

INTERNATIONAL STANDARD

NORME INTERNATIONALE



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

**Réseaux de communication industriels – Profils –
Partie 3-14: Bus de terrain de sécurité fonctionnelle – Spécifications
supplémentaires pour CPF 14**



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2010 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester.

If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de la CEI ou du Comité national de la CEI du pays du demandeur.

Si vous avez des questions sur le copyright de la CEI ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de la CEI de votre pays de résidence.

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
info@iec.ch
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.

Useful links:

IEC publications search - www.iec.ch/searchpub

The advanced search enables you to find IEC publications by a variety of criteria (reference number, text, technical committee,...).

It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

Stay up to date on all new IEC publications. Just Published details all new publications released. Available on-line and also once a month by email.

Electropedia - www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 30 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary (IEV) on-line.

Customer Service Centre - webstore.iec.ch/csc

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: csc@iec.ch.

A propos de la CEI

La Commission Electrotechnique Internationale (CEI) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications CEI

Le contenu technique des publications de la CEI est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Liens utiles:

Recherche de publications CEI - www.iec.ch/searchpub

La recherche avancée vous permet de trouver des publications CEI en utilisant différents critères (numéro de référence, texte, comité d'études,...).

Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

Just Published CEI - webstore.iec.ch/justpublished

Restez informé sur les nouvelles publications de la CEI. Just Published détaille les nouvelles publications parues. Disponible en ligne et aussi une fois par mois par email.

Electropedia - www.electropedia.org

Le premier dictionnaire en ligne au monde de termes électroniques et électriques. Il contient plus de 30 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans les langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (VEI) en ligne.

Service Clients - webstore.iec.ch/csc

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: csc@iec.ch.



IEC 61784-3-14

Edition 1.0 2010-06

INTERNATIONAL STANDARD

NORME INTERNATIONALE



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

**Réseaux de communication industriels – Profils –
Partie 3-14: Bus de terrain de sécurité fonctionnelle – Spécifications
supplémentaires pour CPF 14**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

PRICE CODE
CODE PRIX

XB

ICS 25.040.40, 35.100.05

ISBN 978-2-88912-946-1

**Warning! Make sure that you obtained this publication from an authorized distributor.
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.**

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.....	

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	37
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	21
--	----

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 $\varepsilon = 10^{-2}$	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	38
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.

This bilingual version (2012-02) corresponds to the monolingual English version, published in 2010-06.

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.

The French version of this standard has not been voted upon.

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.

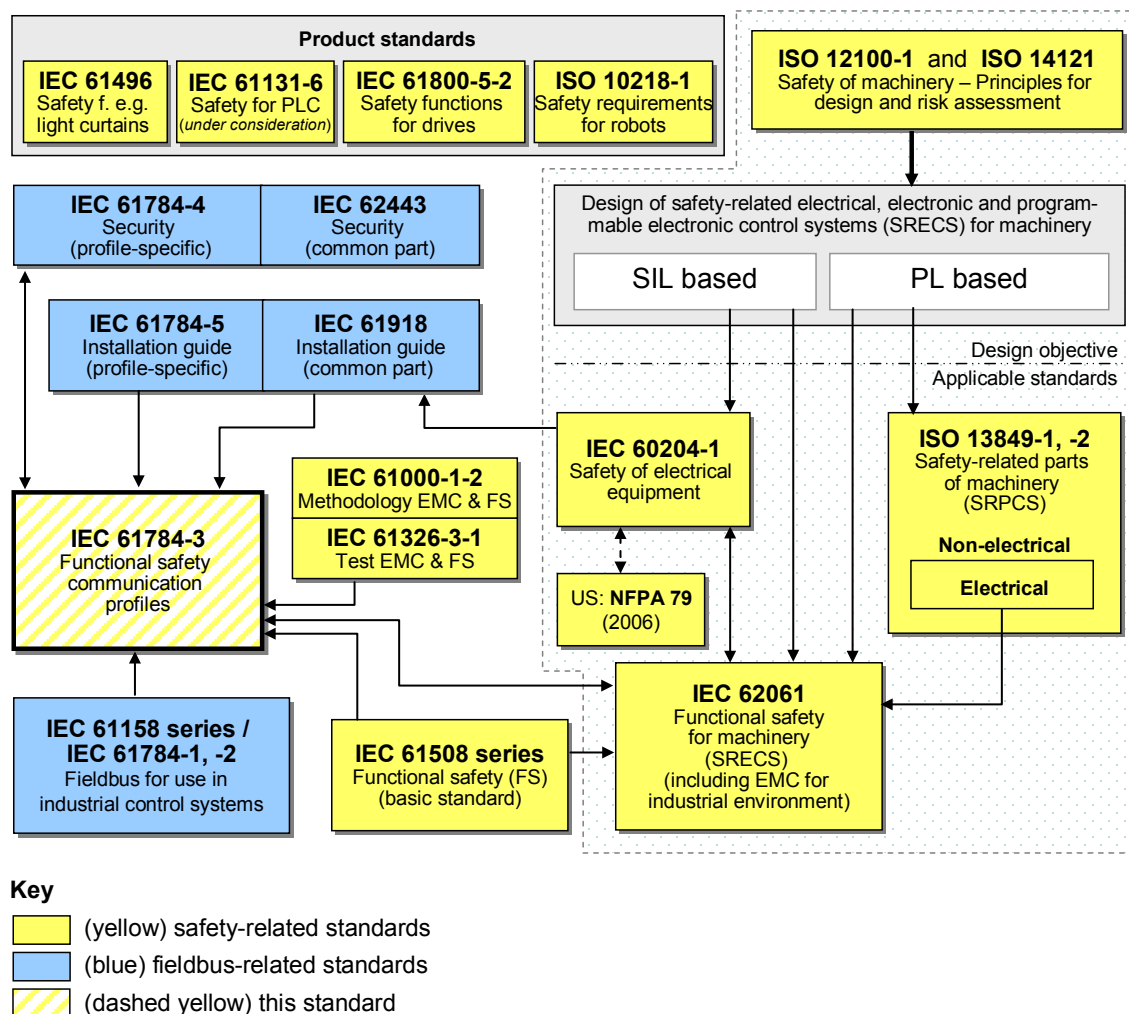
0 Introduction

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.

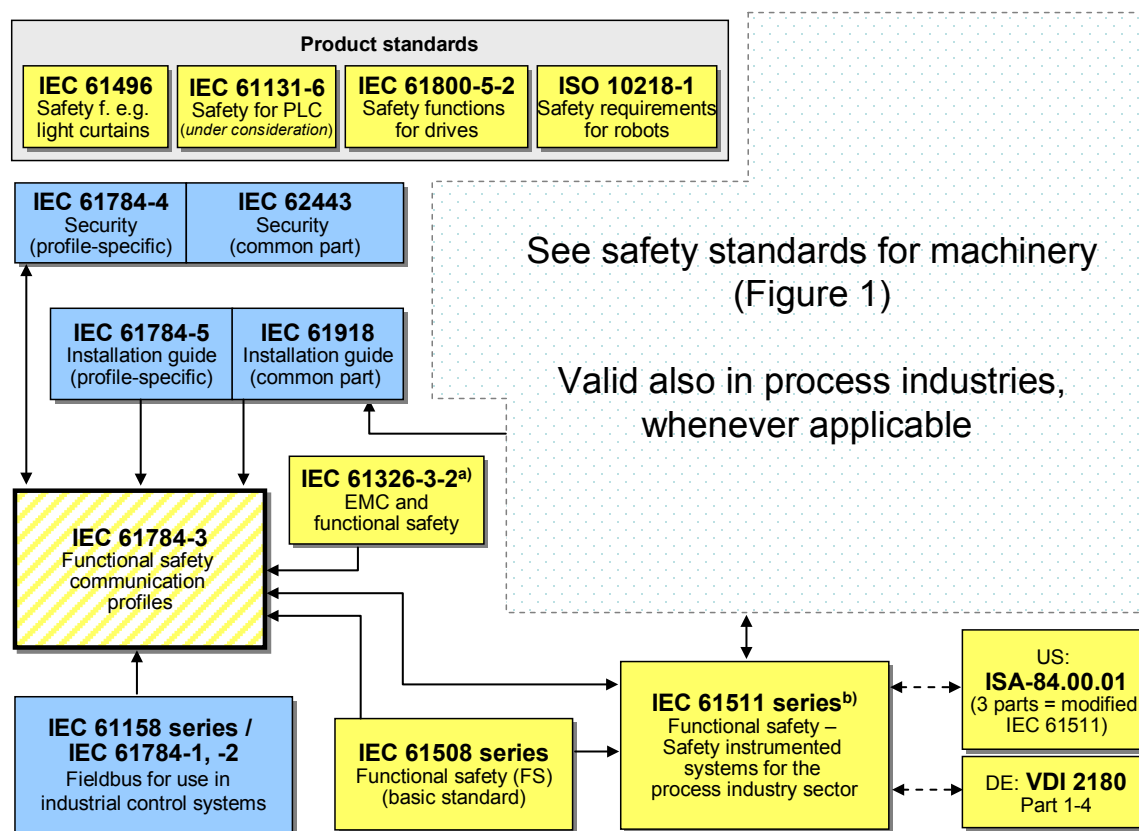
Figure 1 shows the relationships between this standard and relevant safety and fieldbus standards in a machinery environment.



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 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

bridge

abstract device that connects multiple network segments along the data link layer

3.1.1.4

communication channel

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

3.1.1.5

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

3.1.1.6

connection

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

³ In preparation.

3.1.1.7**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 [40], [41]⁴.

3.1.1.8**error**

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

[IEC 61508-4:2010⁵], [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*.

