IEC 61784-3-1

Edition 1.0 2007-12

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Industrial communication networks – Profiles – Part 3-1: Functional safety fieldbuses – Additional specifications for CPF 1

Réseaux de communication industriels – Profils – Partie 3-1: Bus de terrain à sécurité fonctionnelle – Spécifications complémentaires pour le CPF 1

IEC 61784-3-1:2007-12(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 It also gives information on projects, replaced and withdrawn publications.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 more than 30 000 terms and definitions in English and French, with equivalent terms in 14 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary
More than 55 000 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 plus de 30 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans 14 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

Glossaire IEC - std.iec.ch/glossary
Plus de 55 000 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 61784-3-1

Edition 1.0 2007-12

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Industrial communication networks – Profiles – Part 3-1: Functional safety fieldbuses – Additional specifications for CPF 1

Réseaux de communication industriels – Profils – Partie 3-1: Bus de terrain à sécurité fonctionnelle – Spécifications complémentaires pour le CPF 1

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

PRICE CODE XB
CODE PRIX

ICS 25.040.40; 35.100.05

ISBN 978-2-8322-1985-0

CONTENTS

FOREWORD 6
INTRODUCTION 8
1 Scope 11
2 Normative references 11
3 Terms, definitions, symbols, abbreviated terms and conventions 12
3.1 Terms and definitions 12
3.1.1 Common terms and definitions 12
3.1.2 CPF 1: Additional terms and definitions 16
3.2 Symbols and abbreviated terms 17
3.2.1 Common symbols and abbreviated terms 17
3.2.2 CPF 1: Additional symbols and abbreviated terms 18
3.3 Conventions 18
3.3.1 State Diagrams 18
3.3.2 Use of colors in figures 19
4 Overview of FSCP 1/1 (FOUNDATION Fieldbus™ SIS) 20
4.1 General 20
4.2 Key concepts of FSCP 1/1 21
4.2.1 Black channel 21
4.2.2 Connection key 21
4.2.3 Cross-check 21
4.2.4 FSCP 1/1 21
4.2.5 Programmable electronic system 21
4.2.6 Queuing delays 21
4.2.7 Redundancy 22
4.2.8 SIL environment 22
4.3 Key components of FSCP 1/1 22
4.3.1 Overview 22
4.3.2 Black channel 22
4.4 Relationship to the ISO OSI basic reference model 23
5 General 23
5.1 External documents providing specifications for the profile 23
5.2 Safety functional requirements 23
5.2.1 Requirements for functional safety 23
5.2.2 Functional constraints 24
5.2.3 Device manufacturer requirements 24
5.3 Safety measures 25
5.3.1 Sequence number 25
5.3.2 Time stamp 25
5.3.3 Time expectation 25
5.3.4 Connection authentication 25
5.3.5 Data integrity assurance 25
5.3.6 Redundancy with cross checking 25
5.3.7 Different data integrity assurance systems 25
5.3.8 Relationships between errors and safety measures 25
5.4 Safety communication layer structure 26
5.4.1 Network topology and device connectivity 26

5.4.2 Device architecture 26
5.5 Relationships with FAL (and DLL, PhL) 27
5.5.1 General 27
5.5.2 Data Types 28
6 Safety communication layer services 28
6.1 Application Process (AP) 28
6.1.1 Overview 28
6.1.2 Network visible objects 29
6.1.3 Application layer interface 29
6.1.4 Object dictionary 29
6.1.5 Application program directory 29
6.2 Function block application processes 29
6.2.1 General 29
6.2.2 Function block model 29
6.2.3 Application process 32
6.3 Device to device communications 34
6.3.1 General 34
6.3.2 Client/server 34
6.3.3 Publisher/subscriber 35
6.3.4 Report distribution 35
6.3.5 FBAP operation in a linking device 35
6.3.6 System management kernel protocol (SMKP) communications 35
6.4 Profiles 35
6.4.1 General 35
6.4.2 FSCP 1/1 profile 35
6.5 Device descriptions 36
6.6 Common file formats 37
6.7 Configuration information 37
6.7.1 Overview 37
6.7.2 Level 1 configuration: manufacturer device definition 37
6.7.3 Level 2 configuration: network definition 37
6.7.4 Level 3 configuration: distributed application definition 37
6.7.5 Level 4 configuration: device configuration 37
7 Safety communication layer protocol 37
7.1 Safety PDU format 37
7.1.1 General 37
7.1.2 Safety communication layer CRC 38
7.1.3 Black channel time synchronization monitoring 38
7.1.4 Sequence number 38
7.1.5 Virtual header 39
7.1.6 Connection key 39
7.1.7 Redundancy and cross-check 40
7.2 Protocol extensions for use in safety-related systems 40
7.2.1 Overview 40
7.2.2 Publisher-subscriber interactions 40
7.2.3 Client-server interactions 46
7.2.4 Time synchronization 51
7.2.5 Device start-up 52
7.3 Communications entity 52

7.3.1 General 52
7.3.2 Network management 52
7.3.3 FMS 52
7.3.4 H1 stack 52
8 Safety communication layer management 53
8.1 Overview 53
8.2 SMK communications 53
8.3 FMS services 53
8.4 SMK services 53
8.4.1 General 53
8.4.2 Address assignment 53
8.4.3 Time synchronization 53
8.5 Safety communication layer configuration and start-up 53
8.5.1 H1 configuration and start-up 53
8.5.2 FSCP 1/1 FBAP 54
8.5.3 Testing 54
9 System requirements 54
9.1 Indicators and switches 54
9.2 Installation guidelines 54
9.3 Safety function response time 54
9.4 Duration of demands 55
9.5 Constraints for calculation of system characteristics 55
9.5.1 Message rate 55
9.5.2 SIL level 55
9.6 Maintenance 55
9.7 Safety manual 55
10 Certification 55
Annex A (informative) Additional information for functional safety communication profiles of CPF 1 56
A.1 Hash function calculation 56
A.2 Fault conditions arising from locations beyond the output function block 58
Bibliography 60

Table 1 – Example state transition table 19
Table 2 – Safety measures and possible communication errors 26
Table 3 – Data types used within FSCP 1/1 28
Table 4 – Fault state behaviour 31
Table 5 – Publisher states 41
Table 6 – Publisher state table - Received transitions 42
Table 7 – Publisher state table - Internal transitions 42
Table 8 – Subscriber states 44
Table 9 – Subscriber state table - Received transitions 45
Table 10 – Subscriber state table - Internal transitions 45
Table 11 – Server states during read operations 47
Table 12 – Received transitions for a FSCP 1/1 Server during read operations 48
Table 13 – States of a FSCP 1/1 server during write operations 49

Table 14 – Received transitions for a FSCP 1/1 Server during write operations 50
Table A.1 – Fault conditions arising from locations beyond the output function block 59

Figure 1 – Relationships of IEC 61784-3 with other standards (machinery) 8
Figure 2 – Relationships of IEC 61784-3 with other standards (process) 9
Figure 3 – Example state diagram 19
Figure 4 – Use of colors in figures 19
Figure 5 – Scope of FSCP 1/1 20
Figure 6 – FSCP 1/1 architecture (H1) 22
Figure 7 – Black channel 23
Figure 8 – FSCP 1/1 in system architecture 26
Figure 9 – FSCP 1/1 H1 device 27
Figure 10 – FSCP 1/1 protocol layers 27
Figure 11 – Relationship between FSCP 1/1 and the other layers of IEC 61158 Type 1 28
Figure 12 – Key write-lock 30
Figure 13 – Password write-lock 30
Figure 14 – Example of FSCP 1/1 communication 34
Figure 15 – Example of device description 36
Figure 16 – Safety PDU showing virtual content 41
Figure 17 – Safety PDU showing duplication of data and addition of CRC 41
Figure 18 – State transition diagram for a FSCP 1/1 Publisher 42
Figure 19 – Safety PDU showing duplication of data and addition of CRC 43
Figure 20 – Safety PDU showing virtual content 43
Figure 21 – State transition diagram for a FSCP 1/1 subscriber 44
Figure 22 – Safety PDU showing virtual content 46
Figure 23 – Safety PDU showing virtual content with sub index 46
Figure 24 – Safety PDU showing duplication of data, addition of sequence number and CRC 47
Figure 25 – State transition diagram for a FSCP 1/1 Server during read operations 47
Figure 26 – Safety PDU showing duplication of data and addition of sequence number and CRC 48
Figure 27 – Example of FSCP 1/1 write 49
Figure 28 – Example of FSCP 1/1 write with sub index 49
Figure 29 – State transition diagram for a FSCP 1/1 Server during write operations 50
Figure 30 – Safety PDU showing duplication of data and CRC 51
Figure 31 – Example of safety function response time components 54

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES

Part 3-1: Functional safety fieldbuses – Additional specifications for CPF 1

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 provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with an IEC Publication.
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.

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

US 6,999,824	[FF]	System and method for implementing safety instrumented systems in a fieldbus architecture

IEC takes no position concerning the evidence, validity and scope of these patent rights.

The holders of these patents rights have assured the IEC that they are willing to negotiate licences under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statement of the holders of these patent rights are registered with IEC.

Information may be obtained from:

[FF] Fieldbus Foundation

9005 Mountain Ridge Drive
Bowie Bldg. - Suite 190
Austin, TX 78759-5316
Tel: +1 512 794 8890

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.

International Standard IEC 61784-3-1 has been prepared by subcommittee 65C: Industrial networks, of IEC technical committee 65: Industrial process measurement, control and automation.

This bilingual version (2014-12) corresponds to the English version, published in 2007-12.

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

FDIS	Report on voting
65C/470/FDIS	65C/481/RVD

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

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

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

The committee has decided that the contents of this publication will remain unchanged until the maintenance result 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.

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

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.

INTRODUCTION

The IEC 61158 fieldbus standard together with its companion standards IEC 61784-1 and IEC 61784-2 defines a set of communication protocols that enable distributed control of automation applications. Fieldbus technology is now considered well accepted and well proven. Thus many fieldbus enhancements are emerging, addressing not yet standardized areas such as real time, safety-related and security-related applications.

This standard explains the relevant principles for functional safety communications with reference to IEC 61508 series and specifies several safety communication layers (profiles and corresponding protocols) based on the communication profiles and protocol layers of IEC 61784-1, IEC 61784-2 and the IEC 61158 series. It does not cover electrical safety and intrinsic safety aspects.

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

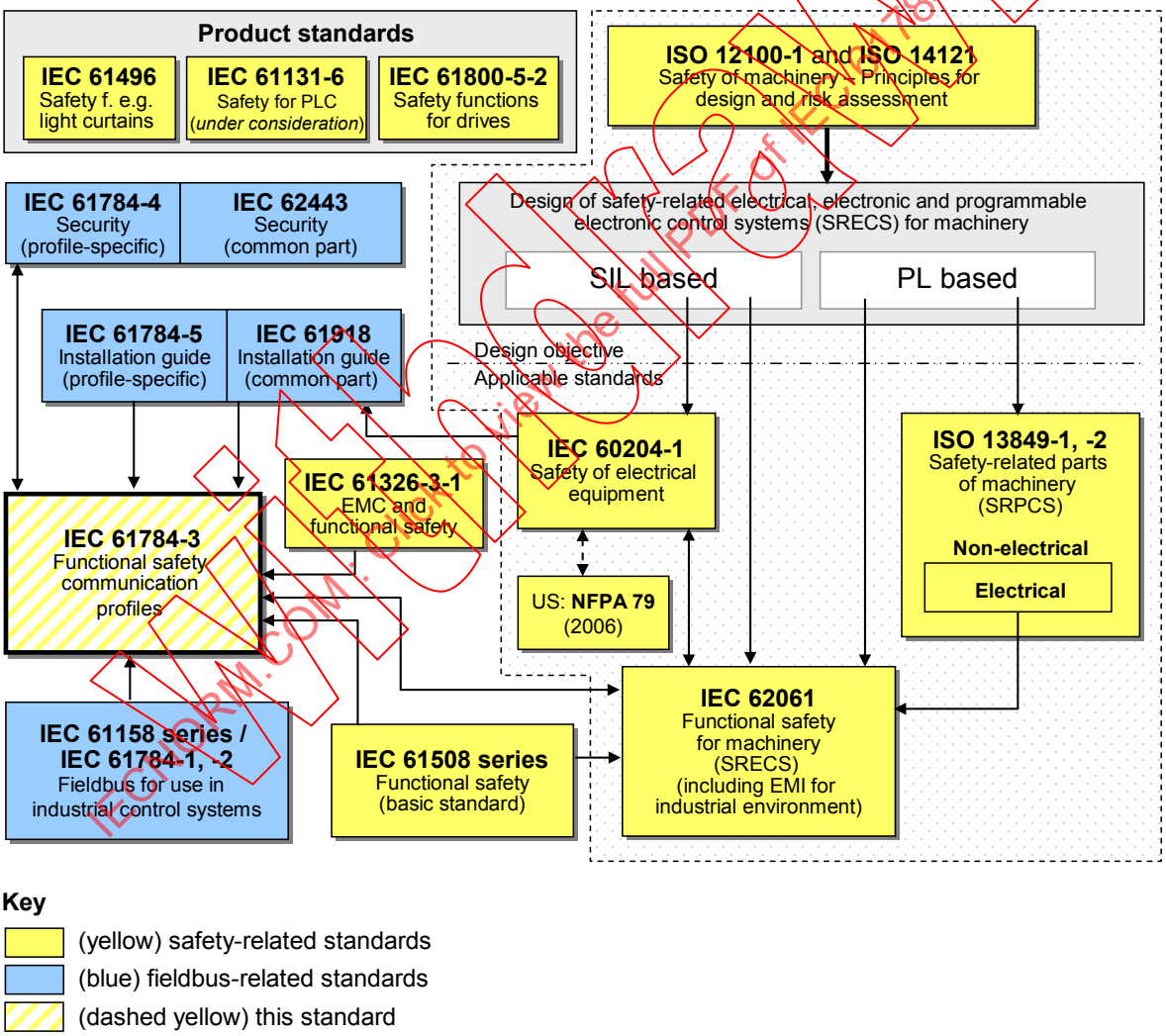
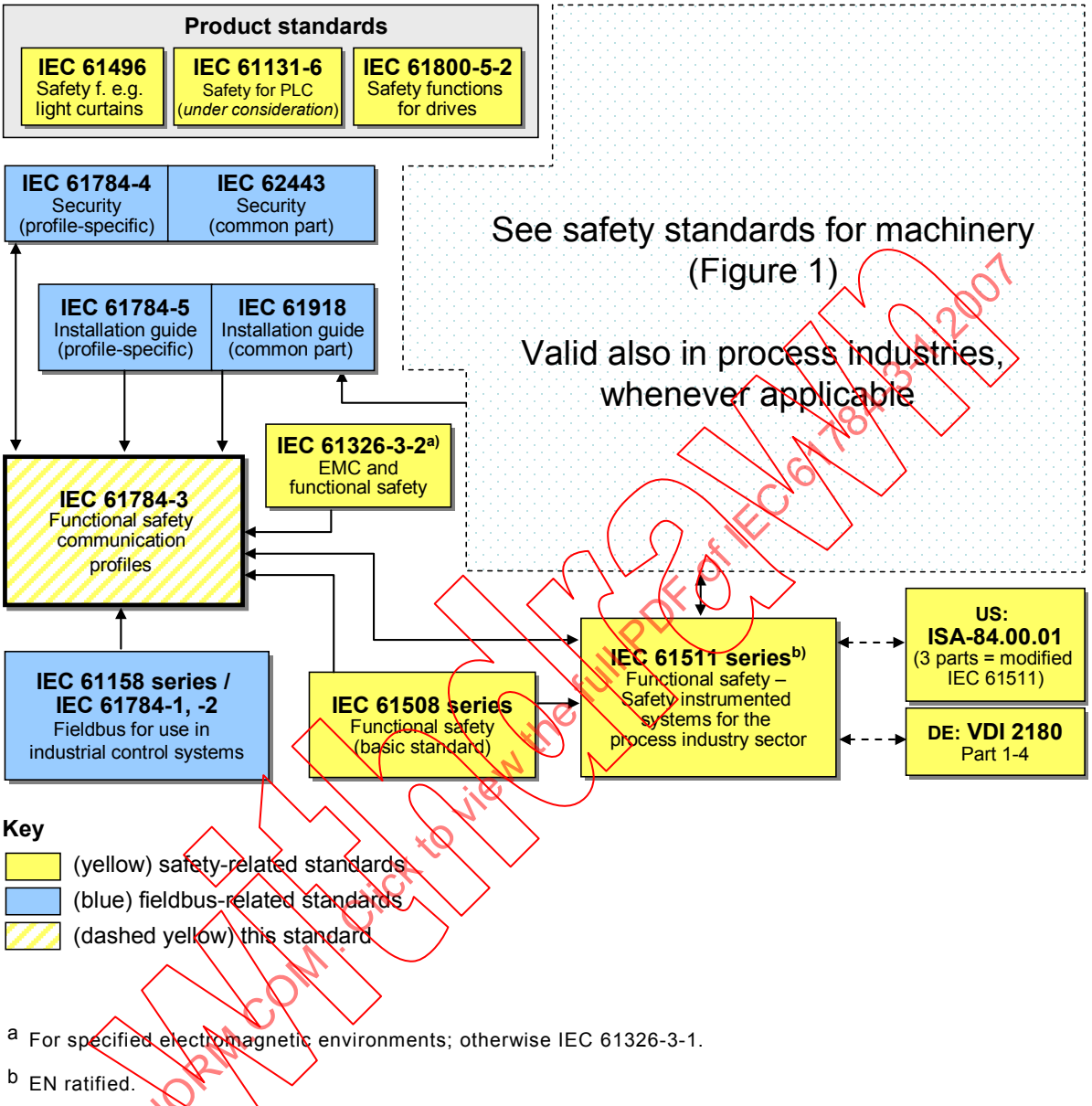


Figure 1 – Relationships of IEC 61784-3 with other standards (machinery)

Figure 2 shows the relationships between this standard and relevant safety and fieldbus standards in a process environment.



[a] For specified electromagnetic environments; otherwise IEC 61326-3-1.

[b] EN ratified.

Figure 2 – Relationships of IEC 61784-3 with other standards (process)

Safety communication layers which are implemented as parts of safety-related systems according to IEC 61508 series provide the necessary confidence in the transportation of messages (information) between two or more participants on a fieldbus in a safety-related system, or sufficient confidence of safe behaviour in the event of fieldbus errors or failures.

Safety communication layers specified in this standard do this in such a way that a fieldbus can be used for applications requiring functional safety up to the Safety Integrity Level (SIL) specified by its corresponding functional safety communication profile.

The resulting SIL claim of a system depends on the implementation of the selected functional safety communication profile within this system – implementation of a functional safety communication profile in a standard device is not sufficient to qualify it as a safety device.

This standard describes

— basic principles for implementing the requirements of IEC 61508 series for safety-related data communications, including possible transmission faults, remedial measures and considerations affecting data integrity;

— individual description of functional safety profiles for several communication profile families in IEC 61784-1 and IEC 61784-2;

— safety layer extensions to the communication service and protocols sections of the IEC 61158 series.

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES

Part 3-1: Functional safety fieldbuses – Additional specifications for CPF 1

1 Scope

This part of the IEC 61784-3 series specifies a safety communication layer (services and protocol) based on CPF 1 of IEC 61784-1 and IEC 61158 Type 1 and 9. It identifies the principles for functional safety communications defined in IEC 61784-3 that are relevant for this safety communication layer.

NOTE 1 It does not cover electrical safety and intrinsic safety aspects. Electrical safety relates to hazards such as electrical shock. Intrinsic safety relates to hazards associated with potentially explosive atmospheres.

This part[1] defines mechanisms for the transmission of safety-relevant messages among participants within a distributed network using fieldbus technology in accordance with the requirements of IEC 61508 series for functional safety. These mechanisms may be used in various industrial applications such as process control, manufacturing automation and machinery.

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

NOTE 2 The resulting SIL claim of a system depends on the implementation of the selected functional safety communication profile within this system – implementation of a functional safety communication profile according to this part in a standard device is not sufficient to qualify it as a safety device.

2 Normative references

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

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

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

IEC 61158-3-1, *Industrial communication networks – Fieldbus specifications – Part 3-1: Data-link layer service definition – Type 1 elements*

IEC 61158-4-1, *Industrial communication networks – Fieldbus specifications – Part 4-1: Data-link layer protocol specification – Type 1 elements*

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

IEC 61158-5-9, *Industrial communication networks – Fieldbus specifications – Part 5-9: Application layer service definition – Type 9 elements*

IEC 61158-6-5, *Industrial communication networks – Fieldbus specifications – Part 6-5: Application layer protocol specification – Type 5 elements*

---

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

IEC 61158-6-9, *Industrial communication networks – Fieldbus specifications – Part 6-9: Application layer protocol specification – Type 9 elements*

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

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

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

IEC 61784-3, *Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions*

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

IEC 62280-1:2002, *Railway applications – Communication, signalling and processing systems – Part 1: Safety-related communication in closed transmission systems*

3 Terms, definitions, symbols, abbreviated terms and conventions

3.1 Terms and definitions

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

3.1.1 Common terms and definitions

3.1.1.1
availability
probability for an automated system that for a given period of time there are no unsatisfactory system conditions such as loss of production

NOTE Availability depends on MTBF (mean time between failure) and MDT (mean down time): Availability = MTBF / (MTBF + MDT).

3.1.1.2
black channel
communication channel without available evidence of design or validation according to IEC 61508 series

3.1.1.3
bridge
abstract device that connects multiple network segments along the data link layer

3.1.1.4
communication channel
logical connection between two end-points within a *communication system*

3.1.1.5
communication system
arrangement of hardware, software and propagation media to allow the transfer of *messages* (ISO/IEC 7498 application layer) from one application to another

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

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

<method> procedure used to calculate the redundant data

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

NOTE 2 See also [28], [29][2].

3.1.1.8
error
discrepancy between a computed, observed or measured value or condition and the true, specified or theoretically correct value or condition

NOTE 1 An error can be caused by a faulty item, e.g. a computing error made by faulty computer equipment.

[IEV 191-05-24], [IEC 61508-4:1998], [IEC 61158]

NOTE 2 Errors may be due to design mistakes within hardware/software and/or corrupted information due to electromagnetic interference and/or other effects.

NOTE 3 Errors do not necessarily result in a *failure* or a *fault*.

3.1.1.9
failure
termination of the ability of a functional unit to perform a required function

NOTE 1 The definition in IEV 191-04-01 is the same, with additional notes.

[IEC 61508-4:1998], [ISO/IEC 2382-14.01.11]

NOTE 2 Failure may be due to an *error* (for example, problem with hardware/software design or message disruption)

3.1.1.10
fault
abnormal condition that may cause a reduction in, or loss of, the capability of a functional unit to perform a required function

NOTE IEV 191-05-01 defines “fault” as a state characterized by the inability to perform a required function, excluding the inability during preventative maintenance or other planned actions, or due to lack of external resources.

[IEC 61508-4:1998], [ISO/IEC 2382-14.01.10]

3.1.1.11
fieldbus
communication system based on serial data transfer and used in industrial automation or process control applications

3.1.1.12
frame
denigrated synonym for DLPDU

2 Figures in square brackets refer to the bibliography.

3.1.1.13
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, in order to detect data corruption

NOTE 1 An FCS can be derived using for example a CRC or other hash function.

