

This is a preview - click here to buy the full publication



IEC 61784-3-14

Edition 1.0 2010-06

INTERNATIONAL STANDARD



**Industrial communication networks – Profiles –
Part 3-14: Functional safety fieldbuses – Additional specifications for CPF 14**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

PRICE CODE **XB**

ICS 25.040.40; 35.100.05

ISBN 978-2-88910-983-8

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 CPF 14: 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 14: Additional symbols and abbreviated terms	17
3.3 Conventions	17
4 Overview of FSCP 14/1 (EPASafety®).....	18
4.1 EPASafety®	18
4.2 Principle of EPA safety communications.....	18
4.3 Safety function processing	19
5 General	19
5.1 External documents providing specifications for the profile.....	19
5.2 Safety functional requirements	20
5.3 Safety measures	20
5.4 Safety communication layer structure	21
5.4.1 Combination of standard communication and safety communication systems.....	21
5.4.2 CP 14/1 safety communication structure.....	22
5.5 Relationships with FAL (and DLL, PhL)	23
5.5.1 Overview	23
5.5.2 Data types.....	23
6 Safety communication layer services	24
6.1 Overview	24
6.2 FSCP 14/1 object extensions.....	24
6.2.1 General	24
6.2.2 Functional safety communication management object.....	25
6.2.3 Functional Safety Link Object	26
6.2.4 Functional safety communication alert object.....	29
6.3 Extended services	30
6.3.1 General	30
6.3.2 SafetyCommunicationOpen	31
6.3.3 SafetyCommunicationClose	32
7 Safety communication layer protocol	34
7.1 Safety PDU format	34
7.1.1 General	34
7.1.2 APDU header structure.....	34
7.1.3 Functional safety PDU.....	34
7.2 Safety communication operation.....	36

7.2.1	Sequence number	36
7.2.2	RelationKey	36
7.2.3	Feedback message	37
7.2.4	CRC-cross-check	37
7.2.5	Scheduling number	38
7.2.6	Time stamp	39
7.2.7	Time expectation	39
7.2.8	Time synchronization monitoring	39
7.2.9	Communication scheduling precision monitoring	39
7.3	Safety communication behaviour	39
7.3.1	Protocol state description of periodic data transmission	39
7.3.2	Protocol state description of non-periodic data transmission	41
7.3.3	Protocol state description of alert report for communication fault	46
7.3.4	Function description	49
7.4	Code	51
7.4.1	Object code	51
7.4.2	Service code	53
8	Safety communication layer management	59
8.1	Time synchronization diagnostics	59
8.1.1	Time synchronization process	59
8.1.2	Time synchronization management	60
8.2	CSME diagnostics	60
8.2.1	General	60
8.2.2	CSME diagnostics management	60
8.3	Communication fault management	61
8.3.1	Configuration management	61
8.3.2	Communication fault report process	61
9	System requirements	64
9.1	Indicators and switches	64
9.2	Installation guidelines	64
9.3	Safety function response time	64
9.3.1	General	64
9.3.2	Calculation of the network reaction time	65
9.4	Duration of demands	66
9.5	Constraints for calculation of system characteristics	66
9.6	Maintenance	67
9.7	Safety manual	67
10	Assessment	67
Annex A (informative) Additional information for functional safety communication profiles of CPF 14		68
A.1 Hash function calculation		68
A.2		69
Annex B (informative) Information for assessment of the functional safety communication profiles of CPF 14		70
Bibliography		71
Table 1 – Relationships between errors and safety measures		21
Table 2 – Data types used within FSCP 14/1		24

Table 3 – FSCP 14/1 object extensions	24
Table 4 – Functional safety service extension	31
Table 5 – SafetyCommunicationOpen Service Parameters	31
Table 6 – SafetyCommunicationClose Service Parameters	33
Table 7 – Encoding of APDU Header	34
Table 8 – Structure of Functional Safety PDU (FSPDU) Header	35
Table 9 – CRC calculation polynomials	37
Table 10 – Functional safety communication state description	40
Table 11 – States and transitions of periodic data transmission	40
Table 12 – Functional safety communication states description	42
Table 13 – States and transitions of non-periodic data transmission	42
Table 14 – Communication alert state description	47
Table 15 – Communication alert states and transitions	47
Table 16 – LinkObjectType function description	49
Table 17 – CRCCheck function description	49
Table 18 – CrossCheck function description	50
Table 19 – TimeDelayCheck function description	50
Table 20 – PeriodUncomfrimedSNCheck function description	50
Table 21 – Non-periodicSNCheck function description	50
Table 22 – Functional safety communication management object encoding	51
Table 23 – Functional safety link object encoding	51
Table 24 – Functional safety communication alert object encoding	53
Table 25 – Encoding of SafetyCommunicationOpen request parameters	56
Table 26 – SafetyCommunicationOpen positive response parameters	56
Table 27 – SafetyCommunicationOpen negative response parameters	57
Table 28 – SafeCommunicationClose request parameters	57
Table 29 – SafeCommunicationClose positive response parameters	57
Table 30 – SafeCommunicationClose negative response parameters	57
Table 31 – Error class and code	58
Table 32 – Communication process of confirmed service between two devices	61
Table 33 – Settings for time expectation margin	65
Table 34 – Constraints for system characteristics at $\epsilon = 10^{-2}$	67
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 – Safety communication architecture	19
Figure 4 – Safety function processing	19
Figure 5 – Standard communication and safety communication	22
Figure 6 – CP 14/1 protocol hierarchy	23
Figure 7 – Relationship between the SCL and the other layers of CP 14/1	23
Figure 8 – Functional safety communication message structure	34
Figure 9 – Structure of Functional Safety PDU (FSPDU)	35
Figure 10 – Structure of Virtual Safety Check Message (VSCM)	35