3.1.1.9**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)

3.1.1.10**fault**

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

NOTE IEC 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]

3.1.1.11**fieldbus**

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

3.1.1.12**frame**

denigrated synonym for DLPDU

3.1.1.13**hash function**

(mathematical) function that maps values from a (possibly very) large set of values into a (usually) smaller range of values

⁴ Figures in square brackets refer to the bibliography.

⁵ To be published.

NOTE 1 Hash functions can be used to detect data corruption.

NOTE 2 Common hash functions include parity, checksum or CRC.

[IEC/TR 62210, modified]

3.1.1.14

hazard

state or set of conditions of a system that, together with other related conditions will inevitably lead to harm to persons, property or environment

3.1.1.15

message

ordered series of octets intended to convey information

[ISO/IEC 2382-16.02.01, modified]

3.1.1.16

message sink

part of a *communication system* in which *messages* are considered to be received

[ISO/IEC 2382-16.02.03]

3.1.1.17

message source

part of a *communication system* from which *messages* are considered to originate

[ISO/IEC 2382-16.02.02]

3.1.1.18

performance level (PL)

discrete level used to specify the ability of safety-related parts of control systems to perform a safety function under foreseeable conditions

[ISO 13849-1]

3.1.1.19

redundancy

existence of means, in addition to the means which would be sufficient for a functional unit to perform a required function or for data to represent information

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

[IEC 61508-4:2010, modified], [ISO/IEC 2382-14.01.12, modified]

3.1.1.20

reliability

probability that an automated system can perform a required function under given conditions for a given time interval (t_1, t_2)

NOTE 1 It is generally assumed that the automated system is in a state to perform this required function at the beginning of the time interval.

NOTE 2 The term "reliability" is also used to denote the reliability performance quantified by this probability.

NOTE 3 Within the MTBF or MTTF period of time, the probability that an automated system will perform a required function under given conditions is decreasing.

NOTE 4 Reliability differs from availability.

[IEC 62059-11, modified]

3.1.1.21

risk

combination of the probability of occurrence of harm and the severity of that harm

NOTE For more discussion on this concept see Annex A of IEC 61508-5:2010⁶.

[IEC 61508-4:2010], [ISO/IEC Guide 51:1999, definition 3.2]

3.1.1.22

safety communication layer (SCL)

communication layer that includes all the necessary measures to ensure safe transmission of data in accordance with the requirements of IEC 61508

3.1.1.23

safety data

data transmitted across a safety network using a safety protocol

NOTE The Safety Communication Layer does not ensure safety of the data itself, only that the data is transmitted safely.

3.1.1.24

safety device

device designed in accordance with IEC 61508 and which implements the functional safety communication profile

3.1.1.25

safety function

function to be implemented by an E/E/PE safety-related system or other risk reduction measures, that is intended to achieve or maintain a safe state for the EUC, in respect of a specific hazardous event

NOTE The definition in IEC 61508-4 is the same, with an additional example and reference.

[IEC 61508-4:2010, modified]

3.1.1.26

safety function response time

worst case elapsed time following an actuation of a safety sensor connected to a fieldbus, before the corresponding safe state of its safety actuator(s) is achieved in the presence of errors or failures in the safety function channel

NOTE This concept is introduced in IEC 61784-3:2010, 5.2.4 and addressed by the functional safety communication profiles defined in this part.

3.1.1.27

safety integrity level (SIL)

discrete level (one out of a possible four), corresponding to a range of safety integrity values, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest

NOTE 1 The target failure measures (see IEC 61508-4:2010, 3.5.17) for the four safety integrity levels are specified in Tables 2 and 3 of IEC 61508-1:2010⁷.

NOTE 2 Safety integrity levels are used for specifying the safety integrity requirements of the safety functions to be allocated to the E/E/PE safety-related systems.

NOTE 3 A safety integrity level (SIL) is not a property of a system, subsystem, element or component. The correct interpretation of the phrase “SILn safety-related system” (where n is 1, 2, 3 or 4) is that the system is potentially capable of supporting safety functions with a safety integrity level up to n.

[IEC 61508-4:2010]

⁶ To be published.

⁷ To be published.

3.1.1.28

safety measure

<this standard> measure to control possible communication *errors* that is designed and implemented in compliance with the requirements of IEC 61508

NOTE 1 In practice, several safety measures are combined to achieve the required safety integrity level.

NOTE 2 Communication *errors* and related safety measures are detailed in IEC 61784-3:2010, 5.3 and 5.4.

3.1.1.29

safety-related application

programs designed in accordance with IEC 61508 to meet the SIL requirements of the application

3.1.1.30

safety-related system

system performing *safety functions* according to IEC 61508

3.1.1.31

time stamp

time information included in a *message*

3.1.2 CPF 14: Additional terms and definitions

3.1.2.1

configuration

definition of the standard communication connections and communication parameters for bus entities of a particular application

NOTE The configuration for safety communication comprises the definition of the Functional Safety Link Object and Functional Safety Management Object for safety-related bus entities of a particular safety-related application.

3.1.2.2

cross-check

verification that the redundantly transmitted data are identical

3.1.2.3

macro-cycle

one iteration of the link level schedule

3.1.2.4

masquerade

error due to mistaken identification information

3.1.2.5

publisher

message source that transmits messages on a periodic basis

3.1.2.6

subscriber

message sink that receives messages from a publisher

3.2 Symbols and abbreviated terms

3.2.1 Common symbols and abbreviated terms

CP	Communication Profile	[IEC 61784-1]
CPF	Communication Profile Family	[IEC 61784-1]
CRC	Cyclic Redundancy Check	

DLL	Data Link Layer	[ISO/IEC 7498-1]
DLPDU	Data Link Protocol Data Unit	
EMC	Electromagnetic Compatibility	
EUC	Equipment Under Control	[IEC 61508-4:2010]
E/E/PE	Electrical/Electronic/Programmable Electronic	[IEC 61508-4:2010]
FAL	Fieldbus Application Layer	[IEC 61158-5]
FS	Functional Safety	
FSCP	Functional Safety Communication Profile	
MTBF	Mean Time Between Failures	
MTTF	Mean Time To Failure	
PDU	Protocol Data Unit	[ISO/IEC 7498-1]
PFD	Probability of dangerous Failure on Demand	[IEC 61508-6:2010 ⁸]
PFH	Average frequency of dangerous failure [h ⁻¹] per hour	[IEC 61508-6:2010]
PhL	Physical Layer	[ISO/IEC 7498-1]
PL	Performance Level	[ISO 13849-1]
PLC	Programmable Logic Controller	
SCL	Safety Communication Layer	
SIL	Safety Integrity Level	[IEC 61508-4:2010]

3.2.2 CPF 14: Additional symbols and abbreviated terms

AP	Application Process	
APDU	Application Process Data Unit	
ASE	Application Service Element	
ASIC	Application Specific Integrated Circuit	
CSME	Communication Schedule Management Entity	
EPA	Ethernet for Plant Automation	
EPASafety	EPA Safety	
FB	Function Block	
FBAP	Function Block Application Process	
FSPDU	Functional Safety Protocol Data Unit	
IP	Internet Protocol	(RFC 791, see [37])
LED	Light Emitting Diode	
MAC	Medium Access Layer	
MIB	Management Information Base	
SN	Sequence Number	
TCP	Transport Control Protocol	(RFC 793, see [37])
UDP	User Datagram Protocol	(RFC 768, see [37])
VSCM	Virtual Safety Check Message	

3.3 Conventions

This part mainly uses flow charts as appropriate to describe definitions.

⁸ To be published.

4 Overview of FSCP 14/1 (EPASafety®)

4.1 EPASafety®

Communication Profile Family 14 (commonly known as EPA®⁹) defines communication profiles based on IEC 61158-3-14, IEC 61158-4-14, IEC 61158-5-14, and IEC 61158-6-14.

The basic profiles CP 14/1 and CP 14/2 are defined in IEC 61784-2. The CPF 14 functional safety communication profile FSCP 14/1 (EPASafety®⁹) is based on the CPF 14 basic profiles in IEC 61784-2 and the safety communication layer specifications defined in this part.

The EPA system is a real-time Ethernet specified in IEC 61158 and IEC 61784-2. EPA defines a deterministic communication control system based on an Ethernet network defined by ISO/IEC 8802-3 to connect field devices and small systems, and to control/monitor equipment in the industrial field.

EPASafety describes the safe communication specification used to connect safety field devices and controllers in EPA systems. It is a supplementary technology based on the EPA protocol specified in IEC 61158 to reduce the failure or error probability of the data transmission between safety transmitters, actuators and field controllers to the level required by the relevant standards, or better.

4.2 Principle of EPA safety communications

EPA communication is based on the black channel principle as shown in Figure 3. A black channel includes non safety-relevant devices such as wires, fiber optics, repeater, barrier, power supplies, ASIC, communication stack, EPA bridge, interface etc. Communication stack includes physical layer, data link layer, network layer (IP layer), transport layer (UDP layer) and application layer.

During data transferring in a black channel, some fault or error may occur because of the following reasons:

- a) random fault;
- b) standard hardware failure/fault;
- c) system failure caused by standard hardware or software components.

In an EPASafety system, safety applications and standard applications are sharing the same communication channel at the same time. The safe transmission function comprises all measures to deterministically discover all above possible faults / hazards that shall be infiltrated by the standard transmission system or to keep the residual error (fault) probability under a certain limit.

⁹ EPA® and EPASafety® are trade names of Zhejiang SUPCON® Sci&Tech Group Co. Ltd. China. This information is given for the convenience of users of this International Standard and does not constitute an endorsement by IEC of the trade name holder or any of its products. Compliance to this standard does not require use of the trade names EPA® or EPASafety®. Use of the trade names EPA® or EPASafety® requires permission of SUPCON®.

