

INTERNATIONAL STANDARD

NORME INTERNATIONALE



**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**



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2016 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'IEC ou du Comité national de l'IEC du pays du demandeur. Si vous avez des questions sur le copyright de l'IEC ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de l'IEC de votre pays de résidence.

IEC Central Office
3, rue de Varembe
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.

INTERNATIONAL STANDARD

NORME INTERNATIONALE



**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

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

CONTENTS

FOREWORD.....	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.

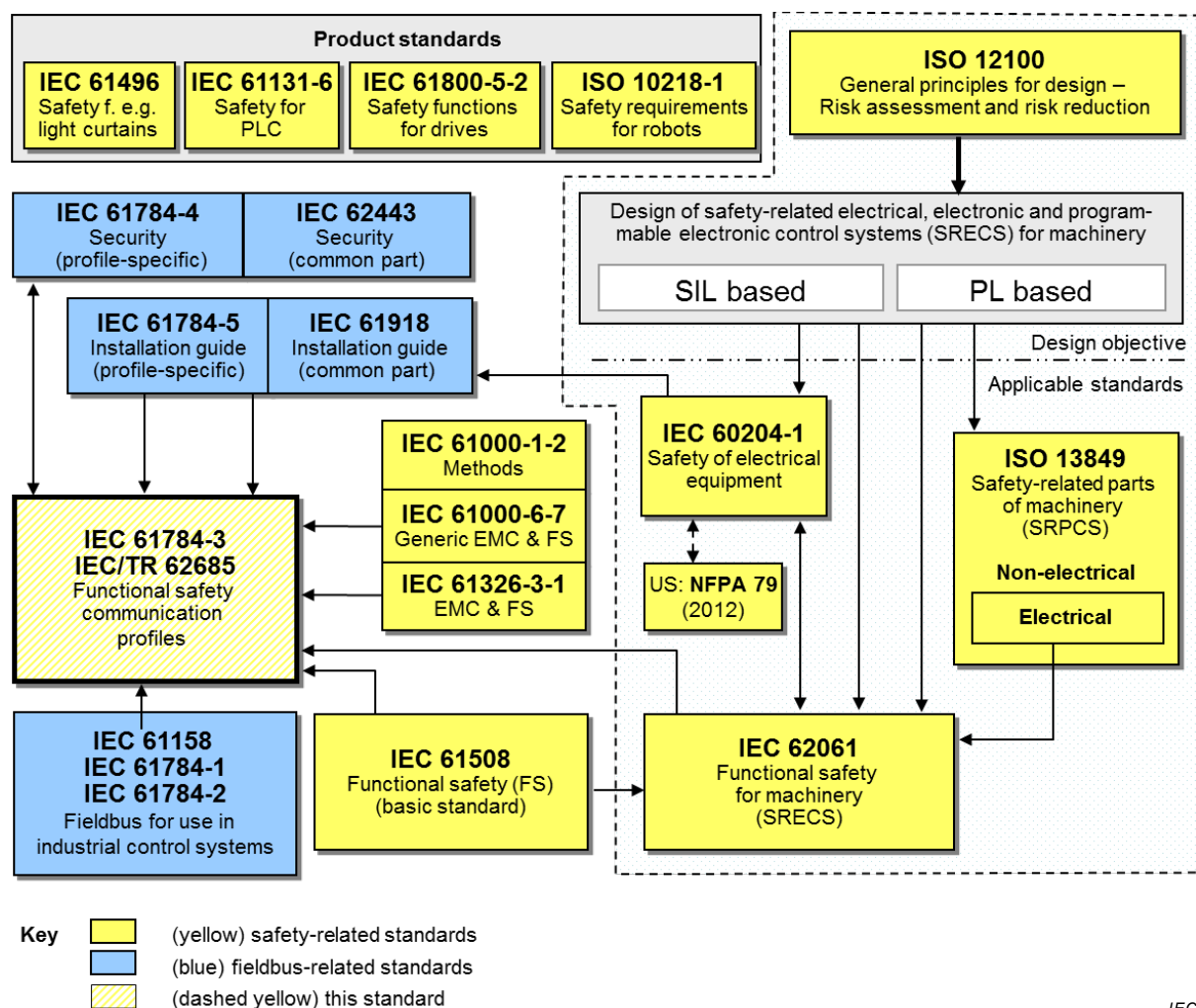
0 Introduction

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.