Figure 11 – FSPDU mapping	36
Figure 12 – Time-sharing communication scheduling	38
Figure 13 – Format of EndofNonPeriodicDataSending PDU	39
Figure 14 – State transfer figure of periodic data transmission	40
Figure 15 – Functional safety communication state transfer	41
Figure 16 – Communication alert report state transfer figure	46
Figure 17 – CRC check for time synchronization process	59
Figure 18 – The process of communication fault report	63
Figure 19 – Example application for FSCP 14/1 communication	64
Figure 20 – Calculation of the network reaction time	65

INTERNATIONAL ELECTROTECHNICAL COMMISSION

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES –

Part 3-14: Functional safety fieldbuses – Additional specifications for CPF 14

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 61784-3-14 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.

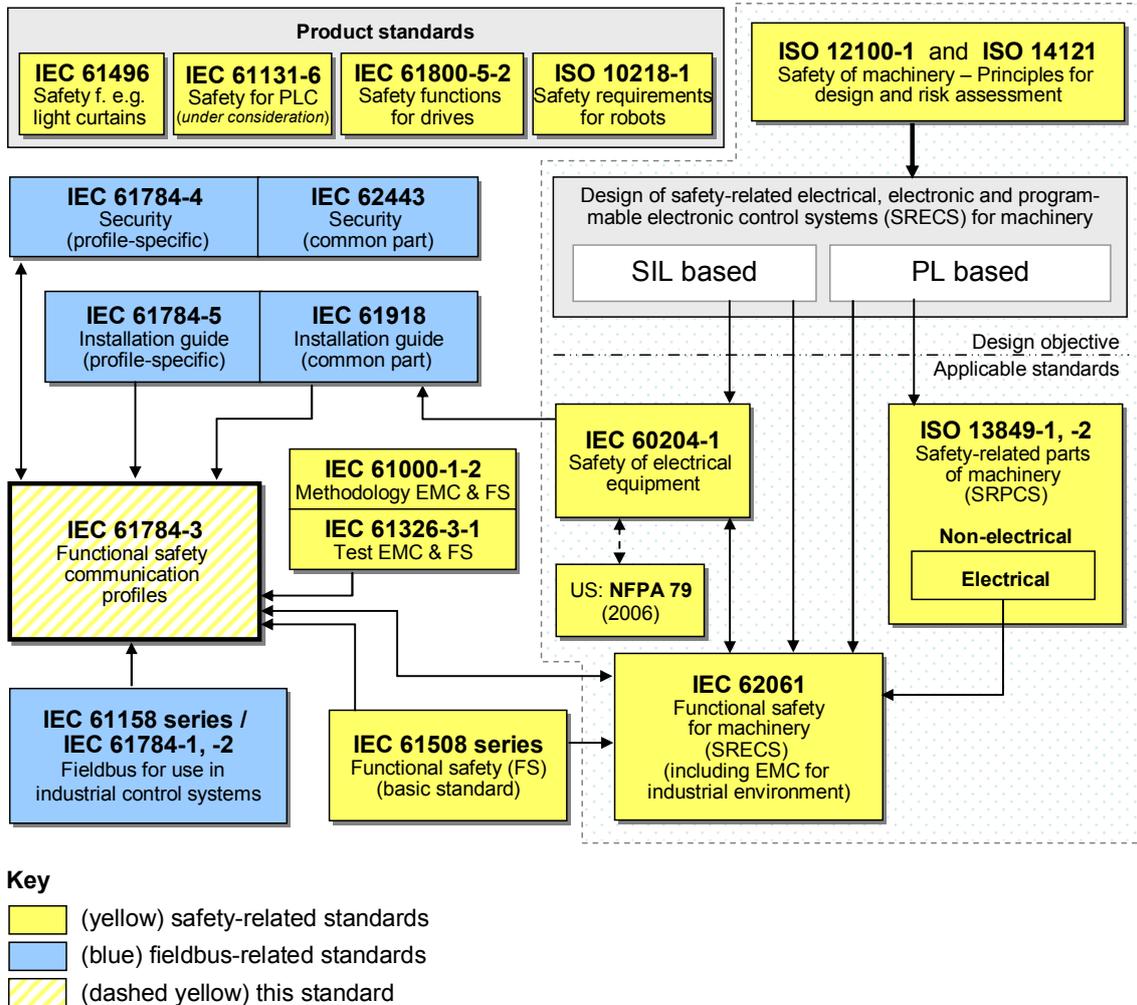
0 Introduction

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.