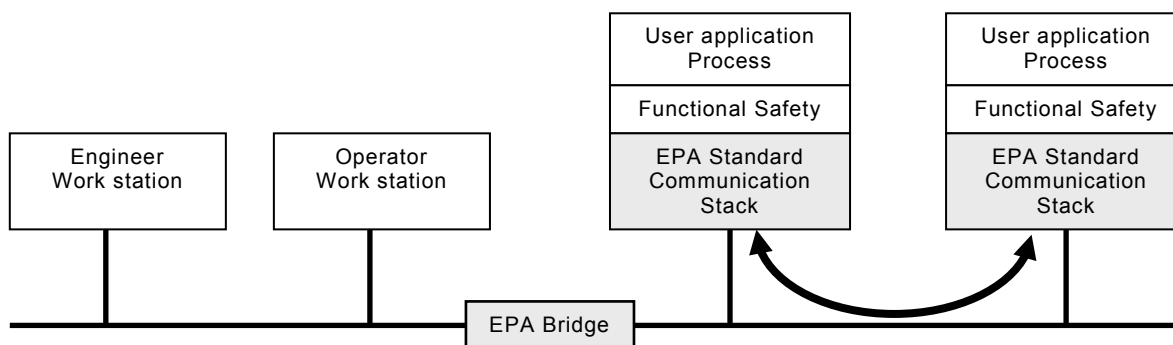


Figure 3 – Safety communication architecture

4.3 Safety function processing

As the Function Block Application Process model specified in IEC 61158, the safety function performed by the safety communication system shall be decomposed into the following function blocks: Input safety data, Safe communication, Safety calculation, and Output safety data.

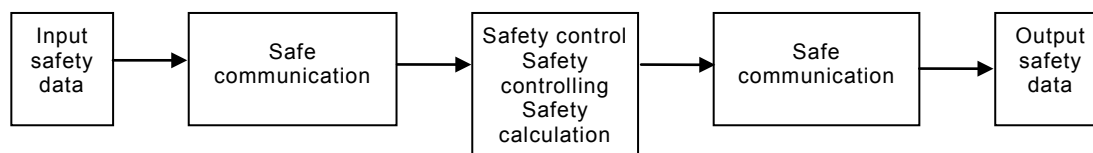


Figure 4 – Safety function processing

As shown in Figure 4, the safety function is implemented as follows:

- The input function block reads the physical input signals from sensors and transfers it to the safety communication stack;
- The safety communication stack performs the safety-relevant communication services of the input function block resident field device (e.g. EPA safe-relevant transmitter);
- The input device sends the safety relevant input data to the controlling function block in the safety controlling calculation device through the safety transmission channel;
- The safety communication stack performs the safety-relevant communication services of the safety controlling function block resident field device (e.g. EPA safe-relevant field controller);
- The safety controlling block performs the controlling task (e.g. PID) of the received input signals and generates new safety relevant output data based on safety relevant application software;
- Through the safe communication stack processing, the output function block reads the received output data from the communication channel, transforms them into the physical output signal, and makes them available at the terminal block of a safety relevant output device (e.g. EPA safe-relevant actuator).

5 General

5.1 External documents providing specifications for the profile

There is no external document providing specifications for the profiles.

5.2 Safety functional requirements

The designer of safety related devices shall take into account the requirements of IEC 61508.

Safety communication and standard communication shall be able to use the same communication channel. Transmission equipment shall remain unmodified (black channel). Redundancy may be used not only for increased availability but also for safety communication.

The measures in FSCP 14/1 communication systems for reducing possible transmission errors are provided as follows:

- FSCP 14/1 shall be designed to permit vendors to develop products suitable for use in SIL3 (IEC 61508) applications;
- the protocol shall support the process-data transmission and message-data transmission between field device and work station;
- the safety related protocol shall prevent interference from non-safety related devices. E.g. a non-safety related handheld shall not be permitted to change parameters in a safety related device;
- the protocol shall protect against unintended or non-authorized configuration changes to an FSCP 14/1 safety device,
- there shall be an FSCP 14/1 application guide for the end-user to implement a safety related system using FSCP 14/1 safety devices,
- the contribution of the FSCP 14/1 communication protocol to the PFD/PFH shall be less than 1% of the value required by SIL level,
- PFD/PFH calculations shall be based on the low demand mode and the high demand mode respectively (as defined in IEC 61508).
- the protocol shall implement measures to control the following faults:
 - data bit error;
 - unintended repetition;
 - loss;
 - insertion;
 - incorrect sequence;
 - masquerade;
 - unacceptable delay;
 - addressing error.
- it shall be possible to calculate the reaction time for the application;
- it shall be possible to use devices with different SIL levels on the same network;
- it shall be possible to by-pass and maintain the devices in a safe manner;
- the safe state of the safety devices shall principally be the deenergized state.

5.3 Safety measures

The measures in FSCP 14/1 communication systems for reducing possible transmission errors are provided as follows:

- sequence number;
- timestamp;
- communication relationship key;
- feedback message;
- cyclic redundancy check and cross-check for safety data integrity;

- scheduling number;
- time expectation.

The relationship between safety measures and communication errors is defined in Table 1. One or more safety measures shall be used for mastering one kind of possible communication error.

Table 1 – Relationships between errors and safety measures

Communication errors	Safety measures							
	Sequence number 1 (see NOTE 1)	Time stamp	Time expectation	Connection authentication (see NOTE 2)	Feedback message	Data integrity assurance	Redundancy with cross checking	Different data integrity assurance systems
Corruption						X	X	
Unintended repetition	X	X						
Incorrect sequence	X	X						
Loss	X				X			
Unacceptable delay		X	X					
Insertion	X			X	X			
Masquerade				X	X			X
Addressing				X				
NOTE 1 The sequence number is combined of two parts. One is the sequence number, the other is the schedule number. The sequence number is integrated into messages exchanged between message source and message sink. It may be realised as an additional data field with a number that changes from one message to the next in a predetermined way. The schedule number is for the order of sending message of devices in each macro cycle. NOTE 2 Connection authentication will be implemented as communication relation key.								

The message is packed with the time stamp which is the local time of the sender, the sequence number, relation key and CRC checksum.

5.4 Safety communication layer structure

5.4.1 Combination of standard communication and safety communication systems

Figure 5 shows the system architecture including standard devices and safety devices. Typically, the system is composed of interconnected CP 14/1 host devices (e.g. operation station or engineering station), safety field controllers, safety actuators, safety transmitters, standard actuators and standard transmitters on one CP 14/1 Micro-segment.

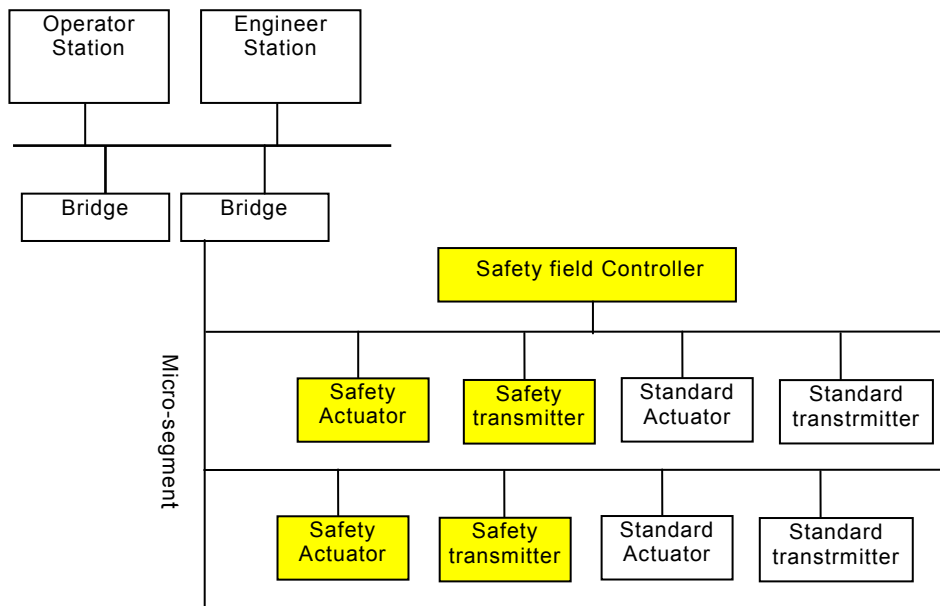


Figure 5 – Standard communication and safety communication

Here, safety communications and standard communications shall share the same transmission medium. Safety transmitters and safety actuators send or receive safety relevant data. Standard transmitters and standard actuators send or receive non-safety relevant data while safety field controllers shall receive, send and process both safety and non-safety relevant data. That is, safety field controllers shall support both safety and standard communication services.

5.4.2 CP 14/1 safety communication structure

FSCP 14/1 functional safety communication extended profile is located in the application layer and it is the upper layer of Socket Mapping Entity and Standard Application Layer Entity. The architecture can achieve independence between standard and safety communication, ensure functional safety for safety message. Also, it makes no changes in original system structure and performance. Safety devices and standard devices shall work in the same network.

FSCP 14/1 functional safety communication extended profile is located above the communication stack (includes Standard Application Layer Entity, Socket Mapping Entity, UDP/IP, Communication Schedule Management Entity, Ethernet Data Link Layer and Physical Layer) and under the user layer FBAP. The protocol hierarchy of CP 14/1 and FSCP 14/1 safety communication is shown in Figure 6.

