IEC 61784-3-17

Edition 1.0 2016-07

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Industrial communication networks – Profiles – Part 3-17: Functional safety fieldbuses – Additional specifications for CPF 17

Réseaux de communication industriels – Profils – Partie 3-17: Bus de terrain de sécurité fonctionnelle – Spécifications supplémentaires pour CPF 17

IEC 61784-3-17:2016-07(en-fr)

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.

IEC Catalogue - webstore.iec.ch/catalogue
The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

IEC publications search - www.iec.ch/searchpub
The advanced search enables 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 It also gives information on projects, replaced and withdrawn publications.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 online and also once a month by email.

Electropedia - www.electropedia.org
The world's leading online dictionary of electronic and electrical terms containing 20 000 terms and definitions in English and French, with equivalent terms in 15 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary
65 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

IEC 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 l'IEC
La Commission Electrotechnique Internationale (IEC) 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 IEC
Le contenu technique des publications IEC est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Catalogue IEC - webstore.iec.ch/catalogue
Application autonome pour consulter tous les renseignements bibliographiques sur les Normes internationales, Spécifications techniques, Rapports techniques et autres documents de l'IEC. Disponible pour PC, Mac OS, tablettes Android et iPad.

Recherche de publications IEC - www.iec.ch/searchpub
La recherche avancée permet de trouver des publications IEC 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.

IEC Just Published - webstore.iec.ch/justpublished
Restez informé sur les nouvelles publications IEC. 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 de termes électroniques et électriques. Il contient 20 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans 15 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

Glossaire IEC - std.iec.ch/glossary
65 000 entrées terminologiques électrotechniques, en anglais et en français, extraites des articles Termes et Définitions des publications IEC parues depuis 2002. Plus certaines entrées antérieures extraites des publications des CE 37, 77, 86 et CISPR de l'IEC.

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 61784-3-17

Edition 1.0 2016-07

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Industrial communication networks – Profiles – Part 3-17: Functional safety fieldbuses – Additional specifications for CPF 17

Réseaux de communication industriels – Profils – Partie 3-17: Bus de terrain de sécurité fonctionnelle – Spécifications supplémentaires pour CPF 17

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

ICS 25.040.40, 35.100.05

ISBN 978-2-8322-3493-8

CONTENTS

FOREWORD....5
0 Introduction....7
0.1 General....7
0.2 Patent declaration....9
1 Scope....10
2 Normative references....10
3 Terms, definitions, symbols, abbreviated terms, and conventions....11
3.1 Terms and definitions....11
3.1.1 Common terms and definitions....11
3.1.2 CPF 17: Additional terms and definitions....17
3.2 Symbols and abbreviated terms....17
3.2.1 Common symbols and abbreviated terms....17
3.2.2 CPF 17: Additional symbols and abbreviated terms....18
3.3 Conventions....18
4 Overview of FSCP 17/1 (RAPIEnet Safety™)....18
5 General....20
5.1 External documents providing specifications for the profile....20
5.2 Safety functional requirements....20
5.3 Safety measures....20
5.3.1 General....20
5.3.2 (Virtual) sequence number....21
5.3.3 Time expectation with watchdog....21
5.3.4 Connection authentication....21
5.3.5 Feedback message....21
5.3.6 Data integrity assurance....21
5.4 Safety communication layer structure....22
5.4.1 Principle of FSCP 17/1 safety communications....22
5.4.2 CPF 17 communication structures....22
5.5 Relationships with FAL (and DLL, PhL)....22
5.5.1 General....22
5.5.2 Data types....23
6 Safety communication layer services....23
6.1 Overview....23
6.2 Functional Safety connection....23
6.2.1 General....23
6.2.2 Initiator class specification....23
6.2.3 Responder-class specification....24
6.2.4 Sender class specification....25
6.2.5 Receiver class specification....27
6.3 Functional Safety data transmission service....29
6.4 Functional Safety connection relation....29
7 Safety communication layer protocol....30
7.1 Safety PDU format....30
7.1.1 General....30
7.1.2 FSPDU command....31

7.1.3 Authentication key 31
7.1.4 FSPDU CRC 31
7.2 FSCP 17/1 communication procedure 34
7.2.1 FSCP 17/1 device states 34
7.3 Response to communication errors 42
7.3.1 General 42
7.4 State table for SCL of CPF 17 42
7.4.1 General 42
7.4.2 Events 43
7.4.3 State table for Initiator 44
7.4.4 State table for Responder 53
8 Safety communication layer management 62
8.1 FSCP 17/1 parameter handling 62
8.2 Functional Safety communication parameters 62
9 System requirements 62
9.1 Indicators and switches 62
9.2 Installation guidelines 62
9.3 Safety function response time 62
9.4 Duration of demands 65
9.5 Constraints for calculation of system characteristics 65
9.5.1 General 65
9.5.2 Number of devices 65
9.5.3 Probabilistic consideration 65
9.6 Maintenance 66
9.7 Safety manual 66
10 Assessment 66
Annex A (informative) Additional information for functional safety communication profiles of CPF 17 67
A.1 Hash function calculation 67
A.2 68
Annex B (informative) Information for assessment of the functional safety communication profiles of CPF 17 69
Bibliography 70

Figure 1 – Relationships of IEC 61784-3 with other standards (machinery) 7
Figure 2 – Relationships of IEC 61784-3 with other standards (process) 8
Figure 3 – Communication relationships among FSCP 17 devices 19
Figure 4 – Safety layer architecture 22
Figure 5 – Functional Safety Cycle 29
Figure 6 – Connection relationships among FSCP 17/1 devices 30
Figure 7 – Functional Safety PDU for CPF 17 over type 21 PDU 30
Figure 8 – FSPDU CRC code generation process 32
Figure 9 – Example of sequence number changing 33
Figure 10 – CRC comparison operation 34
Figure 11 – FSCP 17/1 device states 35
Figure 12 – State diagram for Functional Safety device 43
Figure 13 – State diagram for Initiator 44

Figure 14 – State diagram for Responder 53
Figure 15 – Safety function response time 63
Figure 16 – Residual error rate of FSCP 17/1 66

Table 1 – Deployed measures to manage errors 21
Table 2 – General FSPDU 31
Table 3 – FSPDU command 31
Table 4 – FSPDU with 4 octets of safety data and RESET command after restart (reset connection) or error 36
Table 5 – FSPDU with 4 octets of safety data and RESET command to acknowledge a reset command from the Initiator 36
Table 6 – Connection request PDU for the Initiator in CONNECTION state 37
Table 7 – Connection response PDU for the Responder in CONNECTION state 37
Table 8 – Safety data transferred in the SET_PARA state 38
Table 9 – Sending FSPDU with 6 octets of safety data from the Initiator in SET_PARA state 38
Table 10 – Expected FSPDU with 6 octets of safety data from the Responder in SET_PARA state 39
Table 11 – Safety data from the Initiator in the WAIT_PARA state 39
Table 12 – Sending FSPDU with 6 octets of safety data from the Initiator in the WAIT_PARA state 40
Table 13 – Receiving FSPDU with 6 octets of safety data from the Responder in the WAIT_PARA state 40
Table 14 – FSPDU of Safety data in the DATA state 41
Table 15 – Example of 4 octets of safety data from a Sender 41
Table 16 – Example of ACK PDU from the Receiver with 4 octets of safety data 41
Table 17 – Functional Safety communication errors 42
Table 18 – Functional Safety communication error codes 42
Table 19 – States of the Functional Safety Initiator 43
Table 20 – States of the Functional Safety Responder 43
Table 21 – Events in the Functional Safety state 44
Table 22 – Functional Safety communication parameters 62
Table A.1 – the lookup table for FSCP 17/1 68

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES –

Part 3-17: Functional safety fieldbuses – Additional specifications for CPF 17

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 61784-3-17 has been prepared by subcommittee 65C: Industrial networks, of IEC technical committee 65: Industrial-process measurement, control and automation.

The text of this standard is based on the following documents:

FDIS	Report on voting
65C/851/FDIS	65C/854/RVD

Full information on the voting for the approval of this standard can be found in the report on voting indicated in the above table.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

A list of all parts of the IEC 61784-3 series, published under the general title *Industrial communication networks – Profiles – Functional safety fieldbuses*, can be found on the IEC website.

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC web site under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

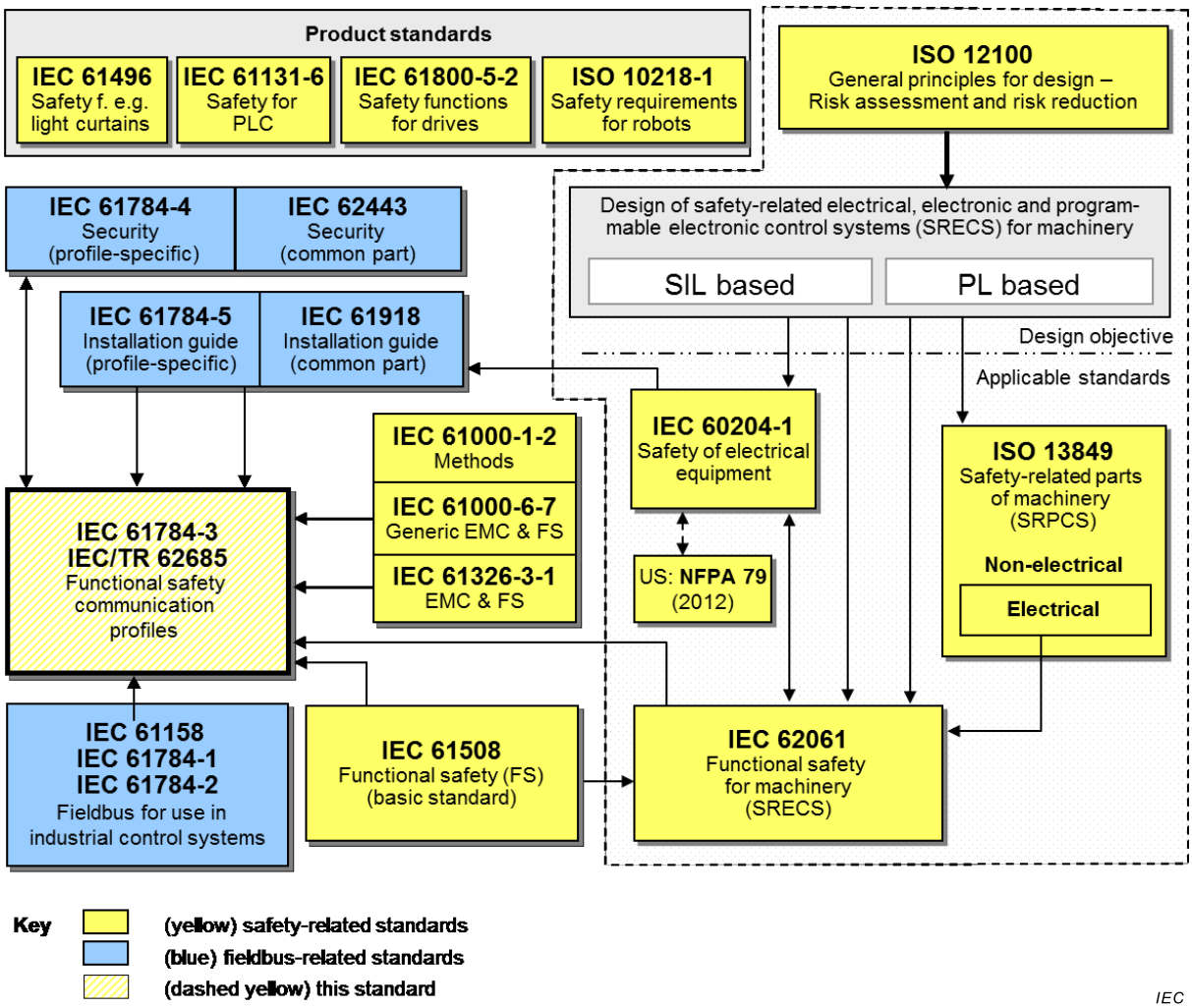
0 Introduction

0.1 General

The IEC 61158 fieldbus standard together with its companion standards IEC 61784-1 and IEC 61784-2 defines a set of communication protocols that enable distributed control of automation applications. Fieldbus technology is now considered well accepted and well proven. Thus fieldbus enhancements continue to emerge, addressing applications for 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 61784-2 and the IEC 61158 series. It does not cover electrical safety and intrinsic safety aspects.

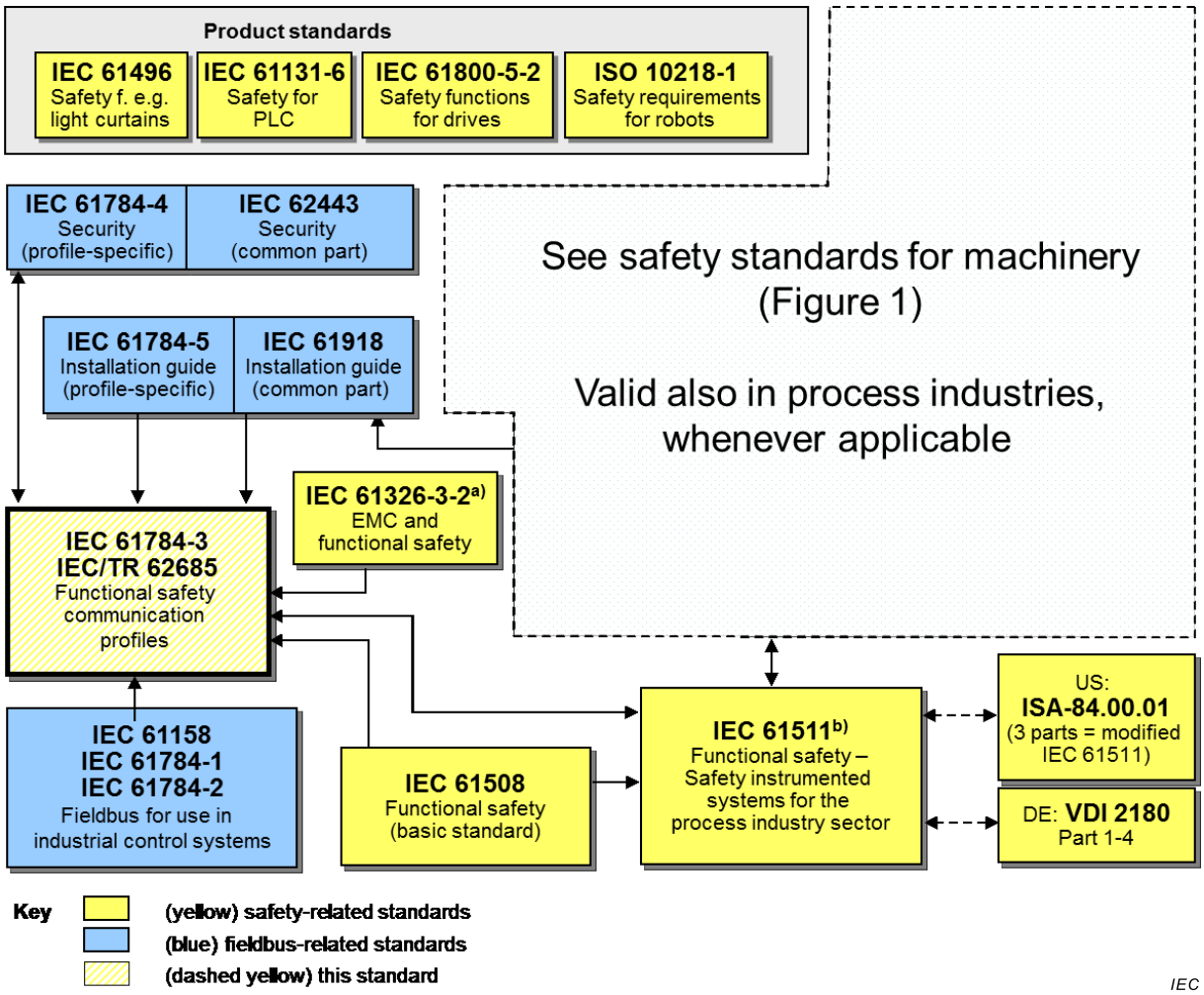
Figure 1 shows the relationships between this standard and relevant safety and fieldbus standards in a machinery environment.



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 or IEC 61000-6-7.

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 (FSCP) 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;
- functional safety communication profiles for several communication profile families in IEC 61784-1 and IEC 61784-2, including 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 17 as follows, where the [xx] notation indicates the holder of the patent right:

PCT/KR2012/008651	[LSIS]	Communication apparatus and Communication method
PCT/KR2012/008653	[LSIS]	Communication apparatus and Communication method
PCT/KR2012/008654	[LSIS]	Communication apparatus and Communication method
PCT/KR2012/008655	[LSIS]	Communication apparatus and Communication method
KR 10-1389604	[LSIS]	Communication Device and communication method
KR 10-1442963	[LSIS]	Communication Device and communication method
KR 10-1389646	[LSIS]	Communication Device and communication method

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 either free of charge or under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statements of the holders of these patent rights are registered with IEC.

Information may be obtained from:

[LSIS] LSIS Co Ltd
LS Tower
1026-6, Hogye-Dong
Dongan-Gu
Anyang, Gyeonggi-Do, 431-848
South Korea

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 3-17: Functional safety fieldbuses – Additional specifications for CPF 17

1 Scope

This part of the IEC 61784-3 series specifies a safety communication layer (services and protocol) based on CPF 17 of IEC 61784-2 (CP 17/1) and IEC 61158 Type 21. It identifies the principles for functional safety communications defined in IEC 61784-3 that are relevant for this safety communication layer. This safety communication layer is intended for implementation in safety devices only.

NOTE 1 It does not cover electrical safety and intrinsic safety aspects. Electrical safety is related to hazards such as electrical shock. Intrinsic safety is related 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 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 for it to qualify as a safety device.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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

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

IEC 61158-3-21:2010, *Industrial communication networks – Fieldbus specifications – Part 3-21: Data-link layer service definition – Type 21 elements*

IEC 61158-4-21:2010, *Industrial communication networks – Fieldbus specifications – Part 4-21: Data-link layer protocol specification – Type 21 elements*

IEC 61158-5-21:2010, *Industrial communication networks – Fieldbus specifications – Part 5-21: Application layer service definition –Type 21 elements*

1 In the following pages of this standard, “this part” will be used for “this part of the IEC 61784-3 series.”

2 In the following pages of this standard, “IEC 61508” will be used for “IEC 61508 series.”

IEC 61158-6-21:2010, *Industrial communication networks – Fieldbus specifications – Part 6-21: Application layer protocol specification – Type 21 elements*

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

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

IEC 61508 (all parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

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

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:—[3], *Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions*

IEC 61784-5-17:2013, *Industrial communication networks – Profiles – Part 5: Installation of fieldbuses – Installation profiles for CPF 17*

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

3 Terms, definitions, symbols, abbreviated terms, and conventions

3.1 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

NOTE Italics are used in the definitions to highlight terms which are themselves defined in 3.1.

3.1.1 Common terms and definitions

NOTE These common terms and definitions are inherited from IEC 61784-3:—.

3.1.1.1
availability
probability in 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
defined communication system containing one or more elements without evidence of design or validation according to IEC 61508

Note 1 to entry: This definition expands the usual meaning of channel to include the system that contains the channel.

[3] To be published.

3.1.1.3
closed communication system
fixed number or fixed maximum number of participants linked by a communication system with well-known and fixed properties, and where the risk of unauthorized access is considered negligible

[SOURCE: IEC 62280:2014, 3.16, modified – transmission replaced by communication]

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 7498-1 application layer) from one application to another

3.1.1.6
connection
logical binding between two application objects within the same or different devices

3.1.1.7
Cyclic Redundancy Check
CRC
<value> redundant data derived from, and stored or transmitted together with, a block of data to detect data corruption

<method> procedure used to calculate the redundant data

Note 1 to entry: Terms “CRC code” and “CRC signature” and labels such as CRC1, CRC2 may also be used in this standard to refer to redundant data.

Note 2 to entry: See also [34], [35][4].

3.1.1.8
defined communication system
defined channel
fixed number or fixed maximum number of participants linked by a fieldbus based communication system with well-known and fixed properties, such as installation conditions, electromagnetic immunity, industrial (active) network elements, and where the risk of unauthorized access is reduced to a tolerated level according to the lifecycle model of IEC 62443, using for example zones and conduits

3.1.1.9
error
discrepancy between a computed, observed, or measured value or condition and the true, specified, or theoretically correct value or condition

Note 1 to entry: Errors may be due to design mistakes within hardware/software and/or corrupted information due to electromagnetic interference and/or other effects.

Note 2 to entry: Errors do not necessarily result in a *failure* or a *fault*.

[SOURCE: IEC 61508-4:2010, 3.6.11, modified – notes added]

4 Figures in square brackets refer to the bibliography.

3.1.1.10
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 to entry: Failure may be due to an *error* (for example, problem with hardware/software design or message disruption).

[SOURCE: IEC 61508-4:2010, 3.6.4, modified – notes and figures replaced]

3.1.1.11
fault
abnormal condition that may cause a reduction in or loss of the capability of a functional unit to perform a required function

Note 1 to entry: IEC 60050-191:1990, 191.05.01 defines “fault” as a state characterized by the inability to perform a required function, excluding such inability during preventive maintenance or other planned actions or due to lack of external resources.

[SOURCE: IEC 61508-4:2010, 3.6.1, modified – figure reference deleted]

3.1.1.12
fieldbus
communication system based on serial data transfer and used in industrial automation or process-control applications

3.1.1.13
fieldbus system
system using a *fieldbus* with connected devices

3.1.1.14
frame
denigrated synonym for DLPDU

3.1.1.15
Frame Check Sequence
FCS
redundant data derived from a block of data within a DLPDU (frame) using a hash function and stored or transmitted together with the block of data to detect data corruption

Note 1 to entry: An FCS can be derived using for example a CRC or other hash function.

Note 2 to entry: See also [34], [35].

3.1.1.16
hash function
(mathematical) function that maps values from a (possibly very) large set of values into a (usually) smaller range of values

Note 1 to entry: Hash functions can be used to detect data corruption.

Note 2 to entry: Common hash functions include parity, checksum, or CRC.

[SOURCE: IEC TR 62210:2003, 4.1.12, modified – addition of “usually” and notes]

3.1.1.17
hazard
state or set of conditions of a system that, together with other related conditions, will inevitably lead to harm to persons, property, or the environment

3.1.1.18
message
ordered series of octets intended to convey information

[SOURCE: ISO/IEC 2382-16:1996, 16.02.01, modified – character replaced by octet]

3.1.1.19
nuisance trip
spurious trip with no harmful effect

Note 1 to entry: Internal abnormal errors can arise in communication systems, such as wireless transmission, for example, by too many retries in the presence of interference.

3.1.1.20
proof test
periodic test performed to detect dangerous hidden failures in a *safety-related system* so that, if necessary, a repair can restore the system to an “as new” condition or as close as practical to this condition

Note 1 to entry: A proof test is intended to confirm that the safety-related system is in a condition that assures the specified safety integrity.

[SOURCE: IEC 61508-4:2010, 3.8.5, modified – replacement of the four notes with another one]

3.1.1.21
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

[SOURCE: ISO 13849-1:2006, 3.1.23]

3.1.1.22
redundancy
existence of more than one means for performing a required function or for representing information

[SOURCE: IEC 61508-4:2010, 3.4.6, modified – example and notes deleted]

3.1.1.23
reliability
probability that an automated system can perform a required function under given conditions for a given time interval (t1, t2)

Note 1 to entry: 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 to entry: The term “reliability” is also used to denote the reliability of performance quantified by this probability.

Note 3 to entry: 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 to entry: Reliability differs from availability.

[SOURCE: IEC 62059-11:2002, 3.17, modified – use automated system, two notes added]

3.1.1.24
residual error probability
RP
probability of an error undetected by the SCL safety measures

3.1.1.25
residual error rate
statistical rate at which the SCL safety measures fail to detect errors

3.1.1.26
risk
combination of the probability of occurrence of harm and the severity of that harm

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6], [SOURCE: ISO/IEC Guide 51:2014, definition 3.9, modified – different note]

3.1.1.27
safety communication channel
communication channel starting at the top of the SCL of the source and ending at the top of the SCL of the sink

Note 1 to entry: It can be modelled as two SCLs connected by a black channel or a defined communication system, or a defined channel.

3.1.1.28
safety communication layer
SCL
communication layer above the FAL that includes all necessary additional measures to ensure safe transmission of data in accordance with the requirements of IEC 61508

3.1.1.29
safety connection
connection that utilizes the safety protocol for communications transactions

3.1.1.30
safety data
data transmitted across a safety network using a safety protocol

Note 1 to entry: The safety communication layer does not ensure the safety of the data themselves, but only that the data are transmitted safely.

3.1.1.31
safety device
device designed in accordance with IEC 61508 that implements the functional safety communication profile

3.1.1.32
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

[SOURCE: IEC 61508-4:2010, 3.5.1, modified – references and example deleted]

3.1.1.33
safety function response time
SFRT
worst-case elapsed time following actuation of a safety sensor connected to a fieldbus, until the corresponding safe state of its safety actuator(s) is achieved in the presence of errors or failures in the safety function

Note 1 to entry: This concept is introduced in IEC 61784-3:—, 5.2.4 and addressed by the functional safety communication profiles defined in this part.

3.1.1.34
safety integrity level
SIL
discrete level (one of four possible) 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 to entry: The target failure measures (see IEC 61508-4:2010, 3.5.15) for the four safety integrity levels are specified in Tables 2 and 3 of IEC 61508-1:2010.

Note 2 to entry: Safety integrity levels are used to specify the safety integrity requirements of the safety functions to be allocated to the E/E/PE safety-related systems.

Note 3 to entry: 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.

[SOURCE: IEC 61508-4:2010, 3.5.8]

3.1.1.35
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 to entry: In practice, several safety measures are combined to achieve the required safety integrity level.

Note 2 to entry: Communication *errors* and related safety measures are detailed in IEC 61784-3:—, 5.3 and 5.4.

3.1.1.36
safety PDU
SPDU
PDU transferred through the safety communication channel

Note 1 to entry: The SPDU may include more than one copy of the safety data using differing coding structures and hash functions together with explicit parts of additional protections such as a key, a sequence count, or a time stamp mechanism.

Note 2 to entry: Redundant SCLs may provide two different versions of the SPDU for insertion into separate fields of the fieldbus frame.

3.1.1.37
safety-related application
programs designed in accordance with IEC 61508 to meet the SIL requirements of the application

3.1.1.38
safety-related system
system performing *safety functions* according to IEC 61508

3.1.1.39
spurious trip
trip caused by the safety system without a process demand

3.1.1.40
time stamp
time information included in a *message*

3.1.2 CPF 17: Additional terms and definitions

3.1.2.1
heartbeat
timer for Sender or Receiver to monitor whether communication partner is alive

3.1.2.2
initiator
role of an FSCP 17/1 device that is responsible for establishing a connection

3.1.2.3
responder
role of an FSCP 17/1 device that is following connection establishing by an Initiator

3.1.2.4
receiver
passive communication entity able to receive messages and send them in response to another communication entity, which may be a Sender or a Receiver

3.1.2.5
sender
active communication entity that is able to initiate and schedule communication activities of other stations, which may be Senders or Receivers

3.1.2.6
SUID
64 bits value of logical connection identification number of FSCP 17/1, which is a combination of the UIDs of two devices

3.1.2.7
UID
identification number of CPF 17, which is a combination of the 48 bits MAC address and 16 bits device address

3.1.2.8
virtual sequence number
internal value for each FSCP 17/1 device used to check message sequence but this is not transmitted in the message frame

3.2 Symbols and abbreviated terms

3.2.1 Common symbols and abbreviated terms

CP	Communication Profile	[IEC 61784-2:2010]
CPF	Communication Profile Family	[IEC 61784-2:2010]
CRC	Cyclic Redundancy Check	
DLL	Data Link Layer	[ISO/IEC 7498-1]
DLPDU	Data Link Protocol Data Unit	
EMC	Electromagnetic Compatibility	
EMI	Electromagnetic Interference	
EUC	Equipment Under Control	[IEC 61508-4:2010]
E/E/PE	Electrical/Electronic/Programmable Electronic	[IEC 61508-4:2010]

FAL	Fieldbus Application Layer	[IEC 61158-5-21:2010]
FCS	Frame Check Sequence	
FS	Functional Safety	
FSCP	Functional Safety Communication Profile	
HD	Hamming Distance	
MTBF	Mean Time Between Failures	
MTTF	Mean Time To Failure	
PDU	Protocol Data Unit	[ISO/IEC 7498-1]
PELV	Protective Extra Low Voltage	
PFD	Probability of Dangerous Failure on Demand	[IEC 61508-4:2010]
PFH	Average Frequency of Dangerous Failure [h^{-1}]	[IEC 61508-4:2010]
PhL	Physical Layer	[ISO/IEC 7498-1]
PL	Performance Level	[ISO 13849-1]
PLC	Programmable Logic Controller	
SCL	Safety Communication Layer	
SFRT	Safety Function Response Time	
SIL	Safety Integrity Level	[IEC 61508-4:2010]

3.2.2 CPF 17: Additional symbols and abbreviated terms

For the purposes of this document, the abbreviations and acronyms given in IEC 61784-3 as well as the following apply.

ASE	Application Service Element
DLE	Data Link Layer Entity
FC	Frame Control
FSPDU	Functional Safety PDU
MAC	Media Access Control
MIB	Management Information Base
PHY	Physical Interface Transceiver
SUID	Safety Unique Identification

3.3 Conventions

Conventions used in this document are defined in IEC 61158 type 21 and IEC 61784-2 CPF 17.

4 Overview of FSCP 17/1 (RAPIEnet Safety™)

Communication Profile Family 17 (commonly known as RAPIEnet™ [5]) defines the communication profile based on IEC 61158-3-21:2010, IEC 61158-4-21:2010, IEC 61158-5-21:2010, and IEC 61158-6-21:2010.

---

5 RAPIEnet™ and RAPIEnet Safety™ are trade names of the non-profit organization RAPIEnet Association. 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 with this standard does not require use of the registered logos for RAPIEnet™ and RAPIEnet Safety™. Use of the registered logos for RAPIEnet™ requires permission of RAPIEnet Association and compliance with conditions for their use (such as testing and validation).

The basic profile, CP 17/1, is defined in IEC 61784-2. The CPF 17 functional safety communication profile FSCP 17/1(RAPIEnet Safety™) is based on the CPF 17 basic profiles in IEC 61784-2 and the safety communication layer specifications defined in this part.

FSCP 17/1 is based on a peer-to-peer communication model using a one-to-one communication relationship, as shown in Figure 3. One controller can operate any mixture of standard and safety devices connected to the network. Assigning safety tasks and standard tasks to different controllers is also possible.

For realization of FSCP 17/1, the following four measures have been chosen:

- (virtual) sequence numbering;
- watchdog time monitoring;
- SUID per communication relationship;
- cyclic redundancy checking for data integrity.

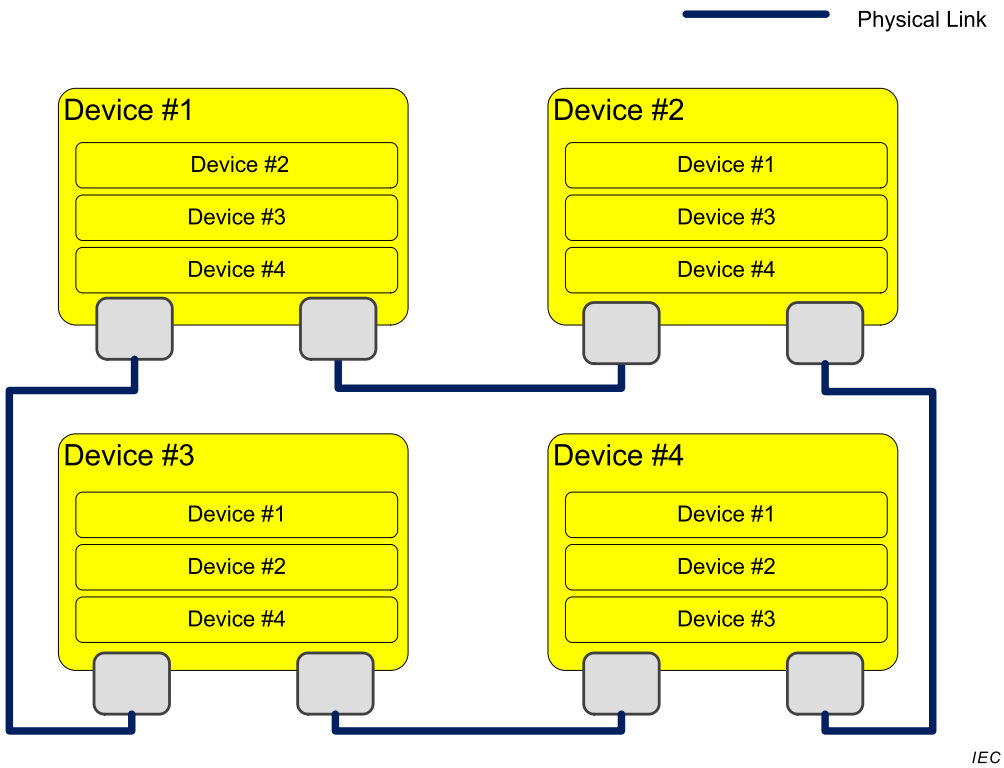


Figure 3 – Communication relationships among FSCP 17 devices

The virtual sequence number is a type of counter for each peer device to determine whether the receiving frame is in the right order. It is automatically added for the Initiator, and the value of the sequence number is reflected in the CRC field. A receiving device uses the CRC to determine whether the sequence number is correct. It is called virtual due to the fact that it cannot be seen within the safety PDU.

The watchdog timer is used to prevent unexpected delays and to detect the condition of the network. If a receiving device cannot receive the expected response from its partner within a specified period, then it changes its state to the FAIL-SAFE state.

The SUID is a key value of each functional safety communication relationship. This consists of the MAC address and ID number, such as the device address or user predefined values of both communication partners. The value of the SUID is unique in an FSCP 17/1 network.

The CRC is used to ensure the integrity of the message frame. CRC32 is used in FSCP 17/1 to detect bit errors, and it covers the residual bit-error probability under a certain limit.

5 General

5.1 External documents providing specifications for the profile

There are no external documents providing specifications for the profile.

5.2 Safety functional requirements

The following requirements apply for the development of FSCP 17/1 technology.

a) Safety communication and standard communication shall be independent. However, standard devices and safety devices shall be able to use the same communication channel.

b) Safety communication shall be suitable for Safety Integrity Level SIL3 (see IEC 61508).

c) The transmission duration times shall be monitored.

d) Implementations of FSCP 17/1 shall comply with IEC 61508.

e) The basic requirements for the development of the FSCP 17/1 protocol are defined in IEC 61784-3.

f) Transmission equipment, such as controllers, ASICs, links, couplers, etc., shall remain unmodified (black channel). The safety functions shall be above FAL (i.e., profile, no standard protocol changes or enhancements).

g) Environmental conditions shall be according to general automation requirements, mainly IEC 61326-3-1 and IEC 61326-3-2, if there are no particular product standards.

h) There shall always be a 1:1 communication relationship between a functional safety Sender controller and its functional safety field device.

5.3 Safety measures

5.3.1 General

The safety measures mentioned in Table 1 for managing possible transmission errors are a significant component of the FSCP 17/1 profile. The selection in Table 1 of the generic safety measures listed in IEC 61784-3:—, 5.5 is required for FSCP 17/1.

The safety measures shall be processed and monitored within one safety unit.

Table 1 – Deployed measures to manage errors

Communication error	Safety measures				
	(virtual) Sequence number [a]	Time expectation with watchdog	Connection authentication	Feedback message	Data integrity assurance
Corruption					X
Unintended repetition	X				
Incorrect sequence	X				
Loss	X	X		X	
Unacceptable delay		X			
Insertion	X		X		
Masquerade			X	X	X
Addressing			X		

[a] Instance of “sequence number” of IEC 61784-3.

5.3.2 (Virtual) sequence number

The sequence number with a width of 16 bits is used to confirm the frame sequence. The sequence number is not shown in a frame, but it is used to generate FSPDUs. At each sending or receiving operation, each device increases the sequence number of dedicate connection. The sequence number is reflected in CRC codes. If the validity of sequence number is not confirmed, the connection shall go to the Safe state.

5.3.3 Time expectation with watchdog

The watchdog timer is providing the time expectation of logical connections. And the watchdog timer is related to the safety response time which is the time between the detection of an event at the safety input and the response at the corresponding output channel(s) on the safety output. For details see also 9.3.