NOTE 2 See also [28], [29].

3.1.1.14
hash function
(mathematical) function that maps values from a (possibly very) large set of values into a (usually) smaller range of values

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

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

[IEC 62210, modified]

3.1.1.15
hazard
state or set of conditions of a system that, together with other related conditions will inevitably lead to harm to persons, property or environment

3.1.1.16
master
active communication entity able to initiate and schedule communication activities by other stations which may be masters or slaves

3.1.1.17
message
ordered series of octets intended to convey information
[ISO/IEC 2382-16.02.01, modified]

3.1.1.18
message sink
part of a *communication system* in which *messages* are considered to be received
[ISO/IEC 2382-16.02.03]

3.1.1.19
message source
part of a *communication system* from which *messages* are considered to originate
[ISO/IEC 2382-16.02.02]

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

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

[IEC 61508-4 and IEC 62061, modified]

3.1.1.21
redundancy
existence of means, in addition to the means which would be sufficient for a functional unit to perform a required function or for data to represent information

EXAMPLE Duplicated functional components and the addition of parity bits are both instances of redundancy.

NOTE 1 Redundancy is used primarily to improve reliability or availability.

NOTE 2 The definition in IEV 191-15-01 is less complete.

[IEC 61508-4:1998], [ISO/IEC 2382-14.01.12]

3.1.1.22
reliability
probability that an automated system can perform a required function under given conditions for a given time interval (t1,t2)

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

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

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

NOTE 4 Reliability differs from availability.

[IEC 62059-11, modified]

3.1.1.23
risk
combination of the probability of occurrence of harm and the severity of that harm
[IEC 61508-4:1998]

3.1.1.24
safety communication layer (SCL)
communication layer that includes all the necessary measures to ensure safe transmission of data in accordance with the requirements of IEC 61508

3.1.1.25
safety data
data transmitted across a safety network using a safety protocol

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

3.1.1.26
safety device
device designed in accordance with IEC 61508 and which implements the functional safety communication profile

3.1.1.27
safety function
function to be implemented by an E/E/PE safety-related system, other technology *safety-related system* or external risk reduction facilities, which is intended to achieve or maintain a safe state for the EUC, in respect of a specific hazardous event
[IEC 61508-4:1998]

3.1.1.28
safety function response time
worst case elapsed time following an actuation of a safety sensor connected to a fieldbus, before the corresponding safe state of its safety actuator(s) is achieved in the presence of errors or failures in the safety function channel

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

3.1.1.29
safety integrity level (SIL)
discrete level (one out of a possible four) for specifying the safety integrity requirements of the *safety functions* to be allocated to the E/E/PE safety-related systems, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest

NOTE The target failure measures for the four safety integrity levels are specified in Tables 2 and 3 of IEC 61508-1.

[IEC 61508-4:1998]

3.1.1.30
safety measure
<this standard> measure to control possible communication *errors* that is designed and implemented in compliance with the requirements of IEC 61508

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

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

3.1.1.31
safety-related application
programs designed in accordance with IEC 61508 to meet the SIL requirements of the application

3.1.1.32
safety-related system
system performing *safety functions* according to IEC 61508

3.1.1.33
slave
passive communication entity able to receive messages and send them in response to another communication entity which may be a master or a slave

3.1.1.34
spurious trip
trip caused by the safety system without a process demand

3.1.1.35
time stamp
time information included in a *message*

3.1.2 CPF 1: Additional terms and definitions

3.1.2.1
client
connection entity that requests information from a server

3.1.2.2
cross-check
verification that the redundantly transmitted data are identical

3.1.2.3
H1
fieldbus standard communication data link

3.1.2.4
host
information processing unit that is able to perform the safety profile mechanisms, and services the black channel

3.1.2.5
macro cycle
single iteration of the link level schedule

3.1.2.6
masquerade
error due to mistaken identification information

3.1.2.7
publisher
message source that transmits messages on a periodic basis

3.1.2.8
queuing
sequential handling of items

3.1.2.9
server
communication entity that handles messages from a client

3.1.2.10
SIL environment
hardware and software suitable for SIS functions

3.1.2.11
subscriber
message sink that receives messages from a publisher

3.2 Symbols and abbreviated terms

3.2.1 Common symbols and abbreviated terms

CP	Communication Profile	[IEC 61784-1]
CPF	Communication Profile Family	[IEC 61784-1]
CRC	Cyclic Redundancy Check	
DLL	Data Link Layer	[ISO/IEC 7498-1]
DLPDU	Data Link Protocol Data Unit	
EMI	Electro-Magnetic Interference	
EUC	Equipment Under Control	[IEC 61508-4:1998]
FAL	Fieldbus Application Layer	[IEC 61158-5]
FCS	Frame Check Sequence	
FSCP	Functional Safety Communication Profile	
E/E/PE	Electrical/Electronic/Programmable Electronic	[IEC 61508-4:1998]
PDU	Protocol Data Unit	[ISO/IEC 7498-1]
PES	Programmable Electronic System	[IEC 61508-4:1998]
PFD	Average Probability of Failure on Demand	[IEC 61508-6:1998]
PFH	Probability of Failure per Hour	[IEC 61508-6:1998]
PhL	Physical Layer	[ISO/IEC 7498-1]

PLC	Programmable Logic Controller	
SCL	Safety Communication Layer	
SIL	Safety Integrity Level	[IEC 61508-4:1998]
SR	Safety Relevant	

3.2.2 CPF 1: Additional symbols and abbreviated terms

AP	Application Process
ASIC	Application Specific Integrated Circuit
CAS	Cascade
CF	Common File
CFF	Common File Format
DD	Device Description
DO	Digital Output
FBAP	Function Block Application Process
FMS	Fieldbus Message Specification
FIFO	First-In First-Out
FMS	Field Message Specification
LAS	Link Active Scheduler
LO	Local Override
LRSN	Last Sequence Number Received
MAU	Medium Attachment Unit
MD5	Message Digest Algorithm 5
MIB	Management Information Base
NMA	Network Management Agent
NMIB	Network Management Information Base
OD	Object Dictionary
OOS	Out Of Service
SIS	Safety Instrumented System
SMIB	System Management Information Base
SMK	System Management Kernel
SMKP	System Management Kernel Protocol
VCR	Virtual Communication Relationship

3.3 Conventions

3.3.1 State Diagrams

Figure 3 shows an example state diagram which will be used in this part. A state is indicated by an oval with the state name in the center of the oval. In Figure 3, “Not Connected”, “Connected/Good”, and “Connected/Bad” are all states. A transition is indicated by a line or curve with an arrow indicating the direction of the transition. Each transition is named with a label on the line or curve. In Figure 3, “R1”, “R2”, “R3”, and “R4” are transitions.

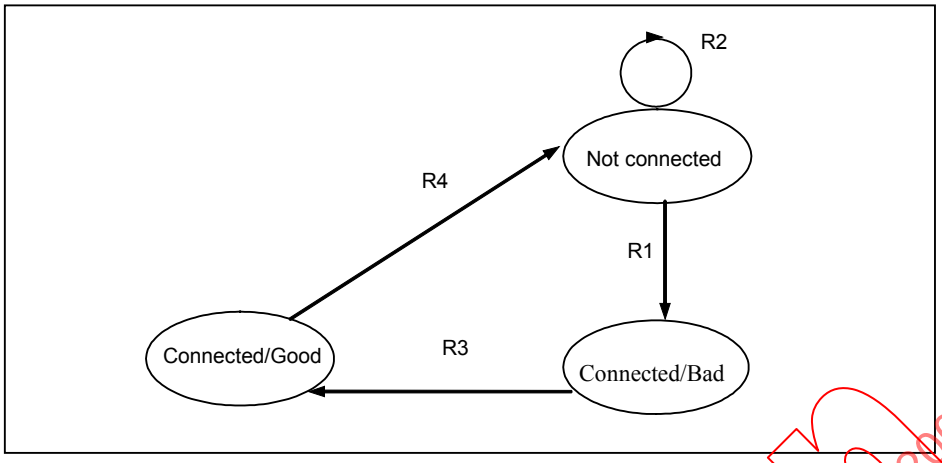


Figure 3 – Example state diagram

For each state diagram there will be a corresponding table as shown in Table 1. The first column labelled "#" contains the transition name. The second column labelled "Current state" contains the state that this transition applies to. The third column labelled "Event and condition action" contains the event, any conditions for the transition, and any actions. The actions are indented from the conditions. In Table 1, "RcvMsg() = "FMS Initiate.cnf"" is a condition where a "SET Sequence Number = MCN" is an action. The fourth column labelled "Next state" contains the new state after this transition.

Table 1 – Example state transition table

#	Current state	Event and condition action	Next state
R1	Not connected	RcvMsg() = "FMS Initiate.cnf" SET Sequence Number = MCN	Connected/ Bad
R2	Not connected	RcvMsg() = "Any message (not FMS Initiate.cnf)"	Same
R3	Connected/ Bad	RcvMsg() = "Abort.ind" OR RcvMsg() = "Abort.req"	Not connected
R4	Connected/ Good	RcvMsg() = "Abort.ind" OR RcvMsg() = "Abort.req"	Not connected

3.3.2 Use of colors in figures

The use of colors in figures is not normative and is used only for clarity of the figure. The convention for use of colors is described in Figure 4. Any colors not shown are used for clarity of the figure only.

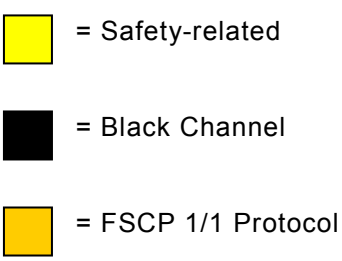


Figure 4 – Use of colors in figures

4 Overview of FSCP 1/1 (FOUNDATION Fieldbus™ SIS)

4.1 General

Communication Profile Family 1 (commonly known as FOUNDATION™ Fieldbus[3]) defines communication profiles based on IEC 61158-2 Type 1, IEC 61158-3-1, IEC 61158-4-1, IEC 61158-5-5, IEC 61158-5-9, IEC 61158-6-5, and IEC 61158-6-9.

The basic profiles CP 1/1, CP 1/2, and CP 1/3 are defined in IEC 61784-1. The CPF 1 functional safety communication profile FSCP 1/1 (FF-SIS™[3]) is based on the CP 1/1 basic profile in IEC 61784-1 and the safety communication layer specifications defined in this part.

NOTE 1 The FOUNDATION™ Fieldbus Specifications AG-180 [37], FF-807 [38], FF-884 [39], and FF-895 [40] are applicable to this protocol.

There are applications that require a safety integrity level of one through four as defined by IEC 61508 series.

NOTE 2 These safety-related applications are also called safety instrumented systems (SIS) (see IEC 61511 series).

The FSCP 1/1 safety communication layer specified in this part makes it possible to use intelligent devices in a safety-related system adding more capability to the system, yet the system can meet its safety integrity level requirements. The safety communication layer specified in this part is only applicable to CP 1/1 as described in IEC 61784-1.

This part does not define requirements for engineering tools or internal measurement functionality of devices. The safety communication layer ensures that a configuration created using an engineering tool is downloaded into the safety devices without the protocol impacting the safety integrity level. The scope of this part is defined in Figure 5.

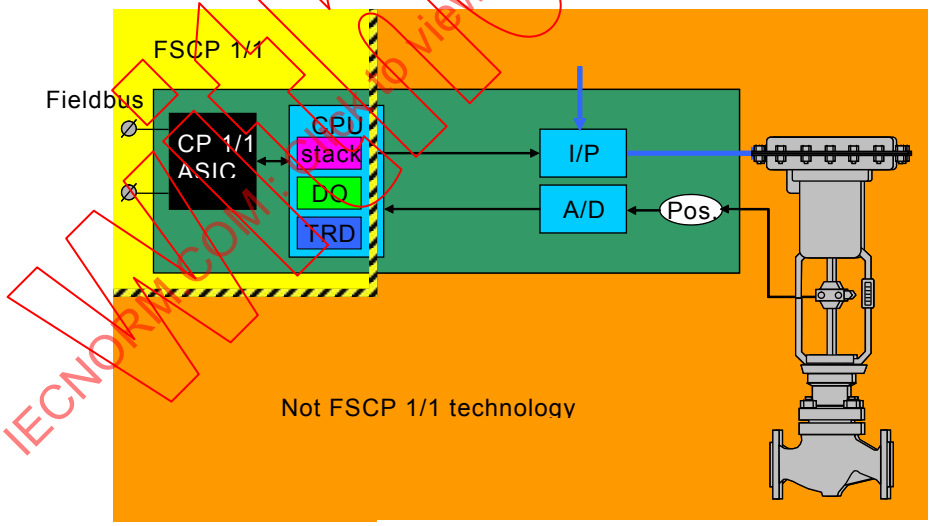


Figure 5 – Scope of FSCP 1/1

FSCP 1/1 alone does not ensure functional safety. In addition to FSCP 1/1 protocol interoperability registration, the vendor will also obtain functional safety certification for the products, systems, and software. The user shall ascertain the suitability of use of all safety-related equipment in the safety function in accordance with IEC 61508 series.

---

3 FOUNDATION™ Fieldbus and FF-SIS™ are trade names of the non-profit organization Fieldbus Foundation. This information is given for the convenience of users of this International Standard and does not constitute an endorsement by IEC of the trade name holder or any of its products. Compliance to this part of IEC 61784-3 does not require use of the trade names Foundation Fieldbus™ or FF-SIS™. Use of the trade names FOUNDATION™ Fieldbus or FF-SIS™ requires permission from the Fieldbus Foundation.

4.2 Key concepts of FSCP 1/1

4.2.1 Black channel

This is the concept of using a non-trusted communication system (for example wires, fiber optics, repeater, barrier, ASIC, communication stack, linking device, interface) to provide a reliable communication channel. The black channel includes the part in a device known as the communications entity as well as the SMK and SMKP. FSCP 1/1 diagnostics control faults in the black channel. The black channel can fail any time but communications failures are detected so as to control faults within the process safety time. The failure detection diagnostics shall comply with IEC 61508 series, the black channel needs not. The FSCP 1/1 protocol does not rely on the 16-bit CRC in the H1 data-link layer FCS.

4.2.2 Connection key

The connection key is a unique number for each connection, a source-destination relationship "codeword", which is given by the host to each safety link object at configuration time. Unlike the black channel address, the connection key is protected by the safety communication layer CRC. The connection key is unique within the safety communication layer. When devices are replaced, the same connection key may be reused and downloaded to the new device. The device configuration including the connection key is cleared in a removed device before it is connected on a FSCP 1/1 network again in another service. Devices may automatically clear their configuration when the black channel address is changed; alternatively, devices may have a reset button or equivalent to clear their configuration.

4.2.3 Cross-check

This is a comparison of the application data, sequence number, and CRC that have been redundantly transmitted (twice within the same message) to ascertain that the two copies are identical.

4.2.4 FSCP 1/1

FSCP 1/1 provides a closed transmission system suitable for use in a safety-related system. It achieves trusted communication between safety-related applications.
(Adapted from IEC 62280-1).

4.2.5 Programmable electronic system

This is a system for control, protection or monitoring based on one or more programmable electronic devices. It includes all elements of the system such as power supplies, sensors and other input devices, data highways and other communication paths, and actuators and other output devices. The structure of a PES may have the programmable electronics as a unit distinct from sensors and actuators on the EUC and their interfaces, but the programmable electronics could exist at several places in the PES.
(Adapted from IEC 61508-4:1998, 3.3.2).

4.2.6 Queuing delays

One possible fault is that messages are held up in the black channel due to queuing in the device communication stack or in intelligent network hardware including repeaters, hubs, bridges, switches, and linking devices. Unconfirmed published messages may be coming through the black channel successfully, even at an acceptable rate, but may, due to long or multiple queuing at various stages along the black channel path, be older than the process safety time allows. This fault is a type of delay fault, where the delay is introduced by devices in the black channel queuing messages.

4.2.7 Redundancy

Redundancy is the use of additional hardware, software or data above that needed in an error free environment.

EXAMPLE Duplicated functional components and the addition of parity bits are both instances of redundancy.

NOTE Redundancy is used primarily to improve reliability or availability (IEC 61508-4:1998, 3.3.10).

4.2.8 SIL environment

FSCP 1/1 compliant hardware and software components may be built into a system that is a suitable environment for implementation of safety-related applications.

4.3 Key components of FSCP 1/1

4.3.1 Overview

The fieldbus communication hardware and stack are not trusted. A safety communication layer above the communication stack ensures trustworthy communication over the fieldbus, and a safety link object in the FBAP contains the additional information required by the FSCP 1/1 protocol. These are shown in Figure 6. In a safety device the application process and safety communication layer will execute in a SIL environment. A set of simplified function blocks suitable for safety-related applications have been created.

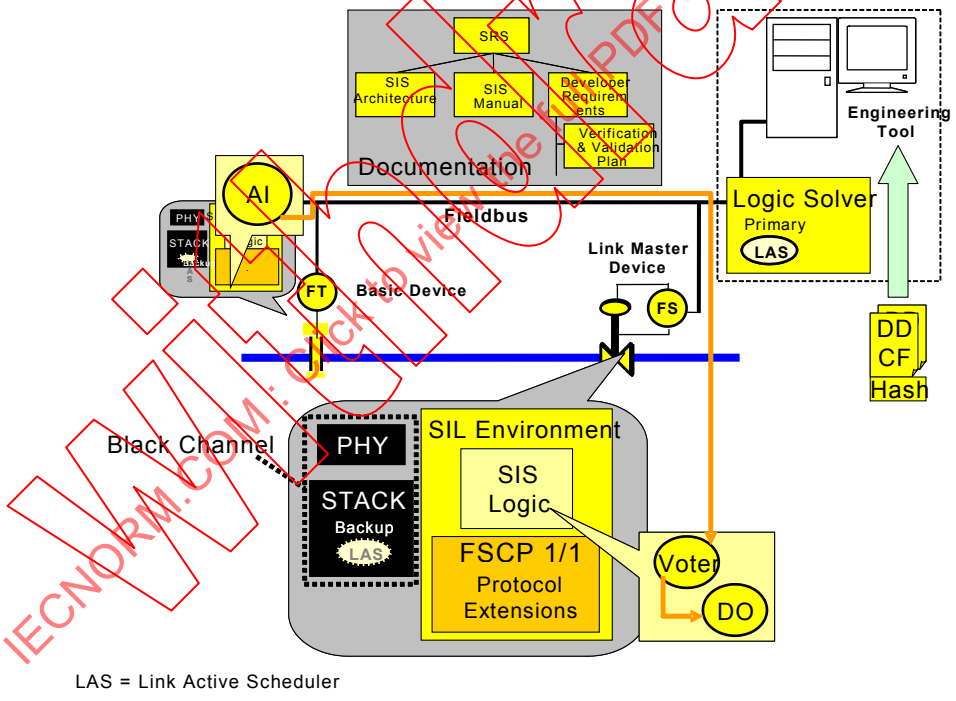


Figure 6 – FSCP 1/1 architecture (H1)

The FSCP 1/1 protocol controls failures such as device or wire malfunctions as well as sporadic disturbances such as EMI. The safety communication layer detects the following types of communication error: repetition, deletion, insertion, re-sequencing, data corruption, masquerading, and delay.

4.3.2 Black channel

The black channel concept as shown in Figure 7 permits safety data to be transmitted across a non-trusted bus. There is no need for physical separation of safety functions and non-safety hardware. Safety and non-safety devices and data can share the bus, as shown in Figure 7.

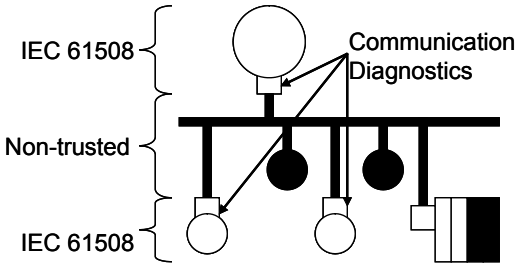


Figure 7 – Black channel

Only one LAS is permitted on an H1 network. Safety-related and non-safety-related applications can exist in the same device. FSCP 1/1 transmission is logically separated from non-FSCP 1/1 transmission. A single-channel configuration, that is a non-redundant bus, is sufficient. A safety device can provide both safety and non-safety function blocks. FSCP 1/1 protocol is used with safety function block links. Regular CP 1/1 is used with non-safety function block links. Thus a safety device can be used for safety or non-safety functions.

Failures may result from effects other than actual failures of hardware components (for example electromagnetic interference, decoding errors), however, such failures are considered to be random hardware failures.
(Adapted from IEC 61508-2, 7.4.3.2.2).

To increase availability, hot-standby bus redundancy may be used. A single channel is expected to be used between instruments and a logic-solver. Redundant channels are expected to be used for communication between logic-solvers.

4.4 Relationship to the ISO OSI basic reference model

The safety communication layer is implemented above the communication stack in the application layer.

5 General

5.1 External documents providing specifications for the profile

The following documents provide additional specifications which may be relevant for the design of FSCP 1/1:

- FOUNDATION™ Fieldbus AG-180 [37];
- FOUNDATION™ Fieldbus FF-807 [38];
- FOUNDATION™ Fieldbus FF-884 [39];
- FOUNDATION™ Fieldbus FF-895 [40].

5.2 Safety functional requirements

5.2.1 Requirements for functional safety

The following list are the functional safety requirements used in the development of the FSCP 1/1 protocol.

- FSCP 1/1 shall be designed to permit vendors to develop products suitable for use in SIL 2 (IEC 61508) applications, SIL 3 is recommended.
- The protocol shall support the publisher/subscriber and client/server connection.

- The safety related protocol shall prevent interference from non-safety related devices. For example a non-safety related handheld shall not be permitted to change parameters in a safety related device.
- The protocol shall protect against unintended or non-authorized configuration changes to a safety device.
- The contribution of the FSCP 1/1 protocol to PFD/PFH shall be less than 1 % of the value required by the SIL level.
- PFD/PFH calculations shall be based on demand mode and high demand mode (as defined in IEC 61508).
- The protocol shall implement measures to control the following faults:
  - transmission bit failure/falsifying;
  - retransmission;
  - omission;
  - insertion/expansion;
  - wrong order;
  - delay;
  - addressing failures/masquerading;
  - queuing.

  NOTE A queuing fault is a type of delay fault.
- It shall be possible to calculate the reaction time for the application.
- The function block implementation shall be in accordance with IEC 61508-3 to the required SIL.
- Devices with different SIL levels shall be possible on the same network.
- It shall be possible to by-pass the devices in a safe manner.

5.2.2 Functional constraints

The following is a list of functional constraints used in the development of FSCP 1/1.

- Using safety communication and standard communication by means of standard devices and safety devices at the same CP 1/1 bus shall be possible.
- ASICs, communication stack, repeaters, wiring hardware, power supplies, and accessories shall remain unmodified (black channel) safety functions above OSI layer 7.
- The protocol shall have the mechanisms to permit a host to detect a mismatch in the device type or device revision or DD revision or capability file revision or SIL level.

5.2.3 Device manufacturer requirements

The following list is the requirements that FSCP 1/1 places on the device vendor.

- Environmental conditions and electrical safety according to IEC 61131-2 requirements.
- The hardware shall be in accordance with IEC 61508-2 to the required SIL.
- The software shall be in accordance with IEC 61508-3 to the required SIL.
- Hardware and software certification shall be done by a competent test organization according to IEC 61508-1 to 61508-7.