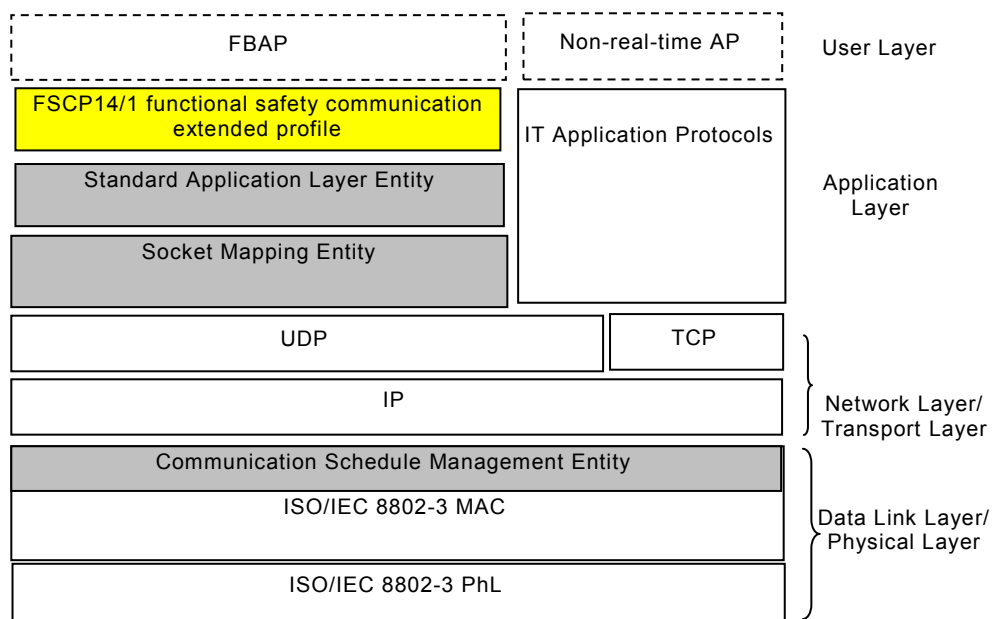


Figure 6 – CP 14/1 protocol hierarchy

The communication stack is used for getting the safety data from the functional communication protocol, generating a standard message with standard header and safety data and transferring the standard message to UDP/IP. On the other hand, the communication stack is used for getting the standard message from UDP/IP, decoding the standard message and transferring the safety data to functional safety communication protocol.

The functional safety communication protocol is used for getting user-data, encoding the user-data with safety measure (such as CRC check, time-stack, and sequence number) to safety data and transferring the safety data to the communication stack with an interface. On the other hand, the functional safety communication protocol is used for getting safety data from the communication stack, decoding the safety data to user-data and handling the related service.

5.5 Relationships with FAL (and DLL, PhL)

5.5.1 Overview

Figure 7 shows the relationship between the Safety Communication Layer (SCL) and the other layers of CP 14/1.

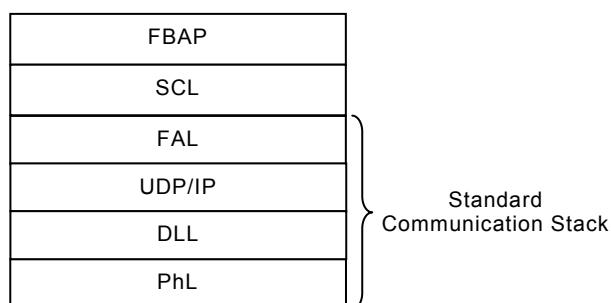


Figure 7 – Relationship between the SCL and the other layers of CP 14/1

5.5.2 Data types

FSCP 14/1 protocol supports all the data types as defined in IEC 61158-5-14 (see Table 2).

Table 2 – Data types used within FSCP 14/1

Data type name	Number of octets
Integer8	1
Integer16	2
Integer32	4
Unsigned8 (used as bits)	1
Unsigned16 (used as bits)	2
Unsigned32 (used as bits)	4
Unsigned16	2
Unsigned32	4
Floating Point 32	4
Date	
TimeOfDay with date indication	
TimeOfDay without date indication	
TimeDifference with date indication	
TimeDifference without date indication	
Visible String	1,2,3, ...

6 Safety communication layer services

6.1 Overview

This subclause defines the extension to existing objects and extended services of CP 14/1 standard Application Layer Entity for FSCP 14/1. The extended objects are stored in the device MIB (Management Information Base). These objects are used to define the behaviour of the safety communication and the action taken when the communication error occurs. The Safety Communication services are used to open or close a safety communication between host and safety devices.

6.2 FSCP 14/1 object extensions

6.2.1 General

This subclause describes the additional objects (as shown in Table 3) in device MIB used in FSCP 14/1 relevant devices.

Table 3 – FSCP 14/1 object extensions

Object	Object ID	Illustration
Functional safety communication management object	10	FSCP 14/1 communication management object
Functional safety communication alert object	11	Functional Safety communication alert object
Functional Safety Link object 1	6 000	Functional Safety Link object 1
Functional Safety Link object 2	6 001	Functional Safety Link object 2
.....		

6.2.2 Functional safety communication management object

6.2.2.1 General

For nonperiodic communication, functional safety communication management object is added to information management base.

6.2.2.2 Form model

ASE:	SYSTEM MANAGEMENT ASE
CLASS:	FUNCTIONAL Safety COMM MANAGEMENT OBJECT
CLASS ID:	Not Used
PARENT CLASS:	TOP

ATTRIBUTES:

1. (m) Key attribute: Object ID
2. (m) Attribute: Max Nonperiodic Channel Number
3. (m) Attribute: Free Nonperiodic Channel Number
4. (m) Attribute: MaxResponseTime
5. (m) Attribute: Service Option

SERVICES:

1. (o) Ops Service: Read
2. (o) Ops Service: Write
3. (o) Ops Service: SafetyCommunicationClose
4. (o) Ops Service: SafetyCommunicationOpen

6.2.2.3 Attribute

Object ID

This attribute identifies functional safety communication management object in CP 14/1 device MIB. Its value is 10. This attribute's data type is Unsigned16, and the access right is Read only.

Max Nonperiodic Channel Number

This attribute specifies the maximum nonperiodic channel number supported by the device. This attribute's data type is Unsigned8, and the access right is Read only.

Free Nonperiodic Channel Number

This attribute specifies current value of the free nonperiodic channel number in the device. This attribute's data type is Unsigned8, and the access right is Read only.

MaxResponseTime

This attribute specifies the maximum response time from sending the service request to receiving the service response. If the response has not been received in MaxResponseTime, the requester considers that a communication failure has occurred in the communication and retries the same service request three times. Its data type is 4 bytes of TimeDifference, and the access right is Read and Write.

Service Option

This attribute specifies the kinds of services which the FSCP 14/1 safety layer supports. This attribute's data type is Unsigned16, and the access right is Read and Write. It may be set by the user application:

- Bit 0——Distribute service;
- Bit 1——Read service;
- Bit 2——Write service;
- Bit 3——Event notify service;
- Bit 4——Event notify acknowledge service;

- Bit 5——Domain upload service;
- Bit 6——Domain download service;
- Other——reserved.

6.2.2.4 Service

Read

This optional service provides reading the attribute of the Functional Safety Configuration Object. The Read service is defined in IEC 61158-5-14.

Write

This optional service permits users to configure the attributes of the Functional Safety Configuration Object. The Write service is defined in IEC 61158-5-14.

SafetyCommunicationOpen

This optional service permits users to initial the value of the Functional Safety Communication Management Object. The SafetyCommunicationOpen service is defined in 6.3.2.

SafetyCommunicationClose

This optional service permits users to reset the value of the Functional Safety Communication Management Object. The SafetyCommunicationClose service is defined in 6.3.3.

6.2.3 Functional Safety Link Object

6.2.3.1 General

The Functional Safety Link Object is the extension of link object defined in IEC 61158-5-14. It specifies the communication relationship for periodic data transmission.

6.2.3.2 Form model

ASE:		APPLICATION RELATIONSHIP ASE
CLASS:		FUNCTIONAL SAFETY LINK OBJECT
CLASS ID:		Not Used
PARENT CLASS:		TOP
ATTRIBUTES:		
1. (m)	Key attribute:	Object ID
2. (m)	Attribute:	Local App ID
3. (m)	Attribute:	Local Object ID
4. (m)	Attribute:	Remote App ID
5. (m)	Attribute:	Remote Object ID
6. (m)	Attribute:	ServiceOperation
7. (m)	Attribute:	Service Role
8. (m)	Attribute:	Remote IP Address
9. (m)	Attribute:	Send Time Offset
10. (m)	Attribute:	Configured Scheduling Number
11. (m)	Attribute:	Scheduling Precision Requirement
12. (m)	Attribute:	RelationKey
13. (m)	Attribute:	LinkageFault
14. (m)	Attribute:	FaultReportConfiguration
15. (m)	Attribute:	FaultAcknowledgeConfiguration
SERVICES:		
1. (o)	Ops Service:	Read
2. (o)	Ops Service:	Write
3. (o)	Ops Service:	SafetyCommunicationClose
4. (o)	Ops Service:	SafetyCommunicationOpen

6.2.3.3 Attribute

Object ID

This attribute identifies functional safety Link Object in MIB. The number of ObjectID of Link Object shall be appointed in series. Its data type is unsigned16, and the access right is Read.

LocalAppID

This attribute identifies local FB instance. Its data type is unsigned16, and the access right is Read and Write.

Local Object ID

This attribute identifies local variant object. Its data type is unsigned16, and the access right is Read and Write.

Remote App ID

This attribute identifies remote FB instantiation. Its data type is unsigned16, and the access right is Read and Write.