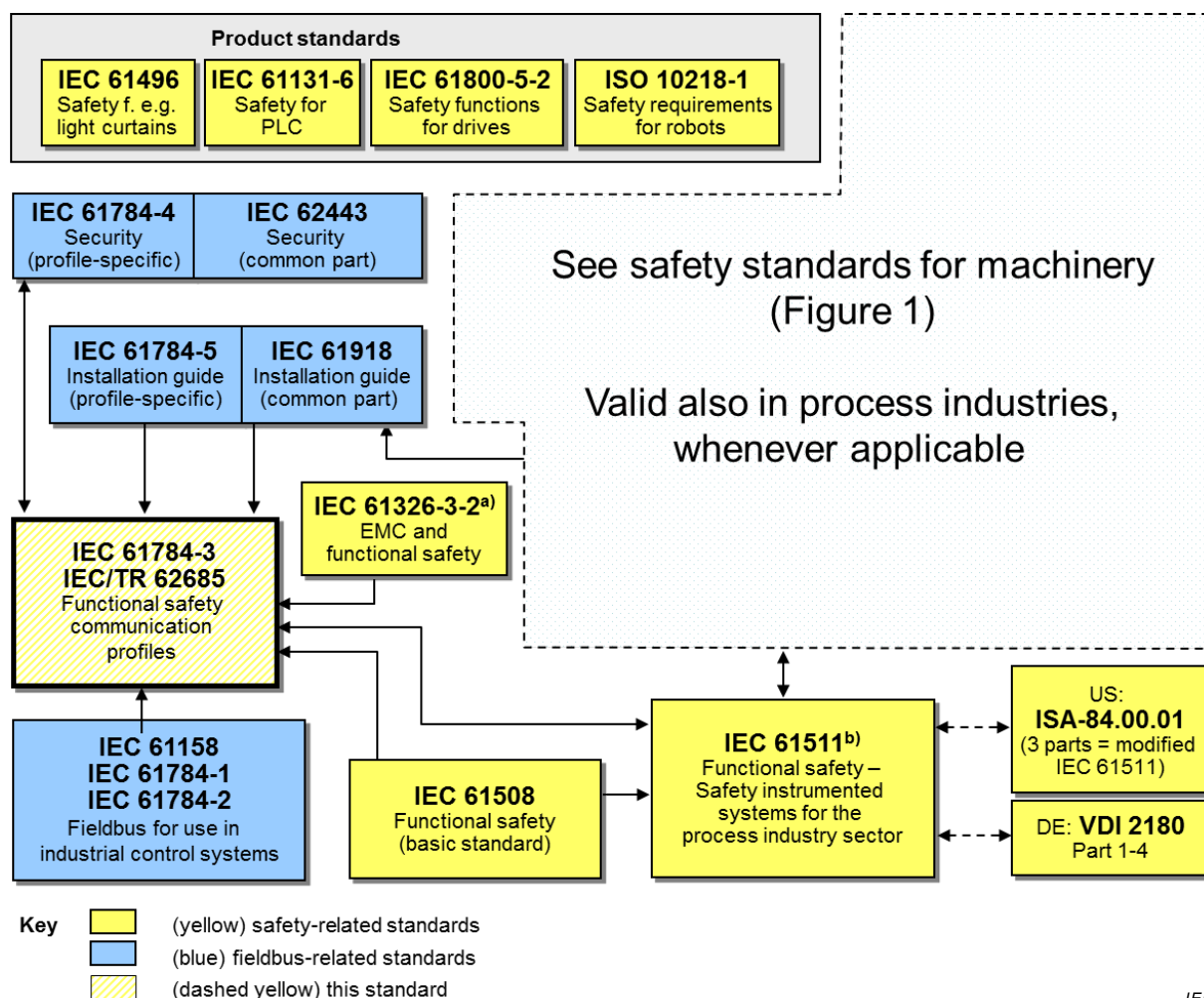
Figure 1 shows the relationships between this standard and relevant safety and fieldbus standards in a machinery environment.