5.3 Safety measures

5.3.1 Sequence number

Each safety protocol data unit has an incrementing sequence number which is the macro cycle number when the message was generated.

5.3.2 Time stamp

The sequence number included in the safety protocol data unit is also a time stamp, since it is the macro cycle number.

5.3.3 Time expectation

The sequence number/time stamp is used to verify that messages are delivered in a timely manner. There is also a stale counter for each connection that detects when messages have not been received within the expected time frame.

5.3.4 Connection authentication

There is a connection key associated with each connection that is used to verify that a safety protocol data unit is from the correct message source.

5.3.5 Data integrity assurance

Each safety protocol data unit has a CRC to insure data integrity.

5.3.6 Redundancy with cross checking

Each safety protocol data unit contains two copies of the data and CRC. The duplication of the data and CRC is used to cross check the data.

5.3.7 Different data integrity assurance systems

The safety protocol data unit has additional CRCs that are different from the black channel data integrity system.

5.3.8 Relationships between errors and safety measures

The safety measures outlined in 5.3.1 to 5.3.7 can be related to the set of possible errors. This relationship is shown in Table 2. Each safety measure can provide protection against one or more errors in transmission. It shall be demonstrated that there is at least one corresponding safety measure or combination of safety measures for the defined possible errors in accordance with Table 2.

Table 2 – Safety measures and possible communication errors

Communication errors	Safety measures							
	Sequence number	Time stamp	Time expectation	Connection authentication	Feedback message	Data integrity assurance	Redundancy with cross checking	Different data integrity assurance systems
Corruption						X	X	
Unintended repetition	X	X						
Incorrect sequence	X	X						
Loss	X							
Unacceptable Delay		X	X					
Insertion	X							
Masquerade								X
Addressing				X				
NOTE Table adapted from IEC 61784-3.								

5.4 Safety communication layer structure

5.4.1 Network topology and device connectivity

5.4.1.1 General

Safety and non-safety devices can share the same fieldbus, as shown in Figure 8. The entire safety function from sensor to actuator shall be taken into account. The fieldbus link is designed to consume no more than 1 % of the PFD budget.

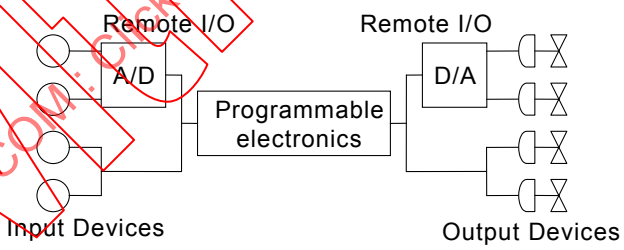


Figure 8 – FSCP 1/1 in system architecture

NOTE The programmable electronics are shown centrally located but could exist at several places in the PES.

5.4.1.2 Single H1 link topology

A safety function consists of a single H1 link. The link is part of the black channel. Safety devices and non-safety H1 devices are networked identically.

5.4.2 Device architecture

5.4.2.1 General

The black channel concept permits the communication hardware (including ASIC and MAU) and communication software stack to be non-trusted while the FSCP 1/1 protocol communications diagnostics and function block application executes in a SIL environment

consisting of SIL hardware and software. The safety communication layer is the interface between the SIL application process and the non-trusted black channel communication entity, as shown in Figure 9.

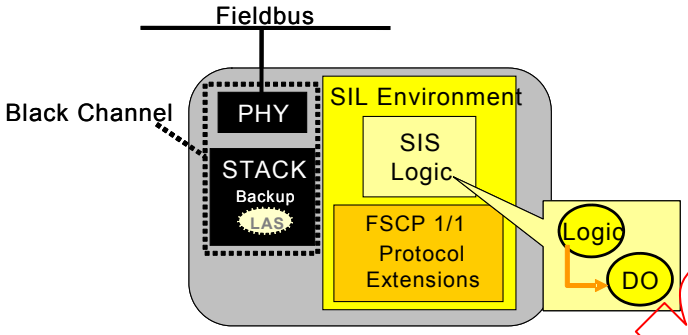


Figure 9 – FSCP 1/1 H1 device

Care needs to be taken when implementing the black channel concept to ensure that non-SIL hardware and software does not interfere with the SIL hardware and software.

5.4.2.2 H1 device architecture

Application processes are safety related and will be executed in a SIL environment. The communications entity consists of the communication stack, FMS, NMA, and NMIB which are non-trusted. The communications entity, as well as SMK and SMKP, are part of the black channel. Their relationship is shown in Figure 10.

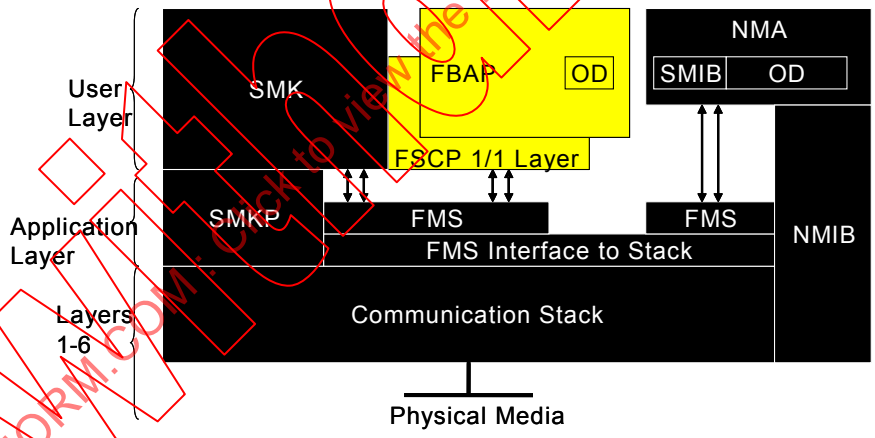


Figure 10 – FSCP 1/1 protocol layers

5.5 Relationships with FAL (and DLL, PhL)

5.5.1 General

Figure 11 shows the relationship between FSCP 1/1 and the other layers of IEC 61158 Type 1.

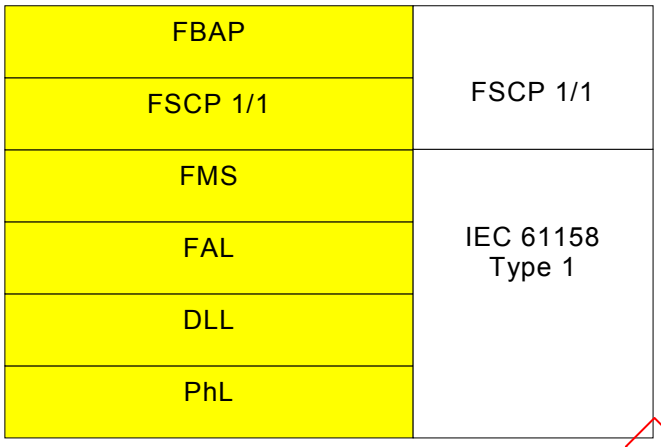


Figure 11 – Relationship between FSCP 1/1 and the other layers of IEC 61158 Type 1

5.5.2 Data Types

FSCP 1/1 uses the basic data types listed in Table 3 according to CPF 1 in IEC 61784-1.

Table 3 – Data types used within FSCP 1/1

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

6 Safety communication layer services

6.1 Application Process (AP)

6.1.1 Overview

Safety and non-safety functions can be allocated in the same or different application processes in a device. The AP for safety functions requires a SIL environment and is not part of the black channel.

The FSCP 1/1 layer is independent of the application process and therefore can be used with the function block application process or another kind of application process.

6.1.2 Network visible objects

The application process accesses the application layer in the black channel communication stack, not directly, but through the FSCP 1/1 layer.

6.1.3 Application layer interface

The same set of messaging services provided by FMS for non-safety objects is provided by the safety communication layer for the safety objects.

6.1.4 Object dictionary

There is no change to the fieldbus Object dictionary to support the black channel.

6.1.5 Application program directory

There is no change the Application Process directory to support the black channel.

6.2 Function block application processes

6.2.1 General

Simple function blocks have been defined and are suitable for safety-related applications. A FBAP containing safety objects will execute in a SIL environment.

The use of function blocks is optional. A host will probably not implement function blocks.

6.2.2 Function block model

6.2.2.1 Stale count

The end-to-end stale count check, which is based on sequence number mismatch, controls faults in scheduling and execution of the logic chain up to the output function block. A stale data timer after the output function block controls faults in scheduling and execution of the output function block itself. If update from the output function block is not received within the set time limit due to a scheduling or execution error, the output will go to the fault state. The use of a stale data timer after the output function block is a safety measure independent of the non-SIL SMK that checks that the function blocks are executing. If a function block is not executing, the outputs are not propagated to the black channel. The missing publication is a fault controlled downstream, the sequence number mismatch will cause a preconfigured fault state action. The sequence number for the link used in the FSCP 1/1 protocol is computed from the macro cycle number based on data link time and therefore changes for every new PDU delivered to the black channel. If the black channel misbehaves and is publishing old data, the sequence number will not match making it possible to detect such faults downstream.

The end-to-end stale-count mechanism detects faults such as: function block stopping executing, executing in the wrong order, at the wrong time, or with too much jitter. These faults may be due to faults in scheduling, in the function block itself, or longer than the worst expected function block execution time.

6.2.2.2 Simulation

To enable simulation, the write-lock in the resource block and simulation protection will be off. If the write-lock is turned back on, simulation is automatically disabled. In addition, simulation

enable is required to be in non-volatile memory. When power is turned on simulation is always disabled.

A non-safety function alarm is issued when simulation is enabled. The host needs to check periodically to determine if simulation is enabled in any of the devices.

6.2.2.3 Write-lock

A write-lock protects the device configuration. When the write-lock in the safety device resource block is set, all writes to the resource are disabled, including the MIB but excluding the write-lock itself. Protected contents of the MIB include object (blocks, links, VCRs), address, parameters and device tag.

A safety lock function block in every safety device is able to write to the write-lock parameter in the resource block of the same device. The safety lock function block has a write-lock input which accepts a safety function block link. This permits writes to several devices to be enabled or disabled remotely from a central location. The safety lock function block can activate and deactivate the write-lock in the device using key switch though a DI function block. Figure 12 shows the architecture of this lock.

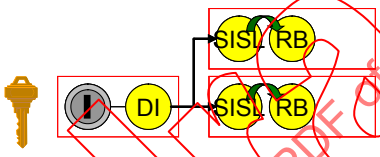


Figure 12 – Key write-lock

Write-lock can also be activated and deactivated by writing a parameter in the safety lock function block. Writing this parameter is usually protected by appropriate passwords in the host. Figure 13 shows the architecture of this lock.

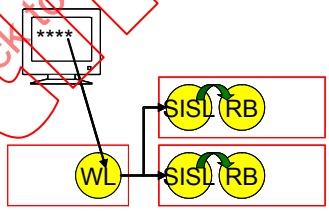


Figure 13 – Password write-lock

6.2.2.4 Trip and reset

For the FSCP 1/1 output function block the fault state can be configured de-energized-to-trip, energized-to-trip, or hold last value. If the cascade input of an output function block has a Bad status, for example due to lost communication, this is also reflected as a Bad::non-specific substatus on the feedback output of the output function block. The physical output may trigger on a genuine process demand from the logic solver logic, communication or upstream function block execution error, through operator intervention, or on device fault.

There is a distinction between preconfigured fault state action in response to process demand, communication or upstream function block execution error and trip due to device and power fault. On a process demand the output function block acts on its input signal where zero (0) always means preconfigured fault state action, and one (1) always means OK to run. For energize-to-trip the signal is inverted in the output function block. On a communication error the output function block does not take action until fault-state time has elapsed, and then it either holds its last position or goes to the fault value as set by the fault-state option and fault-state value.

In normal operation the output function block is in cascade mode. By default the mode will remain in cascade on a process demand. Optionally for process demand and for communication error, the output can be latched in its fault state. When the latch fault state option is enabled and a process demand or communication error occurs, the DO function block goes to local-override (LO) mode. Even if the demand or fault condition is cleared, the output remains in its fault state until reset by the user. A logic solver can monitor the output from the feedback output of the output function block and optionally alarm on Bad status. If latched, operator will unlatch it, either through resource block fault state clear or through the reset input of the output function block. If a device is configured for a de-energized fault state this may through the hardware result in, for example, a valve opening or closing. Table 4 lists this behaviour.

If the input status is Bad or Good::Initiate-fault-state the output will also take preconfigured fault state action.

Table 4 – Fault state behaviour

Condition	Example	DO Fault State Delay	DO Fault State Option	DO Fault State Latch	Remark
Bad status, communication or upstream function block execution error	Cascade input bad due to safety communication layer CRC failure, sequence number mismatch or redundancy cross-check mis-comparison	Yes	Energized		
De-energized					
Hold	Optional LO mode				
Initiate fault-state	Substatus received from another function block or logic solver	Yes	Energized		
De-energized					
Hold	Optional LO mode				
Operator intervention	Set fault-state from resource block	No	Energized		
De-energized					
Hold	Always LO mode				
Process demand from logic solver	Discrete cascade input is zero (0)	No	No	Optional LO mode	Usually CAS mode
Black channel failure	Time synchronization error	Yes	Energized		
De-energized					
Hold	Optional LO mode				

Provided the condition that caused the preconfigured fault state action has cleared, the user can reset the latched output by using the clear fault state parameter in the resource block or a clear fault state input in the output function block itself.

6.2.3 Application process

6.2.3.1 General

Standard FSCP 1/1 function blocks have been defined. Manufacturers can create enhanced and custom safety function blocks. All FSCP 1/1 blocks are identified by profile numbers within a specified range. This permits the host to interact with FSCP 1/1 blocks as required.

6.2.3.2 Block types

6.2.3.2.1 General

Additional standard function blocks and resource block have been created for FSCP 1/1. The standard FSCP 1/1 function blocks are identified by profile numbers within a specified range. The FSCP 1/1 function blocks have fewer permitted mode and parameter options than their regular counterparts. The manual mode is only allowed while the device is not write-locked, the same applies to the automatic mode for output function blocks. When the device writes are unlocked, the function block modes will go to the operational automatic and cascade modes respectively.

Fault state behaviour in safety output function blocks is mandatory.

6.2.3.2.2 Safety device resource block

The resource block write-lock parameter has the important function of a lockout mechanism that prevents writing to the entire resource.

The current safety communication layer statistics can be accessed through the safety device resource block. FSCP 1/1 protocol statistics consist of a counter of the number bad safety communication layer CRC faults detected.

The safety communication layer statistics also contain a black channel error parameter with a flag indicating that a time synchronization fault occurred.

The safety device resource block contains a parameter to unlock write protection of the device. This will be done before parameters and other objects can be written. The safety lock function block simplifies the locking and unlocking of writes in multiple devices.

The safety device resource block contains a parameter to clear all tripped outputs that have been latched in fault state output.

The safety device resource block contains a macro cycle duration parameter since the data in the black channel cannot be relied on.

The safety device resource block contains parameters informing the hardware revision and firmware revision as well as checksums for the firmware and the configuration.

6.2.3.2.3 Additional function blocks

6.2.3.2.3.1 General

Safety applications require inputs, outputs, and logic. Therefore a new set of safety function blocks providing these capabilities is provided. The new safety function blocks include:

- safety analog input;
- safety discrete input;
- safety lock;

- safety discrete output;
- safety logic;
- safety analog comparator.

The SR-AI, SR-DI, and SR-DO function blocks have reduced functionality as compared to their regular counterparts so as to simplify certification for implementers and reduce mistakes and make verification easier for users. Simplification includes fewer supported modes and no alarms.

6.2.3.2.3.2 Safety output function blocks

The safety output function blocks are important because these are where the preconfigured fault state action is taken. Apart from preconfigured fault state action on the process demand value received on the cascade input, the output function block will also take preconfigured fault state action on bad status, initiate fault state, upstream function block execution error, and stale communication. The output transducer will trip on the failure of its associated output function block in the safety function to execute. The output transducer controls scheduling and communication faults for the safety function by tripping if it has not been updated with fresh data within the stale data timer setting. When the output function block takes preconfigured fault state action due to a genuine process demand status, or communication fault, the mode will by default remain in cascade. Safety output function blocks include optional functionality to latch tripped outputs. A feedback output on the output function block shows Bad::non-specific status if the cascade input has bad communication. Other faults in the output will also be reflected by the status. Optionally a non-safety alert may be sent on fault state if the device supports it. The feedback status and alarm details will indicate if the fault state is a genuine process demand or due to a fault. From the mode parameter in the output function block it is possible to see if the output is in a fault state condition using FSCP 1/1 communication. An individual latched output can be cleared using a reset input parameter in each output function block. The reset input accepts a safety function block link thus permitting the fault state to be reset remotely and through logic from another function block. All tripped outputs can be cleared using a parameter contained in the resource block.

Advanced valve diagnostics such as partial stroke testing, analog position feedback on discrete valves, and position deviation alarms, are expected to be implemented in transducer blocks by vendor specific means. Future transducer block profile teams may define standard parameters for these devices.

6.2.3.2.3.3 Safety lock function block

The safety lock function block unlocks write-protection based on link inputs enabling central locking and unlocking of several devices.

Before parameters can be written the resource will be unlocked. This is equivalent to a lockout key on a safety system console. Because there may be many safety devices, and they are often inconveniently mounted in hazardous areas and otherwise inaccessible, unlocking and lockdown will be possible through FSCP 1/1 communication. Soft write-lock is mandatory in the safety resource block.

6.2.3.2.4 Safety link object

The FSCP 1/1 protocol extensions are reflected in the safety link object. A different link object storing additional information is used for FSCP 1/1 function block links. The safety link object contains the connection key and end-to-end stale count limit required for safety applications. Multiple independent safety function chains can exist on the same network or in same device or logic-solver, a failure in one safety function chain shall not require a shutdown in the other safety function chains on the same bus or in the same devices or logic solver. To ensure interoperability with existing equipment in non-safety-related applications it is mandatory that a device also supports the non-safety link object.

6.2.3.2.5 Stale data timer

The end-to-end stale count mechanism catches function block execution errors up to, but excluding, the output function block. A second mechanism, the Stale Data Timer trips the output if the output transducer block does not get updated by the output function block in a timely manner, such as due to output function block execution failure. The output stale data time is configured through the output function block. The stale data time shall not be confused with the fault-state time.

Similarly a manufacturer specific mechanism monitors execution of other blocks, including transducer blocks.

EXAMPLE If the input transducer block is not executed properly then the input function block output status is bad.

6.3 Device to device communications

6.3.1 General

FSCP 1/1 communication is supported for publisher/subscriber and client/server communications but not for report distribution. A safety device can still use the report distribution VCR to transmit alerts, but the mechanism cannot be trusted. Figure 14 illustrates this communication.

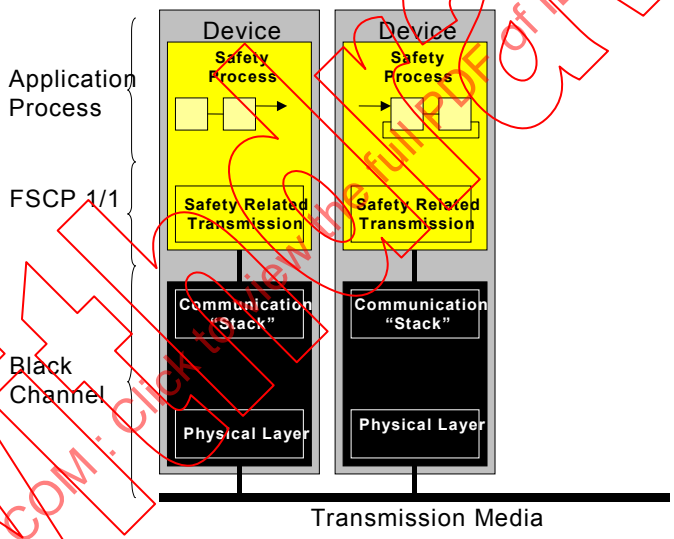


Figure 14 – Example of FSCP 1/1 communication

6.3.2 Client/server

Client/server read and write is supported in a safety device. Client/server is used by the user to write parameters. After changes are made, a functional test should be done by the user as defined in IEC 61508 series.

The client/server VCR is not deterministic and not truly timed. Client/server VCRs are not suitable for the shutdown path.

Parameters and objects can be written, but FSCP 1/1 communications is first required to enable writes. A write-lock exists in the resource block that protects all the objects in the resource. After a configuration change the user is required to perform a proof test. FSCP 1/1 communications is then used to disable the further writing.

Read-requests and write-responses use the regular CP 1/1 protocol. Write-requests and read-responses use the FSCP 1/1 protocol. A client/server link object (with connection key etc.)

shall be created for each client (interface) that will be permitted to read/write a device. Every message will have a CRC. The connection key is included as part of the virtual header, which is used in the calculation of the CRC.

FSCP 1/1 function blocks have FSCP 1/1 links configured in safety link objects. The FSCP 1/1 protocol is an extension of the PDU, not a new data type.

FSCP 1/1 uses redundant transmission, meaning that data, sequence number, and CRC are transmitted twice and cross-checked at the receiving end.

6.3.3 Publisher/subscriber

FSCP 1/1 function blocks have FSCP 1/1 links configured in safety link objects. The FSCP 1/1 protocol is an extension of the PDU, not a new data type. In addition to the safety communication layer CRC, the published safety PDU also includes a sequence number that permits the subscribers control of additional faults.

FSCP 1/1 uses redundant transmission, meaning that data, sequence number, and CRC are transmitted twice and cross-checked at the receiving end.

6.3.4 Report distribution

There is no FSCP 1/1 protocol extension for the report distribution VCR and therefore it is not trusted. A safety device can send non-safety alerts.

6.3.5 FBAP operation in a linking device

An application process in a linking device is accessed in the same way as a FSCP 1/1 FBAP.

6.3.6 System management kernel protocol (SMKP) communications

SMKP is part of the black channel. Faults in the local interface between the SMKP and the application process are controlled by manufacturer specific means.

6.4 Profiles

6.4.1 General

A profile is a subset, a selection, chosen from a larger general specification. An FSCP 1/1 profile is thus a restricted version of the full FSCP 1/1 functionality. New profiles are created for FSCP 1/1.

6.4.2 FSCP 1/1 profile

6.4.2.1 General

FSCP 1/1 H1 devices can also be categorized into classes based on their capabilities. FSCP 1/1 H1 devices belong to one or more of the following sets of classes:

- H1 FSCP 1/1 Field devices - control devices that reside on H1 links;
- FSCP 1/1 Host devices - perform user interface and configuration functions - a logic solver with configuration tool.

6.4.2.2 Block parameterization

All parameters in safety blocks can be written either using non-FSCP 1/1 client/server VCR, before the FSCP 1/1 client/server link object has been created, or FSCP 1/1 client/server VCR once the FSCP 1/1 client/server link object has been created. FSCP 1/1 requires the resource

block to be "unlocked" before anything in the resource can be written. After changes are made a functional test should be done.

6.4.2.3 Block parameterization lockout

Before parameters can be written the resource needs to be unlocked. This is equivalent to a lockout key on a safety-related system console. Because there may be many safety devices, and they are often mounted in hazardous areas or otherwise inaccessible, unlocking and locking will also be possible through FSCP 1/1 communication. Soft write-lock is mandatory in the safety resource block.