RemoteObjectID

This attribute identifies remote variant object. Its data type is unsigned16, and the access right is Read and Write.

ServiceOperation

This attribute specifies the application service to be used in the relevant communication relationship:

- 0——local link, no application service is used;
- 1 through 23—— the ServiceID of application services is used;
- Others—— invalid service.

Its data type is unsigned8, and the access right is Read and Write.

ServiceRole

This attribute defines the AREP role of local device in communication process:

- 0——SENDER, indicating that the AREP role of the local device is CLIENT or PUBLISHER;
- 1——RECEIVER, indicating that the AREP role of the local device is SERVER or SUBSCRIBER;
- Others——Link Object is invalid, and 0xFF indicates that the Link Object is not configured or the Link Object has been deleted.

Its data type is unsigned8, and the access right is Read and Write.

RemoteIPAddress

This attribute identifies IP address of remote device. This attribute shall be ignored if local FB instantiation object and remote FB instantiation object are in the same device. Its data type is unsigned32, and the access right is Read and Write.

SendTimeOffset

This attribute defines the time offset when the relevant message shall be sent from the start time of a communication macro-cycle. This attribute is valid when Service ID is 0x0E (DISTRIBUTE) and ServiceRole is 0x00. Its data type is 4 bytes of TimeDifference, and the access right is Read and Write.

Configured Scheduling Number

This attribute specifies the sequence number in one macro-cycle for local device to send the data related to this functional safety link object. Its data type is unsigned16, and the access right is Read and Write.

Scheduling Precision Requirement

This attribute indicates the expected data sending time precision for local device. It may be set by the user application:

- 0——no precision requirement;
- 1——data sending time precision < 1 s;
- 2——data sending time precision < 100 ms;
- 3——data sending time precision < 10 ms;
- 4——data sending time precision < 1 ms;
- 5——data sending time precision < 100 µs;
- 6——data sending time precision < 10 µs;
- 7——data sending time precision < 1 µs.

Its data type is unsigned16, and the access right is Read and Write.

RelationKey

This attribute specifies the current value of RelationKey for the FS link object.

Its data type is unsigned32, and access right is SafetyCommunicationOpen and SafetyCommunicationClose.

LinkageFault

This attribute is defined to record the current communication faults. It may be set by the user application:

- Bit 0——linkage state;
- Bit 1——fault report state;
- Bit 2——fault acknowledge state;
- Other——reserved.

Its data type is unsigned16, and the access right is Read and Write.

FaultReportConfiguration

This attribute is defined to determine whether to report the communication fault to the special application or not. It may be set by the user application:

- 0——report the communication fault;
- 1——do not report the communication fault;
- Other——reserved

Its data type is unsigned8, and the access right is Read and Write.

FaultAcknowledgeConfiguration

This attribute is defined to determine whether the communication fault is acknowledged by the special application or not. It may be set by the user application:

- 0—the communication fault needs acknowledge;
- 1—the communication fault does not need acknowledge;
- Other—reserved

Its data type is unsigned8, and the access right is Read and Write.

6.2.3.4 Service

Read

This optional service provides reading the attribute of Functional Safety Configuration Object. The Read service is defined in IEC 61158-5-14.

Write

This optional service permits users to configure the attributes of Functional Safety Configuration Object. The Write service is defined in IEC 61158-5-14.

SafetyCommunicationOpen

This optional service permits users to initial the value of RelationKey in the Functional Safety Link Object. SafetyCommunicationOpen is defined in 6.3.2.

SafetyCommunicationClose

This optional service permits users to reset the value of RelationKey in the Functional Safety Link Object. SafetyCommunicationClose is defined in 6.3.3.

6.2.4 Functional safety communication alert object

6.2.4.1 General

Every functional safety device has only one universal Functional Safety Alert Object, which is used to send the communication failure to the special application.

6.2.4.2 Form model

ASE:	SYSTEM MANAGEMENT ASE
CLASS:	FUNCTIONAL SAFETY COMM ALERT OBJECT
CLASS ID:	Not Used
PARENT CLASS:	TOP
ATTRIBUTES:	
1. (m)	Key attribute: Object ID
2. (m)	Attribute: Total Fault Counter
3. (o)	Attribute: Local Fault Recorders
3.1 (m)	Attribute: CRC Error Counter
3.2 (m)	Attribute: Sequence Error Counter
3.3 (m)	Attribute: Time Delay Counter
3.4 (m)	Attribute: Time Synchronize Error Counter
3.5 (m)	Attribute: Communication Scheduling Error Counter
SERVICES:	
1. (o)	Ops Service: Read
2. (o)	Ops Service: EventNotification
3. (o)	Ops Service: AcknowledgeEventNotification

6.2.4.3 Attribute

Object ID

This attribute identifies Functional Safety Alert Object in device MIB. Its value is 11. This attribute's data type is Unsigned16, and the access right is Read only.

Total Fault Counter

This attribute specifies the counter for all communication faults to be detected. Its data type is unsigned16, and the access right is Read only.

Local Fault Recorders

This attribute specifies the recorders for each communication faults to be detected. Its data type is unsigned16, and the access right is Read only.

CRC Error Counter

This attribute specifies the recorders for CRC Error to be detected. Its data type is unsigned16, and the access right is Read only.

Sequence Error Counter

This attribute specifies the recorders for Sequence Error to be detected. Its data type is unsigned16, and the access right is Read only.

Time Delay Counter

This attribute specifies the recorders for Time Delay to be detected. Its data type is unsigned16, and the access right is Read only.

Time Synchronize Error Counter

This attribute specifies the recorders for Time Synchronize Error to be detected. Its data type is unsigned16, and the access right is Read only.

Communication Scheduling Error Counter

This attribute specifies the recorders for Communication Scheduling Error to be detected. Its data type is unsigned16, and the access right is Read only.

6.2.4.4 Service

Read

This optional service provides reading the attribute of Functional Safety Link Object. The Read service is defined IEC 61158-5-14.

EventNotification

This optional service allows the safety device to send the communication failure to the special host determined by Functional Safety Link Object. The EventNotification service is defined in IEC 61158-5-14.

AcknowledgeEventNotification

This optional service allows the special host to acknowledge alert of communication failure from failed device. The AcknowledgeEventNotification service is defined in IEC 61158-5-14.

6.3 Extended services

6.3.1 General

Table 4 defines additional services for use in safety devices. The index and ServiceID are specified in IEC 61158-5-14.

Table 4 – Functional safety service extension

Index	Service name	ServiceID	Confirmed / Unconfirmed	Priority	Description of Service
19	SafetyCommunicationOpen	18	Confirmed	2	Initialize link relationship of function safety communication
20	SafetyCommunicationClose	19	Confirmed	2	Close link relationship of function safety communication

6.3.2 SafetyCommunicationOpen

6.3.2.1 Service general

The SafetyCommunicationOpen service is a confirmed service. This service is used to enable the function safety communication relationship.

6.3.2.2 Service primitives

The service parameters for SafetyCommunicationOpen service are shown in Table 5.

Table 5 – SafetyCommunicationOpen Service Parameters

Parameter name	.req	.ind	.rsp	.cnf
Argument	M	M(=)		
MessageID	M	M(=)		
SourceAppID	M	M(=)		
SourceIPAddress	M	M(=)		
DestinationIPAddress	M	M(=)		
RelationKey	M	M(=)		
CommunicationType	M	M(=)		
LinkObjectType	S	S		
LinkObjectID	M	M(=)		
CommunicationObjectType	S	S		
AccessRight	M	M(=)		
Result(+)			S	S(=)
MessageID			M	M(=)
DestinationAppID			M	M(=)
Result(-)			S	S(=)
MessageID			M	M(=)
DestinationAppID			M	M(=)
ErrorType			M	M(=)

Argument

The argument contains the parameters of this service.

MessageID

This parameter contains the invoked number of this service. Each time this service is invoked, the value of this parameter is increased by adding 1.

SourceAppID

This parameter contains the identifier of source FB instantiation.

Source IP Address

This parameter contains the source IP address to which the service request is to be sent.

Destination IP Address

This parameter contains the destination IP address to which the service request is to be sent.

RelationKey

This parameter contains the value of RelationKey for the communication channel. Each safety nonperiodic channel applies an only 32-bit RelationKey.

CommunicationType

This parameter contains the type of communication:

- 0——Link Object type;
- 1——Communication Object type;
- Other——Reserved.

LinkObjectID

This parameter contains the ID of Link Object which shall be configured to be for functional safety communication.

AccessRight

This parameter contains the access right needed for the communication channel.

- 0——Read only, the safety communication channel is read-only;
- 1——Writable, the safety communication channel is writable;
- Others—— invalid.

Result(+)

This optional parameter indicates that the service request succeeded.

DestinationAppID

This parameter contains the identifier of destination FB instantiation.

Result(-)

This optional parameter indicates that the service request failed.

ErrorType

This parameter contains the reason that caused failure.

6.3.2.3 Service procedure

The confirmed service procedure specified in IEC 61158-5-14 applies to this service.

6.3.3 SafetyCommunicationClose

6.3.3.1 Service general

The SafetyCommunicationClose service is a confirmed service. This service is used to disable the function safety communication channel.

6.3.3.2 Service primitives

The service parameters for SafetyCommunicationClose service are shown in Table 6.

Table 6 – SafetyCommunicationClose Service Parameters

Parameter name	.req	.ind	.rsp	.cnf
Argument	M	M(=)		
MessageID	M	M(=)		
SourceAppID	M	M(=)		
SourceIPAddress	M	M(=)		
DestinationIPAddress	M	M(=)		
LinkObjectID	M	M(=)		
Result(+)			S	S(=)
MessageID			M	M(=)
DestinationAppID			M	M(=)
Result(-)			S	S(=)
MessageID			M	M(=)
DestinationAppID			M	M(=)
ErrorType			M	M(=)

Argument

The argument contains the parameters of this service.