The value of the watchdog timer is set by user as a user parameter in the INITIALIZE state.

5.3.4 Connection authentication

The connection authentication is used to verify that a FSPDU is from its specific communication partner. The SUID is used for the connection authentication. The SUID is a combination value of UIDs of the communication partners and the value for two devices is a unique in a network. Thus, the SUID distinguishes a logical connection from other logical connections or non-safety connections in a network.

5.3.5 Feedback message

The feedback message is provided by acknowledgement. The feedback message contains error status and command on a field of the message. It also contains sequence number and authentication information in the CRC code fields.

5.3.6 Data integrity assurance

The data integrity assurance is achieved by using 32 bits CRC for each 4 octets field on a message. Each CRC code field covers dedicate 4 octets field only. The polynomial for the CRC code is different from general Ethernet FCS.

5.4 Safety communication layer structure

5.4.1 Principle of FSCP 17/1 safety communications

In using FSCP 17/1, safety applications and standard applications share the same standard CPF 17 communication systems at the same time. The safe transmission function comprises all measures to deterministically discover all possible faults/hazards that could be infiltrated by the standard transmission system or to keep the residual error (fault) probability below a certain limit. This includes

- random malfunctions, for example due to EMI impact on the transmission channel,
- failures/faults of the standard hardware,
- systematic malfunctions of components within the standard hardware and software.

This principle delimits the assessment effort to the “safe transmission functions.” The “standard transmission system” (black channel) does not require any additional safety assessment.

Transmission is performed via electrical or optical conductors. Permissible topologies and transmission features of the standard transmission system and the components of the “black channel” are described in 5.4.2.

5.4.2 CPF 17 communication structures

The basic communication structure is shown in Figure 4. The safety communication of FSCP 17/1 is managed in SCL, which is above the CP 17/1 communication layers.

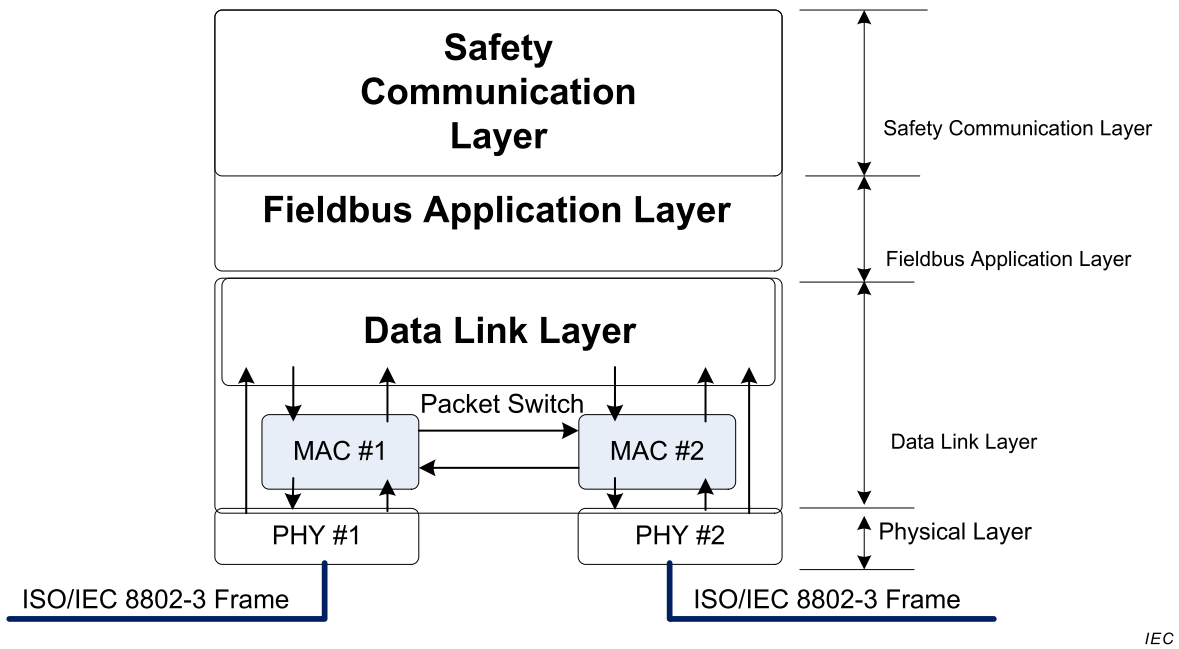


Figure 4 – Safety layer architecture

5.5 Relationships with FAL (and DLL, PhL)

5.5.1 General

This safety communication layer is designed to be used in conjunction with the CPF 17 communication profile. However, it is not restricted to this communication profile.

5.5.2 Data types

Data types of safety data are specified in IEC 61158-5-21.

6 Safety communication layer services

6.1 Overview

Clause 6 defines an extension to the existing communication layer services of the CP 17/1 standard Application Layer Entity for FSCP 17/1.

6.2 Functional Safety connection

6.2.1 General

The connection between two FSCP 17/1 communication partners (FSCP 17/1 devices) is referred to as a functional safety connection. In a functional safety connection process, one communication partner is the functional safety Initiator, and the other is the functional safety Responder by its MAC address and device ID.

The functional safety Initiator initializes the functional safety connection after power-on or after a communication fault, whereas the functional safety Responder is limited to responses. The functional safety Initiator handles the establishment of safety-related communication with its parameters and, optionally, the safety-related application parameters of the functional safety Responder.

After the connection process, the safety process data can be transferred from any FSCP 17/1 device.

6.2.2 Initiator class specification

6.2.2.1 General

The Initiator class supports connection management to the SCL user.

6.2.2.2 Model

SCL ASE:			Connection SASE
CLASS:			Initiator
CLASS ID:			not used
PARENT CLASS:			not used
ATTRIBUTES:			
1	(m)	Attribute:	Command
2	(m)	Attribute:	SUID
3	(m)	Attribute:	Sequence value
4	(m)	Attribute:	Service code
5	(m)	Attribute:	Error/status
6	(m)	Attribute	Watchdog

6.2.2.3 Attributes

Command
This element contains state information of the Initiator. Command can have one of following values:

- RESET;
- CONNECTION;
- PARAMETER;
- DATA;
- FAIL-SAFE.

SUID
This element is used to check the validity of a connection with its communication partner. Each connection of FSCP 17/1 has unique identification.

Sequence value
This element is used to check the message order of transmission. This value is contained in the message indirectly.

Service code
This element is used to figure out status of the message. Three statements are defined:

- connection phase,
- data phase,
- error notification.

Error/status
This element represents the status of the station with respect to sending or receiving message frames.

Watchdog
This element is used to check transmission path or communication partner fault.

6.2.3 Responder-class specification

6.2.3.1 General

The Responder class supports SCL user replies to the Initiator or checks the validity of the receiving frame from the Initiator.

6.2.3.2 Model

SCL ASE:			Connection SASE
CLASS:			Responder
CLASS ID:			not used
PARENT CLASS:			not used
ATTRIBUTES:			
1	(m)	Attribute:	Command
2	(m)	Attribute:	SUID
3	(m)	Attribute:	Sequence value
4	(m)	Attribute:	Service code
5	(m)	Attribute:	Error/status
6	(m)	Attribute	Watchdog

6.2.3.3 Attributes

Command
See 6.2.2.3.

SUID
See 6.2.2.3.

Sequence value
See 6.2.2.3.

Service code
See 6.2.2.3.

Error/status
See 6.2.2.3.

Watchdog
See 6.2.2.3.

6.2.4 Sender class specification

6.2.4.1 General

The Sender class supports connection management to the SCL user.

6.2.4.2 Read request service

6.2.4.2.1 Model

SCL ASE			DATA SASE
CLASS			Sender Read request
CLASS ID			not used
PARENT CLASS			not used
ATTRIBUTES:			
1	(m)	Attribute:	Command
2	(m)	Attribute:	SUID
3	(m)	Attribute:	Sequence value
4	(m)	Attribute:	Service code
5	(m)	Attribute:	Error/status
6	(m)	Attribute	Watchdog
7	(m)	Attribute	Data
7.1	(m)	Attribute	Address
7.2	(m)	Attribute	Length

6.2.4.2.2 Attributes

Command
See 6.2.2.3.

SUID
See 6.2.2.3.

Sequence value
See 6.2.2.3.

Service code
See 6.2.2.3.

Error/status
See 6.2.2.3.

Watchdog
See 6.2.2.3.

Address
This element is used to point out where the Sender needs to access on the Receiver.

Length
This element is used to address the length of data to read from the Receiver.

6.2.4.3 Write request service

6.2.4.3.1 Model

SCL ASE			DATA SASE
CLASS			Sender Write request
CLASS ID			not used
PARENT CLASS			not used
ATTRIBUTES:			
1	(m)	Attribute:	Command
2	(m)	Attribute:	SUID
3	(m)	Attribute:	Sequence value
4	(m)	Attribute:	Service code
5	(m)	Attribute:	Error/status
6	(m)	Attribute	Watchdog
7	(m)	Attribute	Data
7.1	(m)	Attribute	Address
7.2	(m)	Attribute	Length
7.3	(m)	Attribute	SafeData[0]
7.4	(m)	Attribute	SafeData[1]
…	…	…	…
7.n	(m)	Attribute	SafeData[n-3]

6.2.4.3.2 Attributes

Command
See 6.2.2.3.

SUID
See 6.2.2.3.

Sequence value
See 6.2.2.3.

Service code
See 6.2.2.3.

Error/status
See 6.2.2.3.

Watchdog
See 6.2.2.3.

Address
See 6.2.4.2.2.

Length
See 6.2.4.2.2.

Data
This element is actual safe data that the Sender intends to write to the Receiver.

6.2.5 Receiver class specification

6.2.5.1 General

The Receiver class supports SCL-user replies to the Initiator or checks the validity of the receiving frame from the Initiator.

6.2.5.2 Read response service

6.2.5.2.1 Model

SCL ASE			DATA SASE
CLASS			Receiver Read response
CLASS ID			not used
PARENT CLASS			not used
ATTRIBUTES:			
1	(m)	Attribute:	Command
2	(m)	Attribute:	SUID
3	(m)	Attribute:	Sequence value
4	(m)	Attribute:	Service code
5	(m)	Attribute:	Error/status
6	(m)	Attribute	Watchdog
7	(m)	Attribute	Data
7.1	(m)	Attribute	SafeData[0]
7.2	(m)	Attribute	SafeData[1]
…	…	…	…
7.n	(m)	Attribute	SafeData[n-1]

6.2.5.2.2 Attributes

Command
See 6.2.2.3.

SUID
See 6.2.2.3.

Sequence value
See 6.2.2.3.

Service code
See 6.2.2.3.

Error/status
See 6.2.2.3.

Watchdog
See 6.2.2.3.

Address
See 6.2.4.2.2.

Length
See 6.2.4.2.2.

Data
See 6.2.4.3.2.

6.2.5.3 Write response service

6.2.5.3.1 Model

SCL ASE			DATA SASE
CLASS			Sender Write response
CLASS ID			not used
PARENT CLASS			not used
ATTRIBUTES:			
1	(m)	Attribute:	Command
2	(m)	Attribute:	SUID
3	(m)	Attribute:	Sequence value
4	(m)	Attribute:	Service code
5	(m)	Attribute:	Error/status
6	(m)	Attribute	Watchdog
7	(m)	Attribute	Data
7.1	(m)	Attribute	Acknowledgement

6.2.5.3.2 Attributes

Command
See 6.2.2.3.

SUID
See 6.2.2.3.

Sequence value
See 6.2.2.3.

Service code
See 6.2.2.3.

Error/status
See 6.2.2.3.

Watchdog
See 6.2.2.3.

Data
See 6.2.4.3.2.

Acknowledgement
This element is used to confirm to the Sender that the write service is accomplished.

6.3 Functional Safety data transmission service

An FSCP 17/1 device sends an FSPDU to the partner and starts the functional safety watchdog.

After checking the integrity of the FSPDU, the FSCP 17/1 Receiver transfers the safety data to the safety application. It calculates the FSPDU with the parameters in the frame and given parameters from the safety application and sends an acknowledgement to the Sender. The Receiver also starts its functional safety watchdog, as shown in Figure 5.

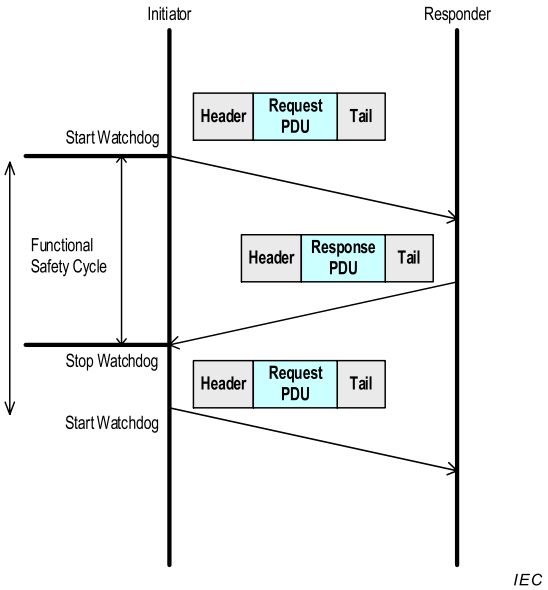


Figure 5 – Functional Safety Cycle

6.4 Functional Safety connection relation

For each functional safety connection, each device has to manage its partners' information concerning each connection relationship in the SCL. Figure 6 shows an example of the relationships among various connections.

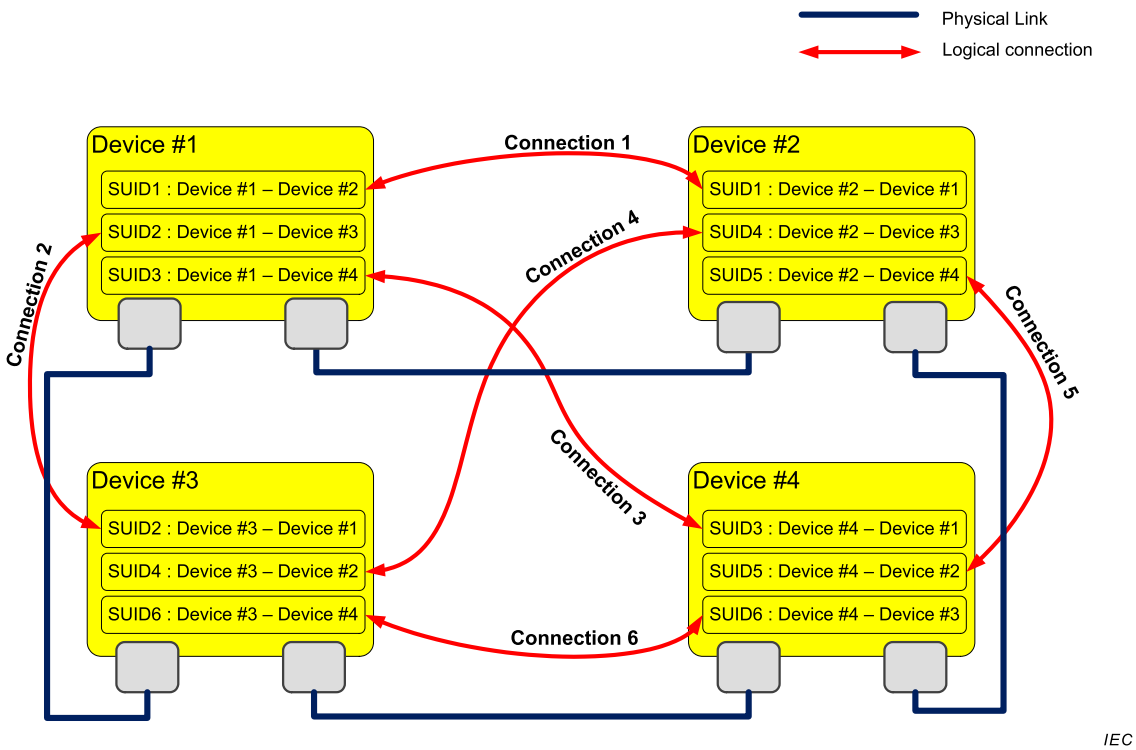


Figure 6 – Connection relationships among FSCP 17/1 devices

7 Safety communication layer protocol

7.1 Safety PDU format

7.1.1 General

Ethernet Header	Type 21	Type 21 PDU		Ethernet
Ethernet Header	Frame HDR	Type 21 Header	DATA	FCS

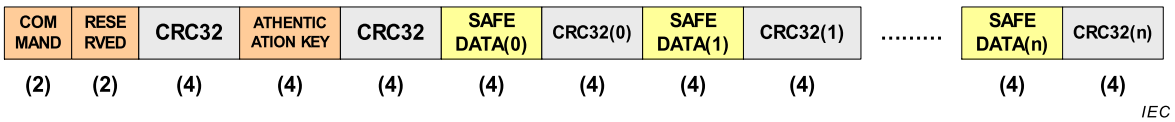


Figure 7 – Functional Safety PDU for CPF 17 over type 21 PDU

The FSPDU is transferred via the FSCP 17/1 network. Each FSCP 17/1 device receives safety PDU from the designated partner. The safety PDU format is shown in Figure 7.

The FSPDU contains information to validate the command and the communication partner.

During the process of establishing a connection, the safety data field can be assigned a value of zero.

Table 2 – General FSPDU

Octet	Name	Description
0	Command	Command, 2 octets
2	Reserved	Reserved, 2 octets
4	CRC32_H0	CRC32 for header, 4 octets
8	Authentication key	Lower 32 bits SUID,4 octets
12	CRC32_H1	CRC32 for authentication key, 4 octets
16	SafeData[0]	Safety data,4 octets
20	CRC32_0	CRC32 for SafeData[0], 4 octets
24	Safe Data [1]	Safety data, 4 octets
28	CRC32_1	CRC32 for SafeData[1], 4 octets
…	…	…
n × 8 + 16	SafeData[n]	Safety data, 4 octets
n × 8 + 20	CRC32_n	CRC32 for SafeData[n], 4 octets

The FSPDU can transfer n safety data blocks, each consisting of 4 octets. Each data block has 4 octets CRC code. It is described in Table 2.

7.1.2 FSPDU command

The FSPDU command determines the meaning of the safety data based on the scheme shown in Table 3.

Table 3 – FSPDU command

Command	Description
0x01	RESET
0x02	CONNECTION
0x03	PARAMETER
0x04	DATA
0x05	FAIL-SAFE

7.1.3 Authentication key

The authentication key is implemented by 64 bits SUID. The SUID is a combination of UIDs of two devices. A FSPDU has CRC code fields and each CRC code is generated with SUID. If a device receives a frame without valid SUID, the frame shall be discarded by CRC comparison. The lower 32 bits of SUID is shown in the authentication key field.

7.1.4 FSPDU CRC

7.1.4.1 CRC calculation

The distinction between safety relevant and non-safety relevant messages is ensured by validating the uniqueness of safety messages to contain a properly formatted CRC codes, 4 octets fields, the SUID and the virtual sequence number. Each CRC code covers designated 4 octets of the header or safety data field only. Figure 8 shows how to generate CRC code for safety data.

```
CRC_i:=        f(SUID, (virtual) Sequence_Number, command or 4 octets Data[i])
```

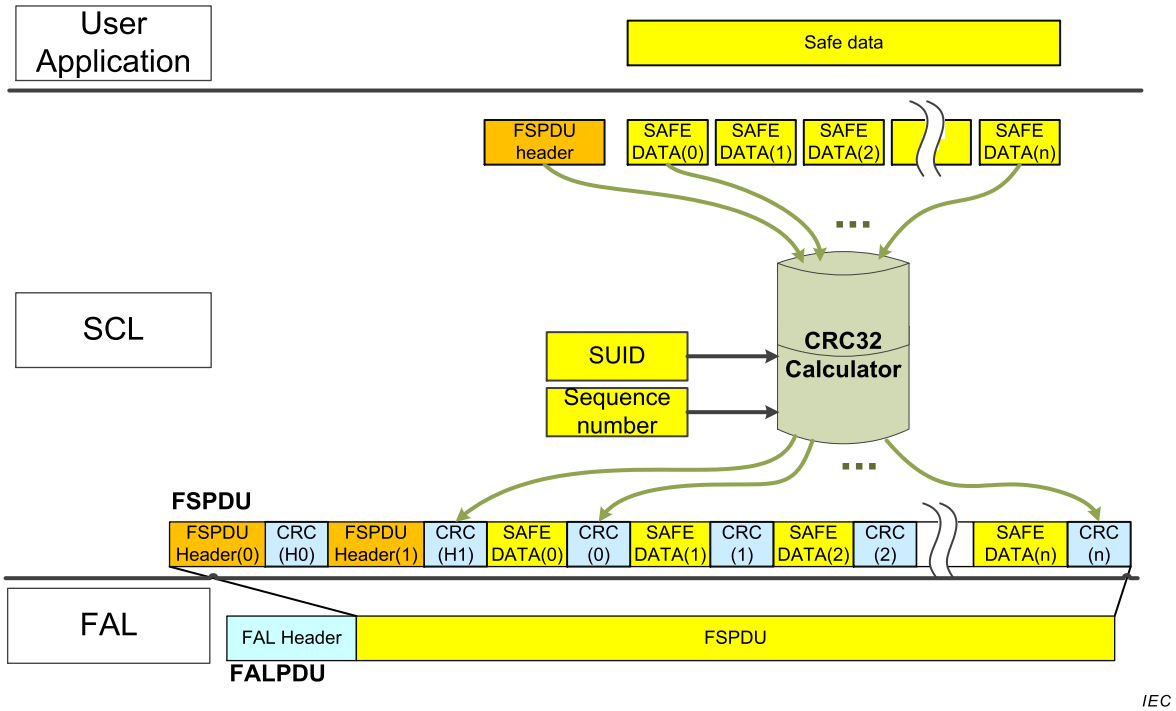


Figure 8 – FSPDU CRC code generation process

7.1.4.2 CRC polynomial selection

The polynomial G(x) = $\{x^{32}+x^{16}+x^{14}+x^{12}+x^{11}+x^{9}+x^{6}+x^{5}+x^{2}+x^{1}+1\}$ is used to calculate the CRCs and is referred to as the safety polynomial.

To allow the FSPDU to be transported via a black channel, the transfer characteristics of which are not included in the safety considerations, a bit error rate of 10^{-2} shall be used to determine the residual error probability. The residual error probability shall not exceed 10^{-9}.

Safety is ensured based on the functional safety Sender and the functional safety Receiver switching to the reset state (i.e., safe state) as soon as an error is detected.

All CRC calculation factors have a fixed expected value, so that only safety data have to be considered in the calculation of the residual error probability.

7.1.4.3 SUID

The SUID is an 8 octets value used for the identification of each connection. It is a combination of the MAC address and device ID of each connection participant. These are unique values in FSCP 17/1, thus SUID is a unique value in an FSCP 17/1 network.

```
SUID = f(source MAC address and device ID, destination MAC address and device ID)
```

The SUID is set on the INITIALIZE state and it shall not be changed on functional safety operation.

7.1.4.4 Sequence number

The sequence number is used to figure out the right order of transmitted frame sequence and to generate dedicate CRC codes for the frame. The sequence number with width of 16 bits belongs to logical connection. The sequence number is not shown in a frame but managed in the SCL.

The sequence number is increased from a device which sends a request message. A device which sends a request message increases internal sequence number and builds a FSPDU with increased sequence number. A receiving device increases sequence number when it receives a request message from the communication partner. If the receiving device receives a respond message from the communication partner, it shall not increase internal sequence number and examine the received frame with present sequence number. An example of sequence number changing is shown in Figure 9.

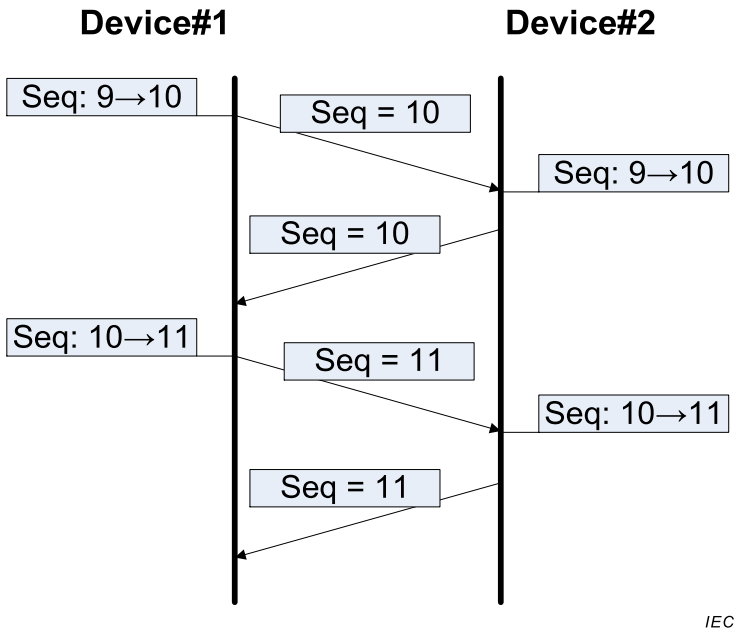


Figure 9 – Example of sequence number changing

7.1.4.5 Communication error detection with CRC

In FSCP 17/1, communication errors are detected by CRC codes except time related communication errors such as loss or unacceptable delay. The error detection is achieved by CRC comparison operation on the receiving device.

Each CRC code in a FSPDU is calculated with variable field and fixed fields. The variable field is safe data field with width of 4 octets. The fixed fields are SUID and sequence number.

A sending device calculates CRC codes with safe data fields, sequence number and SUID to build a FSPDU. The sequence number is not shown in the FSPDU but the two devices have synchronized sequence numbers. When a device receives a request message, the device shall calculate expected CRC codes with SUID, present sequence number and safe data field of the message. Then it compares to each CRC codes of the received message to check the validity of the message. If there is any mismatch of the comparison, the received frame shall be discarded. The error detection operation with CRC code is shown in Figure 10.

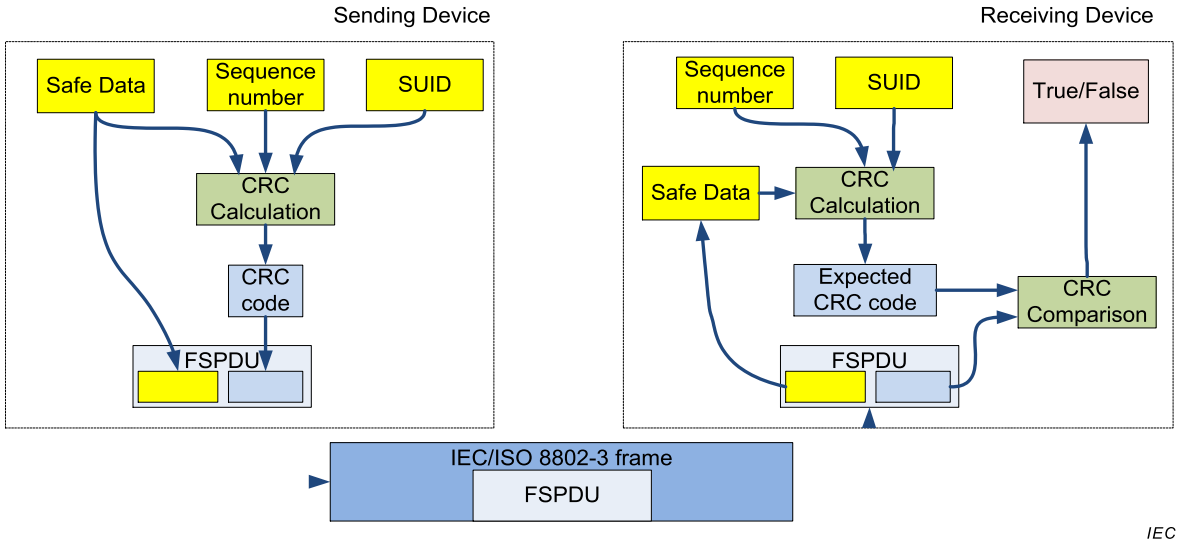


Figure 10 – CRC comparison operation

7.2 FSCP 17/1 communication procedure

7.2.1 FSCP 17/1 device states

7.2.1.1 General

While the functional safety connection is being established, the FSCP 17/1 devices take on different states before the safety data become valid and the system exits from the safety state.

Figure 11 shows the functional safety device states.

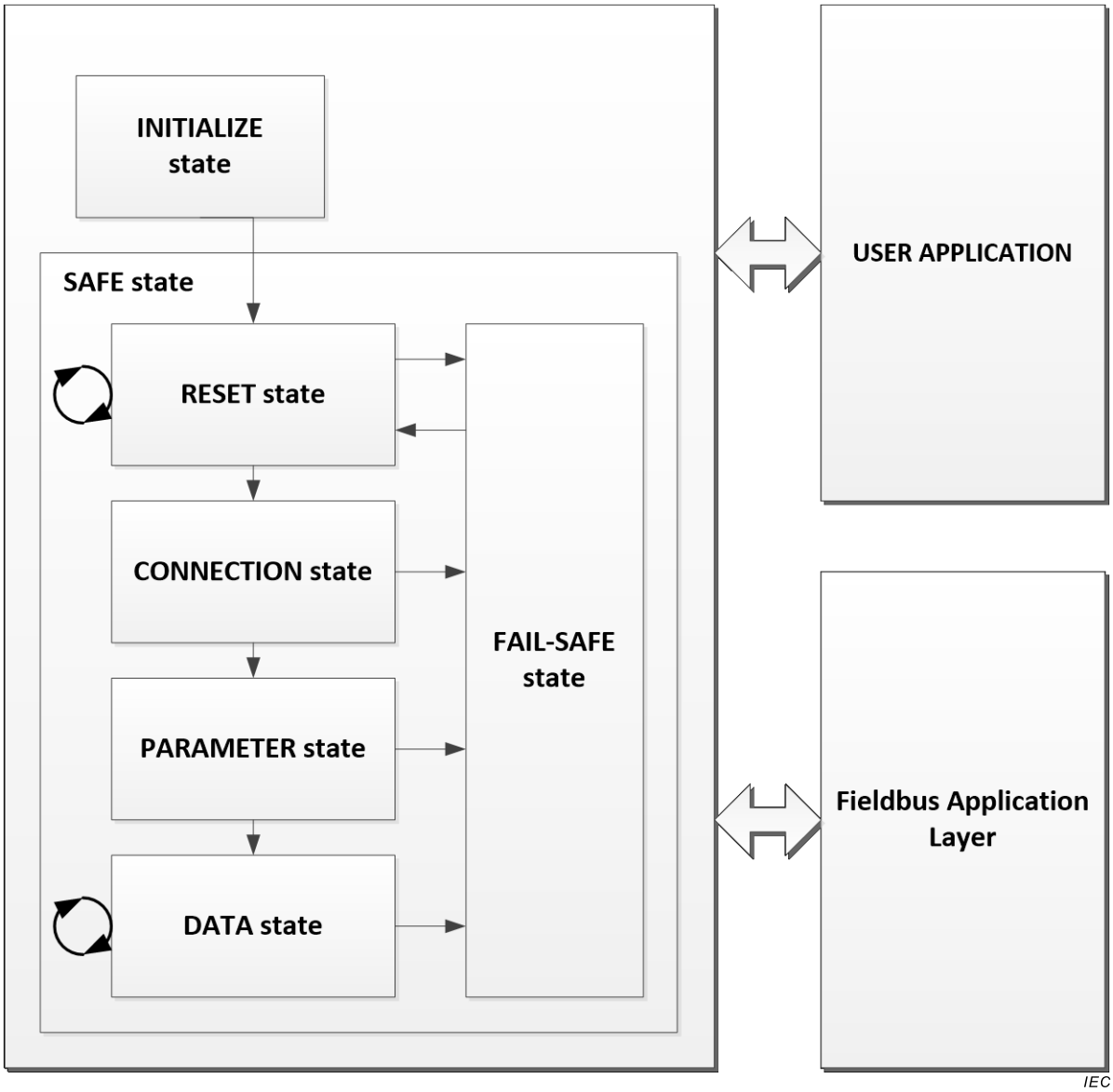


Figure 11 – FSCP 17/1 device states

After power-on, all of the functional safety devices are in the INITIALIZE state. While in this state, they set their initial parameters according to their respective user-defined values. When all parameters are set, functional safety device switches to RESET state. Before entering DATA state, output is kept in a de-energized state. The DATA state can then be assumed via CONNECTION and PARAMETER states.

7.2.1.2 INITIALIZE state

In the INITIALIZE state, user-defined parameters (for example, device ID, watchdog timer value and heartbeat timer value) are set for the devices.

After INITIALIZE state, each device starts its Safe states from RESET state.

7.2.1.3 RESET state

The RESET state is used to start the functional safety connection after the INITIALIZE state. When the Responder receives a valid reset request message, it sends the reset response message to the Initiator. If the Initiator receives a valid reset response message, it changes to the CONNECTION state. The Initiator exits the RESET state when it sends a connection request message with a CONNECTION command to the Responder. If the Responder

receives a valid connection request message, the Responder changes to the CONNECTION state.

If any CRC field on a received frame does not match the expected value, it is determined that a communication error has occurred.

When any communication error is detected, the state of the device should be changed to FAIL-SAFE. An exception to this rule is if the watchdog timer of the Initiator expires while the Initiator is in the RESET state; in this case, the expiration should be ignored, and the Initiator should continue to send reset request message to the Responder until it receives a valid response.

Table 4 shows the format of an FSPDU with 4 octets of safety data and the RESET command.

Table 4 – FSPDU with 4 octets of safety data and RESET command after restart (reset connection) or error

Octet	Name	Description
0	Command	RESET
2	Reserved	Reserved, 2 octets
4	CRC32_H0	CRC32 for header, 4 octets
8	Authentication key	Lower 32 bits SUID,4 octets
12	CRC32_H1	CRC32 for authentication key, 4 octets
16	SafeData[0]	Zero padding,4 octets
20	CRC32_0	CRC32 for SafeData[0], 4 octets

The Responder acknowledges the reset command by setting the SafeData[0] message to 0.

Table 5 shows the format of the safety response PDU for 4 octets of safety data and the RESET command.

Table 5 – FSPDU with 4 octets of safety data and RESET command to acknowledge a reset command from the Initiator

Octet	Name	Description
0	Command	RESET
2	Reserved	Reserved, 2 octets
4	CRC32_H0	CRC32 for header, 4 octets
8	Authentication key	Lower 32 bits SUID,4 octets
12	CRC32_H1	CRC32 for authentication key, 4 octets
16	SafeData[0]	Zero padding, 4 octets,
20	CRC32_0	CRC32 for SafeData[0], 4 octets

The Responder also sends an FSPDU with the reset command during a restart (reset connection) or in the event of an error. This is shown in Table 5, using an example of 4 octets of safety data.

7.2.1.4 CONNECTION state

In the CONNECTION state, the Initiator and the Responder confirm each other as their repective communication partners. When the Initiator changes from the RESET to the CONNECTION state, it sends a connection request message to the Responder. When the

Responder changes from RESET to the CONNECTION state, it sends a connection response message to the Initiator.

If the Initiator receives a valid connection response message, the Initiator changes its state to the PARAMETER state. If the Responder receives a valid parameter request message, it changes its state to the PARAMETER state.

If any CRC field on a received frame does not match the expected value or if the watchdog timer expires, both the Initiator and the Responder shall send a fail-safe request message to its respective communication partners and change to the FAIL-SAFE state.

The functional safety PDUs in CONNECTION state is shown in Table 6 and Table 7.

Table 6 – Connection request PDU for the Initiator in CONNECTION state

Octet	Name	Description
0	Command	CONNECTION
2	Reserved	Reserved, 2 octets
4	CRC32_H0	CRC32 for header, 4 octets
8	Authentication key	Lower 32 bits SUID,4 octets
12	CRC32_H1	CRC32 for authentication key, 4 octets
16	SafeData[0]	Upper 4 octets of the UID
20	CRC32_0	CRC32 for SafeData[0], 4 octets
24	SafeData[1]	Lower 4 octets of the UID
28	CRC32_1	CRC32 for SafeData[1], 4 octets

The Responder acknowledges the connection command by sending back the UID in the data field.

Table 7 – Connection response PDU for the Responder in CONNECTION state

Octet	Name	Description
0	Command	CONNECTION
2	Reserved	Reserved, 2 octets
4	CRC32_H0	CRC32 for header, 4 octets
8	Authentication key	Lower 32 bits SUID,4 octets
12	CRC32_H1	CRC32 for authentication key, 4 octets
16	SafeData[0]	Upper 4 octets of the UID
20	CRC32_0	CRC32 for SafeData[0], 4 octets
24	SafeData[1]	Lower 4 octets of the UID
28	CRC32_1	CRC32 for SafeData[1], 4 octets

Because the UID is a combination of the device address and MAC address, it can be used to examine the address validity of the communication partner, so that invalid addressing shall be detected.