One of many conceivable implementations of this is a function block which, when an input is activated, writes the write-lock parameter in the device in order to enable configuration. A function block is provided for this purpose.

6.4.2.4 User authentication

The host software has to ensure that only authorized users are given access to programming and parameterization.

6.4.2.5 Programming lockout

Before objects can be changed the resource needs to be unlocked. This is equivalent to a lockout key on a safety-related system console. Because there may be many safety devices, and they are often mounted in hazardous areas and otherwise inaccessible, unlocking and locking will be possible through FSCP 1/1 communication. The programming lockout is based on the resource write-lock parameter in the resource block. Objects other than blocks, such as link objects, can only be written when the resource is unlocked.

Program changes should be done with the process shutdown (the devices will still be executing blocks) where the host communicates with the devices.

6.5 Device descriptions

Device descriptions are an integral part of the configuration tool. An MD5 hash will be generated for each of the DD and capabilities files to ensure the integrity of the file. The MD5 hash for the DD/CF files will be stored under a special keyword in the FSCP 1/1 capabilities file. This is shown in Figure 15.

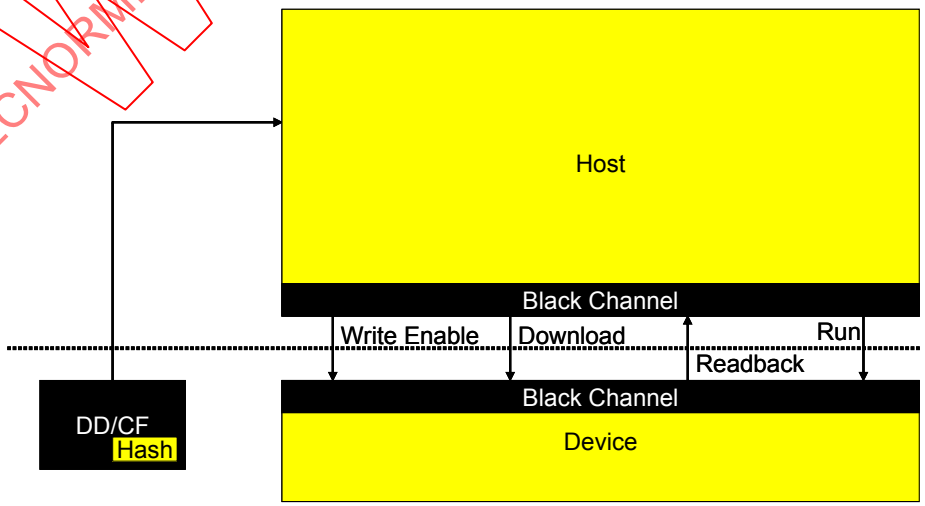


Figure 15 – Example of device description

6.6 Common file formats

Capabilities files are an integral part of the configuration tool. The hash mechanism is described for DD and is the same for CF.

The digest of the MD5 hash over the DD and CFF files is stored in the end of the CFF file.

The capabilities file contains parameters that inform the failure rates of the device. There are also parameters for product design level, that is, the fault avoidance gained (for example during the design process requirements for a SIL 2 device may have been followed, even though failure rates are good for SIL 3).

6.7 Configuration information

6.7.1 Overview

FSCP 1/1 configuration will be largely the same as non-safety configuration but with the addition of writing safety function block parameters such as the Stale Data Timer, end-to-end stale count limit, and macro cycle. FSCP 1/1 function block links use the safety link object where the connection key needs to be set. It is expected that the configuration tool will automatically manage the configuration of the connection key and macro cycle. Once a device is operational, changes to any function blocks are not permitted.

6.7.2 Level 1 configuration: manufacturer device definition

Implementation issues for safety devices include measures for physical or logical separation of safety (application process and safety communication layer) and non-trusted (black channel stack) functions in order to ensure of non-interference. Function block applications for safety-related and non-safety-related applications may reside in same or different VFDs.

6.7.3 Level 2 configuration: network definition

Configuration of the black channel is unchanged.

6.7.4 Level 3 configuration: distributed application definition

A special link object is used for safety function blocks. The expected propagation time for the channel shall be calculated.

The user defines the process safety time. The macro cycle, end-to-end stale count limits and stale data timer needs to be configured accordingly.

6.7.5 Level 4 configuration: device configuration

The macro cycle time shall be set using the parameter in the resource block.

7 Safety communication layer protocol

7.1 Safety PDU format

7.1.1 General

The FSCP 1/1 protocol controls failures during communication. The FSCP 1/1 protocol is applied to the FMS communications protocol. Faults in the local interface between the application process and the SMK as well as the SMIB in the NMA are controlled by manufacturer specific means. The FSCP 1/1 protocol is applied to FMS communications across the fieldbus.

7.1.2 Safety communication layer CRC

Cyclic redundancy check is used to control data corruption failures in fieldbus communication. Data is transmitted together with a calculated CRC checksum for each safety PDU. The safety communication layer CRC is defined by CCITT 32 V.42 and ISO/IEC 8802-3 (IEEE 802.3). It is a 32 bit polynomial calculated as follows:

$(x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1)$.

The receiver safety communication layer re-calculates the checksum of the received data and compares the result with the received checksum. Corrupted messages are rejected.

7.1.3 Black channel time synchronization monitoring

The sequence number is based on the macro cycle number derived from the data link time for each publication. The sequence number is in effect a sort of timestamp. All devices on the H1 network have a common sense of macro cycle. Devices on an H1 network thus rely on a common sense of time based on a correctly working time synchronization mechanism. Synchronized time is required to ensure synchronous execution of function blocks and communications thus ensuring the shortest safety function response time possible. The time synchronization mechanism corrects the data link time and frequency and resides in the black channel but it is monitored by the safety communication layer. The safety communication layer has an independent safety time source and detects loss of time synchronization in the black channel by comparing the frequency of FSCP 1/1 clock with the frequency of black channel clock at clock synchronization. If deviation is more than a permitted value, a preconfigured fault state action is triggered by setting function block inputs and outputs to bad status. The resource block has a black channel error parameter with time synchronization error flag.

Time distribution from the time master (LAS) to the other devices could be affected by communication queuing delays, just like other link publications. The local black channel includes a function that measures the roundtrip delay through the black channel to compensate for queuing delays. This is done periodically including start-up and LAS change. This is not a safety function. This is a function to avoid spurious trips thus ensuring better availability.

The black channel time synchronization monitor controls faults such as:

- LAS time fast, slow or jump;
- queuing fault (publisher/subscriber or time distribution);
- device restart;
- safety function restart;
- LAS switch over;
- LAS restart;
- schedule corruption (LAS or field device);
- initial start-up (configuration) (same as safety function restart);
- communication (lost time distribution, compel data, or publishing).

7.1.4 Sequence number

For publisher/subscriber VCRs the sequence number for each publication is based on macro cycle number which is computed by the safety communication layer from the data link time at the beginning of each macro cycle. The black channel time synchronization monitoring function in the safety communication layer ensures the data link time is good. The publisher/subscriber sequence number is in effect a timestamp. All devices on the H1 network have a common sense of macro cycle. There can be no sub-schedules, that is, function

blocks can only be executed once per macro cycle. The result is that during normal operation the sequence number increments by one for each new link publication. The sequence number is included with the message and compared against an expected sequence number in the safety communication layer at the receiving end. If a maximum permitted difference is exceeded it will provide a bad status to the input of the function block so that the application process knows that the data is stale.

If the overall response time from sensor to actuator is compromised due to communication errors, function block execution, scheduling faults or any other reason the output will take the preconfigured fault state action. When there is a chain of linked function blocks making up a safety function it would be possible for several individual link stale counts to add up to a long response time before detection. Rather than a stale count per link as used for non-FSCP 1/1 communications, the stale counts are diagnosed end-to-end. This is effectively a propagation delay measurement. The maximum response time from sensor to actuator permitted by the application (expressed in macro cycle units) shall be configured in the end-to-end stale count limit of the link object. If the end-to-end stale count limit is exceeded the safety communication layer sets the input status to the function block to BAD. Because the safety communication layer derives the sequence number from the macro cycle number only when function block outputs have been updated, and each individual function block only updates its output if input conditions are right (the subsequent publication thus triggering the generation of the sequence number), stale counts are propagated downstream and added up. That is, when all links are working and all function blocks execute as they should, the sequence number (based on macro cycle number at sensor) propagated from end to end matches the macro cycle (expected sequence number) in the valve. When compared to the macro cycle in the output device, it indicates the total missed communications and executions in the chain of function blocks making up the safety function. This results in a much shorter worst case response time. The criteria to refresh with a new output or not is function block specific. A new sequence number is only generated by the safety communication layer as the message is published. Certain function blocks may require all used inputs to be current while other function blocks may have voting capability that only requires a certain number of the used inputs to be current.

The FSCP 1/1 layer requires one sequence number counter for each client/server VCR. The client/server sequence number is incremented by one for each new transaction. For a client-server VCR if the sequence number is out of synch then the connection is aborted. The sequence numbers are reset when a new connection is established.

7.1.5 Virtual header

The protocol header, such as address, in the black channel frame is not protected by the safety communication layer CRC and therefore cannot be relied upon in safety-related applications. There is therefore a need to use a different mechanism to uniquely identify the source-destination relationship within the FSCP 1/1 message, but protected by the safety communication layer CRC. The connection key is used for this purpose. Sending the connection key in every message, however, would create overhead. To reduce the overhead, the safety communication layer CRC is calculated on the safety data and a virtual header including the connection key and object index. The connection key is not transmitted on the bus but the safety communication layer CRC in the recipient will fail if the connection key is wrong. The safety link object contains the connection key making it possible to compute the CRC.

7.1.6 Connection key

The protocol contains a mechanism to uniquely identify FSCP 1/1 messages so one FSCP 1/1 message is not masquerading as another FSCP 1/1 message: FSCP 1/1 function block links will be identified by a unique 32-bit connection key. The connection key will be administered by the host and written in the safety link objects. The connection key is part of the virtual header embedded in the safety communication layer CRC, but is not communicated. Any mismatch in the connection key is not explicitly checked in the subscriber or server, but a

mismatch will cause a safety communication layer CRC error. That is, a safety communication layer CRC error could indicate data corruption or a connection key mismatch.

7.1.7 Redundancy and cross-check

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

One possible implementation is that in a device containing two redundant microcontrollers, each controller builds its transmission message completely independently. The two independent data messages are added together by the black channel interface and transmitted together as a single frame. Conversely, when receiving the two independent data messages in the frame from the black channel are unpacked to its respective microcontroller, which then perform the cross-check.

7.2 Protocol extensions for use in safety-related systems

7.2.1 Overview

In order to use fieldbus devices in a safety-related system, it is necessary to extend the fieldbus protocol to ensure that the process can be taken to a safe state when failures occur. FMS and all other communication layers, including the SMK are treated as a black channel. Hence, all the protocol extensions are implemented in the User Layer or Function Block Application Process.

No new data types are specified, other than the safety link object. The data that is communicated using FMS will include the protocol extensions. The extensions are specific to the type of interaction.

NOTE The CRC 32 is described in 7.1.2.

7.2.2 Publisher-subscriber interactions

7.2.2.1 General

There is only one macro cycle for the whole H1 segment. All devices in an H1 segment, including the LAS shall be configured with the same macro cycle count. A function block in a device shall be scheduled to execute only once during the macro cycle.

At the beginning of execution of a function block, the current macro cycle number (MCN) shall be calculated as follows:

MCN = DL - Time DIV macro cycle duration

MCN shall be a 16-bit unsigned integer.

NOTE If a device has multiple function blocks, if feasible, the MCN may be calculated at the beginning of the macro cycle rather than at the beginning of execution of every function block.

7.2.2.2 Publisher

7.2.2.2.1 Connection establishment

The publishing of a safety function block parameter to be used in a safety function is indicated by the presence of a safety link object. If a safety link object exists for publishing, the publisher FBAP shall establish the publisher connection in a manner identical to non-safety publisher connections.

7.2.2.2.2 Publishing of data

At the end of execution, the safety function block shall determine which of its output parameters are to be published. The output parameters to be published are dependent on the type of the function block and the status of its input parameters. The parameters published are outside the scope of this part.

A function block publishes its selected output parameters (if so configured) using the extended protocol. The publishing of safety function block parameters to be used in a safety function is indicated by the presence of a safety link object. The published parameter value will be protected from possible corruption, duplication, and out of sequence reception caused by the black channel. To protect the data from corruption, a CRC 32 is used. A virtual PDU is formed as shown in Figure 16.

Connection key (4 octets)	Object index (4 octets)	Sequence number (2 octets)	Object value & status (2-120 octets)

Figure 16 – Safety PDU showing virtual content

Only the lower two octets of the Object Index are used. The higher two octets are set to zero. The CRC32 is calculated over the Virtual Safety PDU. The data on the call for the Information Report is modified to include a sequence number and CRC32 and is duplicated. The data format is shown in Figure 17.

Data 1			Data 2		
Original data	Sequence number	CRC32	Original data	Sequence number	CRC32

Figure 17 – Safety PDU showing duplication of data and addition of CRC

The “Original Data” is identical in format to the data that would have been contained in the data portion of the information report for non-safety data. The sequence number and the CRC32 are appended to this data. The function block shall set the sequence number to be the macro cycle number.

The function block shall set the status of the published output parameter to bad::black channel failure if the black channel time synchronization is not working properly i.e. BLK_CHN_ERR is non-zero.

Table 5, Figure 18, Table 6 and Table 7 define the state machine for the publisher.

Table 5 – Publisher states

State	Description
Not connected	No VCR for publishing established
Connected/Bad	VCR established but black channel errors not cleared
Connected/Good	VCR established, normal publications occurring

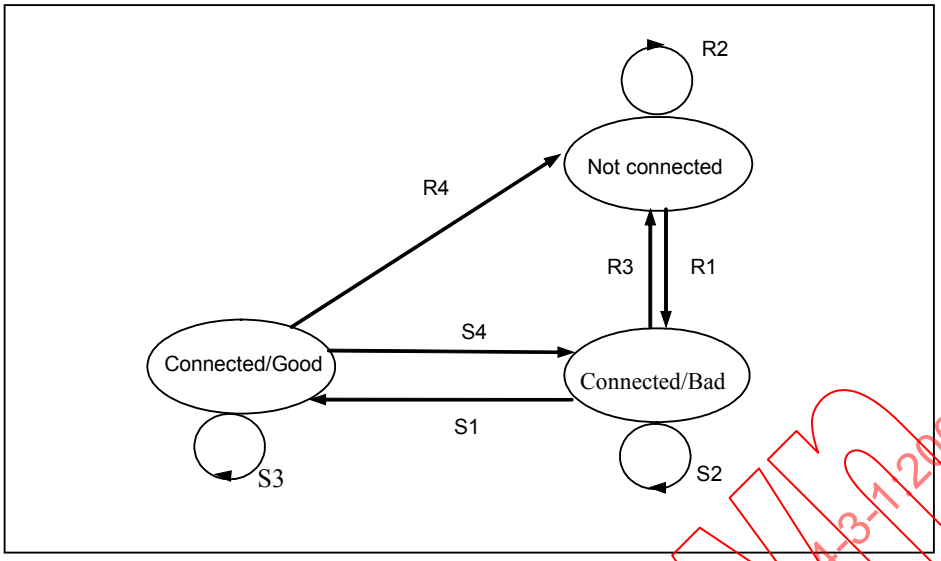


Figure 18 – State transition diagram for a FSCP 1/1 Publisher

Table 6 – Publisher state table - Received transitions

#	Current State	Event & Condition Action	Next State
R1	Not connected	RcvMsg() = “FMS Initiate.cnf"	Connected/ Bad
R2	Not connected	RcvMsg() = "Any message (not FMS Initiate.cnf)"	Same
R3	Connected/ Bad	RcvMsg() = "Abort.ind" OR RcvMsg() = "Abort.req"	Not connected
R4	Connected/G Good	RcvMsg() = "Abort.ind" OR RcvMsg() = "Abort.req"	Not connected

Table 7 – Publisher state table - Internal transitions

#	Current State	Event & Condition Action	Next State
S1	Connected/ bad	BLK_CHN_ERR = 0 SET Sequence Number = MCN	Connected/ Good
S2	Connected/ Bad	BLK_CHN_ERR <> 0 SET Black Channel Failure SET Sequence Number = MCN	Same
S3	Connected/ Good	BLK_CHN_ERR = 0 SET Sequence Number = MCN	Same
S4	Connected/ Good	BLK_CHN_ERR <> 0 SET Black Channel Failure SET Sequence Number = MCN NOTE The Function Block determines if its output parameters will be published or not. The logic is dependent on the sequence numbers received on its input parameters.	Connected/ Bad

7.2.2.3 Subscriber

7.2.2.3.1 Connection establishment

The subscription of a safety function block parameter to be used in a safety function is indicated by the presence of a safety link object. If a safety link object exists for subscribing, the subscriber FBAP shall establish the subscriber connections in manner identical to non-safety subscriber connections.

7.2.2.3.2 Subscribing of data

The MCN, calculated at the beginning of block execution, is the sequence number that is expected from the publisher of each of the publisher-subscriber connections in the block. If the published data is not state or if there are no accumulated delays in the black channel then the received sequence numbers will match the MCN.

When the FBAP receives FMS data, as shown in Figure 19, for a VCR associated with a safety link object,

a) The two copies of the original data are compared (Data 1 and Data 2), if they are identical proceed to b), otherwise the message is discarded and increment the Stale Count by 1.

Data 1			Data 2		
Original data	Sequence number	CRC32	Original data	Sequence number	CRC32

Figure 19 – Safety PDU showing duplication of data and addition of CRC

b) A Virtual Safety PDU, identical to the VSPDU used in the Publication of the data, is formed as shown in Figure 20.

Expected connection key (4 octets)	Expected object index (4 octets)	Received sequence number (2 octets)	Received object value & status (2-120 octets)

Figure 20 – Safety PDU showing virtual content

The expected connection key and the expected object index are extracted from the safety link object. For H1, only the lower two octets of the object index are used. The higher two octets are set to zero. The sequence number and the object value and status are filled in from the received data. The sequence number, and the duplicate data indication provided by the black channel are ignored.

c) A CRC 32 is calculated over the VSPDU. The CRC 32 is then compared with the CRC 32 received in the data portion of the FMS PDU. If the calculated CRC 32 does not match the received CRC 32, the PDU will be discarded. If the CRC does not match, the stale count is incremented by 1.

d) If CRC32 is valid and the sequence number matches the MCN, the received data is used.

e) If CRC 32 is valid, and the sequence number does not match the MCN, the stale count is incremented by 1. Data is discarded.

f) If stale count exceeds the configured end-to-end stale count limit, the status of the Input parameter shall be set to bad::black channel failure. The data is discarded.

g) If the black channel time synchronization is not working i.e. BLK_CHN_SYNC_ERR bit in the BLK_CHN_ERR parameter in resource block is TRUE, the status of the input parameters shall be set to bad::black channel failure. The data is discarded.

Table 8, Figure 21, Table 9 and Table 10 define the state machine for the subscriber.

Table 8 – Subscriber states

State	Description
Not connected	No VCR for subscribing established
Connected/Stale	VCR established but black channel errors or stale count not cleared
Connected/Good	VCR established, normal publications occurring

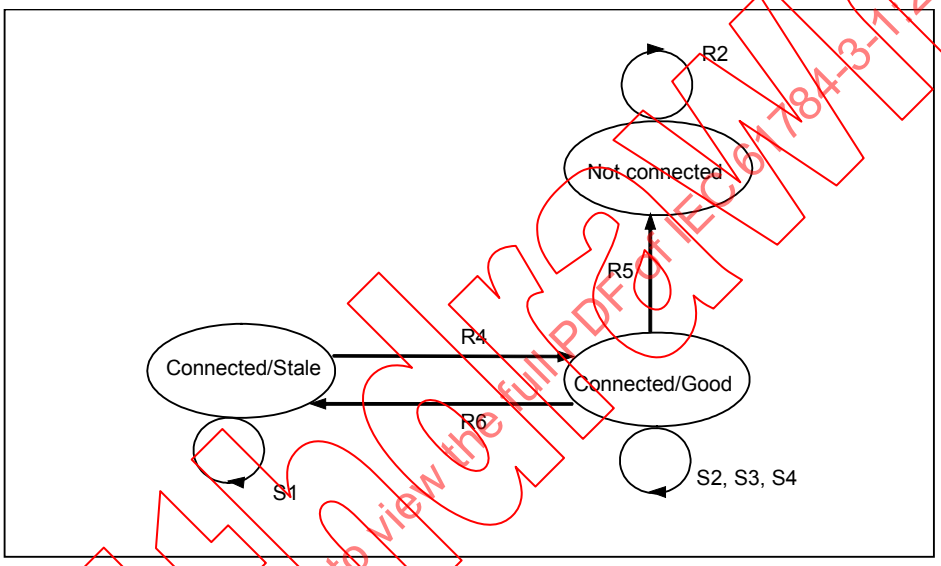


Figure 21 – State transition diagram for a FSCP 1/1 subscriber

Table 9 – Subscriber state table - Received transitions

#	Current State	Event and condition action	Next State
R1	Not connected	RcvMsg() = “FMS Initiate.cnf"	Connected/ stale
R2	Not connected	RcvMsg() = "Any message (not FMS Initiate.cnf)"	Same
R3	Connected/ Stale	RcvMsg() = "Abort.ind" OR RcvMsg() = "Abort.req"	Not connected
R4	Connected/ Stale	Sequence Number = MCN AND BLK_CHN_ERR = 0 SET Use Data Stale Count = 0	Connected/ Good
R5	Connected/ Good	RcvMsg() = "Abort.ind" OR RcvMsg() = "Abort.req"	Not connected
R6	Connected/ Good	Stale Count > End-to-end stale count OR BLK_CHN_ERR <> 0 SET Status = Bad::Black channel failure Discard data	Connected/ Stale

Table 10 – Subscriber state table - Internal transitions

#	Current state	Event and condition action	Next state
S1	Connected/ Stale	Sequence Number = MCN OR Data 1 <> Data 2 OR BLK_CHN_ERR <> 0 SET Status = Bad::Black channel failure Discard data	Connected/ Good
S2	Connected/ Good	(Sequence Number <> MCN OR Data 1 <> Data 2) AND Stale Count <= End-to-end stale count AND BLK_CHN_ERR = 0 Increment Stale Count Discard data	Same
S3	Connected/ Good	CRC 32 is invalid AND BLK_CHN_ERR = 0 Increment Stale Count Discard data	Same
S4	Connected/ Good	Sequence Number = MCN AND Data 1 = Data 2 AND BLK_CHN_ERR = 0 SET Stale Count = 0 Use data	Same

7.2.3 Client-server interactions

7.2.3.1 General

Client-Server VCRs to read data from safety function blocks shall be set up with maximum concurrency of 1. The device shall reject all FMS Initiate requests to VCRs set up with a concurrency greater than 1.

7.2.3.2 Read

The read request for reading data from safety function blocks (i.e. data to be used in a safety function) is identical to that of reading data from non safety function blocks.

FMS supplies the index of the object (and the optional sub index) that is being read. If the read is for a safety function block, the device shall check if a valid safety link object, with service operation set to SIS_ACCESS, exists for that block. If a valid link object does not exist, the device responds to the read just like a read of a non-safety function block parameter.