MessageID

This parameter contains the invoked number of this service. Each time this service is invoked, the value of this parameter is increased by adding 1.

SourceAppID

This parameter contains the identifier of source FB instantiation.

Source IP Address

This parameter contains the source IP address to which the service request is to be sent.

Destination IP Address

This parameter contains the destination IP address to which the service request is to be sent.

LinkObjectID

This parameter contains the ID of Link Object which shall be reset to normal communication. If the LinkObjectID is 0x0000, it means that the service wants to close the communication object.

Result(+)

This optional parameter indicates that the service request succeeded.

DestinationAppID

This parameter contains the identifier of destination FB instantiation.

Result(-)

This optional parameter indicates that the service request failed.

ErrorType

This parameter contains the reason that caused failure.

6.3.3.3 Service procedure

The confirmed service procedure specified in IEC 61158-5-14 applies to this service.

7 Safety communication layer protocol

7.1 Safety PDU format

7.1.1 General

Figure 8 shows the functional safety communication message structure, including CP 14/1 protocol type, IP header, UDP header, APDU Header and redundant functional safety PDU (FSPDU).

Functional safety transmission message follows the standard message format.

TYPE	IP Header	UDP Header	APDU Header	Redundant FSPDU
------	-----------	------------	-------------	-----------------

Figure 8 – Functional safety communication message structure

7.1.2 APDU header structure

The structure of APDU header is shown in Table 7.

Table 7 – Encoding of APDU Header

No.	Parameter name	Data type	Octet offset	Octet length	Description
1	ServiceID	Unsigned8	0	1	This parameter describes the service type and message type. Bit 7 to 6 indicates the message type: 00 – request message 01 – response message 10 – error message 11 – reserved The lowest six bits used to signify the service ID
2	CommType	Unsigned8	1	1	0 – standard communication 1 – safety communication Others – reserved
3	Reserved	OctetString	2	2	Not used
4	Length	Unsigned16	4	2	This parameter describes the length of the whole message
5	MessageID	Unsigned16	6	2	This parameter describes the ID of the message

7.1.3 Functional safety PDU

Functional safety PDU(FSPDU) consists of CRC, functional safety header and standard UserData (see Figure 9).

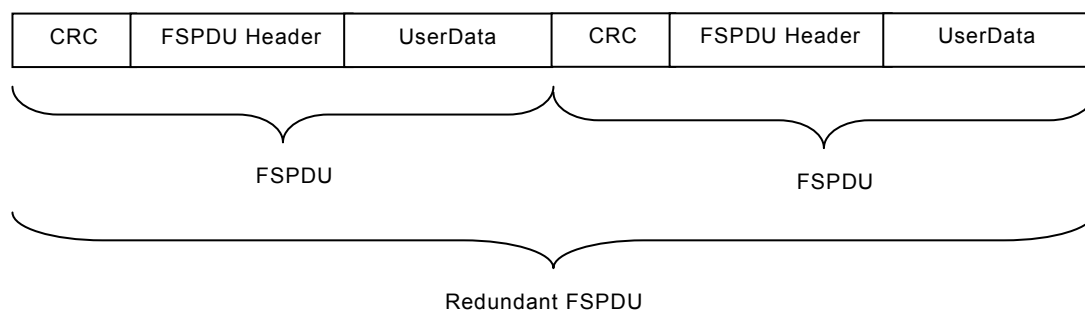


Figure 9 – Structure of Functional Safety PDU (FSPDU)

The CRC check code is calculated by the CRC check algorithms on the Virtual Safety Check Message (VSCM) which consists of RelationKey, sequence number, scheduling number, timestamp and original user data. The data structure of VSCM is shown in Figure 10.

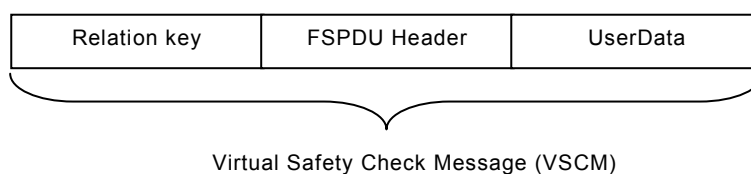


Figure 10 – Structure of Virtual Safety Check Message (VSCM)

The structure of Functional safety PDU (FSPDU) Header is defined as Table 8.

Table 8 – Structure of Functional Safety PDU (FSPDU) Header

Index	Parameter name	Data type	Octet offset	Octet length	Description
1	SequenceNumber	Unsigned16	0	2	Sequence Number
2	SchedulingNumber	Unsigned16	2	2	Scheduling Number
3	TimeStamp	BinaryDate	4	8	The current time of FSPDU

The functional safety PDU mapping is shown in Figure 11.

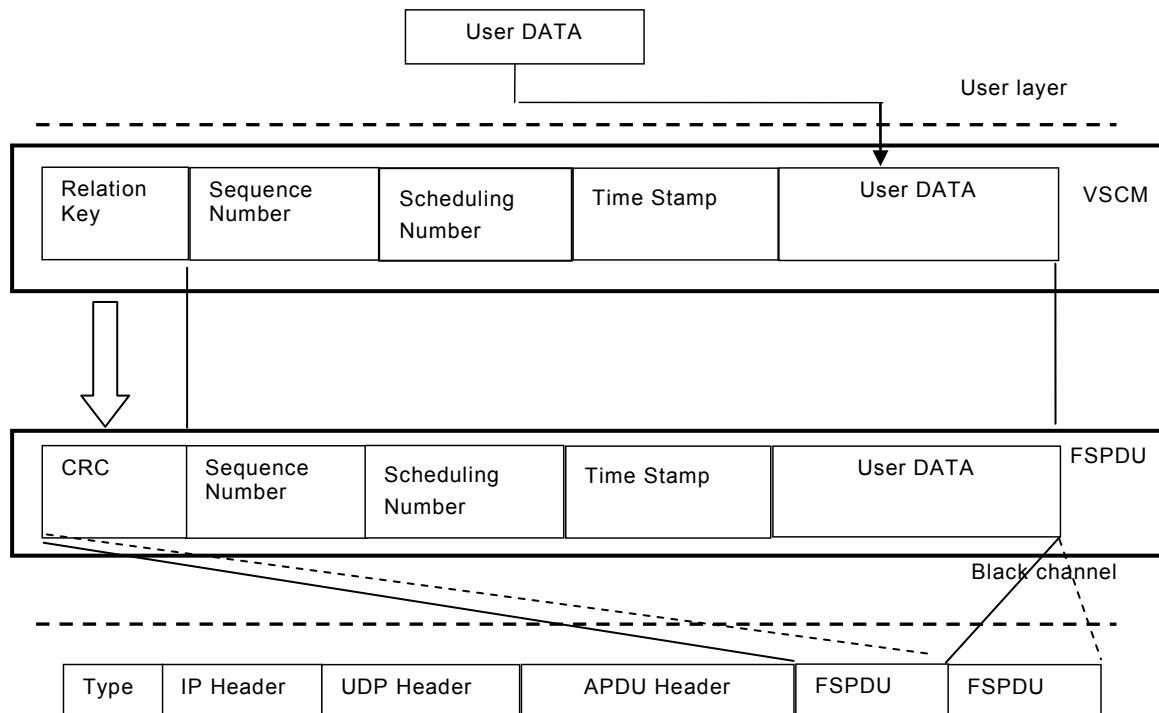


Figure 11 – FSPDU mapping

7.2 Safety communication operation

7.2.1 Sequence number

For periodic data transmission, a sequence number is used to track the process data transmission and is also used to detect the communication errors, such as loss, repetition and incorrect sequence.

For non-periodic data transmission, a sequence number is mainly used to track the continuous data transmission but is also used to detect the communication errors, such as loss, repetition and incorrect sequence.

The initial value of sequence number is set to 0 and its value is increased by adding 1 when each FSPDU is delivered to the black channel.

7.2.2 RelationKey

7.2.2.1 General

RelationKey is initialized by a configuration tool. RelationKey is not transmitted after the configuration process is completed, but only participates in constructing VSCM. The data type of RelationKey is 32-bit OctetString.

7.2.2.2 Configuration and initialization

During system configuration, the configuration tool shall specify the RelationKey attribute of functional safety link objects for each safety relevant device using the Write service defined in IEC 61158-5-14.

After receiving the SafetyCommunicationOpen request, each safety relevant device shall get an initialization value for the RelationKey attribute for nonperiodic communication according to the parameters of the SafetyCommunicationOpen request.

7.2.2.3 Operation

Each safety link object and safety non-periodic channel applies an only 32-bit RelationKey in micro segment.

When generating functional safety PDU (FSPDU), the safety relevant sender shall use the RelationKey to generate the value of CRC segment of FSPDU as shown in 7.1.3. The RelationKey shall not appear in encoding FSPDU.

When receiving the FSPDU, the safety relevant device shall generate a local CRC value, using VSCM segment and RelationKey. Only the local CRC value is equal to the value of CRC segment in FSPDU, the values in VSCM segment are legal.

7.2.3 Feedback message

In functional safety communication systems, any device shall report the fault state (as shown in Functional safety communication alert object) to the system operators using EventNotification or AcknowledgeEventNotification services when it detects any communication errors. After receiving and confirming the communication fault, the system operator shall take corresponding measures to remove the faults.