7.2.1.5 SET_PARA state

The SET_PARA state is for the Initiator. If the Initiator changes its state from CONNECTION state to the SET_PARA state, it sends the parameter request message to the Responder with 6 octets of safety-related application parameters in the data field. If the Initiator receives a valid parameter response message, it changes its state to the DATA state.

Table 8 shows the content of the safety data transferred in the SET_PARA state.

Table 8 – Safety data transferred in the SET_PARA state

Safety data octet	Description
0	Low octet (bits 0_7) of the functional safety watchdog timer value (in ms)
1	High octet (bits 8_15) of the functional safety watchdog timer value (in ms)
2	Low octet (bits 0_7) of the local heartbeat timer value (in ms)
3	High octet (bits 8_15) of the local heartbeat timer value (in ms)
4	Low octet (bits 0_7) of the remote heartbeat timer value (in ms)
5	High octet (bits 8_15) of the remote heartbeat timer value (in ms)

The functional safety parameter is transferred as 6 octets of the safety-related parameters in the data field; this is shown in Table 9 to Table 10. The first FSPDU is sent by the Initiator, as shown in Table 9, and the Initiator expects an FSPDU message,as an acknowledgement, in accordance with Table 10. When the Initiator receives an FSPDU from the Responder without any error and containing the same functional safety parameter as that which was sent, the state of the Initiator will be changed to the DATA state. However, if the received FSPDU does not match the expected value, the Initiator changes its state to FAIL-SAFE and sends a failsafe request message to its partner.

Table 9 – Sending FSPDU with 6 octets of safety data from the Initiator in SET_PARA state

Octet	Name	Description
0	Command	PARAMETER
2	Reserved	Reserved, 2 octets
4	CRC32_H0	CRC32 for header, 4 octets
8	Authentication key	Lower 32 bits SUID,4 octets
12	CRC32_H1	CRC32 for authentication key, 4 octets
16	SafeData[0]	2 octets functional safety watchdog timer value (in ms), 2 octets local heartbeat timer value (in ms),
20	CRC32_0	CRC32 for SafeData[0], 4 octets
24	SafeData[1]	2 octets remote heartbeat timer value (in ms) 2 octets zero padding
28	CRC32_1	CRC32 for SafeData[1], 4 octets

When the Responder receives a message with functional safety parameters from the Initiator, the Responder sets its functional safety parameters with the parameter in the message and returns parameters to the Initiator to confirm.

The Responder acknowledges a correct PARAMETER command by sending back the safety data.

Table 10 – Expected FSPDU with 6 octets of safety data from the Responder in SET_PARA state

Octet	Name	Description
0	Command	PARAMETER
2	Reserved	Reserved, 2 octets
4	CRC32_H0	CRC32 for header, 4 octets
8	Authentication key	Lower 32 bits SUID,4 octets
12	CRC32_H1	CRC32 for authentication key, 4 octets
16	SafeData[0]	Repeated 2 octets functional safety watchdog timer value (in ms), 2 octets local heartbeat timer value (in ms),
20	CRC32_0	CRC32 for SafeData[0], 4 octets
24	SafeData[1]	2 octets remote heartbeat timer value (in ms) 2 octets zero padding
28	CRC32_1	CRC32 for SafeData[1], 4 octets

The functional safety communication parameter is configured via the safety configurator of the Initiator.

7.2.1.6 WAIT_PARA state

The WAIT_PARA state is for the Responder. When the Responder receives a valid parameter request message, it sets its parameter with given values in the received message and sends a response message to the Initiator with set parameter in the data field.

Table 11 shows the content of the safety data transferred in the WAIT_PARA state.

Table 11 – Safety data from the Initiator in the WAIT_PARA state

Safety data octet	Description
0	Low octet (bits 0_7) of the functional safety watchdog (in ms)
1	High octet (bits 8_15) of the functional safety watchdog (in ms)
2	Low octet (bits 0_7) of the local heartbeat timer value (in ms)
3	High octet (bits 8_15) of the local heartbeat timer value (in ms)
4	Low octet (bits 0_7) of the remote heartbeat timer value (in ms)
5	High octet (bits 8_15) of the remote heartbeat timer value (in ms)

The functional safety parameter is transferred as 6 octets of safety parameter data in the data field; this is shown in Table 12 and Table 13. When an FSPDU is received from the Initiator, as shown in Table 12, the Responder compares the functional safety parameters in the FSPDU to the pre-configured functional safety communication parameter. If the received FSPDU has no error, the Responder sets its functional safety communication parameter to the received value and sends acknowledgement to the Initiator. Table 13 shows the FSPDU format from the Responder to the Initiator with the change in state to DATA. If the received FSPDU has any error, the Responder shall change its state to FAIL-SAFE and sends a fail-safe request message to its partner.

Table 12 – Sending FSPDU with 6 octets of safety data from the Initiator in the WAIT_PARA state

Octet	Name	Description
0	Command	PARAMETER
2	Reserved	Reserved, 2 octets
4	CRC32_H0	CRC32 for header, 4 octets
8	Authentication key	Lower 32 bits SUID,4 octets
12	CRC32_H1	CRC32 for authentication key, 4 octets
16	SafeData[0]	Repeated 2 octets functional safety watchdog timer value (in ms), 2 octets local heartbeat timer value (in ms),
20	CRC32_0	CRC32 for SafeData[0], 4 octets
24	SafeData[1]	2 octets remote heartbeat timer value (in ms) 2 octets zero padding
28	CRC32_1	CRC32 for SafeData[1], 4 octets

The Responder acknowledges the parameter configuration result by sending its parameter in the safety data field.

Table 13 – Receiving FSPDU with 6 octets of safety data from the Responder in the WAIT_PARA state

Octet	Name	Description
0	Command	PARAMETER
2	Reserved	Reserved, 2 octets
4	CRC32_H0	CRC32 for header, 4 octets
8	Authentication key	Lower 32 bits SUID,4 octets
12	CRC32_H1	CRC32 for authentication key, 4 octets
16	SafeData[0]	Repeated 2 octets functional safety watchdog timer value (in ms), 2 octets local heartbeat timer value (in ms),
20	CRC32_0	CRC32 for SafeData[0], 4 octets
24	SafeData[1]	2 octets remote heartbeat timer value (in ms) 2 octets zero padding
28	CRC32_1	CRC32 for SafeData[1], 4 octets

7.2.1.7 DATA state

If the Initiator changes state from SET_PARA to the DATA state, it sends a data request message to the Responder. If the Responder changes state from WAIT_PARA to the DATA state, it sends a data response message to the Initiator.

After establishment of the functional safety connection, both the Initiator and the Responder are in the DATA state until either a communication error occurs or a functional safety device is stopped locally. In the DATA state, the roles of the Initiator and the Responder are released, and each device can send or receive safety data as a Sender or a Receiver.

In the DATA state, each device uses a heartbeat timer to monitor the connection status between the communication partners. All devices on FSCP 17/1 network send heartbeat message by the local heartbeat timer. If there is no valid message from the partner or

heartbeat message until the remote heartbeat timer, the device shall send a fail-safe request message and change its state to the FAIL-SAFE state.

Table 14 shows the format of the general FSPDU in the DATA state.

Table 14 – FSPDU of Safety data in the DATA state

Octet	Name	Description
0	Command	DATA
2	Reserved	Reserved, 2 octets
4	CRC32_H0	CRC32 for header, 4 octets
8	Authentication key	Lower 32 bits SUID,4 octets
12	CRC32_H1	CRC32 for authentication key, 4 octets
16	SafeData[0]	SafeData[0], 4 octets
20	CRC32_0	CRC32 for SafeData[0], 4 octets
	SafeData[1]	SafeData[1], 4 octets
	CRC32_1	CRC32 for SafeData[1], 4 octets
…		
16+8i	SafeData[i]	SafeData[i], 4 octets
16+(8i+4)	CRC32_1	CRC32 for SafeData[i], 4 octets

When the Sender sends safety data, the Receiver acknowledges its receipt with a repetition of the received safety data. Table 15 and Table 16 show examples of sending and acknowledging 4 octets of safety data between a Sender and a Receiver.

Table 15 – Example of 4 octets of safety data from a Sender

Octet	Name	Description
0	Command	DATA
2	Reserved	Reserved, 2 octets
4	CRC32_H0	CRC32 for header, 4 octets
8	Authentication key	Lower 32 bits SUID,4 octets
12	CRC32_H1	CRC32 for authentication key, 4 octets
16	SafeData[0]	Safety data, 4 octets
20	CRC32_0	CRC32 for SafeData[0], 4 octets

Table 16 – Example of ACK PDU from the Receiver with 4 octets of safety data

Octet	Name	Description
0	Command	DATA
2	Reserved	Reserved, 2 octets
4	CRC32_H0	CRC32 for header, 4 octets
8	Authentication key	Lower 32 bits SUID,4 octets
12	CRC32_H1	CRC32 for authentication key, 4 octets
16	SafeData[0]	Received safety data, 4 octets
20	CRC32_0	CRC32 for SafeData[0], 4 octets

7.3 Response to communication errors

7.3.1 General

A functional safety device can detect the errors listed in Table 17.

Table 17 – Functional Safety communication errors

Error	Description
Unexpected command	The received command is not allowed in the state
Invalid connection ID	The connection does not match the SUID transferred in the connection state
CRC error	At least one of the received CRC fields does not match the calculated CRC
Watchdog has expired	No valid FSPDU was received within the functional safety watchdog time
Invalid safety data	The safety data received from a communication partner does not match the expected values
Invalid safety data	The safety data sent back by the Receiver in the DATA state does not match the safety data sent by the Sender
Invalid communication parameter	The content of the communication parameter is unacceptable
Heartbeat has expired	No valid heartbeat message was received from communication partner within remote heartbeat time

If a functional safety device detects any communication error, a fail-safe request message is sent by the device, as well as the associated error code in the data field for diagnostic purposes. The device that has detected an error or a fault switches to the FAIL-SAFE state and sends a fail-safe request message. When the communication partner receives the fail-safe request message, it changes its state to the FAIL-SAFE state. The functional safety communication error codes are listed in Table 18.

Table 18 – Functional Safety communication error codes

Error Code	Description
1	Unexpected command (INVALID_CMD)
2	Invalid connection ID (INVALID_CONNID)
3	CRC error (INVALID_CRC)
4	Watchdog has expired (WD_EXPIRED)
5	Invalid safety data (INVALID_DATA)
6	Invalid communication parameter(INVALID_PARA)
7	Heartbeat timer has expired(HB_EXPIRED)

7.4 State table for SCL of CPF 17

7.4.1 General

Depending on the communication procedure, the functional safety Initiator can have the states listed in Table 19 and Table 20.

Table 19 – States of the Functional Safety Initiator

State	Description
INITIALIZE	Device parameters and functional safety-related parameter are set by user
RESET	The functional safety connection is reset (outputs are in safe state)
CONNECTION	The UID of each device is being transferred (outputs are in safe state)
SET_PARA	The parameters are being transferred (outputs are in safe state)
DATA	Safety data are being transferred
FAIL-SAFE	Stop communication until user trigger (outputs are in safe state)

Table 20 – States of the Functional Safety Responder

State	Description
INITIALIZE	Device parameters and functional safety-related parameters are set by user
RESET	The functional safety connection is reset (outputs are in safe state)
CONNECTION	The UID of each device is being confirmed (outputs are in safe state)
WAIT_PARA	The parameters are being configured (outputs are in safe state)
DATA	Safety data are being transferred
FAIL-SAFE	Stop communication until user trigger (outputs are in safe state)

The state diagram for the functional safety device is shown in Figure 12.

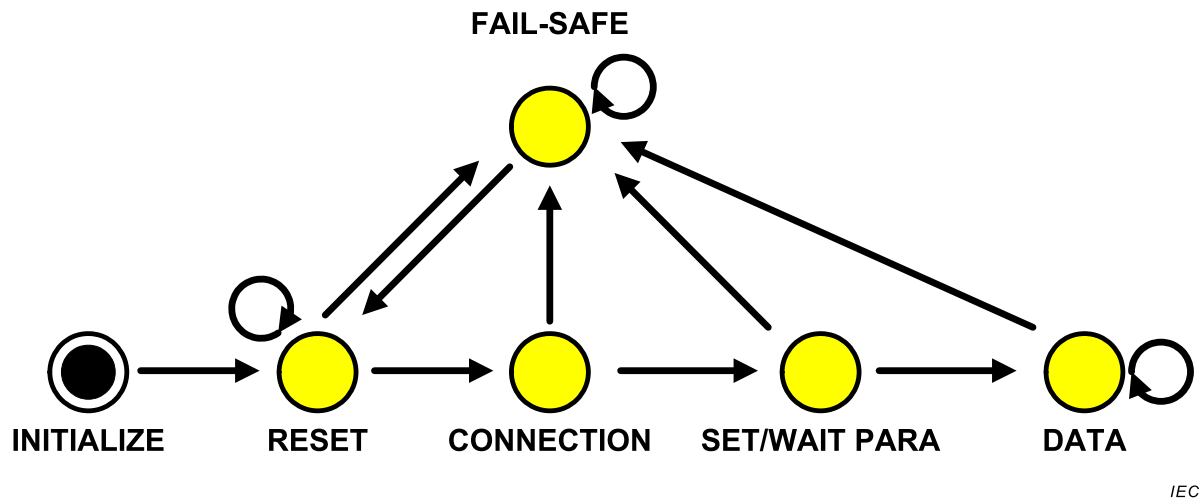


Figure 12 – State diagram for Functional Safety device

The following sections analyze the events that can occur in the functional safety device for each state. Each event is considered under conditions with different actions or subsequent states.

7.4.2 Events

An event can include different parameters, which are referred to in the state tables. Table 21 lists the possible events.

Table 21 – Events in the Functional Safety state

Event	Description
Frame receive	An FSPDU has been received from a communication partner
Frame send	In the DATA state, functional safety application needs to send a message to a partner
Initialize complete	A device is ready to start functional safety communication with user-set parameters
User trigger	User input to escape from the FAIL-SAFE state
Watchdog expired	The functional safety watchdog has expired, (i.e., no valid FSPDU was received within the watchdog time)
Heartbeat timer expired	A periodic timer for monitoring the communication partner has expired while in the DATA state

7.4.3 State table for Initiator

7.4.3.1 General

The state diagram for initiator is shown in Figure 13.

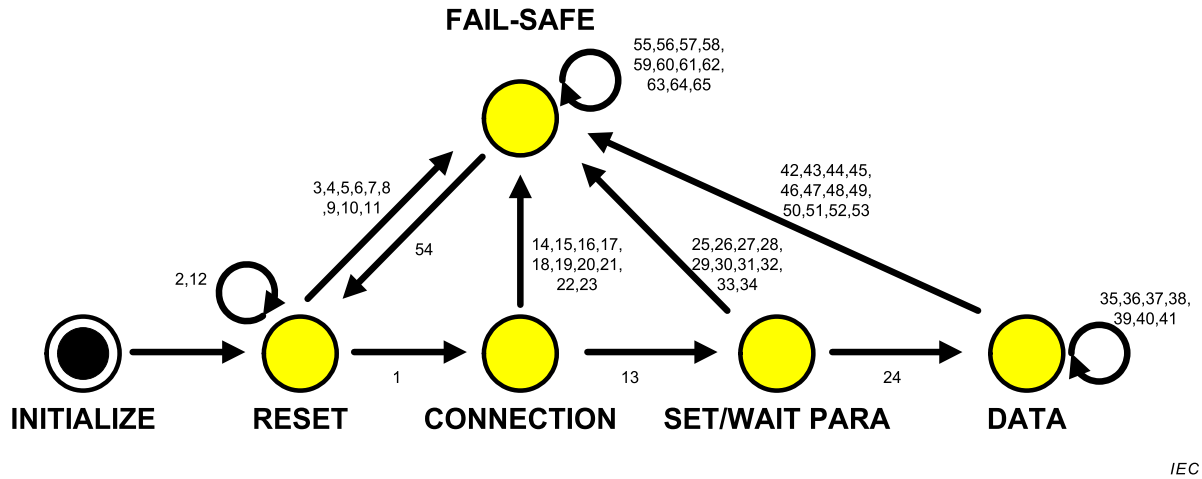


Figure 13 – State diagram for Initiator

7.4.3.2 RESET state

#	Current	Event /Condition =>actions	Next state
1	RESET	RECEIVE reset response message /CRC_Check() = TRUE => command = 0x02(CONNECTION) watchdog restart() & WD = 1 SEND connection request message	CONNECTION
2	RESET	INITIALIZE complete => command = 0x01(RESET) watchdog start() & WD = 1 SEND reset request message	RESET
3	RESET	RECEIVE fail-safe request message =>	FAIL-SAFE

#	Current	Event /Condition =>actions	Next state
4	RESET	RECEIVE reset request message => INVALID_CMD command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	FAIL-SAFE
5	RESET	RECEIVE reset response message /CRC_Check() = FALSE => INVALID_CRC command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	FAIL-SAFE
6	RESET	RECEIVE connection request message => INVALID_CMD watchdog stop() & WD = 0 command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	FAIL-SAFE
7	RESET	RECEIVE connection response message => INVALID_CMD command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	FAIL-SAFE
8	RESET	RECEIVE parameter request message => INVALID_CMD command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	FAIL-SAFE
9	RESET	RECEIVE parameter response message => INVALID_CMD command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	FAIL-SAFE
10	RESET	RECEIVE data request message => INVALID_CMD command = 0x05(FAIL-SAFE) service code = error notification	FAIL-SAFE

#	Current	Event /Condition =>actions	Next state
		SEND fail-safe request message	
11	RESET	RECEIVE data response message => INVALID_CMD command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	FAIL-SAFE
12	RESET	watchdog expired() => WD_EXPIRED command = 0x01(RESET) watchdog start() & WD = 1 SEND reset request message	RESET

7.4.3.3 CONNECTION state

#	Current	Event /Condition =>actions	Next state
13	CONNECTION	RECEIVE connection response message /CRC_Check() = TRUE => command = 0x03(PARAMETER) watchdog restart() & WD = 1 SEND parameter request message	SET_PARA
14	CONNECTION	RECEIVE fail-safe request message =>	FAIL-SAFE
15	CONNECTION	RECEIVE reset request message => INVALID_CMD command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	FAIL-SAFE
16	CONNECTION	RECEIVE reset response message => INVALID_CMD command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	FAIL-SAFE
17	CONNECTION	RECEIVE connection request message => INVALID_CMD command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	FAIL-SAFE

#	Current	Event /Condition =>actions	Next state
18	CONNECTION	RECEIVE connection response message /CRC_Check() = FALSE => INVALID_CRC command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	FAIL-SAFE
19	CONNECTION	RECEIVE parameter request message => INVALID_CMD command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	FAIL-SAFE
20	CONNECTION	RECEIVE parameter response message => INVALID_CMD command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	FAIL-SAFE
21	CONNECTION	RECEIVE data request message => INVALID_CMD command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	FAIL-SAFE
22	CONNECTION	RECEIVE data response message => INVALID_CMD command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	FAIL-SAFE
23	CONNECTION	Watchdog expired() => WD_EXPIRED command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	FAIL-SAFE

7.4.3.4 SET PARAMETER state

#	Current	Event /Condition =>actions	Next state
24	SET_PARA	RECEIVE parameter response message /CRC_Check() = TRUE => command = 0x04(DATA) service code = connection phase watchdog restart() & WD = 1 SEND data request message	DATA
25	SET_PARA	RECEIVE fail-safe request message =>	FAIL-SAFE
26	SET_PARA	RECEIVE reset request message => INVALID_CMD command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	FAIL-SAFE
27	SET_PARA	RECEIVE reset response message => INVALID_CMD command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	FAIL-SAFE
28	SET_PARA	RECEIVE connection request message => INVALID_CMD command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	FAIL-SAFE
29	SET_PARA	RECEIVE connection response message => INVALID_CMD command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	FAIL-SAFE
30	SET_PARA	RECEIVE parameter request message => INVALID_CMD command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	FAIL-SAFE
31	SET_PARA	RECEIVE parameter response message /CRC_Check = FALSE =>	FAIL-SAFE

#	Current	Event /Condition =>actions	Next state
		INVALID_CRC command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	
32	SET_PARA	RECEIVE data request message => INVALID_CMD command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	FAIL-SAFE
33	SET_PARA	RECEIVE data response message => INVALID_CMD command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	FAIL-SAFE
34	SET_PARA	Watchdog expired() => WD_EXPIRED command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	FAIL-SAFE

7.4.3.5 DATA state

#	Current	Event /Condition =>actions	Next state
35	DATA	RECEIVE data response message /CRC_Check() = TRUE /service code = connection phase => watchdog stop() & WD = 0 local heartbeat timer start() remote heartbeat timer start() SEND heartbeat message	DATA
36	DATA	Functional safety application needs to send request message to the partner => command = 0x04(DATA) service code = data phase watchdog start() & WD = 1 SEND data request message	DATA
37	DATA	Functional safety application needs to send response message to the partner	DATA

#	Current	Event /Condition =>actions	Next state
		=> command = 0x04(DATA) service code = data phase SEND data response message	
38	DATA	RECEIVE data request message /CRC_Check() = TRUE /service code = data phase => Received data forwarding to the functional safety application	DATA
39	DATA	RECEIVE data response message /CRC_Check() = TRUE /service code = data phase => watchdog stop() & WD = 0 Received data forwarding to the functional safety application	DATA
40	DATA	RECEIVE heartbeat message /CRC_Check() = TRUE => remote heartbeat timer restart()	DATA
41	DATA	local heartbeat timer expired => local heartbeat timer start() SEND heartbeat message	DATA
42	DATA	RECEIVE fail-safe request message =>	FAIL-SAFE
43	DATA	RECEIVE reset request message => INVALID_CMD command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	FAIL-SAFE
44	DATA	RECEIVE reset response message => INVALID_CMD command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	FAIL-SAFE
45	DATA	RECEIVE connection request message => INVALID_CMD command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	FAIL-SAFE

#	Current	Event /Condition =>actions	Next state
46	DATA	RECEIVE connection response message => INVALID_CMD command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	FAIL-SAFE
47	DATA	RECEIVE parameter request message => INVALID_CMD command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	FAIL-SAFE
48	DATA	RECEIVE parameter response message => INVALID_CMD command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	FAIL-SAFE
49	DATA	RECEIVE data request message /service code = connection phase => INVALID_CMD command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	FAIL-SAFE
50	DATA	RECEIVE data request message /service code = data phase /CRC_Check = FALSE => INVALID_CRC command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	FAIL-SAFE
51	DATA	RECEIVE data response message /CRC_Check() = FALSE => INVALID_CRC command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	FAIL-SAFE
52	DATA	Watchdog expired() => WD_EXPIRED	FAIL-SAFE

#	Current	Event /Condition =>actions	Next state
		command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	
53	DATA	remote heartbeat timer expired => HB_EXPIRED command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	FAIL-SAFE

7.4.3.6 FAIL-SAFE state

#	Current	Event /Condition =>actions	Next state
54	FAIL-SAFE	User trigger => command = 0x02 (RESET) watchdog start() & WD = 1 SEND reset request message	RESET
55	FAIL-SAFE	watchdog expired =>	FAIL-SAFE
56	FAIL-SAFE	local heartbeat timer expired =>	FAIL-SAFE
57	FAIL-SAFE	remote heartbeat timer expired =>	FAIL-SAFE
58	FAIL-SAFE	RECEIVE reset request message => discard message	FAIL-SAFE
59	FAIL-SAFE	RECEIVE reset response message => discard message	FAIL-SAFE
60	FAIL-SAFE	RECEIVE connection request message => discard message	FAIL-SAFE
61	FAIL-SAFE	RECEIVE connection response message => discard message	FAIL-SAFE
62	FAIL-SAFE	RECEIVE parameter request message => discard message	FAIL-SAFE
63	FAIL-SAFE	RECEIVE parameter response message => discard message	FAIL-SAFE

#	Current	Event /Condition =>actions	Next state
64	FAIL-SAFE	RECEIVE data request message => discard message	FAIL-SAFE
65	FAIL-SAFE	RECEIVE data response message => discard message	FAIL-SAFE

7.4.4 State table for Responder

7.4.4.1 General

The state diagram for Responder is shown in Figure 14.

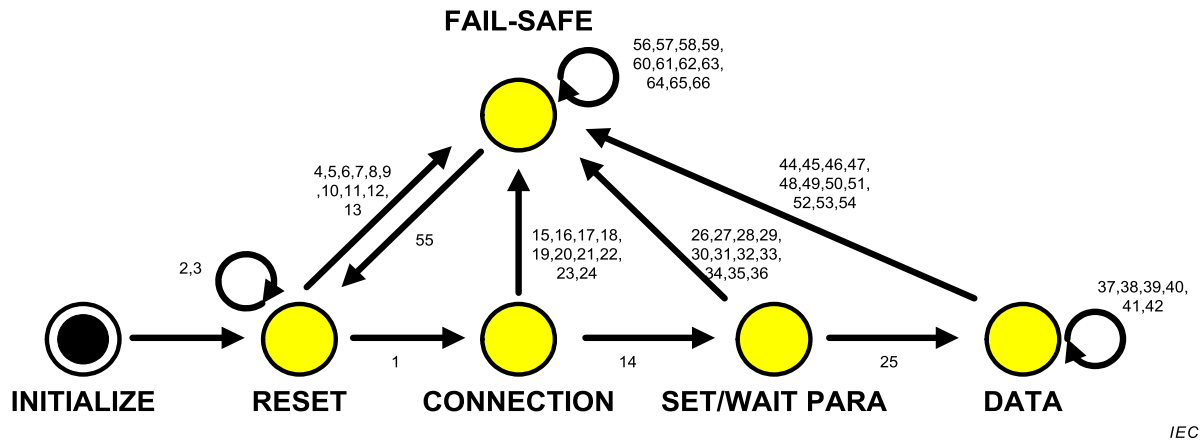


Figure 14 – State diagram for Responder

7.4.4.2 RESET state

#	Current	Event /Condition =>actions	Next state
1	RESET	RECEIVE connection request message /CRC_Check() = TRUE => command = 0x02 (CONNECTION) watchdog restart() & WD = 1 SEND connection response message	CONNECTION
2	RESET	INITIALIZE complete => await message	RESET
3	RESET	RECEIVE reset request message /CRC_Check() = TRUE => command = 0x01 (RESET) watchdog restart() & WD = 1 SEND reset response message	RESET

#	Current	Event /Condition =>actions	Next state
4	RESET	RECEIVE fail-safe request message =>	FAIL-SAFE
5	RESET	RECEIVE reset request message /CRC_Check() = FALSE => INVALID_CRC command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	FAIL-SAFE
6	RESET	RECEIVE reset response message => INVALID_CMD command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	FAIL-SAFE
7	RESET	RECEIVE connection request message /CRC_Check() = FALSE => INVALID_CRC command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	FAIL-SAFE
8	RESET	RECEIVE connection response message => INVALID_CMD command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	FAIL-SAFE
9	RESET	RECEIVE parameter request message => INVALID_CMD command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	FAIL-SAFE
10	RESET	RECEIVE parameter response message => INVALID_CMD command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	FAIL-SAFE
11	RESET	RECEIVE data request message => INVALID_CMD	FAIL-SAFE

#	Current	Event /Condition =>actions	Next state
		command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	
12	RESET	RECEIVE data response message => INVALID_CMD command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	FAIL-SAFE
13	RESET	Watchdog expired() => WD_EXPIRED command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	FAIL-SAFE

7.4.4.3 CONNECTION state

#	Current	Event /Condition =>actions	Next state
14	CONNECTION	RECEIVE parameter request message /CRC_Check() = TRUE => command = 0x03 (PARAMETER) watchdog restart() & WD = 1 SEND parameter response message	WAIT_PARA
15	CONNECTION	RECEIVE fail-safe request message =>	FAIL-SAFE
16	CONNECTION	RECEIVE reset request message => INVALID_CMD command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	FAIL-SAFE
17	CONNECTION	RECEIVE reset response message => INVALID_CMD command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	FAIL-SAFE
18	CONNECTION	RECEIVE connection request message => INVALID_CMD	FAIL-SAFE

#	Current	Event /Condition =>actions	Next state
		command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	
19	CONNECTION	RECEIVE connection response message => INVALID_CMD command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	FAIL-SAFE
20	CONNECTION	RECEIVE parameter request message /CRC_Check() = FALSE => INVALID_CRC command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	FAIL-SAFE
21	CONNECTION	RECEIVE parameter response message => INVALID_CMD command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	FAIL-SAFE
22	CONNECTION	RECEIVE data request message => INVALID_CMD command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	FAIL-SAFE
23	CONNECTION	RECEIVE data response message => INVALID_CMD command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	FAIL-SAFE
24	CONNECTION	Watchdog expired() => WD_EXPIRED command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	FAIL-SAFE

7.4.4.4 WAIT PARAMETER state

#	Current	Event /Condition =>actions	Next state
25	WAIT_PARA	RECEIVE data request message /CRC_Check() = TRUE /service code = connection phase => watchdog stop() & WD = 0 command = 0x04 (DATA) service code = connection phase SEND data response message local heartbeat timer start() remote heartbeat timer start()	DATA
26	WAIT_PARA	RECEIVE fail-safe request message =>	FAIL-SAFE
27	WAIT_PARA	RECEIVE reset request message => INVALID_CMD command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	FAIL-SAFE
28	WAIT_PARA	RECEIVE reset response message => INVALID_CMD command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	FAIL-SAFE
29	WAIT_PARA	RECEIVE connection request message => INVALID_CMD command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	FAIL-SAFE
30	WAIT_PARA	RECEIVE connection response message => INVALID_CMD command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	FAIL-SAFE
31	WAIT_PARA	RECEIVE parameter request message => INVALID_CMD command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	FAIL-SAFE

#	Current	Event /Condition =>actions	Next state
32	WAIT_PARA	RECEIVE parameter response message => INVALID_CMD command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	FAIL-SAFE
33	WAIT_PARA	RECEIVE data request message /service code = data phase => INVALID_CMD command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	FAIL-SAFE
34	WAIT_PARA	RECEIVE data request message /CRC check() = FALSE => INVALID_CRC command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	FAIL-SAFE
35	WAIT_PARA	RECEIVE data response message => INVALID_CMD command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	FAIL-SAFE
36	WAIT_PARA	Watchdog expired() => WD_EXPIRED command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	FAIL-SAFE

7.4.4.5 DATA state

#	Current	Event /Condition =>actions	Next state
37	DATA	Functional safety application needs to send request message to the partner => watchdog start() & WD = 1 command = 0x04 (DATA) service code = data phase SEND data request message	DATA

#	Current	Event /Condition =>actions	Next state
38	DATA	Functional safety application needs to send response message to the partner => command = 0x04 (DATA) service code = data phase SEND data response message	DATA
39	DATA	RECEIVE data request message /CRC_Check() = TRUE /service code = data phase => Received data forwarding to the functional safety application	DATA
40	DATA	RECEIVE data response message /CRC_Check() = TRUE /service code = data phase => watchdog stop() & WD = 0 Received data forwarding to the functional safety application	DATA
41	DATA	RECEIVE heartbeat message /CRC_Check() = TRUE => remote heartbeat timer restart()	DATA
42	DATA	local heartbeat timer expired => local heartbeat timer start() SEND heartbeat message	DATA
43	DATA	RECEIVE fail-safe request message =>	FAIL-SAFE
44	DATA	RECEIVE reset request message => INVALID_CMD command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	FAIL-SAFE
45	DATA	RECEIVE reset response message => INVALID_CMD command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	FAIL-SAFE
46	DATA	RECEIVE connection request message => INVALID_CMD command = 0x05(FAIL-SAFE) service code = error notification	FAIL-SAFE

#	Current	Event /Condition =>actions	Next state
		SEND fail-safe request message	
47	DATA	RECEIVE connection response message => INVALID_CMD command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	FAIL-SAFE
48	DATA	RECEIVE parameter request message => INVALID_CMD command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	FAIL-SAFE
49	DATA	RECEIVE parameter response message => INVALID_CMD command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	FAIL-SAFE
50	DATA	RECEIVE data request message /CRC_Check() = FALSE => INVALID_CRC command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	FAIL-SAFE
51	DATA	RECEIVE data response message /service code = connection phase => INVALID_CMD command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	FAIL-SAFE
52	DATA	RECEIVE data response message /service code = data phase /CRC_Check() = FALSE => INVALID_CRC command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	FAIL-SAFE
53	DATA	Watchdog expired() =>	FAIL-SAFE

#	Current	Event /Condition =>actions	Next state
		WD_EXPIRED command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	
54	DATA	remote heartbeat timer expired => HB_EXPIRED command = 0x05(FAIL-SAFE) service code = error notification SEND fail-safe request message	FAIL-SAFE

7.4.4.6 FAIL-SAFE state

#	Current	Event /Condition =>actions	Next state
55	FAIL-SAFE	User trigger => await message	RESET
56	FAIL-SAFE	watchdog expired =>	FAIL-SAFE
57	FAIL-SAFE	local heartbeat timer expired =>	FAIL-SAFE
58	FAIL-SAFE	remote heartbeat timer expired =>	FAIL-SAFE
59	FAIL-SAFE	RECEIVE reset request message => discard message	FAIL-SAFE
60	FAIL-SAFE	RECEIVE reset response message => discard message	FAIL-SAFE
61	FAIL-SAFE	RECEIVE connection request message => discard message	FAIL-SAFE
62	FAIL-SAFE	RECEIVE connection response message => discard message	FAIL-SAFE
63	FAIL-SAFE	RECEIVE parameter request message => discard message	FAIL-SAFE
64	FAIL-SAFE	RECEIVE parameter response message => discard message	FAIL-SAFE
65	FAIL-SAFE	RECEIVE data request message	FAIL-SAFE

#	Current	Event /Condition =>actions	Next state
		=> discard message	
66	FAIL-SAFE	RECEIVE data response message => discard message	FAIL-SAFE

8 Safety communication layer management

8.1 FSCP 17/1 parameter handling

The FSCP 17/1 device compares parameters with its communication partner. The functional safety Responder checks parameters received from the functional safety Initiator in the parameter state.

8.2 Functional Safety communication parameters

The functional safety communication between the functional safety Initiator and the functional safety Responder uses the functional safety communication parameters defined in Table 22.

Table 22 – Functional Safety communication parameters

Name	Data Type	Range	Description
SUID	UINT64	0 … 2^{64}-1	Unique connection ID between the functional safety Sender and the functional safety Receiver
Functional Safety watchdog time	UINT16	1 … 2^{16}-1	Watchdog time for the functional safety connection in ms
local heartbeat timer	UINT16	1 … 2^{16}-1	Local heartbeat time in ms
remote heartbeat timer	UINT16	1 … 2^{16}-1	Remote heartbeat time in ms

9 System requirements

9.1 Indicators and switches

Each safety device shall have a red LED, which shall represent the following states:

- Off: No error; device is in safety process-data mode.
- On: Failure state of the device; device has failed.

Each safety device shall have one or more switches to determine the device address on the CPF 17 network.

9.2 Installation guidelines

The installation guidelines of IEC 61918 and the CPF 17 specific amendments in IEC 61784-5-17 shall apply.

9.3 Safety function response time

The safety function response time is a safety related event whether as input to the system or as a fault within the system, until the time that the system is in the safety state. The scope of the reaction time is defined in Figure 15.

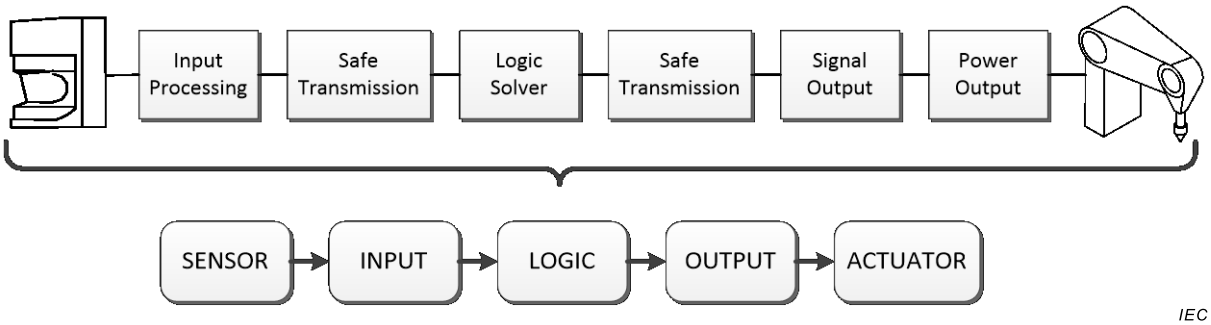


Figure 15 – Safety function response time

In Figure 15, the sensor (for example switch, light curtain or transmitter) gets physical input that is converted into an electrical signal. The signal data are contained in a functional safety message that is transferred to a safety logic device (for example safety PLC) via a safety communication channel. The safety logic device analyses the safety message and generates a safety output message for the functional safety output device. The output device performs a safety action as indicated by the received safety message.