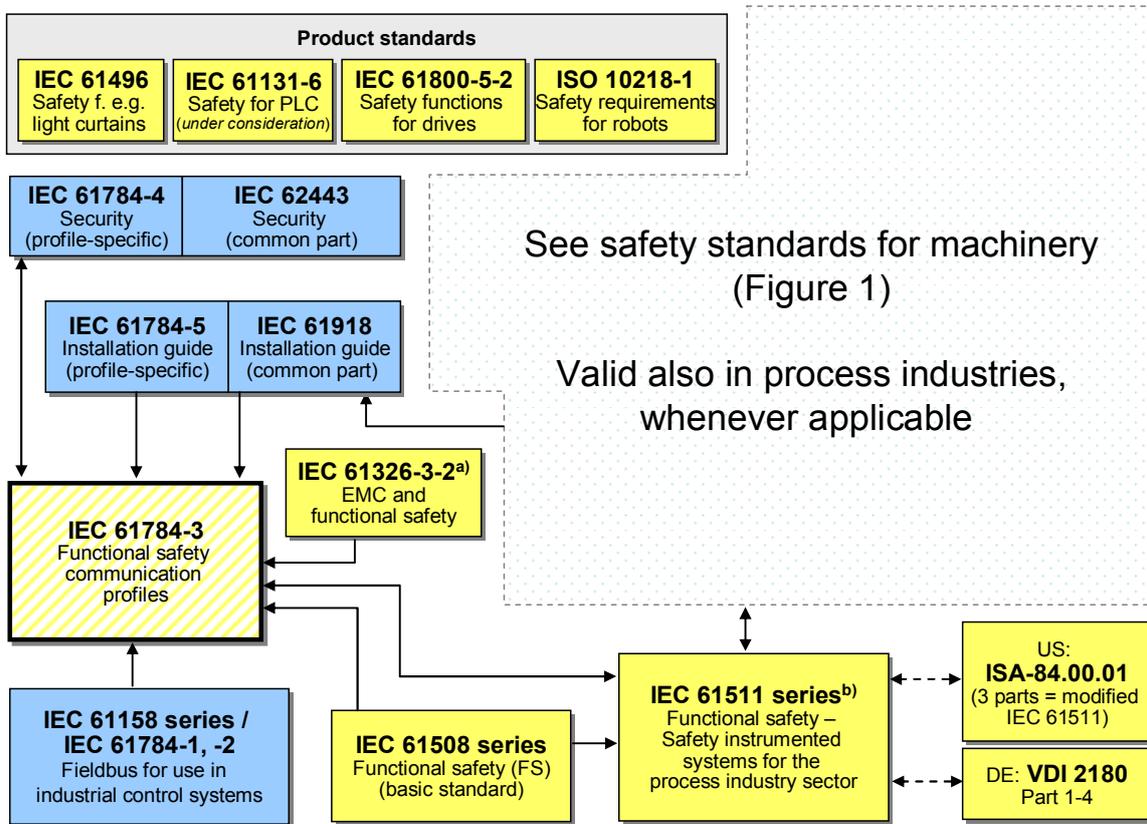
Figure 1 shows the relationships between this standard and relevant safety and fieldbus standards in a machinery environment.



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 14 as follows, where the [xx] notation indicates the holder of the patent right:

CN1960247	[SxZ]	Method of Safety communication for industrial network
CN1929373	[SxZ]	The safety communication for the safety instrument system applied in industrial process.
CN101035030	[SxZ]	The diagnosis method and the equipment for monitoring the industrial Ethernet message.

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:

[SxZ] SUPCON and Zhejiang university
Dongqin FENG

(1) Zhejiang SUPCON Technology Co., Ltd.
Liuhe Road 309, Bingjiang District,
Hangzhou, CHINA 310053

(2) Zhejiang University
Zheda Road 38,
Hangzhou CHINA 310027

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 3-14: Functional safety fieldbuses – Additional specifications for CPF 14

1 Scope

This part of the IEC 61784-3 series specifies a safety communication layer (services and protocol) based on CPF 14 of IEC 61784-2 and IEC 61158 Type 14. 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 (all parts), *Industrial communication networks – Fieldbus specifications*

IEC 61158-3-14, *Industrial communication networks – Fieldbus specifications – Part 3-14: Data-link layer service definition – Type 14 elements*

IEC 61158-4-14, *Industrial communication networks – Fieldbus specifications – Part 4-14: Data-link layer protocol specification – Type 14 elements*

IEC 61158-5-14, *Industrial communication networks – Fieldbus specifications – Part 5-14: Application layer service definition – Type 14 elements*

IEC 61158-6-14, *Industrial communication networks – Fieldbus specifications – Part 6-14: Application layer protocol specification – Type 14 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 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 61588, *Precision clock synchronization protocol for networked measurement and control 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*

ISO/IEC 8802-3, *Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications*

³ In preparation.