8802-3	EN 61784-2	-
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	-

This document is a preview generated by EVS

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	12
3.1 Terms and definitions	12
3.1.1 Common terms and definitions	12
3.1.2 CPE 12: Additional terms and definitions	17
3.2 Symbols and abbreviated terms.....	17
3.2.1 Common symbols and abbreviated terms	17
3.2.2 CPF 12: Additional symbols and abbreviated terms	18
3.3 Conventions	18
4 Overview of FSCP 12/1 (Safety-over-EtherCAT™)	18
5 General	20
5.1 External document providing specifications for the profile.....	20
5.2 Safety functional requirements	20
5.3 Safety measures	21
5.4 Safety communication layer structure	21
5.5 Relationships with FAL (and DLL, Pn)	22
5.5.1 General	22
5.5.2 Data types	22
6 Safety communication layer services	22
6.1 FSoE Connection	22
6.2 FSoE Cycle	22
6.3 FSoE services	23
7 Safety communication layer protocol	24
7.1 Safety PDU format	24
7.1.1 Safety PDU structure	24
7.1.2 Safety PDU command.....	25
7.1.3 Safety PDU CRC	25
7.2 FSCP 12/1 communication procedure.....	29
7.2.1 Message cycle.....	29
7.2.2 FSCP 12/1 node states.....	29
7.3 Reaction on communication errors	39
7.4 State table for FSoE Master	40
7.4.1 FSoE Master state machine.....	40
7.4.2 Reset state	44
7.4.3 Session state.....	45
7.4.4 Connection state	48
7.4.5 Parameter state.....	52
7.4.6 Data state.....	55
7.5 State table for FSoE Slave	58
7.5.1 FSoE Slave state machine.....	58
7.5.2 Reset state	62

7.5.3	Session state.....	64
7.5.4	Connection state	68
7.5.5	Parameter state.....	73
7.5.6	Data state.....	78
8	Safety communication layer management.....	81
8.1	FSCP 12/1 parameter handling.....	81
8.2	FSoE communication parameters	81
9	System requirements.....	82
9.1	Indicators and switches	82
9.1.1	Indicator states and flash rates.....	82
9.1.2	Indicators	83
9.2	Installation guidelines.....	84
9.3	Safety function response time	84
9.3.1	General	84
9.3.2	Determination of FSoE Watchdog time	85
9.3.3	Calculation of the worst case safety function response time	86
9.4	Duration of demands.....	87
9.5	Constraints for calculation of system characteristics.....	87
9.5.1	General	87
9.5.2	Probabilistic considerations	87
9.6	Maintenance.....	89
9.7	Safety manual	89
10	Assessment.....	89
	Annex A (informative) Additional information for functional safety communication profiles of CPF 12.....	90
A.1	Hash function calculation.....	90
A.2		94
	Annex B (informative) Information for assessment of the functional safety communication profiles of CPF 12.....	95
	Bibliography.....	96
	Table 1 – State machine description elements	18
	Table 2 – Communication errors and detection measures	21
	Table 3 – General Safety PDU	24
	Table 4 – Shortest Safety PDU	25
	Table 5 – Safety PDU command	25
	Table 6 – CRC_0 calculation sequence.....	26
	Table 7 – CRC_i calculation sequence (i>0)	26
	Table 8 – Example for CRC_0 inheritance	27
	Table 9 – Example for 4 octets of safety data with interchanging of octets 1-4 with 5-8.....	28
	Table 10 – Safety Master PDU for 4 octets of safety data with command = Reset after restart (reset connection) or error	31
	Table 11 – Safety Slave PDU for 4 octets of safety data with command = Reset for acknowledging a Reset command from the FSoE Master	31
	Table 12 – Safety Slave PDU for 4 octets of safety data with command = Reset after restart (reset connection) or error	32

