

FINAL VERSION



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

CONTENTS

FOREWORD	6
0 Introduction	8
0.1 General	8
0.2 Patent declaration	10
INTRODUCTION to Amendment 1	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 CPF 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, PhL)	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
	Annex B (informative) Information for assessment of the functional safety communication profiles of CPF 12.....	95
	Bibliography.....	96
	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
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 or 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	34
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

Currently in preview, click buy full version

INTERNATIONAL ELECTROTECHNICAL COMMISSION

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES –

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

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.
- 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.

DISCLAIMER

This Consolidated version is not an official IEC Standard and has been prepared for user convenience. Only the current versions of the standard and its amendment(s) shall be considered the official documents.

This Consolidated version of IEC 61784-3-12 bears the edition number 1.1. It consists of the first edition (2010-06) [documents 65C/591A/FDIS and 65C/603/RVD] and its amendment 1 (2019-11) [documents 65C/960/CDV and 65C/980/RVC]. The technical content is identical to the base edition and its amendment.

This Final version does not show where the technical content is modified by amendment 1. A separate Redline version with all changes highlighted is available in this publication.

International Standard IEC 61784-3-12 has been prepared by subcommittee 65C: Industrial networks, of IEC technical committee 65: Industrial process measurement, control and automation.

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 the base publication and its amendment 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.

A bilingual version of this publication may be issued at a later date.

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.

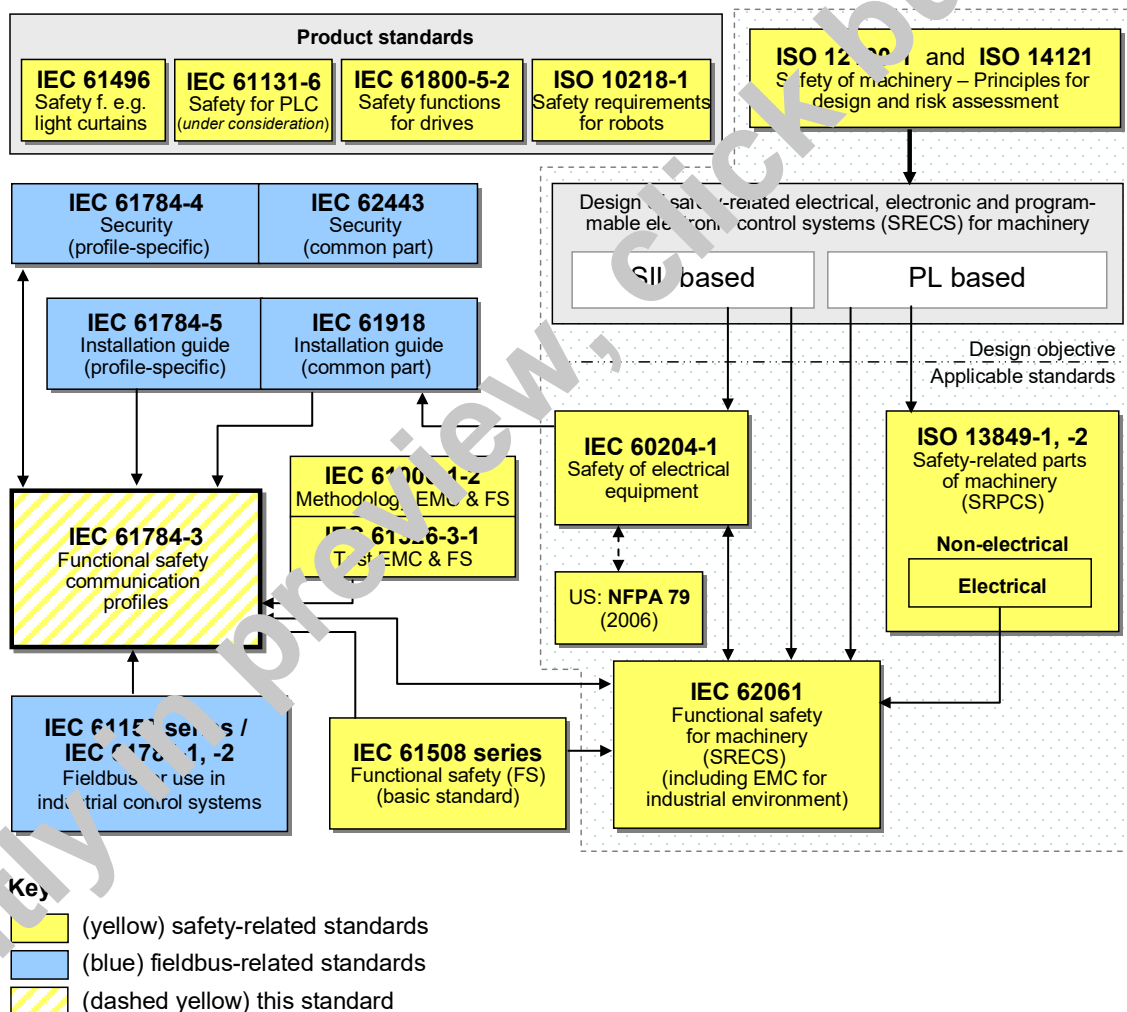
0 Introduction

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.