The safety function response time is calculated with Formula (1):

$$T_{FS\_RSP} = T_{Sensor} + T_{Input} + 2 \times T_{Delay} + T_{Logic} + T_{Output} + T_{Actuator} \quad (1)$$

where

T_{FS_RSP} is the safety function response time;

T_{Sensor} is the sensor reaction time;

T_{Input} is the input reaction time;

T_{Delay} is the network delivery time for one way;

T_{Logic} is the safety controller reaction time;

T_{Output} is the output reaction time;

$T_{Actuator}$ is the actuator reaction time.

These time values depend on the system characteristics except the network delivery time T_{Delay}. The network delivery time varies with packet transmit time, cable length, node latency of each relaying device, traversal time of each device from PHY to SCL. The network delivery time T_{Delay} is calculated by Formula (2).

$$T_{DELAY} = max\left\{T_{SND} + T_{PKT} + T_{CPD} + \sum_{i=0}^{N} T_{NLD\_i} + T_{RCV}, WDT\right\} \quad (2)$$

where

T_{DELAY} is the delivery time in microseconds;

T_{SND} is the sender stack traversal time including PHY and MAC in microseconds;

T_{PKT} is the packet transmit time in microseconds, see Formula (3);

T_{CPD} is the cable propagation delay time in microseconds, see Formula (4);

T_{NLD_i} is the node latency delay time of node i in microseconds, see Formula (5);

T_{RCV} is the receiver stack traversal time including PHY and MAC in microseconds;

N is the number of nodes between sending and receiving devices. In FSCP 17/1, the maximum number is 128;

WDT is the watchdog timer. The value is width of 16 bits in ms.

NOTE In FSCP 17/1, the number of node means how many times the frame is relayed. Thus number of node includes switches in the path to the communication partner.

The packet transmit time T_{PKT} can be calculated by Formula (3).

$$T_{PKT} = \frac{(FSPDUsize + POsize) \times 8}{LDR} \quad (3)$$

where

T_{PKT} is the packet transmit time in microseconds;

$FSPDUsize$ is the size of the FSCP 17/1 FSPDU in octets;

LDR is the link data rate in bit per seconds;

$POsize$ is the size of the protocol overhead of CPF 17 in octets.

The cable propagation delay time T_{CPD} can be calculated by Formula (4).

$$T_{CPD} = T_{CPD/M} \times L_{TC} \quad (4)$$

where

T_{CPD} is the cable propagation delay time in microseconds;

$T_{CPD/M}$ is the cable propagation delay in nanoseconds per meter (depending on the characteristics of the selected cable);

L_{TC} is the total cable length in meter.

The node latency delay time T_{NLD_i} can be calculated by Formula (5).

$$T_{NLD\_i} = T_{NPD\_i} + T_{PKT\_i} + \sum_{j=0}^{M} T_{TX\_PKT\_ij} \quad (5)$$

where

T_{NLD_i} is the node latency delay time of node i in microseconds;

T_{NPD_i} is the node propagation delay time of node i in microseconds;

T_{PKT_i} is the packet transmit time of node i in microseconds, see Formula (3);

$T_{TX\_PKT\_ij}$ is the packet transmit time of packet j in microseconds in the port transmit queue of node i in front of this packet (depending on FSPDU size of node i), see Formula (3);

M is the number of packets in the port transmit queue of node i in front of this packet.

9.4 Duration of demands

The duration of a demand by a safety-related application to the SCL shall be sufficient to ensure that it is longer than the watchdog time or the heartbeat time to be detected by the application.

9.5 Constraints for calculation of system characteristics

9.5.1 General

Safety devices are designed for normal industrial environments according to IEC 61000-6-2 or IEC 61131-2 and provide increased immunity according to IEC 61326-3-1 or IEC 61326-3-2.

Several constraints shall be used for calculating safety related characteristics of systems using FSCP 17/1.

9.5.2 Number of devices

FSCP 17/1 implementations are limited to a maximum of 128 devices. To calculate the residual error rate for a specific safety function, Formula (1) in IEC 61784-3:— shall be applied.

9.5.3 Probabilistic consideration

FSCP 17/1 provides for a residual error rate under 10^{-9} per hour with a bit error rate of 0,01. The FSCP 17/1 PDU for functional safety communication has multiple CRC fields in a frame, the CRC polynomial is not the same as the FCS of Ethernet frame.

For example, an FSPDU with a 4 octets header field and a 4 octets safety data field has a residual error probability of approximately $1{,}06 \times 10^{-20}$ with the given CRC polynomial.

The error probability of an FSPDU is calculated according to Formula (6):

$$PE(BER) = 1 - \left\{1 - R_{sl}(BER)\right\}^{n} \tag{6}$$

where

$PE(BER)$ is the packet error rate of the FSPDU;

$R_{sl}(BER)$ is the residual error rate of the basic FSPDU, with a value of $1{,}06 \times 10^{-20}$;

BER is the bit error rate, with a value of 0,01;

n is the number of safety data blocks include the header field, with the unit of value being a set of 4 octets.

Figure 16 shows the residual error rate of FSCP 17/1.

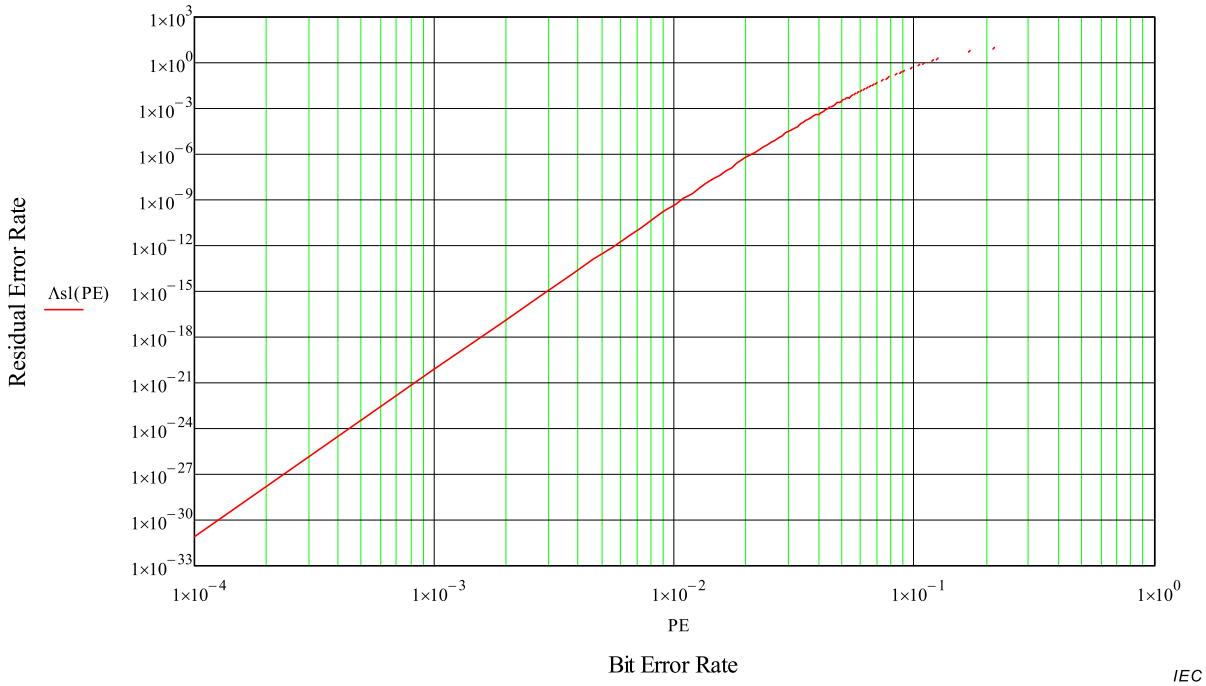


Figure 16 – Residual error rate of FSCP 17/1

9.6 Maintenance

There are no special maintenance requirements for this protocol.

9.7 Safety manual

Implementers of this part shall supply a safety manual with the following information at a minimum:

- Constraints for calculation of system characteristics.
- Users' responsibilities for the proper parameterization of the device.

In addition to the requirements of Clause 9, the safety manual shall follow all requirements in IEC 61508.

10 Assessment

It is highly recommended that implementers of FSCP 17/1 obtain verification for all functional safety aspects of the product, including both the protocol and any application, in accordance with the independence and competence requirements of IEC 61508-1:2010, Clause 8. It is highly recommended that implementers of FSCP 17/1 obtain confirmation that a suitable conformance test has been performed.

Annex A
(informative)

Additional information for functional safety communication profiles of CPF 17

A.1 Hash function calculation

```
// The crc polynomial chosen is [0x00015A67], it is in detail:
// G(x)={x32+x16+x14+x12+x11+x9+x6+x5+x2+x1+1}

#define POLYNOMIAL 0x00015A67

void gen_crc_code()
{
        uint32 i, j;
        uint32 crc_accum;

        for(i=0; i<256; i++)
        {
                crc_accum = (i << 24);
                for(j=0; j<8; j++)
                {
                        if(crc_accum & 0x80000000)
                                crc_accum = (crc_accum << 1) ^ POLYNOMIAL;
                        else
                                crc_accum = (crc_accum << 1);
                }
                crc_table[i] = crc_accum;
        }
        return;
}

uint32 CRCTable[256];
uint32 CRC32(uint8 *pucData, uint32 ulSize)
{
        uint32 crc_accum = 0;
        uint32 i, j, k;

        for(j=0;j<ulSize;j++){
                i = (crc_accum ^ * pucData ++);
                crc_accum = 0;
                for(k=0;k<4;k++)
                {
                        crc_accum = crc_accum ^ (CRCTable[(i >> (k*8)) & 0xff] << k*8);
                }
        }
        return crc_accum;
}
```

The CRC32 for FSCP 17/1 is calculated using the following algorithm:

$$G(x)=\{x^{32}+x^{16}+x^{14}+x^{12}+x^{11}+x^{9}+x^{6}+x^{5}+x^{2}+x^{1}+1\}$$

This polynomial provides a minimum hamming distance of 11 up to 65 bits code word [39].

The lookup table for this polynomial for each 8 bits is shown in Table A.1 below.

Table A.1 – the lookup table for FSCP 17/1

CRC lookup table (0...255)							
00000000	00015a67	0002b4ce	0003eea9	0005699c	000433fb	0007dd52	00068735
000ad338	000b895f	000867f6	00093d91	000fbaa4	000ee0c3	000d0e6a	000c540d
0015a670	0014fc17	001712be	001648d9	0010cfec	0011958b	00127b22	00132145
001f7548	001e2f2f	001dc186	001c9be1	001a1cd4	001b46b3	0018a81a	0019f27d
002b4ce0	002a1687	0029f82e	0028a249	002e257c	002f7f1b	002c91b2	002dcbd5
00219fd8	0020c5bf	00232b16	00227171	0024f644	0025ac23	0026428a	002718ed
003eea90	003fb0f7	003c5e5e	003d0439	003b830c	003ad96b	003937c2	00386da5
003439a8	003563cf	00368d66	0037d701	00315034	00300a53	0033e4fa	0032be9d
005699c0	0057c3a7	00542d0e	00557769	0053f05c	0052aa3b	00514492	00501ef5
005c4af8	005d109f	005efe36	005fa451	00592364	00587903	005b97aa	005acdcd
00433fb0	004265d7	00418b7e	0040d119	0046562c	00470c4b	0044e2e2	0045b885
0049ec88	0048b6ef	004b5846	004a0221	004c8514	004ddf73	004e31da	004f6bbd
007dd520	007c8f47	007f61ee	007e3b89	0078bcbc	0079e6db	007a0872	007b5215
00770618	00765c7f	0075b2d6	0074e8b1	00726f84	007335e3	0070db4a	0071812d
00687350	00692937	006ac79e	006b9df9	006d1acc	006c40ab	006fae02	006ef465
0062a068	0063fa0f	006014a6	00614ec1	0067c9f4	00669393	00657d3a	0064275d
00ad3380	00ac69e7	00af874e	00aedd29	00a85a1c	00a9007b	00aaeed2	00abb4b5
00a7e0b8	00a6badf	00a55476	00a40e11	00a28924	00a3d343	00a03dea	00a1678d
00b895f0	00b9cf97	00ba213e	00bb7b59	00bdfc6c	00bca60b	00bf48a2	00be12c5
00b246c8	00b31caf	00b0f206	00b1a861	00b72f54	00b67533	00b59b9a	00b4c1fd
00867f60	00872507	0084cbae	008591c9	008316fc	00824c9b	0081a232	0080f855
008cac58	008df63f	008e1896	008f42f1	0089c5c4	00889fa3	008b710a	008a2b6d
0093d910	00928377	00916dde	009037b9	0096b08c	0097eaeb	00940442	00955e25
00990a28	0098504f	009bbee6	009ae481	009c63b4	009d39d3	009ed77a	009f8d1d
00fbaa40	00faf027	00f91e8e	00f844e9	00fec3dc	00ff99bb	00fc7712	00fd2d75
00f17978	00f0231f	00f3cdb6	00f297d1	00f410e4	00f54a83	00f6a42a	00f7fe4d
00ee0c30	00ef5657	00ecb8fe	00ede299	00eb65ac	00ea3fcb	00e9d162	00e88b05
00e4df08	00e5856f	00e66bc6	00e731a1	00e1b694	00e0ecf3	00e3025a	00e2583d
00d0e6a0	00d1bcc7	00d2526e	00d30809	00d58f3c	00d4d55b	00d73bf2	00d66195
00da3598	00db6fff	00d88156	00d9db31	00df5c04	00de0663	00dde8ca	00dcb2ad
00c540d0	00c41ab7	00c7f41e	00c6ae79	00c0294c	00c1732b	00c29d82	00c3c7e5
00cf93e8	00cec98f	00cd2726	00cc7d41	00cafa74	00cba013	00c84eba	00c914dd
This table contains 32 bit values in hexadecimal representation for each value (0...255) of the 8 bits variations. The table should be used in ascending order from top left (0) to bottom right (255).							

A.2 ...

Void

Annex B
(informative)

Information for assessment of the functional safety communication profiles of CPF 17

According to IEC rules, this standard does not make a statement on how to validate conformance. However, test and validation of compliance of FSCP 17/1 devices with IEC 61784-3-17 may be required by law.

Corresponding information relative to the test and compliance with this standard can be retrieved from the local National Committees of the IEC or from the relevant fieldbus organization.

NOTE For IEC 61784-3-17, the relevant fieldbus organization is Automation Control Team, LSIS Co Ltd, see www.lsis.biz.

Bibliography

[1] IEC 60050 (all parts), *International Electrotechnical Vocabulary* available at <http://www.electropedia.org/)

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

[2] IEC 60050-191:1990, *International Electrotechnical Vocabulary – Part 191: Dependability and quality of service*

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

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

[5] IEC 61000-6-7:2014, *Electromagnetic compatibility (EMC) – Part 6-7: Generic standards – Immunity requirements for equipment intended to perform functions in a safety-related system (functional safety) in industrial locations*

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

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

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

[9] IEC 61508-2, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*

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

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

[12] IEC 61511 (all parts), *Functional safety – Safety instrumented systems for the process industry sector*

[13] IEC 61784-4 [6], *Industrial communication networks – Profiles – Part 4: Secure communications for fieldbuses*

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

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

[16] IEC TR 62059-11:2002, *Electricity metering equipment – Dependability – Part 11: General concepts*

6 Proposed new work item under consideration.

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

[18] IEC TR 62210:2003, *Power system control and associated communications – Data and communication security*

[19] IEC 62280:2014, *Railway applications – Communication, signalling and processing systems –Safety related communication in transmission systems*

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

[21] IEC TR 62685, *Industrial communication networks – Profiles – Assessment guideline for safety devices using IEC 61784-3 functional safety communication profiles (FSCPs)*

[22] ISO/IEC Guide 51:2014, *Safety aspects – Guidelines for their inclusion in standards*

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

[24] ISO/IEC 2382-16:1996, *Information technology – Vocabulary – Part 16: Information theory*

[25] ISO/IEC 7498-1:1994, *Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model*

[26] ISO 10218-1, *Robots and robotic devices – Safety requirements for industrial robots – Part 1: Robots*

[27] ISO 12100, *Safety of machinery – General principles for design – Risk assessment and risk reduction*

[28] ISO 13849 (all parts), *Safety of machinery – Safety-related parts of control systems*

[29] ISO 13849-1:2006, *Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design*

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

[31] IEEE 802.3, *IEEE Standard for 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*

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

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

[34] ANDREW S. TANENBAUM, DAVID J. WETHERALL, *Computer Networks,* 5th Edition, Prentice Hall, N.J., ISBN-10: 0132126958, ISBN-13: 978-0132126953

[35] W. WESLEY PETERSON, EDWARD J. WELDON, *Error-Correcting Codes*, 2nd Edition 1972, MIT-Press, ISBN 0-262-16-039-0

[36] NFPA79 (2012), *Electrical Standard for Industrial Machinery*

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

[38] 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

[39] JUSTIN RAY and PHILIP KOOPMAN: *Efficient High Hamming Distance CRCs for Embedded Networks*, Proceedings of the 2006 International Conference on Dependable Systems and Networks (DSN'06), IEEE Conference Publications 2006, pp3-12.

SOMMAIRE

AVANT-PROPOS 77
0 Introduction 79
0.1 Généralités 79
0.2 Déclaration de droits de propriété 82
1 Domaine d'application 84
2 Références normatives 84
3 Termes, définitions, symboles, abréviations et conventions 85
3.1 Termes et définitions 85
3.1.1 Termes et définitions communs 85
3.1.2 CPF 17: Termes et définitions supplémentaires 91
3.2 Symboles et abréviations 92
3.2.1 Symboles et abréviations communs 92
3.2.2 CPF 17: Symboles et abréviations supplémentaires 92
3.3 Conventions 93
4 Présentation générale de FSCP 17/1 (RAPIEnet Safety™) 93
5 Généralités 95
5.1 Documents externes de spécifications applicables au profil 95
5.2 Exigences fonctionnelles de sécurité 95
5.3 Mesures de sécurité 95
5.3.1 Généralités 95
5.3.2 Numéro de séquence (virtuel) 96
5.3.3 Délai avec le chien de garde 96
5.3.4 Authentification de connexion 96
5.3.5 Message de réaction 96
5.3.6 Assurance d'intégrité des données 96
5.4 Structure de la couche de communication de sécurité 97
5.4.1 Principe des communications de sécurité FSCP 17/1 97
5.4.2 Structures de communication CPF 17 97
5.5 Relations avec la FAL (et DLL, PhL) 98
5.5.1 Généralités 98
5.5.2 Types de données 98
6 Services de la couche de communication de sécurité 98
6.1 Présentation générale 98
6.2 Connexion de sécurité fonctionnelle 98
6.2.1 Généralités 98
6.2.2 Spécification de classe d'initiateur 99
6.2.3 Spécification de la classe du répondeur 100
6.2.4 Spécification de classe d'émetteur 101
6.2.5 Spécification de classe de récepteur 103
6.3 Service de transmission de données de sécurité fonctionnelle 104
6.4 Relation de connexion de sécurité fonctionnelle 105
7 Protocole de couche de communication de sécurité 106
7.1 Format PDU de sécurité 106
7.1.1 Généralités 106
7.1.2 Commande FSPDU 107

7.1.3 Clé d'authentification 108
7.1.4 FSPDU CRC 108
7.2 Procédure de communication FSCP 17/1 111
7.2.1 États de l'appareil FSCP 17/1 111
7.3 Réponse aux erreurs de communication 119
7.3.1 Généralités 119
7.4 Table d'état de la SCL de CPF 17 120
7.4.1 Généralités 120
7.4.2 Événements 121
7.4.3 Table d'état de l'initiateur 122
7.4.4 Table d'état du répondeur 128
8 Gestion de la couche de communication de sécurité 135
8.1 Gestion des paramètres FSCP 17/1 135
8.2 Paramètres de communication de sécurité fonctionnelle 135
9 Exigences système 135
9.1 Voyants et commutateurs 135
9.2 Lignes directrices d'installation 135
9.3 Temps de réponse de la fonction de sécurité 135
9.4 Durée des demandes 138
9.5 Contraintes liées au calcul des caractéristiques du système 138
9.5.1 Généralités 138
9.5.2 Nombre d'appareils 138
9.5.3 Considération en matière de probabilité 138
9.6 Maintenance 139
9.7 Manuel de sécurité 139
10 Évaluation 140
Annexe A (informative) Informations supplémentaires pour les profils de communication de sécurité fonctionnelle de CPF 17 141
A.1 Calcul de la fonction de hachage 141
A.2 … 142
Annexe B (informative) Informations pour l'évaluation des profils de communication de sécurité fonctionnelle de CPF 17 143
Bibliographie 144

Figure 1 – Relations entre l'IEC 61784-3 et d'autres normes (machines) 80
Figure 2 – Relations entre l'IEC 61784-3 et d'autres normes (transformation) 82
Figure 3 – Relations de communication entre les appareils FSCP 17 94
Figure 4 – Architecture de couche de sécurité 98
Figure 5 – Cycle de sécurité fonctionnelle 105
Figure 6 – Relations de connexion parmi les appareils FSCP 17/1 106
Figure 7 – PDU de sécurité fonctionnelle pour CPF 17 sur PDU de type 21 107
Figure 8 – Processus de génération du code FSPDU CRC 109
Figure 9 – Exemple de modification de numéro de séquence 110
Figure 10 – Opération de comparaison CRC 111
Figure 11 – États de l'appareil FSCP 17/1 112
Figure 12 – Diagramme d'états de l'appareil de sécurité fonctionnelle 121
Figure 13 – Diagramme d'états de l'initiateur 122

Figure 14 – Diagramme d'états du répondeur 128
Figure 15 – Temps de réponse de la fonction de sécurité 136
Figure 16 – Taux d'erreurs résiduelles de FSCP 17/1 139

Tableau 1 – Mesures déployées pour maîtriser les erreurs 96
Tableau 2 – FSPDU général 107
Tableau 3 – Commande FSPDU 108
Tableau 4 – FSPDU avec 4 octets de données de sécurité et la commande RESET après redémarrage (connexion de réinitialisation) ou après une erreur 113
Tableau 5 – FSPDU avec 4 octets de données de sécurité et la commande RESET pour acquitter une commande de réinitialisation à partir de l'initiateur 114
Tableau 6 – PDU de demande de connexion pour l'initiateur à l'état CONNECTION 114
Tableau 7 – PDU de réponse de connexion pour le répondeur à l'état CONNECTION 115
Tableau 8 – Données de sécurité transférées à l'état SET_PARA 115
Tableau 9 – Envoi d'un FSPDU avec 6 octets de données de sécurité de la part de l'initiateur à l'état SET_PARA 116
Tableau 10 – FSPDU prévu avec 6 octets de données de sécurité provenant du répondeur à l'état SET_PARA 116
Tableau 11 – Données de sécurité provenant de l'initiateur à l'état WAIT_PARA 117
Tableau 12 – Envoi d'un FSPDU avec 6 octets de données de sécurité de la part de l'initiateur à l'état WAIT_PARA 117
Tableau 13 – Réception du FSPDU avec 6 octets de données de sécurité provenant du répondeur à l'état WAIT_PARA state 118
Tableau 14 – FSPDU de données de sécurité à l'état DATA 119
Tableau 15 – Exemple de 4 octets de données de sécurité provenant d'un émetteur 119
Tableau 16 – Exemple d'ACK PDU provenant du récepteur avec 4 octets de données de sécurité 119
Tableau 17 – Erreurs de communication de sécurité fonctionnelle 120
Tableau 18 – Codes d'erreur de communication de sécurité fonctionnelle 120
Tableau 19 – États de l'initiateur de sécurité fonctionnelle 121
Tableau 20 – États du répondeur de sécurité fonctionnelle 121
Tableau 21 – Événements de l'état de sécurité fonctionnelle 122
Tableau 22 – Paramètres de communication de sécurité fonctionnelle 135
Tableau A.1 – Table de recherche pour FSCP 17/1 142

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

RÉSEAUX DE COMMUNICATION INDUSTRIELS – PROFILS –

Partie 3-17: Bus de terrain de sécurité fonctionnelle – Spécifications supplémentaires pour CPF 17

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. À cet effet, l'IEC – 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 l'IEC"). 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 l'IEC, participent également aux travaux. L'IEC 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 l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC 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 l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) L'IEC 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 l'IEC. L'IEC 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 l'IEC, 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 l'IEC, 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 l'IEC ou de toute autre Publication de l'IEC, 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.

La Norme internationale IEC 61784-3-17 a été établie par le sous-comité 65C: Réseaux industriels, du comité d'études 65 de l'IEC: Mesure, commande et automation dans les processus industriels.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
65C/851/FDIS	65C/854/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à l'approbation de cette norme.

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

Une liste de toutes les parties de la série IEC 61784-3, publiées sous le titre général *Réseaux de communication industriels – Profils – Bus de terrain de sécurité fonctionnelle*, peut être consultée sur le site web de l'IEC.

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 l'IEC sous "http://webstore.iec.ch" dans les données relatives à la publication recherchée. À 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 couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

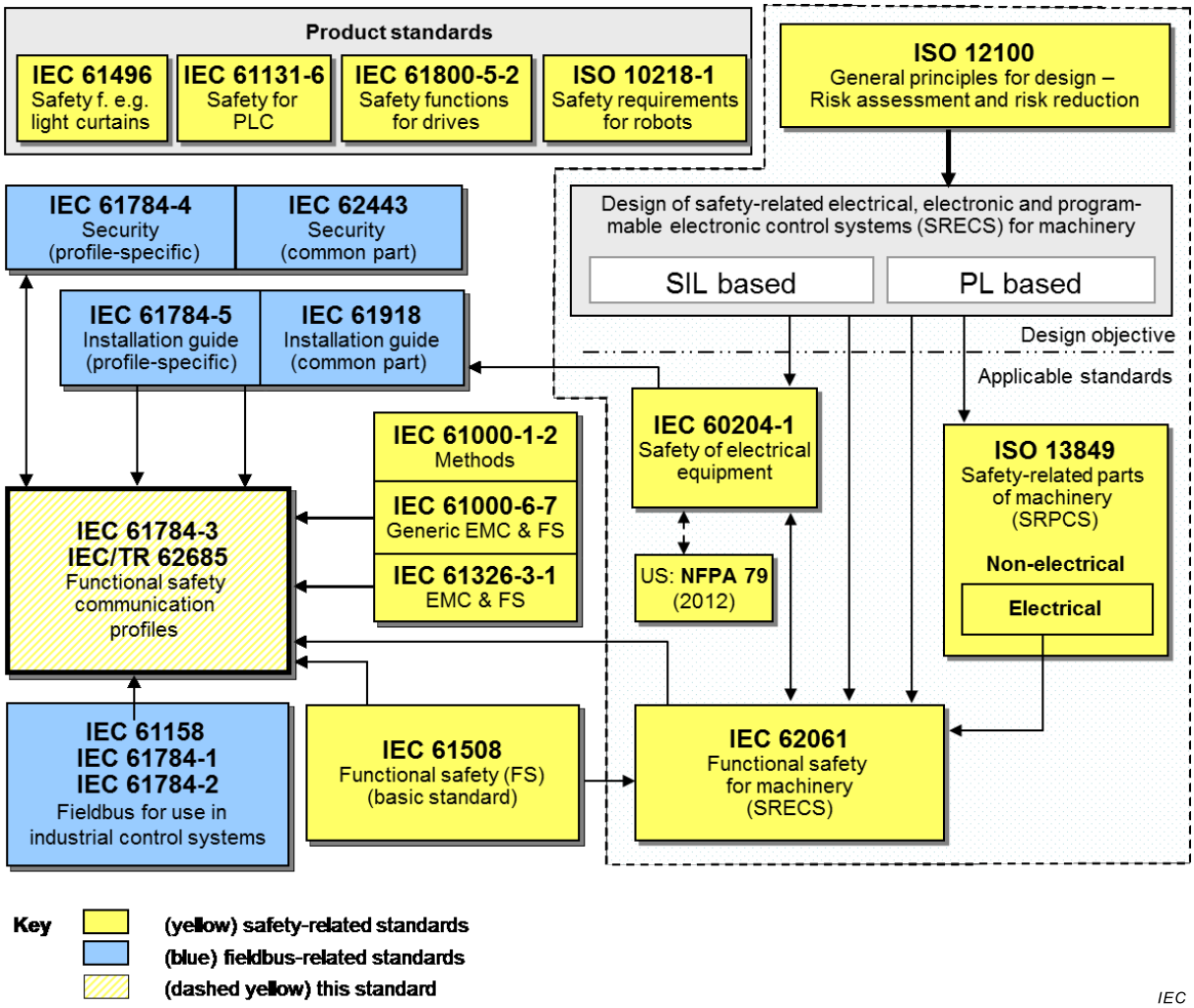
0 Introduction

0.1 Généralités

L'IEC 61158 relative aux bus de terrain, ainsi que ses normes associées IEC 61784-1 et IEC 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, les améliorations des bus de terrain continuent à se développer, traitant des applications pour des domaines 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 IEC 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 l'IEC 61784-2 et de la série IEC 61158. Elle ne couvre pas les aspects relatifs à la sécurité électrique et à la sécurité intrinsèque.

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



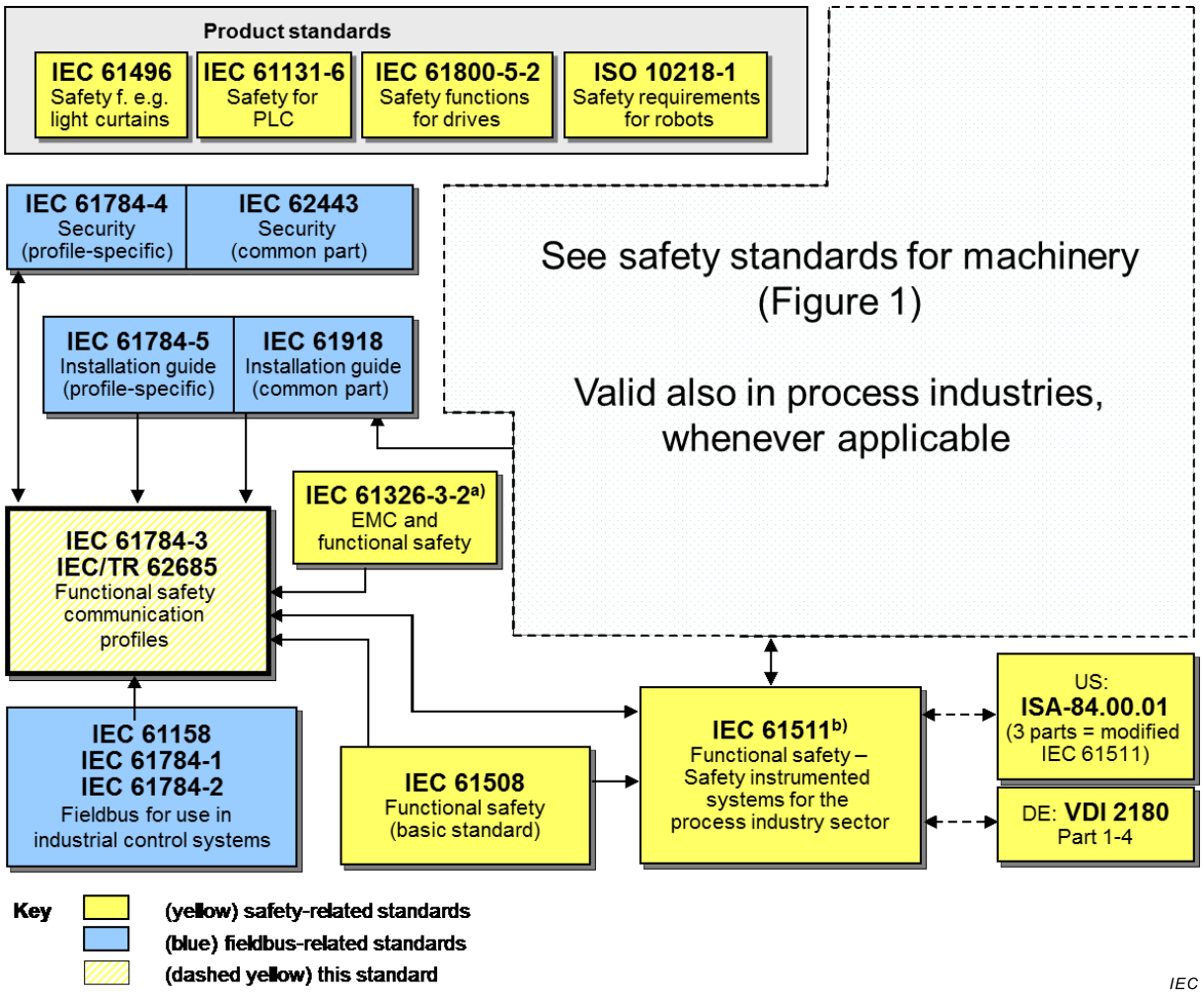
Anglais	Français
Product standards	Normes de produits
Safety function, e.g. light curtains	Fonction de sécurité, par exemple rideaux de lumière
Safety for PLC	Sécurité relative aux automates programmables

Anglais	Français
Safety functions for drives	Fonctions de sécurité applicables aux entraînements
Safety requirements for robots	Exigences de sécurité applicables aux robots
General principles for design – Risk assessment and risk reduction	Principes généraux de conception – Appréciation du risque et réduction du risque
Security (profile-specific)	Sûreté (spécifique au profil)
Security (common part)	Sûreté (partie commune)
Design of safety-related electrical, electronic and programmable electronic control systems (SRECS) 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)
Design objective	Objectif de conception
Applicable standards	Normes applicables
Methods	Méthodes
Generic EMC & FS	CEM & FS génériques
EMC & FS	CEM & FS
Safety of electrical equipment	Sécurité des équipements électriques
Safety-related parts of machinery (SRPCS)	Sécurité des machines – Parties des systèmes de commande relatives à la sécurité
Non-electrical	Non électrique
Electrical	Électrique
Functional safety communication profiles	Profils de communication de sécurité fonctionnelle
Fieldbus for use in industrial control systems	Bus de terrain pour utilisation dans des systèmes de commande industriels
Functional safety (FS) (basic standard)	Sécurité fonctionnelle (FS) (norme de base)
Functional safety for machinery (SRECS)	Sécurité fonctionnelle des machines
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

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

Figure 1 – Relations entre l'IEC 61784-3 et d'autres normes (machines)

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



IEC

Anglais	Français
Product standards	Normes de produits
Safety function, e.g. light curtains	Fonction de sécurité, par exemple rideaux de lumière
Safety for PLC	Sécurité relative aux automates programmables
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
EMC and functional safety	CEM et sécurité fonctionnelle
Fieldbus for use in industrial control systems	Bus de terrain pour utilisation dans des systèmes de commande industriels
Functional safety (basic standard)	Sécurité fonctionnelle (norme de base)
Functional safety – Safety instrumented systems for the process industry sector	Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur des industries de transformation
3 parts = modified IEC 61511	3 parties = IEC 61511 modifiée

Anglais	Français
Part 1 –4	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 IEC 61326-3-1 ou IEC 61000-6-7

[b] EN ratifiée.

Figure 2 – Relations entre l'IEC 61784-3 et d'autres normes (transformation)

Les couches de communication de sécurité mises en œuvre dans le cadre de systèmes relatifs à la sécurité conformément à la série IEC 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 (FSCP) retenu au sein du système – la mise en œuvre du profil de communication de sécurité fonctionnelle dans un appareil normal ne suffit pas à le qualifier d'appareil de sécurité.

La présente norme décrit:

- les principes de base de la mise en œuvre des exigences de la série IEC 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;
- les profils de communication de sécurité fonctionnelle pour plusieurs familles de profils de communication dans l'IEC 61784-1 et l'IEC 61784-2, y compris les extensions de la couche de sécurité aux sections relatives au service et aux protocoles de communication de la série IEC 61158.