Table 13 – Safety Master PDU for 4 octets of safety data with command = Session.....	32
Table 14 – Safety Slave PDU for 4 octets of safety data with command = Session.....	33
Table 15 – Safety data transferred in the connection state.....	33
Table 16 – Safety Master PDU for 4 octets of safety data in Connection state	34
Table 17 – Safety Slave PDU for 4 octets of safety data in Connection state	34
Table 18 – Safety data transferred in the parameter state.....	35
Table 19 – First Safety Master PDU for 4 octets of safety data in parameter state	35
Table 20 – First Safety Slave PDU for 4 octets of safety data in parameter state	36
Table 21 – Second Safety Master PDU for 4 octets of safety data in parameter state	36
Table 22 – Second Safety Slave PDU for 4 octets of safety data in parameter state	37
Table 23 – Safety Master PDU for 4 octets of ProcessData in data state	37
Table 24 – Safety Slave PDU for 4 octets of ProcessData in data state	38
Table 25 – Safety Master PDU for 4 octets of fail-safe data in data state	38
Table 26 – Safety Slave PDU for 4 octets of fail-safe data in data state	39
Table 27 – FSoE communication error	39
Table 28 – FSoE communication error codes	40
Table 29 – States of the FSoE Master	40
Table 30 – Events in the FSoE Master state table	42
Table 31 – Functions in the FSoE Master state table	42
Table 32 – Variables in the FSoE Master state table	43
Table 33 – Macros in the FSoE Master state table	43
Table 34 – States of the FSoE Slave	58
Table 35 – Events in the FSoE Slave state table	60
Table 36 – Functions in the FSoE Slave state table	60
Table 37 – Variables in the FSoE Slave state table	61
Table 38 – Macros in the FSoE Slave state table	61
Table 39 – FSoE Communication parameters	82
Table 40 – Indicator States	82
Table 41 – FSoE STATUS indicator states	83
Table 42 – Definition of times	85
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 – Basic FSCP 12/1 system	19
Figure 4 – FSCP 12/1 software architecture	21
Figure 5 – FSoE Cycle	23
Figure 6 – FSCP 12/1 communication structure	23
Figure 7 – Safety PDU for CPF 12 embedded in Type 12 PDU.....	24
Figure 8 – FSCP 12/1 node states	30
Figure 9 – State diagram for FSoE Master	41
Figure 10 – State diagram for FSoE Slave	59
Figure 11 – Indicator flash rates	83

Figure 12 – Components of a safety function	84
Figure 13 – Calculation of the FSoE Watchdog times for input and output connections	85
Figure 14 – Calculation of the worst case safety function response time	86
Figure 15 – Safety PDU embedded in standard PDU	88
Figure 16 – Residual error rate for 8/16/24 bit safety data and up to 12 144 bit standard data.....	89