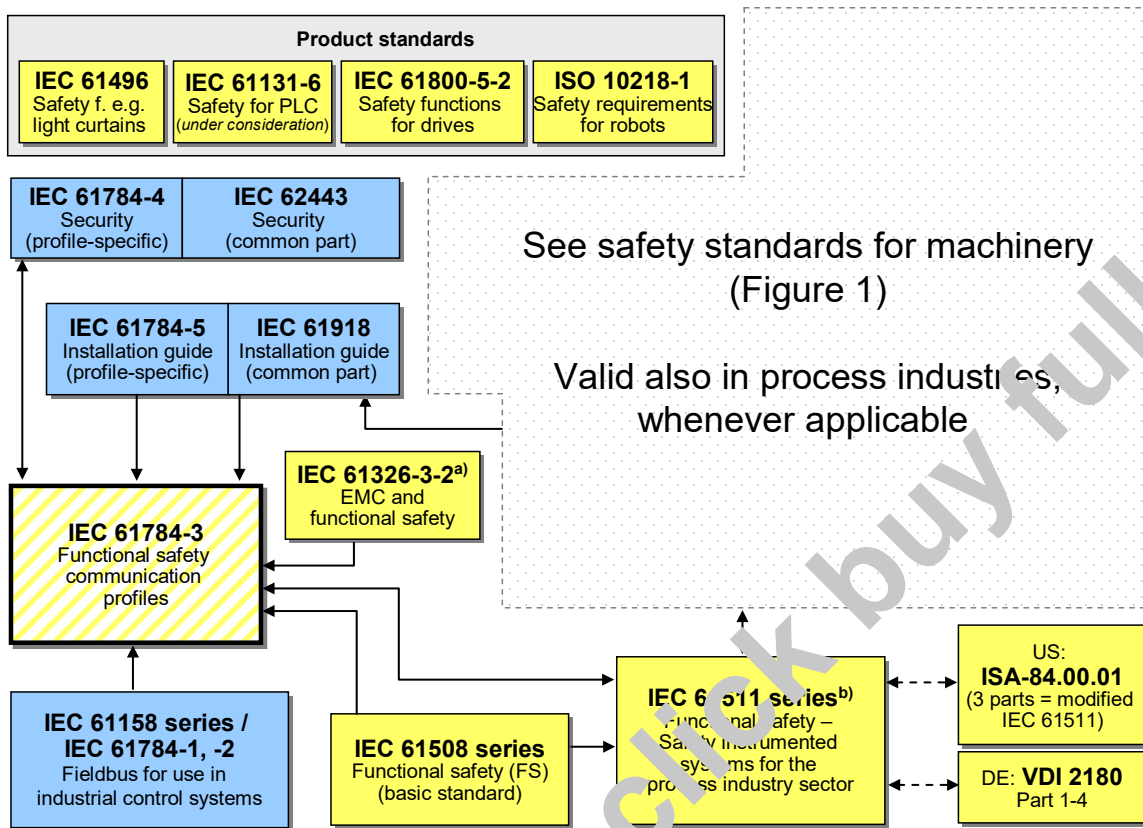
Figure 1 shows the relationships between this standard and relevant safety and fieldbus standards in a machinery environment.



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.



- 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 statements 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.

INTRODUCTION to Amendment 1

This Amendment 1 corrects technical errors in state tables for the FSoE Slave.

Correct invalid value for the “bNew” parameter of SendFrame in transitions RESET_OK (Reset state), SESSION_STAY2 (Session state), CONN_RESET2 (Connection state), PARA_RESET2 (Parameter state), and DATA_RESET2 (Data state). This parameter shall only be set to “FALSE” in all back-to-reset-transitions when all values are set to their defaults.

- Add missing action in Transition SESSION_FAIL5 (Session state).
- Correct invalid value for the address parameter of STORE_DATA in transition CONN_STAY1 (Connection state).

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”.