0.2 Déclaration de droits de propriété

La Commission Électrotechnique Internationale (IEC) attire l'attention sur le fait qu'il est déclaré que la conformité aux dispositions du présent document peut impliquer l'utilisation de brevets intéressant les profils de communication de sécurité fonctionnelle pour la famille 17 tels que définis ci-après, où la notation [xx] désigne le détenteur des droits de propriété:

PCT/KR2012/008651 [LSIS] Appareil de communication et méthode de communication

PCT/KR2012/008653 [LSIS] Appareil de communication et méthode de communication

PCT/KR2012/008654 [LSIS] Appareil de communication et méthode de communication

PCT/KR2012/008655 [LSIS] Appareil de communication et méthode de communication

KR 10-1389604 [LSIS] Appareil de communication et méthode de communication

KR 10-1442963	[LSIS]	Appareil de communication et méthode de communication
KR 10-1389646	[LSIS]	Appareil de communication et méthode de communication

L'IEC ne prend pas position quant à la preuve, à la validité et à la portée de ces droits de propriété.

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

Des informations peuvent être demandées à:

[LSIS] LSIS Co Ltd
LS Tower
1026-6, Hogye-Dong
Dongan-Gu
Anyang, Gyeonggi-Do, 431-848
Corée du Sud

L'attention est d'autre part attirée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété intellectuelle autres que ceux identifiés ci-dessus. L'IEC 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 3-17: Bus de terrain de sécurité fonctionnelle – Spécifications supplémentaires pour CPF 17

1 Domaine d'application

La présente partie de la série IEC 61784-3 spécifie une couche de communication de sécurité (services et protocole) reposant sur CPF 17 de l'IEC 61784-2 (CP 17/1) et de l'IEC 61158 Type 21. Elle identifie les principes en matière de communications de sécurité fonctionnelle définies dans l'IEC 61784-3 pertinents pour cette couche de communication de sécurité. Cette couche de communication de sécurité est destinée à la mise en œuvre sur les appareils de sécurité uniquement.

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 IEC 61508[2] pour 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 d'appareils 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 appareil normal ne suffit pas à le qualifier d'appareil de sécurité.

2 Références normatives

Les documents suivants sont cités en référence de manière normative, en intégralité ou en partie, dans le présent document et sont indispensables pour son application. 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 61000-6-2, *Compatibilité électromagnétique (CEM) – Partie 6-2: Normes génériques – Immunité pour les environnements industriels*

IEC 61131-2, *Automates programmables – Partie 2: Exigences et essais des équipements*

IEC 61158-3-21:2010, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 3-21: Définition des services de la couche liaison de données – Éléments de Type 21*

---

1 Dans les pages suivantes de la présente norme, "la présente partie" se substitue à "cette partie de la série IEC 61784-3".

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

IEC 61158-4-21:2010, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 4-21: Spécification du protocole de la couche liaison de données – Éléments de Type 21*

IEC 61158-5-21:2010, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 5-21: Définition des services de la couche application – Éléments de Type 21*

IEC 61158-6-21:2010, *Industrial communication networks – Fieldbus specifications – Part 6 21: Application layer protocol specification – Type 21 elements* (disponible en anglais seulement)

IEC 61326-3-1, *Matériel électrique de mesure, de commande et de laboratoire – Exigences relatives à la CEM – Partie 3-1: Exigences d'immunité pour les systèmes relatifs à la sécurité et pour les matériels destinés à réaliser des fonctions relatives à la sécurité (sécurité fonctionnelle) – Applications industrielles générales*

IEC 61326-3-2, *Matériel électrique de mesure, de commande et de laboratoire – Exigences relatives à la CEM – Partie 3-2: Exigences d'immunité pour les systèmes relatifs à la sécurité et pour les matériels destinés à réaliser des fonctions relatives à la sécurité (sécurité fonctionnelle) – Applications industrielles dont l'environnement électromagnétique est spécifié*

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

IEC 61508-1:2010, *Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité – Partie 1: Exigences générales*

IEC 61784-2, *Réseaux de communication industriels – Profils – Partie 2: Profils de bus de terrain supplémentaires pour les réseaux en temps réel basés sur l'ISO/CEI 8802-3*

IEC 61784-3:—[3], *Réseaux de communication industriels – Profils – Partie 3: Bus de terrain de sécurité fonctionnelle – Règles générales et définitions de profils*

IEC 61784-5-17:2013, *Réseaux de communication industriels – Profils – Partie 5-17: Installation des bus de terrain – Profils d'installation pour CPF 17*

IEC 61918, *Réseaux de communication industriels – Installation de réseaux de communication dans des locaux industriels*

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.

NOTE Les définitions des termes eux-mêmes définis en 3.1 sont marquées en italique.

3.1.1 Termes et définitions communs

NOTE Ces termes et définitions communs sont issus de l'IEC 61784-3:—.

3.1.1.1
disponibilité
probabilité, pour un système automatisé, qu'il ne se produise pas de condition opérationnelle non satisfaisante, par exemple la perte de production, pendant une période donnée

[3] A publier.

3.1.1.2
canal noir
système de communication défini qui contient un ou plusieurs éléments sans preuve de conception ou de validation conformément à l'IEC 61508

Note 1 à l'article: Cette définition étend la signification habituelle du canal pour inclure le système qui contient le canal.

3.1.1.3
système de communication fermé
nombre fixe ou nombre maximal fixe d'éléments reliés par un système de communication dont les propriétés sont connues et fixées et où le risque d'accès non autorisé est considéré comme négligeable

[SOURCE: IEC 62280:2014, 3.1.6, modifié – "transmission" remplacé par "communication"]

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

3.1.1.5
système de communication
ensemble de matériels, de logiciels et de supports de propagation qui permet la transmission de *messages* (ISO/IEC 7498-1, couche d'application) d'une application à une autre

3.1.1.6
connexion
liaison logique entre objets applicatifs au sein du même appareil ou d'appareils différents

3.1.1.7
contrôle de redondance cyclique
CRC
<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 à l'article: Les termes "code CRC" et "signature CRC", ainsi que les étiquettes comme CRC1, CRC2, peuvent également être utilisés dans la présente norme pour se référer aux données redondantes.

Note 2 à l'article: Voir également [34], [35][4].

3.1.1.8
système de communication défini
canal défini
nombre fixe ou nombre maximal fixe d'éléments reliés par un système de communication à bus de terrain, dont les propriétés sont connues et fixées, par exemple les conditions d'installation, l'immunité électromagnétique, les éléments (actifs) de réseau industriel, et où le risque d'accès non autorisé est réduit à un niveau tolérable conformément au modèle de cycle de vie de l'IEC 62443, en utilisant par exemple des zones et des conduits

3.1.1.9
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

_____

4 Les chiffres entre crochets se réfèrent à la bibliographie.

Note 1 à l'article: Les erreurs peuvent être causées par des erreurs de conception du matériel/logiciel et/ou des informations altérées du fait d'un brouillage électromagnétique et/ou autres effets.

Note 2 à l'article: Les erreurs ne produisent pas nécessairement une *défaillance* ou une *anomalie*.

[SOURCE: IEC 61508 4:2010, 3.6.11, modifié – notes ajoutées]

3.1.1.10
défaillance
cessation de l'aptitude d'une unité fonctionnelle à accomplir une fonction requise ou à fonctionner comme prévu

Note 1 à l'article: Une défaillance peut être causée par une *erreur* (problème de conception matérielle/logicielle ou rupture de message, par exemple).

[SOURCE: IEC 61508 4:2010, 3.6.4, modifié – notes et figures remplacées]

3.1.1.11
anomalie
condition anormale qui peut entraîner une réduction de capacité ou la perte de capacité d'une unité fonctionnelle à accomplir une fonction requise

Note 1 à l'article: L'IEC 60050-191:1990, 191-05-01, définit le terme "fault" (en français "panne") comme un état d'inaptitude à accomplir une fonction requise, en excluant l'inaptitude due à la maintenance préventive, à d'autres actions programmées ou à un manque de ressources extérieures.

[SOURCE: IEC 61508 4:2010, 3.6.1, modifié – référence à la figure supprimée]

3.1.1.12
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

3.1.1.13
système de bus de terrain
système qui utilise un *bus de terrain* avec des appareils reliés

3.1.1.14
DLPDU
DÉCONSEILLÉ: trame
Data Link Protocol Data Unit (Unité de données de protocole de liaison de données)

3.1.1.15
séquence de contrôle de trame
FCS
données redondantes issues d'un bloc de données d'une DLPDU (trame), qui utilisent une fonction de hachage et enregistrées ou transmises avec le bloc de données, afin de déterminer l'altération des données

Note 1 à l'article: Une FCS peut être calculée à l'aide, par exemple, d'un CRC ou d'une autre fonction de hachage.

Note 2 à l'article: Voir également [34], [35].

Note 3 à l'article: L'abréviation «FCS» est dérivée du terme anglais développé correspondant «Frame Check Sequence»

3.1.1.16
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 à l'article: Les fonctions de hachage peuvent être utilisées pour déterminer l'altération des données.

Note 2 à l'article: Les fonctions de hachage communes incluent la parité, la somme de contrôle ou le CRC.

[SOURCE: IEC TR 62210:2003, 4.1.12, modifié – ajout de "habituellement" et de notes]

3.1.1.17
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

3.1.1.18
message
série ordonnée d'octets, destinée à véhiculer des informations

[SOURCE: ISO/IEC 2382 16:1996, 16.02.01, modifié – "caractère" remplacé par "octet"]

3.1.1.19
déclenchement de nuisance
déclenchement parasite sans effet préjudiciable

Note 1 à l'article: Les erreurs anormales internes peuvent être générées dans des systèmes de communication, par exemple des systèmes de transmission par ondes radioélectriques, du fait d'un trop grand nombre de nouvelles tentatives en présence de perturbations.

3.1.1.20
essai périodique
essai périodique destiné à détecter les défaillances cachées dangereuses d'un système relatif à la sécurité de telle sorte que, lorsque nécessaire, une réparation peut rétablir le système dans une condition “comme neuf’’ ou dans une condition aussi proche que possible de celle-ci

Note 1 à l'article: Un essai de validité est destiné à confirmer que l’état du système relatif à la sécurité garantit l’intégrité de sécurité spécifiée.

[SOURCE: IEC 61508-4:2010, 3.8.5, modifié – remplacement des quatre notes par une autre note]

3.1.1.21
niveau de performances
PL
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

Note 1 à l'article: L’abréviation «PL» est dérivée du terme anglais développé correspondant «performance level».

[SOURCE: ISO 13849 1:2006, 3.1.23, traduction française modifiée – amélioration]

3.1.1.22
redondance
existence de plusieurs moyens pour accomplir une fonction requise ou pour représenter des informations

[SOURCE: IEC 61508-4:2010, 3.4.6, modifié – exemple et notes supprimés]

3.1.1.23
fiabilité
probabilité pour qu'un système automatisé puisse accomplir une fonction requise, dans des conditions données, pendant un intervalle de temps donné (t1, t2)

Note 1 à l'article: 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 à l'article: Le terme "fiabilité" est aussi employé pour désigner l'aptitude caractérisée par cette probabilité.

Note 3 à l'article: Au cours de la période MTBF ou MTTF, la probabilité qu'un système automatisé exécute une fonction exigée dans les conditions données décroît.

Note 4 à l'article: La fiabilité diffère de la disponibilité.

[SOURCE: IEC TR 62059 11:2002, 3.17, modifié – utilisation des mots "un système automatisé" à la place de "une entité" et ajout de deux notes]

3.1.1.24
probabilité d'erreurs résiduelles
RP
probabilité de non-détection d'une erreur par les mesures de sécurité SCL

Note 1 à l'article: L'abréviation «RP» est dérivée du terme anglais développé correspondant «Residual Error Probability».

3.1.1.25
taux d'erreurs résiduelles
taux statistique de défaut de détection d'erreurs par les mesures de sécurité SCL

3.1.1.26
risque
combinaison de la probabilité d'un dommage et de sa gravité

Note 1 à l'article: Pour plus d'informations sur ce concept, voir l'Annexe A de l'IEC 61508-5:2010.

[SOURCE: IEC 61508 4:2010, 3.1.6, et Guide ISO/IEC 51:2014, définition 3.9, modifié – note différente]

3.1.1.27
canal de communication de sécurité
canal de communication qui débute au sommet de la SCL de la source et qui se termine au sommet de la SCL du collecteur

Note 1 à l'article: Le canal peut être modélisé sous la forme de deux SCL reliées par un canal noir, un système de communication défini ou un canal défini.

3.1.1.28
couche de communication de sécurité
SCL
couche de communication située au-dessus de la FAL qui comprend toutes les mesures supplémentaires nécessaires qui permettent d'assurer la transmission de données en toute sécurité conformément aux exigences de l'IEC 61508

Note 1 à l'article: L'abréviation «SCL» est dérivée du terme anglais développé correspondant «safety Communication Layer».

3.1.1.29
connexion de sécurité
connexion qui utilise le protocole de sécurité pour des transactions de communications

3.1.1.30
données de sécurité
données transmises par un réseau de sécurité qui utilise un protocole de sécurité

Note 1 à l'article: 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.

3.1.1.31
appareil de sécurité
appareil conçu conformément à l'IEC 61508 et qui met en œuvre le profil de communication de sécurité fonctionnelle

3.1.1.32
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

[SOURCE: IEC 61508 4:2010, 3.5.1, modifié – références et exemples supprimés]

3.1.1.33
temps de réponse de la fonction de sécurité
temps écoulé dans le cas le plus défavorable à la suite de l'activation d'un capteur de sécurité relié à un bus de terrain, avant que ne soit atteint l'état de sécurité correspondant de ses actionneurs de sécurité, du fait d'erreurs ou de défaillances dans la fonction de sécurité

Note 1 à l'article: Ce concept, introduit dans l'IEC 61784-3:—, 5.2.4, est traité par les profils de communication de sécurité fonctionnelle définis dans la présente partie.

3.1.1.34
niveau d'intégrité de sécurité
SIL
niveau discret (parmi quatre possibles) correspondant à une gamme de valeurs d'intégrité de sécurité, où le niveau 4 d'intégrité de sécurité possède le plus haut degré d'intégrité et le niveau 1 possède le plus bas

Note 1 à l'article: Les objectifs chiffrés de défaillance (voir l'IEC 61508 4:2010, 3.5.17) pour les quatre niveaux d'intégrité de sécurité sont indiqués dans les Tableaux 2 et 3 de l'IEC 61508 1:2010.

Note 2 à l'article: Les niveaux d'intégrité de sécurité sont utilisés pour spécifier les exigences concernant l'intégrité de sécurité des fonctions de sécurité à allouer aux systèmes E/E/PE relatifs à la sécurité.

Note 3 à l'article: Un niveau d'intégrité de sécurité (SIL) ne constitue pas une propriété d'un système, sous-système, élément ou composant. L'interprétation correcte de l'expression "système relatif à la sécurité à SIL n" (où n est 1, 2, 3 ou 4) signifie que le système est potentiellement capable de prendre en charge les fonctions de sécurité avec un niveau d'intégrité de sécurité jusqu'à n.

Note 4 à l'article: L'abréviation «SIL» est dérivée du terme anglais développé correspondant «safety integrity level».

[SOURCE: IEC 61508 4:2010, 3.5.8, modifié — ajout de la Note 4]

3.1.1.35
mesure de sécurité
mesure permettant de contrôler les *erreurs* de communication éventuelles, qui est conçue et mise en œuvre conformément aux exigences de l'IEC 61508

Note 1 à l'article: Dans la pratique, plusieurs mesures de sécurité sont combinées pour atteindre le niveau d'intégrité de sécurité exigé.

Note 2 à l'article: Les *erreurs* de communication et les mesures de sécurité associées sont détaillées dans l'IEC 61784-3:—, 5.3 et 5.4.

3.1.1.36
PDU de sécurité
SPDU
PDU transféré via le canal de communication de sécurité

Note 1 à l'article: Le SPDU peut comporter plusieurs exemplaires des données de sécurité qui utilisent des structures de codage et des fonctions de hachage différentes, associées à des parties explicites de protections supplémentaires, par exemple une clé, un nombre de séquences ou un mécanisme d'horodatage.

Note 2 à l'article: Les SCL redondantes peuvent fournir deux versions différentes du SPDU en vue de son insertion dans des champs séparés de la trame de bus de terrain.

Note 3 à l'article: L'abréviation «SPDU» est dérivée du terme anglais développé correspondant «safety protocol data unit».

3.1.1.37
application relative à la sécurité
programmes conçus conformément à l'IEC 61508 pour satisfaire aux exigences SIL de l'application

3.1.1.38
système relatif à la sécurité
système qui exécute les *fonctions de sécurité* conformément à l'IEC 61508

3.1.1.39
déclenchement parasite
déclenchement provoqué par le système de sécurité sans injonction du processus

3.1.1.40
horodatage
information temporelle incluse dans un *message*

3.1.2 CPF 17: Termes et définitions supplémentaires

3.1.2.1
cadence
temporisateur de l'émetteur ou du récepteur permettant de surveiller si le partenaire de communication est actif

3.1.2.2
initiateur
rôle d'un appareil FSCP 17/1 chargé d'établir une connexion

3.1.2.3
répondeur
rôle d'un appareil FSCP 17/1 qui suit l'établissement de la connexion par un initiateur

3.1.2.4
récepteur
entité de communication passive capable de recevoir des messages et de les envoyer en réponse à une autre entité de communication qui peut être un émetteur ou un récepteur

3.1.2.5
émetteur
entité de communication active qui est capable d'initier et de programmer les activités de communication effectuées par d'autres postes, qui peuvent être des émetteurs ou des récepteurs

3.1.2.6
SUID
valeur de 64 bits du numéro d'identification de connexion logique de FSCP 17/1, qui est une combinaison des UID de deux appareils

3.1.2.7
UID
numéro d'identification de CPF 17, qui est une combinaison de l'adresse MAC de 48 bits et de l'adresse de l'appareil de 16 bits

3.1.2.8
numéro de séquence virtuel
valeur interne à chaque appareil FSCP 17/1 permettant de vérifier la séquence de message, mais qui n'est pas transmise dans la trame du message

3.2 Symboles et abréviations

3.2.1 Symboles et abréviations communs

CP	Communication Profile (Profil de communication)	[IEC 61784-2:2010]
CPF	Communication Profile Family (Famille de profils de communication)	[IEC 61784-2:2010]
CRC	Cyclic Redundancy Check (Contrôle de redondance cyclique)	
DLL	Data Link Layer (Couche de liaison de données)	[ISO/IEC 7498-1]
DLPDU	Data Link Protocol Data Unit (Unité de données de protocole de liaison de données)	
EMC	Electromagnetic Compatibility (Compatibilité électromagnétique)	
EMI	Electromagnetic Interference (Brouillage électromagnétique)	
EUC	Equipment Under Control (Équipement commandé)	[IEC 61508-4:2010]
E/E/PE	Electrical/Electronic/Programmable Electronic (Électrique/électronique/électronique programmable)	[IEC 61508-4:2010]
FAL	Fieldbus Application Layer (Couche application de bus de terrain)	[IEC 61158-5-21:2010]
FCS	Frame Check Sequence (Séquence de contrôle de trame)	
FS	Functional Safety (Sécurité fonctionnelle)	
FSCP	Functional Safety Communication Profile (Profil de communication de sécurité fonctionnelle)	
HD	Hamming Distance (Distance de Hamming)	
MTBF	Mean Time Between Failures (Durée moyenne de bon fonctionnement)	
MTTF	Mean Time To Failure (Durée moyenne de fonctionnement avant défaillance)	
PDU	Protocol Data Unit (Unité de données de protocole)	[ISO/IEC 7498-1]
PELV	Protective Extra Low Voltage (Très basse tension de protection)	
PFD	Probability of dangerous Failure on Demand (Probabilité de défaillance dangereuse sur sollicitation)	[IEC 61508-4:2010]
PFH	Average Frequency of Dangerous Failure [h^{-1}] (Fréquence moyenne de défaillance dangereuse [h^{-1}])	[IEC 61508-4:2010]
PhL	Physical Layer (Couche physique)	[ISO/IEC 7498-1]
PL	Performance Level (Niveau de performance)	[ISO 13849-1]
PLC	Programmable Logic Controller (Automate programmable)	
SCL	Safety Communication Layer (Couche de communication de sécurité)	
SFRT	Safety Function Response Time (Temps de réponse de la fonction de sécurité)	
SIL	Safety Integrity Level (Niveau d'intégrité de sécurité)	[IEC 61508-4:2010]

3.2.2 CPF 17: Symboles et abréviations supplémentaires

Pour les besoins du présent document, les abréviations et acronymes donnés dans l'IEC 61784-3 ainsi que les suivants, s'appliquent.

ASE	Application Service Element (Élément de service d'application)
DLE	Data Link Layer Entity (Couche de liaison de données)
FC	Frame Control (Contrôle de trame)
FSPDU	Functional Safety PDU (PDU de sécurité fonctionnelle)
MAC	Media Access Control (Contrôle d'accès au support)
MIB	Management Information Base (Base d'informations de gestion)
PHY	Physical interface controller (Émetteur-récepteur d'interface physique)
SUID	Safety Unique Identification (Identification unique de sécurité)

3.3 Conventions

Les conventions utilisées dans le présent document sont définies dans le Type 21 de l'IEC 61158 et CPF 17 de l'IEC 61784-2.

4 Présentation générale de FSCP 17/1 (RAPIEnet Safety™)

La Famille de profils de communication 17 (communément appelée RAPIEnet™[5]) définit les profils de communication reposant sur l'IEC 61158-3-21:2010, l'IEC 61158-4-21:2010, l'IEC 61158-5-21:2010 et l'IEC 61158-6-21:2010.

Le profil de base CP 17/1 est défini dans l'IEC 61784-2. Le profil de communication de sécurité fonctionnelle CPF 17 FSCP 17/1 (RAPIEnet Safety™) repose sur les profils de base CPF 17 de l'IEC 61784-2 et les spécifications de couche de communication de sécurité définis dans la présente partie.

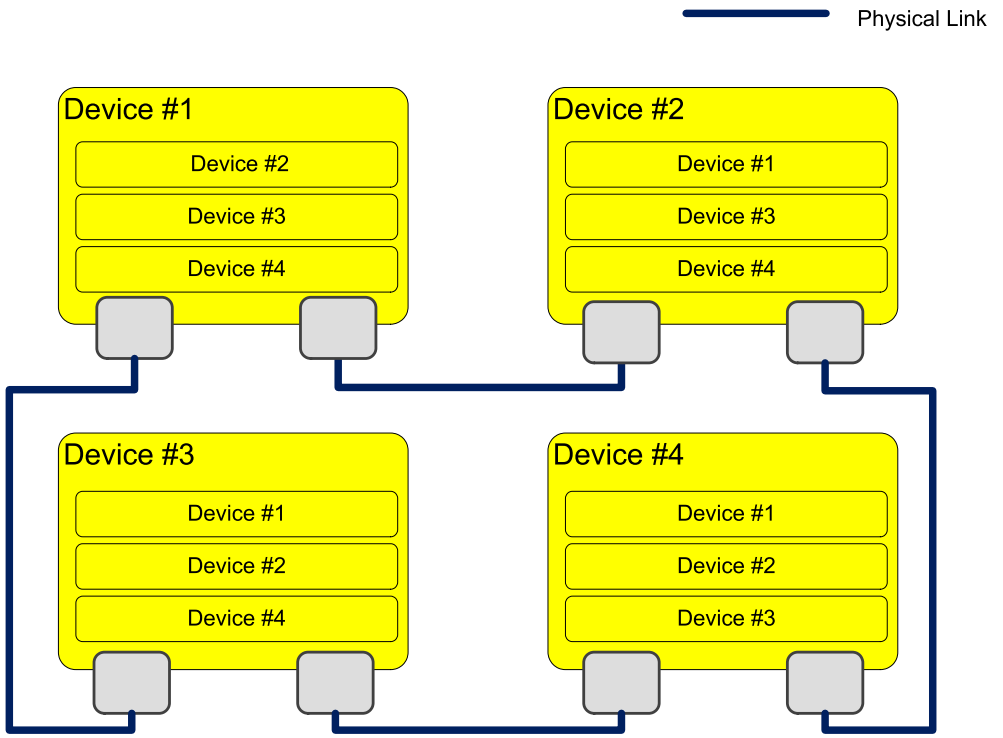
FSCP 17/1 repose sur un modèle de communication entre homologues s'appuyant sur une relation de communication "un-un" (voir la Figure 3). Un contrôleur peut utiliser une combinaison d'appareils standards et de sécurité reliés au réseau. Il est également possible d'affecter des tâches de sécurité et des tâches normales à différents contrôleurs.

Les quatre mesures suivantes ont été retenues pour réaliser le protocole FSCP 17/1:

- numérotation de séquence (virtuelle);
- contrôle du temps de fonctionnement du chien de garde;
- SUID par relation de communication;
- contrôle de redondance cyclique pour l'intégrité des données.

---

5 RAPIEnet™ et RAPIEnet Safety™ sont des appellations commerciales de l'organisme sans but lucratif RAPIEnet Association. Cette information est donnée à l'intention des utilisateurs de la présente Norme internationale et ne signifie nullement que l'IEC 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 logos déposés pour RAPIEnet™ et RAPIEnet Safety™. L'utilisation des logos déposés pour RAPIEnet™ nécessite l'autorisation de RAPIEnet Association et la conformité aux conditions d'utilisation (essais et validation).



Anglais	Français
Physical Link	Liaison physique
Device #1	Appareil n° 1
Device #2	Appareil n° 2
Device #3	Appareil n° 3
Device #4	Appareil n° 4

Figure 3 – Relations de communication entre les appareils FSCP 17

Le numéro de séquence virtuel est un type de compteur pour chaque appareil homologue permettant de déterminer si la trame de réception est dans le bon ordre. Il est ajouté automatiquement pour l'initiateur, et la valeur du numéro de séquence est reflétée dans le champ CRC. Un appareil de réception utilise un CRC pour déterminer si le numéro de séquence est correct. Il est dit "virtuel", car il ne peut pas être vu au sein du PDU de sécurité.

Le temporisateur de chien de garde permet d'éviter les délais imprévus et de détecter l'état du réseau. Si un appareil de réception ne peut pas recevoir la réponse attendue de la part de son partenaire dans une période spécifiée, il passe à l'état FAIL-SAFE.

Le SUID est une valeur clé de chaque relation de communication de sécurité fonctionnelle. Il est composé de l'adresse MAC et de son numéro d'ID (l'adresse de l'appareil ou les valeurs prédéfinies par l'utilisateur des partenaires de communication, par exemple). La valeur du SUID est unique dans un réseau FSCP 17/1.

Le CRC est utilisé pour assurer l'intégrité de la trame de message. CRC32 est utilisé dans FSCP 17/1 pour détecter les erreurs sur les bits et couvrir la probabilité d'erreurs résiduelles sur les bits dans certaines limites.

5 Généralités

5.1 Documents externes de spécifications applicables au profil

Il n'existe aucun document externe de spécifications applicables au profil.

5.2 Exigences fonctionnelles de sécurité

Les exigences suivantes s'appliquent dans le cadre du développement de la technologie FSCP 17/1.

a) La communication de sécurité et la communication standard doivent être indépendantes. Toutefois, les appareils standards et les appareils de sécurité doivent être en mesure d'utiliser le même canal de communication.

b) La communication de sécurité doit être adaptée au niveau d'intégrité de sécurité SIL3 (voir l'IEC 61508).

c) Les durées de transmission doivent être surveillées.

d) Les mises en œuvre des protocoles FSCP 17/1 doivent être conformes à l'IEC 61508.

e) Les exigences de base qui s'appliquent au développement du protocole FSCP 17/1 sont définies dans l'IEC 61784-3.

f) Le matériel de transmission (les contrôleurs, ASIC, liaisons, coupleurs, etc.) ne doit pas être modifié (canal noir). Les fonctions de sécurité doivent être au-dessus de la FAL (c'est-à-dire pas de modification ni d'amélioration du protocole standard).

g) Les conditions environnementales doivent satisfaire aux exigences d'automatisation générales, essentiellement l'IEC 61326-3-1 et l'IEC 61326-3-2, en l'absence de normes de produits particulières.

h) Le contrôleur de l'émetteur de sécurité fonctionnelle et son appareil de terrain de sécurité fonctionnelle doivent toujours entretenir des relations de communication 1:1.

5.3 Mesures de sécurité

5.3.1 Généralités

Les mesures de sécurité mentionnées au Tableau 1 pour la gestion des erreurs de transmission éventuelles sont une composante essentielle du profil FSCP 17/1. Le choix des mesures de sécurité génériques du Tableau 1 dans l'IEC 61784-3:—, 5.5 est exigé pour FSCP 17/1.

Les mesures de sécurité doivent être traitées et surveillées dans une seule unité de sécurité.

Tableau 1 – Mesures déployées pour maîtriser les erreurs

Erreur de communication	Mesures de sécurité				
	Numéro de séquence (virtuel) [a]	Délai avec le chien de garde	Authentification de connexion	Message de rétroaction	Assurance d'intégrité des données
Corruption					X
Répétition non prévue	X				
Séquence incorrecte	X				
Perte	X	X		X	
Retard inacceptable		X			
Insertion	X		X		
Déguisement			X	X	X
Adressage			X		
[a] Instance du "numéro de séquence" de l'IEC 61784-3.					

5.3.2 Numéro de séquence (virtuel)

Le numéro de séquence d'une largeur de 16 bits permet de confirmer la séquence de trame. Le numéro de séquence n'est pas présenté dans une trame, mais il est utilisé pour générer des FSPDU. À chaque opération d'envoi ou de réception, chaque appareil augmente le numéro de séquence de la connexion dédiée. Le numéro de séquence est reflété dans les codes CRC. Si la validité du numéro de séquence n'est pas confirmée, la connexion doit passer à l'état de sécurité.

5.3.3 Délai avec le chien de garde

Le temporisateur de chien de garde fournit le délai des connexions logiques. Le temporisateur de chien de garde est lié au temps de réponse de sécurité, qui est le temps qui s'écoule entre la détection d'un événement à l'entrée de sécurité et la réponse apportée par le(s) canal(aux) de sortie correspondant(s) de la sortie de sécurité. Pour plus de détails, voir également 9.3.

La valeur du temporisateur de chien de garde est définie par l'utilisateur. Il s'agit d'un paramètre utilisateur à l'état INITIALIZE.

5.3.4 Authentification de connexion

L'authentification de connexion permet de vérifier qu'un FSPDU provient de son partenaire de communication spécifique. Le SUID est utilisé pour l'authentification de connexion. Le SUID est une combinaison des UID des partenaires de communication, la valeur pour les deux appareils étant unique dans le réseau. Par conséquent, le SUID distingue une connexion logique d'autres connexions logiques ou non sûres dans un réseau.

5.3.5 Message de réaction

Le message de réaction est fourni par acquittement. Le message de réaction contient un état d'erreur et des commandes sur un champ du message. Il contient également un numéro de séquence et des informations d'authentification dans les champs de code du CRC.

5.3.6 Assurance d'intégrité des données

L'assurance d'intégrité des données est obtenue en utilisant un CRC de 32 bits pour chaque champ de 4 octets d'un message. Chaque champ de code CRC couvre uniquement un champ de 4 octets dédié. Le polynôme correspondant au code CRC est différent de la séquence de contrôle de trame Ethernet générale.

5.4 Structure de la couche de communication de sécurité

5.4.1 Principe des communications de sécurité FSCP 17/1

Avec FSCP 17/1, les applications de sécurité et les applications standard partagent simultanément les mêmes systèmes de communication CPF 17 standard. La fonction de transmission sécurisée comprend toutes les mesures de détection déterministe de toutes les anomalies/tous les dangers potentiels que le système de transmission standard est susceptible d'introduire, ou le maintien sous une certaine limite de la probabilité d'erreur (anomalie) résiduelle. Ceci comprend:

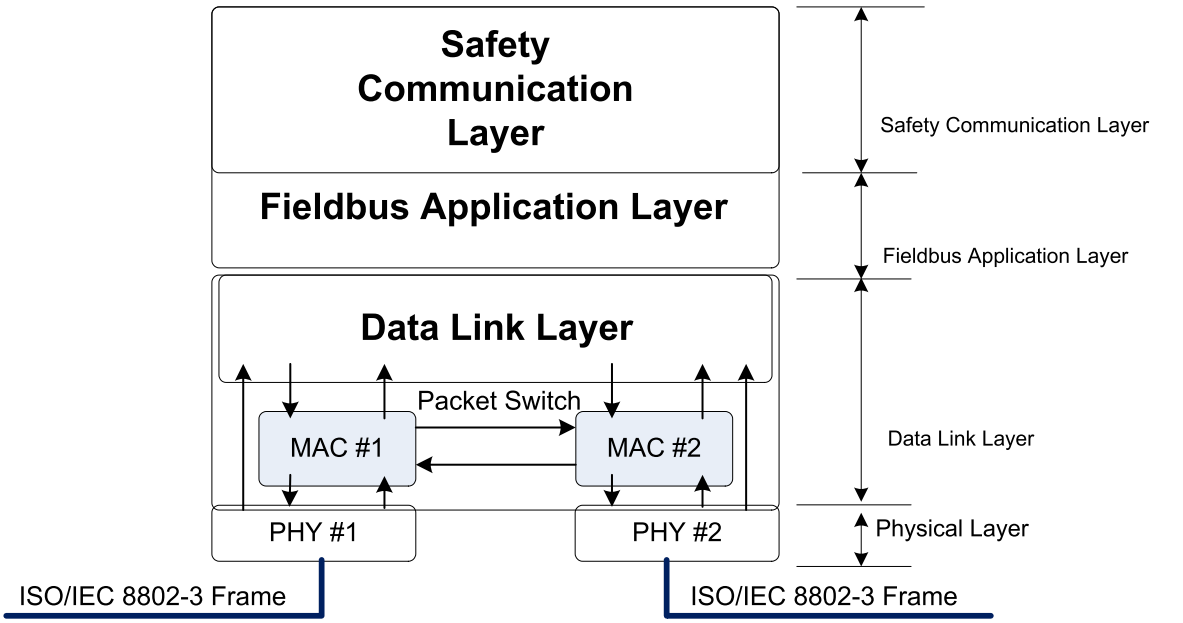
- les dysfonctionnements aléatoires dus, par exemple, à l'impact des interférences électromagnétiques sur le canal de transmission
- les défaillances/anomalies du matériel standard
- les dysfonctionnements systématiques des composants des matériels et logiciels standards.

Ce principe établit les limites de l'effort d'évaluation aux "fonctions de transmission sécurisée". Le "système de transmission standard"" (canal noir) n'exige pas d'évaluation de sécurité supplémentaire.

La transmission est assurée par l'intermédiaire de conducteurs électriques ou optiques. Les topologies et fonctions de transmission admises du système de transmission standard et les composants du "canal noir" sont décrits en 5.4.2.

5.4.2 Structures de communication CPF 17

La structure de communication de base est présentée à la Figure 4. La communication de sécurité de FSCP 17/1 est gérée dans la SCL, qui est au-dessus des couches de communication CP 17/1.



Anglais	Français
Safety Communication Layer	Couche de communication de sécurité
Fieldbus Application Layer	Couche d'application de bus de terrain
Data Link Layer	Couche de liaison de données
Physical Layer	Couche physique
Packet Switch	Commutation de paquets
ISO/IEC 8802-3 Frame	Trame ISO/IEC 8802-3

Figure 4 – Architecture de couche de sécurité

5.5 Relations avec la FAL (et DLL, PhL)

5.5.1 Généralités

Cette couche de communication de sécurité est destinée à être utilisée conjointement avec le profil de communication CPF 17. Toutefois, elle n'est pas limitée à ce profil de communication.

5.5.2 Types de données

Les types de données de sécurité sont spécifiés dans l'IEC 61158-5-21.

6 Services de la couche de communication de sécurité

6.1 Présentation générale

L'Article 6 définit une extension aux services de couche de communication existants de l'entité de couche d'application standard CP 17/1 pour FSCP 17/1.

6.2 Connexion de sécurité fonctionnelle

6.2.1 Généralités

La connexion entre deux partenaires de communication FSCP 17/1 (appareils FSCP 17/1) est appelée connexion de sécurité fonctionnelle. Dans un processus de connexion de sécurité fonctionnelle, un partenaire de communication est l'initiateur de sécurité fonctionnelle, l'autre

partenaire étant le répondeur de sécurité fonctionnelle par son adresse MAC et son ID d'appareil.

L'initiateur de sécurité fonctionnelle lance la connexion de sécurité fonctionnelle après la mise sous tension ou par suite d'un défaut de communication, alors que le répondeur de sécurité fonctionnelle n'apporte que des réponses. L'initiateur de sécurité fonctionnelle gère l'établissement de la communication de sécurité avec ses paramètres et, éventuellement, les paramètres de l'application relative à la sécurité du répondeur de sécurité fonctionnelle.