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, Hogue-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 part¹ defines mechanisms for the transmission of safety-relevant messages among participants within a distributed network using fieldbus technology in accordance with the requirements of IEC 61508 series² for functional safety. These mechanisms may be used in various industrial applications such as process control, manufacturing automation, and machinery.

This part provides guidelines for both developers and assessors of compliant devices and systems.

NOTE 2 The resulting SIL claim of a system depends on 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 (t_1 , t_2)

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.

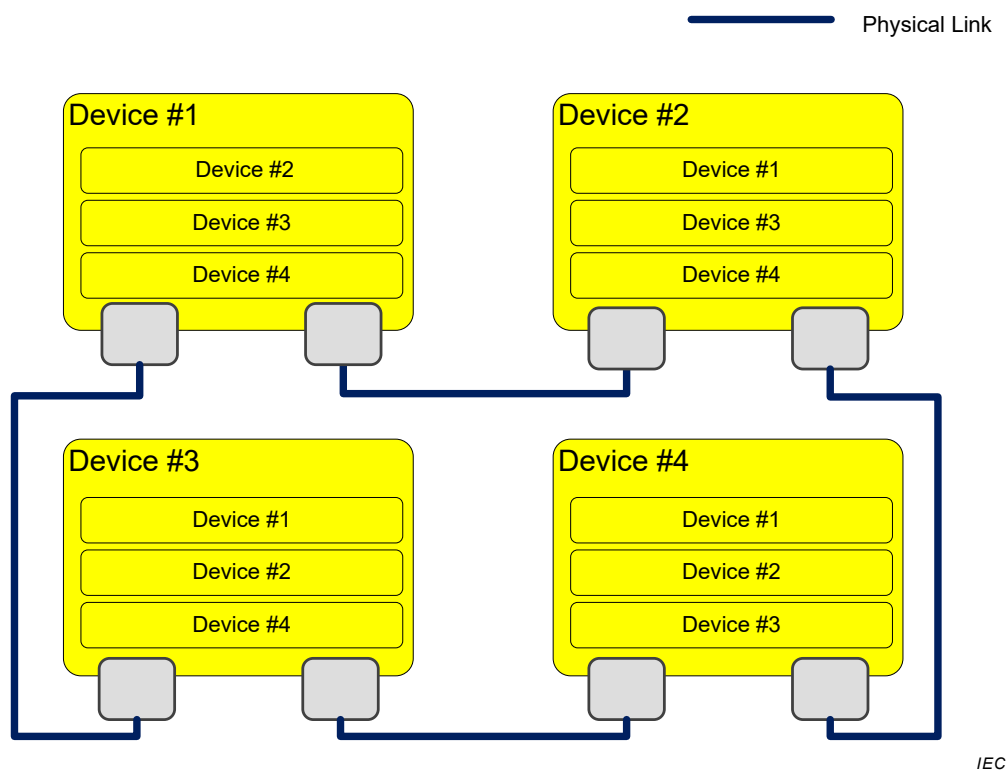


Figure 3 – Communication relationships among FSCP 17 devices

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

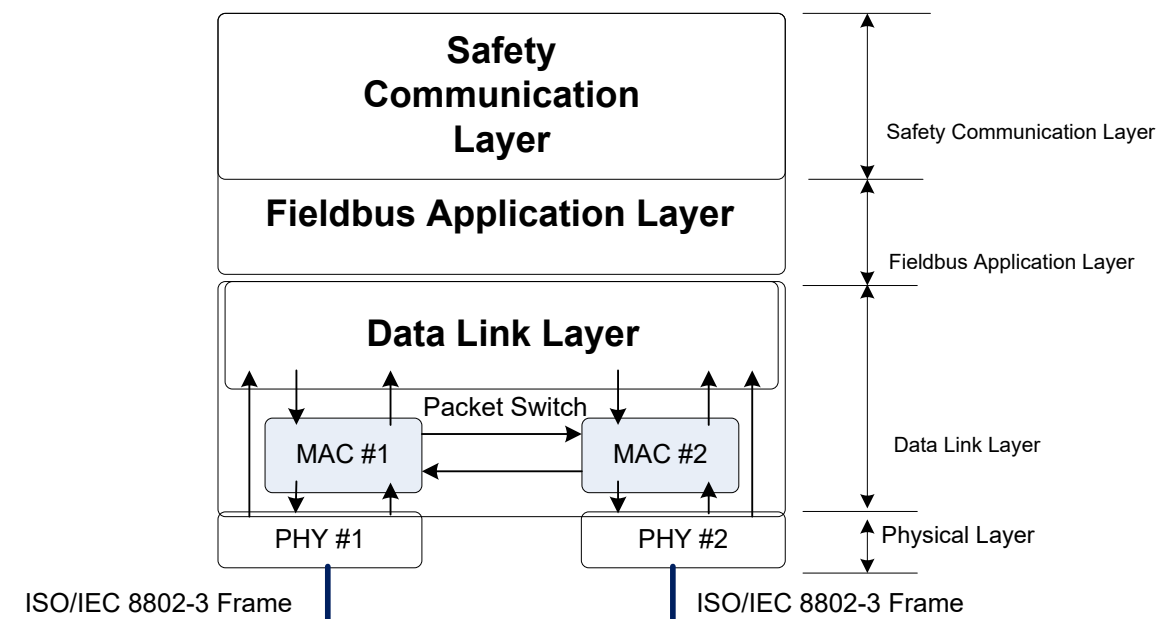
- random malfunctions, for example due to EMI impact on the transmission channel,
- failures/faults of the standard hardware,
- systematic malfunctions of components within the standard hardware and software.

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.



IEC

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.

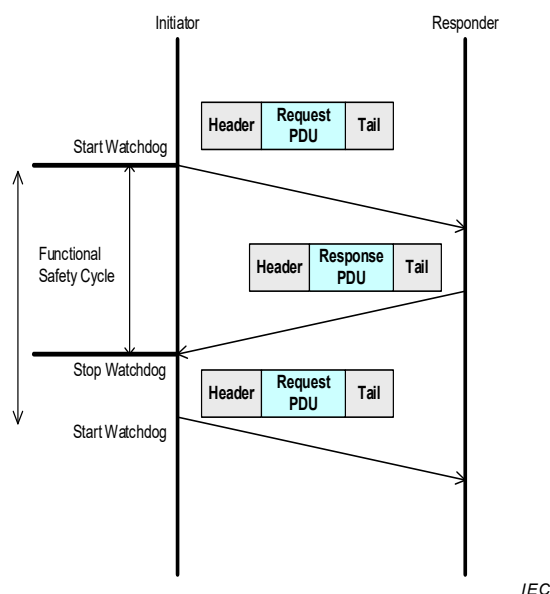
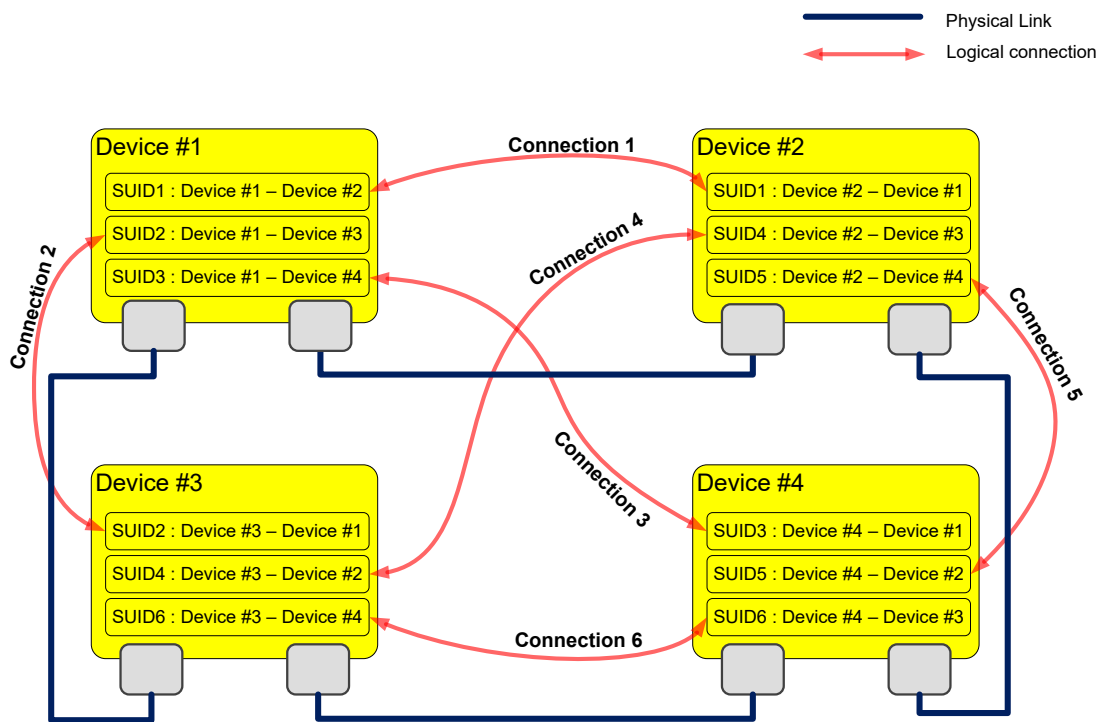