If a valid safety link object exists, and there is already a read or write request pending, the device shall reject the read or write request and send a negative response.

If a valid safety link object exists, and there is no other outstanding read/write request, the device responds to the data using the extended protocol. This data will be protected from possible corruption, duplication, and out of sequence reception caused by the black channel. To protect the data from corruption, a CRC 32 is used and to calculate the CRC 32, a virtual PDU is formed as shown in Figure 22. If the read is a read by sub index, the sub index is also used in calculating the CRC 32. For H1, only the lower two octets of the object index are used. The higher two octets are set to zero.

Connection key (4 octets)	Object index (4 octets)	Sequence number (2 octets)	Object value & status (2-120 octets)

Figure 22 – Safety PDU showing virtual content

If the read is by sub index, the VSPDU shall include the sub index. The sub index shall be included in the calculation of CRC 32. This virtual PDU is shown in Figure 23.

Connection key (4 octets)	Object index (4 octets)	Sub index (1 octets)	Sequence number (2 octets)	Object value & status (2-120 octets)

Figure 23 – Safety PDU showing virtual content with sub index

The CRC 32 is calculated over the Virtual Safety PDU. The data on the call for the FMS Read.res is modified to duplicate the data and to include a sequence number and CRC 32. The data format is shown in Figure 24.

Data 1			Data 2		
Original data	Sequence number	CRC32	Original data	Sequence number	CRC32

Figure 24 – Safety PDU showing duplication of data, addition of sequence number and CRC

The “Original data” is identical in format to the data that would have been contained in the data portion of the FMS Read.res for non safety function blocks. The Sequence Number and the CRC32 are appended to this data. The sequence number is incremented for every PDU handed over to the black channel for communication.

The sequence number count is maintained for each safety communication layer connection, i.e. connection key. The sequence number is reset to zero after connection establishment. The sequence number rolls over to 1.

NOTE The Invoke ID is not included in the CRC 32 calculation.

If the device is responding with a negative response, the response is identical to negative response for non-safety function blocks. That is, the sequence number is not incremented; virtual safety PDU need not be formed.

The state machine for processing reads is shown in Table 11, Figure 25 and Table 12.

Table 11 – Server states during read operations

State	Description
Not connected	No Connection established
Connected	Connection established

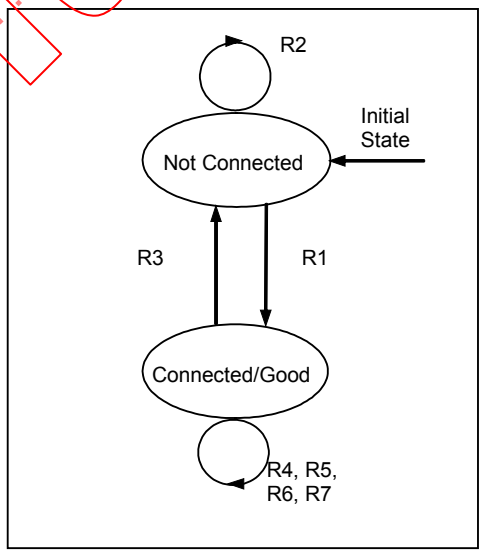


Figure 25 – State transition diagram for a FSCP 1/1 Server during read operations

Table 12 – Received transitions for a FSCP 1/1 Server during read operations

#	Current state	Event and condition action	Next state
R1	Not connected	RcvMsg() = “Connection Request valid response" Set Sequence number = o	Connected
R2	Not connected	RcvMsg() = "Any message (not connection request valid response)"	Same
R3	Connected	RcvMsg() = "Abort.ind" OR RcvMsg() = "Abort.req"	Not connected
R4	Connected	Valid Read request AND safety link object exists AND No other FMS requests outstanding Respond using safety communication layer protocol	Connected
R5	Connected	Valid Read request AND safety link object does not exist Respond using FMS protocol	Connected
R6	Connected	Valid Read request AND safety link object exists AND Other FMS requests outstanding Return negative response	Connected
R7	Connected	Invalid Read request Return negative response	Connected

7.2.3.3 Write

The request for writing data to safety function blocks will follow the extended protocol. Clients initiating the write request shall format the data according to the safety PDU format described below and shown in Figure 26.

FMS supplies the index of the object that is being written. If the write is for a safety function block, the device shall check if the write is formatted according to the extended protocol.

That is it checks to see if Data 1 is identical to Data 2. If identical it determines if the packet has a valid sequence number and a CRC32 added. If not identical the data is discarded and a negative response is returned. A sequence is valid if it is 1 more (using unsigned arithmetic) than the last sequence number received on that connection (LRSN) i.e. sequence numbers have to be tracked per connection key. If the sequence number is incorrect, the device shall discard the write and abort the connection. If the sequence number is correct, the device shall increment the LRSN.

Data 1			Data 2		
Original data	Sequence number	CRC32	Original data	Sequence number	CRC32

Figure 26 – Safety PDU showing duplication of data and addition of sequence number and CRC

The “Original data” is identical in format to the data that would have been contained in the data portion of the FMS Write.ind for non safety function blocks.

The device then determines if a valid safety link object, with Service Operation set to SIS_ACCESS, exists for that block. If a valid link object does not exist, the device discards the write request and returns a negative response.

If a valid Link object exists, the device constructs a virtual Safety PDU (VSPDU) as shown in Figure 27 . The expected Connection Key is taken from the safety link object. If the write is by sub index, the sub index shall also be included as shown in Figure 28. The lower two octets of the Object Index are used. The higher two octets are set to zero.

Expected connection key (4 octets)	Object index (4 octets)	Sequence number (2 octets)	Object value & status (2-120 octets)

Figure 27 – Example of FSCP 1/1 write

Expected connection Key (4 octets)	Object index (4 octets)	Sub index (1 octets)	Sequence number (2 octets)	Object value & status (2-120 octets)

Figure 28 – Example of FSCP 1/1 write with sub index

The CRC 32 is calculated over the Virtual Safety PDU, and compared with the CRC 32 in the received data. If it does not match, the device shall discard the data, and return a negative response.

If all the checks pass, the device honours the write request. A positive or negative response is returned by the specific block that is being written to.

A positive or negative write response has the same format as a write response from a non-safety function block.

The state machine for processing writes is shown in Table 13, Figure 29 and Table 14.

Table 13 – States of a FSCP 1/1 server during write operations

State	Description
Not connected	No connection established
Connected	Connection established

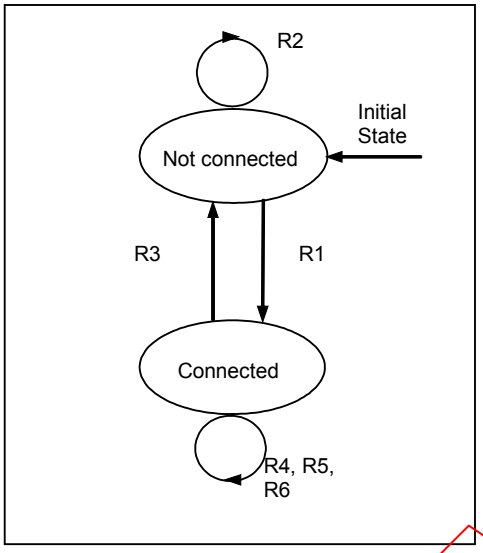


Figure 29 – State transition diagram for a FSCP 1/1 Server during write operations

Table 14 – Received transitions for a FSCP 1/1 Server during write operations

#	Current state	Event and condition action	Next state
R1	Not connected	RcvMsg() = “Connection Request valid response" Set LRSN = 0	Connected
R2	Not connected	RcvMsg() = "Any message (not connection request valid response)"	Same
R3	Connected	RcvMsg() = "Abort.ind" OR RcvMsg() = "Abort.req"	Not connected
R4	Connected	Valid Write request AND safety link object exists AND CRC 32 is OK AND Sequence Number OK AND No other FMS requests outstanding Increment LRSN Respond using safety related communication layer protocol	Connected
R5	Connected	Data 1 not identical to Data 2 OR safety link object does not exist OR CRC 32 not OK OR Invalid Write request Return negative response	Connected
R6	Connected	Valid Write request AND safety link object exists AND Sequence Number OK AND Other FMS requests outstanding Return negative response	Connected

7.2.3.4 Writes to safety link object

Writes to the safety link object shall be according to the extended protocol as specified below.

The request for writing data to safety function blocks will follow the extended protocol. The client shall compute CRC 32 over the index of the safety link object and Link Object data, in that order.

FMS supplies the index of the object that is being written. If the write is for a safety link object, the device shall check if the write is formatted according to the extended PDU content shown in Figure 30. That is it compares Data 1 to Data 2 and if identical it checks to see if the packet has a valid CRC 32 added. If not identical the write is discarded and a negative response is returned. CRC 32 is computed over the index of the safety link object and safety link object data, in that order. If the calculated CRC does not match the received CRC, the device shall discard the write and return a negative response. The device shall not support write by sub index to the safety link object. If a device receives a write by sub index, it shall discard the request and return a negative response.

Data 1		Data 2	
Safety link object data	CRC32	Safety link object data	CRC32

Figure 30 – Safety PDU showing duplication of data and CRC

The device then determines if the safety link object is formatted correctly. If it is not the device shall discard the write and return a negative response.

The safety object shall be written only when the resource block is OOS. If the resource block is not in OOS, the device shall discard the write and return a negative response.

If all the checks pass, the device honours the write request and returns a positive response.

A positive or negative write response has the same format as a write response from a non-safety function block.

With respect to connection management, a successful write to safety link object shall trigger the same behaviour as a successful write to non-safety link objects. In addition, a successful write shall reset (set to 0) the sequence number associated with the connection key that is written.

The device shall store the CRC in its non-volatile storage as part of the safety link object. The device is expected to check the integrity of its entire configured link objects on a periodic basis and immediately after start-up in accordance with IEC 61508 requirements. If the integrity is bad, the device shall set its resource block to OOS.

7.2.4 Time synchronization

Time (DL-time) is synchronized by the black channel. The safety communication layer time sync monitor shall monitor whether the black channel time synchronization is working correctly or not. Each device shall have a crystal in the safety communication layer of at least 100 parts per million accuracy and a resolution of at least 100 µs. See device development requirements specification for more information.

a) The safety communication layer time sync monitor shall execute after the black channel has processed a received Time Distribution PDU. It shall determine if the drift between black channel time and the safety communication layer time is greater than the allowable drift. Unsigned 16-bit arithmetic shall be used.

Allowable drift = $(TLCTD_n - TLCTD_{n-1}) \times 2 \times 10^{-4}$

Actual drift = (TTD_n - TTD_{n-1}) - ($TLCTD_n$ - $TLCTD_{n-1}$)

Where,

$TLCTD_n$ is the time of safety communication layer clock after processing of the current TD;

$TLCTD_{n-1}$ is the time of safety communication layer clock after processing of the previous TD;

TTD_n is the DL-Time after processing of the current TD;

TTD_{n-1} is the DL-Time after processing of the previous TD;

b) If the absolute value of Actual Drift exceeds the Allowable Drift, the monitor shall set the BLK_CHN_SYNC_ERR bit of the BLK_CHN_ERROR parameter in the Resource Block to TRUE; otherwise the flag shall be set to FALSE.

c) If the black channel does not receive a valid TD in 6 consecutive Time Distribution Periods, the monitor shall set the BLK_CHN_SYNC_ERR bit of the BLK_CHN_ERROR parameter in the Resource Block to TRUE.

d) If the BLK_CHN_SYNC_ERR is TRUE, the Time Sync Monitor shall require the black channel to attempt to synchronize time — periodically (once every TD period) command the black channel to send out CT sequences.

e) When the resource block's CLR_FAULT_STATE is written, a DL_RESET primitive shall be sent to the data link layer if the BLK_CHN_SYNC_ERR is TRUE.

7.2.5 Device start-up

The resource block in the safety communication layer shall be in OOS mode until the following have been completed:

a) The device is on the live list (the device is either LAS or the device has received a valid PN/PR/Activation PDU sequence;

b) The black channel DL-Time is valid — the device is LAS, or the device has updated the time based on valid TD and RR PDUs.

7.3 Communications entity

7.3.1 General

The communications entity and the SMK are the parts of the black channel that exist in a device and, therefore, do not have to execute in a SIL environment.

No changes are made to the communications entity.

7.3.2 Network management

Network management is part of the black channel. No change is needed.

7.3.3 FMS

FMS is part of the black channel. No change is needed.

7.3.4 H1 stack

The H1 stack is part of the black channel. No change is needed.

8 Safety communication layer management

8.1 Overview

The SMK is not trusted and is defined to be part of the black channel. Therefore, SMK need not be executed in a SIL environment. Internal manufacturer specific checks that meet the requirements of IEC 61508 are required for any local interface interaction between the SMK and the application process.

It is only possible to set an address when the write enable mode is set in the device resource block. When the address is changed the link objects are deleted. The address and tag of a device can only be written when the resource is in out-of-service mode.

8.2 SMK communications

The SMK is part of the black channel and its communications with the application layer are not trusted. Communications between SMK and the application process are on a local interface and verifications are internal using manufacturer specific means.

8.3 FMS services

The SMIB is part of the black channel, but exchanges information with the application process via SMK through a local interface. The manufacturer specific diagnostics shall verify this local interface. These internal faults can be controlled by manufacturer specific means.

8.4 SMK services

8.4.1 General

SMK services are part of the black channel and therefore not trusted. Verifications are internal between SMK and the application process on a local interface. These internal faults can be controlled by manufacturer specific means.

The resource block contains a macro cycle parameter since the data in the black channel cannot be relied on.

8.4.2 Address assignment

Address is part of the black channel. Address duplication masquerading faults are controlled using the connection key. It is expected that devices will automatically clear their configuration when the black channel address is changed.

8.4.3 Time synchronization

Time synchronization is a black channel function. A black channel time synchronization monitor function in the safety communication layer diagnoses the integrity of the H1 time synchronization mechanism. FSCP 1/1 protocol extensions, stale data timer, and end-to-end stale count limit will indirectly control the faults caused by any synchronization problems.

8.5 Safety communication layer configuration and start-up

8.5.1 H1 configuration and start-up

MIB is part of the black channel. There are no changes to its configuration. FBAP is different, (see 8.5.2). The safety communication layer is configured from data in link objects and the resource block transferred by internal vendor specific means.

8.5.2 FSCP 1/1 FBAP

Function block objects and parameters may be configured according to the Function Block AP specification.

8.5.3 Testing

After a device configuration has been changed it is necessary to test and verify the correct function.

9 System requirements

9.1 Indicators and switches

There are no indicators or switches that are required for a device.

9.2 Installation guidelines

The installation guidelines of IEC 61918 shall apply.

NOTE Specific amendments to the installation guidelines of IEC 61918 may also be defined in a future IEC 61784-5-1 for CPF 1.

9.3 Safety function response time

The safety function response time is the worst case elapsed time following an actuation of a safety sensor (for example switch, pressure transmitter, light curtain) connected to a fieldbus, before the corresponding safe state of its safety actuator(s) (for example relay, valve, drive) is achieved in the presence of errors or failures in the safety function channel.

The demand (actuation) on a safety function is caused either by an analog signal crossing a threshold or a digital signal changing state.

Figure 31 shows an example of typical components making up a safety function response time.

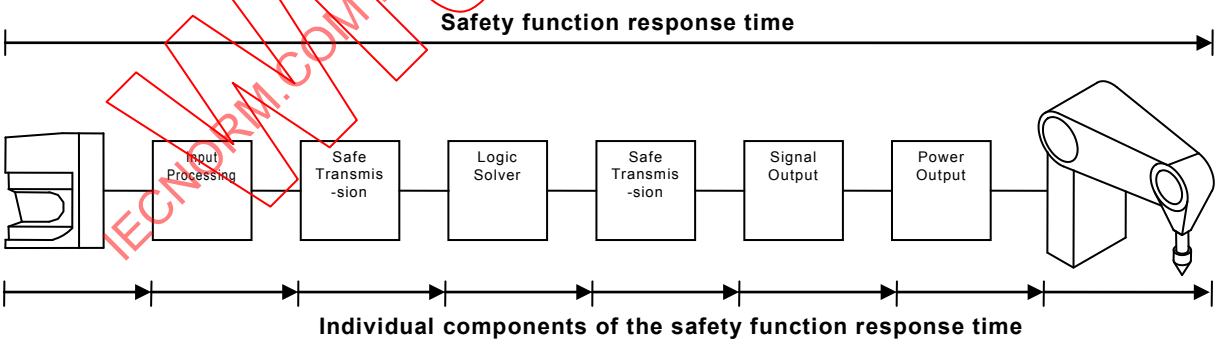


Figure 31 – Example of safety function response time components

Safe transmission time = 2 x macro cycle + ((stale count) x macro cycle)

This time is only for the safe transmission and does not include time for other components of the safety response time. The safety manual for each device will have a more detailed description on how to calculate the safety function response time for a device.

9.4 Duration of demands

The demand has to exist for at least 2 macro cycles to guarantee that the functional safety communication system detects the demand.

9.5 Constraints for calculation of system characteristics

9.5.1 Message rate

The maximum message rate used in calculations of the safety integrity level was 10 000 messages per second. This message rate cannot be obtained in a H1 network. Since the message rate used far exceeds the possible message rate on a H1 segment, there are no constraints on the message rate on a H1 segment.

9.5.2 SIL level

The FSCP 1/1 protocol technology is designed for use in a SIL 3 safety function and to use up no more than 1 % of the PFD budget (1 % of 10^{-8} in continuous high-demand mode). It is possible to use FSCP 1/1 in products designed for safety functions up to SIL 3, suitable for logic solvers.

9.6 Maintenance

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

9.7 Safety manual

The safety device manufacturer shall supply a safety manual that is appropriate to the device.

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

10 Certification

FSCP 1/1 alone does not make a safety-related system or safety device. In addition to FSCP 1/1 protocol interoperability registration, the device, systems, and software, etc. will also have applicable SIL certification. The user shall ascertain the suitability of use of every Safety device in the safety function in accordance with IEC 61508 series. In addition to Fieldbus considerations, the user will also take the IEC 61508 safety aspects into consideration. It shall be the manufacturer's responsibility to develop the device to the appropriate development process according to the safety standards (see IEC 61508, IEC 61511 series) and certification by an appropriate agency shall be achieved.

Annex A
(informative)

Additional information
for functional safety communication profiles of CPF 1

A.1 Hash function calculation

```
//
// Usage:
//   crc32eth [infile]
//   calculates Ethernet-CRC32 over the content of file [infile]
//
// Compile:
//   (this source should compile on any C++ compiler)
//   g++ -Wall -o crc32eth crc32eth.cc                  #GNU-C++ under Linux
//   g++ -Wall -mno-cygwin -o crc32eth.exe crc32eth.cc   #with cygwin GNU-C++
//
// ------------------------------------------------------------------------------
// CRC calculation is mathematically the evaluation of the remainder of a polynomial division

// with the generator polynomial as divisor.
// For Ethernet-CRC32 the generator polynomial is 0xedb88320, the bits correspond (f.l.t.r.)

// with the coefficients fuer x^0, x^1 .. x^31, the coefficient for x^32 ist implicitly 1.
// This "unnatural" bit order (least significant bit left) is also applied to any single
// octet of the input data block and to the result of the polynomial division.
// ------------------------------------------------------------------------------

#include <iostream>
#include <iomanip>
#include <fstream>

// ------------------------------------------------------------------------------

const unsigned long maCRC32Ether[256] = {
  // Table for generator polynom 0xedb88320
  0x00000000, 0x77073096, 0xee0e612c, 0x990951ba,
  0x076dc419, 0x706af48f, 0xe963a535, 0x9e6495a3,
  0x0edb8832, 0x79dcb8a4, 0xe0d5e91e, 0x97d2d988,
  0x09b64c2b, 0x7eb17cbd, 0xe7b82d07, 0x90bf1d91,
  0x1db71064, 0x6ab020f2, 0xf3b97148, 0x84be41de,
  0x1adad47d, 0x6ddde4eb, 0xf4d4b551, 0x83d385c7,
  0x136c9856, 0x646ba8c0, 0xfd62f97a, 0x8a65c9ec,
  0x14015c4f, 0x63066cd9, 0xfa0f3d63, 0x8d080df5,
  0x3b6e20c8, 0x4c69105e, 0xd56041e4, 0xa2677172,
  0x3c03e4d1, 0x4b04d447, 0xd20d85fd, 0xa50ab56b,
  0x35b5a8fa, 0x42b2986c, 0xdbbbc9d6, 0xacbcf940,
  0x32d86ce3, 0x45df5c75, 0xdcd60dcf, 0xabd13d59,
  0x26d930ac, 0x51de003a, 0xc8d75180, 0xbfd06116,
  0x21b4f4b5, 0x56b3c423, 0xcfba9599, 0xb8bda50f,
  0x2802b89e, 0x5f058808, 0xc60cd9b2, 0xb10be924,
  0x2f6f7c87, 0x58684c11, 0xc1611dab, 0xb6662d3d,
  0x76dc4190, 0x01db7106, 0x98d220bc, 0xefd5102a,
  0x71b18589, 0x06b6b51f, 0x9fbfe4a5, 0xe8b8d433,
  0x7807c9a2, 0x0f00f934, 0x9609a88e, 0xe10e9818,
  0x7f6a0dbb, 0x086d3d2d, 0x91646c97, 0xe6635c01,
  0x6b6b51f4, 0x1c6c6162, 0x856530d8, 0xf262004e,
  0x6c0695ed, 0x1b01a57b, 0x8208f4c1, 0xf50fc457,
```

```
  0x65b0d9c6, 0x12b7e950, 0x8bbeb8ea, 0xfcb9887c,
  0x62dd1ddf, 0x15da2d49, 0x8cd37cf3, 0xfbd44c65,
  0x4db26158, 0x3ab551ce, 0xa3bc0074, 0xd4bb30e2,
  0x4adfa541, 0x3dd895d7, 0xa4d1c46d, 0xd3d6f4fb,
  0x4369e96a, 0x346ed9fc, 0xad678846, 0xda60b8d0,
  0x44042d73, 0x33031de5, 0xaa0a4c5f, 0xdd0d7cc9,
  0x5005713c, 0x270241aa, 0xbe0b1010, 0xc90c2086,
  0x5768b525, 0x206f85b3, 0xb966d409, 0xce61e49f,
  0x5edef90e, 0x29d9c998, 0xb0d09822, 0xc7d7a8b4,
  0x59b33d17, 0x2eb40d81, 0xb7bd5c3b, 0xc0ba6cad,
  0xedb88320, 0x9abfb3b6, 0x03b6e20c, 0x74b1d29a,
  0xead54739, 0x9dd277af, 0x04db2615, 0x73dc1683,
  0xe3630b12, 0x94643b84, 0x0d6d6a3e, 0x7a6a5aa8,
  0xe40ecf0b, 0x9309ff9d, 0x0a00ae27, 0x7d079eb1,
  0xf00f9344, 0x8708a3d2, 0x1e01f268, 0x6906c2fe,
  0xf762575d, 0x806567cb, 0x196c3671, 0x6e6b06e7,
  0xfed41b76, 0x89d32be0, 0x10da7a5a, 0x67dd4acc,
  0xf9b9df6f, 0x8ebeeff9, 0x17b7be43, 0x60b08ed5,
  0xd6d6a3e8, 0xa1d1937e, 0x38d8c2c4, 0x4fdff252,
  0xd1bb67f1, 0xa6bc5767, 0x3fb506dd, 0x48b2364b,
  0xd80d2bda, 0xaf0a1b4c, 0x36034af6, 0x41047a60,
  0xdf60efc3, 0xa867df55, 0x316e8eef, 0x4669be79,
  0xcb61b38c, 0xbc66831a, 0x256fd2a0, 0x5268e236,
  0xcc0c7795, 0xbb0b4703, 0x220216b9, 0x5505262f,
  0xc5ba3bbe, 0xb2bd0b28, 0x2bb45a92, 0x5cb36a04,
  0xc2d7ffa7, 0xb5d0cf31, 0x2cd99e8b, 0x5bdeae1d,
  0x9b64c2b0, 0xec63f226, 0x756aa39c, 0x026d930a,
  0x9c0906a9, 0xeb0e363f, 0x72076785, 0x05005713,
  0x95bf4a82, 0xe2b87a14, 0x7bb12bae, 0x0cb61b38,
  0x92d28e9b, 0xe5d5be0d, 0x7cdcefb7, 0x0bdbdf21,
  0x86d3d2d4, 0xf1d4e242, 0x68ddb3f8, 0x1fda836e,
  0x81be16cd, 0xf6b9265b, 0x6fb077e1, 0x18b74777,
  0x88085ae6, 0xff0f6a70, 0x66063bca, 0x11010b5c,
  0x8f659eff, 0xf862ae69, 0x616bffd3, 0x166ccf45,
  0xa00ae278, 0xd70dd2ee, 0x4e048354, 0x3903b3c2,
  0xa7672661, 0xd06016f7, 0x4969474d, 0x3e6e77db,
  0xaed16a4a, 0xd9d65adc, 0x40df0b66, 0x37d83bf0,
  0xa9bcae53, 0xdebb9ec5, 0x47b2cf7f, 0x30b5ffe9,
  0xbdbdf21c, 0xcabac28a, 0x53b39330, 0x24b4a3a6,
  0xbad03605, 0xcdd70693, 0x54de5729, 0x23d967bf,
  0xb3667a2e, 0xc4614ab8, 0x5d681b02, 0x2a6f2b94,
  0xb40bbe37, 0xc30c8ea1, 0x5a05df1b, 0x2d02ef8d
};

// GetCRC32Ether() calculates the CRC over a data block located at address [pStart] with a
size
// of [len] octets. GetCRC32Ether() works incrementally with the result of the last portion given

// as [preset] value for the subsequent portion. For the first portion a preset value of 0xffffffff

// (=CRC32ETHER_PRESET) has to be used.
// GetCRC32Ether() implements the highly efficient table technique for CRC calculation.

enum {CRC32ETHER_PRESET= 0xffffffff};

unsigned long GetCRC32Ether(const void*   pStart,
                            size_t        len,
                            unsigned long preset) {
  size_t bytecount;
  unsigned char * buf= (unsigned char *) pStart;
  unsigned long crcword= preset;
  for (bytecount= len; (bytecount > 0); bytecount--, buf++) {
```

```
    crcword= maCRC32Ether[(crcword ^ *buf) & 0x0ff] ^ ( crcword >> 8L );
  }
  return crcword;
};

// ------------------------------------------------------------------------------------------
enum {BUFSIZE= 1024}; //Groesse des Read-Buffers

int main(int argc, char * argv[]) {

  if (argc != 2) {
    std::cerr << "Usage:" << std::endl;
    std::cerr << "  "  << argv[0] << " infile" << std::endl;
    return 2;
  }

  std::ifstream infile;
  infile.open(argv[1], std::ios_base::in | std::ios_base::binary);
  if (!infile) {
    std::cerr << "ERR: unable to open file " << argv[1] << std::endl;
    exit(1);
  }

  char buf[BUFSIZE];                  //Read-Buffer
  size_t totalCount= 0;               //Laenge in Bytes
  unsigned long sig= CRC32ETHER_PRESET; //Preset of the signatur

  while (infile) {
    infile.read(&buf[0], BUFSIZE);
    size_t portionCount= infile.gcount();
    totalCount+= portionCount;
    sig= GetCRC32Ether(&buf[0], portionCount, sig);
  }
  if (!infile.eof()) {
    std::cerr << "ERR: error while reading file " << argv[1] << std::endl;
    exit(1);
  }
  infile.close();
  std::cout << argv[0] << ": bytes read from file " << argv[1] << ": " << totalCount << std::endl;

  std::cout << argv[0] << ": CRC: 0x" << std::hex << std::setw(8) << std::setfill('0') << sig <<
std::endl;

return 0;
}
```