Besides, a Socket Timer object and a Socket Mapping object defined in Socket Mapping Entity in IEC 61158-5-14 is used to monitor the response primitive for each confirmed service. If the service requestor does not receive the response primitive in MaxResponseTime after the service request primitive is sent, the Socket Mapping Entity shall report the overtime error. If necessary, it shall retransmit the service request primitive in MaxRetransmitNumber times defined in Socket Mapping object.

7.2.4 CRC-cross-check

The functional safety communication protocol contains a mechanism that transmits two copies of the whole data including a timestamp, a scheduling number, a sequence number and CRC in a single frame. At the receiving end, the two copies are cross-checked to detect whether corruption has occurred.

Cyclic redundancy check (CRC) is also used to control data corruption failures in functional safety communication systems. Data is transmitted in frames, together with a calculated CRC checksum for each frame. The receiver re-calculates the checksum of the received data and compares the result with the received checksum. Corrupted messages are rejected.

To ensure the integrity of a message and conceal a RelationKey, a CRC check mechanism is defined to check the Virtual Safety Check Message (VSCM) including a RelationKey, a sequence number, a scheduling number and the user data (see 7.1.3).

Table 9 shows the CRC calculation polynomial defined in the functional safety communication protocol.

Table 9 – CRC calculation polynomials

CRC mode code	CRC mode	Generator polynomial
1	CRC32	$g(x) = x^{32} + x^{30} + x^{29} + x^{28} + x^{26} + x^{20} + x^{19} + x^{17} + x^{16} + x^{15} + x^{11} + x^{10} + x^7 + x^6 + x^4 + x^2 + x + 1$ Bit-reversed to [0xBA0DC66B]

7.2.5 Scheduling number

A scheduling number is used to track the transmission sequence for all devices and all data transmissions in a communication macro-cycle in functional safety communication systems.

The scheduling number is included within the message and compared against the value of ConfiguredSchedulingNumber attribute of functional safety link object, both locally and at the receiving end.

A communication macro-cycle in the CP 14/1 control system consists of periodic packet transferring phase (T_p) and non-periodic packet transferring phase (T_n) (as shown in Figure 12).

During the periodic packet transferring phase, the process measure and/or the control data are transmitted in broadcast mode. That is, once the process data are broadcasted, all other devices in the same micro-segment can share them according to the application.

At the beginning of each communication macro-cycle, the value of the scheduling number shall be set to 1 by the first device which shall broadcast the periodic packet which contains the local process data and the scheduling number (as shown in Figure 11 above). Other devices shall obtain the current scheduling number used in this communication macro-cycle. Thereafter, the value of the scheduling number shall be increased by adding 1 at each next sending end.

At both, the sending end and the data receiving end, the current scheduling number shall be compared against the value of ConfiguredSchedulingNumber attribute of local functional safety link object. If they do not match, the CommunicationSchedulingError fault shall be recorded and reported.

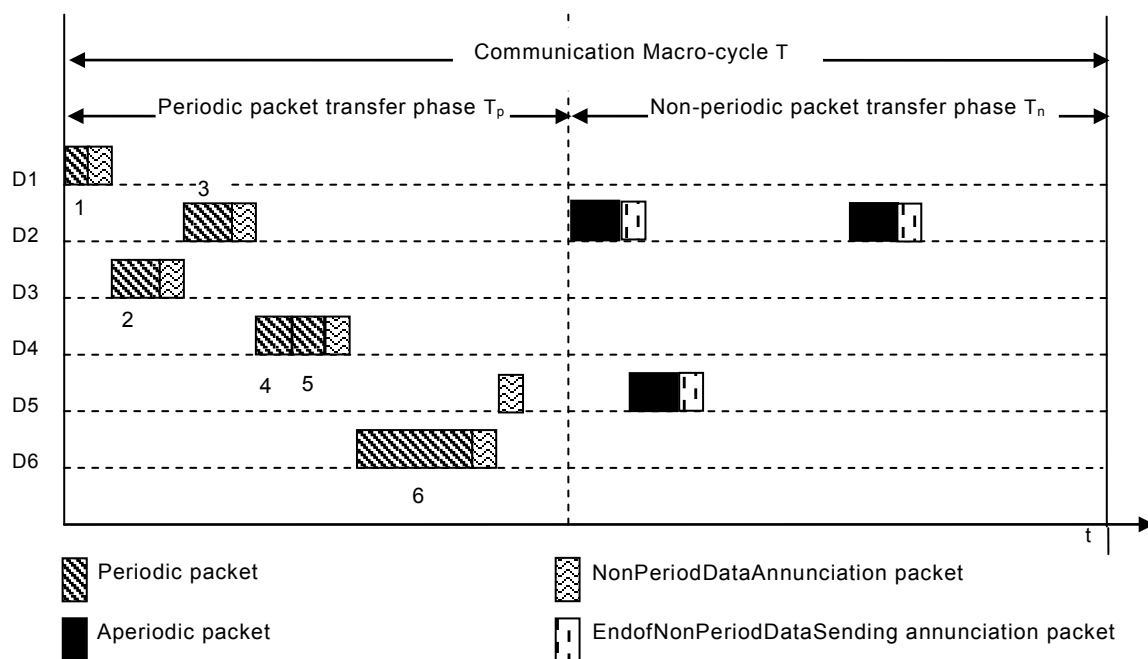


Figure 12 – Time-sharing communication scheduling

During the non-periodic packet transferring phase (T_n), the scheduling number is broadcasted with the EndofNonPeriodicDataSending service request message (as shown in Figure 13). Thereafter, the value of scheduling number shall be increased by adding 1 at each next sending end.

TYPE	IP Header	UDP Header	ENPMTA_TAG	PRI	Scheduling number
------	-----------	------------	------------	-----	-------------------

Figure 13 – Format of EndofNonPeriodicDataSending PDU

7.2.6 Time stamp

A time stamp is used to record the time when the user data layer sends a message in functional safety unconfirmed service to ensure the validity of time. Time stamp consists in the VSCM and FSPDU of sender. After checking the safety integrity and the sequence matching of FSPDU by receiver, the time validity is judged. If the difference between time stamp of FSPDU and current time of receiver exceeds the most time tolerance, it is concluded that the message has been delayed.

7.2.7 Time expectation

According to the system structure and the communication load, the time expectation is specified in worst cases, the communication is considered failure when this time is expired after serial tools sending confirmed service request and not receiving a response from a field device.

In a functional safety communication system, the value of the time expectation is the MaxResponseTime defined in the functional safety communication management object.

7.2.8 Time synchronization monitoring

In functional safety communication systems, a precisely synchronized time is required to ensure synchronous communications based on ISO/IEC 8802-3. The time synchronization mechanism based on IEC 61588 corrects the absolute time and resides in the black channel but it is monitored by the functional safety communication protocol.

The functional safety communication protocol shall check the time synchronization frequency and precision against the attribute value of TimeSynchronization object defined in IEC 61158-6-14. If the deviation between the host time and the local time is more than a permitted value, TargetTimeSyncClass of TimeSynchronization object, a preconfigured fault state action shall be triggered. If the duration between two continuous actions of the time synchronization is TimeRequestInterval, or the time synchronization request is timeout, the preconfigured fault state action shall be triggered and the communication fault state shall be reported also.

7.2.9 Communication scheduling precision monitoring

In each CP 14/1 device, the functional safety communication layer shall track the actual time offset, ActualDeliveryTimeOffset, from the beginning of communication macro-cycle for each message to be delivered to the physical link. The value of ActualDeliveryTimeOffset shall be compared against the value of SendTimeOffset attribute of the functional safety link object.

If the difference between them is more than the value of SchedulingPrecisionRequirement attribute of the functional safety link object, a preconfigured fault state action shall be triggered, and the communication fault state shall be reported.

7.3 Safety communication behaviour

7.3.1 Protocol state description of periodic data transmission

7.3.1.1 State description

Figure 14 shows the states of periodic data transmission and the terms are specified in Table 10.

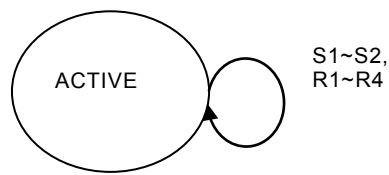


Figure 14 – State transfer figure of periodic data transmission

The states S1~S2 and R1~R4 are specified in 7.3.1.2.

Table 10 – Functional safety communication state description

State name	Description
ACTIVE	Functional safety entity in ACTIVE state is ready for transferring primitive to user layer and application entity, or receiving primitive from user layer and application entity.

7.3.1.2 State table

Table 11 describes the states and their transitions of the periodic data transmission.

Table 11 – States and transitions of periodic data transmission

#	Current state	Event or condition => Action	Next state
S1	ACTIVE	Unconfirmed_Service.req && LinkObjectType() = Non-Safety => Unconfirmed_Service.req { Data := User Data, Destination_ip := remote_ip_address, }	ACTIVE
S2	ACTIVE	Unconfirmed_Service.req && LinkObjectType() = Safety => Create safety date based on user data Unconfirmed_Service.req { Data := Safety Data, Destination_ip := remote_ip_address, }	ACTIVE
R1	ACTIVE	Unconfirmed_Service.ind &&LinkObjectType() = Non-Safety => Unconfirmed_Service.ind { Data := User Data, Destination_ip := remote_ip_address, }	ACTIVE
R2	ACTIVE	Unconfirmed_Service.ind && LinkObjectType() = Safety && CRCCheck() = FALSE => ErrorCountCheck(); EventNotifyManagement()	ACTIVE
R3	ACTIVE	Unconfirmed_Service.ind && LinkObjectType() = Safety && CRCCheck() = TRUE &&PeriodicSNCheck() = FALSE => ErrorCountCheck(LinkObjectID); EventNotifyManagement()	ACTIVE

#	Current state	Event or condition => Action	Next state
R4	ACTIVE	Unconfirmed_Service.ind && LinkObjectType() = Safety && CRCCheck() = TRUE && PeriodicSNCheck() = TRUE => Create User Data base on Safety Data; Unconfirmed_Service.ind { Data := User Data, Destination_ip := remote_ip_address, }	ACTIVE

7.3.2 Protocol state description of non-periodic data transmission

7.3.2.1 State description

Figure 15 shows the states of non-periodic data transmission and the terms are specified in Table 12.

