IEC 61784-3-14

Edition 1.0 2010-06

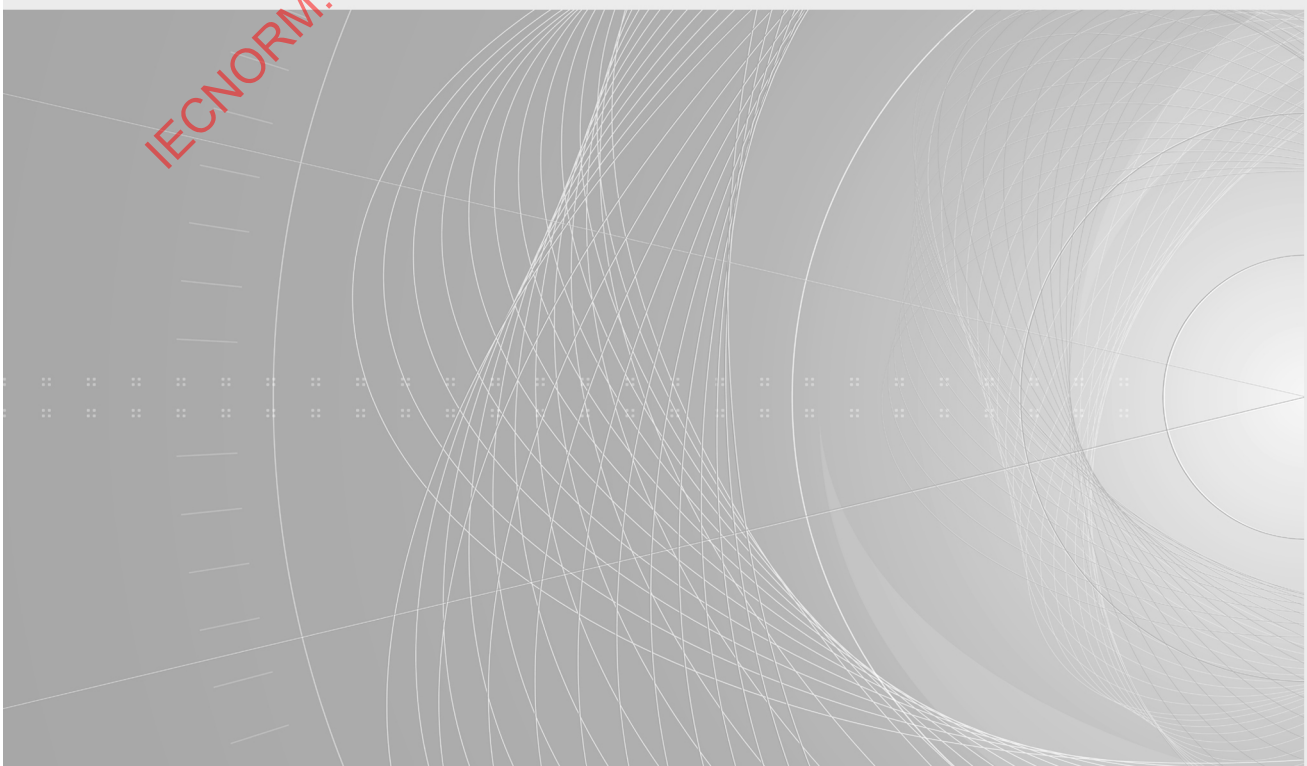
INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

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



IEC 61784-3-14:2010

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It also gives information on projects, replaced and withdrawn publications.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

colour inside

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 XB
CODE PRIX

ICS 25.040.40, 35.100.05

ISBN 978-2-88912-946-1

CONTENTS

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.

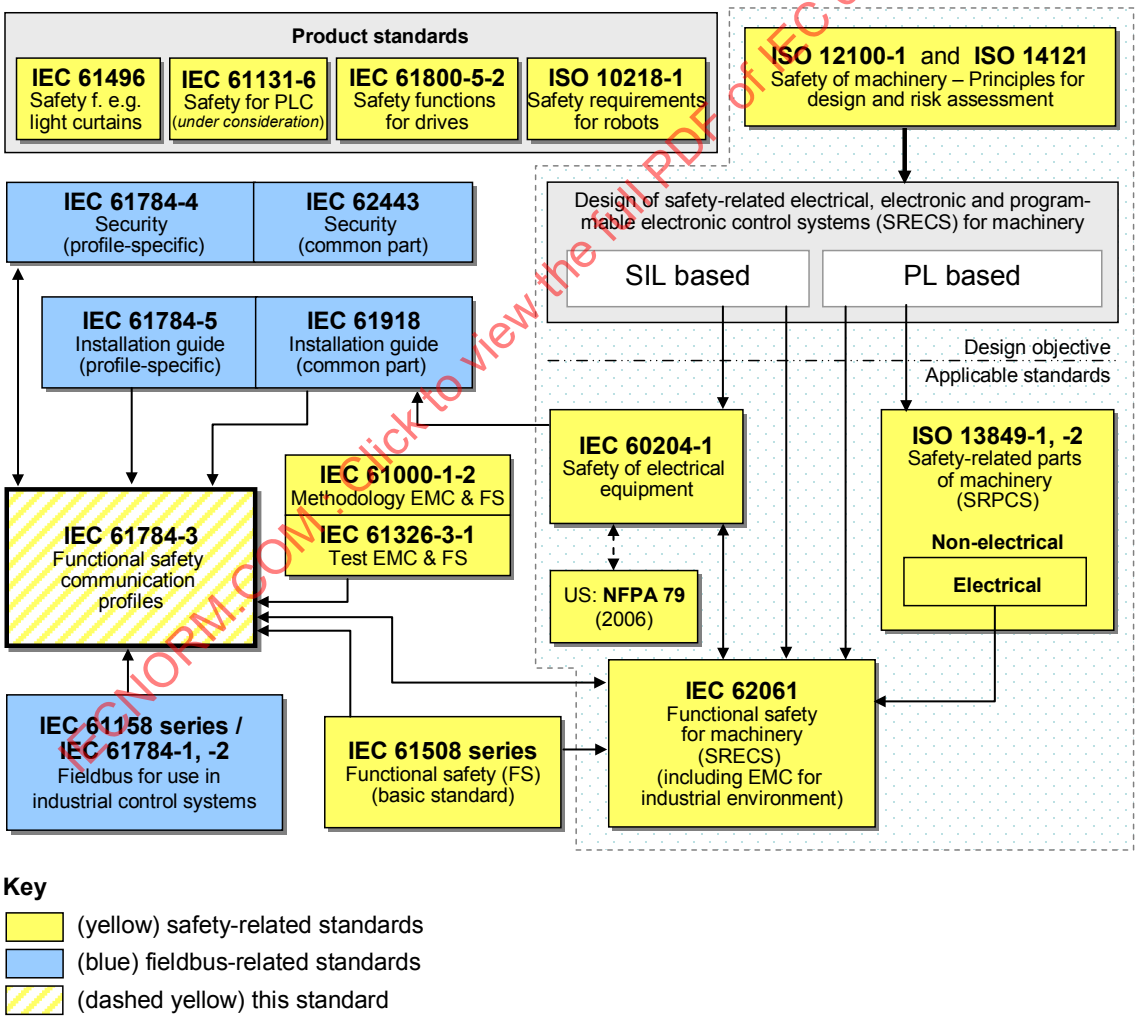
0 Introduction

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.

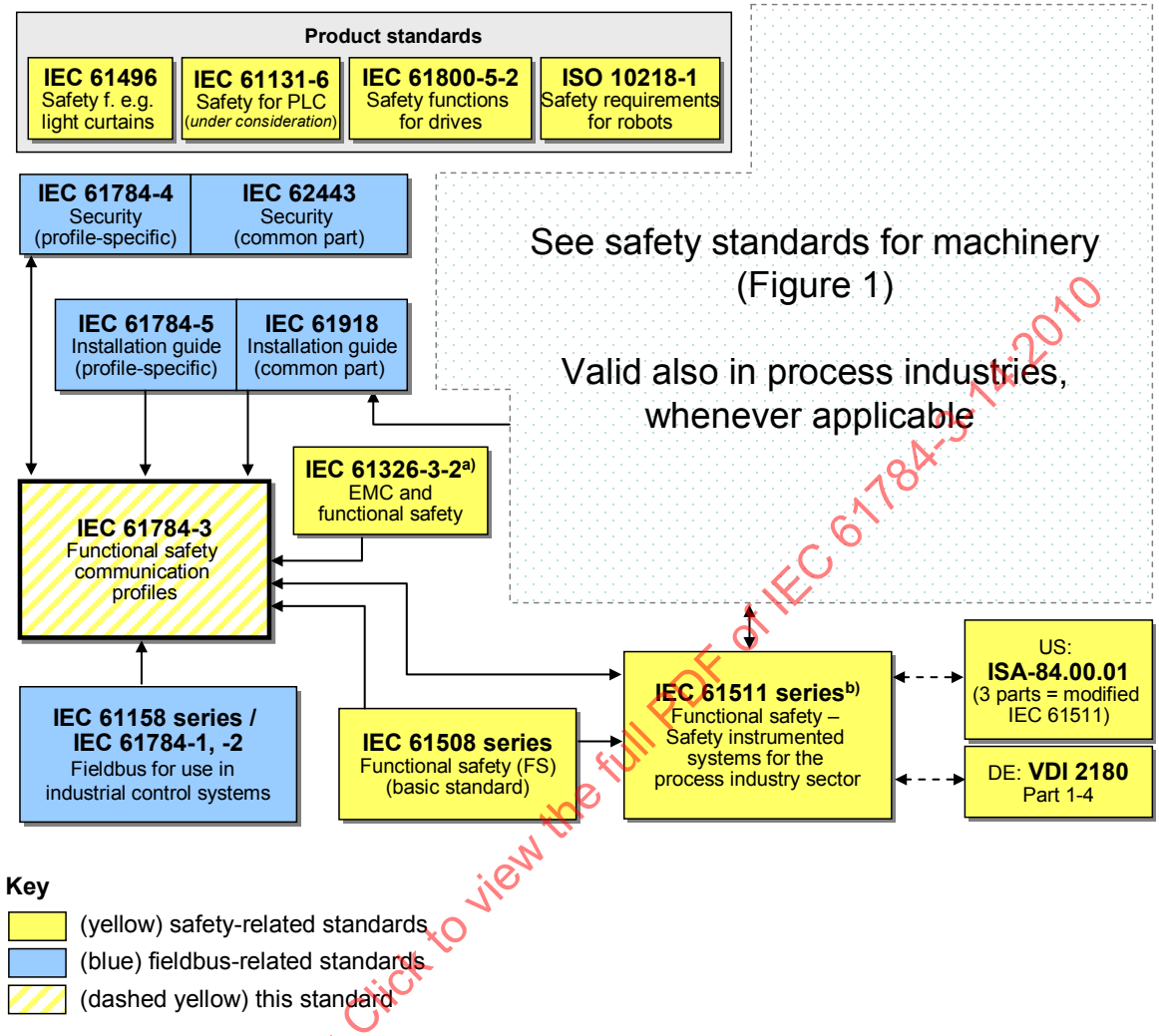
Figure 1 shows the relationships between this standard and relevant safety and fieldbus standards in a machinery environment.



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.



[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 part[1] 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 series[2] 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 61784-3:2010[3], *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 61508-4:2010[5]], [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 IEV 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 (t1,t2)

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 61508-5:2010[6].

[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 61508-1:2010[7].

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®.

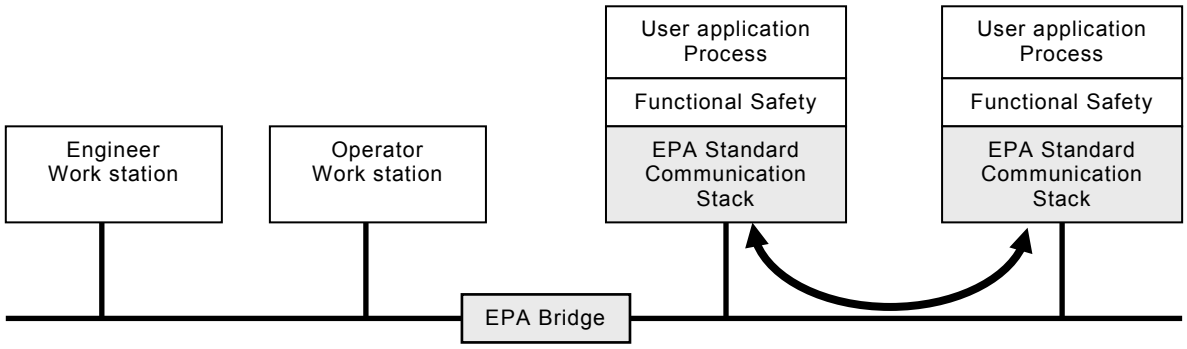


Figure 3 – Safety communication architecture

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.

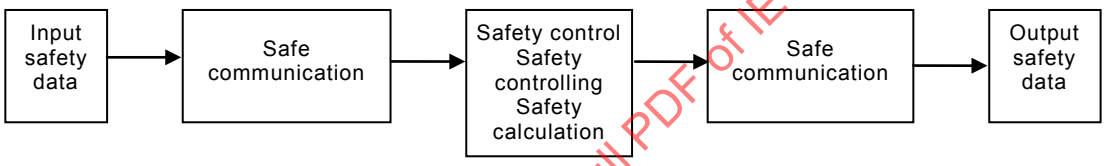


Figure 4 – Safety function processing

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

a) The input function block reads the physical input signals from sensors and transfers it to the safety communication stack;

b) The safety communication stack performs the safety-relevant communication services of the input function block resident field device (e.g. EPA safe-relevant transmitter);

c) 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;

d) 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);

e) 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;

f) 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

	Safety measures							
Communication errors	**Sequence number (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.

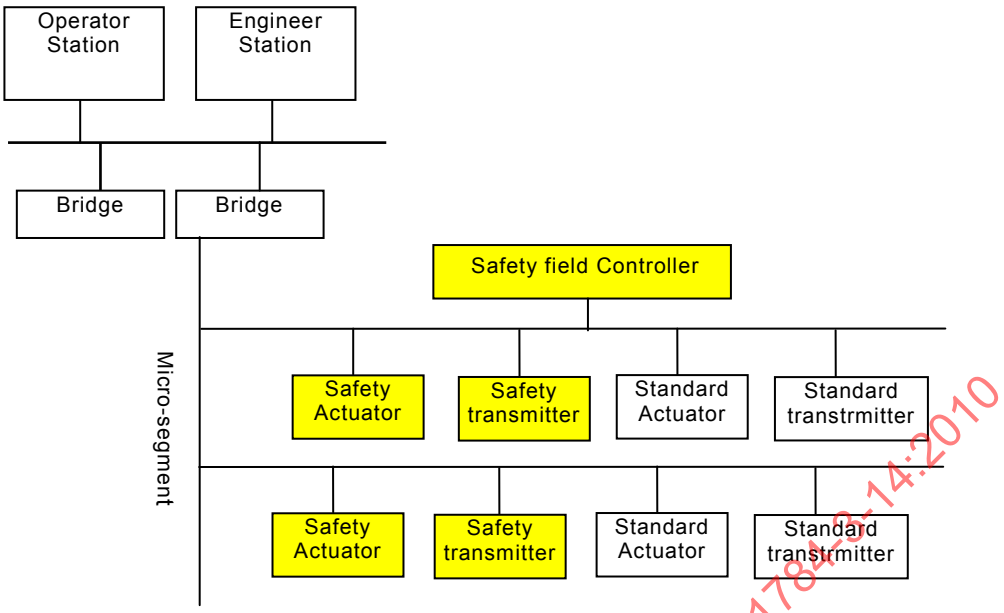


Figure 5 – Standard communication and safety communication

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.

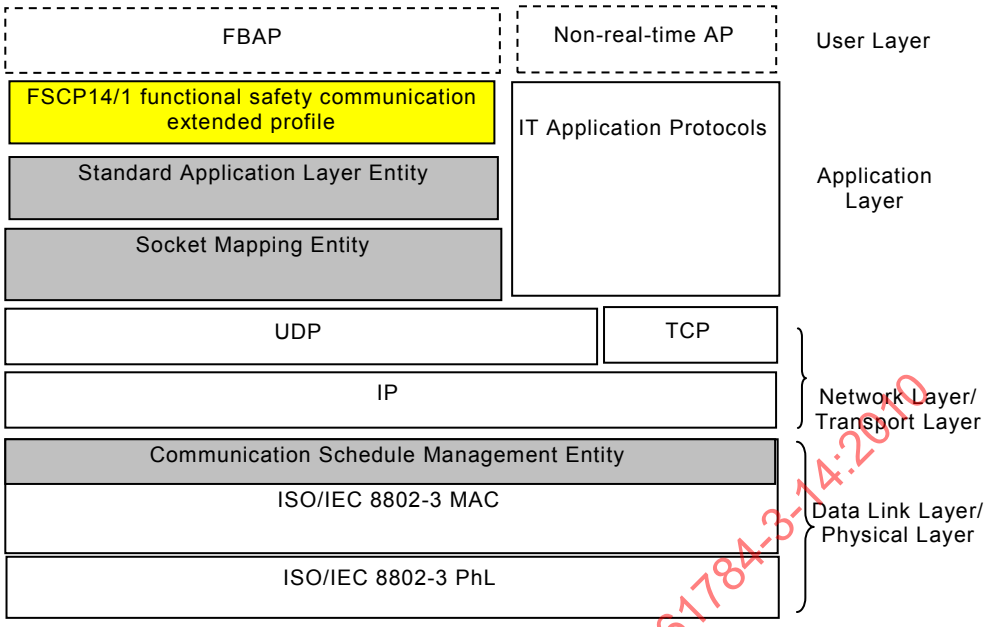


Figure 6 – CP 14/1 protocol hierarchy

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 UPD/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.

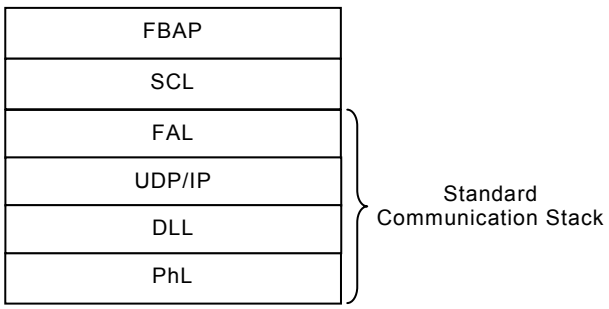


Figure 7 – Relationship between the SCL and the other layers of CP 14/1

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 invocated number of this service. Each time this service is invocated, 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 invocated number of this service. Each time this service is invocated, 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).

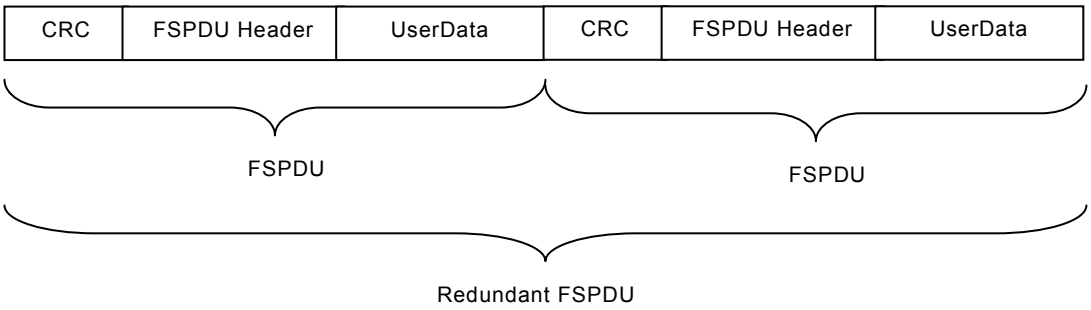


Figure 9 – Structure of Functional Safety PDU (FSPDU)

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.

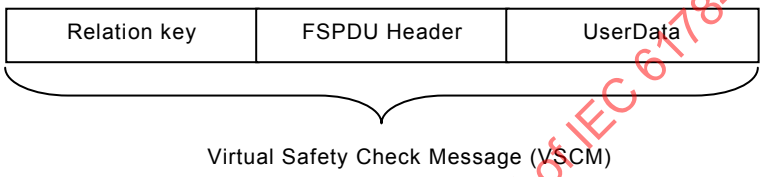


Figure 10 – Structure of Virtual Safety Check Message (VSCM)

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.

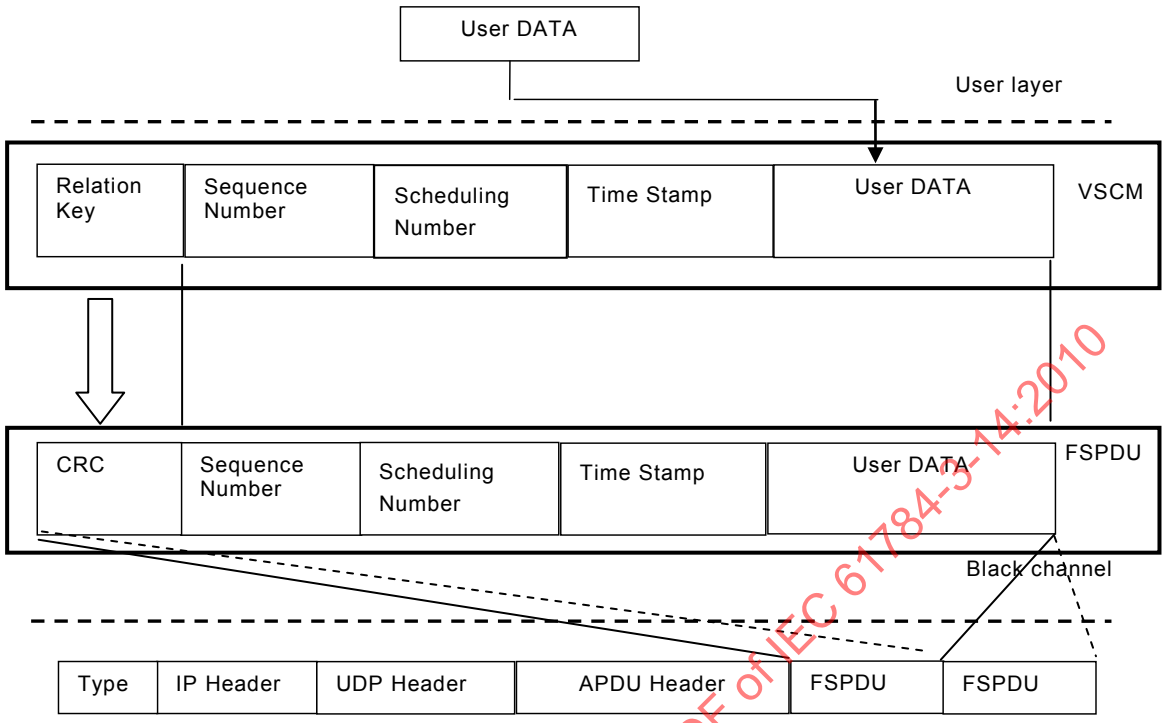


Figure 11 – FSPDU mapping

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 (Tp) and non-periodic packet transferring phase (Tn) (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.

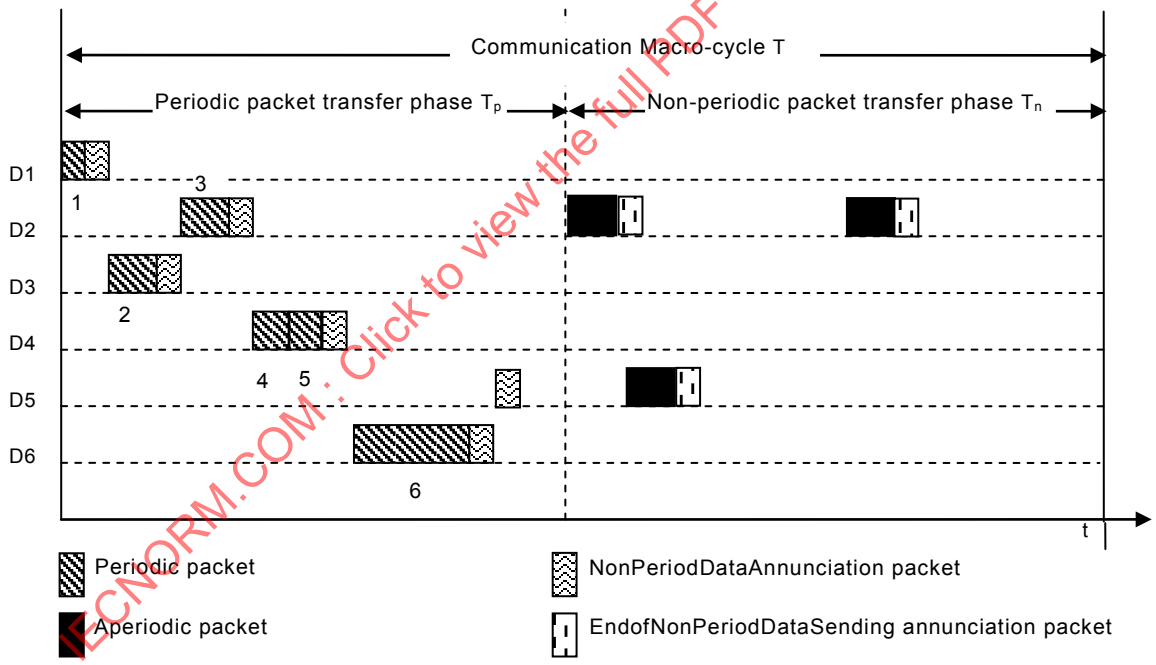


Figure 12 – Time-sharing communication scheduling

During the non-periodic packet transferring phase (Tn), 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.