A.2 Fault conditions arising from locations beyond the output function block

When diagnostics on the device output detect a field fault arising from locations beyond the output function block or beyond the device itself, for example a connected actuator, the action taken is not defined in the output function block, but rather in the transducer block or hardware. On a device failure the output goes to the de-energized state just as if power to the device itself was lost. Some output devices may use auxiliary power to drive the actuator, and if this is lost the physical output goes to its de-energized state. Since these faults occur after the output function block, the fault state configuration is not applicable. Table A.1 shows this behaviour.

A device failure will always result in a latched output that will need to be reset by the user.

Table A.1 – Fault conditions arising from locations beyond the output function block

Condition	Example	Remark
Field fault	Partial stroke testing failure (valve or actuator fault), solenoid wiring open or short circuit	Diagnostics and action determined by transducer block and hardware. Feedback through output function block
Auxiliary power failure	Loss of supply air, line power, or hydraulic pressure	Action determined by hardware. Feedback through output function block
Device power failure	Bus power or separate power lost	Action determined by hardware.
Device failure	Memory fault or CPU watchdog	Action determined by hardware
Stale data timer	Output block execution or scheduling fault	Diagnostics and action determined by transducer block and hardware. Feedback through output function block

Bibliography

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

NOTE See also the IEC Multilingual Dictionary – Electricity, Electronics and Telecommunications (available on CD-ROM and at <http://domino.iec.ch/iev>).

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

[3] IEC 61131-6: *Programmable controllers – Part 6: Functional safety*[4]

[4] IEC 61158 (all parts), *Industrial communication networks – Fieldbus specifications*

[5] 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*[5]

[6] 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 EM environment*[5]

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

[8] IEC 61508-4:1998, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations*

[9] IEC 61508-6:1998, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3*

[10] IEC 61784-2, *Industrial communication networks – Profiles – Part 2: Additional fieldbus profiles for real-time networks based on ISO/IEC 8802-3*

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

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

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

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

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

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

[17] IEC 62443, *Security for industrial process measurement and control – Network and system security*[6]

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

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

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

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

4 Under consideration.

5 To be published.

6 In preparation.

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

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

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

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

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

[27] GS-ET-26; *Grundsatz für die Prüfung und Zertifizierung von Bussystemen für die Übertragung sicherheitsrelevanter Nachrichten*, May 2002. HVBG, Gustav-Heinemann-Ufer 130, D-50968 Köln ("*Principles for Test and Certification of Bus Systems for Safety relevant Communication*")[7]

[28] Andrew S. Tanenbaum, *Computer Networks*, 2nd Edition, Prentice Hall, N.J., ISBN 0-13-162959-X

[29] W. Wesley Peterson, *Error-Correcting Codes*, 2nd Edition 1981, MIT-Press, ISBN 0-262-16-039-0

[30] Bruce P. Douglass, *Doing Hard Time*, 1999, Addison-Wesley, ISBN 0-201-49837-5

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

[32] Dieter Conrads, *Datenkommunikation*, 3rd Edition 1996, Vieweg, ISBN 3-528-245891

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

[34] NFPA79 (2002): *Electrical Standard for Industrial Machinery*

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

[36] 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

[37] Foundation™ Fieldbus AG-180, *User Application Guide for FF-SIS*

[38] Foundation™ Fieldbus FF-807, *FS-SIS Application Model – Phase 1*

[39] Foundation™ Fieldbus FF-884, *FF-SIS Protocol Specification*

[40] Foundation™ Fieldbus FF-895, *FF-SIS Function Block Application Process – Phase 1*

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

SOMMAIRE

AVANT-PROPOS 66
INTRODUCTION 68
1 Domaine d'application 72
2 Références normatives 72
3 Termes, définitions, symboles, abréviations et conventions 73
3.1 Termes et définitions 73
3.1.1 Termes et définitions communs 73
3.1.2 CPF 1: Termes et définitions supplémentaires 77
3.2 Symboles et abréviations 78
3.2.1 Symboles et abréviations communs 78
3.2.2 CPF 1: Symboles et abréviations supplémentaires 78
3.3 Conventions 79
3.3.1 Diagrammes d'états 79
3.3.2 Utilisation de couleurs dans les figures 80
4 Présentation générale de FSCP 1/1 (FOUNDATION Fieldbus™ SIS) 80
4.1 Généralités 80
4.2 Concepts clés du FSCP 1/1 81
4.2.1 Canal noir 81
4.2.2 Clé de connexion 82
4.2.3 Contre-vérification 82
4.2.4 FSCP 1/1 82
4.2.5 Système électronique programmable 82
4.2.6 Retards de mise en file d'attente 82
4.2.7 Redondance 82
4.2.8 Environnement SIL 82
4.3 Composantes clés du FSCP 1/1 83
4.3.1 Présentation générale 83
4.3.2 Canal noir 84
4.4 Relation avec le modèle de référence de base OSI de l'ISO 85
5 Généralités 85
5.1 Documents externes de spécifications applicables au profil 85
5.2 Exigences de sécurité fonctionnelle 85
5.2.1 Exigences relatives à la sécurité fonctionnelle 85
5.2.2 Contraintes de fonctionnement 86
5.2.3 Exigences du fabricant d'appareils 86
5.3 Mesures de sécurité 86
5.3.1 Numéro de séquence 86
5.3.2 Datation (horodatage) 86
5.3.3 Délai 86
5.3.4 Authentification de connexion 86
5.3.5 Assurance d'intégrité des données 86
5.3.6 Redondance avec contre-vérification 86
5.3.7 Différents systèmes d'assurance d'intégrité des données 86
5.3.8 Relations entre les erreurs et les mesures de sécurité 86
5.4 Structure de la couche de communication de sécurité 87
5.4.1 Topologie de réseau et connectivité des appareils 87

5.4.2 Architecture des appareils 88
5.5 Relations avec la FAL (et DLL, PhL) 89
5.5.1 Généralités 89
5.5.2 Types de données 89
6 Services de la couche de communication de sécurité 90
6.1 Processus d'Application (AP) 90
6.1.1 Présentation générale 90
6.1.2 Objets visibles de réseau 90
6.1.3 Interface de couche application 90
6.1.4 Dictionnaire d'objets 90
6.1.5 Répertoire de programmes d'application 90
6.2 Processus d'application de blocs de fonctions 90
6.2.1 Généralités 90
6.2.2 Modèle de blocs de fonctions 91
6.2.3 Processus d'Application 93
6.3 Communications entre appareils 96
6.3.1 Généralités 96
6.3.2 Client/serveur 97
6.3.3 Editeur/abonné 97
6.3.4 Diffusion de rapports 97
6.3.5 Opération FBAP dans un appareil de liaison 97
6.3.6 Communications de protocole de noyau de gestion de système (SMKP) 97
6.4 Profils 97
6.4.1 Généralités 97
6.4.2 Profil FSCP 1/1 98
6.5 Descriptions d'appareils 98
6.6 Formats de fichiers communs 99
6.7 Informations de configuration 99
6.7.1 Présentation générale 99
6.7.2 Configuration de niveau 1: définition des appareils du fabricant 99
6.7.3 Configuration de niveau 2: définition de réseau 100
6.7.4 Configuration de niveau 3: définition d'une application répartie 100
6.7.5 Configuration de niveau 4: Configuration des appareils 100
7 Protocole de couche de communication de sécurité 100
7.1 Format PDU de sécurité 100
7.1.1 Généralités 100
7.1.2 CRC de couche de communication de sécurité 100
7.1.3 Contrôle de la synchronisation temporelle par le canal noir 100
7.1.4 Numéro de séquence 101
7.1.5 En-tête virtuel 102
7.1.6 Clé de connexion 102
7.1.7 Redondance et contre-vérification 102
7.2 Extensions de protocole pour utilisation dans des systèmes relatifs à la sécurité 103
7.2.1 Présentation générale 103
7.2.2 Interactions éditeur-abonné 103
7.2.3 Interactions client-serveur 108
7.2.4 Synchronisation temporelle 115

7.2.5 Démarrage de l'appareil 116
7.3 Entité de communications 116
7.3.1 Généralités 116
7.3.2 Gestion de Réseau 116
7.3.3 FMS 116
7.3.4 Pile H1 116
8 Gestion de la couche de communication de sécurité 116
8.1 Présentation générale 116
8.2 Communications SMK 117
8.3 Services FMS 117
8.4 Services SMK 117
8.4.1 Généralités 117
8.4.2 Attribution d'adresse 117
8.4.3 Synchronisation temporelle 117
8.5 Configuration de la couche de communication de sécurité et démarrage 117
8.5.1 Configuration H1 et démarrage 117
8.5.2 FBAP FSCP 1/1 117
8.5.3 Essais 117
9 Exigences système 117
9.1 Voyants et commutateurs 117
9.2 Lignes directrices d'installation 117
9.3 Temps de réponse de la fonction de sécurité 118
9.4 Durée des demandes 118
9.5 Contraintes liées au calcul des caractéristiques des systèmes 118
9.5.1 Taux de messages 118
9.5.2 Niveau SIL 119
9.6 Maintenance 119
9.7 Manuel de sécurité 119
10 Certification 119
Annexe A (informative) Informations supplémentaires pour les profils de communication de sécurité fonctionnelle de protocole CPF 1 120
A.1 Calcul de la fonction de hachage 120
A.2 Conditions de panne issues d'emplacements situés au-delà du bloc de fonctions de sortie 122
Bibliographie 124

Tableau 1 – Exemple de tableau de transitions d'état 80
Tableau 2 – Mesures de sécurité et erreurs de communication possibles 87
Tableau 3 – Types de données utilisés dans le protocole FSCP 1/1 90
Tableau 4 – Comportement d'états d'anomalie 93
Tableau 5 – Etats de l'éditeur 104
Tableau 6 – Tableau d'états de l'éditeur – Transitions reçues 105
Tableau 7 - Tableau d'états de l'éditeur – Transitions internes 105
Tableau 8 – Etats de l'abonné 107
Tableau 9 - Tableau d'états de l'abonné – Transitions reçues 108
Tableau 10 - Tableau d'états de l'abonné – Transitions internes 108
Tableau 11 – Etats du serveur pendant les opérations de lecture 110

Tableau 12 – Transitions reçues pour un serveur FSCP 1/1 pendant les opérations de lecture 111
Tableau 13 – Etats d'un serveur FSCP 1/1 au cours des opérations d'écriture 113
Tableau 14 – Transitions reçues pour un serveur FSCP 1/1 pendant les opérations d'écriture 114
Tableau A.1 - Conditions de panne issues d'emplacements situés au–delà du bloc de fonctions de sortie 123

Figure 1 - Relation entre la CEI 61784–3 et d'autres normes (machines) 69
Figure 2 - Relations entre la CEI 61784–3 et d'autres normes (transformation) 71
Figure 3 – Exemple de diagramme d'états 79
Figure 4 – Utilisation de couleurs dans les figures 80
Figure 5 – Domaine d'application du FSCP 1/1 81
Figure 6 – Architecture du protocole FSCP 1/1 (H1) 84
Figure 7 – Canal noir 84
Figure 8 – Protocole FSCP 1/1 dans l'architecture de système 87
Figure 9 – Appareil H1 FSCP 1/1 88
Figure 10 – Couches de protocole FSCP 1/1 89
Figure 11 - Relation entre le FSCP 1/1 et les autres couches du type 1 de la CEI 61158 89
Figure 12 – Système d'interdiction d'écriture à clé 92
Figure 13 – Système d'interdiction d'écriture à mots de passe 92
Figure 14 – Exemple de communication FSCP 1/1 96
Figure 15 – Exemple de description d'appareils 99
Figure 16 – Illustration du contenu virtuel d'un PDU de sécurité 104
Figure 17 – PDU de sécurité illustrant la duplication des données et l'ajout du CRC 104
Figure 18 – Diagramme de transition d'états pour un éditeur FSCP 1/1 105
Figure 19 – PDU de sécurité illustrant la duplication des données et l'ajout du CRC 106
Figure 20 – Illustration du contenu virtuel d'un PDU de sécurité 106
Figure 21 – Diagramme de transition d'états pour un abonné FSCP 1/1 107
Figure 22 – Illustration du contenu virtuel d'un PDU de sécurité 109
Figure 23 – Illustration du contenu virtuel d'un PDU de sécurité avec sous-index 109
Figure 24 – PDU de sécurité illustrant la duplication des données et l'ajout du numéro de séquence et du CRC 110
Figure 25 – Diagramme de transition d'états pour un serveur FSCP 1/1 pendant les opérations de lecture 111
Figure 26 – PDU de sécurité illustrant la duplication des données et l'ajout du numéro de séquence et du CRC 112
Figure 27 – Exemple d'écriture FSCP 1/1 112
Figure 28 – Exemple d'écriture FSCP 1/1 avec sous-index 113
Figure 29 – Diagramme de transition d'états pour un serveur FSCP 1/1 pendant les opérations d'écriture 114
Figure 30 – PDU de sécurité illustrant la duplication des données et le CRC 115
Figure 31 – Exemple des composantes du temps de réponse de la fonction de sécurité 118

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

RÉSEAUX DE COMMUNICATION INDUSTRIELS – PROFILS –

Partie 3-1: Bus de terrain à sécurité fonctionnelle - Spécifications complémentaires pour le CPF 1

AVANT-PROPOS

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

La commission électrotechnique internationale (CEI) attire l'attention sur le fait qu'il est déclaré que la conformité avec le présent document peut impliquer l'utilisation de brevets concernant les profils de communication de sécurité fonctionnelle pour la famille 1, où la notation [xx] désigne le détenteur des droits de propriété.

US 6,999,824	[FF]	Système et méthode de mise en œuvre des systèmes instrumentés de sécurité dans une architecture de bus de terrain

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

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

Des informations peuvent être obtenues auprès de:

[FF] Fieldbus Foundation

9005 Mountain Ridge Drive
Bowie Bldg. - Suite 190
Austin, TX 78759-5316
USA
Tel: +1 512 794 8890

L'attention est attirée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété autres que ceux mentionnés ci-dessus. La CEI ne doit pas être tenue pour responsable de ne pas avoir dûment signalé tout ou partie de ces droits de propriété.

La Norme internationale CEI 61784-3-1 a été établie par le sous-comité 65C: Réseaux industriels, du comité d'études 65 de la CEI: Mesure, commande et automation dans les processus industriels.

La présente version bilingue (2014-12) correspond à la version anglaise monolingue publiée en 2007-12.

Le texte anglais de cette norme est issu des documents 65C/470/FDIS et 65C/481/RVD.

Le rapport de vote 65C/481/RVD donne toute information sur le vote ayant abouti à l'approbation de cette norme.

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

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

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

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

La liste de toutes les parties de la série CEI 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 la CEI.

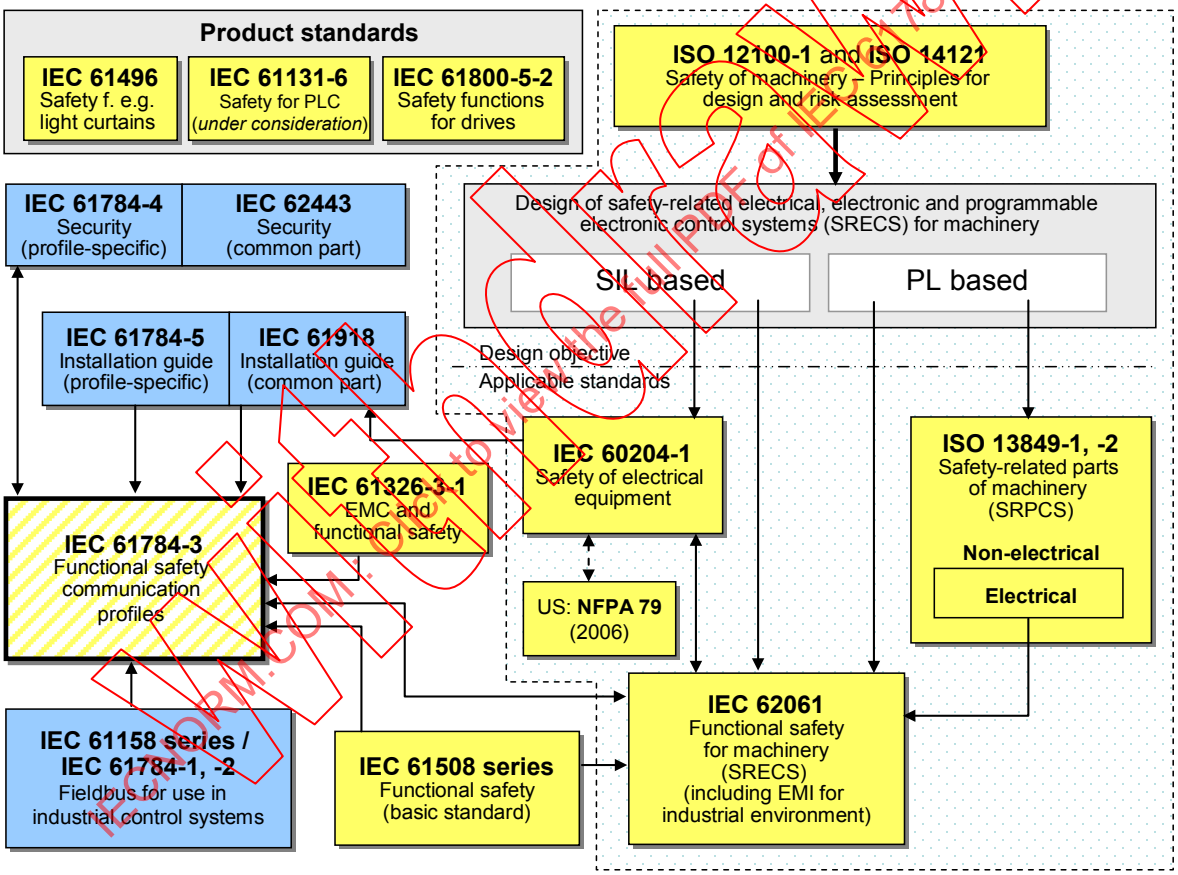
IMPORTANT – Le logo *"colour inside"* qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une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