This document is a preview generated by EVS

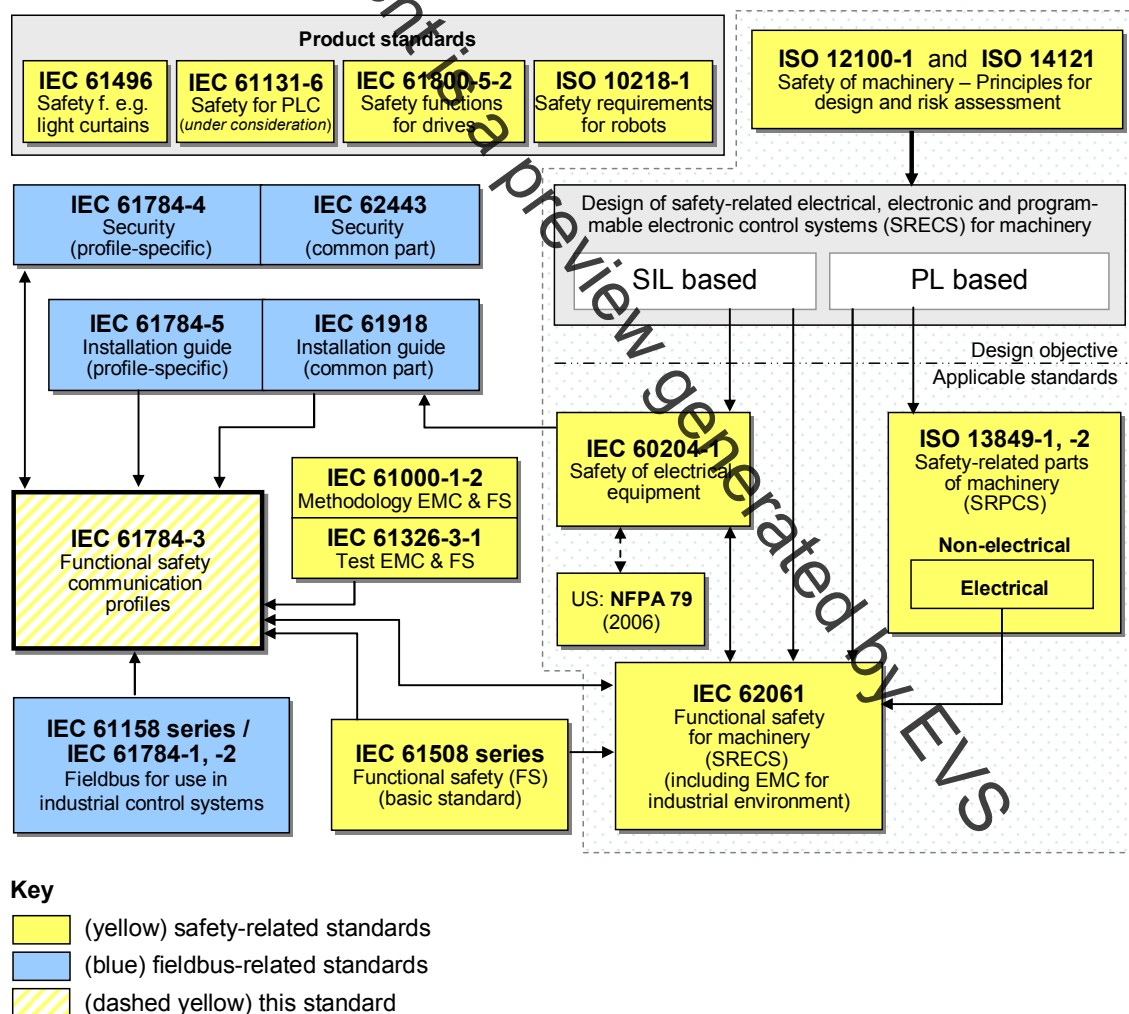
0 Introduction

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.