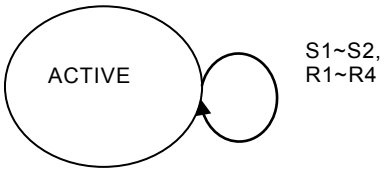


Figure 14 – State transfer figure of periodic data transmission

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.

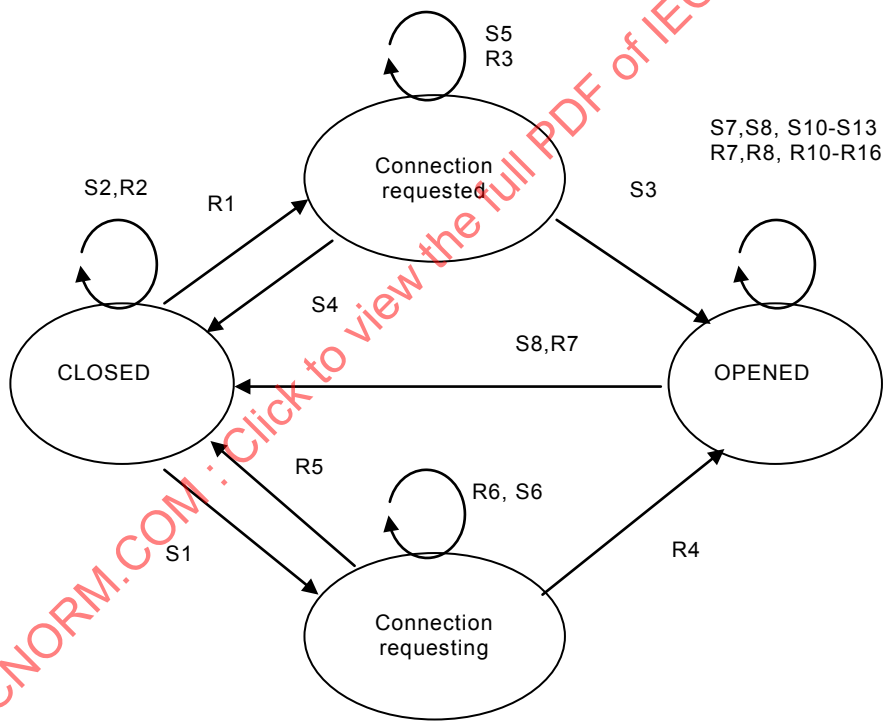


Figure 15 – Functional safety communication state transfer

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 SafetyConmmunicationOpen.rsp which is the response from the SafetyCommunicationOpen service
Connection requesting	Functional safety entity in Connection requesting state is ready for receiving message SafetyConmmunicationClose.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

#	Current state	Event or Condition => Action	Next state

S13	OPENED	Time out of functional safety response time
		=>
		Confirmed service.cnf(-)
		{
		user_data := ErrorCode,
		Destination_ip : = remote_ip_address,
		}
			OPENED

S14	OPENED	Time out of Max Service Interval => (No Action)	CLOSED

7.3.3 Protocol state description of alert report for communication fault

7.3.3.1 State description

Figure 16 shows the states of the communication alert report and the terms are specified in Table 14.

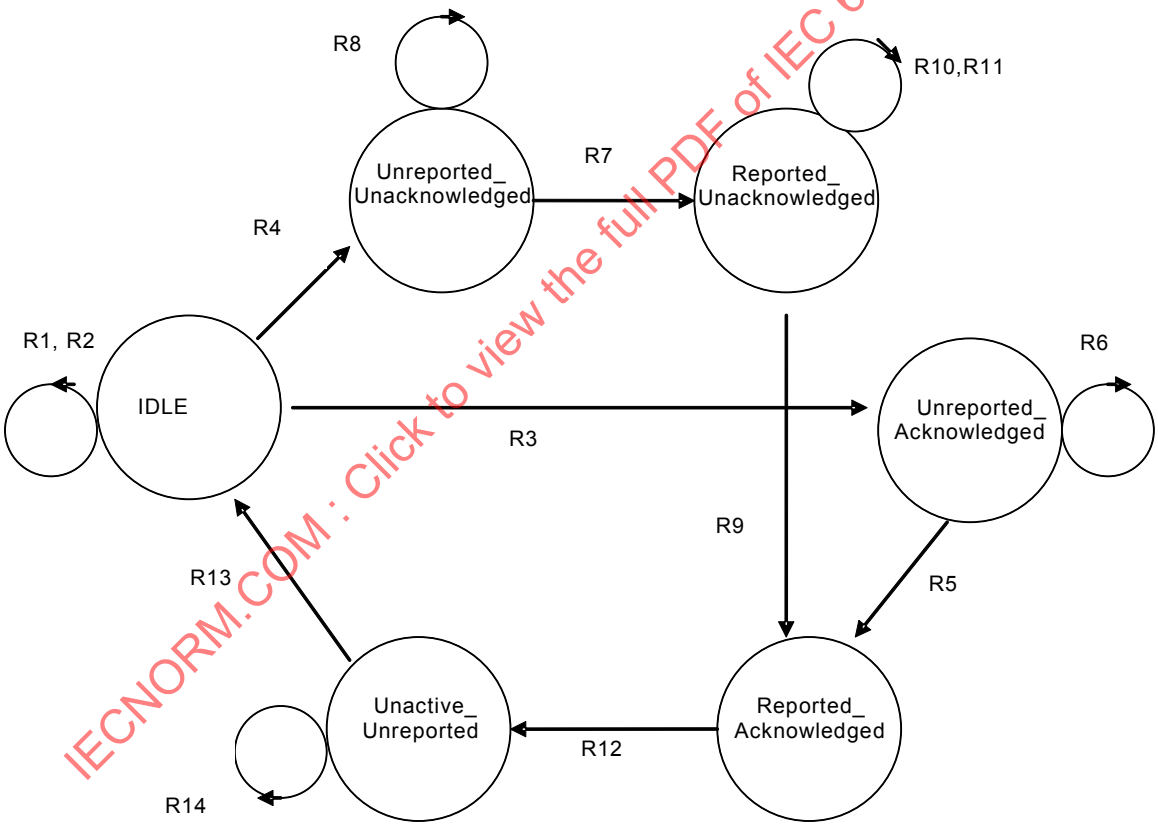


Figure 16 – Communication alert report state transfer figure

The states R1~R14 are specified in 7.3.3.2.

Table 14 – Communication alert state description

State name	Description
IDLE	Device in IDLE state has no communication fault
Unreported_ Unacknowledged	Device in Unreported_Unacked state has communication fault, and sends the EventNotify service to special host determined by RemoteIpAddress of functional safety link object which ServiceOperation is 0x0f and service role is SEND, but neither received AcknowledgeEventNotify service request from special host nor received write service for special host
Unreported_ Acknowledged	Device in Unreported_Unacked state has communication fault, and sends the EventNotify service to special host determined by RemoteIpAddress of functional safety link object which ServiceOperation is 0x0f and service role is SEND, but not received AcknowledgeEventNotify service from special host and it does not need the write service for special host according to the configuration (corresponding FaultAcknowledgeConfiguration is set)
Reported_ Unacknowledged	Device in Reported_Unacked state has communication fault, and received the AcknowledgeEventNotify service from special host determined by RemoteIpAddress of functional safety link object which ServiceOperation is 0x0f and service role is SEND, but not received write service for special host
Reported_ Acknowledged	Device in Reported_Acked state has communication fault, and received the write service from special host determined by RemoteIpAddress of functional safety link object which ServiceOperation is 0x0f and service role is SEND
Unactive_ Unreported	Device in Unactive_Unreported state reset the communication fault, and send the EventNotify service to special host determined by RemoteIpAddress of functional safety link object which ServiceOperation is 0x0f and service role is SEND, but has not received AcknowledgeEventNotify service from special host

7.3.3.2 State table

Table 15 describes the communication alert states and transitions.

Table 15 – Communication alert states and transitions

#	Current state	Event or Condition => Action	Next State
R1	IDLE	No communication fault in device => (No action);	IDLE
R2	IDLE	Communication fault in device && corresponding FaultReportConfiguration is set (not report) => (No action);	IDLE

R3	IDLE	Communication fault in device
		&& corresponding FaultReportConfiguration is not set (report)
		&& corresponding FaultAcknowledgeConfiguration is set (not ack)
		=>
		EventNotify.req
		{
		Failure code of communication failure
		}
		Start Timer of response time;
			Unreported_ Acknowledged

R4	IDLE	Communication failure in device
		&& corresponding FaultReportConfiguration is not set (report)
		&& corresponding FaultAcknowledgeConfiguration is not set (ack)
		=>
		EventNotify.req
		{
		Failure code of communication failure
		}
		Start Timer of response time;
			Unreported_ UnAcknowledged

R5	Unreported_ Acknowledged	AcknowlegeEventNotification.req => AcknowlegeEventNotification.rsp Stop Timer of response time;	Reported_ Acknowledged

#	Current state	Event or Condition => Action	Next State

R6	Unreported_
	Acknowledged
		TimerOut of expected response time
		&&(No service || Receive service not AcknowlegeEventNotification.req)
		=>
		EventNotify.req
		{
		Failure code of communication failure
		}
		Start Timer of response time;
			Unreported_
			Acknowledged

R7	Unreported_
	Unacknowledged
		AcknowlegeEventNotification.req
		=>
		AcknowlegeEventNotification.rsp
		{
		}
		Stop Timer of response time;
			Reported_
			Unacknowledged

R8	Unreported_
	Unacknowledged
		TimerOut of expected response time
		&& Relative bit of LinkageFault attribute is set
		&&(No service || Receive service not AcknowlegeEventNotification.req)
		=>
		EventNotify.req
		{
		Failure code of communication failure
		}
		Start Timer of response time;
			Unreported_
			Unacknowledged

R9	Reported_
	Unacknowledged
		Write.ind
		&& Write object is acknowledge state
		&& Relative bit of acknowledge state change to unset
		=>
		Reset the relative bit of acknowledge attribute
		Write.rsp
		{
		}
			Reported_
			Acknowledged

R10	Reported_ Unacknowledged	Service except Write.ind => (No action)	Reported_ Unacknowledged
R11	Reported_ Unacknowledged	Write.ind && (Write object is not acknowledge state || (Write object is acknowledge state && Not relative bit of acknowledge state change to unset) => (No action)	Reported_ Unacknowledged

R12	Reported_
	Acknowledged
		Relative communication fault recover
		=>
		Rest the relative bit of linkage failure attribute.
		EventNotify.req()
		{
		Failure recover information
		}
		Start timer of response time
			Unactive_
			Unreported

R13	Unactive_
	Unreported
		AcknowlegeEventNotification.req
		&& Relative bit of LinkageFault attribute is unset
		=>
		AcknowlegeEventNotification.rsp
		{
		}
		Stop timer of response time
			IDLE

#	Current state	Event or Condition => Action	Next State

R14	Unactive_
	Unreported
		TimeOut of response time
		&& Relative bit of LinkageFault attribute is unset
		&&(No service || Receive service not AcknowlegeEventNotification.req)
		=>|
		EventNotify.req()
		{
		Failure reset information
		}
		Start timer of response time
			Unactive_
			Unreported

7.3.4 Function description

7.3.4.1 LinkObjectType function

Table 16 describes the LinkObjectType function.

Table 16 – LinkObjectType function description

Name	LinkObjectType	Use	Functional safety
Input		Output	
Link Object ID		Non-Safety or Safety	
function			
Check whether there is a link object whose attributes and RemoteIPAddress are equal to LinkType. If it exists, return Safety; otherwise return Non-Safety.			

7.3.4.2 CRCCheck function

Table 17 describes the CRCCheck function.

Table 17 – CRCCheck function description

Name	CRCCheck	Use	Functional safety
Input		Output	
Link Object ID ; FSPDU		TRUE or FALSE	
Function			
Checks whether the communication error of Data bit error occurs during transferring in black channel. (1)Makes up VSCM from RelationKey of Link Object and user data, sequence number, schedule number, time stamp (2)Checks the VSCM by CRC, which builds Check Code (3)If the built Check Code and received Check Code are equal, it shall be concluded that the message has not been damaged, and return TRUE; otherwise return FALSE.			

7.3.4.3 CrossCheck function

Table 18 describes the CrossCheck function.

Table 18 – CrossCheck function description

Name	CRCCheck	Use	Functional safety
Input		Output	
Link Object ID 、FSPDU		TRUE or FALSE	
Function			
Checks whether the communication error of Data bit error occurs during transferring in black channel. If the redundant safety data copies are equal, it shall be concluded that the message has not been damaged, and return TRUE; otherwise return FALSE.			

7.3.4.4 TimeDelayCheck function

Table 19 describes the TimeDelayCheck function.

Table 19 – TimeDelayCheck function description

Name	TimeDelayCheck	Use	Functional safety
Input		Output	
Link Object ID, FSPDU		TRUE or FALSE	
Function			
Checks if the communication error of unacceptable delay has occurred during transferring in black channel.			

7.3.4.5 PeriodicSNCheck function

Table 20 describes the PeriodicSNCheck function.

Table 20 – PeriodUncomfrimedSNCheck function description

Name	PeriodUncomfrimedSNCheck	Use	Functional safety
Input		Output	
Link Object ID, FSPDU		TRUE or FALSE	
Function			
In case of periodic data transmission, checks if the communication error such as incorrect sequence loss and unintended repetition has occurred during transferring in black channel.			

7.3.4.6 Non-periodicSNCheck function

Table 21 describes the non-periodicSNCheck function.

Table 21 – Non-periodicSNCheck function description

Name	Non-periodicSNCheck	Use	Funtional safety
Input		Output	
Link Object ID , FSPDU		TRUE or FALSE	
Function			
In case of non-periodic data transmission, checks if the communication error such as incorrect sequence loss and unintended repetition has occurred during transferring in black channel.			

7.4 Code

7.4.1 Object code

7.4.1.1 Functional safety communication management object

The encoding of the functional safety communication management object is shown in Table 22.

Table 22 – Functional safety communication management object encoding

Index	Parameter name	Access right	Data type	Octet offset	Octet length	Description
1	ObjectID	Read only	Unsigned16	0	2	The index of functional safety communication management object in MIB
2	Max Nonperiodic Channel Number	Read only	Unsigned8	2	1	The max number of non-periodic channel
3	Free Nonperiodic Channel Number	Read only	Unsigned8	3	1	The number of current free non-periodic channel
4	MaxResponseTime	Read/Write	TimeDifference	4	4	Maximum response time from sending the service request to receiving the service response
5	Service option	Read/Write	Unsigned16	8	2	The kinds of services which the functional safety layer supports. It may be set by 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

7.4.1.2 Functional safety link object

The encoding of the functional safety link object is shown in Table 23.

Table 23 – Functional safety link object encoding

Index	Parameter name	Access right	Data type	Octet offset	Octet length	Description
1	ObjectID	Read only	Unsigned16	0	2	Functional safety link object in MIB
2	LocalAppID	Read/Write	Unsigned16	2	2	Local function block application ID
3	LocalObjectID	Read/Write	Unsigned16	4	2	Local object ID
4	RemoteAppID	Read/Write	Unsigned16	6	2	Remote function block application ID
5	RemoteObjectID	Read/Write	Unsigned16	8	2	Remote object ID
6	ServiceOperation	Read/Write	Unsigned8	10	1	Service operation implicated by link object

Index	Parameter name	Access right	Data type	Octet offset	Octet length	Description
7	ServiceRole	Read/Write	Unsigned8	11	1	Service role of local AREP
8	RemoteIPAddress	Read/Write	Unsigned32	12	4	IP address of remote device
9	SendTimeOffset	Read/Write	Time Difference	16	4	Offset of sending relative to the beginning of macro-cycle
10	Configured Scheduling Number	Read/Write	Unsigned16	20	2	Sequence number in one macro-cycle for local device to send the data related to this functional safety link object
11	Scheduling Precision Requirement	Read/Write	Unsigned8	22	2	Expected data sending time precision for local device
12	RelationKey	SafetyCommunication-Open / SafetyCommunication-Close	Unsigned32	24	4	Current RelationKey value for the Link Object
13	LinkageFault	Read/Write	Unsigned16	28	2	Records 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
14	FaultReport Configuration	Read/Write	Unsigned8	30	1	Determines 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
15	FaultAcknowledge Configuration	Read/Write	Unsigned8	31	1	Determines 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

7.4.1.3 Functional safety communication alert object

The encoding of the functional safety communication alert object is shown in Table 24.

Table 24 – Functional safety communication alert object encoding

Index	Parameter name	Access right	Data type	Octet offset	Octet length	Description
1	ObjectID	Read only	Unsigned16	0	2	The index of functional safety communication alert object in system management base
2	Total Fault Counter	Read only	Unsigned16	2	2	The counter for all communication faults to be detected
3	Local Fault Recoders	Read only	Unsigned16	4	2	The recorders for each communication faults to be detected
4	CRC Error Counter	Read only	Unsigned16	6	2	The recorders for CRC Error to be detected
5	Sequence Error Counter	Read only	Unsigned16	8	2	The recorders for Sequence Error to be detected
6	Time Delay Counter	Read only	Unsigned16	10	2	The recorders for Time Delay to be detected
7	Time Synchronize Error Counter	Read only	Unsigned16	12	2	The recorders for Time Synchronize Error to be detected
8	Communication Scheduling Error Counter	Read only	Unsigned16	14	2	The recorders for Communication Scheduling Error to be detected

7.4.2 Service code

7.4.2.1 Extended syntax description

7.4.2.1.1 Confirmed service request

```
Confirmed- Request : : = CHOICE {
        EM_GetDeviceAttribute          [0]  IMPLICIT EM_GetDeviceAttribute-RequestPDU,
        EM_SetDeviceAttribute          [1]  IMPLICIT EM_SetDeviceAttribute-RequestPDU,
        EM_ClearDeviceAttribute        [2]  IMPLICIT EM_ClearDeviceAttribute-RequestPDU,
        DomainDownload                 [3]  IMPLICIT DomainDownload-RequestPDU,
        DomainUpload                   [4]  IMPLICIT DomainUpload-RequestPDU,
        AcknowledgeEventNotification[5]  IMPLICIT AcknowledgeEventNotifi-RequestPDU,
        AlterEventConditionMonitor     [6]  IMPLICIT AlterEventConditionMon-RequestPDU,
        Read                           [7]  IMPLICIT Read-RequestPDU,
        Write                          [8]  IMPLICIT Write-RequestPDU,
        SafetyCommunicationOpen        [9]  IMPLICIT SafetyCommunicationOpen-RequestPDU
        SafetyCommunicationClose       [10] IMPLICIT SafetyCommunicationClose-RequestPDU
}
```

7.4.2.1.2 Confirmed service response

```
Confirmed- Response : : = CHOICE {
        EM_GetDeviceAttribute          [0]  IMPLICIT EM_GetDeviceAttribute-ResponsePDU,
        EM_SetDeviceAttribute          [1]  IMPLICIT EM_SetDeviceAttribute-ResponsePDU,
```

```
        EM_ClearDeviceAttribute      [2]  IMPLICIT EM_ClearDeviceAttribute-ResponsePDU,
        DomainDownload               [3]  IMPLICIT DomainDownload-ResponsePDU,
        DomainUpload                 [4]  IMPLICIT DomainUpload-ResponsePDU,
        AcknowledgeEventNotification[5]  IMPLICIT AcknowledgeEventNotifi-ResponsePDU,
        AlterEventConditionMonitor   [6]  IMPLICIT AlterEventConditionMon-ResponsePDU,
        Read                         [7]  IMPLICIT  Read-ResponsePDU,
        Write                        [8]  IMPLICIT  Write-ResponsePDU,
        SafetyCommunicationOpen      [9]  IMPLICIT SafetyCommunicationOpen-ResponsePDU
        SafetyCommunicationClose     [10] IMPLICIT SafetyCommunicationClose-ResponsePDU
}
```

7.4.2.1.3 Unconfirmed service request

```
Unconfirmed-Request: : = CHOICE {
        EM_FindTagQuery              [0]  IMPLICIT  EM_FindTagQuery-RequestPDU,
        EM_FindTagReply              [1]  IMPLICIT  EM_FindTagReply-RequestPDU,
        EM_DeviceAnnunciation        [2]  IMPLICIT  EM_DeviceAnnunciation-RequestPDU,
        EventNotification            [3]  IMPLICIT  EventNotification-RequestPDU,
        Distribute                   [4]  IMPLICIT  Distribute-RequestPDU,
}
```

7.4.2.1.4 APDU header format

```
PDUHeader : : = SEQUENCE {
        ServiceID                    [0]  IMPLICIT  Unsigned8,
        Safety CommunicationType     [1]  IMPLICIT  Unsigned8,
        Reserved                     [2]  IMPLICIT  Unsigned16,
        Length                       [3]  IMPLICIT  Unsigned16,
        MessageID                    [4]  IMPLICIT  Unsigned16
}
```

7.4.2.1.5 Function safety extended service

7.4.2.1.5.1 SafetyCommunicationOpen

```
SafetyCommunicationOpen -RequestPDU : : = SEQUENCE {
        SourceAppID                  [0]  IMPLICIT Unsigned16
        SourceIPAddress              [1]  IMPLICIT  Unsigned32,
        DestinationIPAddress         [2]  IMPLICIT  Unsigned32,
        RelationKey                  [3]  IMPLICIT  Unsigned32
        CommunicationType            [4]  IMPLICIT Unsigned16
        LinkObjectType
            LinkObjectID             [5]  IMPLICIT  Unsigned16
        LinkObjectType
            AccessRight              [5]  IMPLICIT  Unsigned32
```

```
}

SafetyCommunicationOpen -ResponsePDU : : = CHOICE {
        SafetyCommunicationOpen -PositiveResponsePDU,
        SafetyCommunicationOpen -NegativeResponsePDU
}

SafetyCommunicationOpen -PositiveResponsePDU : : = SEQUENCE {
        DestinationAppID            [0]  IMPLICIT  Unsigned16,
}

SafetyCommunicationOpen -NegativeResponsePDU : : = SEQUENCE {
        DestinationAppID            [0]  IMPLICIT  Unsigned16,
        Reserved                    [1]  IMPLICIT  OctetString,
        ErrorType                   [2]  IMPLICIT  ErrorType
}
```

7.4.2.1.5.2 SafetyCommunicationClose

```
SafetyCommunicationClose -RequestPDU : : = SEQUENCE {
        SourceAppID                 [0]  IMPLICIT Unsigned16
        SourceIPAddress             [1]  IMPLICIT  Unsigned32,
        DestinationIPAddress        [2]  IMPLICIT  Unsigned32,
        LinkObjectID                [3]  IMPLICIT  Unsigned16,
}

SafetyCommunicationClose -ResponsePDU : : = CHOICE {
        SafetyCommunicationClose -PositiveResponsePDU,
        SafetyCommunicationClose -NegativeResponsePDU
}

SafetyCommunicationClose -PositiveResponsePDU : : = SEQUENCE {
        DestinationAppID            [0]  IMPLICIT  Unsigned16,
}

SafetyCommunicationClose -NegativeResponsePDU : : = SEQUENCE {
        DestinationAppID            [0]  IMPLICIT  Unsigned16,
        Reserved                    [1]  IMPLICIT  OctetString,
        ErrorType                   [2]  IMPLICIT  ErrorType
}
```

7.4.2.2 Encoding of additional services for safety communication

7.4.2.2.1 SafetyCommunicationOpen service

7.4.2.2.1.1 SafetyCommunicationOpen service request

The SafetyCommunicationOpen service is used to initialize the link relationship of a functional safety communication. The SafetyCommunicationOpen request service parameters are specified in Table 25.