Figure 5 – Functional Safety Cycle

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.



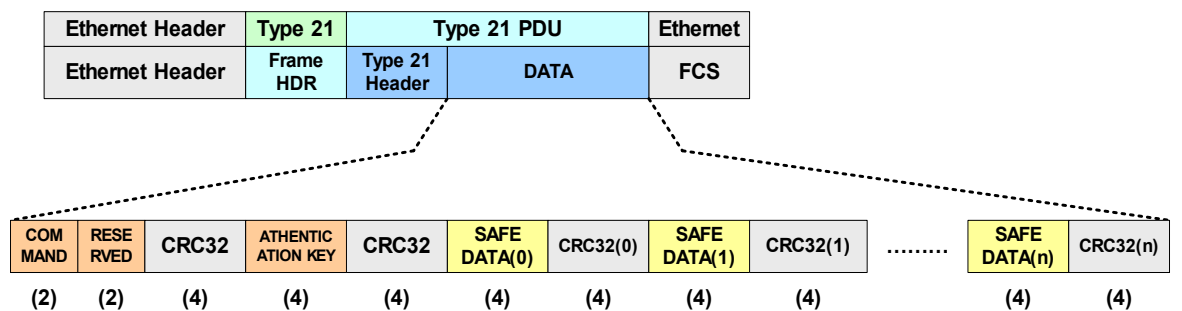
IEC

Figure 6 – Connection relationships among FSCP 17/1 devices

7 Safety communication layer protocol

7.1 Safety PDU format

7.1.1 General



IEC

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
...	...	...
$n \times 8 + 16$	SafeData[n]	Safety data, 4 octets
$n \times 8 + 20$	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.