À l'issue du processus de connexion, les données du processus de sécurité peuvent être transférées depuis n'importe quel appareil FSCP 17/1.

6.2.2 Spécification de classe d'initiateur

6.2.2.1 Généralités

La classe Initiateur prend en charge la gestion des connexions à l'utilisateur SCL.

6.2.2.2 Modèle

ASE SCL:			SASE de connexion
CLASS:			Initiateur
CLASS ID:			non utilisé
PARENT CLASS:			non utilisé
ATTRIBUTES:			
1	(m)	Attribut:	Commande
2	(m)	Attribut:	SUID
3	(m)	Attribut:	Valeur de séquence
4	(m)	Attribut:	Code de service
5	(m)	Attribut:	Erreur/état
6	(m)	Attribut	Chien de garde

6.2.2.3 Attributs

Commande
Cet élément contient les informations d'état de l'initiateur. L'une des valeurs suivantes peut être attribuée à la commande:

- RESET;
- CONNECTION;
- PARAMETER;
- DATA;
- FAIL-SAFE.

SUID
Cet élément permet de vérifier la validité d'une connexion avec son partenaire de communication. Chaque connexion de FSCP 17/1 dispose d'une identification unique.

Valeur de séquence
Cet élément permet de vérifier l'ordre de transmission des messages. Cette valeur est indirectement contenue dans le message.

Code de service
Cet élément permet de déterminer l'état du message. Trois états sont définis:

- phase de connexion,
- phase de données,
- notification d'erreur.

Erreur/état
Cet élément représente l'état du poste en fonction de l'envoi ou de la réception des trames de message.

Chien de garde
Cet élément permet de vérifier l'anomalie du chemin de transmission ou du partenaire de communication.

6.2.3 Spécification de la classe du répondeur

6.2.3.1 Généralités

La classe du répondeur prend en charge les réponses de l'utilisateur SCL à l'initiateur ou vérifie la validité de la trame de réception provenant de l'initiateur.

6.2.3.2 Modèle

ASE SCL:			SASE de connexion
CLASS:			Répondeur
CLASS ID:			non utilisé
PARENT CLASS:			non utilisé
ATTRIBUTES:			
1	(m)	Attribut:	Commande
2	(m)	Attribut:	SUID
3	(m)	Attribut:	Valeur de séquence
4	(m)	Attribut:	Code de service
5	(m)	Attribut:	Erreur/état
6	(m)	Attribut	Chien de garde

6.2.3.3 Attributs

Commande
Voir 6.2.2.3.

SUID
Voir 6.2.2.3.

Valeur de séquence
Voir 6.2.2.3.

Code de service
Voir 6.2.2.3.

Erreur/état
Voir 6.2.2.3.

Chien de garde
Voir 6.2.2.3.

6.2.4 Spécification de classe d'émetteur

6.2.4.1 Généralités

La classe Émetteur prend en charge la gestion des connexions à l'utilisateur SCL.

6.2.4.2 Service de demande de lecture

6.2.4.2.1 Modèle

ASE SCL			SASE DE DONNÉES
CLASS			Demande de lecture de l'émetteur
CLASS ID			non utilisé
PARENT CLASS			non utilisé
ATTRIBUTES:			
1	(m)	Attribut:	Commande
2	(m)	Attribut:	SUID
3	(m)	Attribut:	Valeur de séquence
4	(m)	Attribut:	Code de service
5	(m)	Attribut:	Erreur/état
6	(m)	Attribut	Chien de garde
7	(m)	Attribut	Données
7.1	(m)	Attribut	Adresse
7.2	(m)	Attribut	Longueur

6.2.4.2.2 Attributs

Commande
Voir 6.2.2.3.

SUID
Voir 6.2.2.3.

Valeur de séquence
Voir 6.2.2.3.

Code de service
Voir 6.2.2.3.

Erreur/état
Voir 6.2.2.3.

Chien de garde
Voir 6.2.2.3.

Adresse
Cet élément permet de déterminer si l'émetteur a besoin d'accéder au récepteur.

Longueur
Cet élément permet d'adresser la longueur de données à lire à partir du récepteur.

6.2.4.3 Service de demande d'écriture

6.2.4.3.1 Modèle

ASE SCL			SASE DE DONNÉES
CLASS			Demande d'écriture de l'émetteur
CLASS ID			non utilisé
PARENT CLASS			non utilisé
ATTRIBUTES:			
1	(m)	Attribut:	Commande
2	(m)	Attribut:	SUID
3	(m)	Attribut:	Valeur de séquence
4	(m)	Attribut:	Code de service
5	(m)	Attribut:	Erreur/état
6	(m)	Attribut	Chien de garde
7	(m)	Attribut	Données
7.1	(m)	Attribut	Adresse
7.2	(m)	Attribut	Longueur
7.3	(m)	Attribut	SafeData[0]
7.4	(m)	Attribut	SafeData[1]
…	…	…	…
7.n	(m)	Attribut	SafeData[n-3]

6.2.4.3.2 Attributs

Commande
Voir 6.2.2.3.

SUID
Voir 6.2.2.3.

Valeur de séquence
Voir 6.2.2.3.

Code de service
Voir 6.2.2.3.

Erreur/état
Voir 6.2.2.3.

Chien de garde
Voir 6.2.2.3.

Adresse
Voir 6.2.4.2.2.

Longueur
Voir 6.2.4.2.2.

Données
Cet élément représente les données de sécurité réelles que l'émetteur tente d'écrire au récepteur.

6.2.5 Spécification de classe de récepteur

6.2.5.1 Généralités

La classe du récepteur prend en charge les réponses de l'utilisateur SCL à l'initiateur ou vérifie la validité de la trame de réception provenant de l'initiateur.

6.2.5.2 Service de réponse de lecture

6.2.5.2.1 Modèle

ASE SCL			SASE DE DONNÉES
CLASS			Réponse de lecture du récepteur
CLASS ID			non utilisé
PARENT CLASS			non utilisé
ATTRIBUTES:			
1	(m)	Attribut:	Commande
2	(m)	Attribut:	SUID
3	(m)	Attribut:	Valeur de séquence
4	(m)	Attribut:	Code de service
5	(m)	Attribut:	Erreur/état
6	(m)	Attribut	Chien de garde
7	(m)	Attribut	Données
7.1	(m)	Attribut	SafeData[0]
7.2	(m)	Attribut	SafeData[1]
…	…	…	…
7.n	(m)	Attribut	SafeData[n-1]

6.2.5.2.2 Attributs

Commande
Voir 6.2.2.3.

SUID
Voir 6.2.2.3.

Valeur de séquence
Voir 6.2.2.3.

Code de service
Voir 6.2.2.3.

Erreur/état
Voir 6.2.2.3.

Chien de garde
Voir 6.2.2.3.

Adresse
Voir 6.2.4.2.2.

Longueur
Voir 6.2.4.2.2.

Données
Voir 6.2.4.3.2.

6.2.5.3 Service de réponse d'écriture

6.2.5.3.1 Modèle

ASE SCL			SASE DE DONNÉES
CLASS			Réponse d'écriture de l'émetteur
CLASS ID			non utilisé
PARENT CLASS			non utilisé
ATTRIBUTES:			
1	(m)	Attribut:	Commande
2	(m)	Attribut:	SUID
3	(m)	Attribut:	Valeur de séquence
4	(m)	Attribut:	Code de service
5	(m)	Attribut:	Erreur/état
6	(m)	Attribut	Chien de garde
7	(m)	Attribut	Données
7.1	(m)	Attribut	Acquittement

6.2.5.3.2 Attributs

Commande
Voir 6.2.2.3.

SUID
Voir 6.2.2.3.

Valeur de séquence
Voir 6.2.2.3.

Code de service
Voir 6.2.2.3.

Erreur/état
Voir 6.2.2.3.

Chien de garde
Voir 6.2.2.3.

Données
Voir 6.2.4.3.2.

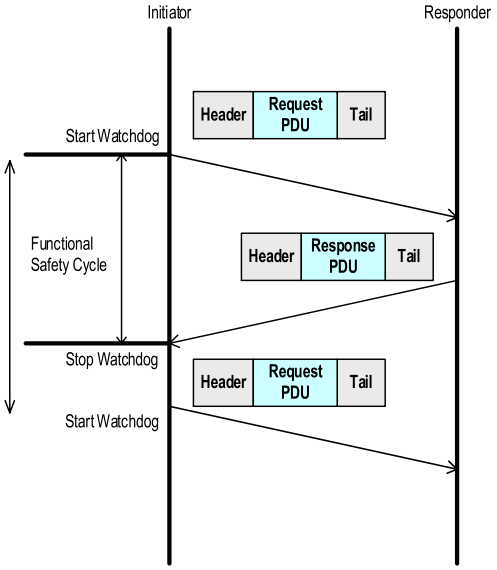
Acquittement
Cet élément permet de confirmer à l'émetteur que le service d'écriture a été réalisé.

6.3 Service de transmission de données de sécurité fonctionnelle

Un appareil FSCP 17/1 envoie un FSPDU au partenaire et lance le chien de garde de sécurité fonctionnelle.

Après avoir vérifié l'intégrité du FSPDU, le récepteur FSCP 17/1 transfère les données de sécurité à l'application de sécurité. Il calcule le FSPDU avec les paramètres de la trame et les paramètres provenant de l'application de sécurité, puis envoie un acquittement à l'émetteur.

Le récepteur démarre également son chien de garde de sécurité fonctionnelle (voir la Figure 5).

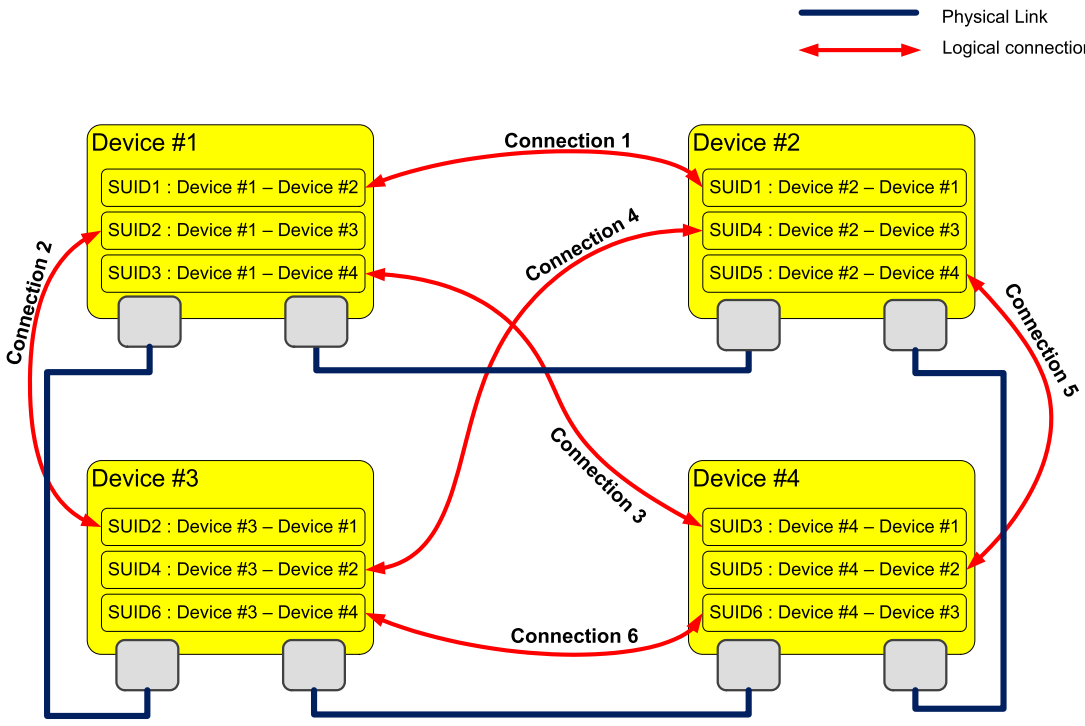


Anglais	Français
Initiator	Initiateur
Responder	Répondeur
Start Watchdog	Lancer le chien de garde
Functional Safety Cycle	Cycle de sécurité fonctionnelle
Header	En-tête
Request PDU	PDU de demande
Tail	Queue
Response PDU	PDU de réponse
Stop Watchdog	Arrêter le chien de garde

Figure 5 – Cycle de sécurité fonctionnelle

6.4 Relation de connexion de sécurité fonctionnelle

Pour chaque connexion de sécurité fonctionnelle, chaque appareil doit gérer les informations de ses partenaires relatives à chaque relation de connexion dans la SCL. La Figure 6 présente un exemple de relations entre différentes connexions.



Anglais	Français
Physical Link	Liaison physique
Logical connection	Connexion logique
Device #1	Appareil n° 1
Device #2	Appareil n° 2
Device #3	Appareil n° 3
Device #4	Appareil n° 4
Connection 1	Connexion 1
Connection 2	Connexion 2
Connection 3	Connexion 3
Connection 4	Connexion 4
Connection 5	Connexion 5
Connection 6	Connexion 6

Figure 6 – Relations de connexion parmi les appareils FSCP 17/1

7 Protocole de couche de communication de sécurité

7.1 Format PDU de sécurité

7.1.1 Généralités

Ethernet Header	Type 21	Type 21 PDU		Ethernet
Ethernet Header	Frame HDR	Type 21 Header	DATA	FCS

COMMAND	RESERVED	CRC32	ATHENTICATION KEY	CRC32	SAFE DATA(0)	CRC32(0)	SAFE DATA(1)	CRC32(1)	.....	SAFE DATA(n)	CRC32(n)
(2)	(2)	(4)	(4)	(4)	(4)	(4)	(4)	(4)		(4)	(4)

IEC

Anglais	Français
Ethernet Header	En-tête Ethernet
Frame HDR	Trame HDR
Type 21 Header	En-tête de type 21
Type 21	Type 21
Type 21 PDU	PDU de type 21
DATA	DONNÉES
COMMAND	COMMANDE
RESERVED	RESERVÉ
AUTHENTICATION KEY	CLÉ D'AUTHENTIFICATION
SAFE DATA	DONNÉES DE SÉCURITÉ

Figure 7 – PDU de sécurité fonctionnelle pour CPF 17 sur PDU de type 21

Le FSPDU est transféré par l'intermédiaire du réseau FSCP 17/1. Chaque appareil FSCP 17/1 reçoit un PDU de sécurité de la part du partenaire désigné. Le format de PDU de sécurité est représenté à la Figure 7.

Le FSPDU contient des informations permettant de valider la commande et le partenaire de communication.

Au cours du processus d'établissement d'une connexion, une valeur nulle peut être attribuée au champ de données de sécurité.

Tableau 2 – FSPDU général

Octet	Nom	Description
0	Commande	Commande, 2 octets
2	Réservé	Réservé, 2 octets
4	CRC32_H0	CRC32 pour l'en-tête, 4 octets
8	Clé d'authentification	SUID inférieur à 32 bits,4 octets
12	CRC32_H1	CRC32 de la clé d'authentification, 4 octets
16	SafeData[0]	Données de sécurité, 4 octets
20	CRC32_0	CRC32 pour SafeData[0], 4 octets
24	SafeData[1]	Données de sécurité, 4 octets
28	CRC32_1	CRC32 pour SafeData[1], 4 octets
…	…	…
n × 8 + 16	SafeData[n]	Données de sécurité, 4 octets
n × 8 + 20	CRC32_n	CRC32 pour SafeData[n], 4 octets

Le FSPDU peut transférer n blocs de données de sécurité, chacun étant composé de 4 octets. Chaque bloc de données contient un code CRC de 4 octets. Il est décrit au Tableau 2.

7.1.2 Commande FSPDU

La commande FSPDU détermine la signification des données de sécurité en fonction du schéma présenté au Tableau 3.

Tableau 3 – Commande FSPDU

Commande	Description
0x01	RESET
0x02	CONNECTION
0x03	PARAMETER
0x04	DATA
0x05	FAIL-SAFE

7.1.3 Clé d'authentification

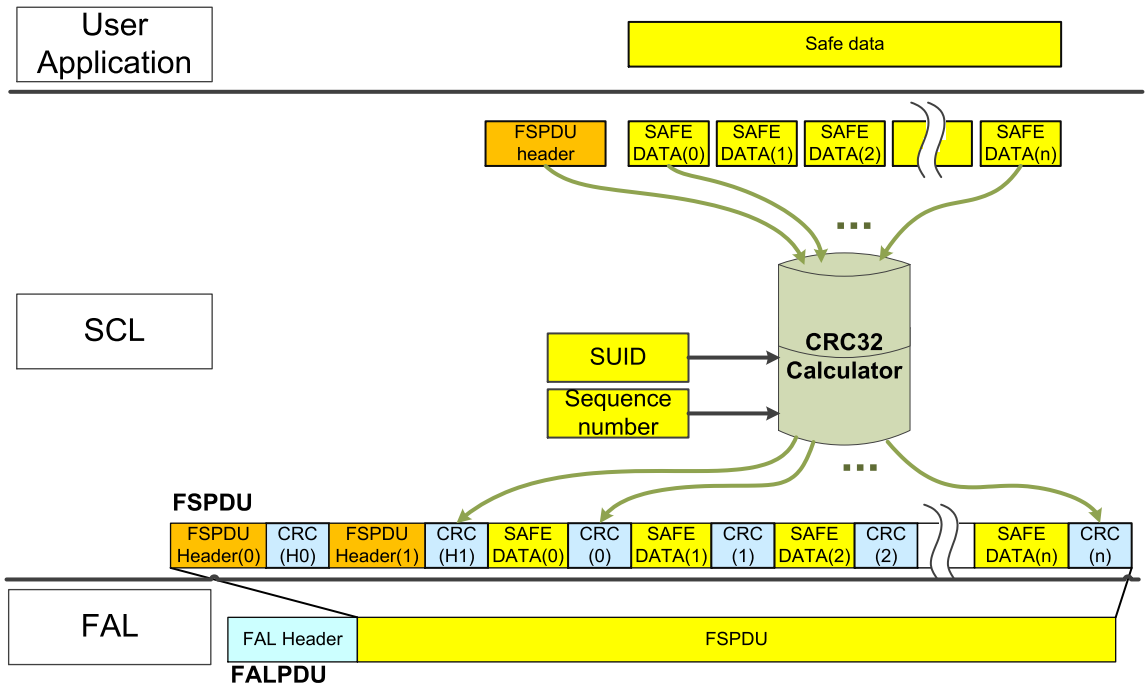
La clé d'authentification est mise en œuvre par le SUID de 64 bits. Le SUID est une combinaison des UID de deux appareils. Un FSPDU contient des champs de code CRC, chaque code CRC étant généré avec un SUID. Si un appareil reçoit une trame sans SUID valide, la trame doit être ignorée par comparaison CRC. Les 32 bits inférieurs du SUID sont présentés dans le champ de clé d'authentification.

7.1.4 FSPDU CRC

7.1.4.1 Calcul CRC

La distinction entre les messages pertinents de sécurité et les messages pertinents non relatifs à la sécurité est assurée en validant le caractère unique des messages de sécurité contenant des codes CRC correctement formatés, des champs de 4 octets, le SUID et le numéro de séquence virtuel. Chaque code CRC couvre les 4 octets désignés du champ d'en-tête ou de données de sécurité uniquement. La Figure 8 présente comment générer un code CRC pour les données de sécurité.

```
CRC_i:=      f(SUID, (virtual) Sequence_Number, command or 4 octets Data[i])
```



Anglais	Français
User Application	Application utilisateur
Safe data	Données de sécurité
FSPDU header	En-tête de FSPDU

Anglais	Français
Sequence number	Numéro de séquence
CRC32 Calculator	Calculateur CRC32
FAL Header	En-tête FAL

Figure 8 – Processus de génération du code FSPDU CRC

7.1.4.2 Sélection polynomiale CRC

Le polynôme G(x) = $\{x^{32}+x^{16}+x^{14}+x^{12}+x^{11}+x^{9}+x^{6}+x^{5}+x^{2}+x^{1}+1\}$ permet de calculer les CRC et est appelé polynôme de sécurité.

Pour pouvoir transporter le FSPDU par l'intermédiaire d'un canal noir, dont les caractéristiques de transfert ne sont pas incluses dans les considérations de sécurité, un taux d'erreur sur les bits de 10^{-2} doit être utilisé pour déterminer la probabilité d'erreurs résiduelles. La probabilité d'erreurs résiduelles ne doit pas dépasser 10^{-9}.

La sécurité est assurée lorsque l'émetteur de sécurité fonctionnelle et le répondeur de sécurité fonctionnelle passent à l'état de réinitialisation (c'est-à-dire à l'état de sécurité) dès qu'une erreur est détectée.

Tous les facteurs de calcul CRC comportent une valeur prévue fixe, de manière à ne prendre en compte que les données de sécurité dans le calcul de la probabilité d'erreurs résiduelles.

7.1.4.3 SUID

Le SUID est une valeur de 8 octets utilisée pour l'identification de chaque connexion. Il s'agit d'une combinaison de l'adresse MAC et de l'ID d'appareil de chaque participant à la connexion. Étant donné qu'il s'agit de valeurs uniques dans FSCP 17/1, le SUID est une valeur unique dans un réseau FSCP 17/1.

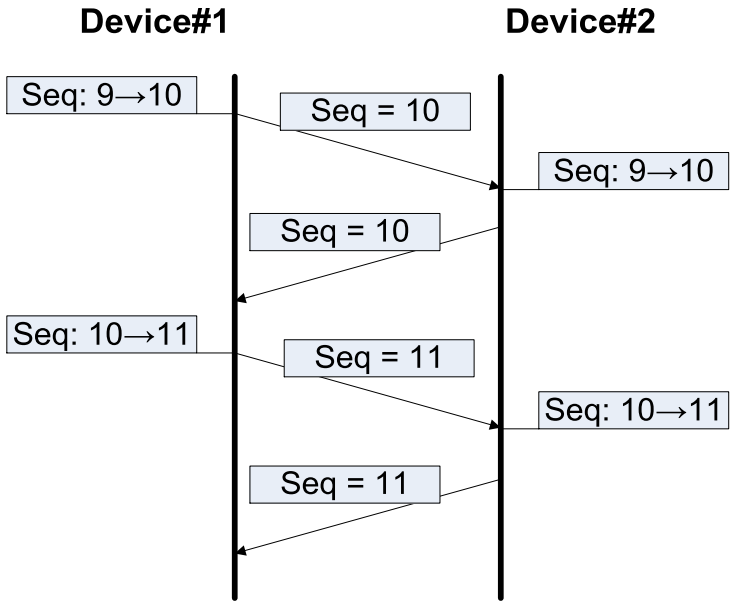
```
SUID = f(source MAC address and device ID, destination MAC address and device ID)
```

Le SUID est défini sur INITIALIZE et ne doit pas être modifié pendant l'opération de sécurité fonctionnelle.

7.1.4.4 Numéro de séquence

Le numéro de séquence permet de déterminer l'ordre correct de la séquence de trame transmise et de générer des codes CRC dédiés pour la trame. Le numéro de séquence d'une largeur de 16 bits appartient à la connexion logique. Le numéro de séquence n'apparaît pas dans une trame, mais il est géré dans la SCL.

Le numéro de séquence est augmenté à partir d'un appareil qui envoie un message de demande. Un appareil qui envoie un message de demande augmente le numéro de séquence interne et génère un FSPDU avec ce numéro de séquence augmenté. Un appareil de réception augmente le numéro de séquence lorsqu'il reçoit un message de demande provenant du partenaire de communication. Si l'appareil de réception reçoit un message de réponse de la part du partenaire de communication, il ne doit pas augmenter le numéro de séquence interne et examiner la trame reçue avec le numéro de séquence présent. Un exemple de modification de numéro de séquence est présenté à la Figure 9.



Anglais	Français
Device#1	Appareil n° 1
Device#2	Appareil n° 2

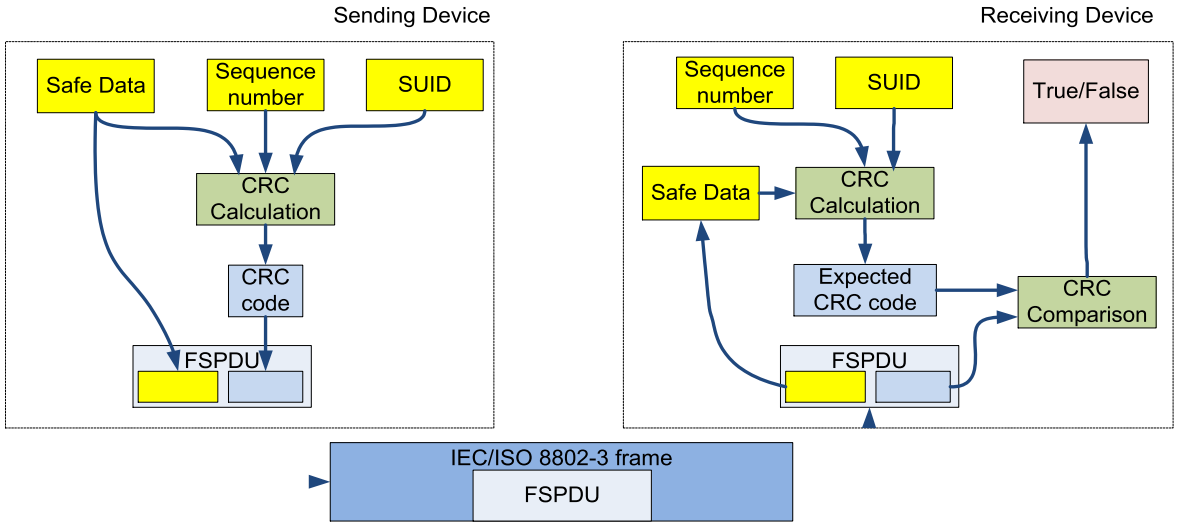
Figure 9 – Exemple de modification de numéro de séquence

7.1.4.5 Détection d'erreur de communication avec CRC

Dans FSCP 17/1, les erreurs de communication sont détectées par des codes CRC, à l'exception des erreurs de communication liées au temps, comme la perte ou le retard inacceptable. La détection d'erreur est obtenue par comparaison CRC sur l'appareil de réception.

Chaque code CRC d'un FSPDU est calculé avec un champ variable et des champs fixes. Le champ variable est celui des données de sécurité. Sa largeur est de 4 octets. Les champs fixes sont ceux du SUID et du numéro de séquence.

Un appareil émetteur calcule les codes CRC avec les champs de données de sécurité, le numéro de séquence et le SUID afin de générer un FSPDU. Le numéro de séquence n'apparaît pas dans le FSPDU, mais les deux appareils disposent d'un numéro de séquence synchronisé. Lorsqu'un appareil reçoit un message de demande, il doit calculer les codes CRC prévus avec le SUID, le numéro de séquence présent et le champ des données de sécurité du message. Ensuite, il procède à une comparaison avec chaque code CRC du message afin de vérifier la validité du message. Si la comparaison n'est pas satisfaisante, la trame reçue doit être ignorée. L'opération de détection d'erreur avec le code CRC est présentée à la Figure 10.



Anglais	Français
Safe Data	Données de sécurité
Sequence number	Numéro de séquence
Sending Device	Appareil émetteur
Receiving Device	Appareil récepteur
CRC Calculation	Calcul CRC
CRC code	Code CRC
Expected CRC code	Code CRC prévu
CRC Comparison	Comparaison CRC
IEC/ISO 8802-3 frame	Trame IEC/ISO 8802-3
True/False	Vrai/Faux

Figure 10 – Opération de comparaison CRC

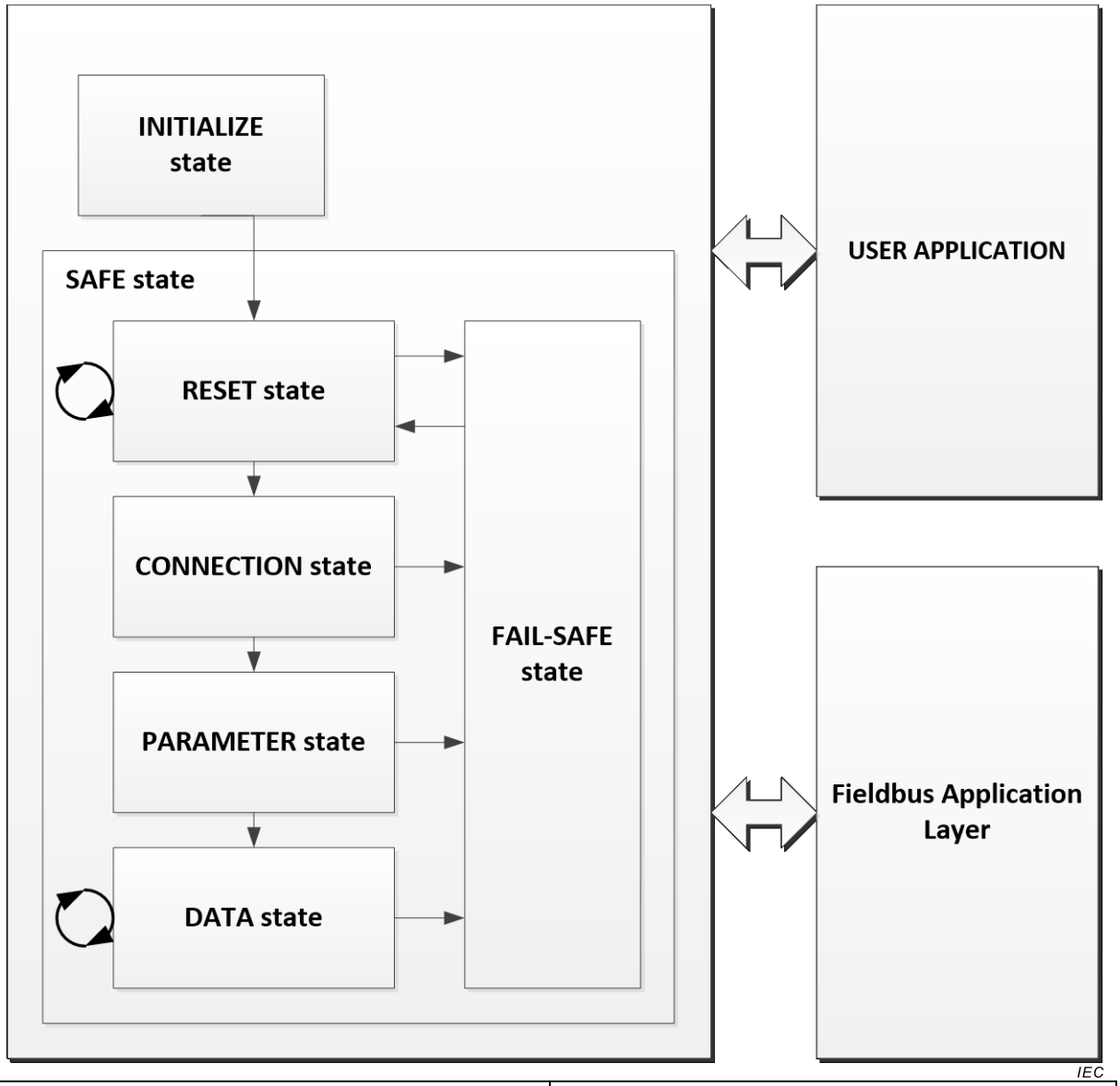
7.2 Procédure de communication FSCP 17/1

7.2.1 États de l'appareil FSCP 17/1

7.2.1.1 Généralités

Lors de l'établissement de la connexion de sécurité fonctionnelle, les appareils FSCP 17/1 passent par différents états avant que les données de sécurité ne soient valides et que le système ne quitte l'état de sécurité.

La Figure 11 présente les états de l'appareil de sécurité fonctionnelle.



Anglais	Français
INITIALIZE state	État INITIALIZE
SAFE state	État SAFE
RESET state	État RESET
CONNECTION state	État CONNECTION
PARAMETER state	État PARAMETER
DATA state	État DATA
FAIL-SAFE state	État FAIL-SAFE
USER APPLICATION	APPLICATION UTILISATEUR
Fieldbus Application Layer	Couche d'application de bus de terrain

Figure 11 – États de l'appareil FSCP 17/1

À la mise sous tension, l'ensemble des appareils de sécurité fonctionnelle sont à l'état INITIALIZE. Dans cet état, ils définissent leurs paramètres initiaux en fonction des valeurs définies par l'utilisateur respectives. Lorsque tous les paramètres sont définis, l'appareil de sécurité fonctionnelle bascule à l'état RESET. Avant de passer à l'état DATA, la sortie est maintenue à l'état hors tension. L'état DATA peut alors être considéré via les états CONNECTION et PARAMETER.

7.2.1.2 État INITIALIZE

À l'état INITIALIZE, les paramètres définis par l'utilisateur (ID de l'appareil, valeur du temporisateur de chien de garde et valeur du temporisateur de cadence, par exemple) sont établis pour les appareils.

Après l'état INITIALIZE, chaque appareil passe de l'état RESET à l'état de sécurité.

7.2.1.3 État RESET

L'état RESET permet de démarrer la connexion de sécurité fonctionnelle après l'état INITIALIZE. Lorsque le répondeur reçoit un message de demande de réinitialisation valide, il envoie le message de réponse de réinitialisation à l'initiateur. Si l'initiateur reçoit un message de réponse de réinitialisation valide, il passe à l'état CONNECTION. L'initiateur quitte l'état RESET lorsqu'il envoie un message de demande de connexion avec une commande CONNECTION au répondeur. Si le répondeur reçoit un message de demande de réinitialisation valide, il passe à l'état CONNECTION.

Si un champ CRC d'une trame reçue ne correspond pas à la valeur prévue, une erreur de communication est considérée s'être produite.

Si une erreur de communication est détectée, il convient de passer l'état de l'appareil à l'état FAIL-SAFE. Une exception à cette règle est l'expiration du temporisateur de chien de garde de l'initiateur lorsque ce dernier est à l'état RESET, auquel cas, il convient d'ignorer l'expiration et que l'initiateur continue à envoyer le message de demande de réinitialisation au répondeur tant qu'il n'a pas reçu de réponse valide.

Le Tableau 4 présente le format d'un FSPDU avec 4 octets de données de sécurité et la commande RESET.

Tableau 4 – FSPDU avec 4 octets de données de sécurité et la commande RESET après redémarrage (connexion de réinitialisation) ou après une erreur

Octet	Nom	Description
0	Commande	RESET
2	Réservé	Réservé, 2 octets
4	CRC32_H0	CRC32 pour l'en-tête, 4 octets
8	Clé d'authentification	SUID inférieur à 32 bits, 4 octets
12	CRC32_H1	CRC32 de la clé d'authentification, 4 octets
16	SafeData[0]	Zéro remplissage, 4 octets
20	CRC32_0	CRC32 pour SafeData[0], 4 octets

Le répondeur acquitte la commande de réinitialisation en attribuant la valeur 0 au message SafeData[0].

Le Tableau 5 présente le format du PDU de réponse de sécurité pour 4 octets de données de sécurité et la commande RESET.

Tableau 5 – FSPDU avec 4 octets de données de sécurité et la commande RESET pour acquitter une commande de réinitialisation à partir de l'initiateur

Octet	Nom	Description
0	Commande	RESET
2	Réservé	Réservé, 2 octets
4	CRC32_H0	CRC32 pour l'en-tête, 4 octets
8	Clé d'authentification	SUID inférieur à 32 bits, 4 octets
12	CRC32_H1	CRC32 de la clé d'authentification, 4 octets
16	SafeData[0]	Zéro remplissage, 4 octets,
20	CRC32_0	CRC32 pour SafeData[0], 4 octets

Le répondeur envoie également un FSPDU avec la commande de réinitialisation lors d'un redémarrage (connexion de réinitialisation) ou en cas d'erreur. Cela est présenté au Tableau 5, à l'aide d'un exemple de 4 octets de données de sécurité.

7.2.1.4 État CONNECTION

À l'état CONNECTION, l'initiateur et le répondeur se confirment l'un à l'autre leur condition de partenaire de communication respective. Lorsque l'initiateur passe de l'état RESET à l'état CONNECTION, il envoie un message de demande de connexion au répondeur. Lorsque le répondeur passe de l'état RESET à l'état CONNECTION, il envoie un message de réponse de connexion à l'initiateur.

Si l'initiateur reçoit un message de réponse de connexion valide, il passe à l'état PARAMETER. Si le répondeur reçoit un message de demande de paramètre valide, il passe à l'état PARAMETER.

Si un champ CRC d'une trame reçue ne correspond pas à la valeur prévue ou si le temporisateur de chien de garde expire, l'initiateur et le répondeur doivent envoyer un message de demande de sécurité intrinsèque à leurs partenaires de communication respectifs et passer à l'état FAIL-SAFE.