Table 25 – Encoding of SafetyCommunicationOpen request parameters

Index	Parameter name	Data type	Octet offset	Octet length	Description
1	SourceAppID	Unsigned16	0	2	Identifier of source application
2	SourceIPAddress	Unsigned32	2	4	IP address of source
3	DestinationIPAddress	Unsigned32	6	4	IP address of destination
4	RelationKey	Unsigned32	10	4	RelationKey for communication channel
5	CommunicationType	Unsigned16	14	2	The type of communication. 0——Link Object type; 1——Communication Object type; Other——Reserved.
6	LinkObjectID	Unsigned16	16	2	The ID of Link Object which shall be configured to be functional safety communication
7	AccessRight	Unsigned32	18	4	AccessRight for communication channel

7.4.2.2.1.2 SafetyCommunicationOpen service positive response parameters

If a device receives SafetyCommunicationOpen request service and operates correctly, it shall return SafetyCommunicationOpen service positive response. SafetyCommunicationOpen service positive response parameters are specified in Table 26.

Table 26 – SafetyCommunicationOpen positive response parameters

Index	Parameter name	Data type	Octet offset	Octet length	Description
1	DestinationAppID	Unsigned16	0	2	Application ID of Destination

7.4.2.2.1.3 SafetyCommunicationOpen negative response parameters

The SafetyCommunicationOpen service negative response returns a SafetyCommunicationOpen request service's error reason. The SafetyCommunicationOpen service negative response parameters are specified in Table 27.

Table 27 – SafetyCommunicationOpen negative response parameters

Index	Parameter name	Data type	Octet offset	Octet length	Description
1	DestinationAppID	Unsigned16	0	2	Application ID of Destination
2	Reserved	Octetstring	2	2	Reserved
3	Error Type	ErrorType	4	N	See error type

7.4.2.2.2 SafeCommunicationClose

7.4.2.2.2.1 SafeCommunicationClose request parameters

The SafeCommunicationClose service request is used to close the link relationship of function safety communication. The SafeCommunicationClose service request parameters are specified in Table 28.

Table 28 – SafeCommunicationClose request parameters

Index	Parameter name	Data type	Octet offset	Octet length	Description
1	SourceAppID	Unsigned16	0	2	Source application ID
2	SourceIPAddress	Unsigned32	2	4	Source IP address
3	DestinationIPAddress	Unsigned32	6	4	Destination IP address
4	LinkObjectID	Unsigned16	10	2	Link object ID

7.4.2.2.2.2 SafeCommunicationClose positive response parameters

If a device receives a SafeCommunicationClose request service and operates correctly, it shall return a SafeCommunicationClose service positive response. The SafeCommunicationClose service positive response parameters are specified in Table 29.

Table 29 – SafeCommunicationClose positive response parameters

Index	Parameter name	Data type	Octet offset	Octet length	Description
1	DestinationAppID	Unsigned16	0	2	Application ID of destination

7.4.2.2.2.3 SafeCommunicationClose negative response parameters

The SafeCommunicationClose service negative response returns a SafeCommunicationClose request service's error reason. The SafeCommunicationClose service negative response parameters are specified in Table 30.

Table 30 – SafeCommunicationClose negative response parameters

Index	Parameter name	Data type	Octet offset	Octet length	Description
1	DestinationAppID	Unsigned16	0	2	Application ID of destination
2	Reserved	Octetstring	2	2	Reserved
3	Error Type	ErrorType	4	N	See error type

7.4.2.3 Error code

7.4.2.3.1 Error Type Structure

```
ErrorType : : = SEQUENCE {
        ErrorClass              [0]     IMPLICIT  Integer8,
        ErrorCode               [1]     IMPLICIT  Integer8,
        AdditionalCode          [2]     IMPLICIT  Integer8,
        Reserved                [3]     IMPLICIT  OctetString,
        AdditionalDescription   [4]     IMPLICIT  VisibleString
}
```

7.4.2.3.2 Error Type

Table 31 – Error class and code

Error category		Error Class		Reason	Error Code
ErrorClass ::= CHOICE {					
	Resource	[0]	IMPLICIT Integer8 {		
				memory-unavailable	(0)
				Other	(1)
	},				
	Service	[1]	IMPLICIT Integer8 {		
				object-state-conflict	(0)
				object-constraint-conflict	(1)
				parameter-inconsistent	(2)
				illegal-parameter	(3)
				Size Error	(4)
				Other	(5)
	}				
	Access	[2]	IMPLICIT Integer8 {		
				object-access-unsupported	(0)
				object-non-existent	(1)
				object-access-denied	(2)
				hardware-fault	(3)
				type-conflict	(4)
				object-attribute-inconsistent	(5)
				Access-to-element-unsupported	(6)
				Other	(7)
	}				
	Timer	[3]	IMPLICIT Integer8 {		
				Timer-Expire	(0)
				Timer-Error	(1)
				Other	(2)
	},				

Error category		Error Class		Reason	Error Code
	Safety	[4]	IMPLICIT Integer8{		
				CRC-Match-Error	(0)
				Repetition	(1)
				Timer-Out-Error	(2)
				Loss	(3)
				Sequence Error	(4)
				Other	(5)
	}				
	Other	[5]	IMPLICIT Integer8 {		
				Other	(0)

The value of ErrorClass and ErrorCode for the error is defined as its priority. When more than one error is detected, the ErrorClass shall be compared: if the ErrorClass is the same, then the ErrorCode shall be compared. If the value is smaller, the priority is higher.

8 Safety communication layer management

8.1 Time synchronization diagnostics

8.1.1 Time synchronization process

The time synchronization procedure is specified in IEC 61158-6-14.

In order to make sure the time synchronization message is suitable for the functional safety communication, a CRC check mechanism is added for checking the data integrity.

The CRC check mechanism is show as Figure 17.

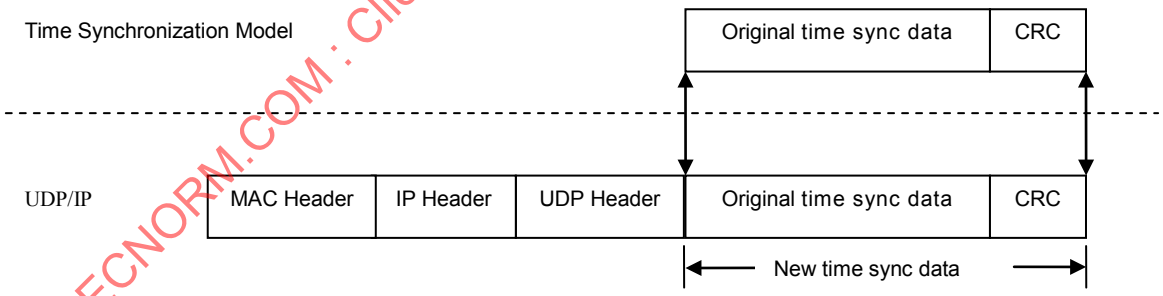


Figure 17 – CRC check for time synchronization process

The content for CRC check is the original time synchronization data which is defined by IEC 61588. The new time sync data built by original time synchronization data and CRC is looked as user data from the UDP/IP side.

The CRC polynomial for the time synchronization process is as follows:

$$G(x) = (x^{32} + x^{29} + x^{28} + x^{25} + x^{22} + x^{20} + x^{19} + x^{13} + x^{12} + x^{10} + x^{7} + x^{4} + x^{3} + 1)$$

8.1.2 Time synchronization management

Time is synchronized by the black channel. The time synchronization monitor shall watch whether the black channel time synchronization is working correctly or not. Each device shall manage and monitor the time synchronization process, and report the time synchronization fault.

At each time of synchronization, a local device receives a synchronization message from a master clock for a system-specified time. The local clock compares with the master clock contained in the Sync or Follow-Up message, and the difference is the actual drift between local clock and master clock. If the actual drift exceeded the TargetTimeSyncClass in MIB, the device should indicate that all data sent from this device is fault for all destination devices and that the relative bit in the LinkageFault attribute shall be set by the safety application layer entity.

8.2 CSME diagnostics

8.2.1 General

The CSME diagnostics can be an independent device or can be resident in a general device. It is used to monitor the schedule of the data transmission in the macro-cycle. If some error happened, the CSME monitor shall report the fault through alert reporting.

8.2.2 CSME diagnostics management

8.2.2.1 Periodic packets diagnostics management

The periodic packets diagnostics module shall receive all the data in the periodic packet transferring phase (Tp). Due to an error, fault or interference, a message is not received or some messages are not transferring according to the configured schedule. The schedule number is not sequential. Periodic packets diagnostics module compares the schedule number in the received functional safety PDU with the local CSME information. Once the error of loss or wrong schedule has been detected, the CSME shall report the message with the type of fault to the special application.

8.2.2.2 Non-periodic packets diagnostics management

8.2.2.2.1 General

The non-periodic packets diagnostics module should record all NonPeriodDataAnnuciation messages in a communication macro-cycle, and maintain a schedule table for each communication macro-cycle. The non-periodic packets diagnostics module should watch all non-periodic packets in non-periodic packet transferring phase. If the non-periodic packets are not received according to the schedule table formed in the periodic packet transferring phase, the module should set the relative bit in the LinkageFault attribute. Mostly, there are three kinds of faults that can happen in the non-periodic packet transferring phase.

8.2.2.2.2 Non-periodic packet loss error

In the non-periodic packet transferring phase, the non-periodic packets diagnostics receives low priority non-periodic packets without a special high priority packet announcement in NonPeriodDataAnnunciation packet. Then, the Non-periodic packets diagnostics asserts that as a high priority packet loss, and set relative bit in the LinkageFault attribute.

8.2.2.2.3 Non-periodic packet sequence error

In the non-periodic packet transferring phase, the non-periodic packets diagnostics receives a low priority non-periodic packet before a special high priority packet announcement in NonPeriodDataAnnunciation packet. Then, the Non-periodic packets diagnostics asserts that a sequence error for this two packets occurred, and sets a relative bit in the LinkageFault attribute.

8.2.2.2.4 Non-periodic packet insertion error

In the non-periodic packet transferring phase, the Non-periodic packets diagnostics receives a packet without announce in any NonPeriodDataAnnunciation packet. Then, the non-periodic packets diagnostics asserts that the packet was unexpected, and sets a relative bit in the LinkageFault attribute.

8.3 Communication fault management

8.3.1 Configuration management

Each functional safety link object shall manage and monitor the process of reporting the communication fault in data transmission.

The LinkageFault attribute in functional safety link object is defined to record the current communication faults. If the communication fault is detected by a safety application layer entity, the relative bit in the LinkageFault attribute shall be set.

Whether the communication fault is reported to the special application or not, is determined by the FaultReportConfiguration attribute in functional safety link object. The special application is determined by functional safety link object which ServiceRole is Safety Alert Req.

If the relative bits in FaultReportConfiguration attribute are set, the relative communication faults shall not report to the special application. If the communication fault is not required to report, the acknowledge to the relative communication fault shall be ignored.

Whether the communication fault is acknowledged by the special application or not, is determined by FaultAcknowledgeConfiguration attribute in functional safety link object. If the relative bits in FaultAcknowledgeConfiguration attribute are set, it is not necessary for the special application to acknowledge the relative communication faults.

If more than one communication fault is detected at the same time, the first reported communication fault is determined by the priority of ErrorClass (see 7.4.2.3.2). The communication fault with higher priority shall be reported to the special application first, and the communication fault with lower priority shall be reported to the special application when there is no higher priority communication fault or higher priority communication faults have been already reported.

8.3.2 Communication fault report process

The state of communication fault is defined by the linkage state attribute, fault report state attribute and fault acknowledge state attribute in functional safety link object. Table 32 shows the relation between state of communication and the attributes in safety communication fault.

Table 32 – Communication process of confirmed service between two devices

LinkageFault	Linkage state	Fault report state	Fault acknowledge state
IDLE	0	0	0
Unreported_Unacknowledged	1	1	1
Unreported_Acknowledgeed	1	1	0
Reported_Unacknowledged	1	0	1
Reported_Acknowledged	1	0	0
Unactive_Unreported	0	1	0

If the relative bits of the LinkageFault attribute: linkage state attribute, fault report state attribute and fault acknowledge state attribute are zero, the state of communication fault is IDLE.

If the current state of communication fault is IDLE and the communication fault is detected, the relative bit of the LinkageFault attribute shall be set. The bit of fault report state attribute shall be set if the corresponding FaultReportConfiguration attribute is zero. Otherwise, the bit of fault report state attribute shall keep unchangeable. The bit of fault acknowledge state attribute shall be set if corresponding FaultAcknowledgeConfiguration is zero. Otherwise, the bit of fault acknowledge state attribute shall keep unchangeable.

If relative bit of fault report state attribute is set, communication fault shall be sent via EventNotification service request to the special application determined by the functional safety link object.

After the safety device receives the AcknowledgeEventNotification service request, the relative bit of fault report state attribute shall be cleared.

Acknowledge to communication fault is determined by the relative bit of fault acknowledge state attribute. If the relative bit of fault acknowledge state is set, an integrated communication fault report shall be completed when the device receives write service request resetting the relative bit of acknowledge state attribute.

If the device has not received the AcknowledgeEventNotification service request during the MaxResponseTime defined in functional safety communication fault object, this device shall send the EventNotification service request again.

The device shall send the AcknolowledgeEventNotification service response after processing the AcknowledgeEventNotification service request.

If the communication fault recovered, the relative bit of the LinkageFault attribute shall be reset, and the bit of fault report state attribute shall be set if the corresponding FaultReportConfiguration attribute is zero. Otherwise, the bit of fault report state shall keep unchangeable.

It's unnecessary for the special application determined by the functional safety link object to acknowledge the recovering of communication fault.

The process of a communication fault report is shown in Figure 18.

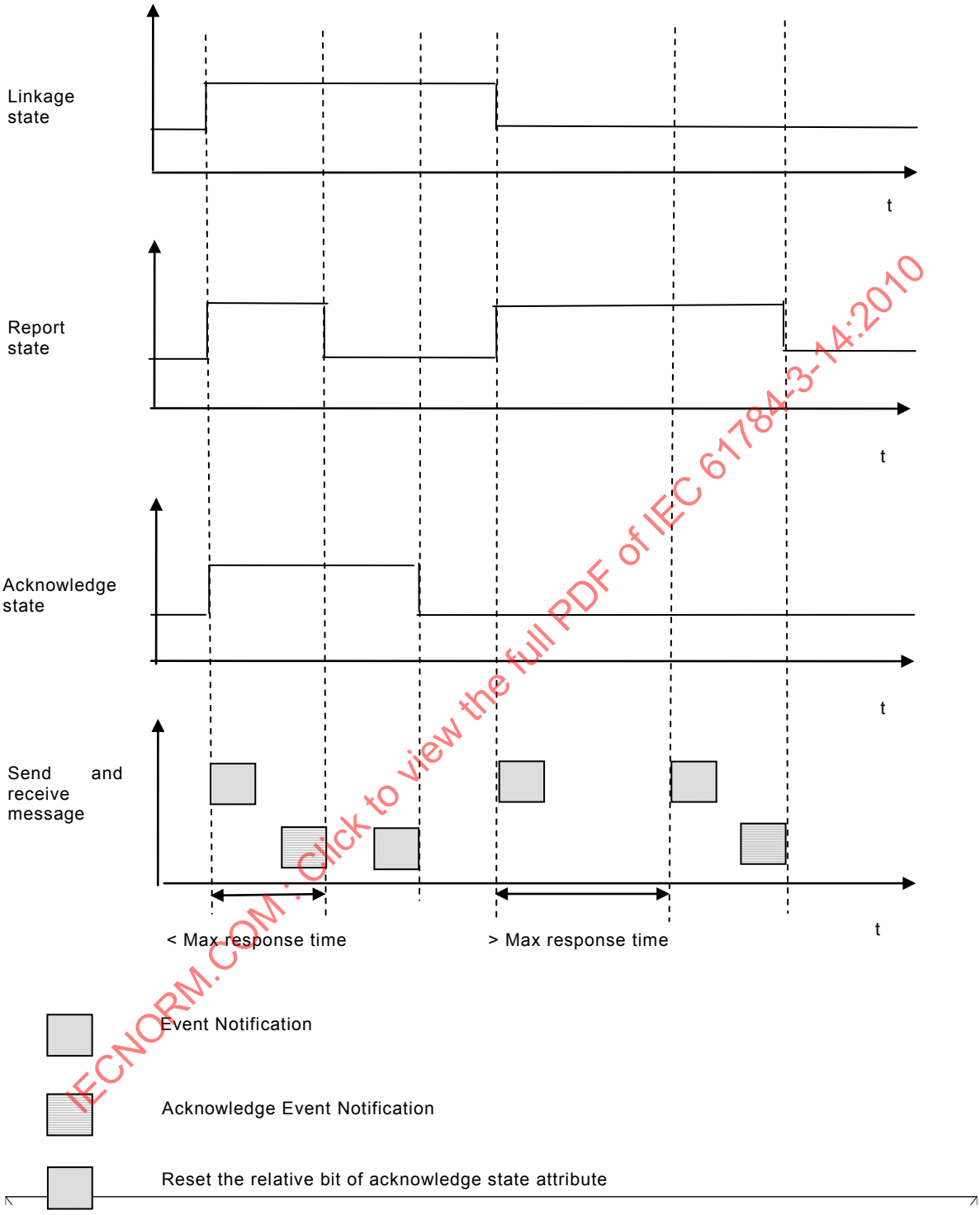


Figure 18 – The process of communication fault report

9 System requirements

9.1 Indicators and switches

Each safety device shall have a red LED. This LED shall represent the following states:

- Off: no error; device in process data mode.
- On: Failure state of the device; device fails.

9.2 Installation guidelines

The installation guidelines of IEC 61784-5-14 for CPF 14 shall apply.

9.3 Safety function response time

9.3.1 General

The safety function response time is the worst-case time from a safety-related event, as input to the system or as a fault within the system, until the time that the system is in the safe state.

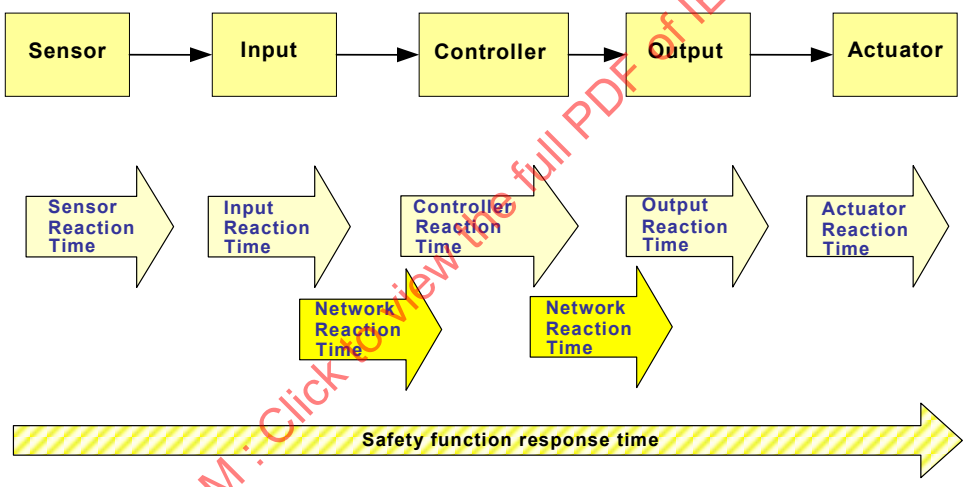


Figure 19 – Example application for FSCP 14/1 communication

To determine the safety function time of any control chain, the user shall add up the components of the safety chain.

Using the example in Figure 19, the safety function response time would be:

Safety function response time = Sensor reaction time
+ Input reaction time
+ Network reaction time
+ Controller reaction time
+ Network reaction time
+ Output reaction time
+ Actuator reaction time

9.3.2 Calculation of the network reaction time

The network reaction time is a portion of the safety function response time. The network reaction time is the worst case time, from the time the data is captured by the safety data sender, until the receiving application recognizes a safety state. This also includes errors during sending and receiving.

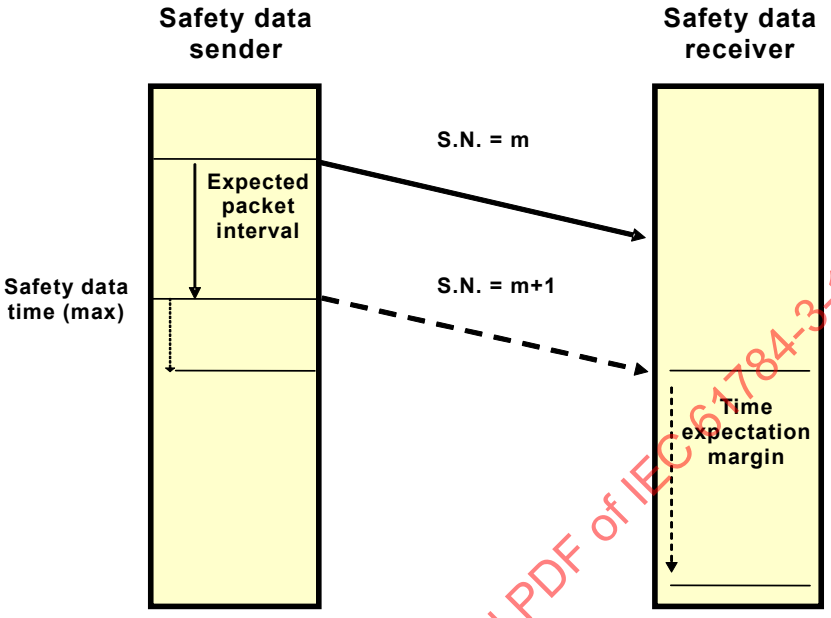


Figure 20 – Calculation of the network reaction time

Using the example in Figure 20, the network reaction time would be:

Network reaction time = Expected packet interval
+ Safety message time(max)
+ Time expectation margin

where:

Expected Packet Interval is the time interval used by the safety sender to send data.

Safety data time(max) is the actual time from the data being captured by the safety data sender until the time that the safety data is passed to the receiving application for use.

Time expectation margin is the additional margin on expectation time according to the attribute Scheduling Precision Requirement which shall be set by the user application (see Table 34).

Table 33 – Settings for time expectation margin

Scheduling precision requirement	Time expectation margin
1	1 s
2	100 ms
3	10 ms
4	1 ms
5	100 µs
6	10 µs
7	1 µs

9.4 Duration of demands

The duration of the demand shall be at least of one macro cycle, in order to guarantee that the functional safety communication system detects the demand.

9.5 Constraints for calculation of system characteristics

Configuration tools shall set the Communication Macro-Cycle long enough to carry out the safety data package either in Cyclic and Acyclic Package Deliver Phase.

Calculation of the residual error rate is performed assuming:

a given binary symmetric channel with a bit-error rate of ε,

a communication system transmitting each message twice,

and a CRC C(1) performed separately on each of the two messages.

The receiving device should then perform a cross-check between both messages. The total message is accepted only if there is no checksum fault and the two partial messages are identical bit by bit. The length of a single message shall be n bits.

A new check sum procedure (a linear code) C(2) has be defined using the rule "2 x CRC + crosscheck".

If $P_{ue}(\varepsilon, C^{(1)})$ and $P_{ue}(\varepsilon, C^{(2)})$ are the probabilities of undetected errors for C(1) and C(2), respectively,

then $P_{ue}(\varepsilon, C^{(2)}) \leq P_{ue}(\varepsilon^2, C^{(1)})$

This means that, at a bit-error rate of ε, the double transmission procedure C(2) is performing at least as well as the single CRC C(1) at a bit-error rate of ε^2.

The following worst case formula is used when calculating constraints for system characteristics:

$$P_{ue}(\varepsilon) \leq \sum_{l=d}^{n} \binom{n}{l} \times \varepsilon^{l} \times (1-\varepsilon)^{n-l}$$

where

P_{ue} is the probability of residual fault

ε is the bit error probability

d is the Hamming distance

n is the total message length

To calculate the residual error rate per hour resulting from P_{ue}, the following formula shall be used:

$$\Lambda = 3\,600 \times P_{ue} \times v \times (m\text{-}1) \times 100 \text{ [transmission errors/hour]}$$

where

v is the number of safety relevant messages per second

P_{ue} is defined above

(m-1) is the worst case number of transmissions with m participants

The factor 100 indicates that the transmissions only contributes 1% to the error rate

The constraints for system characteristics for different message rates and number of participants are shown in Table 34.