$CRC_i := f(SUID, (virtual) Sequence_Number, command \text{ or } 4 \text{ octets Data}[i])$

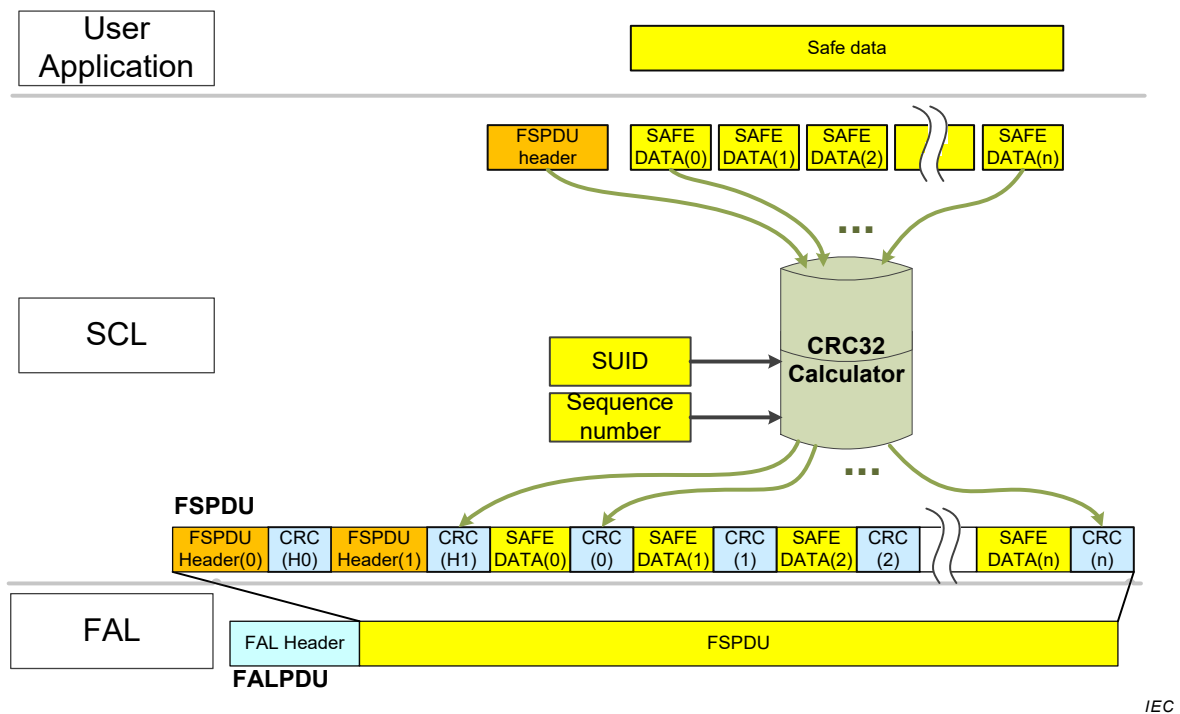


Figure 8 – FSPDU CRC code generation process

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.

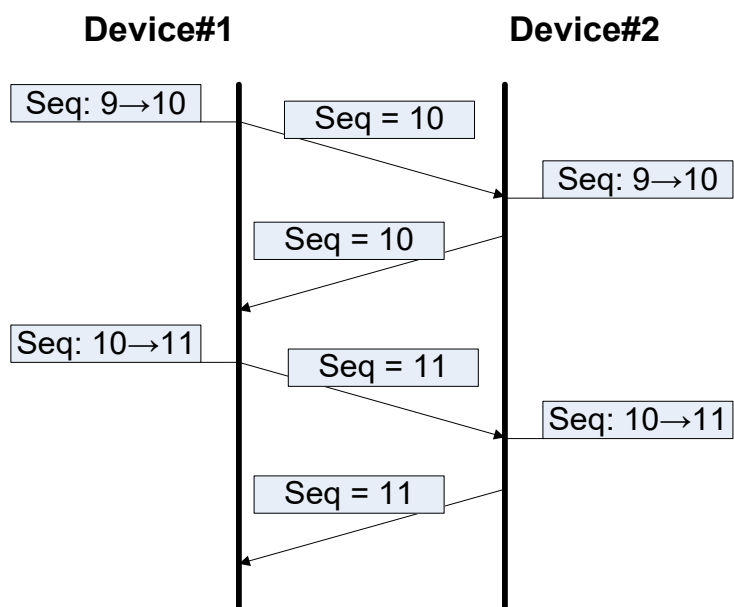
$SUID = f(\text{source MAC address and device ID, destination MAC address and device ID})$

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.