INTRODUCTION

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

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

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



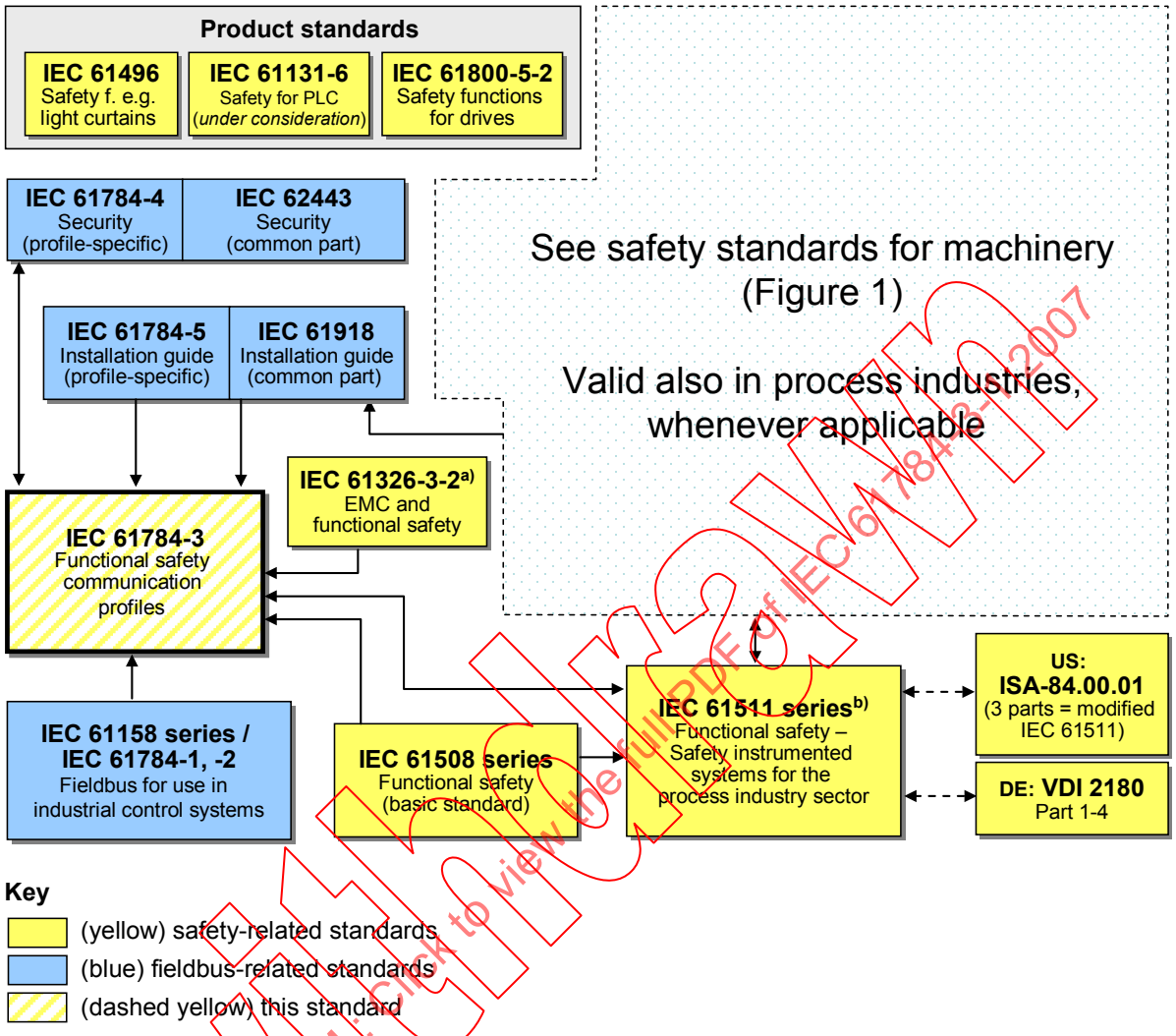
Légende

Anglais	Français
Product standards	Normes de produits
Safety function, e.g. light curtains	Fonction de sécurité, par exemple rideaux de lumière

Anglais	Français
Safety for PLC (under consideration)	Sécurité relative aux automates programmables (à l'étude)
Safety functions for drives	Fonctions de sécurité applicables aux entraînements
Safety of machinery - ... assessment	Sécurité des machines – principes généraux de conception et appréciation du risque
Security (profile-specific)	Sûreté (spécifique au profil)
Security (common part)	Sûreté (partie commune)
Design of safety-related .... for machinery	Conception des systèmes de commande électriques, électroniques et électroniques programmables relatifs à la sécurité pour les machines
SIL based	Basé sur SIL
PL based	Basé sur PL
Installation guide (profile-specific)	Guide d'installation (spécifique au profil)
Installation guide (common part)	Guide d'installation (partie commune)
Design objective	Objectif de conception
Applicable standards	Normes applicables
Safety of electrical equipment	Sécurité des équipements électriques
Safety-related parts of machinery	Parties des systèmes de commande relatives à la sécurité
Non-electrical	Non électrique
Electrical	Électrique
EMC & functional safety	CEM et sécurité fonctionnelle
Functional safety communication profiles	Profils de communication de sécurité fonctionnelle
IEC 61158 series / Fieldbus for use in industrial control systems	Série CEI 61158 / Bus de terrain pour utilisation dans des systèmes de commande industriels
IEC 61508 series, Functional safety (basic standard)	Série CEI 61508 Sécurité fonctionnelle (norme de base)
Functional safety for machinery ... for industrial environment)	Sécurité fonctionnelle des systèmes de commande électriques, électroniques et électroniques programmables (y compris les interférences électromagnétiques dans l'environnement industriel)
Key	Légende
(yellow) safety-related standards	(jaune) normes relatives à la sécurité
(blue) fieldbus-related standards	(bleu) normes relatives au bus de terrain
(dashed) yellow) this standard	(jaune pointillé) la présente norme
IEC	CEI

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

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



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

b EN ratifiée.

Légende

Anglais	Français
Product standards	Normes de produits
Safety function, e.g. light curtains	Fonction de sécurité, par exemple rideaux de lumière
Safety for PLC (under consideration)	Sécurité relative aux automates programmables (à l'étude)
Safety functions for drives	Fonctions de sécurité applicables aux entraînements
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 … applicable	Valable également dans les industries de

Anglais	Français
	transformation, le cas échéant
Functional safety communication profiles	Profils de communication de sécurité fonctionnelle
EMC and functional safety	CEM & sécurité fonctionnelle
IEC 61158 series Fieldbus for use in industrial control systems	Série CEI 61158 Bus de terrain pour utilisation dans des systèmes de commande industriels
IEC 61508 series, Functional safety (basic standard)	Série CEI 61508 Sécurité fonctionnelle (norme de base)
IEC 61511 series Functional safety … sector	Série CEI 61511 sécurité fonctionnelle – systèmes instrumentés de sécurité pour le secteur des industries de transformation
(3 parts = modified IEC 61511)	(3 parties = CEI 61511 modifiée)
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
IEC	CEI

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

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

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

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

La présente norme décrit:

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

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

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

RÉSEAUX DE COMMUNICATION INDUSTRIELS – PROFILS –

Partie 3-1: Bus de terrain à sécurité fonctionnelle - Spécifications complémentaires pour le CPF 1

1 Domaine d'application

La présente partie de la série CEI 61784-3 spécifie une couche de communication relative à la sécurité (services et protocole) fondée sur la CPF 1 de la CEI 61784-1 et les types 1 et 9 de la CEI 61158. Elle identifie les principes applicables aux communications de sécurité fonctionnelle définies dans la CEI 61784-3, et appropriés à cette couche de communication de sécurité.

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

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

La présente partie fournit des lignes directrices tant pour les développeurs que pour les évaluateurs 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 de référence suivants sont indispensables pour l'application du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

IEC 61131-2, *Programmable controllers – Part 2: Equipment requirements and tests* (disponible en anglais seulement)

CEI 61158-2, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 2: Spécification et définition des services de la couche physique*

CEI 61158-3-1, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 3-1: Définition des services de la couche liaison de données – Éléments de type 1*

CEI 61158-4-1, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 4-1: Spécification du protocole de la couche liaison de données – Éléments de type 1*

CEI 61158-5–5, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 5-5: Définition des services de la couche liaison de données – Éléments de type 5*

CEI 61158-5–9, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 5-9: Définition des services de la couche application – Éléments de type 9*

---

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

CEI 61158-6–5, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 6-5: Spécification du protocole de la couche application – Éléments de type 5*

CEI 61158-6–9, *Réseaux de communication industriels – Spécifications des bus de terrain – Part 6-9: Spécification du protocole de la couche application – Éléments de type 9*

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

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

CEI 61784-1, *Réseaux de communication industriels – Profils – Partie 1: Profils de bus de terrain*

CEI 61784-3, *Réseaux de communication industriels – Profils – Partie 3: Bus de terrain de sécurité fonctionnelle – Règles générales et définitions de profil*

IEC 61918, *Industrial communication networks – Installation of communication networks in industrial premises* (disponible en anglais seulement)

CEI 62280-1:2002, *Applications ferroviaires - Systèmes de signalisation, de télécommunication et de traitement – Partie 1: Communication de sécurité sur des systèmes de transmission fermés*

3 Termes, définitions, symboles, abréviations et conventions

3.1 Termes et définitions

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

3.1.1 Termes et définitions communs

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

NOTE La disponibilité dépend de la MTBF (moyenne des temps de bon fonctionnement entre défaillances) et du MDT (temps moyen d'indisponibilité):
Disponibilité = MTBF / (MTBF + MDT).

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

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

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

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

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

<méthode> procédure utilisée pour calculer les données redondantes

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

NOTE 2 Voir également [28], [29][2].

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

NOTE 1 Une erreur peut être causée par une entité en panne, par exemple une erreur de calcul faite par un ordinateur en panne.

[VEI 191-05-24], [CEI 61508-4:1998], [CEI 61158]

NOTE 2 Les erreurs peuvent être causées par des erreurs de conception du matériel/logiciel et/ou des informations altérées du fait de perturbations électromagnétiques et/ou autres effets.

NOTE 3 Les erreurs ne produisent nécessairement pas une *défaillance* ou une *panne*.

3.1.1.9
défaillance
cessation de l'aptitude d'une unité fonctionnelle à accomplir une fonction requise

NOTE 1 La définition du VEI 191-04-01 est identique avec des notes complémentaires.

[CEI 61508-4:1998], [ISO/CEI 2382-14.01.11]

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

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

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

[CEI 61508-4:1998], [ISO/CEI 2382-14.01.10]

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

3.1.1.12
trame
synonyme discrédité de DLPDU

3.1.1.13
séquence de contrôle de trame (FCS - Frame check sequence)
données redondantes issues d'un bloc de données d'un DLPDU (trame), utilisant une fonction de hachage, et enregistrées ou transmises avec le bloc de données, afin de déterminer l'altération des données

NOTE 1 Il est possible de calculer une FCS à l'aide, par exemple, d'un CRC ou d'une autre fonction de hachage.

NOTE 2 Voir également [28], [29].

---

[2] Les chiffres entre crochets font référence à la bibliographie.

3.1.1.14
fonction de hachage
fonction (mathématique) de mise en correspondance des valeurs d'un ensemble (éventuellement) très grand de valeurs en une plage de valeurs (habituellement) plus petite

NOTE 1 Les fonctions de hachage peuvent être utilisées pour déterminer la corruption des données.

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

[CEI 62210, modifiée]

3.1.1.15
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

3.1.1.16
maître
entité de communication active capable d'initier et de programmer des activités de communication effectuées par d'autres stations qui peuvent être des maîtres ou des esclaves

3.1.1.17
message
série ordonnée d'octets destinée à communiquer des informations
[ISO/CEI 2382-16.02.01, modifiée]

3.1.1.18
collecteur de messages
partie d'un *système de communication* destiné à recevoir des *messages*
[ISO/CEI 2382-16.02.03]

3.1.1.19
source de messages
partie d'un *système de communication* destiné à envoyer des *messages*
[ISO/CEI 2382-16.02.02]

3.1.1.20
essai périodique
essai périodique destiné à détecter les défaillances d'un *système relatif à la sécurité* de telle sorte que, lorsque nécessaire, le système puisse être rétabli dans une condition "comme neuf'' ou dans une condition aussi proche que possible de celle-ci

NOTE Un essai périodique est destiné à confirmer que l'état du système relatif à la sécurité garantit l'intégrité de sécurité spécifiée.

[CEI 61508-4 et CEI 62061, modifiée]

3.1.1.21
redondance
existence de moyens, outre les moyens qui se révèleraient suffisants pour qu'une unité fonctionnelle accomplisse une fonction requise ou que des données représentent une information

EXEMPLE Les composantes fonctionnelles dupliquées et l'ajout de bits de parité constituent tous deux des instances de redondance.

NOTE 1 La redondance est principalement utilisée pour améliorer la fiabilité ou la disponibilité.

NOTE 2 La définition dans le VEI 191-15-01 est moins complète.

[CEI 61508-4:1998], [ISO/CEI 2382-14.01.12]

3.1.1.22
fiabilité
probabilité qu'un système automatisé puisse accomplir une fonction requise, dans des conditions données, pendant un intervalle de temps donné (t1, t2)

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

NOTE 2 Le terme “fiabilité” est aussi employé pour désigner l’aptitude caractérisée par cette probabilité.

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

NOTE 4 La fiabilité est différente de la disponibilité.

[CEI 62059-11, modifiée]

3.1.1.23
risque
combinaison de la probabilité d’occurrence d’un dommage ou préjudice et de la gravité de ce dernier

[CEI 61508-4:1998]

3.1.1.24
couche de communication de sécurité (SCL - safety communication layer)
couche de communication qui comprend toutes les mesures nécessaires permettant d’assurer la transmission de données en toute sécurité conformément aux exigences de la CEI 61508

3.1.1.25
données de sécurité
données transmises par un réseau de sécurité utilisant un protocole de sécurité

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

3.1.1.26
appareil de sécurité
appareil conçu conformément à la CEI 61508 et qui met en œuvre le profil de communication de sécurité fonctionnelle

3.1.1.27
fonction de sécurité
fonction qu’un système E/E/PE relatif à la sécurité, autre *système* de technologie *relative à la sécurité* ou d’autres mesures de réduction du risque externe sont tenus de mettre en œuvre, et qui est destinée à atteindre ou à maintenir un état de sécurité de l’équipement commandé, compte tenu d’un événement dangereux spécifique

[CEI 61508-4:1998]

3.1.1.28
temps de réponse de la fonction de sécurité
temps écoulé du cas le plus défavorable suite à l’activation d’un capteur de sécurité relié à un bus de terrain, avant que ne soit atteint l’état de sécurité correspondant de son (ses) actionneur(s) de sécurité, du fait d’erreurs ou de défaillances avérées dans le canal de fonction de sécurité

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

3.1.1.29
niveau d’intégrité de sécurité (SIL - safety integrity level)
niveau discret (un sur quatre niveaux possibles) pour spécifier les exigences d’intégrité de sécurité des fonctions équivalentes à attribuer aux systèmes E/E/PE relatifs à la sécurité, où le niveau d’intégrité de sécurité 4 est le niveau le plus élevé et le niveau d’intégrité de sécurité 1 est le niveau le plus faible

NOTE Les objectifs chiffrés de défaillance pour les quatre niveaux d'intégrité de sécurité sont indiqués dans les Tableaux 2 et 3 de la CEI 61508-1.

[CEI 61508-4:1998]

3.1.1.30
mesure de sécurité
<la présente norme> mesure permettant de contrôler les *erreurs* de communication éventuelles, qui est conçue et mise en œuvre conformément aux exigences de la CEI 61508

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

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

3.1.1.31
application relative à la sécurité
programmes conçus conformément à la CEI 61508 pour satisfaire aux exigences SIL de l'application

3.1.1.32
système relatif à la sécurité
système qui exécute les *fonctions de sécurité* conformément à la CEI 61508

3.1.1.33
esclave
entité de communication passive capable de recevoir des messages et de les envoyer en réponse à une autre entité de communication qui peut être maître ou esclave

3.1.1.34
déclenchement parasite
déclenchement provoqué par le système de sécurité sans injonction du processus

3.1.1.35
horodatage
information temporelle incluse dans un *message*

3.1.2 CPF 1: Termes et définitions supplémentaires

3.1.2.1
client
entité de connexion qui sollicite des informations d'un serveur

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

3.1.2.3
H1
liaison de données de communication standard d'un bus de terrain

3.1.2.4
hôte
unité de traitement de l'information capable d'exécuter les mécanismes de profil de sécurité, et qui dessert le canal noir

3.1.2.5
macro cycle
itération simple du programme de niveau de liaison

3.1.2.6
déguisement
erreur occasionnée par des informations d'identification erronées

3.1.2.7
éditeur
source de message qui transmet des messages de manière régulière

3.1.2.8
mise en file d'attente
traitement séquentiel d'éléments

3.1.2.9
serveur
entité de communication qui traite les messages en provenance d'un client

3.1.2.10
environnement SIL
matériel(s) et logiciel(s) adaptés à des fonctions SIS

3.1.2.11
abonné
collecteur de messages qui reçoit les messages en provenance d'un éditeur

3.2 Symboles et abréviations

3.2.1 Symboles et abréviations communs

CP	Profil de communication (communication profile)	[CEI 61784-1]
CPF	Famille de profils de communication (Communication Profile Family)	[CEI 61784-1]
CRC	Contrôle de redondance cyclique (Cyclic Redundancy Check)	
DLL	Couche liaison de données (Data Link Layer)	[ISO/CEI 7498-1]
DLPDU	Ensemble (Unité) de données de protocole de liaison de données (Data Link Protocol Data Unit)	
EMI	Perturbation électromagnétique (Electro-Magnetic Interference)	
EUC	Équipement commandé (Equipment Under Control)	[CEI 61508-4:1998]
FAL	Couche Application de bus de terrain (Fieldbus Application Layer)	[CEI 61158-5]
FCS	Séquence de contrôle de trame (Frame Check Sequence)	
FSCP	Profil de communication de sécurité fonctionnelle (Functional Safety Communication Profile)	
E/E/PE	Électrique/électronique/électronique programmable (Electrical/Electronic/Programmable Electronic)	[CEI 61508-4:1998]
PDU	Ensemble (unité) de données de protocole (Protocol Data Unit)	[ISO/CEI 7498-1]
PES	Système électronique programmable (Programmable Electronic System)	[CEI 61508-4:1998]
PFD	Probabilité moyenne de défaillance sur sollicitation (Average Probability of Failure on Demand)	[CEI 61508-6:1998]
PFH	Probabilité de défaillance dangereuse [h^{-1}] par heure (Probability of Failure per Hour)	[CEI 61508-6:1998]
PhL	Couche physique (Physical Layer)	[ISO/CEI 7498-1]
PLC	Automate programmable (Programmable Logic Controller)	
SCL	Couche de communication de sécurité (Safety Communication Layer)	
SIL	Niveau d'intégrité de sécurité (Safety Integrity Level)	[CEI 61508-4:1998]
SR	Relatif à la sécurité (Safety Relevant)	

3.2.2 CPF 1: Symboles et abréviations supplémentaires

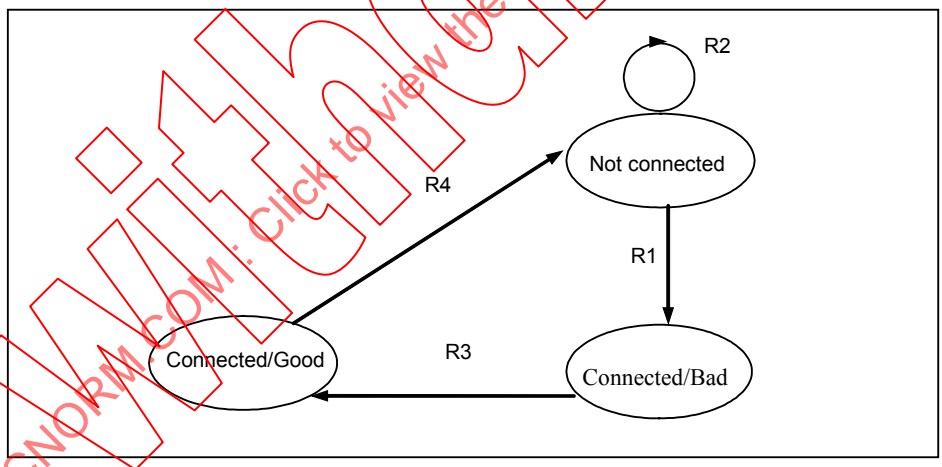
AP	Processus d'Application (Application Process)
ASIC	Circuit intégré à application spécifique (Application Specific Integrated Circuit)
CAS	Cascade
CF	Fichier commun (Common File)
CFF	Format de fichier commun (Common File Format)
DD	Description d'appareil (Device Description)
DO	Sortie numérique (Digital Output)
FBAP	Processus d'application de blocs de fonctions (Function Block Application Process)
FMS	Spécification de messages de bus de terrain (Fieldbus Message Specification)
FIFO	Premier entré, premier sorti (First-In First-Out)
FMS	Spécification de messages de bus de terrain (Field Message Specification)
LAS	Echéancier actif de liaison (Link Active Scheduler)
LO	Neutralisation locale (Local Override)

LRSN	Dernier numéro de séquence reçu (Last Sequence Number Received)
MAU	Unité de Connexion au Support (Medium Attachment Unit)
MD5	Algorithme de résumé de messages 5 (Message Digest Algorithm 5)
MIB	Base d'information de gestion (Management Information Base)
NMA	Agent de gestion de réseau (Network Management Agent)
NMIB	Base d'information de gestion de réseau (Network Management Information Base)
OD	Dictionnaire d'objets (Object Dictionary)
OOS	Hors service (Out Of Service)
SIS	Système instrumenté de sécurité (Safety Instrumented System)
SMIB	Base d'information de gestion de systèmes (System Management Information Base)
SMK	Noyau de gestion de système (System Management Kernel)
SMKP	Protocole de noyau de gestion de système (System Management Kernel Protocol)
VCR	Relation de communication virtuelle (Virtual Communication Relationship)

3.3 Conventions

3.3.1 Diagrammes d'états

La Figure 3 présente un exemple de diagramme d'états utilisé dans la présente partie. Un état est désigné par un ovale comportant le nom de l'état en son centre. Dans la Figure 3, « Non connecté », « Connecté/Correct » et « Connecté/Incorrect » sont tous des états. Une transition est désignée par une ligne ou une courbe comportant une flèche d'indication de sa direction. Une étiquette apposée sur la ligne ou la courbe représente le nom de chaque transition. Dans la Figure 3, "R1", "R2", "R3" et "R4" sont des transitions.



Légende

Anglais	Français
Not connected	Non connecté
Connected/Good	Connecté/Correct
Connected/Bad	Connecté/Incorrect

Figure 3 – Exemple de diagramme d'états

A chaque diagramme d'états est associé un tableau correspondant tel qu'indiqué dans le Tableau 1. La première colonne portant l'étiquette "#" contient le nom de la transition. La deuxième colonne portant l'étiquette « État courant» (''Current state'') contient l'état auquel cette transition s'applique. La troisième colonne portant l'étiquette « Evénement, condition et action » ("Event and condition action") contient l'événement, les conditions de la transition et les actions éventuelles. Les conditions permettent de détailler les actions. Dans le Tableau 1, "RcvMsg() = "FMS Initiate.cnf"" est une condition et "SET Sequence Number = MCN" est une

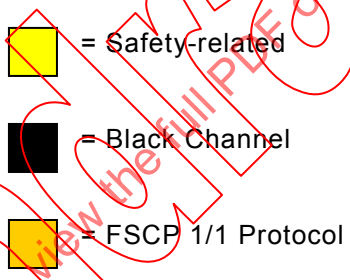
action. La quatrième colonne portant l'étiquette « État suivant » (''Next state'') contient le nouvel état existant après cette transition.