Table 34 – Constraints for system characteristics at $\varepsilon = 10^{-2}$

n	*d*	*v*	*m*	Λ	SIL
184	8	10	11	$9{,}897\,505 \times 10^{-12}$	3
184	8	100	11	$9{,}897\,505 \times 10^{-11}$	3
184	8	100	32	$3{,}068\,226 \times 10^{-10}$	3
184	8	10	500	$4{,}938\,855 \times 10^{-10}$	3

NOTE
n: total message length
d: harming distance
ε: bit error probability
v: number of safety relevant messages per second
m: the worst case number of transmissions with m participants
Λ: residual error rate per hour

9.6 Maintenance

There are no specific maintenance requirements for the FSCP 14/1.

9.7 Safety manual

A safety manual appropriate for the device should been supplied by the safety device manufacturer.

The safety manual shall include the methods necessary for calculating the safety response time for the safety-related system that includes the safety device.

10 Assessment

It shall be the manufacturer's responsibility to develop the implementers of FSCP 14/1 to the appropriate development process according to the safety standards (see IEC 61508 and IEC 61511) and an assessment for functional safety by an independent competent organization shall be achieved. It is highly recommended that implementers of FSCP 14/1 obtain proof that a suitable conformance test has been performed by an independent, competent organization.

Annex A
(informative)

Additional information for functional safety communication profiles of CPF 14

A.1 Hash function calculation

```
// the crc polynomial choosen is [0xBA0DC66B], it is in detail:
//G(x) = x32+x30+x29+x28+x26+x20+x19+x17+ x16+x15+x11+x10+ x7+ x6+ x4+x2+x+1

Uint32 CRC32Table[256] = {
0x00000000, 0x9695C4CA, 0xFB4839C9, 0x6DDDFD03, 0x20F3C3CF, 0xB6660705, 0xDBBBFA06,
0x4D2E3ECC, 0x41E7879E, 0xD7724354, 0xBAAFBE57, 0x2C3A7A9D, 0x61144451, 0xF781809B,
0x9A5C7D98, 0x0CC9B952, 0x83CF0F3C, 0x155ACBF6, 0x788736F5, 0xEE12F23F, 0xA33CCCF3,
0x35A90839, 0x5874F53A, 0xCEE131F0, 0xC22888A2, 0x54BD4C68, 0x3960B16B, 0xAFF575A1,
0xE2DB4B6D, 0x744E8FA7, 0x199372A4, 0x8F06B66E, 0xD1FDAE25, 0x47686AEF, 0x2AB597EC,
0xBC205326, 0xF10E6DEA, 0x679BA920, 0x0A465423, 0x9CD390E9, 0x901A59BB, 0x068FED71,
0x6B521072, 0xFDC7D4B8, 0xB0E9EA74, 0x267C2EBE, 0x4BA1D3BD, 0xDD341777, 0x5232A119,
0xC4A765D3, 0xA97A98D0, 0x3FEF5C1A, 0x72C162D6, 0xE454A61C, 0x89895B1F, 0x1F1C9FD5,
0x13D52687, 0x8540E24D, 0xE89D1F4E, 0x7E08DB84, 0x3326E548, 0xA5B32182, 0xC86EDC81,
0x5EFB184B, 0x7598EC17, 0xE30D28DD, 0x8ED0D5DE, 0x18451114, 0x556B2FD8, 0xC3FEEB12,
0xAE231611, 0x38B6D2DB, 0x347F6B89, 0xA2EAAF43, 0xCF375240, 0x59A2968A, 0x148CA846,
0x82196C8C, 0xEFC4918F, 0x79515545, 0xF657E32B, 0x60C227E1, 0x0D1FDAE2, 0x9B8A1E28,
0xD6A420E4, 0x4031E42E, 0x2DEC192D, 0xBB79DDE7, 0xB7B064B5, 0x2125A07F, 0x4CF85D7C,
0xDA6D99B6, 0x9743A77A, 0x01D663B0, 0x6C0B9EB3, 0xFA9E5A79, 0xA4654232, 0x32F086F8,
0x5F2D7BFB, 0xC9B8BF31, 0x849681FD, 0x12034537, 0x7FDEB834, 0xE94B7CFE, 0xE582C5AC,
0x73170166, 0x1ECAFC65, 0x885F38AF, 0xC5710663, 0x53E4C2A9, 0x3E393FAA, 0xA8ACFB60,
0x27AA4D0E, 0xB13F89C4, 0xDCE274C7, 0x4A77B00D, 0x07598EC1, 0x91CC4A0B, 0xFC11B708,
0x6A8473C2, 0x664DCA90, 0xF0D80E5A, 0x9D05F359, 0x0B903793, 0x46BE095F, 0xD02BCD95,
0xBDF63096, 0x2B63F45C, 0xEB31D82E, 0x7DA41CE4, 0x1079E1E7, 0x86EC252D, 0xCBC21BE1,
0x5D57DF2B, 0x308A2228, 0xA61FE6E2, 0xAAD65FB0, 0x3C439B7A, 0x519E6679, 0xC70BA2B3,
0x8A259C7F, 0x1CB058B5, 0x716DA5B6, 0xE7F8617C, 0x68FED712, 0xFE6B13D8, 0x93B6EEDB,
0x05232A11, 0x480D14DD, 0xDE98D017, 0xB3452D14, 0x25D0E9DE, 0x2919508C, 0xBF8C9446,
0xD2516945, 0x44C4AD8F, 0x09EA9343, 0x9F7F5789, 0xF2A2AA8A, 0x64376E40, 0x3ACC760B,
0xAC59B2C1, 0xC1844FC2, 0x57118B09, 0x1A3FB5C4, 0x8CAA710E, 0xE1778C0D, 0x77E248C7,
0x7B2BF195, 0xEDBE355F, 0x8063C85C, 0x16F60C96, 0x5BD8325A, 0xCD4DF690, 0xA0900B93,
0x3605CF59, 0xB9037937, 0x2F96BDFD, 0x424B40FE, 0xD4DE8434, 0x99F0BAF8, 0x0F657E32,
0x62B88331, 0xF42D47FB, 0xF8E4FEA9, 0x6E713A63, 0x03ACC760, 0x953903AA, 0xD8173D66,
0x4E82F9AC, 0x235F04AF, 0xB5CAC065, 0x9EA93439, 0x083CF0F3, 0x65E10DF0, 0xF374C93A,
0xBE5AF7F6, 0x28CF333C, 0x4512CE3F, 0xD3870AF5, 0xDF4EB3A7, 0x49DB776D, 0x24068A6E,
0xB2934EA4, 0xFFBD7068, 0x6928B4A2, 0x04F549A1, 0x92608D6B, 0x1D663B05, 0x8BF3FFCF,
0xE62E02CC, 0x70BBC606, 0x3D95F8CA, 0xAB003C00, 0xC6DDC103, 0x504805C9, 0x5C81BC9B,
0xCA147851, 0xA7C98552, 0x315C4198, 0x7C727F54, 0xEAE7BB9E, 0x873A469D, 0x11AF8257,
0x4F549A1C, 0xD9C15ED6, 0xB41CA3D5, 0x2289671F, 0x6FA759D3, 0xF9329D19, 0x94EF601A,
0x027AA4D0, 0xFEB31D82, 0x9826D948, 0xF5FB244B, 0x636EE081, 0x2E40DE4D, 0xB8D51A87,
0xD508E784, 0x439D234E, 0xCC9B9520, 0x5A0E51EA, 0x37D3ACE9, 0xA1466823, 0xEC6856EF,
0x7AFD9225, 0x17206F26, 0x81B5ABEC, 0x8D7C12BE, 0x1BE9D674, 0x76342B77, 0xE0A1EFBD,
0xAD8FD1F1, 0x3B1A15BB, 0x56C7E8B8, 0xC0522C72 };

Uint32 CRC32Check(Uint8 *pData, Uint32 DataLength)
{
    Uint32 CRCCode32;
    Uint32 CRCTableValue;
    Uint32 CharCounter;
    Uint32 TempCharIn;
    Uint32 TempCharOut;

    CharCounter = 0;

    CRCCode32 = 0x00000000;

    while (DataLength --)
    {
        TempCharOut = (CRCCode32 >> 24) & 0xFF;
        CRCTableValue = CRC32Table[TempCharOut];
        TempCharIn = pData[CharCounter];
```

```
        CRCCode32 = (CRCCode32 << 8) | TempCharIn;
        CRCCode32 = CRCCode32 ^ CRCTableValue;
        CharCounter ++;
    }
    return CRCCode32;
}
```

A.2 …

Void

Annex B
(informative)

Information for assessment of the functional safety communication profiles of CPF 14

Information about test laboratories which test and validate the conformance of FSCP 14/1 products with IEC 61784-3-14 can be obtained from the National Committees of the IEC or from the following organization:

Zhejiang University
Institute of Cyber-Systems and Control
Zheda Road 38
Hangzhou 310027
Zhejiang
P.R.CHINA

Phone: +86-571-81992701
Fax: +86-571-87951206
E-mail:EPA@supcon.com
URL: http://www.epa.org.cn

Bibliography

[1] IEC 60050 (all parts), *International Electrotechnical Vocabulary*

NOTE See also the IEC Multilingual Dictionary – Electricity, Electronics and Telecommunications (available on CD-ROM and at <http://www.electropedia.org>)

[2] IEC 60204-1, *Safety of machinery – Electrical equipment of machines – Part 1: General requirements*

[3] IEC/TS 61000-1-2, *Electromagnetic compatibility (EMC) – Part 1-2: General – Methodology for the achievement of the functional safety of electrical and electronic equipment with regard to electromagnetic phenomena*

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

[5] IEC 61131-6, *Programmable controllers – Part 6: Functional safety*[10]

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

[7] IEC 61326-3-1, *Electrical equipment for measurement, control and laboratory use – EMC requirements – Part 3-1: Immunity requirements for safety-related systems and for equipment intended to perform safety related functions (functional safety) – General industrial applications*

[8] IEC 61326-3-2, *Electrical equipment for measurement, control and laboratory use – EMC requirements – Part 3-2: Immunity requirements for safety-related systems and for equipment intended to perform safety related functions (functional safety) – Industrial applications with specified electromagnetic environment*

[9] IEC 61496 (all parts), *Safety of machinery – Electro-sensitive protective equipment*

[10] IEC 61508-1:2010[11], *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements*

[11] IEC 61508-4:2010[11], *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations*

[12] IEC 61508-5:2010[11], *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 5: Examples of methods for the determination of safety integrity levels*

[13] IEC 61508-6:2010[11], *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3*

[14] IEC 61784-1, *Industrial communication networks – Profiles – Part 1: Fieldbus profiles*

[15] IEC 61784-4[12], *Industrial communication networks – Profiles – Part 4: Secure communications for fieldbuses*

[16] IEC 61784-5 (all parts), *Industrial communication networks – Profiles – Part 5: Installation of fieldbuses – Installation profiles for CPF x*

[17] IEC 61784-5-14[10], *Industrial communication networks – Profiles – Part 5: Installation of fieldbuses – Installation profiles for CPF 14*

[18] IEC 61800-5-2, *Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional*

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

[20] IEC/TR 62059-11, *Electricity metering equipment – Dependability – Part 11: General concepts*

---

[10] In preparation.

[11] To be published.

[12] Proposed new work item under consideration.

[21] IEC 62061, *Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems*

[22] IEC/TR 62210, *Power system control and associated communications – Data and communication security*

[23] IEC 62280-1, *Railway applications – Communication, signalling and processing systems – Part 1: Safety-related communication in closed transmission systems*

[24] IEC 62280-2, *Railway applications – Communication, signalling and processing systems – Part 2: Safety-related communication in open transmission systems*

[25] IEC 62443 (all parts), *Industrial communication networks – Network and system security*

[26] ISO/IEC Guide 51:1999, *Safety aspects — Guidelines for their inclusion in standards*

[27] ISO/IEC 2382-14, *Information technology – Vocabulary – Part 14: Reliability, maintainability and availability*

[28] ISO/IEC 2382-16, *Information technology – Vocabulary – Part 16: Information theory*

[29] ISO/IEC 7498 (all parts), *Information technology – Open Systems Interconnection – Basic Reference Model*

[30] ISO 10218-1, *Robots for industrial environments – Safety requirements – Part 1: Robot*

[31] ISO 12100-1, *Safety of machinery – Basic concepts, general principles for design – Part 1: Basic terminology, methodology*

[32] ISO 13849-1, *Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design*

[33] ISO 13849-2, *Safety of machinery – Safety-related parts of control systems – Part 2: Validation*

[34] ISO 14121, *Safety of machinery – Principles of risk assessment*

[35] EN 954-1:1996 [13], *Safety of machinery – Safety related parts of control systems – General principles for design*

[36] ANSI/ISA-84.00.01-2004 (all parts), *Functional Safety: Safety Instrumented Systems for the Process Industry Sector*

[37] Internet Engineering Task Force (IETF), Request for Comments (RFC):

RFC 768, User Datagram Protocol
available at <http://www.ietf.org/rfc/rfc0768.txt>

RFC 791, Internet Protocol
available at <http://www.ietf.org/rfc/rfc0791.txt>

RFC 793, Internet Protocol
available at <http://www.ietf.org/rfc/rfc0793.txt>

[38] VDI/VDE 2180 (all parts), *Safeguarding of industrial process plants by means of process control engineering*

[39] GS-ET-26 [14], *Grundsatz für die Prüfung und Zertifizierung von Bussystemen für die Übertragung sicherheitsrelevanter Nachrichten*, May 2002. HVBG, Gustav-Heinemann-Ufer 130, D-50968 Köln ("*Principles for Test and Certification of Bus Systems for Safety relevant Communication*")

[40] ANDREW S. TANENBAUM, *Computer Networks*, 4th Edition, Prentice Hall, N.J., ISBN-10:0130661023, ISBN-13: 978-0130661029

[41] W. WESLEY PETERSON, *Error-Correcting Codes*, 2nd Edition 1981, MIT-Press, ISBN 0-262-16-039-0

[42] BRUCE P. DOUGLASS, *Doing Hard Time*, 1999, Addison-Wesley, ISBN 0-201-49837-5

13 To be replaced by ISO 13849-1 and/or IEC 62061.

14 This document has been one of the starting points for this part. It is currently undergoing a major revision.

[43] *New concepts for safety-related bus systems*, 3rd International Symposium "Programmable Electronic Systems in Safety Related Applications ", May 1998, from Dr. Michael Schäfer, BG-Institute for Occupational Safety and Health.

[44] DIETER CONRADS, *Datenkommunikation*, 3rd Edition 1996, Vieweg, ISBN 3-528-245891

[45] German IEC subgroup DKE AK 767.0.4: *EMC and Functional Safety*, Spring 2002

[46] NFPA79 (2002), *Electrical Standard for Industrial Machinery*

[47] GUY E. CASTAGNOLI, *On the Minimum Distance of Long Cyclic Codes and Cyclic Redundancy-Check Codes*, 1989, Dissertation No. 8979 of ETH Zurich, Switzerland

[48] GUY E. CASTAGNOLI, STEFAN BRÄUER, and MARTIN HERRMANN, *Optimization of Cyclic Redundancy-Check Codes with 24 and 32 Parity Bits*, June 1993, IEEE Transactions On Communications, Volume 41, No. 6

[49] SCHILLER F and MATTES T: *An Efficient Method to Evaluate CRC-Polynomials for Safety-Critical Industrial Communication*, Journal of Applied Computer Science, Vol. 14, No 1, pp. 57-80, Technical University Press, Łódź,Poland, 2006

[50] SCHILLER F and MATTES T: *Analysis of CRC-polynomials for Safety-critical Communication by Deterministic and Stochastic Automata*, 6th IFAC Symposium on Fault Detection, Supervision and Safety for Technical Processes, SAFEPROCESS 2006, pp. 1003-1008, Beijing, China, 2006

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

RÉSEAUX DE COMMUNICATION INDUSTRIELS – PROFILS –

Partie 3-14: Bus de terrain de sécurité fonctionnelle – Spécifications supplémentaires pour CPF 14

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (CEI) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de la CEI). La CEI a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, la CEI – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de la CEI"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec la CEI, participent également aux travaux. La CEI collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de la CEI concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de la CEI intéressés sont représentés dans chaque comité d'études.
3) Les Publications de la CEI se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de la CEI. Tous les efforts raisonnables sont entrepris afin que la CEI s'assure de l'exactitude du contenu technique de ses publications; la CEI ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de la CEI s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de la CEI dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de la CEI et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) La CEI elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de la CEI. La CEI n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à la CEI, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de la CEI, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de la CEI ou de toute autre Publication de la CEI, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de la CEI peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. La CEI ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et de ne pas avoir signalé leur existence.

La Norme internationale CEI 61784-3-14 a été établie par le sous-comité 65C: Réseaux de communication industriels, du comité d'études 65 de la CEI: Mesure, commande et automation dans les processus industriels.

La présente version bilingue (2012-02) correspond à la version anglaise monolingue publiée en 2010-06.

Le texte anglais de cette norme est issu des documents 65C/591A/FDIS et 65C/603/RVD.

Le rapport de vote 65C/603/RVD donne toute information sur le vote ayant abouti à l'approbation de cette norme.

La version française de cette norme n'a pas été soumise au vote.

.Cette publication a été rédigée selon les Directives ISO/CEI, Partie 2.

Une liste de toutes les parties de la série CEI 61784-3, présentées sous le titre général *Réseaux de communication industriels – Profils – Bus de terrain de sécurité fonctionnelle*, est disponible sur le site Web de la CEI.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de stabilité indiquée sur le site web de la CEI sous "http://webstore.iec.ch" dans les données relatives à la publication recherchée. A cette date, la publication sera

- reconduite;
- supprimée;
- remplacée par une édition révisée, ou
- amendée.

IMPORTANT – Le logo "colour inside" qui se trouve sur la page de garde de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à la bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

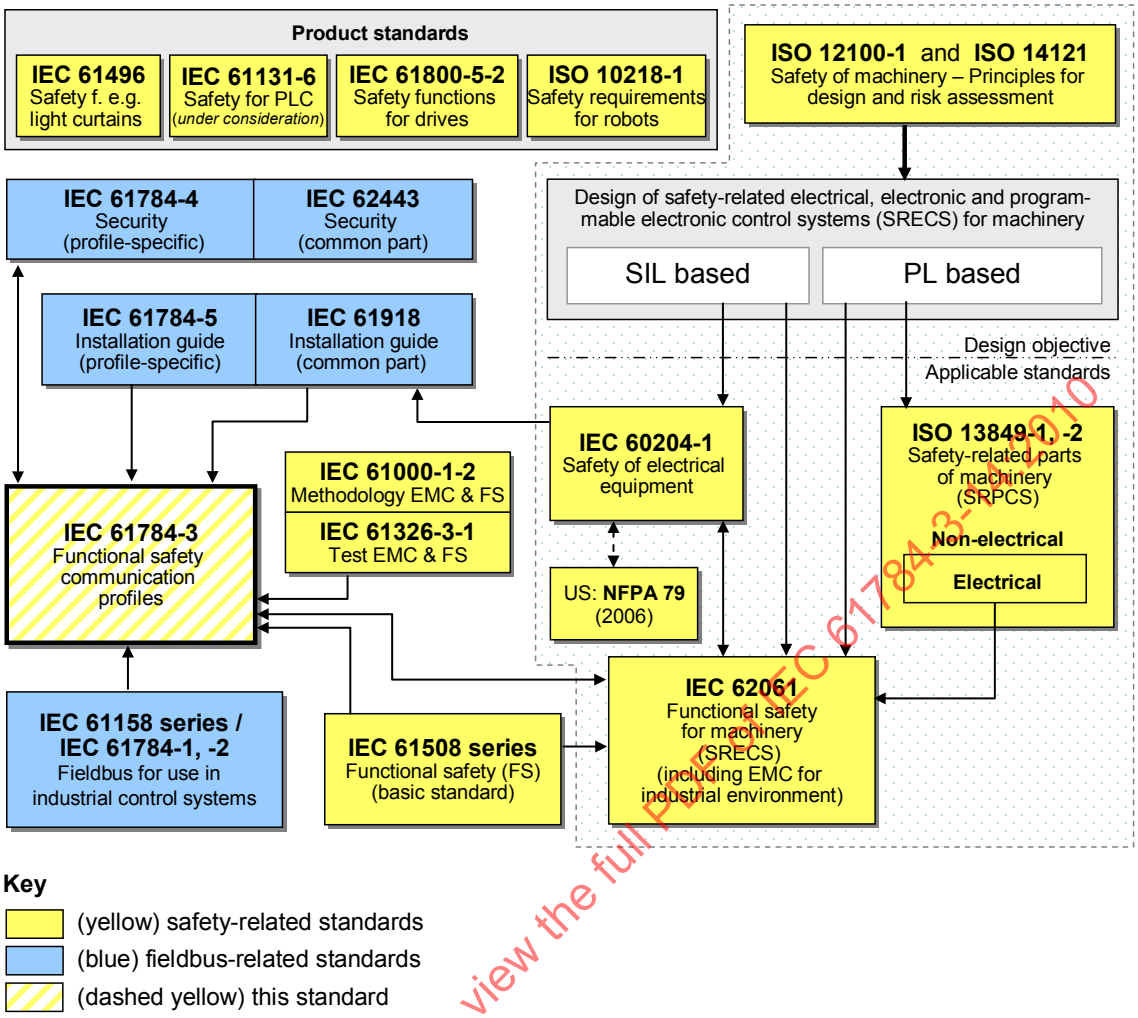
0 Introduction

0.1 Généralités

La norme CEI 61158 relative aux bus de terrain, ainsi que ses normes associées CEI 61784-1 et CEI 61784-2, définit un ensemble de protocoles de communication qui assurent la commande répartie d'applications automatisées. La technologie de bus de terrain est désormais reconnue et bien éprouvée. Ainsi de nombreuses améliorations des bus de terrain se développent pour traiter de domaines non encore normalisés tels que les applications en temps réel relatives à la sécurité et à la sûreté.

La présente norme définit les principes pertinents applicables aux communications en termes de sécurité fonctionnelle en référence à la série CEI 61508, et spécifie plusieurs couches de communication de sécurité (profils et protocoles correspondants) basées sur les profils de communication et les couches de protocole de la CEI 61784-1, la CEI 61784-2 et la série CEI 61158. Elle ne couvre pas les aspects relatifs à la sécurité électrique et à la sécurité intrinsèque.

La Figure 1 illustre les relations entre la présente norme et les normes pertinentes relatives à la sécurité et au bus de terrain dans un environnement machines.