IEC

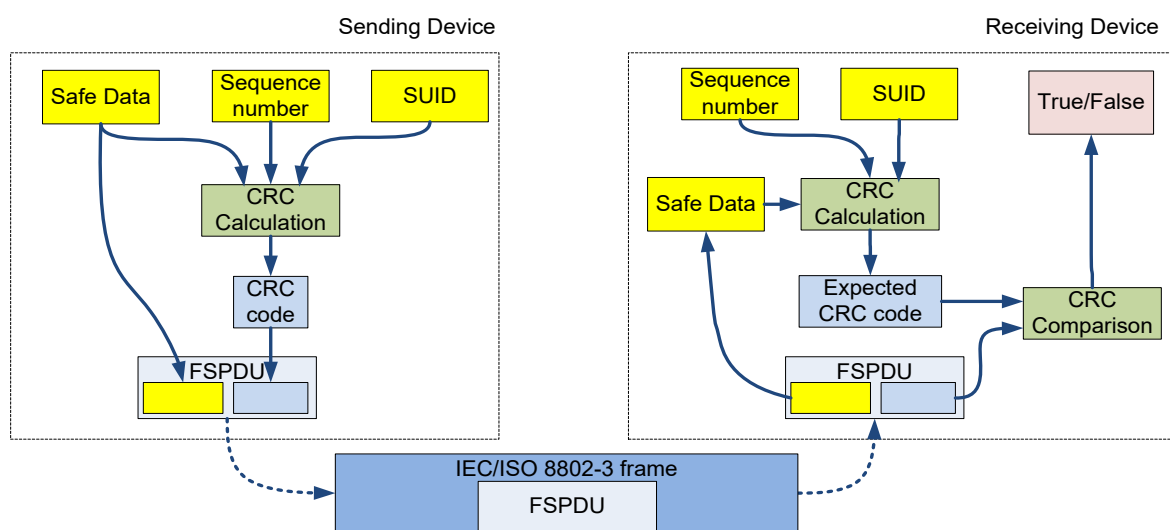
Figure 9 – Example of sequence number changing

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.



IEC

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.