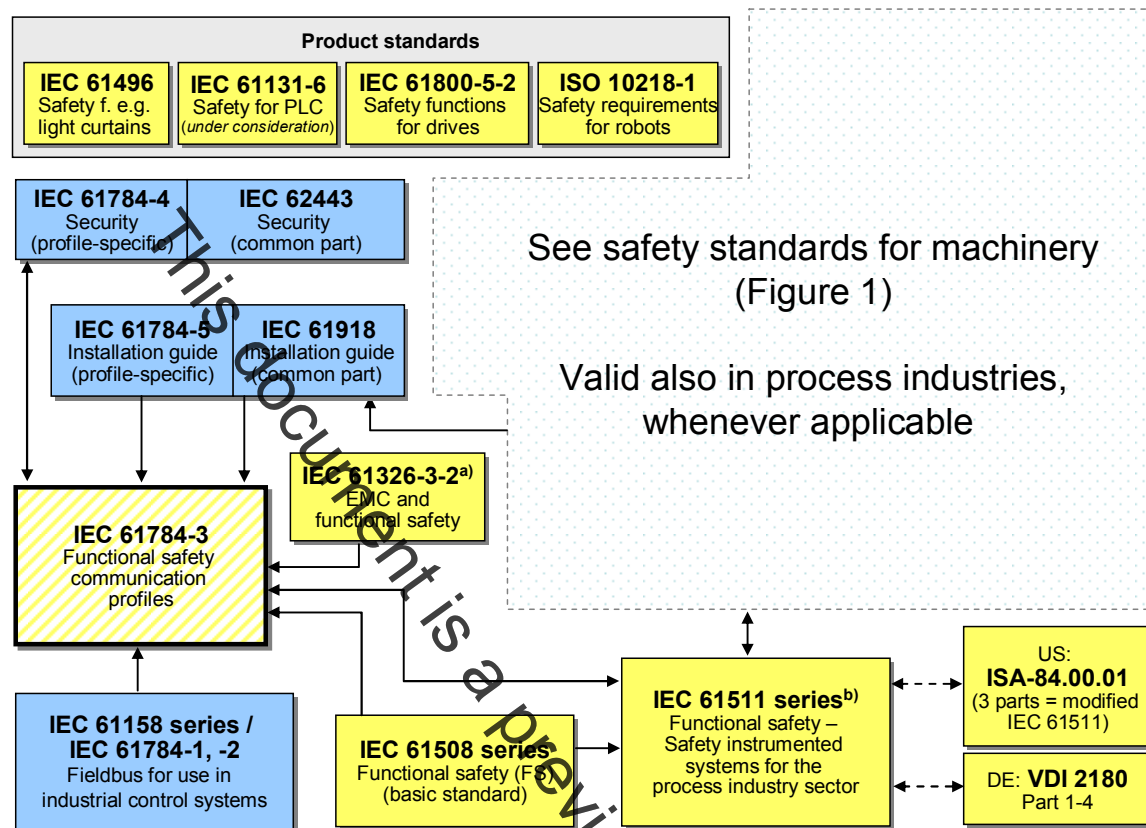
Figure 1 shows the relationships between this standard and relevant safety and fieldbus standards in a machinery environment.



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.



Key

- (yellow) safety-related standards
- (blue) fieldbus-related standards
- (dashed yellow) this standard

^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 the functional safety communication profiles for family 12 as follows, where the [xx] notation indicates the holder of the patent right:

DE 10 2004 044 764.0 [BE] Datenübertragungsverfahren und Automatisierungssystem zum Einsatz eines solchen Datenübertragungsverfahrens

EP 05 733 921.0 [BE] Sicherheitssteuerung

IEC takes no position concerning the evidence, validity and scope of these patent rights.

The holders of these patents 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 statement of the holders of these patent rights are registered with IEC.

Information may be obtained from:

[BE] Beckhoff Automation GmbH
Eiserstrasse 5, 33415 Verl
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.

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES –

Part 3-12: Functional safety fieldbuses – Additional specifications for CPF 12

1 Scope

This part of the IEC 61784-3 series specifies a safety communication layer (services and protocol) based on CPF 12 of IEC 61784-2 and IEC 61158 Type 12. 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 60204-1, *Safety of machinery – Electrical equipment of machines – Part 1: General requirements*

IEC 61000-6-2, *Electromagnetic compatibility (EMC) – Part 6-2: Generic standards – Immunity for industrial environments*

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

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

IEC 61158-3-12, *Industrial communication networks – Fieldbus specifications – Part 3-12: Data-link layer service definition – Type 12 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 61158-4-12, *Industrial communication networks – Fieldbus specifications – Part 4-12: Data-link layer protocol specification – Type 12 elements*

IEC 61158-5-12, *Industrial communication networks – Fieldbus specifications – Part 5-12: Application layer service definition – Type 12 elements*

IEC 61158-6-12, *Industrial communication networks – Fieldbus specifications – Part 6-12: Application layer protocol specification – Type 12 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 61784-2, *Industrial communication networks – Profiles – Part 2: Additional fieldbus profiles for real-time networks based on ISO/IEC 8802-3*

IEC 61784-3:2010³, *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*

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.