Key

(yellow) safety-related standards

(blue) fieldbus-related standards

(dashed yellow) this standard

Légende

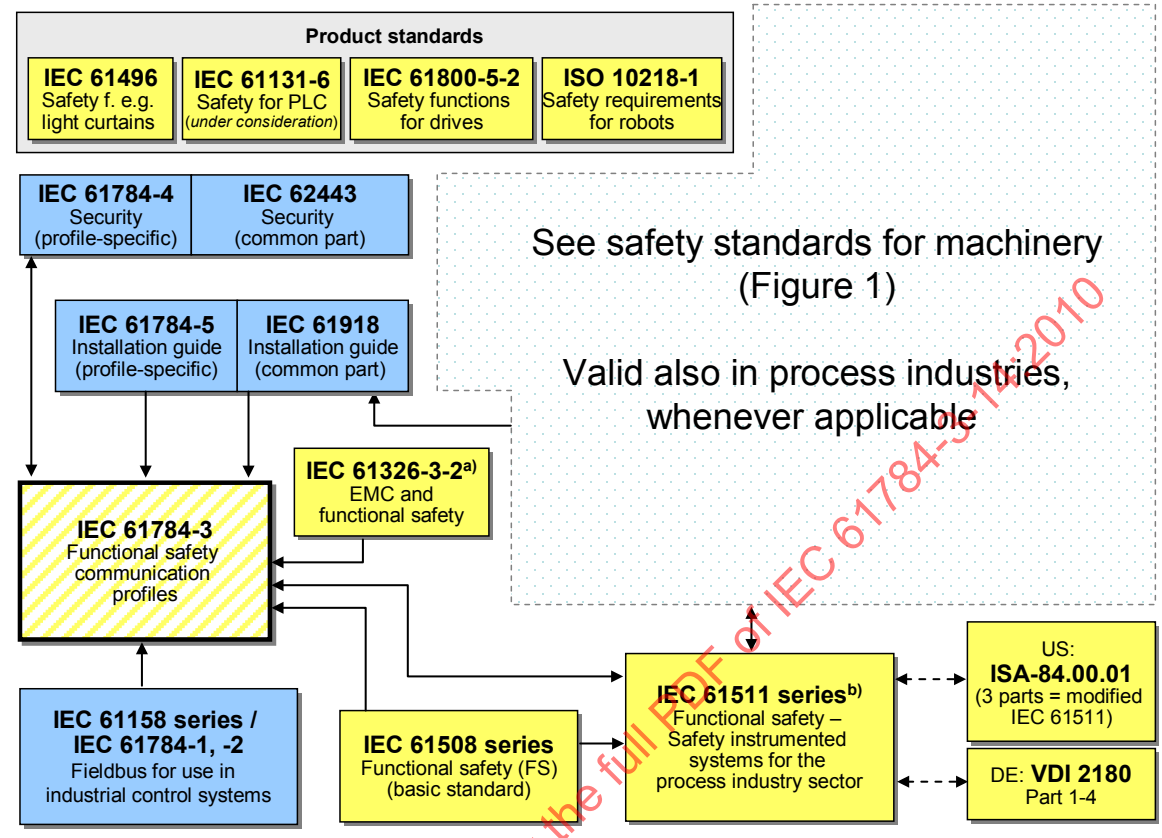
Anglais	Français
Product standards	Normes de produits
Safety function, e.g. light curtains	Fonction de sécurité, par exemple rideaux de lumière
Safety for PLC (under consideration)	Sécurité relative aux automates programmables (à l'étude)
Safety functions for drives	Fonctions de sécurité applicables aux entraînements
Safety requirements for robots	Exigences de sécurité applicables aux robots
Safety of machinery - ... assessment	Sécurité des machines – principes généraux de conception et appréciation du risque
Security (profile-specific)	Sûreté (spécifique au profil)
Security (common part)	Sûreté (partie commune)
Design of safety-related .... for machinery	Conception des systèmes de commande électriques, électroniques et électroniques programmables relatifs à la sécurité pour les machines
SIL based	Basé sur SIL
PL based	Basé sur PL
Installation guide (profile-specific)	Guide d'installation (spécifique au profil)
Installation guide (common part)	Guide d'installation (partie commune)

Anglais	Français
Design objective	Objectif de conception
Applicable standards	Normes applicables
Safety of electrical equipment	Sécurité des équipements électriques
Safety-related parts of machinery	Parties des systèmes de commande relatives à la sécurité
Non-electrical	Non électrique
Electrical	Electrique
Methodology EMC & functional safety	Méthodologie en matière de compatibilité électromagnétique & sécurité fonctionnelle
Test EMC & functional safety	Essai CEM et sécurité fonctionnelle
Functional safety communication profiles	Profils de communication de sécurité fonctionnelle
IEC 61158 series / Fieldbus for use in industrial control systems	Série CEI 61158 / Bus de terrain pour utilisation dans des systèmes de commande industriels
IEC 61508 series, Functional safety (basic standard)	Série CEI 61508 Sécurité fonctionnelle (norme de base)
Functional safety for machinery .... for industrial environment)	Sécurité fonctionnelle des systèmes de commande électriques, électroniques et électroniques programmables (y compris les interférences électromagnétiques dans l'environnement industriel)
Key	Légende
(yellow) safety-related standards	(jaune) normes relatives à la sécurité
(blue) fieldbus-related standards	(bleu) normes relatives au bus de terrain
(dashed) yellow) this standard	(jaune pointillé) la présente norme
IEC	CEI

NOTE Les paragraphes 6.7.6.4 (haute complexité) et 6.7.8.1.6 (faible complexité) de la CEI 62061 spécifient la relation entre PL (catégorie) et SIL.

Figure 1 – Relations entre la CEI 61784–3 et d'autres normes (machines)

La Figure 2 illustre les relations entre la présente norme et les normes pertinentes relatives à la sécurité et au bus de terrain dans un environnement de transformation.



Key

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

Légende

Anglais	Français
Product standards	Normes de produits
Safety function, e.g. light curtains	Fonction de sécurité, par exemple barrières photo électriques
Safety for PLC (under consideration)	Sécurité relative aux automates programmables (à l'étude)
Safety functions for drives	Fonctions de sécurité applicables aux entraînements
Safety requirements for robots	Exigences de sécurité applicables aux robots
Security (profile-specific)	Sûreté (spécifique au profil)
Security (common part)	Sûreté (partie commune)
Installation guide (profile-specific)	Guide d'installation (spécifique au profil)
Installation guide (common part)	Guide d'installation (partie commune)
See safety standards for machinery (Figure 1)	Voir normes de sécurité pour les machines (Figure 1)
Valid also in process industries, whenever applicable	Valable également dans les industries de transformation, le cas échéant
Functional safety communication profiles	Profils de communication de sécurité fonctionnelle

Anglais	Français
IEC 61326-3-2 a) EMC and functional safety	CEI 61326-3-2 a) CEM & sécurité fonctionnelle
IEC 61158 series/ IEC 61784-1-2, Fieldbus for use in industrial control systems	Série CEI 61158/ CEI 61784-1,-2 Bus de terrain pour utilisation dans des systèmes de commande industriels
IEC 61508 series, Functional safety (basic standard)	Série CEI 61508 Sécurité fonctionnelle (norme de base)
IEC 61511 seriesb) Functional safety–safety instrumented systems for the process industry sector	Série CEI 61511b) sécurité fonctionnelle – systèmes instrumentés de sécurité pour le secteur des industries de transformation
US: ISA 84.00.1 (3 parts = modified IEC 61511)	US: ISA 84.00.1 (3 parties = CEI 61511 modifiée)
DE : VDI 2180 Part 1 –4	DE : VDI 2180 Parties 1 à 4
Key	Légende
(yellow) safety-related standards	(jaune) normes relatives à la sécurité
(blue) fieldbus-related standards	(bleu) normes relatives au bus de terrain
(dashed) yellow) this standard	(jaune pointillé) la présente norme

[a] Pour des environnements électromagnétiques spécifiés, sinon CEI 61326-3-1.

[b] EN ratifiée.

Figure 2 – Relation entre la CEI 61784–3 et d'autres normes (transformation)

Les couches de communication de sécurité mises en œuvre dans la trame de systèmes relatifs à la sécurité conformément à la série CEI 61508, assurent la confiance nécessaire à accorder à la transmission de messages (information) entre deux participants ou plus sur un bus de terrain dans un système relatif à la sécurité, ou une fiabilité suffisante dans le comportement de sécurité en cas d'erreurs ou de défaillances du bus de terrain.

Les couches de communication de sécurité spécifiées dans la présente norme permettent de garantir cette assurance en utilisant un bus de terrain dans des applications nécessitant une sécurité fonctionnelle jusqu'au niveau d'intégrité de sécurité (SIL) spécifié par son profil de communication de sécurité fonctionnelle correspondant.

La revendication du SIL qui en résulte pour un système dépend de la mise en œuvre du profil de communication de sécurité fonctionnelle retenu au sein du système – la mise en œuvre du profil de communication de sécurité fonctionnelle dans un dispositif normal ne suffit pas à le qualifier de dispositif de sécurité.

La présente norme décrit:

— les principes de base de mise en œuvre des exigences de la série CEI 61508 pour les communications de données relatives à la sécurité, y compris les défauts de transmission potentiels, les mesures correctives et les considérations concernant l'intégrité des données;

— la description individuelle des profils de sécurité fonctionnelle pour plusieurs familles de profils de communication dans les CEI 61784-1 et CEI 61784-2;

— les extensions de la couche de sécurité aux sections relatives au service et aux protocoles de communication de la série CEI 61158.

0.2 Déclaration de droits de propriété

La commission électrotechnique internationale (CEI) attire l'attention sur le fait qu'il est déclaré que la conformité avec le présent document peut impliquer l'utilisation de brevets concernant les profils de communication de sécurité fonctionnelle pour la famille 14, où la notation [xx] désigne le détenteur des droits de propriété.

CN1960247	[SxZ]	Method of Safety communication for industrial network
CN 1929373	[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.

La CEI ne prend pas position eu égard à la preuve, la validité et la portée de ces droits de propriété.

Les détenteurs de ces droits de propriété ont donné l'assurance à la CEI qu'ils consentent à négocier des licences avec des demandeurs du monde entier, en des termes et à des conditions raisonnables et non discriminatoires. A ce propos, la déclaration des détenteurs de ces droits de propriété est enregistrée à la CEI.

Des informations peuvent être obtenues auprès de:

[SxZ] SUPCON and Zhejiang university
Dongqin FENG

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

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

L'attention est attirée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues autres que ceux mentionnés ci-dessus. . La CEI ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et de ne pas avoir signalé leur existence.

RÉSEAUX DE COMMUNICATION INDUSTRIELS – PROFILS –

Partie 3-14: Bus de terrain de sécurité fonctionnelle – Spécifications supplémentaires pour CPF 14

1 Domaine d'application

La présente partie de la série CEI 61784-3 spécifie une couche de communication relative à la sécurité (services et protocole) fondée sur la CPF 14 de la CEI 61784-2 et le Type 14 de la CEI 61158. Elle identifie les principes applicables aux communications de sécurité fonctionnelle définies dans la CEI 61784-3, et appropriés à cette couche de communication de sécurité.

NOTE 1 Elle ne couvre pas les aspects relatifs à la sécurité électrique et à la sécurité intrinsèque. La sécurité électrique concerne les dangers tels que les chocs électriques. La sécurité intrinsèque concerne les dangers associés aux atmosphères explosibles.

La présente partie [1] définit les mécanismes de transmission des messages propres à la sécurité entre les participants d'un réseau réparti, en utilisant la technologie de bus de terrain conformément aux exigences de la série CEI 61508 [2] concernant la sécurité fonctionnelle. Ces mécanismes peuvent être utilisés dans diverses applications industrielles, telles que la commande de processus, l'usinage automatique et les machines.

La présente partie fournit des lignes directrices tant pour les développeurs que pour les évaluateurs de dispositifs et systèmes conformes.

NOTE 2 La revendication du SIL qui en résulte pour un système dépend de la mise en œuvre du profil de communication de sécurité fonctionnelle retenu au sein du système – la mise en œuvre du profil de communication de sécurité fonctionnelle, conforme à la présente partie, dans un dispositif normal ne suffit pas à le qualifier de dispositif de sécurité.

2 Références normatives

Les documents de référence suivants sont indispensables pour l'application du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

IEC 61158 (all parts), *Industrial communication networks – Fieldbus specifications* (disponible uniquement en anglais)[3]

IEC 61158-3–14, *Industrial communication networks – Fieldbus specifications – Part 3-14: Data-link layer service definition – Type 14 elements* (disponible uniquement en anglais)

IEC 61158-4-14, *Industrial communication networks – Fieldbus specifications – Part 4-14: Data-link layer protocol specification – Type 14 elements* (disponible uniquement en anglais)

---

1 Dans les pages suivantes de la présente norme, "la présente partie" se substitue à "cette partie de la série CEI 617843".

2 Dans les pages suivantes de la présente norme, "CEI 61508" se substitue à "série CEI 61508".

3 Les publications monolingues des séries IEC 61158 et IEC 61784 sont actuellement en cours de traduction.

IEC 61158-5-14, *Industrial communication networks – Fieldbus specifications – Part 5-14: Application layer service definition – Type 14 elements* (disponible uniquement en anglais)

IEC 61158-6-14, *Industrial communication networks – Fieldbus specifications – Part 6-14: Application layer protocol specification – Type 14 elements* (disponible uniquement en anglais)

CEI 61508 (toutes parties), *Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité*

CEI 61511 (toutes parties), *Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur des industries de transformation*

IEC 61588, *Precision clock synchronization protocol for networked measurement and control systems* (disponible uniquement en anglais)

IEC 61784-2, *Industrial communication networks – Profiles – Part 2: Additional fieldbus profiles for real-time networks based on ISO/IEC 8802-3* (disponible uniquement en anglais)

IEC 61784-3:2010[4], *Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions* (disponible uniquement en anglais)

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* (disponible uniquement en anglais)

3 Termes, définitions, symboles, abréviations et conventions

3.1 Termes et définitions

Pour les besoins du présent document, les termes et définitions suivants s'appliquent.

3.1.1 Termes et définitions communs

3.1.1.1
disponibilité
probabilité, pour un système automatisé, qu'il ne se produise pas de conditions opérationnelles non satisfaisantes, telles que la perte de production, pendant une période donnée

3.1.1.2
canal noir
canal de communication sans preuve existante de conception ou de validation conformément à la CEI 61508

3.1.1.3
pont
dispositif abstrait qui relie des segments de réseau multiples le long de la couche de liaison de données

3.1.1.4
canal de communication
connexion logique entre deux points limites d'un *système de communication*

4 En cours d'élaboration.

3.1.1.5
système de communication
disposition de matériels, logiciels et vecteurs de propagation destinée à permettre la transmission de *messages* (couche application définie dans l'ISO/CEI 7498) d'une application à une autre

3.1.1.6
connexion
liaison logique entre deux objets d'application de dispositifs identiques ou différents

3.1.1.7
contrôle de redondance cyclique (CRC[5])
<valeur> donnée redondante déduite, et enregistrée ou transmise simultanément, d'un bloc de données afin de détecter toute corruption des données

<méthode> procédure utilisée pour calculer les données redondantes

NOTE 1 Les termes « code CRC » et « signature CRC », et les étiquettes telles que CRC1, CRC2, peuvent également être utilisés dans la présente norme pour se référer aux données redondantes.

NOTE 2 Voir également [40], [41][6].

3.1.1.8
erreur
écart ou discordance entre une valeur ou une condition calculée, observée ou mesurée, et la valeur ou la condition vraie, prescrite ou théoriquement correcte

[CEI 61508-4:2010[7]] [CEI 61158]

NOTE 1 Les erreurs peuvent être causées par des erreurs de conception du matériel/logiciel et/ou des informations altérées du fait de perturbations électromagnétiques et/ou autres effets.

NOTE 2 Les erreurs ne produisent nécessairement pas une *défaillance* ou une *panne*.

3.1.1.9
défaillance
cessation de l'aptitude d'une unité fonctionnelle à accomplir une fonction requise ou fonctionnement d'une unité fonctionnelle d'une toute autre manière que celle requise

NOTE 1 La définition de la CEI 61508-4 est identique avec des notes complémentaires.

[CEI 61508-4:2010, modifiée], [ISO/CEI 2382-14.01.11, modifiée]

NOTE 2 Une défaillance peut être causée par une *erreur* (par exemple, problème de conception matérielle/logicielle ou rupture de message).

3.1.1.10
panne
condition anormale susceptible de provoquer la réduction ou la perte de la capacité d'une unité fonctionnelle à accomplir une fonction requise

NOTE Le VEI 191-05-01 définit la « panne » comme un état caractérisé par l'incapacité à accomplir une fonction requise, à l'exclusion de l'incapacité au cours de la période de maintenance préventive ou autres actions planifiées, ou du fait de l'absence de ressources externes.

[CEI 61508-4:2010, modifiée], [ISO/CEI 2382-14.01.11, modifiée]

---

5 CRC = *Cyclic Redundancy Check*

6 Les chiffres entre crochets font référence à la bibliographie.

7 A publier.

3.1.1.11
bus de terrain
système de communication basé sur le transfert de données en série et utilisé dans des applications d'automatisation industrielle ou de commande de processus

3.1.1.12
trame
synonyme discrédité de DLPDU

3.1.1.13
fonction de hachage
fonction (mathématique) de mise en correspondance des valeurs d'un ensemble (éventuellement) très grand de valeurs en une plage de valeurs (habituellement) plus petite

NOTE 1 Les fonctions de hachage peuvent être utilisées pour déterminer l'altération des données.

NOTE 2 Les fonctions de hachage courantes incluent la parité, la somme de contrôle ou le CRC.

[CEI/TR 62210, modifiée]

3.1.1.14
danger
état ou ensemble de conditions d'un système qui, avec d'autres conditions associées, entraîne inévitablement un préjudice pour les personnes, les biens ou l'environnement

3.1.1.15
message
série ordonnée d'octets destinée à communiquer des informations

3.1.1.16
collecteur de messages
partie d'un *système de communication* destiné à recevoir *des* messages

[ISO/CEI 2382-16.02.03]

3.1.1.17
source de messages
partie d'un *système de communication* destiné à envoyer *des* messages

[ISO/CEI 2382-16.02.03]

3.1.1.18
niveau de performance (PL[8])
niveau discret utilisé pour spécifier la capacité des parties relatives à la sécurité des systèmes de commande à accomplir une fonction de sécurité dans des conditions prévisibles

[ISO 13849-1]

3.1.1.19
redondance
existence de moyens, outre les moyens qui se révèleraient suffisants pour qu'une unité fonctionnelle accomplisse une fonction requise ou que des données représentent une information

NOTE La définition de la CEI 61508-4 est identique, avec des exemples et des notes supplémentaires.

[CEI 61508-4:2010, modifiée], [ISO/CEI 2382-14.01.12, modifiée]

8 PL = *Performance Level*

3.1.1.20
fiabilité
probabilité qu'un système automatisé puisse accomplir une fonction requise, dans des conditions données, pendant un intervalle de temps donné (t1, t2)

NOTE 1 On suppose en général que le système automatisé est en état d'accomplir la fonction requise au début de l'intervalle de temps donné.

NOTE 2 Le terme "fiabilité" est aussi employé pour désigner l'aptitude caractérisée par cette probabilité.

NOTE 3 Au cours de la période MTBF ou MTTF, la probabilité qu'un système automatisé exécute une fonction requise dans les conditions données décroît.

NOTE 4 La fiabilité est différente de la disponibilité.

[CEI 62059-11, modifiée]

3.1.1.21
risque
combinaison de la probabilité d'occurrence d'un dommage ou préjudice et de la gravité de ce dernier

NOTE Pour plus d'informations sur ce concept, se reporter à l'Annexe A de la CEI 61508-5:2010[9].

[CEI 61508-4:2010], [ISO/CEI Guide 51:1999, définition 3.2]

3.1.1.22
couche de communication de sécurité (SCL[10])
couche de communication qui comprend toutes les mesures nécessaires permettant d'assurer la transmission de données en toute sécurité conformément aux exigences de la CEI 61508

3.1.1.23
données de sécurité
données transmises par un réseau de sécurité utilisant un protocole de sécurité

NOTE La couche de communication de sécurité ne garantit pas la sécurité des données proprement dites, mais uniquement la transmission en toute sécurité de ces dernières.

3.1.1.24
dispositif de sécurité
dispositif conçu conformément à la CEI 61508 et qui met en œuvre le profil de communication de sécurité fonctionnelle

3.1.1.25
fonction de sécurité
fonction à réaliser par un système E/E/PE relatif à la sécurité ou par un dispositif externe de réduction de risque, prévue pour assurer ou maintenir un état de sécurité de l'EUC par rapport à un événement dangereux spécifique

NOTE La définition de la CEI 61508-4 est identique, avec un exemple et des références supplémentaires.

[CEI 61508-4:2010, modifiée]

3.1.1.26
temps de réponse de la fonction de sécurité
temps écoulé du cas le plus défavorable suite à l'activation d'un capteur de sécurité relié à un bus de terrain, avant que ne soit atteint l'état de sécurité correspondant de son (ses) actionneur(s) de sécurité, du fait d'erreurs ou de défaillances avérées dans le canal de fonction de sécurité

---

9 A publier.

10 SCL = *Safety Communication Layer*

NOTE Ce concept est introduit dans la CEI 61784-3:2010, 5.2.4, et traité par les profils de communication de sécurité fonctionnelle définis dans la présente partie.

3.1.1.27
niveau d'intégrité de sécurité (SIL[11])
niveau discret (un sur quatre niveaux possibles), correspondant à une plage de valeurs d'intégrité de sécurité, où le niveau d'intégrité de sécurité 4 est le niveau le plus élevé et le niveau d'intégrité de sécurité 1 est le niveau le plus faible

NOTE 1 Les mesures de défaillance cible (voir la CEI 61508-4:2010, 3.5.17) applicables aux quatre niveaux d'intégrité de sécurité sont spécifiées dans les Tableaux 2 et 3 de la CEI 61508-1:2010[12].

NOTE 2 Les niveaux d'intégrité de sécurité sont utilisés pour spécifier les exigences d'intégrité de sécurité des fonctions équivalentes à attribuer aux systèmes E/E/PE relatifs à la sécurité.

NOTE 3 Le niveau d'intégrité de sécurité (SIL) n'est pas une propriété d'un système, sous-système, élément ou composant. L'interprétation correcte de l'expression « système relatif à la sécurité avec SILn » (où n est égal à 1, 2, 3 ou 4) signifie que le système est potentiellement capable de prendre en charge des fonctions de sécurité avec un niveau d'intégrité de sécurité jusqu'à n.

[CEI 61508-4:2010]

3.1.1.28
mesure de sécurité
<la présente norme> mesure permettant de contrôler les *erreurs* de communication éventuelles, qui est conçue et mise en œuvre conformément aux exigences de la CEI 61508

NOTE 1 Dans la pratique, plusieurs mesures de sécurité sont combinées pour atteindre le niveau d'intégrité de sécurité requis.

NOTE 2 Les *erreurs* de communication et les mesures de sécurité associées sont détaillées dans la CEI 61784-3:2010, 5.3 et 5.4.

3.1.1.29
application relative à la sécurité
programmes conçus conformément à la CEI 61508 pour satisfaire aux exigences SIL de l'application

3.1.1.30
système relatif à la sécurité
système qui exécute les *fonctions de sécurité* conformément à la CEI 61508

3.1.1.31
datation (horodatage)
informations temporelles incluses dans un *message*

3.1.2 CPF 14: Termes et définitions supplémentaires

3.1.2.1
configuration
définition des connexions et paramètres de communication standard des entités de bus d'une application particulière

NOTE La configuration d'une communication de sécurité comprend la définition de l'Objet de liaison de sécurité fonctionnelle et de l'Objet de gestion de sécurité fonctionnelle des entités de bus relatives à la sécurité d'une application relative à la sécurité particulière.

3.1.2.2
contre-vérification
vérification du caractère identique des données à transmission redondante

---

11 SIL = *Safety Integrity Level*

12 A publier.

3.1.2.3
macro-cycle
une itération du programme de niveau de liaison

3.1.2.4
déguisement
erreur occasionnée par des informations d'identification erronées

3.1.2.5
éditeur
source de message qui transmet des messages de manière régulière

3.1.2.6
abonné
collecteur de messages qui reçoit les messages en provenance d'un éditeur

3.2 Symboles et abréviations

3.2.1 Symboles et abréviations communs

CP	Profil de communication (*Communication Profile*)	[CEI 61784-1]
CPF	Famille de profils de communication (*Communication Profile Family*)	[CEI 61784-1]
CRC	Contrôle de redondance cyclique (*Cyclic Redundancy Check*)	
DLL	Couche de liaison de données (*Data Link Layer*)	[ISO/CEI 7498-1]
DLPDU	Unité de données de protocole de liaison de données (*Data Link Protocol Data Unit*)	
CEM	Compatibilité électromagnétique	
EUC	Equipement commandé (*Equipment Under Control*)	[CEI 61508-4:2010]
E/E/PE	Electrique/électronique/électronique programmable (*Electrical/Electronic/Programmable Electronic*)	[CEI 61508-4:2010]
FAL	Couche Application de bus de terrain (*Fieldbus Application Layer*)	[CEI 61158-5]
FS	Sécurité fonctionnelle (*Functional Safety*)	
FSCP	Profil de communication de sécurité fonctionnelle (*Functional Safety Communication Profile*)	
MTBF	Moyenne des temps de bon fonctionnement entre défaillances (*Mean Time Between Failures*)	
MTTF	Durée moyenne de fonctionnement avant défaillance (*Mean Time To Failure*)	
PDU	Unité de données de protocole (*Protocol Data Unit*)	[ISO/CEI 7498-1]
PFD	Probabilité de défaillance dangereuse sur sollicitation (*Probability of dangerous Failure on Demand*)	[CEI 61508-4:2010[13]]
PFH	Fréquence moyenne de défaillance dangereuse $[h^{-1}]$ par heure (*Average frequency of dangerous failure $[h^{-1}]$ per hour*)	[CEI 61508-4:2010]
PhL	Couche physique (*Physical Layer*)	[ISO/CEI 7498-1]
PL	Niveau de performance (*Performance Level*)	[ISO 13849-1]
PLC	Automate programmable (*Programmable Logic Controller*)	
SCL	Couche de communication de sécurité (*Safety Communication Layer*)	
SIL	Niveau d'intégrité de sécurité (*Safety Integrity Level*)	[CEI 61508-4:2010]

3.2.2 CPF 14: Symboles et abréviations supplémentaires

AP	Processus d'Application (*Application Process*)

13 A publier.

APDU	Unité de données de protocole d'application (*Application Protocol Data Unit*)	
ASE	Elément de service d'application (*Application Service Element*)	
ASIC	Circuit intégré à application spécifique (*Application Specific Integrated Circuit*)	
CSME	Entité de gestion de planification des communications EPA (*EPA Communication Scheduling Management Entity*)	
EPA	Ethernet pour automatisation d'installations (*Ethernet for Plant Automation*)	
EPASafety	Sécurité EPA (*EPA Safety*)	
FB	Bloc de fonctions (*Function Block*)	
FBAP	Processus d'application de blocs de fonctions (*Function Block Application Process*)	
FSPDU	Unité de données de protocole de sécurité fonctionnelle (*Functional Safety Protocol Data Unit*)	
IP	Protocole Internet (*Internet Protocol*)	(RFC 791, voir [37])
DEL	Diode ElectroLuminescente (*Light Emitting Diode*)	
MAC	Couche d'accès au support (*Medium Access Layer*)	
MIB	Base d'information de gestion (*Management Information Base*)	
SN	Numéro de séquence (*Sequence Number*)	
TCP	Protocole de contrôle de transport (*Transport Control Protocol*)	(RFC 793, voir [37])
UDP	Protocole de datagramme d'utilisateur (*User Datagram Protocol*)	(RFC 768, voir [37])
VSCM	Message de contrôle de sécurité virtuel (*Virtual Safety Check Message*)	

3.3 Conventions

La présente partie utilise principalement des organigrammes selon le cas pour décrire des définitions.