Les PDU de sécurité fonctionnelle à l'état CONNECTION sont présentés au Tableau 6 et au Tableau 7.

Tableau 6 – PDU de demande de connexion pour l'initiateur à l'état CONNECTION

Octet	Nom	Description
0	Commande	CONNECTION
2	Réservé	Réservé, 2 octets
4	CRC32_H0	CRC32 pour l'en-tête, 4 octets
8	Clé d'authentification	SUID inférieur à 32 bits, 4 octets
12	CRC32_H1	CRC32 de la clé d'authentification, 4 octets
16	SafeData[0]	4 octets supérieurs de l'UID
20	CRC32_0	CRC32 pour SafeData[0], 4 octets
24	SafeData[1]	4 octets inférieurs de l'UID
28	CRC32_1	CRC32 pour SafeData[1], 4 octets

Le répondeur acquitte la commande de connexion en renvoyant l'UID dans le champ de données.

Tableau 7 – PDU de réponse de connexion pour le répondeur à l'état CONNECTION

Octet	Nom	Description
0	Commande	CONNECTION
2	Réservé	Réservé, 2 octets
4	CRC32_H0	CRC32 pour l'en-tête, 4 octets
8	Clé d'authentification	SUID inférieur à 32 bits, 4 octets
12	CRC32_H1	CRC32 de la clé d'authentification, 4 octets
16	SafeData[0]	4 octets supérieurs de l'UID
20	CRC32_0	CRC32 pour SafeData[0], 4 octets
24	SafeData[1]	4 octets inférieurs de l'UID
28	CRC32_1	CRC32 pour SafeData[1], 4 octets

L'UID étant une combinaison de l'adresse de l'appareil et de l'adresse MAC, il peut être utilisé pour examiner la validité de l'adresse du partenaire de communication, de sorte que les adressages non valides doivent être détectés.

7.2.1.5 État SET_PARA

L'état SET_PARA concerne l'initiateur. Si l'initiateur passe de l'état CONNECTION à l'état SET_PARA, il envoie le message de demande de paramètre au répondeur avec 6 octets de paramètres d'application relatifs à la sécurité dans le champ de données. Si l'initiateur reçoit un message de réponse de paramètre valide, il passe à l'état DATA.

Le Tableau 8 présente le contenu des données de sécurité transférées à l'état SET_PARA.

Tableau 8 – Données de sécurité transférées à l'état SET_PARA

Données de sécurité octet	Description
0	Octet inférieur (bits 0_7) de la valeur du temporisateur de chien de garde de sécurité fonctionnelle (en ms)
1	Octet supérieur (bits 8_15) de la valeur du temporisateur de chien de garde de sécurité fonctionnelle (en ms)
2	Octet inférieur (bits 0_7) de la valeur du temporisateur de cadence local (en ms)
3	Octet supérieur (bits 8_15) de la valeur du temporisateur de cadence local (en ms)
4	Octet inférieur (bits 0_7) de la valeur du temporisateur de cadence distant (en ms)
5	Octet supérieur (bits 8_15) de la valeur du temporisateur de cadence distant (en ms)

Le paramètre de sécurité fonctionnelle est transféré sous la forme de 6 octets de paramètres relatifs à la sécurité dans le champ de données (voir du Tableau 9 au Tableau 10). Le premier FSPDU est envoyé par l'initiateur (voir le Tableau 9) et l'initiateur attend un message FSPDU, en tant qu'acquittement, conformément au Tableau 10. Lorsque l'initiateur reçoit un FSPDU de la part du répondeur sans erreur et contenant le même paramètre de sécurité fonctionnelle que celui qui a été envoyé, l'initiateur passe à l'état DATA. Toutefois, si le FSPDU reçu ne correspond pas à la valeur prévue, l'initiateur passe à l'état FAIL-SAFE et envoie un message de demande failsafe à son partenaire.

Tableau 9 – Envoi d'un FSPDU avec 6 octets de données de sécurité de la part de l'initiateur à l'état SET_PARA

Octet	Nom	Description
0	Commande	PARAMETER
2	Réservé	Réservé, 2 octets
4	CRC32_H0	CRC32 pour l'en-tête, 4 octets
8	Clé d'authentification	SUID inférieur à 32 bits, 4 octets
12	CRC32_H1	CRC32 de la clé d'authentification, 4 octets
16	SafeData[0]	Valeur de temporisateur de chien de garde de sécurité fonctionnelle de 2 octets (en ms), Valeur de temporisateur de cadence local de 2 octets(en ms),
20	CRC32_0	CRC32 pour SafeData[0], 4 octets
24	SafeData[1]	Valeur de temporisateur de cadence distant de 2 octets (en ms) Zéro remplissage de 2 octets
28	CRC32_1	CRC32 pour SafeData[1], 4 octets

Lorsque le répondeur reçoit un message avec des paramètres de sécurité fonctionnelle de la part de l'initiateur, il définit ses paramètres de sécurité fonctionnelle avec le paramètre du message et les renvoie à l'initiateur pour confirmer.

Le répondeur acquitte une commande PARAMETER correcte en renvoyant les données de sécurité.

Tableau 10 – FSPDU prévu avec 6 octets de données de sécurité provenant du répondeur à l'état SET_PARA

Octet	Nom	Description
0	Commande	PARAMETER
2	Réservé	Réservé, 2 octets
4	CRC32_H0	CRC32 pour l'en-tête, 4 octets
8	Clé d'authentification	SUID inférieur à 32 bits, 4 octets
12	CRC32_H1	CRC32 de la clé d'authentification, 4 octets
16	SafeData[0]	Répété Valeur de temporisateur de chien de garde de sécurité fonctionnelle de 2 octets (en ms), Valeur de temporisateur de cadence local de 2 octets(en ms),
20	CRC32_0	CRC32 pour SafeData[0], 4 octets
24	SafeData[1]	Valeur de temporisateur de cadence distant de 2 octets (en ms) Zéro remplissage de 2 octets
28	CRC32_1	CRC32 pour SafeData[1], 4 octets

Le paramètre de communication de sécurité fonctionnelle est configuré à l'aide du configurateur de sécurité de l'initiateur.

7.2.1.6 État WAIT_PARA

L'état WAIT_PARA concerne le répondeur. Lorsque le répondeur reçoit un message de demande de paramètre valide, il définit son paramètre avec les valeurs données dans le message reçu et envoie un message de réponse à l'initiateur, avec le paramètre défini dans le champ de données.

Le Tableau 11 présente le contenu des données de sécurité transférées à l'état WAIT_PARA.

Tableau 11 – Données de sécurité provenant de l'initiateur à l'état WAIT_PARA

Données de sécurité octet	Description
0	Octet inférieur (bits 0_7) du chien de garde de sécurité fonctionnelle (en ms)
1	Octet supérieur (bits 8_15) du chien de garde de sécurité fonctionnelle (en ms)
2	Octet inférieur (bits 0_7) de la valeur du temporisateur de cadence local (en ms)
3	Octet supérieur (bits 8_15) de la valeur du temporisateur de cadence local (en ms)
4	Octet inférieur (bits 0_7) de la valeur du temporisateur de cadence distant (en ms)
5	Octet supérieur (bits 8_15) de la valeur du temporisateur de cadence distant (en ms)

Le paramètre de sécurité fonctionnelle est transféré sous la forme de 6 octets de données de paramètre de sécurité dans le champ de données (voir le Tableau 12 et le Tableau 13). Lorsqu'un FSPDU est reçu de la part de l'initiateur (voir le Tableau 12), le répondeur compare les paramètres de sécurité fonctionnelle du FSPDU au paramètre de communication de sécurité fonctionnelle préconfiguré. Si le FSPDU reçu ne contient aucune erreur, le répondeur attribue la valeur reçue à son paramètre de communication de sécurité fonctionnelle et envoie un acquittement à l'initiateur. Le Tableau 13 présente le format FSPDU envoyé par le répondeur à l'initiateur avec le passage à l'état DATA. Si le FSPDU reçu contient une erreur, le répondeur doit passer à l'état FAIL-SAFE, puis envoie un message de demande de sécurité intrinsèque à son partenaire.

Tableau 12 – Envoi d'un FSPDU avec 6 octets de données de sécurité de la part de l'initiateur à l'état WAIT_PARA

Octet	Nom	Description
0	Commande	PARAMETER
2	Réservé	Réservé, 2 octets
4	CRC32_H0	CRC32 pour l'en-tête, 4 octets
8	Clé d'authentification	SUID inférieur à 32 bits, 4 octets
12	CRC32_H1	CRC32 de la clé d'authentification, 4 octets
16	SafeData[0]	Répété Valeur de temporisateur de chien de garde de sécurité fonctionnelle de 2 octets (en ms), Valeur de temporisateur de cadence local de 2 octets (en ms),
20	CRC32_0	CRC32 pour SafeData[0], 4 octets
24	SafeData[1]	Valeur de temporisateur de cadence distant de 2 octets (en ms) Zéro remplissage de 2 octets
28	CRC32_1	CRC32 pour SafeData[1], 4 octets

Le répondeur acquitte le résultat de configuration de paramètre en envoyant son paramètre dans le champ de données de sécurité.

Tableau 13 – Réception du FSPDU avec 6 octets de données de sécurité provenant du répondeur à l'état WAIT_PARA state

Octet	Nom	Description
0	Commande	PARAMETER
2	Réservé	Réservé, 2 octets
4	CRC32_H0	CRC32 pour l'en-tête, 4 octets
8	Clé d'authentification	SUID inférieur à 32 bits, 4 octets
12	CRC32_H1	CRC32 de la clé d'authentification, 4 octets
16	SafeData[0]	Répété Valeur de temporisateur de chien de garde de sécurité fonctionnelle de 2 octets (en ms), Valeur de temporisateur de cadence local de 2 octets (en ms),
20	CRC32_0	CRC32 pour SafeData[0], 4 octets
24	SafeData[1]	Valeur de temporisateur de cadence distant de 2 octets (en ms) Zéro remplissage de 2 octets
28	CRC32_1	CRC32 pour SafeData[1], 4 octets

7.2.1.7 État DATA

Si l'initiateur passe de l'état SET_PARA à l'état DATA, il envoie un message de demande de données au répondeur. Si le répondeur passe de l'état WAIT_PARA à l'état DATA, il envoie un message de réponse de données à l'initiateur.

Après l'établissement de la connexion de sécurité fonctionnelle, l'initiateur et le répondeur sont à l'état DATA tant qu'une erreur de communication ne s'est pas produite ou qu'un appareil de sécurité fonctionnelle ne s'est pas arrêté en local. À l'état DATA, les rôles de l'initiateur et du répondeur sont établis, et chaque appareil peut envoyer ou recevoir des données de sécurité en tant qu'émetteur ou que récepteur.

À l'état DATA, chaque appareil utilise un temporisateur de cadence pour surveiller l'état de la connexion entre les partenaires de communication. Tous les appareils du réseau FSCP 17/1 envoient un message de cadence par le temporisateur de cadence local. En l'absence de message valide de la part du partenaire ou de message de cadence jusqu'au temporisateur de cadence distant, l'appareil doit envoyer un message de demande de sécurité intrinsèque et passer à l'état FAIL-SAFE.

Le Tableau 14 présente le format du FSPDU général à l'état DATA.

Tableau 14 – FSPDU de données de sécurité à l'état DATA

Octet	Nom	Description
0	Commande	DATA
2	Réservé	Réservé, 2 octets
4	CRC32_H0	CRC32 pour l'en-tête, 4 octets
8	Clé d'authentification	SUID inférieur à 32 bits, 4 octets
12	CRC32_H1	CRC32 de la clé d'authentification, 4 octets
16	SafeData[0]	SafeData[0], 4 octets
20	CRC32_0	CRC32 pour SafeData[0], 4 octets
	SafeData[1]	SafeData[1], 4 octets
	CRC32_1	CRC32 pour SafeData[1], 4 octets
…		
16+8i	SafeData[i]	SafeData[i], 4 octets
16+(8i+4)	CRC32_1	CRC32 pour SafeData[i], 4 octets

Lorsque l'émetteur envoie les données de sécurité, le récepteur acquitte leur réception avec une répétition des données de sécurité reçues. Le Tableau 15 et le Tableau 16 présentent des exemples d'envoi et d'acquittement de 4 octets de données de sécurité entre un émetteur et un récepteur.

Tableau 15 – Exemple de 4 octets de données de sécurité provenant d'un émetteur

Octet	Nom	Description
0	Commande	DATA
2	Réservé	Réservé, 2 octets
4	CRC32_H0	CRC32 pour l'en-tête, 4 octets
8	Clé d'authentification	SUID inférieur à 32 bits, 4 octets
12	CRC32_H1	CRC32 de la clé d'authentification, 4 octets
16	SafeData[0]	Données de sécurité, 4 octets
20	CRC32_0	CRC32 pour SafeData[0], 4 octets

Tableau 16 – Exemple d'ACK PDU provenant du récepteur avec 4 octets de données de sécurité

Octet	Nom	Description
0	Commande	DATA
2	Réservé	Réservé, 2 octets
4	CRC32_H0	CRC32 pour l'en-tête, 4 octets
8	Clé d'authentification	SUID inférieur à 32 bits, 4 octets
12	CRC32_H1	CRC32 de la clé d'authentification, 4 octets
16	SafeData[0]	Données de sécurité reçues, 4 octets
20	CRC32_0	CRC32 pour SafeData[0], 4 octets

7.3 Réponse aux erreurs de communication

7.3.1 Généralités

Un appareil de sécurité fonctionnelle peut détecter les erreurs figurant au Tableau 17.

Tableau 17 – Erreurs de communication de sécurité fonctionnelle

Erreur	Description
Commande imprévue	La commande reçue n'est pas admise dans cet état
ID de connexion non valide	La connexion ne correspond pas au SUID transféré dans l'état de connexion
Erreur CRC	Au moins l'un des champs CRC reçus ne correspond pas au CRC calculé
Le chien de garde a expiré	Aucun FSPDU valide n'a été reçu dans le délai du chien de garde de sécurité fonctionnelle
Données de sécurité non valides	Les données de sécurité reçues d'un partenaire de communication ne correspondent pas aux valeurs prévues
Données de sécurité non valides	Les données de sécurité renvoyées par le récepteur à l'état DATA ne correspondent pas à celles envoyées par l'émetteur
Paramètre de communication non valide	Le contenu du paramètre de communication est inacceptable
La cadence a expiré	Aucun message de cadence valide n'a été reçu du partenaire de communication dans le temps de cadence distant

Si un appareil de sécurité fonctionnelle détecte une erreur de communication, un message de demande de sécurité intrinsèque est envoyé par l'appareil, avec le code d'erreur associé dans le champ de données pour les besoins du diagnostic. L'appareil qui a détecté l'erreur ou une anomalie bascule à l'état FAIL-SAFE et envoie un message de demande de sécurité intrinsèque. Lorsque le partenaire de communication reçoit le message de demande de sécurité intrinsèque, il passe à l'état FAIL-SAFE. Les codes d'erreur de communication de sécurité intrinsèque figurent au Tableau 18.

Tableau 18 – Codes d'erreur de communication de sécurité fonctionnelle

Code d'erreur	Description
1	Commande imprévue (INVALID_CMD)
2	ID de connexion non valide (INVALID_CONNID)
3	Erreur CRC (INVALID_CRC)
4	Le chien de garde a expiré (WD_EXPIRED)
5	Données de sécurité non valides (INVALID_DATA)
6	Paramètre de communication non valide (INVALID_PARA)
7	Le temporisateur de cadence a expiré (HB_EXPIRED)

7.4 Table d'état de la SCL de CPF 17

7.4.1 Généralités

Selon la procédure de communication, l'initiateur de sécurité fonctionnelle peut se trouver dans les états figurant au Tableau 19 et au Tableau 20.

Tableau 19 – États de l'initiateur de sécurité fonctionnelle

État	Description
INITIALIZE	Les paramètres de l'appareil et le paramètre relatif à la sécurité fonctionnelle sont définis par l'utilisateur
RESET	La connexion de sécurité fonctionnelle est réinitialisée (les sorties sont à l'état de sécurité)
CONNECTION	L'UID de chaque appareil est en cours de transfert (les sorties sont à l'état de sécurité)
SET_PARA	Les paramètres sont en cours de transfert (les sorties sont à l'état de sécurité)
DATA	Les données de sécurité sont en cours de transfert
FAIL-SAFE	Arrêt de la communication jusqu'au déclenchement par l'utilisateur (les sorties sont à l'état de sécurité)

Tableau 20 – États du répondeur de sécurité fonctionnelle

État	Description
INITIALIZE	Les paramètres de l'appareil et les paramètres relatifs à la sécurité fonctionnelle sont définis par l'utilisateur
RESET	La connexion de sécurité fonctionnelle est réinitialisée (les sorties sont à l'état de sécurité)
CONNECTION	L'UID de chaque appareil est en cours de confirmation (les sorties sont à l'état de sécurité)
WAIT_PARA	Les paramètres sont en cours de configuration (les sorties sont à l'état de sécurité)
DATA	Les données de sécurité sont en cours de transfert
FAIL-SAFE	Arrêt de la communication jusqu'au déclenchement par l'utilisateur (les sorties sont à l'état de sécurité)

Le diagramme d'états de l'appareil de sécurité fonctionnelle est présenté à la Figure 12.

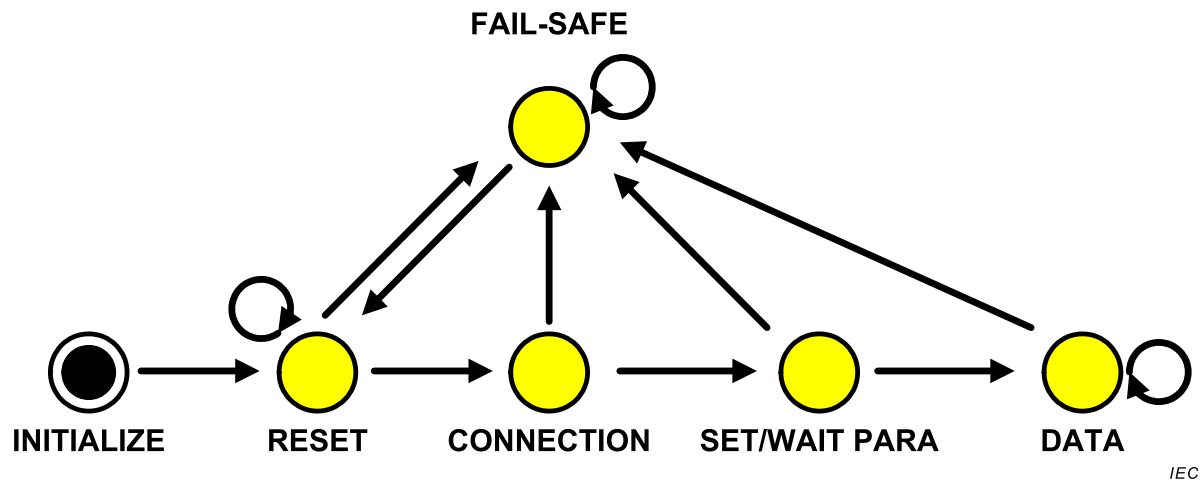


Figure 12 – Diagramme d'états de l'appareil de sécurité fonctionnelle

Les sections suivantes analysent les événements qui peuvent se produire dans l'appareil de sécurité fonctionnelle pour chaque état. Chaque événement est considéré sous conditions avec différentes actions ou des états subséquents.

7.4.2 Événements

Un événement peut inclure différents paramètres, qui sont présentés dans les tables d'états. Le Tableau 21 répertorie les événements possibles.

Tableau 21 – Événements de l'état de sécurité fonctionnelle

Événement	Description
Réception de trame	Un FSPDU a été reçu de la part d'un partenaire de communication
Trame envoyée	À l'état DATA, l'application de sécurité fonctionnelle est tenue d'envoyer un message à un partenaire
Initialisation terminée	Un appareil est prêt à lancer la communication de sécurité fonctionnelle avec les paramètres définis par l'utilisateur
Déclenchement par l'utilisateur	Entrée utilisateur permettant de sortir de l'état FAIL-SAFE
Expiration du chien de garde	Le chien de garde de sécurité fonctionnelle a expiré (c'est-à-dire qu'aucun FSDPU valide n'a été reçu dans le délai du chien de garde)
Expiration du temporisateur de cadence	Un temporisateur périodique de surveillance du partenaire de communication a expiré à l'état DATA

7.4.3 Table d'état de l'initiateur

7.4.3.1 Généralités

Le diagramme d'états de l'initiateur est présenté à la Figure 13.

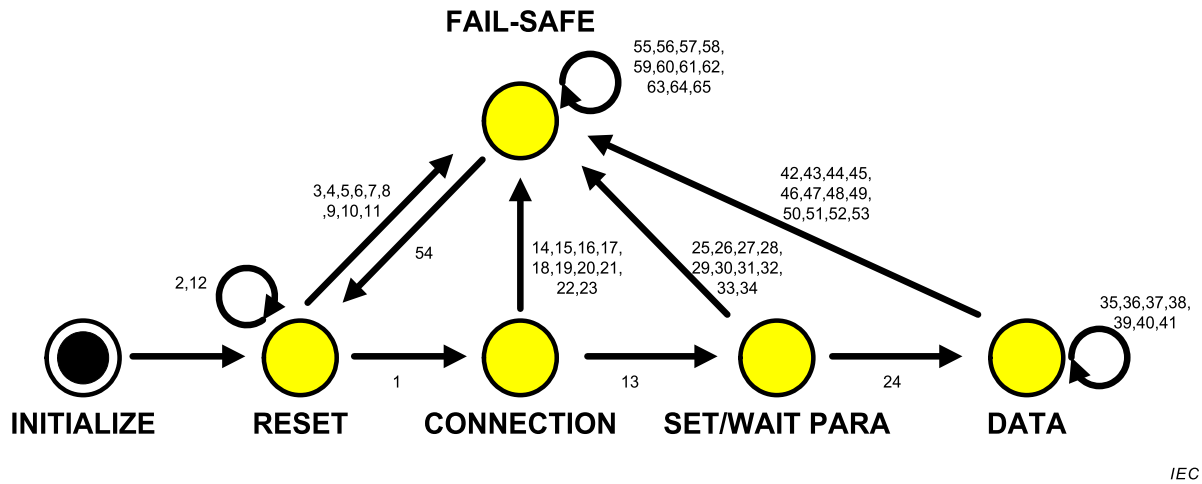


Figure 13 – Diagramme d'états de l'initiateur

7.4.3.2 État RESET

#	Courant	Événement /Condition =>actions	État suivant
1	RESET	RECEVOIR message de réponse de réinitialisation /CRC_Check() = TRUE => commande = 0x02(CONNECTION) chien de garde restart() & WD = 1 ENVOYER message de demande de connexion	CONNECTION
2	RESET	INITIALIZE terminé => commande = 0x01(RESET) chien de garde start() & WD = 1 ENVOYER message de demande de réinitialisation	RESET
3	RESET	RECEVOIR message de demande de sécurité intrinsèque =>	FAIL-SAFE
4	RESET	RECEVOIR message de demande de réinitialisation => INVALID_CMD commande = 0x05(FAIL-SAFE)	FAIL-SAFE

#	Courant	Événement /Condition =>actions	État suivant
		code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	
5	RESET	RECEVOIR message de réponse de réinitialisation /CRC_Check() = FALSE => INVALID_CRC commande = 0x05(FAIL-SAFE) code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	FAIL-SAFE
6	RESET	RECEVOIR message de demande de connexion => INVALID_CMD chien de garde stop() & WD = 0 commande = 0x05(FAIL-SAFE) code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	FAIL-SAFE
7	RESET	RECEVOIR message de réponse de connexion => INVALID_CMD commande = 0x05(FAIL-SAFE) code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	FAIL-SAFE
8	RESET	RECEVOIR message de demande de paramètre => INVALID_CMD commande = 0x05(FAIL-SAFE) code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	FAIL-SAFE
9	RESET	RECEVOIR message de réponse de paramètre => INVALID_CMD commande = 0x05(FAIL-SAFE) code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	FAIL-SAFE
10	RESET	RECEVOIR message de demande de données => INVALID_CMD commande = 0x05(FAIL-SAFE) code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	FAIL-SAFE
11	RESET	RECEVOIR message de réponse de données => INVALID_CMD commande = 0x05(FAIL-SAFE) code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	FAIL-SAFE
12	RESET	chien de garde expired() => WD_EXPIRED commande = 0x01(RESET) chien de garde start() & WD = 1 ENVOYER message de demande de réinitialisation	RESET

7.4.3.3 État CONNECTION

#	Courant	Événement /Condition =>actions	État suivant
13	CONNECTION	RECEVOIR message de réponse de connexion /CRC_Check() = TRUE => commande = 0x03(PARAMETER) chien de garde restart() & WD = 1	SET_PARA

#	Courant	Événement /Condition =>actions	État suivant
		ENVOYER message de demande de paramètre	
14	CONNECTION	RECEVOIR message de demande de sécurité intrinsèque =>	FAIL-SAFE
15	CONNECTION	RECEVOIR message de demande de réinitialisation => INVALID_CMD commande = 0x05(FAIL-SAFE) code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	FAIL-SAFE
16	CONNECTION	RECEVOIR message de réponse de réinitialisation => INVALID_CMD commande = 0x05(FAIL-SAFE) code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	FAIL-SAFE
17	CONNECTION	RECEVOIR message de demande de connexion => INVALID_CMD commande = 0x05(FAIL-SAFE) code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	FAIL-SAFE
18	CONNECTION	RECEVOIR message de réponse de connexion /CRC_Check() = FALSE => INVALID_CRC commande = 0x05(FAIL-SAFE) code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	FAIL-SAFE
19	CONNECTION	RECEVOIR message de demande de paramètre => INVALID_CMD commande = 0x05(FAIL-SAFE) code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	FAIL-SAFE
20	CONNECTION	RECEVOIR message de réponse de paramètre => INVALID_CMD commande = 0x05(FAIL-SAFE) code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	FAIL-SAFE
21	CONNECTION	RECEVOIR message de demande de données => INVALID_CMD commande = 0x05(FAIL-SAFE) code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	FAIL-SAFE
22	CONNECTION	RECEVOIR message de réponse de données => INVALID_CMD commande = 0x05(FAIL-SAFE) code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	FAIL-SAFE
23	CONNECTION	Chien de garde expired() => WD_EXPIRED commande = 0x05(FAIL-SAFE) code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	FAIL-SAFE

7.4.3.4 État SET PARAMETER

#	Courant	Événement /Condition =>actions	État suivant
24	SET_PARA	RECEVOIR message de réponse de paramètre /CRC_Check() = TRUE => commande = 0x04(DATA) code de service = phase de connexion chien de garde restart() & WD = 1 ENVOYER message de demande de données	DATA
25	SET_PARA	RECEVOIR message de demande de sécurité intrinsèque =>	FAIL-SAFE
26	SET_PARA	RECEVOIR message de demande de réinitialisation => INVALID_CMD commande = 0x05(FAIL-SAFE) code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	FAIL-SAFE
27	SET_PARA	RECEVOIR message de réponse de réinitialisation => INVALID_CMD commande = 0x05(FAIL-SAFE) code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	FAIL-SAFE
28	SET_PARA	RECEVOIR message de demande de connexion => INVALID_CMD commande = 0x05(FAIL-SAFE) code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	FAIL-SAFE
29	SET_PARA	RECEVOIR message de réponse de connexion => INVALID_CMD commande = 0x05(FAIL-SAFE) code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	FAIL-SAFE
30	SET_PARA	RECEVOIR message de demande de paramètre => INVALID_CMD commande = 0x05(FAIL-SAFE) code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	FAIL-SAFE
31	SET_PARA	RECEVOIR message de réponse de paramètre /CRC_Check = FALSE => INVALID_CRC commande = 0x05(FAIL-SAFE) code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	FAIL-SAFE
32	SET_PARA	RECEVOIR message de demande de données => INVALID_CMD commande = 0x05(FAIL-SAFE) code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	FAIL-SAFE
33	SET_PARA	RECEVOIR message de réponse de données => INVALID_CMD commande = 0x05(FAIL-SAFE) code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	FAIL-SAFE
34	SET_PARA	Chien de garde expired() => WD_EXPIRED commande = 0x05(FAIL-SAFE) code de service = notification d'erreur	FAIL-SAFE

#	Courant	Événement /Condition =>actions	État suivant
		ENVOYER message de demande de sécurité intrinsèque	

7.4.3.5 État DATA

#	Courant	Événement /Condition =>actions	État suivant
35	DATA	RECEVOIR message de réponse de données /CRC_Check() = TRUE /code de service = phase de connexion => chien de garde stop() & WD = 0 temporisateur de cadence local start() temporisateur de cadence distant start() ENVOYER message de cadence	DATA
36	DATA	L'application de sécurité fonctionnelle est tenue d'envoyer un message de demande au partenaire => commande = 0x04(DATA) code de service = phase de données chien de garde start() & WD = 1 ENVOYER message de demande de données	DATA
37	DATA	L'application de sécurité fonctionnelle est tenue d'envoyer un message de réponse au partenaire => commande = 0x04(DATA) code de service = phase de données ENVOYER message de réponse de données	DATA
38	DATA	RECEVOIR message de demande de données /CRC_Check() = TRUE /code de service = phase de données => Transfert des données reçues vers l'application de sécurité fonctionnelle	DATA
39	DATA	RECEVOIR message de réponse de données /CRC_Check() = TRUE /code de service = phase de données => chien de garde stop() & WD = 0 Transfert des données reçues vers l'application de sécurité fonctionnelle	DATA
40	DATA	RECEVOIR un message de cadence /CRC_Check() = TRUE => temporisateur de cadence distant restart()	DATA
41	DATA	expiration du temporisateur de cadence local => temporisateur de cadence local start() ENVOYER message de cadence	DATA
42	DATA	RECEVOIR message de demande de sécurité intrinsèque =>	FAIL-SAFE
43	DATA	RECEVOIR message de demande de réinitialisation => INVALID_CMD commande = 0x05(FAIL-SAFE) code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	FAIL-SAFE
44	DATA	RECEVOIR message de réponse de réinitialisation => INVALID_CMD commande = 0x05(FAIL-SAFE)	FAIL-SAFE

#	Courant	Événement /Condition =>actions	État suivant
		code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	
45	DATA	RECEVOIR message de demande de connexion => INVALID_CMD commande = 0x05(FAIL-SAFE) code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	FAIL-SAFE
46	DATA	RECEVOIR message de réponse de connexion => INVALID_CMD commande = 0x05(FAIL-SAFE) code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	FAIL-SAFE
47	DATA	RECEVOIR message de demande de paramètre => INVALID_CMD commande = 0x05(FAIL-SAFE) code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	FAIL-SAFE
48	DATA	RECEVOIR message de réponse de paramètre => INVALID_CMD commande = 0x05(FAIL-SAFE) code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	FAIL-SAFE
49	DATA	RECEVOIR message de demande de données /code de service = phase de connexion => INVALID_CMD commande = 0x05(FAIL-SAFE) code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	FAIL-SAFE
50	DATA	RECEVOIR message de demande de données /code de service = phase de données /CRC_Check = FALSE => INVALID_CRC commande = 0x05(FAIL-SAFE) code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	FAIL-SAFE
51	DATA	RECEVOIR message de réponse de données /CRC_Check() = FALSE => INVALID_CRC commande = 0x05(FAIL-SAFE) code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	FAIL-SAFE
52	DATA	Chien de garde expired() => WD_EXPIRED commande = 0x05(FAIL-SAFE) code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	FAIL-SAFE
53	DATA	expiration du temporisateur de cadence distant => HB_EXPIRED commande = 0x05(FAIL-SAFE) code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	FAIL-SAFE

7.4.3.6 État FAIL-SAFE

#	Courant	Événement /Condition =>actions	État suivant
54	FAIL-SAFE	Déclenchement par l'utilisateur => commande = 0x02 (RESET) chien de garde start() & WD = 1 ENVOYER message de demande de réinitialisation	RESET
55	FAIL-SAFE	expiration du chien de garde =>	FAIL-SAFE
56	FAIL-SAFE	expiration du temporisateur de cadence local =>	FAIL-SAFE
57	FAIL-SAFE	expiration du temporisateur de cadence distant =>	FAIL-SAFE
58	FAIL-SAFE	RECEVOIR message de demande de réinitialisation => ignorer le message	FAIL-SAFE
59	FAIL-SAFE	RECEVOIR message de réponse de réinitialisation => ignorer le message	FAIL-SAFE
60	FAIL-SAFE	RECEVOIR message de demande de connexion => ignorer le message	FAIL-SAFE
61	FAIL-SAFE	RECEVOIR message de réponse de connexion => ignorer le message	FAIL-SAFE
62	FAIL-SAFE	RECEVOIR message de demande de paramètre => ignorer le message	FAIL-SAFE
63	FAIL-SAFE	RECEVOIR message de réponse de paramètre => ignorer le message	FAIL-SAFE
64	FAIL-SAFE	RECEVOIR message de demande de données => ignorer le message	FAIL-SAFE
65	FAIL-SAFE	RECEVOIR message de réponse de données => ignorer le message	FAIL-SAFE

7.4.4 Table d'état du répondeur

7.4.4.1 Généralités

Le diagramme d'états du répondeur est présenté à la Figure 14.