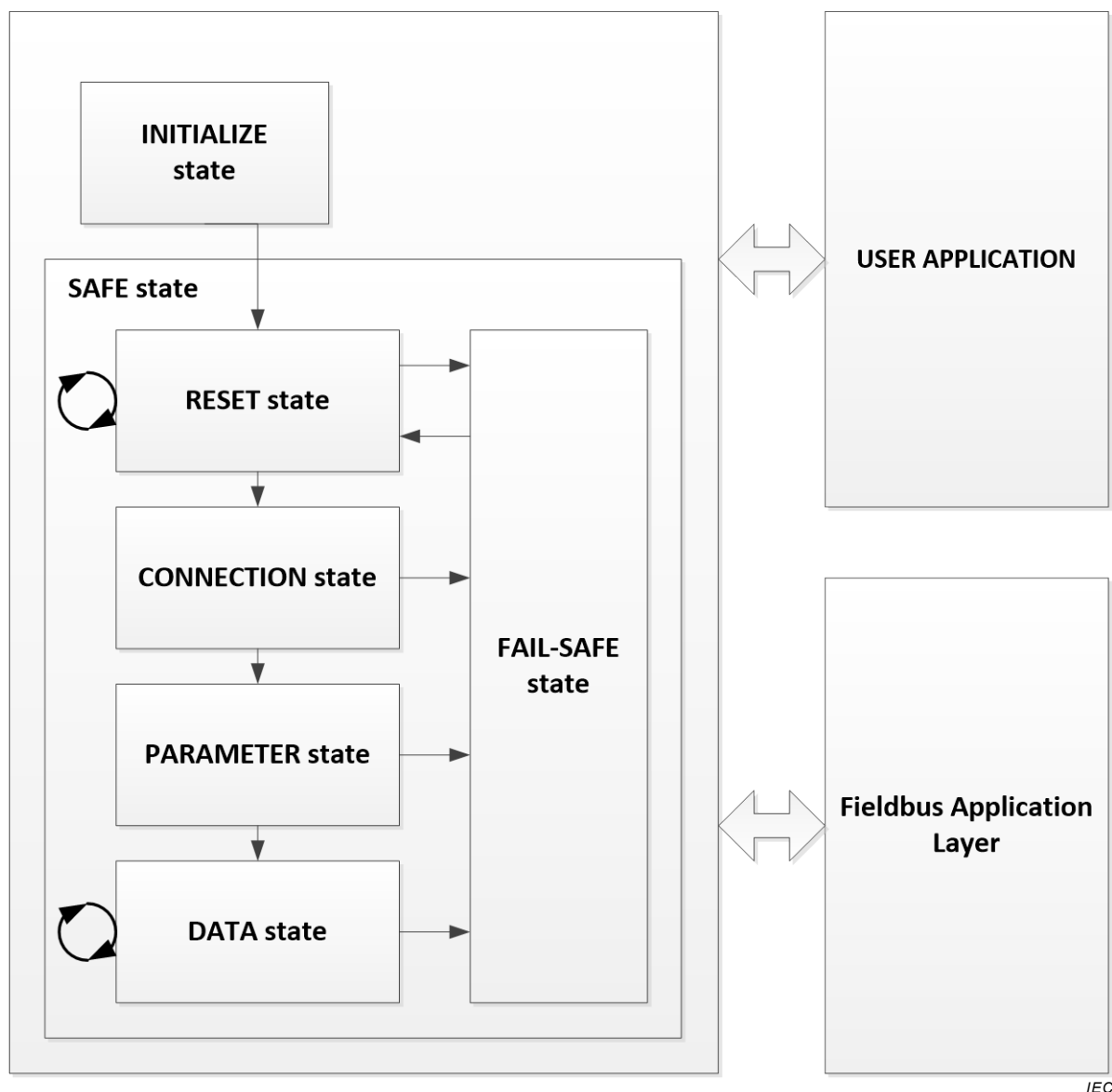


Figure 11 – FSCP 17/1 device states

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 respective 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.

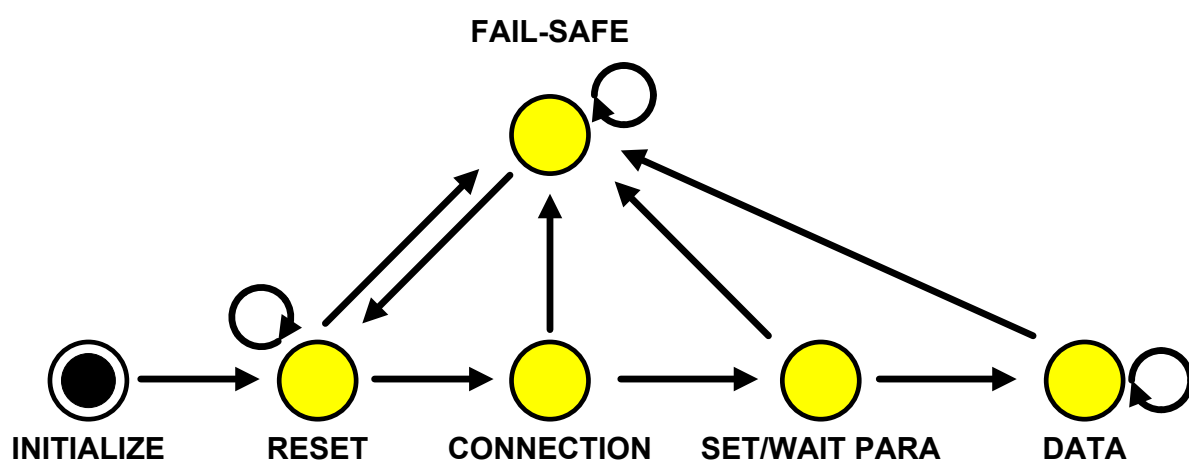
Table 19 – States of the Functional Safety Initiator

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.



IEC

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.