4 Vue d'ensemble de FSCP 14/1 (EPASafety®)

4.1 EPASafety®

La famille de profils de communication 14 (communément appelée EPA®[14]) définit des profils de communication sur la base des CEI 61158-3-14, CEI 61158-4-14, CEI 61158—5-14 et CEI 61158-6-14.

Les profils de base CP 14/1 et CP 14/2 sont définis dans la CEI 61784-2. Le profil de communication de sécurité fonctionnelle CPF 14 FSCP 14/1 (EPASafety®[14]) est basé sur les profils de base de CPF 14 spécifiés dans la CEI 61784-2 et les spécifications de la couche de communication de sécurité définies dans la présente partie.

Le système EPA est un réseau Ethernet en temps réel spécifié dans la CEI 61158 et la CEI 61784-2. Le système EPA définit un système de commande de communication déterministe basé sur un réseau Ethernet défini par l'ISO/CEI 8802-3 pour connecter des dispositifs de terrain et de petits systèmes, et pour contrôler/surveiller les équipements industriels.

Le profil EPASafety décrit la spécification de communication sécurisée utilisée pour la connexion des dispositifs et contrôleurs de terrain de sécurité dans les systèmes EPA. Il s'agit d'une technologie complémentaire fondée sur le protocole EPA spécifié dans la CEI 61158 afin de réduire la défaillance ou la probabilité d'erreur de la transmission des

[14] EPA® et EPASafety® désignent les appellations commerciales de Zhejiang SUPCON® Sci&Tech Group Co. Ltd. China. .. Cette information est donnée à l'intention des utilisateurs de la présente Norme internationale et ne signifient nullement que la CEI approuve ou recommande le détenteur de la marque ou de l'un quelconque de ses produits. . La conformité à la présente norme n'exige pas l'emploi des appellations EPA® ou EPASafety®. L'emploi des appellations EPA® or EPASafety® exige l'autorisation de SUPCON®.

données entre les émetteurs-récepteurs de sécurité, les actionneurs et les contrôleurs de terrain au niveau requis par les normes correspondantes, voire un niveau plus élevé.

4.2 Principe des communications de sécurité EPA

La communication EPA repose sur le principe du canal noir tel qu'illustré à la Figure 3. Le canal noir inclut les dispositifs non relatifs à la sécurité tels que les fils, fibres optiques, répéteurs, barrières, alimentations, ASIC (circuits intégrés à application spécifique), piles de communication, ponts EPA, interfaces, etc. La pile de communication comporte les couches suivantes: physique, liaison de données, réseau (IP), transport (UDP) et application.

Des pannes ou des erreurs peuvent se produire au cours du transfert de données dans le canal noir, pour les raisons suivantes:

a) panne aléatoire;

b) défaillance/panne matérielle standard;

c) défaillance système provoquée par des composants matériels ou des composantes logicielles standard.

Dans un système EPASafety, les applications de sécurité et les applications standard partagent simultanément le même canal de communication. La fonction de transmission sécurisée comprend toutes les mesures de détection déterministe de toutes les pannes/tous les dangers potentiels que le système de transmission standard doit infiltrer, ou de maintien de la probabilité d'erreur (faute) résiduelle sous une certaine limite.

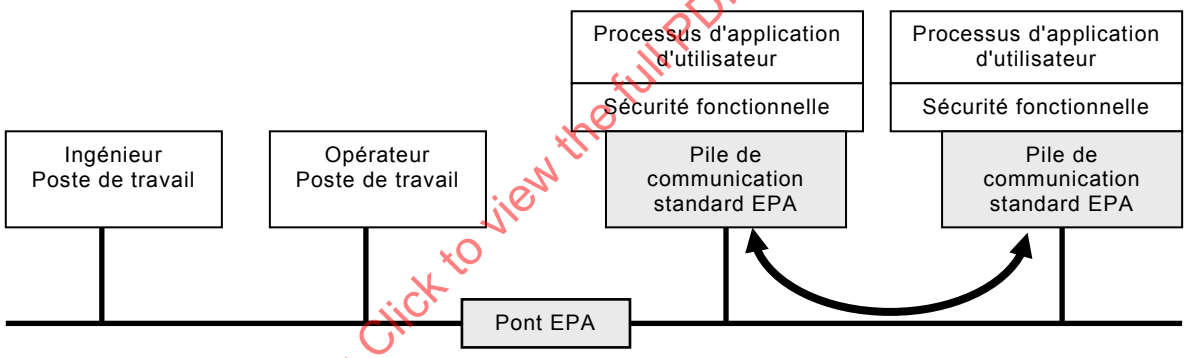


Figure 3 – Architecture de communication de sécurité

4.3 Traitement de la fonction de sécurité

En tant que modèle de processus d'application des blocs de fonctions spécifié dans la CEI 61158, la fonction de sécurité exécutée par le système de communication de sécurité doit être décomposée dans les blocs de fonctions suivants: Données d'entrée sécurisées, Transmission sécurisée, Calcul sécurisé et Données de sortie sécurisées.

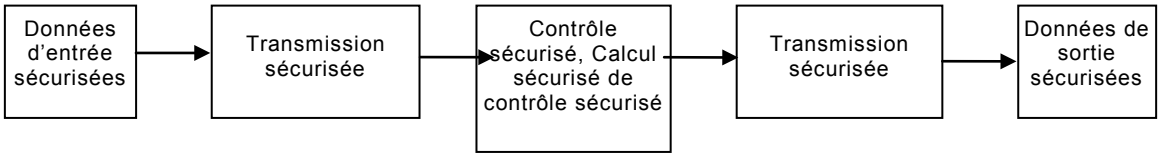


Figure 4 – Traitement de fonction de sécurité

Comme l'illustre la Figure 4, la fonction de sécurité est mise en œuvre comme suit:

a) Le bloc de fonctions d'entrée lit les signaux d'entrée physiques émis par les capteurs et les transfère à la pile de communication de sécurité;

b) La pile de communication de sécurité exécute les services de communication relatifs à la sécurité du dispositif de terrain résident du bloc de fonctions d'entrée (par exemple, émetteur-récepteur relatif à la sécurité EPA);

c) Le dispositif d'entrée transmet les données d'entrée relatives à la sécurité au bloc de fonctions de contrôle du dispositif de calcul de contrôle sécurisé, par l'intermédiaire du canal de transmission de sécurité;

d) La pile de communication de sécurité exécute les services de communication relatifs à la sécurité du dispositif de terrain résident du bloc de fonctions de contrôle sécurisé (par exemple, contrôleur de terrain relatif à la sécurité EPA);

e) Le bloc de contrôle sécurisé procède au contrôle (par exemple, PID) des signaux d'entrée reçus et génère de nouvelles données de sortie de sécurité en fonction du logiciel d'application relatif à la sécurité.

f) Le traitement de la pile de communication de sécurité permet au bloc de fonctions de sortie de lire les données de sortie reçues transmises par le canal de communication, de les transformer en un signal de sortie physique, et de les présenter au bloc d'extrémité d'un dispositif de sortie relatif à la sécurité (par exemple, actionneur relatif à la sécurité EPA).

5 Généralités

5.1 Documents externes de spécifications applicables au profil

Il n'existe aucun document externe concernant les spécifications des profils.

5.2 Exigences fonctionnelles de sécurité

Le concepteur des dispositifs relatifs à la sécurité doit tenir compte des exigences de la CEI 61508.

La communication de sécurité et la communication standard doivent être capables d'utiliser le même canal de communication. Le matériel de transmission ne doit pas être modifié (canal noir). La redondance peut être utilisée non seulement pour une plus grande disponibilité, mais également pour la communication de sécurité.

Les mesures internes aux systèmes de communication FSCP 14/1 visant à réduire les erreurs de transmission potentielles se présentent comme suit:

— Le FSCP 14/1 doit être conçu de manière à permettre aux fournisseurs de développer des produits adaptés à une utilisation dans les applications SIL 3 (CEI 61508);

— le protocole doit prendre en charge la transmission des données de processus et la transmission des données de messagerie entre le dispositif de terrain et le poste de travail;

— le protocole relatif à la sécurité doit éviter les perturbations dues aux dispositifs non relatifs à la sécurité. Par exemple, une unité portative non relative à la sécurité ne doit pas être admise pour modifier les paramètres d'un dispositif relatif à la sécurité;

— le protocole doit assurer une protection contre les changements de configuration involontaires ou non autorisés d'un dispositif de sécurité FSCP 14/1,

— il doit exister un guide d'application FSCP 14/1 destiné à l'utilisateur final afin qu'il mette en œuvre un système relatif à la sécurité utilisant des dispositifs de sécurité FSCP 14/1,

— la contribution du protocole de communication FSCP 14/1 au protocole PFD/PFH doit être inférieure à 1% de la valeur requise par le niveau SIL,

— les calculs PFD/PFH doivent être basés sur les modes à sollicitation faible et à sollicitation élevée respectivement (tel que défini dans la CEI 61508);

— le protocole doit mettre en œuvre les mesures visant à contrôler les anomalies suivantes:

  — erreur sur les bits d'information;

  — répétition non prévue;

  — perte;

  — insertion;

  — séquence incorrecte;

  — déguisement;

  — retard inacceptable;

  — erreur d'adressage;

— le temps de réaction de l'application doit pouvoir être calculé;

— des dispositifs avec des niveaux SIL différents doivent pouvoir être utilisés sur le même réseau;

— le contournement et le maintien sécurisés des dispositifs doivent être possibles;

— l'état hors tension doit être l'état de sécurité principal des dispositifs de sécurité.

5.3 Mesures de sécurité

Les mesures internes aux systèmes de communication FSCP 14/1 visant à réduire les erreurs de transmission potentielles se présentent comme suit:

— numéro de séquence;

— datation (horodatage);

— clé de relation de communication;

— message de réaction;

— contrôle de redondance cyclique et contre-vérification pour l'intégrité des données de sécurité;

— numéro de programmation;

— délai.

La relation entre les mesures de sécurité et les erreurs de communication est définie dans le Tableau 1. Une mesure de sécurité, ou plusieurs mesures, doivent permettre de maîtriser un type d'erreur de communication possible.

Tableau 1 – Relations entre les erreurs et les mesures de sécurité

	Mesures de sécurité							
Erreurs de communication	**Numéro de séquence (voir NOTE 1)**	**Datation (horodatage)**	**Délai**	**Authentification de connexion (voir NOTE 2)**	**Message de réaction**	**Assurance d'intégrité des données**	**Redondance avec contre-vérification**	**Différents systèmes d'assurance d'intégrité des données**
Corruption						X	X	
Répétition non prévue	X	X						
Séquence incorrecte	X	X						
Perte	X				X			
Retard inacceptable		X	X					
Insertion	X			X	X			
Déguisement				X	X			X
Adressage				X				

NOTE 1 Le numéro de séquence comporte deux parties. L'une de ces parties est le numéro de séquence, l'autre partie étant le numéro de programmation. Le numéro de séquence est intégré dans les messages échangés entre la source et le collecteur du message. Il peut prendre la forme d'un champ de données supplémentaire dont le numéro varie d'un message à l'autre de manière prédéterminée. Le numéro de programmation est dédié à l'ordre de transmission du message des dispositifs dans chaque macro-cycle.

NOTE 2 L'authentification de connexion est mise en œuvre comme clé de relation de communication.

Le message est un bloc compact dont la datation est l'heure locale de l'émetteur, et comportant par ailleurs le numéro de séquence, la clé de relation et la somme de contrôle CRC.

5.4 Structure de la couche de communication de sécurité

5.4.1 Combinaison des systèmes de communication standard et de communication de sécurité

La Figure 5 montre l'architecture système incluant les dispositifs standard et les dispositifs de sécurité. Généralement, le système est constitué de dispositifs hôtes CP 14/1 (par exemple, station de fonctionnement ou station technique), contrôleurs de terrain de sécurité, actionneurs de sécurité, émetteurs-récepteurs de sécurité, actionneurs standard et émetteurs-récepteurs standard interconnectés sur un micro-segment CP 14/1.

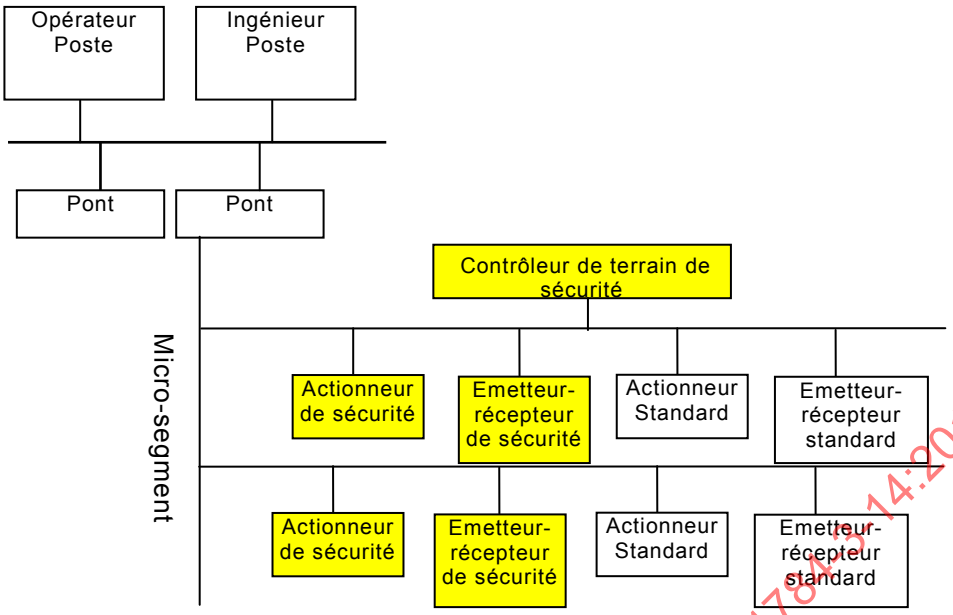


Figure 5 – Communication standard et communication de sécurité

Dans le cas présent, les communications de sécurité et les communications standard doivent partager le même support de transmission. Les émetteurs-récepteurs et les actionneurs de sécurité transmettent ou reçoivent les données relatives à la sécurité. Les émetteurs-récepteurs et les actionneurs standard transmettent ou reçoivent les données non relatives à la sécurité tandis que les contrôleurs de terrain de sécurité doivent recevoir, transmettre et traiter tant les données relatives que non relatives à la sécurité. C'est-à-dire que les contrôleurs de terrain de sécurité doivent prendre en charge tant les services de communication de sécurité que les services de communication standard.

5.4.2 Structure de la communication de sécurité CP 14/1

Le profil étendu de communication de sécurité fonctionnelle FSCP 14/1 se situe dans la couche application, et représente la couche supérieure de l'Entité de mappage de ports de connexion (Socket Mapping Entity) et de l'Entité de couche application standard (Standard Application Layer Entity). L'architecture peut produire une certaine indépendance entre la communication standard et la communication de sécurité, et assurer la sécurité fonctionnelle des messages de sécurité. L'architecture ne modifie également pas la structure et la qualité de fonctionnement du système d'origine. Les dispositifs de sécurité et standard doivent fonctionner dans le même réseau.

Le profil étendu de communication de sécurité fonctionnelle FSCP 14/1 se situe au-dessus de la pile de communication (comprend une Entité de couche application standard, une Entité de mappage de ports de connexion, un protocole UDP/IP, une Entité de gestion de programme de communication (Communication Schedule Management Entity), une couche de liaison de données Ethernet (Ethernet Data Link Layer) et une couche physique), et sous la couche utilisateur FBAP. La hiérarchie de protocole de la communication de sécurité CP 14/1 et FSCP 14/1 est illustrée à la Figure 6.

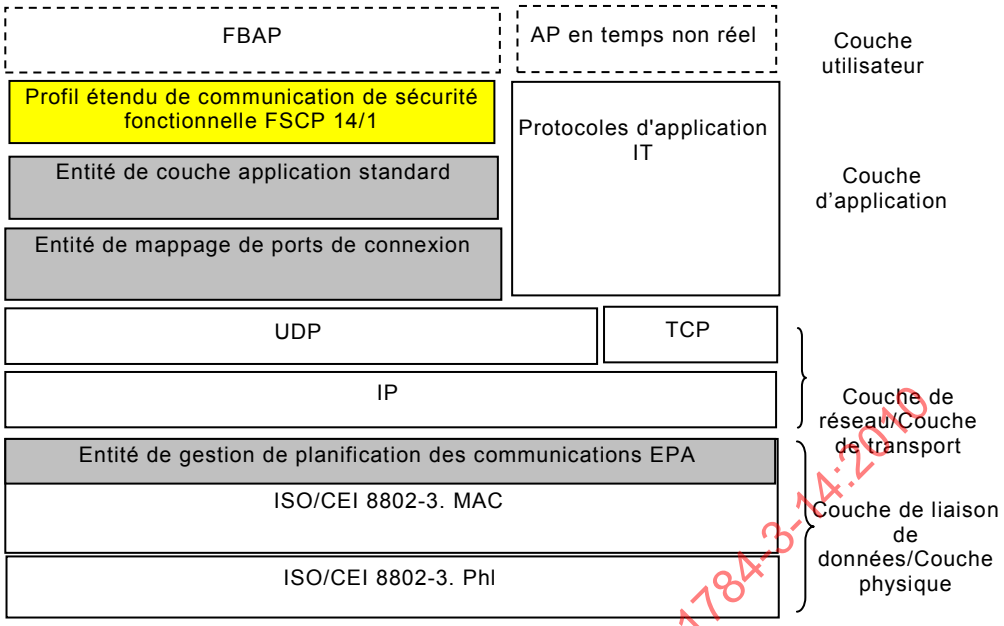


Figure 6 – Hiérarchie de protocole CP 14/1

La pile de communication permet d'obtenir les données de sécurité du protocole de communication fonctionnelle, de générer un message standard avec un en-tête et des données de sécurité standard, et de transférer le message standard au protocole UDP/IP. La pile de communication permet d'autre part d'obtenir le message standard du protocole UPD/IP, de décoder ledit message et de transférer les données de sécurité au protocole de communication de sécurité fonctionnelle.

Le protocole de communication de sécurité fonctionnelle permet d'obtenir les données utilisateur, de coder ces mêmes données avec une mesure de sécurité (telle que contrôle CRC, pile horaire et numéro de séquence) en données de sécurité, et de transférer ces mêmes données à la pile de communication avec une interface. Le protocole de communication de sécurité fonctionnelle permet d'autre part d'obtenir les données de sécurité émises par la pile de communication, de décoder ces mêmes données en données utilisateur et de gérer le service associé.

5.5 Relations avec la FAL (et DLL, PhL)

5.5.1 Vue d'ensemble

La Figure 7 illustre la relation entre la couche de communication de sécurité (SCL) et les autres couches de CP14/1.

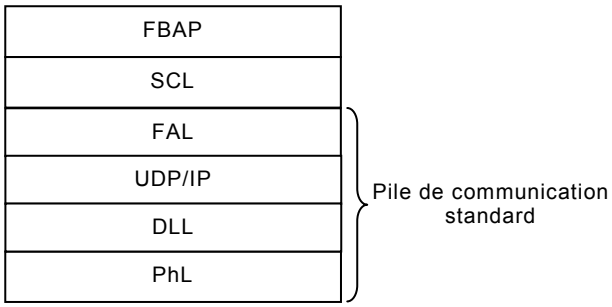


Figure 7 – Relation entre la SCL et les autres couches de CP 14/1

5.5.2 Types de données

Le protocole FSCP 14/1 prend en charge tous les types de données tel que défini dans la CEI 61158-5-14 (voir Tableau 2).

Tableau 2 – Types de données utilisés dans le cadre du protocole FSCP 14/1

Nom du type de données	Nombre d'octets
Integer8	1
Integer16	2
Integer32	4
Unsigned8 (utilisé comme bits)	1
Unsigned16 (utilisé comme bits)	2
Unsigned32 (utilisé comme bits)	4
Unsigned16	2
Unsigned32	4
Floating Point (virgule) 32	4
Date	
TimeOfDay avec indication de date	
TimeOfDay sans indication de date	
TimeDifference avec indication de date	
TimeDifference sans indication de date	
Visible String (Chaîne visible)	1,2,3, …

6 Services de la couche de communication de sécurité

6.1 Vue d'ensemble

Le présent paragraphe définit l'extension des objets existants et les services étendus de l'Entité de la couche application standard CP 14/1 pour le protocole FSCP 14/1. Les objets étendus sont archivés dans la MIB (Base d'informations de gestion) des dispositifs. Ces objets permettent de définir le comportement de la communication de sécurité et l'action entreprise en cas d'erreur de communication effective. Les services de communication de sécurité permettent d'ouvrir ou de fermer une communication de sécurité entre les dispositifs hôtes et de sécurité.

6.2 Extensions des objets FSCP 14/1

6.2.1 Généralités

Le présent paragraphe décrit les objets supplémentaires (tel qu'indiqué dans le Tableau 3) contenus dans la MIB des dispositifs et utilisés dans les dispositifs pertinents FSCP 14/1.

Tableau 3 – Extensions des objets FSCP 14/1

Objet	ID de l'objet	Illustration
Objet de gestion de communication de sécurité fonctionnelle (Functional safety communication management object)	10	Objet de gestion de communication FSCP 14/1
Objet d'alerte de communication de sécurité fonctionnelle (Functional safety communication alert object)	11	Objet d'alerte de communication de sécurité fonctionnelle
Objet de liaison de sécurité fonctionnelle 1 (Functional Safety Link object 1)	6 000	Objet de liaison de sécurité fonctionnelle 1
Objet de liaison de sécurité fonctionnelle 2 (Functional Safety Link object 2)	6 001	Objet de liaison de sécurité fonctionnelle 2
.....		

6.2.2 Objet de gestion de communication de sécurité fonctionnelle

6.2.2.1 Généralités

Pour la communication non périodique, l'objet de gestion de communication de sécurité fonctionnelle est ajouté à la base de gestion des informations.

6.2.2.2 Modèle de forme

ASE: **SYSTEM MANAGEMENT ASE**
CLASS: **FUNCTIONAL Safety COMM MANAGEMENT OBJECT**
CLASS ID: **Non utilisé**
PARENT CLASS: **TOP**
ATTRIBUTES:

1 (m) Attribut clé: Object ID (ID de l'objet)
2 (m) Attribut: Max Nonperiodic Channel Number (Nombre maximal de canaux non périodiques)
3 (m) Attribut: Free Nonperiodic Channel Number (Nombre de canaux libres non périodiques)
4 (m) Attribut: MaxResponseTime (Temps de réponse maximal)
5 (m) Attribut: Service Option (Option de service)

SERVICES:

1 (o) Service Ops: Lecture
2 (o) Service Ops: Ecriture
3 (o) Service Ops: SafetyCommunicationClose
4 (o) Service Ops: SafetyCommunicationOpen

6.2.2.3 Attribut

Object ID

Cet attribut identifie l'objet de gestion de communication de sécurité fonctionnelle dans la MIB des dispositifs CP 14/1. Sa valeur est 10. Ce type de données d'attribut est Unsigned16, et le droit d'accès est Lecture seule.