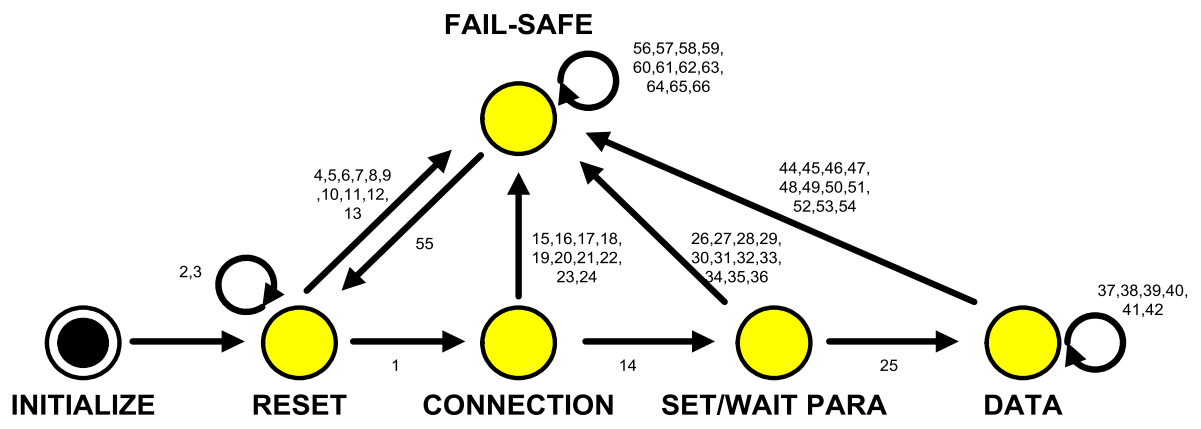


Figure 14 – Diagramme d'états du répondeur

7.4.4.2 État RESET

#	Courant	Événement /Condition =>actions	État suivant
1	RESET	RECEVOIR message de demande de connexion /CRC_Check() = TRUE => commande = 0x02 (CONNECTION) chien de garde restart() & WD = 1 ENVOYER message de réponse de connexion	CONNECTION
2	RESET	INITIALIZE terminé => attente de message	RESET
3	RESET	RECEVOIR message de demande de réinitialisation /CRC_Check() = TRUE => commande = 0x01 (RESET) chien de garde restart() & WD = 1 ENVOYER message de réponse de réinitialisation	RESET
4	RESET	RECEVOIR message de demande de sécurité intrinsèque =>	FAIL-SAFE
5	RESET	RECEVOIR message de demande de réinitialisation /CRC_Check() = FALSE => INVALID_CRC commande = 0x05(FAIL-SAFE) code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	FAIL-SAFE
6	RESET	RECEVOIR message de réponse de réinitialisation => INVALID_CMD commande = 0x05(FAIL-SAFE) code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	FAIL-SAFE
7	RESET	RECEVOIR message de demande de connexion /CRC_Check() = FALSE => INVALID_CRC commande = 0x05(FAIL-SAFE) code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	FAIL-SAFE
8	RESET	RECEVOIR message de réponse de connexion => INVALID_CMD commande = 0x05(FAIL-SAFE) code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	FAIL-SAFE
9	RESET	RECEVOIR message de demande de paramètre => INVALID_CMD commande = 0x05(FAIL-SAFE) code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	FAIL-SAFE
10	RESET	RECEVOIR message de réponse de paramètre => INVALID_CMD commande = 0x05(FAIL-SAFE) code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	FAIL-SAFE
11	RESET	RECEVOIR message de demande de données => INVALID_CMD commande = 0x05(FAIL-SAFE) code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	FAIL-SAFE
12	RESET	RECEVOIR message de réponse de données =>	FAIL-SAFE

#	Courant	Événement /Condition =>actions	État suivant
		INVALID_CMD commande = 0x05(FAIL-SAFE) code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	
13	RESET	Chien de garde expired() => WD_EXPIRED commande = 0x05(FAIL-SAFE) code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	FAIL-SAFE

7.4.4.3 État CONNECTION

#	Courant	Événement /Condition =>actions	État suivant
14	CONNECTION	RECEVOIR message de demande de paramètre /CRC_Check() = TRUE => commande = 0x03 (PARAMETER) chien de garde restart() & WD = 1 ENVOYER message de réponse de paramètre	WAIT_PARA
15	CONNECTION	RECEVOIR message de demande de sécurité intrinsèque =>	FAIL-SAFE
16	CONNECTION	RECEVOIR message de demande de réinitialisation => INVALID_CMD commande = 0x05(FAIL-SAFE) code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	FAIL-SAFE
17	CONNECTION	RECEVOIR message de réponse de réinitialisation => INVALID_CMD commande = 0x05(FAIL-SAFE) code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	FAIL-SAFE
18	CONNECTION	RECEVOIR message de demande de connexion => INVALID_CMD commande = 0x05(FAIL-SAFE) code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	FAIL-SAFE
19	CONNECTION	RECEVOIR message de réponse de connexion => INVALID_CMD commande = 0x05(FAIL-SAFE) code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	FAIL-SAFE
20	CONNECTION	RECEVOIR message de demande de paramètre /CRC_Check() = FALSE => INVALID_CRC commande = 0x05(FAIL-SAFE) code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	FAIL-SAFE
21	CONNECTION	RECEVOIR message de réponse de paramètre => INVALID_CMD commande = 0x05(FAIL-SAFE) code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	FAIL-SAFE
22	CONNECTION	RECEVOIR message de demande de données =>	FAIL-SAFE

#	Courant	Événement /Condition =>actions	État suivant
		INVALID_CMD commande = 0x05(FAIL-SAFE) code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	
23	CONNECTION	RECEVOIR message de réponse de données => INVALID_CMD commande = 0x05(FAIL-SAFE) code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	FAIL-SAFE
24	CONNECTION	Chien de garde expired() => WD_EXPIRED commande = 0x05(FAIL-SAFE) code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	FAIL-SAFE

7.4.4.4 État WAIT PARAMETER

#	Courant	Événement /Condition =>actions	État suivant
25	WAIT_PARA	RECEVOIR message de demande de données /CRC_Check() = TRUE /code de service = phase de connexion => chien de garde stop() & WD = 0 commande = 0x04 (DATA) code de service = phase de connexion ENVOYER message de réponse de données temporisateur de cadence local start() temporisateur de cadence distant start()	DATA
26	WAIT_PARA	RECEVOIR message de demande de sécurité intrinsèque =>	FAIL-SAFE
27	WAIT_PARA	RECEVOIR message de demande de réinitialisation => INVALID_CMD commande = 0x05(FAIL-SAFE) code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	FAIL-SAFE
28	WAIT_PARA	RECEVOIR message de réponse de réinitialisation => INVALID_CMD commande = 0x05(FAIL-SAFE) code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	FAIL-SAFE
29	WAIT_PARA	RECEVOIR message de demande de connexion => INVALID_CMD commande = 0x05(FAIL-SAFE) code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	FAIL-SAFE
30	WAIT_PARA	RECEVOIR message de réponse de connexion => INVALID_CMD commande = 0x05(FAIL-SAFE) code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	FAIL-SAFE
31	WAIT_PARA	RECEVOIR message de demande de paramètre => INVALID_CMD commande = 0x05(FAIL-SAFE) code de service = notification d'erreur	FAIL-SAFE

#	Courant	Événement /Condition =>actions	État suivant
		ENVOYER message de demande de sécurité intrinsèque	
32	WAIT_PARA	RECEVOIR message de réponse de paramètre => INVALID_CMD commande = 0x05(FAIL-SAFE) code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	FAIL-SAFE
33	WAIT_PARA	RECEVOIR message de demande de données /code de service = phase de données => INVALID_CMD commande = 0x05(FAIL-SAFE) code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	FAIL-SAFE
34	WAIT_PARA	RECEVOIR message de demande de données /CRC check() = FALSE => INVALID_CRC commande = 0x05(FAIL-SAFE) code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	FAIL-SAFE
35	WAIT_PARA	RECEVOIR message de réponse de données => INVALID_CMD commande = 0x05(FAIL-SAFE) code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	FAIL-SAFE
36	WAIT_PARA	Chien de garde expired() => WD_EXPIRED commande = 0x05(FAIL-SAFE) code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	FAIL-SAFE

7.4.4.5 État DATA

#	Courant	Événement /Condition =>actions	État suivant
37	DATA	L'application de sécurité fonctionnelle est tenue d'envoyer un message de demande au partenaire => chien de garde start() & WD = 1 commande = 0x04 (DATA) code de service = phase de données ENVOYER message de demande de données	DATA
38	DATA	L'application de sécurité fonctionnelle est tenue d'envoyer un message de réponse au partenaire => commande = 0x04 (DATA) code de service = phase de données ENVOYER message de réponse de données	DATA
39	DATA	RECEVOIR message de demande de données /CRC_Check() = TRUE /code de service = phase de données => Transfert des données reçues vers l'application de sécurité fonctionnelle	DATA
40	DATA	RECEVOIR message de réponse de données /CRC_Check() = TRUE /code de service = phase de données => chien de garde stop() & WD = 0	DATA

#	Courant	Événement /Condition =>actions	État suivant
		Transfert des données reçues vers l'application de sécurité fonctionnelle	
41	DATA	RECEVOIR un message de cadence /CRC_Check() = TRUE => temporisateur de cadence distant restart()	DATA
42	DATA	expiration du temporisateur de cadence local => temporisateur de cadence local start() ENVOYER message de cadence	DATA
43	DATA	RECEVOIR message de demande de sécurité intrinsèque =>	FAIL-SAFE
44	DATA	RECEVOIR message de demande de réinitialisation => INVALID_CMD commande = 0x05(FAIL-SAFE) code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	FAIL-SAFE
45	DATA	RECEVOIR message de réponse de réinitialisation => INVALID_CMD commande = 0x05(FAIL-SAFE) code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	FAIL-SAFE
46	DATA	RECEVOIR message de demande de connexion => INVALID_CMD commande = 0x05(FAIL-SAFE) code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	FAIL-SAFE
47	DATA	RECEVOIR message de réponse de connexion => INVALID_CMD commande = 0x05(FAIL-SAFE) code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	FAIL-SAFE
48	DATA	RECEVOIR message de demande de paramètre => INVALID_CMD commande = 0x05(FAIL-SAFE) code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	FAIL-SAFE
49	DATA	RECEVOIR message de réponse de paramètre => INVALID_CMD commande = 0x05(FAIL-SAFE) code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	FAIL-SAFE
50	DATA	RECEVOIR message de demande de données /CRC_Check() = FALSE => INVALID_CRC commande = 0x05(FAIL-SAFE) code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	FAIL-SAFE
51	DATA	RECEVOIR message de réponse de données /code de service = phase de connexion => INVALID_CMD commande = 0x05(FAIL-SAFE) code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	FAIL-SAFE
52	DATA	RECEVOIR message de réponse de données /code de service = phase de données /CRC_Check() = FALSE	FAIL-SAFE

#	Courant	Événement /Condition =>actions	État suivant
		=> INVALID_CRC commande = 0x05(FAIL-SAFE) code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	
53	DATA	Chien de garde expired() => WD_EXPIRED commande = 0x05(FAIL-SAFE) code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	FAIL-SAFE
54	DATA	expiration du temporisateur de cadence distant => HB_EXPIRED commande = 0x05(FAIL-SAFE) code de service = notification d'erreur ENVOYER message de demande de sécurité intrinsèque	FAIL-SAFE

7.4.4.6 État FAIL-SAFE

#	Courant	Événement /Condition =>actions	État suivant
55	FAIL-SAFE	Déclenchement par l'utilisateur => attente de message	RESET
56	FAIL-SAFE	expiration du chien de garde =>	FAIL-SAFE
57	FAIL-SAFE	expiration du temporisateur de cadence local =>	FAIL-SAFE
58	FAIL-SAFE	expiration du temporisateur de cadence distant =>	FAIL-SAFE
59	FAIL-SAFE	RECEVOIR message de demande de réinitialisation => ignorer le message	FAIL-SAFE
60	FAIL-SAFE	RECEVOIR message de réponse de réinitialisation => ignorer le message	FAIL-SAFE
61	FAIL-SAFE	RECEVOIR message de demande de connexion => ignorer le message	FAIL-SAFE
62	FAIL-SAFE	RECEVOIR message de réponse de connexion => ignorer le message	FAIL-SAFE
63	FAIL-SAFE	RECEVOIR message de demande de paramètre => ignorer le message	FAIL-SAFE
64	FAIL-SAFE	RECEVOIR message de réponse de paramètre => ignorer le message	FAIL-SAFE
65	FAIL-SAFE	RECEVOIR message de demande de données => ignorer le message	FAIL-SAFE
66	FAIL-SAFE	RECEVOIR message de réponse de données => ignorer le message	FAIL-SAFE

8 Gestion de la couche de communication de sécurité

8.1 Gestion des paramètres FSCP 17/1

L'appareil FSCP 17/1 compare les paramètres à ceux de son partenaire de communication. Le répondeur de sécurité fonctionnelle vérifie les paramètres reçus de l'initiateur de sécurité fonctionnelle à l'état PARAMETER.

8.2 Paramètres de communication de sécurité fonctionnelle

La communication de sécurité fonctionnelle entre l'initiateur de sécurité fonctionnelle et le répondeur de sécurité fonctionnelle utilise les paramètres de communication de sécurité fonctionnelle définis au Tableau 22.

Tableau 22 – Paramètres de communication de sécurité fonctionnelle

Nom	Type de Données	Plage	Description
SUID	UINT64	0 ... 2^{64}-1	ID de connexion unique entre l'émetteur de sécurité fonctionnelle et le récepteur de sécurité fonctionnelle
Délai du chien de garde de sécurité fonctionnelle	UINT16	1 ... 2^{16}-1	Délai du chien de garde pour la connexion de sécurité fonctionnelle, en ms
temporisateur de cadence local	UINT16	1 ... 2^{16}-1	Délai de cadence local, en ms
temporisateur de cadence distant	UINT16	1 ... 2^{16}-1	Délai de cadence distant, en ms

9 Exigences système

9.1 Voyants et commutateurs

Chaque appareil de sécurité doit être équipé d'une LED rouge, qui doit représenter les états suivants:

- Désactivée: Pas d'erreur. L'appareil est en mode de traitement sécurisé des données.
- Activée: État de défaillance de l'appareil. L'appareil est en anomalie.

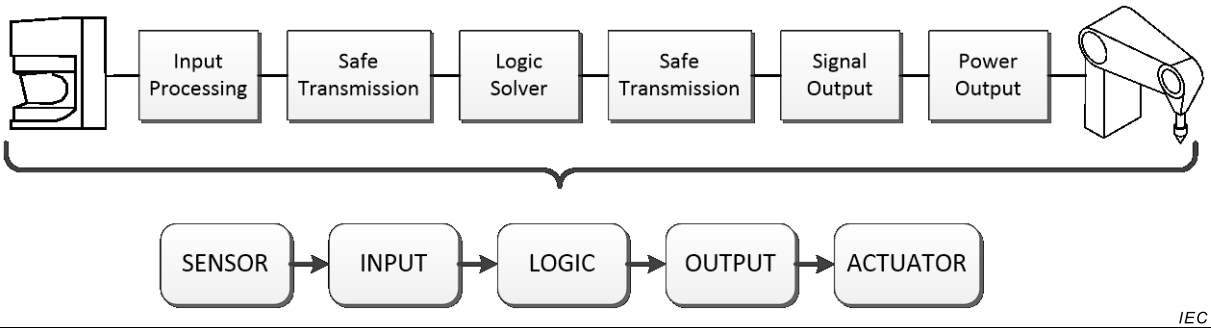
Chaque appareil de sécurité doit être équipé d'au moins un commutateur permettant de déterminer l'adresse de l'appareil sur le réseau CPF 17.

9.2 Lignes directrices d'installation

Les lignes directrices d'installation de l'IEC 61918 et les amendements spécifiques à CPF 17 de l'IEC 61784-5-17 doivent s'appliquer.

9.3 Temps de réponse de la fonction de sécurité

Le temps de réponse de la fonction de sécurité est un événement relatif à la sécurité se présentant sous la forme d'une entrée dans le système ou d'une anomalie à l'intérieur du système, jusqu'à ce que le système passe à l'état de sécurité. Le domaine d'application du temps de réaction est défini à la Figure 15.



Anglais	Français
Input processing	Traitement de l'entrée
Safe Transmission	Transmission sécurisée
Logic Solver	Unité logique
Signal Output	Sortie de signal
Power Output	Puissance de sortie
SENSOR	CAPTEUR
INPUT	ENTRÉE
LOGIC	LOGIQUE
OUTPUT	SORTIE
ACTUATOR	ACTIONNEUR

Figure 15 – Temps de réponse de la fonction de sécurité

À la Figure 15, le capteur (le commutateur, le rideau de lumière ou l'émetteur, par exemple) obtient une entrée physique qui est convertie en signal électrique. Les données du signal sont contenues dans un message de sécurité fonctionnelle transféré vers un appareil logique de sécurité (PLC de sécurité, par exemple) par l'intermédiaire d'un canal de communication de sécurité. L'appareil logique de sécurité analyse le message de sécurité et génère un message de sortie de sécurité adressé à l'appareil de sortie de sécurité fonctionnelle. L'appareil de sortie exécute une action de sécurité conformément au message de sécurité reçu.

Le temps de réponse de la fonction de sécurité est calculé grâce à la Formule (1):

$$T_{FS\_RSP} = T_{Sensor} + T_{Input} + 2 \times T_{Delay} + T_{Logic} + T_{Output} + T_{Actuator} \quad (1)$$

où

T_{FS_RSP} est le temps de réponse de la fonction de sécurité;

T_{Sensor} est le temps de réaction du capteur;

T_{Input} est le temps de réaction de l'entrée;

T_{Delay} est le temps de remise du réseau dans un sens;

T_{Logic} est le temps de réponse du contrôleur de sécurité;

T_{Output} est le temps de réaction de la sortie;

$T_{Actuator}$ est le temps de réaction de l'actionneur.

Ces valeurs de temps dépendent des caractéristiques du système, sauf du temps de remise du réseau T_{Delay}. Le temps de remise du réseau varie selon la durée d'émission du paquet,

la longueur de câble, la latence de nœud de chaque appareil de relais, le temps transversal de chaque appareil entre PHY et SCL. Le temps de remise du réseau T_{Delay} est calculé par la Formule (2).

$$T_{DELAY} = max\left\{T_{SND} + T_{PKT} + T_{CPD} + \sum_{i=0}^{N} T_{NLD\_i} + T_{RCV}, WDT\right\} \quad (2)$$

où

T_{DELAY} est le temps de remise, en microsecondes;

T_{SND} est le temps transversal de la pile de l'émetteur, y compris PHY et MAC, en microsecondes;

T_{PKT} est la durée d'émission du paquet, en microsecondes (voir la Formule (3));

T_{CPD} est le délai de propagation du câble, en microsecondes (voir la Formule (4);

T_{NLD_i} est le délai de latence du nœud i, en microsecondes (voir la Formule (5);

T_{RCV} est le temps transversal de la pile du récepteur, y compris PHY et MAC, en microsecondes;

N est le nombre de nœuds entre les appareils émetteur et récepteur. Dans FSCP 17/1, le nombre maximal est 128;

WDT est le temporisateur de chien de garde. La valeur est de 16 bits en ms.

NOTE Dans FSCP 17/1, le nombre de nœuds indique le nombre de fois que la trame est relayée. Le nombre de nœuds inclut donc les commutateurs dans le chemin vers le partenaire de communication.

La durée d'émission du paquet T_{PKT} peut être calculée par la Formule (3).

$$T_{PKT} = \frac{(FSPDUsize + POsize) \times 8}{LDR} \quad (3)$$

où

T_{PKT} est la durée d'émission du paquet, en microsecondes;

$FSPDUsize$ est la taille du FSPDU FSCP 17/1 en octets;

LDR est la vitesse de transmission des données de liaison, en bit par seconde;

$POsize$ est la taille du traitement de protocoles de CPF 17, en octets.

Le délai de propagation du câble T_{CPD} peut être calculé par la Formule (4).

$$T_{CPD} = T_{CPD/M} \times L_{TC} \quad (4)$$

où

T_{CPD} est le délai de propagation du câble, en microsecondes;

$T_{CPD/M}$ est le délai de propagation du câble, en nanosecondes par mètre (selon les caractéristiques du câble sélectionné);

L_{TC} est la longueur totale du câble, en mètre.

Le délai de latence du nœud T_{NLD_i} peut être calculé par la Formule (5).

$$T_{NLD\_i} = T_{NPD\_i} + T_{PKT\_i} + \sum_{j=0}^{M} T_{TX\_PKT\_ij} \quad (5)$$

où

T_{NLD_i} est le délai de latence du nœud i en microsecondes;

T_{NPD_i} est le délai de propagation du nœud i en microsecondes;

T_{PKT_i} est la durée d'émission du paquet du nœud i en microsecondes (voir la Formule (3));

$T_{TX\_PKT\_ij}$ est la durée d'émission du paquet j, en microsecondes, dans la file d'attente de transmission du port du nœud i en face de ce paquet (selon la taille FSPDU du nœud i), voir la Formule (3));

M est le nombre de paquets dans la file d'attente de transmission du port du nœud i en face de ce paquet.

9.4 Durée des demandes

La durée de la demande entre l'application relative à la sécurité et la couche de communication de sécurité doit être suffisante pour garantir qu'elle est plus longue que le délai du chien de garde ou que le délai de cadence à détecter par l'application.

9.5 Contraintes liées au calcul des caractéristiques du système

9.5.1 Généralités

Les appareils de sécurité sont conçus pour évoluer dans des environnements industriels normaux conformément à l'IEC 61000-6-2 ou à l'IEC 61131-2, et offrent une immunité renforcée conformément à l'IEC 61326-3-1 ou à l'IEC 61326-3-2.

Plusieurs contraintes doivent être utilisées pour calculer les caractéristiques relatives à la sécurité des systèmes utilisant FSCP 17/1.

9.5.2 Nombre d'appareils

Les mises en œuvre FSCP 17/1 sont limitées à 128 appareils au maximum. Pour calculer le taux d'erreurs résiduelles d'une fonction de sécurité spécifique, la formule (1) de l'IEC 61784-3:— doit être appliquée.

9.5.3 Considération en matière de probabilité

FSCP 17/1 offre un taux d'erreurs résiduelles inférieur à 10^{-9} par heure avec un taux d'erreur sur les bits de 0,01. Une trame du PDU FSCP 17/1 pour la communication de sécurité fonctionnelle contient plusieurs champs CRC, le polynôme CRC n'étant pas le même que la FCS de la trame Ethernet.

Par exemple, un FSPDU avec un champ d'en-tête de 4 octets et un champ de données de sécurité de 4 octets présente une probabilité d'erreur résiduelle d'environ $1{,}06 \times 10^{-20}$ avec le polynôme CRC donné.

La probabilité d'erreur d'un FSPDU est calculée selon la Formule (6):

$$PE(BER) = 1 - \{1 - R_{sl}(BER)\}^n \quad (6)$$

où

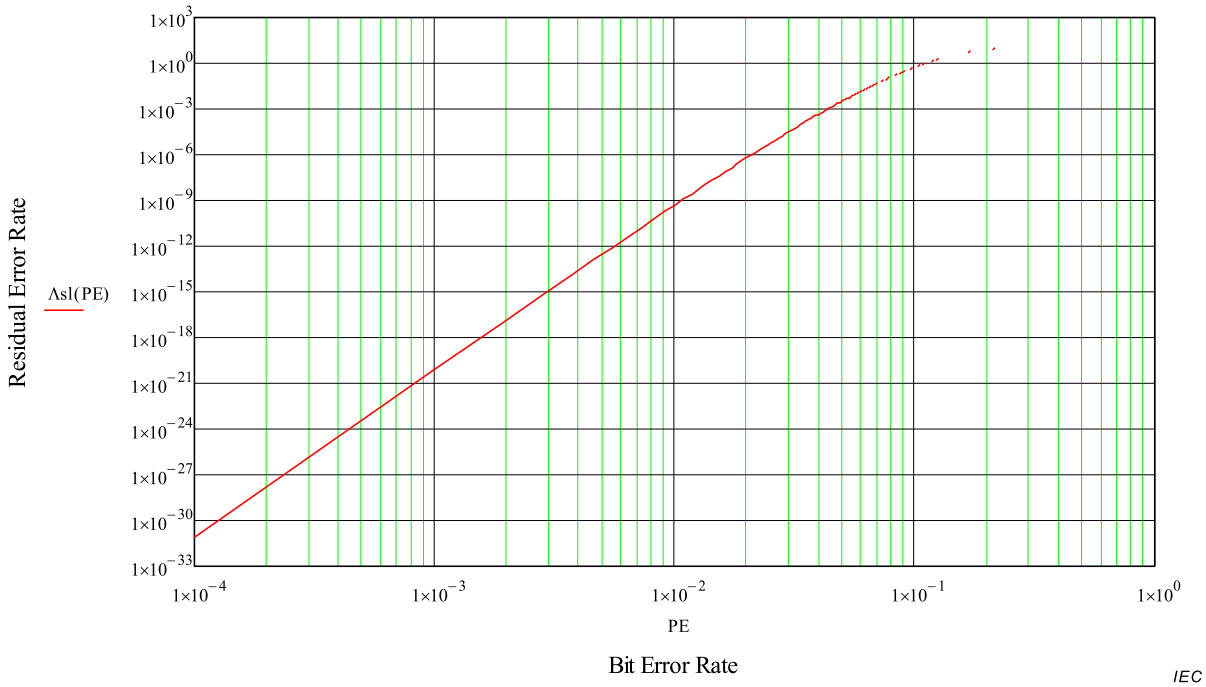
PE(BER) est le taux d'erreur sur les paquets du FSPDU;

$R_{sl}(BER)$ est le taux d'erreurs résiduelles du FSPDU de base, avec une valeur de $1{,}06 \times 10^{-20}$;

BER est le taux d'erreur sur les bits, avec une valeur de 0,01;

n est le nombre de blocs de données de sécurité, champ d'en-tête inclus, l'unité de valeur étant de 4 octets.

La Figure 16 présente le taux d'erreurs résiduelles du protocole FSCP 17/1.



Anglais	Français
Residual Error Rate	Taux d'erreurs résiduelles
Bit Error Rate	Taux d'erreur sur les bits

Figure 16 – Taux d'erreurs résiduelles de FSCP 17/1

9.6 Maintenance

Ce protocole ne fait l'objet d'aucune exigence particulière en matière de maintenance.

9.7 Manuel de sécurité

Les implémenteurs de la présente partie doivent fournir un manuel de sécurité contenant au moins les informations suivantes:

- Contraintes liées au calcul des caractéristiques du système.
- Les responsabilités des utilisateurs quant au paramétrage correct de l'appareil.

Outre les exigences de l'Article 9, le manuel de sécurité doit satisfaire à toutes les exigences de l'IEC 61508.

10 Évaluation

Il est vivement recommandé aux implémenteurs du protocole FSCP 17/1 d'obtenir une vérification pour tous les aspects du produit liés à la sécurité fonctionnelle, y compris le protocole et une application, conformément aux exigences d'indépendance et de compétence de l'IEC 61508-1:2010, Article 8. Il est vivement recommandé aux implémenteurs de FSCP 17/1 d'obtenir confirmation de la réalisation d'un essai de conformité adapté.

Annexe A
(informative)

Informations supplémentaires pour les profils de communication de sécurité fonctionnelle de CPF 17

A.1 Calcul de la fonction de hachage

```
// The crc polynomial chosen is [0x00015A67], it is in detail:
// G(x)={x32+x16+x14+x12+x11+x9+x6+x5+x2+x1+1}

#define POLYNOMIAL 0x00015A67

void gen_crc_code()
{
        uint32 i, j;
        uint32 crc_accum;

        for(i=0; i<256; i++)
        {
                crc_accum = (i << 24);
                for(j=0; j<8; j++)
                {
                        if(crc_accum & 0x80000000)
                                crc_accum = (crc_accum << 1) ^ POLYNOMIAL;
                        else
                                crc_accum = (crc_accum << 1);
                }
                crc_table[i] = crc_accum;
        }
        return;
}

uint32 CRCTable[256];
uint32 CRC32(uint8 *pucData, uint32 ulSize)
{
        uint32 crc_accum = 0;
        uint32 i, j, k;

        for(j=0;j<ulSize;j++){
                i = (crc_accum ^ * pucData ++);
                crc_accum = 0;
                for(k=0;k<4;k++)
                {
                        crc_accum = crc_accum ^ (CRCTable[(i >> (k*8)) & 0xff] <<
k*8);
                }
        }
        return crc_accum;
}
```

Le CRC32 pour le protocole FSCP 17/1 est calculé à l'aide de l'algorithme suivant:

$$G(x)=\{x^{32}+x^{16}+x^{14}+x^{12}+x^{11}+x^{9}+x^{6}+x^{5}+x^{2}+x^{1}+1\}$$

Ce polynôme fournit un mot de code de distance de Hamming minimale de 11 bits à 65 bits [39].

La table de recherche de ce polynôme pour chaque 8 bits est présentée au Tableau A.1 ci-dessous.

Tableau A.1 – Table de recherche pour FSCP 17/1

Table de recherche CRC (0...255)							
00000000	00015a67	0002b4ce	0003eea9	0005699c	000433fb	0007dd52	00068735
000ad338	000b895f	000867f6	00093d91	000fbaa4	000ee0c3	000d0e6a	000c540d
0015a670	0014fc17	001712be	001648d9	0010cfec	0011958b	00127b22	00132145
001f7548	001e2f2f	001dc186	001c9be1	001a1cd4	001b46b3	0018a81a	0019f27d
002b4ce0	002a1687	0029f82e	0028a249	002e257c	002f7f1b	002c91b2	002dcbd5
00219fd8	0020c5bf	00232b16	00227171	0024f644	0025ac23	0026428a	002718ed
003eea90	003fb0f7	003c5e5e	003d0439	003b830c	003ad96b	003937c2	00386da5
003439a8	003563cf	00368d66	0037d701	00315034	00300a53	0033e4fa	0032be9d
005699c0	0057c3a7	00542d0e	00557769	0053f05c	0052aa3b	00514492	00501ef5
005c4af8	005d109f	005efe36	005fa451	00592364	00587903	005b97aa	005acdcd
00433fb0	004265d7	00418b7e	0040d119	0046562c	00470c4b	0044e2e2	0045b885
0049ec88	0048b6ef	004b5846	004a0221	004c8514	004ddf73	004e31da	004f6bbd
007dd520	007c8f47	007f61ee	007e3b89	0078bcbc	0079e6db	007a0872	007b5215
00770618	00765c7f	0075b2d6	0074e8b1	00726f84	007335e3	0070db4a	0071812d
00687350	00692937	006ac79e	006b9df9	006d1acc	006c40ab	006fae02	006ef465
0062a068	0063fa0f	006014a6	00614ec1	0067c9f4	00669393	00657d3a	0064275d
00ad3380	00ac69e7	00af874e	00aedd29	00a85a1c	00a9007b	00aaeed2	00abb4b5
00a7e0b8	00a6badf	00a55476	00a40e11	00a28924	00a3d343	00a03dea	00a1678d
00b895f0	00b9cf97	00ba213e	00bb7b59	00bdfc6c	00bca60b	00bf48a2	00be12c5
00b246c8	00b31caf	00b0f206	00b1a861	00b72f54	00b67533	00b59b9a	00b4c1fd
00867f60	00872507	0084cbae	008591c9	008316fc	00824c9b	0081a232	0080f855
008cac58	008df63f	008e1896	008f42f1	0089c5c4	00889fa3	008b710a	008a2b6d
0093d910	00928377	00916dde	009037b9	0096b08c	0097eaeb	00940442	00955e25
00990a28	0098504f	009bbee6	009ae481	009c63b4	009d39d3	009ed77a	009f8d1d
00fbaa40	00faf027	00f91e8e	00f844e9	00fec3dc	00ff99bb	00fc7712	00fd2d75
00f17978	00f0231f	00f3cdb6	00f297d1	00f410e4	00f54a83	00f6a42a	00f7fe4d
00ee0c30	00ef5657	00ecb8fe	00ede299	00eb65ac	00ea3fcb	00e9d162	00e88b05
00e4df08	00e5856f	00e66bc6	00e731a1	00e1b694	00e0ecf3	00e3025a	00e2583d
00d0e6a0	00d1bcc7	00d2526e	00d30809	00d58f3c	00d4d55b	00d73bf2	00d66195
00da3598	00db6fff	00d88156	00d9db31	00df5c04	00de0663	00dde8ca	00dcb2ad
00c540d0	00c41ab7	00c7f41e	00c6ae79	00c0294c	00c1732b	00c29d82	00c3c7e5
00cf93e8	00cec98f	00cd2726	00cc7d41	00cafa74	00cba013	00c84eba	00c914dd
Ce tableau contient des valeurs de 32 bits en représentation hexadécimale pour chaque valeur (0...255) des variations de 8 bits. Il convient d'utiliser le tableau dans l'ordre croissant, du coin supérieur gauche (0) vers le coin inférieur droit (255).							

A.2 ...

Vide

Annexe B
(informative)

Informations pour l'évaluation des profils de communication de sécurité fonctionnelle de CPF 17

Selon les règles de l'IEC, la présente norme n'énonce pas les conditions de validation de la conformité. Toutefois, les essais et validation de conformité des appareils FSCP 17/1 à l'IEC 61784-3-17 peuvent être exigés par la loi.

L'information correspondante relative aux essais et à la conformité à la présente norme peut être obtenue auprès des comités nationaux locaux de l'IEC ou de l'organisation de bus de terrain compétente.

NOTE Pour l'IEC 61784-3-17, l'organisation de bus de terrain compétente est Automation Control Team, LSIS Co Ltd, voir www.lsis.biz

Bibliographie

[1] IEC 60050 (toutes les parties), *Vocabulaire Électrotechnique International,* disponible à l'adresse http://www.electropedia.org/

NOTE Voir également le dictionnaire multilingue de l'IEC – Électricité, électronique et télécommunications (disponible sur CD-ROM et à l'adresse <http://www.electropedia.org>).

[2] IEC 60050-191:1990, *Vocabulaire Électrotechnique International – Partie 191: Sûreté de fonctionnement et qualité de service*

[3] IEC 60204-1, *Sécurité des machines – Équipement électrique des machines – Partie 1: Règles générales*

[4] IEC TS 61000-1-2*, Compatibilité électromagnétique (CEM) – Partie 1-2: Généralités – Méthodologie pour la réalisation de la sécurité fonctionnelle des matériels électriques et électroniques du point de vue des phénomènes électromagnétiques*

[5] IEC 61000-6-7:2014, *Compatibilité électromagnétique (CEM) – Partie 6-7: Normes génériques – Exigences d'immunité pour les équipements visant à exercer des fonctions dans un système lié à la sécurité (sécurité fonctionnelle) dans des sites industriels*

[6] IEC 61131-6, *Automates programmables – Partie 6: Sécurité fonctionnelleb*

[7] IEC 61158-2, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 2: Spécification et définition des services de la couche physique*

[8] IEC 61496 (toutes les parties), *Sécurité des machines – Équipements de protection électro-sensibles*

[9] IEC 61508-2, *Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité – Partie 2: Exigences pour les systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité*

[10] IEC 61508-4:2010, *Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité – Partie 4: Définitions et abréviationsb*

[11] IEC 61508-5:2010, *Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité – Partie 5: Exemples de méthodes de détermination des niveaux d'intégrité de sécurité*

[12] IEC 61511 (toutes les parties), *Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur des industries de transformationb*

[13] IEC 61784-4 [6], *Industrial communication networks – Profiles – Part 4: Secure communications for fieldbuses* (disponible en anglais seulement)

[14] IEC 61784-5 (toutes les parties), *Réseaux de communication industriels – Profils – Partie 5: Installation des bus de terrain – Profils d'installation pour CPF x*

[15] IEC 61800-5-2, *Entraînements électriques de puissance à vitesse variable – Partie 5-2: Exigences de sécurité – Fonctionnelle*

---

6 Proposition d'un nouveau sujet d'étude à l'étude.

[16] IEC TR 62059-11:2002, *Équipements de comptage de l'électricité – Sûreté de fonctionnement – Partie 11: Concepts généraux*

[17] IEC 62061, *Sécurité des machines – Sécurité fonctionnelle des systèmes de commande électriques, électroniques et électroniques programmables relatifs à la sécurité*

[18] IEC TR 62210:2003, *Power system control and associated communications – Data and communication security* (disponible en anglais seulement)

[19] IEC 62280:2014, *Applications ferroviaires – Systèmes de signalisation, de télécommunication et de traitement – Communication de sécurité dans les systèmes de transmission*

[20] IEC 62443 (toutes les parties), *Industrial communication networks – Network and system security* (disponible en anglais seulement)

[21] IEC TR 62685, *Réseaux de communication industriels – Profils – Lignes directrices pour l'évaluation des appareils de sécurité utilisant les profils de communication pour la sécurité fonctionnelle (FSCP) de la CEI 61784-3*

[22] ISO/IEC Guide 51:2014, *Aspects liés à la sécurité – Principes directeurs pour les inclure dans les normes*

[23] ISO/IEC 2382-14, *Technologies de l'information – Vocabulaire – Partie 14: Fiabilité, maintenabilité et disponibilité*

[24] ISO/IEC 2382-16:1996, *Technologies de l'information – Vocabulaire – Partie 16: Théorie de l'information*

[25] ISO/IEC 7498-1:1994, *Information Technology – Open Systems Interconnection – Basic Reference Model: The Basic Model* (disponible en anglais seulement)

[26] ISO 10218-1, *Robots et dispositifs robotiques – Exigences de sécurité pour les robots industriels – Partie 1: Robots*

[27] ISO 12100, *Sécurité des machines – Principes généraux de conception – Appréciation du risque et réduction du risque*

[28] ISO 13849 (toutes les parties), *Sécurité des machines – Parties des systèmes de commande relatives à la sécurité*

[29] ISO 13849-1:2006, *Sécurité des machines – Parties des systèmes de commande relatives à la sécurité – Partie 1: Principes généraux de conception*

[30] ISO 13849-2, *Sécurité des machines – Parties des systèmes de commande relatives à la sécurité – Partie 2: Validation*

[31] IEEE 802.3, *IEEE Standard for 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* (disponible en anglais seulement)

[32] ANSI/ISA-84.00.01-2004 (toutes les parties), *Functional Safety: Safety Instrumented Systems for the Process Industry Sector* (disponible en anglais seulement)

[33] VDI/VDE 2180 (toutes les parties), *Safeguarding of industrial process plants by means of process control engineering* (disponible en anglais seulement)

[34] ANDREW S. TANENBAUM, DAVID J. WETHERALL, *Computer Networks*, 5th Edition, Prentice Hall, N.J., ISBN-10: 0132126958, ISBN-13: 978-0132126953 (disponible en anglais seulement)

[35] W. WESLEY PETERSON, EDWARD J. WELDON, *Error-Correcting Codes*, 2nd Edition 1972, MIT-Press, ISBN 0-262-16-039-0 (disponible en anglais seulement)

[36] NFPA79 (2012), *Electrical Standard for Industrial Machinery* (disponible en anglais seulement)

[37] GUY E. CASTAGNOLI, *On the Minimum Distance of Long Cyclic Codes and Cyclic Redundancy-Check Codes*, 1989, Dissertation No. 8979 of ETH Zurich, Switzerland (disponible en anglais seulement)

[38] 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 (disponible en anglais seulement)

[39] JUSTIN RAY and PHILIP KOOPMAN: *Efficient High Hamming Distance CRCs for Embedded Networks,* Proceedings of the 2006 International Conference on Dependable Systems and Networks (DSN'06), IEEE Conference Publications 2006, pp3-12 (disponible en anglais seulement)

_____

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

3, rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

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