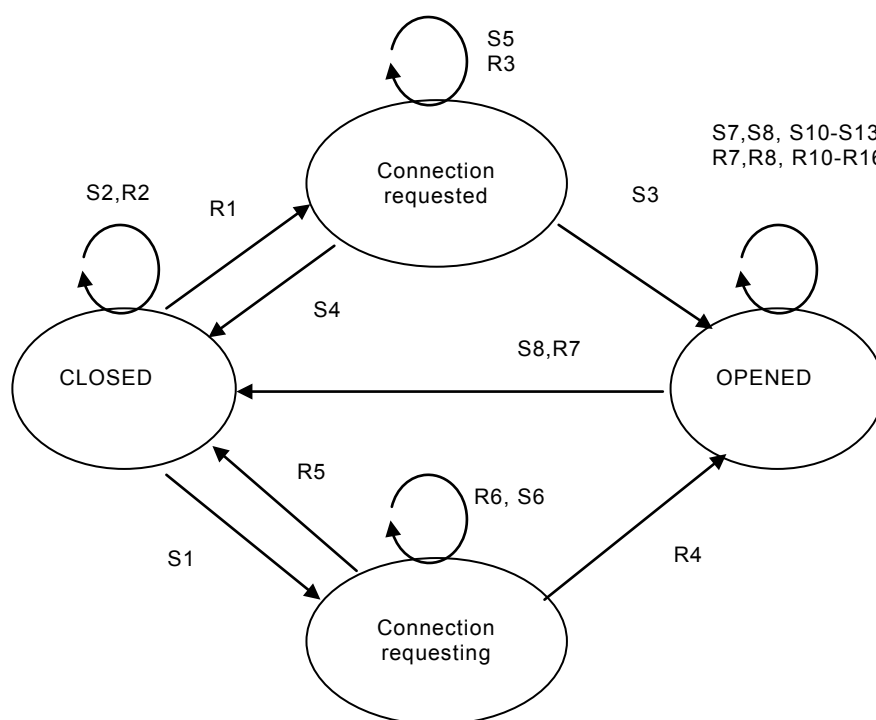


Figure 15 – Functional safety communication state transfer

The states R1~R16 and S1~S14 are specified in 7.3.2.2.

Table 12 – Functional safety communication states description

State name	Description
OPENED	Functional safety entity in OPENED state is ready for transferring primitive to user layer and application entity, or ready for receiving primitive from user layer and application entity
CLOSED	Functional safety entity in CLOSED state is ready for receiving the SafetyCommunicationOpen service
Connection requested	Functional safety entity in Connection requested state is ready for receiving message SafetyCommunicationOpen.rsp which is the response from the SafetyCommunicationOpen service
Connection requesting	Functional safety entity in Connection requesting state is ready for receiving message SafetyCommunicationClose.cnf which is the response from the SafetyCommunicationOpen service

7.3.2.2 State table

Table 13 describes the states and transitions of non-periodic data transmission.

Table 13 – States and transitions of non-periodic data transmission

#	Current state	Event or Condition => Action	Next state
S1	CLOSED	SafetyCommunicationOpen.req => SafetyCommunicationOpen.req { user_data := Data, Destination_ip := remote_ip_address, }	Connection Requesting
S2	CLOSED	Service except SafetyCommunicationOpen.req => Service.cnf(-) { user_data := Error-Status-Closed, Destination_ip := remote_ip_address, }	CLOSED
R1	CLOSED	SafetyCommunicationOpen.ind => SafetyCommunicationOpen.ind { user_data := Data, Destination_ip := remote_ip_address, }	Connection Requested
R2	CLOSED	Service except SafetyCommunicationOpen.ind => Service.rsp(-) { user_data := Error-Status-Closed, Destination_ip := remote_ip_address, }	CLOSED
S3	Connection Requested	SafetyCommunicationOpen.rsp(+) => SafetyCommunicationOpen.rsp(+) { user_data := Data, Destination_ip := remote_ip_address, }	OPENED

#	Current state	Event or Condition => Action	Next state
S4	Connection Requested	SafetyCommunicationOpen.rsp(-) => SafetyCommunicationOpen.rsp(-) { user_data := Data, Destination_ip := remote_ip_address, }	CLOSED
S5	Connection Requested	Service except SafetyCommunicationOpen.rsp => (No Action)	Connection Requested
R3	Connection Requested	Any Service => Service.rsp(-) { user_data := Error-Status-Requested, Destination_ip := remote_ip_address, }	Connection Requested
R4	Connection Requesting	SafetyCommunicationOpen.rsp(+) => SafetyCommunicationOpen.rsp(+) { user_data := Data, Destination_ip := remote_ip_address, }	OPENED
R5	Connection Requesting	SafetyCommunicationOpen.rsp(-) => SafetyCommunicationOpen.rsp(-) { user_data := Data, Destination_ip := remote_ip_address, }	CLOSED
R6	Connection Requesting	Service except SafetyCommunicationOpen.rsp => (No Action)	Connection Requesting
S6	Connection Requesting	Any service => Service.rsp(-) { user_data := Error-Status-Requesting, Destination_ip := remote_ip_address, }	Connection Requesting
S7	OPENED	SafetyCommunicationClose.req => SafetyCommunicationClose.req { user_data := Data, Destination_ip := remote_ip_address, }	OPENED
S8	OPENED	SafetyCommunicationOpen.req => SafetyCommunicationOpen.rsp(-) { user_data := Error-Status-Opened, Destination_ip := remote_ip_address, }	OPENED
R7	OPENED	SafetyCommunicationClose.ind => SafetyCommunicationClose.ind { user_data := Data, Destination_ip := remote_ip_address, }	OPENED

#	Current state	Event or Condition => Action	Next state
R8	OPENED	SafetyCommunicationOpen.ind => SafetyCommunicationOpen.rsp(-) { user_data := Error-Status-Opened, Destination_ip := remote_ip_address, }	OPENED
S9	OPENED	SafetyCommunicationClose.rsp(+) => SafetyCommunicationClose.rsp(+) { user_data := Data, Destination_ip := remote_ip_address, }	CLOSED
S10	OPENED	SafetyCommunicationClose.rsp(-) => SafetyCommunicationClosed.rsp(-) { user_data := Data, Destination_ip := remote_ip_address, }	OPENED
R9	OPENED	SafetyCommunicationClose.rsp(+) => SafetyCommunicationClose.rsp(+) { user_data := Data, Destination_ip := remote_ip_address, }	CLOSED
R10	OPENED	SafetyCommunicationClose.rsp(-) => SafetyCommunicationClose.rsp(-) { user_data := Data, Destination_ip := remote_ip_address,, }	OPENED
S11	OPENED	Confirmed service.req && ServiceType != SafetyCommunicationOpen && ServiceType != SafetyCommunicationClose => Create Safety Data based on user data Confirmed service.req { user_data := Safety Data, Destination_ip := remote_ip_address, } StartTimer(functional safety response time)	OPENED
R11	OPENED	Confirmed service.ind && ServiceType != SafetyCommunicationOpen && ServiceType != SafetyCommunicationClose && CRCCheck() = FALSE => Confirmed Service.rsp(-) { ErrorClass = Communication Error ErrorCode = CRC Error }	OPENED

#	Current state	Event or Condition => Action	Next state
R12	OPEN	Confirmed service.ind && ServiceType != SafetyCommunicationOpen && ServiceType != SafetyCommunicationClose && CRCCheck() = TRUE && Non-periodicSNCheck() = FALSE => Confirmed Service.rsp(-) { ErrorClass = Communication Error ErrorCode = Sequence Number Error }	OPENED
R13	OPEN	Confirmed service.ind && ServiceType != SafetyCommunicationOpen && ServiceType != SafetyCommunicationClose && CRCCheck() = TRUE && Non-periodicSNCheck() = TRUE => Create User Data based on Safety Data Confirmed service.ind { user_data := User Data, Destination_ip := remote_ip_address, }	OPENED
S12	OPENED	Confirmed service.rsq && ServiceType != SafetyCommunicationOpen && ServiceType != SafetyCommunicationClose => Confirmed service.rsq { user_data := Data, Destination_ip := remote_ip_address, }	OPENED
R14	OPENED	Confirmed service.cnf && ServiceType != SafetyCommunicationOpen && ServiceType != SafetyCommunicationClose && CRCCheck() = FALSE => Confirmed Service.rsp(-) { ErrorClass = Communication Error ErrorCode = CRC Error }	OPENED
R15	OPENED	Confirmed service.cnf && ServiceType != SafetyCommunicationOpen && ServiceType != SafetyCommunicationClose && CRCCheck() = TRUE && Non-periodicSNCheck() = FALSE => Confirmed Service.rsp(-) { ErrorClass = Communication Error ErrorCode = Sequence Number Error }	OPENED
R16	OPENED	Confirmed service.cnf && ServiceType != SafetyCommunicationOpen && ServiceType != SafetyCommunicationClose && CRCCheck() = TRUE && Non-periodicSNCheck() = TRUE => Create User Data based on Safety Confirmed service.cnf { user_data := User Data, Destination_ip := remote_ip_address, }	OPENED