Max Nonperiodic Channel Number

Cet attribut spécifie le nombre maximal de canaux non périodiques pris en charge par le dispositif. Ce type de données d'attribut est Unsigned8, et le droit d'accès est Lecture seule.

Free Nonperiodic Channel Number

Cet attribut spécifie la valeur actuelle du nombre de canaux libres non périodiques dans le dispositif. Ce type de données d'attribut est Unsigned8, et le droit d'accès est Lecture seule.

MaxResponseTime

Cet attribut spécifie le temps de réponse maximal entre la transmission de la demande du service et la réception de la réponse du service. Si la réponse n'a pas été reçue dans le MaxResponseTime, le demandeur considère qu'une défaillance de communication s'est produite et réitère à trois reprises la même demande de service. Son type de données est de 4 octets de TimeDifference, et le droit d'accès est Lecture et Ecriture.

Service Option

Cet attribut spécifie les types de services pris en charge par la couche de sécurité FSCP 14/1. Ce type de données d'attribut est Unsigned16, et le droit d'accès est Lecture et Ecriture. Il peut être défini par l'application de l'utilisateur:

Bit 0—— Service Diffusion;

Bit 1—— Service Lecture;

Bit 2—— Service Ecriture;

Bit 3—— Service Notification d'événements;

Bit 4—— Service Acquittement de notification d'événements;

Bit 5—— Service Téléchargement vers l'amont de domaines;

Bit 6—— Service Téléchargement vers l'aval de domaines;

Autre——réservé.

6.2.2.4 Service

Lecture

Ce service facultatif assure la lecture de l'attribut de l'Objet de configuration de sécurité fonctionnelle. Le service Lecture est défini dans la CEI 61158-5-14.

Ecriture

Ce service facultatif permet aux utilisateurs de configurer les attributs de l'Objet de configuration de sécurité fonctionnelle. Le service Ecriture est défini dans la CEI 61158-5-14.

SafetyCommunicationOpen

Ce service facultatif permet aux utilisateurs d'initialiser la valeur de l'Objet de gestion de communication de sécurité fonctionnelle. Le service SafetyCommunicationOpen est défini en 6.3.2.

SafetyCommunicationClose

Ce service facultatif permet aux utilisateurs de réinitialiser la valeur de l'Objet de gestion de communication de sécurité fonctionnelle. Le service SafetyCommunicationClose est défini en 6.3.3.

6.2.3 Objet de liaison de sécurité fonctionnelle

6.2.3.1 Généralités

L'Objet de liaison de sécurité fonctionnelle est l'extension de l'objet de liaison défini dans la CEI 61158-5-14. Il spécifie la relation de communication pour une transmission de données périodique.

6.2.3.2 Modèle de forme

ASE:	**APPLICATION RELATIONSHIP ASE**
CLASS:	**FUNCTIONAL SAFETY LINK OBJECT**
CLASS ID:	**Non utilisé**
PARENT CLASS:	**TOP**

ATTRIBUTES:

1	(m)	Attribut clé:	Object ID
2	(m)	Attribut:	Local Appd ID (ID d'application locale)
3	(m)	Attribut:	Local Object ID (ID d'objet local)
4	(m)	Attribut:	Remote App ID (ID d'application distante)
5	(m)	Attribut:	Remote Object ID (ID d'objet distant)
6	(m)	Attribut:	ServiceOperation (Fonctionnement du service)
7	(m)	Attribut:	Service Role (Rôle du service)
8	(m)	Attribut:	Remote IP Address (Adresse IP distante)
9	(m)	Attribut:	Send Time Offset (Décalage du temps de transmission)
10	(m)	Attribut:	Configured Scheduling Number (Nombre de programmation configuré)
11	(m)	Attribut:	Scheduling Precision Requirement (Exigence de précision de programmation)
12	(m)	Attribut:	RelationKey
13	(m)	Attribut:	LinkageFault
14	(m)	Attribut:	FaultReportConfiguration
15	(m)	Attribut:	FaultAcknowledgeConfiguration

SERVICES:

1	(o)	Service Ops:	Lecture
2	(o)	Service Ops:	Ecriture
3	(o)	Service Ops:	SafetyCommunicationClose
4	(o)	Service Ops:	SafetyCommunicationOpen

6.2.3.3 Attribut

Object ID

Cet attribut identifie l'Objet de liaison de sécurité fonctionnelle dans la MIB. Le numéro de ObjectID de l'Objet de liaison doit être désigné en série. Son type de données est Unsigned16, et le droit d'accès est Lecture.

LocalAppID

Cet attribut identifie l'instance FB locale. Son type de données est Unsigned16, et le droit d'accès est Lecture et Ecriture.

Local Object ID

Cet attribut identifie l'objet variante locale. Son type de données est Unsigned16, et le droit d'accès est Lecture et Ecriture.

Remote App ID

Cet attribut identifie l'instanciation FB distante. Son type de données est Unsigned16, et le droit d'accès est Lecture et Ecriture.

RemoteObjectID

Cet attribut identifie l'objet variante distante. Son type de données est Unsigned16, et le droit d'accès est Lecture et Ecriture.

ServiceOperation

Cet attribut spécifie le service d'application à utiliser dans la relation de communication appropriée:

0——liaison locale, aucun service d'application n'est utilisé;

1 à 23—— Le ServiceID des services d'application est utilisée;

Autres—— service non valide.

Son type de données est Unsigned8, et le droit d'accès est Lecture et Ecriture.

ServiceRole

Cet attribut définit le rôle AREP du dispositif local dans le processus de communication:

0——SENDER, indique que le rôle AREP du dispositif local est CLIENT ou PUBLISHER;

1——RECEIVER, indique que le rôle AREP du dispositif local est SERVER ou SUBSCRIBER:

Autres——L'Objet Liaison est invalide, et 0xFF indique que l'Objet de liaison n'est pas configuré ou qu'il a été supprimé.

Son type de données est Unsigned8, et le droit d'accès est Lecture et Ecriture.

RemoteIPAddress

Cet attribut identifie l'adresse IP du dispositif distant. Cet attribut doit être ignoré si l'objet d'instanciation FB local et l'objet d'instanciation FB distant sont présents dans le même dispositif. Son type de données est Unsigned32, et le droit d'accès est Lecture et Ecriture.

SendTimeOffset

Cet attribut définit le décalage temporel lorsque le message approprié doit être transmis à partir du temps de démarrage d'un macro-cycle de communication. Cet attribut est valide lorsque ServiceID est 0x0E (DISTRIBUTE) et ServiceRole est 0x00. Son type de données est de 4 octets de TimeDifference, et le droit d'accès est Lecture et Ecriture.

Configured Scheduling Number

Cet attribut spécifie le numéro de séquence dans un macro-cycle afin que le dispositif local transmette les données relatives à cet objet de liaison de sécurité fonctionnelle. Son type de données est Unsigned16, et le droit d'accès est Lecture et Ecriture.

Scheduling Precision Requirement

Cet attribut indique la précision du temps de transmission des données prévues pour le dispositif local. Il peut être défini par l'application de l'utilisateur:

0——aucune exigence de précision;

1——précision du temps de transmission des données < 1 s;

2——précision du temps de transmission des données < 100 ms;

3——précision du temps de transmission des données < 10 ms;

4——précision du temps de transmission des données < 1 ms;

5——précision du temps de transmission des données < 100 µs;

6——précision du temps de transmission des données < 10 µs;

7——précision du temps de transmission des données < 1 µs.

Son type de données est Unsigned16, et le droit d'accès est Lecture et Ecriture.

RelationKey

Cet attribut spécifie la valeur actuelle de RelationKey pour l'objet de liaison FS.

Son type de données est Unsigned32, et le droit d'accès est SafetyCommunicationOpen et SafetyCommunicationClose.

LinkageFault

Cet attribut est défini de manière à consigner les anomalies de communication actuelles. Il peut être défini par l'application de l'utilisateur:

Bit 0——état de liaison;

Bit 1——état de consignation des anomalies;

Bit 2——état d'acquittement des anomalies;

Autre——réservé.

Son type de données est Unsigned16, et le droit d'accès est Lecture et Ecriture.

FaultReportConfiguration

Cet attribut est défini de manière à déterminer s'il y a lieu ou non de signaler l'anomalie de communication à l'application particulière. Il peut être défini par l'application de l'utilisateur:

0——signaler l'anomalie de communication;

1——ne pas signaler l'anomalie de communication;

Autre——réservé.

Son type de données est Unsigned8, et le droit d'accès est Lecture et Ecriture.

FaultAcknowledgeConfiguration

Cet attribut est défini de manière à déterminer si l'anomalie de communication est acquittée ou non par l'application particulière. Il peut être défini par l'application de l'utilisateur:

0——l'anomalie de communication doit être acquittée;

1——l'anomalie de communication ne doit pas être acquittée;

Autre——réservé.

Son type de données est Unsigned8, et le droit d'accès est Lecture et Ecriture.

6.2.3.4 Service

Lecture

Ce service facultatif assure la lecture de l'attribut de l'Objet de configuration de sécurité fonctionnelle. Le service Lecture est défini dans la CEI 61158-5-14.

Ecriture

Ce service facultatif permet aux utilisateurs de configurer les attributs de l'Objet de configuration de sécurité fonctionnelle. Le service Ecriture est défini dans la CEI 61158-5-14.

SafetyCommunicationOpen

Ce service facultatif permet aux utilisateurs d'initialiser la valeur de RelationKey de l'Objet de liaison de sécurité fonctionnelle. SafetyCommunicationOpen est défini en 6.3.2.

SafetyCommunicationClose

Ce service facultatif permet aux utilisateurs de réinitialiser la valeur de RelationKey de l'Objet de liaison de sécurité fonctionnelle. SafetyCommunicationClose est défini en 6.3.3.

6.2.4 Objet d'alerte de communication de sécurité fonctionnelle

6.2.4.1 Généralités

Chaque dispositif de sécurité fonctionnelle a un seul Objet d'alerte de sécurité fonctionnelle, qui est utilisé pour transmettre la défaillance de communication à l'application particulière.

6.2.4.2 Modèle de forme

ASE: SYSTEM MANAGEMENT ASE

CLASS: **FUNCTIONAL SAFETY COMM ALERT OBJECT**
CLASS ID: **Non utilisé**
PARENT CLASS: **TOP**
ATTRIBUTES:

1	(m)	Attribut clé:	Object ID
2	(m)	Attribut:	Total Fault Counter (Compteur du nombre total d'anomalies)
3	(o)	Attribut:	Local Fault Recorders (Enregistreurs d'anomalies locales)
3.1	(m)	Attribut:	CRC Error Counter (Compteur d'erreurs CRC)
3.2	(m)	Attribut:	Sequence Error Counter (Compteur d'erreurs de séquence)
3.3	(m)	Attribut:	Time Delay Counter (Compteur de retard)
3.4	(m)	Attribut:	Time Synchronize Error Counter (Compteur d'erreurs de synchronisation temporelle)
3.5	(m)	Attribut:	Communication Scheduling Error Counter (Compteur d'erreurs de programmation de communication)

SERVICES:

1	(o)	Service Ops:	Lecture (Read)
2	(o)	Service Ops:	EventNotification
3	(o)	Service Ops:	AcknowledgeEventNotification

6.2.4.3 Attribut

Object ID

Cet attribut identifie l'Objet d'alerte de sécurité fonctionnelle dans la MIB du dispositif. Sa valeur est 11. Ce type de données d'attribut est Unsigned16, et le droit d'accès est Lecture seule.

Total Fault Counter

Cet attribut spécifie le compteur de toutes les anomalies de communication à détecter. Son type de données est Unsigned16, et le droit d'accès est Lecture seule.

Local Fault Recorders

Cet attribut spécifie les enregistreurs de chaque anomalie de communication à détecter. Son type de données est Unsigned16, et le droit d'accès est Lecture seule.

CRC Error Counter

Cet attribut spécifie les enregistreurs des erreurs CRC à détecter. Son type de données est Unsigned16, et le droit d'accès est Lecture seule.

Sequence Error Counter

Cet attribut spécifie les enregistreurs des erreurs de séquence à détecter. Son type de données est Unsigned16, et le droit d'accès est Lecture seule.

Time Delay Counter

Cet attribut spécifie les enregistreurs de retard à détecter. Son type de données est Unsigned16, et le droit d'accès est Lecture seule.

Time Synchronize Error Counter

Cet attribut spécifie les enregistreurs d'erreurs de synchronisation temporelle à détecter. Son type de données est Unsigned16, et le droit d'accès est Lecture seule.

Communication Scheduling Error Counter

Cet attribut spécifie les enregistreurs d'erreurs de programmation de communication à détecter. Son type de données est Unsigned16, et le droit d'accès est Lecture seule.

6.2.4.4 Service

Lecture

Ce service facultatif assure la lecture de l'attribut de l'Objet de liaison de sécurité fonctionnelle. Le service Lecture est défini dans la CEI 61158-5-14.

EventNotification

Ce service facultatif permet au dispositif de sécurité de transmettre la défaillance de communication à l'hôte spécial déterminé par l'Objet de liaison de sécurité fonctionnelle. Le service EventNotification est défini dans la CEI 61158-5-14.

AcknowledgeEventNotification

Ce service facultatif permet à l'hôte spécial d'acquitter l'alerte de la défaillance de communication du dispositif défaillant. Le service AcknowledgeEventNotification est défini dans la CEI 61158-5-14.

6.3 Services étendus

6.3.1 Généralités

Le Tableau 4 définit des services supplémentaires à utiliser dans les dispositifs de sécurité. L'indice et le ServiceID sont spécifiés dans la CEI 61158-5-14.

Tableau 4 – Extension de services de sécurité fonctionnelle

Indice	Nom du service	ServiceID	Confirmé / Non confirmé	Priorité	Description du service
19	SafetyCommunicationOpen	18	Confirmé	2	Initialiser la relation de liaison de la communication de sécurité fonctionnelle
20	SafetyCommunicationClose	19	Confirmé	2	Fermer la relation de liaison de la communication de sécurité fonctionnelle

6.3.2 SafetyCommunicationOpen

6.3.2.1 Généralités concernant le service

Le service SafetyCommunicationOpen est un service confirmé. Ce service est utilisé pour activer la relation de communication de sécurité fonctionnelle.

6.3.2.2 Primitives de service

Les paramètres de service applicables au service SafetyCommunicationOpen sont présentés dans le Tableau 5.

Tableau 5 – Paramètres du service SafetyCommunicationOpen

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

Argument

L'argument contient les paramètres de ce service.

MessageID

Ce paramètre contient le numéro invoqué de ce service. A chaque invocation de ce service, la valeur de ce paramètre est augmentée en ajoutant 1.

SourceAppID

Ce paramètre contient l'identifiant de l'instanciation FB de source.

Source IP Address

Ce paramètre contient l'adresse IP source à laquelle la demande de service doit être transmise.

Destination IP Address

Ce paramètre contient l'adresse IP de destination à laquelle la demande de service doit être transmise.

RelationKey

Ce paramètre contient la valeur de RelationKey pour le canal de communication. Chaque canal non périodique de sécurité applique une RelationKey de 32 bits uniquement.

CommunicationType

Ce paramètre contient le type de communication:

0——Type d'objet de liaison;

1——Type d'objet de communication;

Autre——réservé.

LinkObjectID

Ce paramètre contient l'ID de l'Objet de liaison qui doit être configuré afin de s'appliquer à la communication de sécurité fonctionnelle.

AccessRight

Ce paramètre contient le droit d'accès nécessaire au canal de communication.

0——Lecture seule, le canal de communication de sécurité est en lecture seule;

1——Accessible en écriture, le canal de communication de sécurité est accessible en écriture;

Autres—— non valide.

Result(+)

Ce paramètre facultatif indique l'aboutissement positif (succès) de la demande de service.

DestinationAppID

Ce paramètre contient l'identifiant de l'instanciation FB de destination.

Result(-)

Ce paramètre facultatif indique l'aboutissement négatif (échec) de la demande de service.

ErrorType

Ce paramètre contient la raison de la défaillance.

6.3.2.3 Procédure de service

La procédure de service confirmée spécifiée dans la CEI 61158-5-14 s'applique à ce service.

6.3.3 SafetyCommunicationClose

6.3.3.1 Généralités concernant le service

Le service SafetyCommunicationClose est un service confirmé. Ce service est utilisé pour désactiver le canal de communication de sécurité fonctionnelle.

6.3.3.2 Primitives de service

Les paramètres de service applicables au service SafetyCommunicationClose sont présentés dans le Tableau 6.

Tableau 6 – Paramètres du service SafetyCommunicationClose

Nom du paramètre	.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

L'argument contient les paramètres de ce service.

MessageID

Ce paramètre contient le numéro invoqué de ce service. A chaque invocation de ce service, la valeur de ce paramètre est augmentée en ajoutant 1.

SourceAppID

Ce paramètre contient l'identifiant de l'instanciation FB de source.

Source IP Address

Ce paramètre contient l'adresse IP source à laquelle la demande de service doit être transmise.

Destination IP Address

Ce paramètre contient l'adresse IP de destination à laquelle la demande de service doit être transmise.

LinkObjectID

Ce paramètre contient l'ID de l'Objet de liaison qui doit être réinitialisé selon une communication normale. Si le LinkObjectID est 0x0000, cela signifie que le service souhaite fermer l'objet de communication.

Result(+)

Ce paramètre facultatif indique l'aboutissement positif (succès) de la demande de service.

DestinationAppID

Ce paramètre contient l'identifiant de l'instanciation FB de destination.

Result(-)

Ce paramètre facultatif indique l'aboutissement négatif (échec) de la demande de service.

ErrorType

Ce paramètre contient la raison de la défaillance.

6.3.3.3 Procédure de service

La procédure de service confirmée spécifiée dans la CEI 61158-5-14 s'applique à ce service.

7 Protocole de couche de communication de sécurité

7.1 Format PDU de sécurité

7.1.1 Généralités

La Figure 8 illustre la structure des messages de communication de sécurité fonctionnelle, y compris le type de protocole CP 14/1, les en-têtes IP, UDP et APDU, ainsi que la PDU de sécurité fonctionnelle redondante (FSPDU).

Le message de transmission de sécurité fonctionnelle suit le format de message standard.

TYPE	En-tête IP	En-tête UDP	En-tête APDU	FSPDU redondante

Figure 8 – Structure de message de communication de sécurité fonctionnelle

7.1.2 Structure d'en-tête APDU

La structure de l'en-tête APDU est présentée dans le Tableau 7.

Tableau 7 – Codage de l'en-tête APDU

N°	Nom du paramètre	Type de données	Décalage d'octet	Longueur en octets	Description
1	ServiceID	Unsigned8	0	1	Ce paramètre décrit le type de service et de message. Le bit 7 à 6 indique le type de message: 00 – message de demande 01 – message de réponse 10 – message d'erreur 11 – réservé Les six bits les plus faibles utilisés pour signifier l'ID de service.
2	CommType	Unsigned8	1	1	0 – communication standard 1 – communication de sécurité Autres – réservé
3	Réservé (Reserved)	OctetString	2	2	Non utilisé
4	Longueur (Length)	Unsigned16	4	2	Ce paramètre décrit la longueur du message entier
5	MessageID	Unsigned16	6	2	Ce paramètre décrit l'ID du message

7.1.3 PDU de sécurité fonctionnelle

La PDU de sécurité fonctionnelle (FSPDU) se compose du CRC, de l'en-tête de sécurité fonctionnelle et des UserData standard (voir Figure 9).

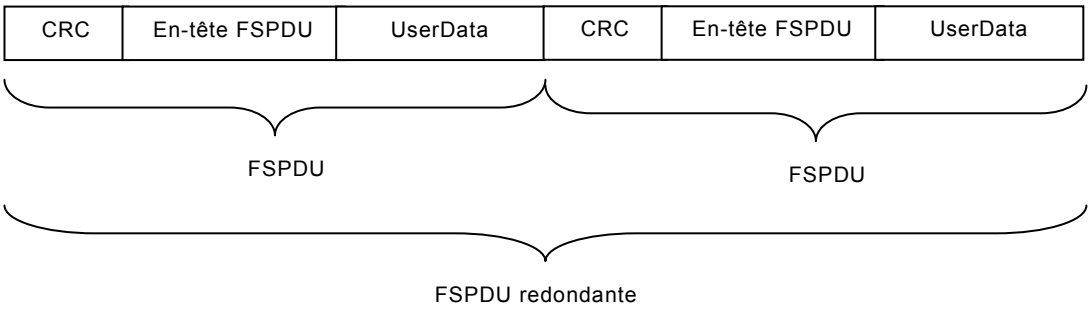


Figure 9 – Structure de la PDU de sécurité fonctionnelle (FSPDU)

Le code de contrôle CRC est calculé par les algorithmes de contrôle CRC sur le message de contrôle de sécurité virtuel (VSCM) qui se compose de la RelationKey, du numéro de séquence, du numéro de programmation, de la datation et des données utilisateur d'origine. La structure des données du VCSM est présentée à la Figure 10.

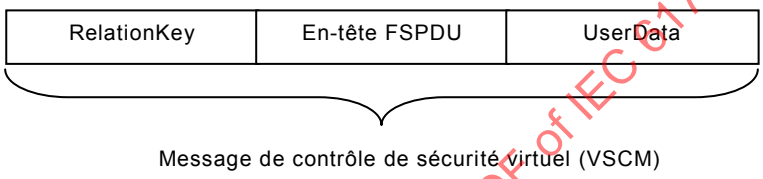


Figure 10 – Structure du message de contrôle de sécurité virtuel (VCSM)

La structure de l'en-tête de la PDU de sécurité fonctionnelle (FSPDU) est définie dans le Tableau 8.

Tableau 8 – Structure de l'en-tête de la PDU de sécurité fonctionnelle (FSPDU)

Indice	Nom du paramètre	Type de données	Décalage d'octet	Longueur en octets	Description
1	SequenceNumber	Unsigned16	0	2	Numéro de séquence
2	SchedulingNumber	Unsigned16	2	2	Numéro de programmation
3	TimeStamp	BinaryDate	4	8	Heure en cours de la FSPDU

La mise en correspondance (mappage) des PDU de sécurité fonctionnelle est illustrée à la Figure 11.

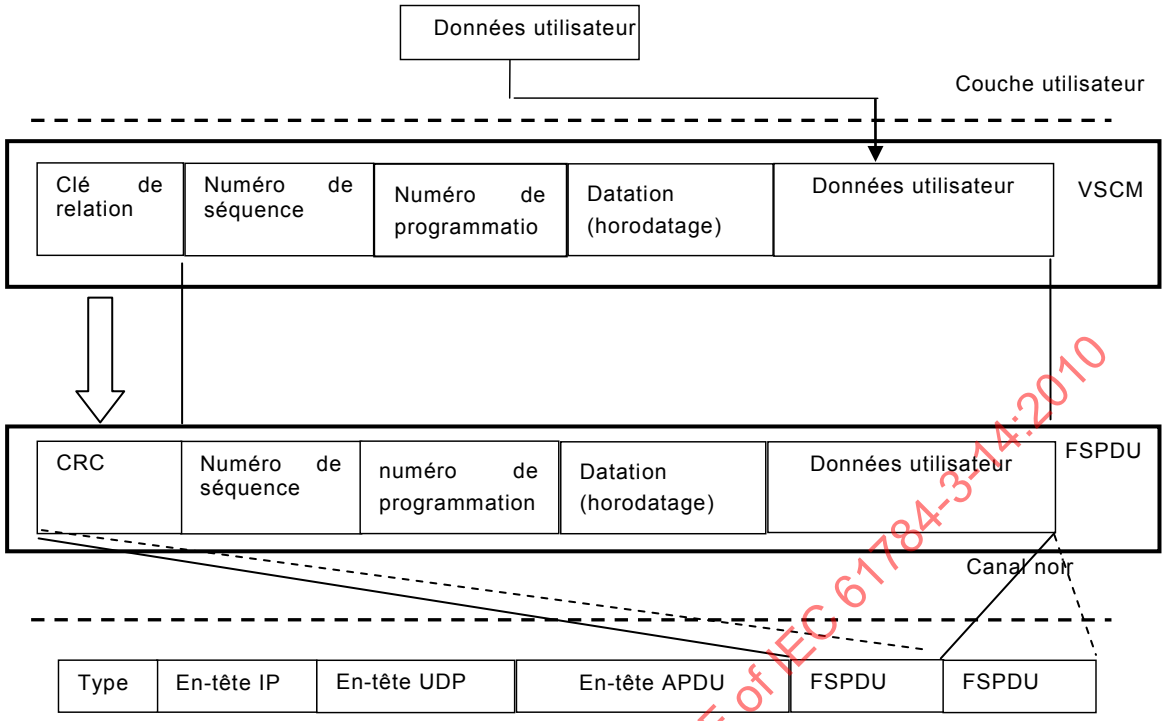


Figure 11 – Mise en correspondance FSPDU

7.2 Fonctionnement de la communication de sécurité

7.2.1 Numéro de séquence

Un numéro de séquence est utilisé pour la transmission de données périodiques afin d'assurer la traçabilité de la transmission des données de processus, ainsi que pour la détection des erreurs de communication, telles que la perte, la répétition et une séquence incorrecte.

Un numéro de séquence est utilisé principalement pour la transmission de données non périodiques afin d'assurer la traçabilité de la transmission des données continues, ainsi que pour la détection des erreurs de communication, telles que la perte, la répétition et une séquence incorrecte.

La valeur initiale du numéro de séquence est fixée à 0, la valeur étant augmentée en ajoutant 1 à chaque transmission de FSPDU au canal noir.

7.2.2 RelationKey

7.2.2.1 Généralités

RelationKey est initialisée par un outil de configuration. Elle n'est pas transmise une fois le processus de configuration achevé, mais participe uniquement à l'élaboration du VSCM. Le type de données de RelationKey est une OctetString de 32 bits.

7.2.2.2 Configuration et initialisation

Lors de la configuration du système, l'outil de configuration doit spécifier l'attribut RelationKey des objets de liaison de sécurité fonctionnelle pour chaque dispositif relatif à la sécurité qui utilise le service Ecriture défini dans la CEI 61158-5-14.

Après réception de la demande SafetyCommunicationOpen, chaque dispositif relatif à la sécurité doit obtenir une valeur d'initialisation pour l'attribut RelationKey applicable à une communication non périodique selon les paramètres de la demande SafetyCommunicationOpen.

7.2.2.3 Fonctionnement

Chaque objet de liaison de sécurité et chaque canal non périodique de sécurité appliquent uniquement une RelationKey de 32 bits dans un micro-segment.

Lors de la génération d'une PDU de sécurité fonctionnelle (FSPDU), l'émetteur relatif à la sécurité doit utiliser la RelationKey pour générer la valeur du segment CRC de la FSPDU tel qu'illustré en 7.1.3. La RelationKey ne doit pas figurer dans le codage de la FSPDU.

Lors de la réception de la FSPDU, le dispositif relatif à la sécurité doit générer une valeur CRC locale, au moyen d'un segment VSCM et d'une RelationKey. Seule la valeur CRC locale est égale à la valeur du segment CRC dans la FSPDU, les valeurs du segment VSCM étant pour leur part légales.

7.2.3 Message de réaction

Dans les systèmes de communication de sécurité fonctionnelle, tout dispositif doit signaler l'état de défaut (tel que le montre l'objet d'alerte de communication de sécurité fonctionnelle) aux opérateurs système, en utilisant les services EventNotification ou AcknowledgeEventNotification lorsqu'il détecte des erreurs de communication. Après réception et confirmation de l'anomalie de communication, l'opérateur système doit prendre les mesures correspondantes permettant de supprimer les anomalies.

En outre, un objet Temporisateur de ports de connexion (Socket Timer object) et un objet Mappage de ports de connexion (Socket Mapping object) définis dans l'Entité de mappage de ports de connexion (Socket Mapping Entity) spécifiée dans la CEI 61158-5-14, permettent de contrôler la primitive de réponse pour chaque service confirmé. Si le demandeur de service ne reçoit pas la primitive de réponse dans le MaxResponseTime après la transmission de la primitive de demande de service, l'Entité de mappage des ports de connexion doit signaler l'erreur de prolongation. Si nécessaire, il doit retransmettre la primitive de demande de service selon les MaxRetransmitNumber fois définis dans l'objet de Mappage de ports de connexion.

7.2.4 Contre-vérification du CRC

Le protocole de communication de sécurité fonctionnelle comporte un mécanisme qui transmet deux copies des données dans leur intégralité, y compris un horodatage, un numéro de programmation, un numéro de séquence et le CRC dans une trame unique. Les deux copies font l'objet d'une contre-vérification à l'extrémité de réception afin de détecter toute corruption éventuelle.

Le contrôle de redondance cyclique (CRC) permet également de contrôler les défaillances de corruption de données dans les systèmes de communication de sécurité fonctionnelle. Les données sont transmises par trames, avec une somme de contrôle CRC calculée pour chaque trame. Le récepteur recalcule la somme de contrôle des données reçues et compare le résultat avec la somme de contrôle reçue. Les messages corrompus sont rejetés.

Afin d'assurer l'intégrité d'un message et de masquer une RelationKey, un mécanisme de contrôle CRC est défini pour vérifier le Message de contrôle de sécurité virtuel (VSCM), y compris une RelationKey, un numéro de séquence, un numéro de programmation et les données utilisateur (voir 7.1.3).

Le Tableau 9 montre le polynôme de calcul CRC défini dans le protocole de communication de sécurité fonctionnelle.

Tableau 9 – Polynômes de calcul CRC

Code de mode CRC	Mode CRC	Polynôme générateur
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 inversé sur [0xBA0DC66B]

7.2.5 Numéro de programmation

Il permet la traçabilité de la séquence de transmission de tous les dispositifs, ainsi que de toutes les transmissions de données dans un macro-cycle de communication dans les systèmes de communication de sécurité fonctionnelle. Le numéro de programmation est inclus dans le message et est comparé à la valeur de l'attribut ConfiguredSchedulingNumber de l'objet de liaison de sécurité fonctionnelle, tant au niveau local qu'à l'extrémité de réception.

Un macro-cycle de communication dans le système de commande CP 14/1 consiste en une phase de transfert de paquets périodiques (Tp) et une phase de transfert de paquets non périodiques (Tn) (tel qu'illustré à la Figure 12).

Lors de la phase de transfert de paquets périodiques, la mesure de processus et/ou les données de contrôle sont transmises en mode diffusion. C'est-à-dire que tous les autres dispositifs présents sur le même micro-segment peuvent partager les données de processus selon l'application, une fois que ces données sont diffusées.

Au début de chaque macro-cycle de communication, la valeur du numéro de programmation doit être fixée à 1 par le premier dispositif qui doit alors diffuser le paquet périodique contenant les données de processus locales et le numéro de programmation (tel qu'illustré à la Figure 11 ci-dessus). Les autres dispositifs doivent obtenir le numéro de programmation actuel utilisé dans ce macro-cycle de communication. Ensuite, la valeur du numéro de programmation doit être augmentée en ajoutant 1 à chaque extrémité de transmission suivante.

Le numéro de programmation actuel doit être comparé, que ce soit à l'extrémité de transmission ou à l'extrémité de réception des données, à la valeur de l'attribut ConfiguredSchedulingNumber de l'objet de liaison de sécurité fonctionnelle local. Si ce numéro et cette valeur ne correspondent pas, l'anomalie CommunicationSchedulingError doit être consignée et signalée.

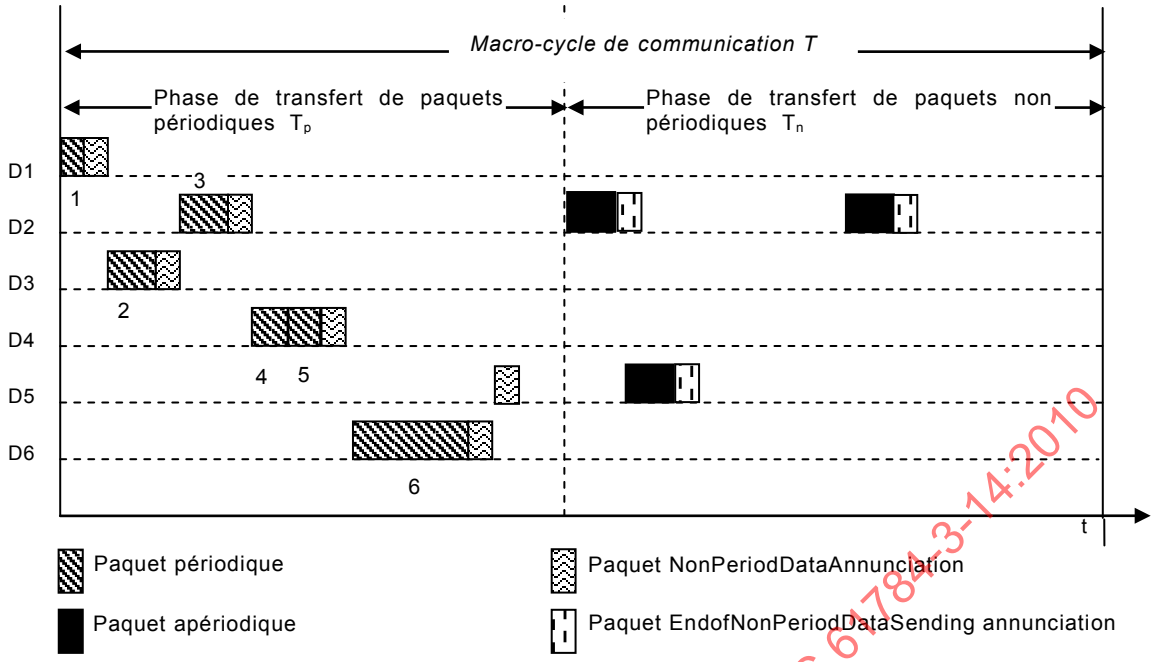


Figure 12 – Programmation de communication de partage de temps

Lors de la phase de transfert de paquets non périodiques (Tn), le numéro de programmation est diffusé avec le message de demande de service EndofNonPeriodicDataSending (tel qu'illustré à la Figure 13) Ensuite, la valeur du numéro de programmation doit être augmentée en ajoutant 1 à chaque extrémité de transmission suivante.

TYPE	En-tête IP	En-tête UDP	ENPMTA_TAG	PRI	Numéro de programmation

Figure 13 – Format de la PDU EndofNonPeriodicDataSending

7.2.6 Datation (horodatage)

La datation permet d'enregistrer l'heure à laquelle la couche de données utilisateur transmet un message dans le service non confirmé de sécurité fonctionnelle afin d'assurer la validité de l'heure. La datation comporte le VCSM et la FSPDU de l'émetteur. La validité de l'heure est évaluée après vérification de l'intégrité de sécurité et de la mise en correspondance des séquences de la FSPDU par le récepteur. Une différence entre la datation de la FSPDU et l'heure actuelle d'indication du récepteur supérieure à la tolérance temporelle maximale permet d'en déduire que le message a été retardé.

7.2.7 Délai

Selon la structure du système et la charge de communication, le délai est spécifié dans les cas les plus défavorables, la communication est considérée comme ayant échoué une fois ce délai expiré après la transmission par les outils de série d'une demande de service confirmée et la non réception d'une réponse provenant d'un dispositif de terrain.

Dans un système de communication de sécurité fonctionnelle, la valeur du délai est la MaxResponseTime définie dans l'objet de gestion de communication de sécurité fonctionnelle.

7.2.8 Contrôle de la synchronisation temporelle

Dans les systèmes de communication de sécurité fonctionnelle, un temps à synchronisation précise est nécessaire pour assurer des communications synchrones basées sur l'ISO/CEI 8802-3. Le mécanisme de synchronisation temporelle basé sur la CEI 61588 corrige le temps

absolu et se trouve dans le canal noir. Son contrôle est toutefois assuré par le protocole de communication de sécurité fonctionnelle.

Le protocole de communication de sécurité fonctionnelle doit vérifier la fréquence de synchronisation temporelle et la précision par rapport à la valeur d'attribut de l'objet TimeSynchronization défini dans la CEI 61158-6-14. Si l'écart entre le temps hôte et le temps local est supérieur à une valeur admise, TargetTimeSyncClass de l'objet TimeSynchronization, une action d'état de panne pré-configurée doit être déclenchée. Si la durée entre deux actions continues de la synchronisation temporelle est TimeRequestInterval, ou si la demande de synchronisation temporelle est "temporisation", l'action d'état de panne pré-configurée doit alors être déclenchée et l'état d'anomalie de communication doit également être consigné.

7.2.9 Contrôle de précision de la programmation de communication

Dans chaque dispositif CP 14/1, la couche de communication de sécurité fonctionnelle doit suivre le décalage temporel réel, ActualDeliveryTimeOffset, par rapport au début du macro-cycle de communication pour chaque message à fournir à la liaison physique. La valeur de ActualDeliveryTimeOffset doit être comparée à la valeur de l'attribut SendTimeOffset de l'objet de liaison de sécurité fonctionnelle.

Si la différence entre ces deux valeurs est supérieure à la valeur de l'attribut SchedulingPrecisionRequirement de l'objet de liaison de sécurité fonctionnelle, une action d'état de panne pré-configurée doit être déclenchée et l'état d'anomalie de communication doit être consigné.

7.3 Comportement de la communication de sécurité

7.3.1 Description d'état de protocole d'une transmission de données périodiques

7.3.1.1 Description d'état

La Figure 14 montre les états de transmission de données périodiques, les termes y afférents étant spécifiés dans le Tableau 10.

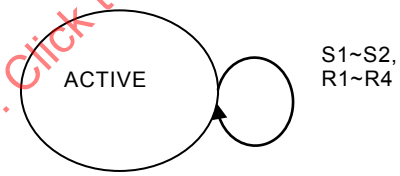


Figure 14 – Schéma de transfert d'états d'une transmission de données périodiques

Les états S1~S2 et R1~R4 sont spécifiés en 7.3.1.2.

Tableau 10 – Description des états de communication de sécurité fonctionnelle

Nom de l'état	Description
ACTIVE	L'entité de sécurité fonctionnelle à l'état ACTIVE est prête à transférer la primitive à la couche utilisateur et à l'entité d'application, ou à recevoir la primitive de ladite couche et de ladite entité.

7.3.1.2 Tableau d'états

Le Tableau 11 décrit les états et transitions de la transmission de données périodiques.

Tableau 11 – Etats et transitions d'une transmission de données périodiques

#	État en cours	Evénement ou condition => Action	État suivant

S1	ACTIVE	Unconfirmed_Service.req
		&& LinkObjectType() = Non-Safety (Non relatif à la sécurité)
		=>
		Unconfirmed_Service.req
		{
		Données:= Données utilisateur,
		Destination_ip: = remote_ip_address,
		}
			ACTIVE

S2	ACTIVE	Unconfirmed_Service.req
		&& LinkObjectType() = Sécurité
		=>
		Créer des données de sécurité sur la base des données utilisateur
		Unconfirmed_Service.req
		{
		Données:= Données de sécurité,
		Destination_ip: = remote_ip_address,
		}
			ACTIVE

R1	ACTIVE	Unconfirmed_Service.ind
		&&LinkObjectType() = Non-Sécurité
		=>
		Unconfirmed_Service.ind
		{
		Données:= Données utilisateur,
		Destination_ip: = remote_ip_address,
		}
			ACTIVE

R2	ACTIVE	Unconfirmed_Service.ind && LinkObjectType() = Sécurité && CRCCheck()= FALSE => ErrorCountCheck(); EventNotifyManagement()	ACTIVE
R3	ACTIVE	Unconfirmed_Service.ind && LinkObjectType() = Sécurité && CRCCheck()= TRUE &&PeriodicSNCheck()= FALSE => ErrorCountCheck(LinkObjectID); EventNotifyManagement()	ACTIVE

R4	ACTIVE	Unconfirmed_Service.ind
		&& LinkObjectType() = Sécurité
		&& CRCCheck()= TRUE
		&& PeriodicSNCheck()= TRUE
		=>
		Créer des données utilisateur sur la base des données de sécurité;
		Unconfirmed_Service.ind
		{
		Données:= Données utilisateur,
		Destination_ip: = remote_ip_address,
		}
			ACTIVE

7.3.2 Description d'état de protocole d'une transmission de données non périodiques

7.3.2.1 Description d'état

La Figure 15 montre les états de transmission de données non périodiques, les termes y afférents étant spécifiés dans le Tableau 12.

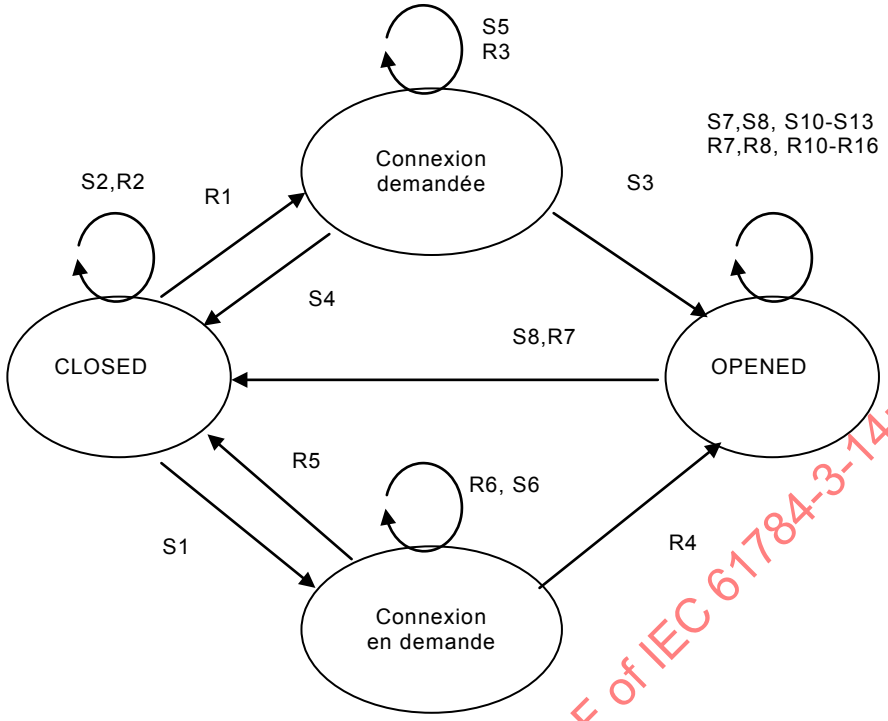


Figure 15 – Transfert des états de communication de sécurité fonctionnelle

Les états R1~R16 et S1~S4 sont spécifiés en 7.3.2.2.

Tableau 12 – Description des états de communication de sécurité fonctionnelle

Nom de l'état	Description
OPENED	L'entité de sécurité fonctionnelle à l'état OPENED est prête à transférer la primitive à la couche utilisateur et à l'entité d'application, ou à recevoir la primitive de ladite couche et de ladite entité.
CLOSED	L'entité de sécurité fonctionnelle à l'état CLOSED est prête à recevoir le service SafetyCommunicationOpen
Connexion demandée	L'entité de sécurité fonctionnelle à l'état Connexion demandée est prête à recevoir la SafetyConmmunicationOpen.rsp de messagerie qui constitue la réponse du service SafetyCommunicationOpen.
Connexion en demande	L'entité de sécurité fonctionnelle à l'état Connexion en demande est prête à recevoir la SafetyConmmunicationClose.cnf de messagerie qui constitue la réponse du service SafetyCommunicationOpen.

7.3.2.2 Tableau d'états

Le Tableau 13 décrit les états et transitions de la transmission de données non périodiques.

Tableau 13 – Etats et transitions d'une transmission de données non périodiques

#	État en cours	Evénement ou condition => Action	État suivant

S1	CLOSED	SafetyCommunicationOpen.req
		=>
		SafetyCommunicationOpen.req
		{
		user_data:= Données,
		Destination_ip: = remote_ip_address,
		}
			Connexion en demande

#	État en cours	Evénement ou condition => Action	État suivant

S2	CLOSED	Service sauf SafetyCommunicationOpen.req
		=>
		Service.cnf(-)
		{
		user_data:= Error-Status-Closed,
		Destination_ip: = remote_ip_address,
		}
			CLOSED

R1	CLOSED	SafetyCommunicationOpen.ind
		=>
		SafetyCommunicationOpen.ind
		{
		user_data:= Données,
		Destination_ip: = remote_ip_address,
		}
			Connexion demandée

R2	CLOSED	Service sauf SafetyCommunicationOpen.ind
		=>
		Service.rsp(-)
		{
		user_data:= Error-Status-Closed,
		Destination_ip: = remote_ip_address,
		}
			CLOSED

S3	Connexion demandée	SafetyCommunicationOpen.rsp(+)
		=>
		SafetyCommunicationOpen.rsp(+)
		{
		user_data:= Données,
		Destination_ip: = remote_ip_address,
		}
			OPENED

S4	Connexion demandée	SafetyCommunicationOpen.rsp(-)
		=>
		SafetyCommunicationOpen.rsp(-)
		{
		user_data:= Données,
		Destination_ip: = remote_ip_address,
		}
			CLOSED

S5	Connexion demandée	Service sauf SafetyCommunicationOpen.rsp => (Aucune Action)	Connexion demandée

R3	Connexion demandée	Tout service
		=>
		Service.rsp(-)
		{
		user_data:= Error-Status-Requeted,
		Destination_ip: = remote_ip_address,
		}
			Connexion demandée

R4	Connexion en demande	SafetyCommunicationOpen.rsp(+)
		=>
		SafetyCommunicationOpen.rsp(+)
		{
		user_data:= Données,
		Destination_ip: = remote_ip_address,
		}
			OPENED

R5	Connexion en demande	SafetyCommunicationOpen.rsp(-)
		=>
		SafetyCommunicationOpen.rsp(-)
		{
		user_data:= Données,
		Destination_ip: = remote_ip_address,
		}
			CLOSED

R6	Connexion en demande	Service sauf SafetyCommunicationOpen.rsp => (Aucune Action)	Connexion en demande

#	État en cours	Evénement ou condition => Action	État suivant

S6	Connexion en demande	Tout service
		=>
		Service.rsp(-)
		{
		user_data:= Error-Status-Requesting,
		Destination_ip: = remote_ip_address,
		}
			Connexion en demande

S7	OPENED	SafetyCommunicationClose.req
		=>
		SafetyCommunicationClose.req
		{
		user_data:= Données,
		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:= Données,
		Destination_ip: = remote_ip_address,
		}
			OPENED

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:= Données,
		Destination_ip: = remote_ip_address,
		}
			CLOSED

S10	OPENED	SafetyCommunicationClose.rsp(-)
		=>
		SafetyCommunicationClosed.rsp(-)
		{
		user_data:= Données,
		Destination_ip: = remote_ip_address,
		}
			OPENED

R9	OPENED	SafetyCommunicationClose.rsp(+)
		=>
		SafetyCommunicationClose.rsp(+)
		{
		user_data:= Données,
		Destination_ip: = remote_ip_address,
		}
			CLOSED

R10	OPENED	SafetyCommunicationClose.rsp(-)
		=>
		SafetyCommunicationClose.rsp(-)
		{
		user_data:= Données,
		Destination_ip: = remote_ip_address,,
		}
			OPENED

#	État en cours	Evénement ou condition => Action	État suivant

S11	OPENED	Confirmed service.req
		&& ServiceType != SafetyCommunicationOpen
		&& ServiceType != SafetyCommunicationClose
		=>
		Créer des données de sécurité sur la base des données utilisateur
		Confirmed service.req
		{
		user_data:= Données de sécurité,
		Destination_ip: = remote_ip_address,
		}
		StartTimer(temps de réponse de la sécurité fonctionnelle)
			OPENED

R11	OPENED	Confirmed service.ind
		&& ServiceType != SafetyCommunicationOpen
		&& ServiceType != SafetyCommunicationClose
		&& CRCCheck()= FALSE
		=>
		Confirmed Service.rsp(-)
		{
		ErrorClass = Erreur de communication
		ErrorCode = Erreur CRC
		}
			OPENED

R12	OPEN	Confirmed service.ind
		&& ServiceType != SafetyCommunicationOpen
		&& ServiceType != SafetyCommunicationClose
		&& CRCCheck()= TRUE
		&& Non-periodicSNCheck() = FALSE
		=>
		Confirmed Service.rsp(-)
		{
		ErrorClass = Erreur de communication
		ErrorCode = Erreur de numéro de séquence
		}
			OPENED

R13	OPEN	Confirmed service.ind
		&& ServiceType != SafetyCommunicationOpen
		&& ServiceType != SafetyCommunicationClose
		&& CRCCheck()= TRUE
		&& Non-periodicSNCheck() = TRUE
		=>
		Créer des données utilisateur sur la base des données de sécurité
		Confirmed service.ind
		{
		user_data:= Données utilisateur,
		Destination_ip: = remote_ip_address,
		}
			OPENED

S12	OPENED	Confirmed service.rsq
		&& ServiceType != SafetyCommunicationOpen
		&& ServiceType != SafetyCommunicationClose
		=>
		Confirmed service.rsq
		{
		user_data:= Données,
		Destination_ip: = remote_ip_address,
		}
			OPENED