Tableau 1 – Exemple de tableau de transitions d'état

#	État courant	Événement, condition et action	État suivant
R1	Non connecté	RcvMsg() = "FMS Initiate.cnf'' DÉFINIR numéro de séquence = MCN	Connecté/Incorrect
R2	Non connecté	RcvMsg() = "Any message (not FMS Initiate.cnf)''	Identique
R3	Connecté/Incorrect	RcvMsg() = "Abort.ind" OU RcvMsg() = "Abort.req''	Non connecté
R4	Connecté/Correct	RcvMsg() = "Abort.ind" OU RcvMsg() = "Abort.req''	Non connecté

3.3.2 Utilisation de couleurs dans les figures

L'utilisation de couleurs dans les figures n'est aucunement normative : elle permet uniquement une plus grande clarté de la figure. La convention d'utilisation de couleurs est décrite à la Figure 4. Les couleurs non illustrées sont destinées uniquement à permettre une plus grande clarté de la figure.



Anglais	Français
Safety -related	Relatif à la sécurité
Black Channel	Canal noir
FSCP 1/1 Protocol	Protocole FSCP 1/1

Figure 4 – Utilisation de couleurs dans les figures

4 Présentation générale de FSCP 1/1 (FOUNDATION Fieldbus™ SIS)

4.1 Généralités

La famille de profils de communication 1 (communément appelée FOUNDATION™ Fieldbus[3])) définit des profils de communication sur la base du type 1 de la CEI 61158-2, de la CEI 61158-3-1, la CEI 61158-4-1, la CEI 61158-5-5, la CEI 61158-5-9, la CEI 61158-6-5 et la CEI 61158-6-9.

Les profils de base CP 1/1, CP 1/2 et CP 1/3 sont définis dans la CEI 61784-1. Le profil de communication de sécurité fonctionnelle CPF 1 FSCP 1/1 (FF-SIS™[3]) est fondé sur le profil de base CP 1/1 dans la CEI 61784-1 et les spécifications de la couche de communication de sécurité définies dans la présente partie.

---

[3] FOUNDATION™ Fieldbus et FF-SIS™ désignent les appellations commerciales de l'organisme sans but lucratif Fieldbus Foundation. Ces informations sont données pour des raisons de commodité des utilisateurs de la présente norme internationale et ne constituent en aucun cas un entérinement par la CEI du titulaire de la marque ou de l'un de ses produits. La conformité à la présente partie de la CEI 61784-3 n'exige pas d'utiliser les appellations commerciales Foundation Fieldbus™ ou FF-SIS™. L'emploi des appellations FOUNDATION™ Fieldbus ou FF-SIS™ exige l'autorisation de la Fieldbus Foundation.

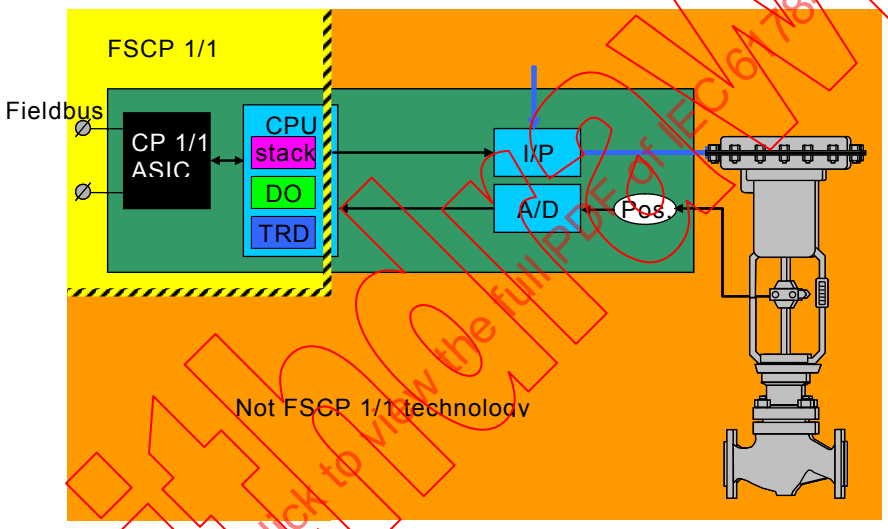
NOTE 1 Les spécifications de FOUNDATION™ Fieldbus AG-180 [37], FF-807 [38], FF-884 [39] et FF-895 [40] s'appliquent à ce protocole.

Certaines applications exigent un niveau d'intégrité de sécurité de un à quatre tel que défini dans la série CEI 61508.

NOTE 2 Ces applications relatives à la sécurité sont également appelées systèmes instrumentés de sécurité (SIS) (voir série CEI 61151).

La couche de communication de sécurité FSCP 1/1 spécifiée dans la présente partie permet d'utiliser des appareils intelligents dans un système relatif à la sécurité en renforçant la capacité de ce dernier. Ledit système peut cependant satisfaire à ses exigences en matière de niveau d'intégrité de sécurité. La couche de communication de sécurité spécifiée dans la présente partie s'applique uniquement au CP 1/1 tel que décrit dans la CEI 61784-1.

La présente partie ne définit aucune exigence concernant les outils techniques ou la fonctionnalité de mesure interne des appareils. La couche de communication de sécurité garantit le téléchargement d'une configuration, créée à l'aide d'un outil technique, dans les appareils de sécurité sans que le protocole n'affecte le niveau d'intégrité de sécurité. Le domaine d'application de la présente partie est défini à la Figure 5.



Légende

Anglais	Français
Fieldbus	Bus de terrain
Not FSCP 1/1 technology	Pas de technologie FSCP 1/1

Figure 5 – Domaine d'application du FSCP 1/1

Le FSCP 1/1 seul ne garantit pas la sécurité fonctionnelle. Outre l'enregistrement de l'interopérabilité du protocole FSCP 1/1, le fournisseur obtiendra également la certification de la sécurité fonctionnelle des produits, systèmes et logiciels. L'utilisateur doit déterminer l'aptitude à l'emploi de tous les matériels relatifs à la sécurité dans la fonction de sécurité conformément à la série CEI 61508.

4.2 Concepts clés du FSCP 1/1

4.2.1 Canal noir

Il s'agit du concept d'utilisation d'un système de communication non validé (par exemple, fils, fibres optiques, répéteur, barrière, ASIC, pile de communication, appareil de liaison, interface) qui permet de fournir un canal de communication fiable. Le canal noir comporte la partie d'un appareil identifiée comme l'entité de communication, ainsi que les SMK et SMKP. Le FSCP 1/1 établit la présence d'anomalies de commande dans le canal noir. Le canal noir peut présenter une défaillance à tout moment, mais les défaillances de communication sont détectées de manière à contrôler les anomalies dans le temps de sécurité du processus. Le diagnostic de détection de défaillances doit satisfaire à la série CEI 61508, contrairement au

canal noir. Le protocole FSCP 1/1 ne repose pas sur le CRC de 16 bits dans la FCS de la couche liaison de données H1.

4.2.2 Clé de connexion

Il s'agit d'un nombre unique pour chaque connexion, une relation source-destination « mot de code », attribuée par l'hôte à chaque objet de liaison de sécurité au moment de la configuration. Contrairement à l'adresse du canal noir, la clé de connexion est protégée par le CRC de la couche de communication de sécurité. La clé de connexion est unique dans la couche de communication de sécurité. En cas de remplacement des appareils, la même clé de connexion peut être réutilisée et téléchargée sur le nouvel appareil. La configuration des appareils, y compris la clé de connexion, est effacée dans un appareil supprimé, avant sa reconnexion sur un réseau FSCP 1/1 dans un autre service. Les appareils peuvent effacer automatiquement leur configuration en cas de modification de l'adresse du canal noir; les appareils peuvent également comporter un bouton de réinitialisation ou équivalent qui permet d'effacer leur configuration.

4.2.3 Contre-vérification

Il s'agit d'une comparaison des données d'application, du numéro de séquence et du CRC qui ont fait l'objet d'une transmission redondante (à deux reprises dans le même message) afin de s'assurer du caractère identique des deux copies.

4.2.4 FSCP 1/1

Le protocole FSCP 1/1 fournit un système de transmission fermé pouvant être utilisé avec un système relatif à la sécurité. Il établit une communication de confiance entre les applications relatives à la sécurité.
(Adapté de la CEI 62280-1).

4.2.5 Système électronique programmable

Il s'agit d'un système de commande, de protection ou de surveillance basé sur un ou plusieurs appareils électroniques programmables. Ce terme recouvre tous les éléments du système, tels que l'alimentation, les capteurs ou autres appareils d'entrée, jusqu'aux actionneurs ou autres appareils de sortie, en passant par les autoroutes de données ou autres voies de communication. La structure d'un PES peut comporter une unité électronique programmable distincte des capteurs et actionneurs de l'EUC et de leurs interfaces, mais l'électronique programmable peut résider en divers autres emplacements du PES.
(Adapté de la CEI 61508-4:1998, 3.3.2).

4.2.6 Retards de mise en file d'attente

Une anomalie éventuelle réside dans le fait que les messages sont conservés dans le canal noir en raison d'une mise en file d'attente dans la pile de communication des appareils ou dans le matériel de réseaux intelligents, y compris les répéteurs, concentrateurs, ponts, commutateurs et appareils de liaison. Des messages édités non confirmés peuvent transiter avec succès par le canal noir, même à une vitesse acceptable, mais peuvent, en raison d'une mise en file d'attente longue ou multiple en divers points de la trajectoire du canal noir, être plus anciens que ce que permet le temps de sécurité du processus. Cette anomalie est un type d'anomalie de retard, ce dernier étant le fait des appareils qui l'introduisent dans les messages de mise en file d'attente dans le canal noir.

4.2.7 Redondance

Utilisation de matériels, logiciels ou données supplémentaires à ceux nécessaires dans un environnement exempt d'erreurs.

EXEMPLE Les composantes fonctionnelles dupliquées et l'ajout de bits de parité constituent tous deux des instances de redondance.

NOTE La redondance permet principalement d'améliorer la fiabilité ou la disponibilité (CEI 61508-4:1998, 3.3.10).

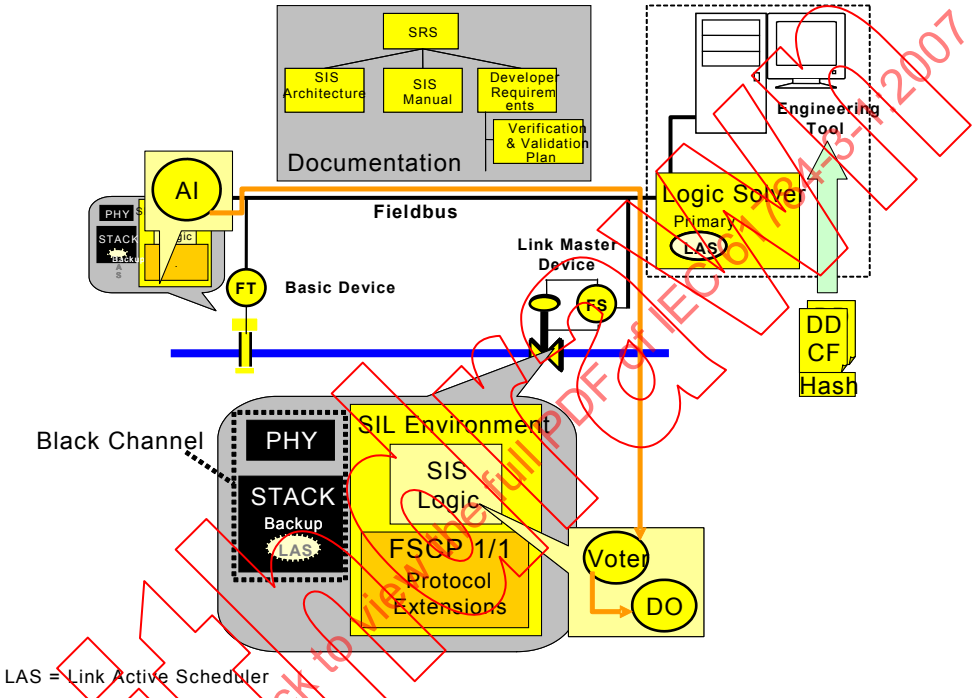
4.2.8 Environnement SIL

Les composants matériels et les composantes logicielles conformes au protocole FSCP 1/1 peuvent être intégrés à un système qui constitue un environnement adapté à la mise en œuvre d'applications relatives à la sécurité.

4.3 Composantes clés du FSCP 1/1

4.3.1 Présentation générale

Le matériel et la pile de communication de bus de terrain ne sont pas validés. Une couche de communication de sécurité placée au-dessus de la pile de communication garantit une communication de confiance sur le bus de terrain, un objet de liaison de sécurité constitutif du FBAP contenant par ailleurs les informations supplémentaires requises par le protocole FSCP 1/1. Ces informations sont présentées à la Figure 6. Dans le cas d'un appareil de sécurité, le processus d'application et la couche de communication de sécurité agissent dans un environnement SIL. Un ensemble de blocs de fonctions simplifiés adaptés aux applications relatives à la sécurité a été créé.



Légende

Anglais	Français
SIS architecture	Architecture SIS
SIS manual	Manuel SIS
Development requirements	Exigences de développement
Verification & Validation Plan	Plan de vérification & validation
PHY	PHYSIQUE
STACK	PILE
Basic Device	Appareil de base
Fieldbus	Bus de terrain
Link Master Device	Appareil maître de liaison
Logic Solver	Résolveur logique
Primary	Primaire
Engineering tool	Outil d'étude
Hash	Hachage
Black Channel	Canal noir
Backup	De secours
SIL Environment	Environnement SIL
SIS logic	Logique SIS

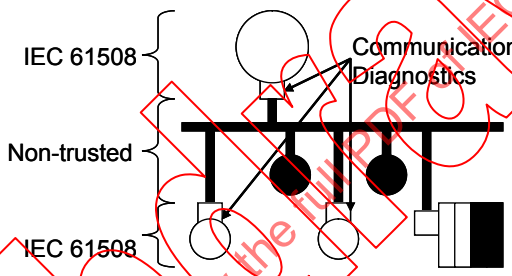
Anglais	Français
Protocol Extensions	Extensions de protocole
LAS = Link Active Scheduler	Echéancier actif de liaison
Voter	Appareil de sélection

Figure 6 – Architecture du protocole FSCP 1/1 (H1)

Le protocole FSCP 1/1 contrôle les défaillances telles que les dysfonctionnements d'appareils ou de fils, ainsi que les perturbations sporadiques telles que les EMI. La couche de communication de sécurité détecte les types suivants d'erreur de communication: répétition, suppression, insertion, reséquencement, corruption des données, processus de déguisement et retard.

4.3.2 Canal noir

Le concept de canal noir tel qu'illustré à la Figure 7 permet la transmission de données de sécurité sur un bus non validé. Aucune séparation physique des fonctions de sécurité et du matériel non relatif à la sécurité n'est nécessaire. Les appareils et données relatifs et non relatifs à la sécurité peuvent partager le bus, tel qu'illustré à la Figure 7.



Légende

Anglais	Français
IEC	CEI
Non-trusted	Non fiable
Communication Diagnostics	Diagnostics de communication

Figure 7 – Canal noir

Un seul LAS est admis sur un réseau H1. Un même appareil peut comporter des applications relatives et non relatives à la sécurité. Une transmission FSCP 1/1 est logiquement séparée d'une transmission autre que FSCP 1/1. Une configuration monocanal, à savoir un bus non redondant, est suffisante. Un appareil de sécurité peut fournir tant des blocs de fonctions relatives à la sécurité que non relatives à la sécurité. Le protocole FSCP 1/1 est utilisé avec des liaisons de blocs de fonctions de sécurité. Un protocole CP 1/1 normal est utilisé avec des liaisons de blocs de fonctions non relatives à la sécurité. Un appareil de sécurité peut ainsi être utilisé pour des fonctions de sécurité et non relatives à la sécurité.

Les défaillances peuvent résulter d'effets autres que les défaillances réelles des composants matériels (par exemple, perturbations électromagnétiques, erreurs de décodage). Toutefois, on considère que des défaillances de cette nature sont des défaillances aléatoires du matériel.
(Adapté de la CEI 61508-2:, 7.4.3.2.2).

Une redondance de bus de secours automatique peut être utilisée pour améliorer la disponibilité. Il est prévu d'utiliser un canal unique entre les instruments et un résolveur logique. Il est prévu d'utiliser des canaux redondants pour une communication entre résolveurs logiques.

4.4 Relation avec le modèle de référence de base OSI de l'ISO

La couche de communication de sécurité est mise en œuvre au-dessus de la pile de communication dans la couche application.

5 Généralités

5.1 Documents externes de spécifications applicables au profil

Les documents suivants fournissent des spécifications supplémentaires qui peuvent se révéler appropriées pour la conception du protocole FSCP 1/1:

- FOUNDATION™ Fieldbus AG-180 [37];
- FOUNDATION™ FIELDBUS FF-807 [38];
- FOUNDATION™ FIELDBUS FF-884 [39];
- FOUNDATION™ FIELDBUS FF-895 [40].

5.2 Exigences de sécurité fonctionnelle

5.2.1 Exigences relatives à la sécurité fonctionnelle

La liste ci-dessous contient les exigences de sécurité fonctionnelle qui s'appliquent dans le développement du protocole FSCP 1/1.

- Le FSCP 1/1 doit être conçu de manière à permettre aux fournisseurs de développer des produits adaptés à une utilisation dans les applications SIL 2 (CEI 61508). Un niveau SIL 3 est recommandé.
- Le protocole doit prendre en charge la connexion éditeur/abonné et client/serveur.
- Le protocole relatif à la sécurité doit éviter les perturbations dues aux appareils non relatifs à la sécurité. Par exemple, une unité portative non relative à la sécurité ne doit pas être admise pour modifier les paramètres d'un appareil relatif à la sécurité.
- Le protocole doit assurer une protection contre les changements de configuration involontaires ou non autorisés d'un appareil de sécurité.
- La contribution du protocole FSCP 1/1 au protocole PFD/PFH doit être inférieure à 1% de la valeur requise par le niveau SIL.
- Les calculs PFD/PFH doivent être basés sur les modes à sollicitation et à sollicitation élevée (tel que défini dans la CEI 61508).
- Le protocole doit mettre en œuvre les mesures visant à contrôler les anomalies suivantes:
  - défaillance/falsification des bits de transmission;
  - retransmission;
  - omission;
  - insertion/extension;
  - ordre erroné;
  - retard;
  - défaillances d'adressage/processus de déguisement;
  - mise en file d'attente.

  NOTE Une anomalie de mise en file d'attente est une anomalie de retard.
- Le temps de réaction de l'application doit pouvoir être calculé.
- La mise en œuvre des blocs de fonctions doit être conforme à la CEI 61508-3 au niveau SIL requis.
- Le même réseau doit pouvoir comporter des appareils avec des niveaux SIL différents.
- Le contournement sécurisé des appareils doit être possible.

5.2.2 Contraintes de fonctionnement

La liste ci-dessous contient les contraintes de fonctionnement qui s'appliquent dans le développement du protocole FSCP 1/1.

- Il doit être possible d'utiliser des communications sécurisée et normale au moyen d'appareils standard et de sécurité avec le même protocole CP 1/1.
- Les ASIC, pile de communication, répéteurs, accessoires de câblage, alimentations et autres accessoires doivent rester des fonctions de sécurité non modifiées (canal noir) au-dessus de la couche OSI 7.
- Le protocole doit comporter des mécanismes permettant à l'hôte de détecter une désadaptation du type ou de la révision d'appareils, de la révision DD, de la révision du fichier de capacités ou du niveau SIL.

5.2.3 Exigences du fabricant d'appareils

La liste ci-dessous constitue les exigences que le FSCP 1/1 impose au fournisseur d'appareils.

- conditions environnementales et sécurité électrique conformément aux exigences de la CEI 61131-2.
- Le matériel doit être conforme à la CEI 61508-2 au niveau SIL requis.
- Le logiciel doit être conforme à la CEI 61508-3 au niveau SIL requis.
- La certification du matériel et du logiciel doit être effectuée par un organisme d'essai compétent conformément aux spécifications de la CEI 61508-1 à la CEI 61508-7.

5.3 Mesures de sécurité

5.3.1 Numéro de séquence

Chaque ensemble de données de protocole de sécurité comporte un numéro de séquence incrémentiel qui est le numéro de macro cycle de génération du message.

5.3.2 Datation (horodatage)

Le numéro de séquence inclus dans l'ensemble de données de protocole de sécurité constitue également une datation, dans la mesure où il représente le numéro de macro cycle.

5.3.3 Délai

Le numéro de séquence la datation permet de vérifier la livraison des messages en temps utile. Il existe également un compteur d'état pour chaque connexion qui détecte le moment où les messages n'ont pas été reçus dans les délais prévus.

5.3.4 Authentification de connexion

Il existe une clé de connexion associée à chaque connexion qui permet de vérifier qu'un ensemble de données de protocole de sécurité provient de la source de message correcte.

5.3.5 Assurance d'intégrité des données

Chaque ensemble de données de protocole de sécurité comporte un CRC visant à assurer l'intégrité des données.

5.3.6 Redondance avec contre-vérification

Chaque ensemble de données de protocole de sécurité comporte deux copies des données et du CRC. La duplication des données et du CRC permet la contre-vérification des données.

5.3.7 Différents systèmes d'assurance d'intégrité des données

L'ensemble de données de protocole de sécurité comporte des CRC supplémentaires différents du système d'intégrité des données du canal noir.

5.3.8 Relations entre les erreurs et les mesures de sécurité

Les mesures de sécurité spécifiées de 5.3.1 à 5.3.7 peuvent être associées à l'ensemble d'erreurs possibles. Cette relation est illustrée dans le Tableau 2. Chaque mesure de sécurité

peut assurer une protection contre une ou plusieurs erreurs de transmission. Il doit être démontré qu'il existe au moins une mesure de sécurité ou une combinaison de mesures de sécurité correspondante pour les erreurs possibles définies conformément au Tableau 2.

Tableau 2 – Mesures de sécurité et erreurs de communication possibles

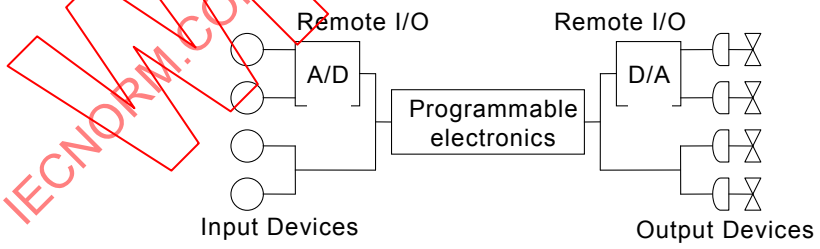
Erreurs de communication	Mesures de sécurité							
	Numéro de séquence	Datation	Délai	Authentification de connexion	Message de réaction	Assurance d'intégrité des données	Redondance avec contre-vérification	Différents systèmes d'assurance d'intégrité des données
Corruption						X	X	
Répétition non prévue	X	X						
Séquence incorrecte	X	X						
Perte	X							
Retard inacceptable		X	X					
Insertion	X							
Déguisement								X
Adressage				X				
NOTE Tableau adapté de la CEI 61784-3.								

5.4 Structure de la couche de communication de sécurité

5.4.1 Topologie de réseau et connectivité des appareils

5.4.1.1 Généralités

Les appareils relatifs et non relatifs à la sécurité peuvent partager le même bus de terrain, tel qu'illustré à la Figure 8. La fonction de sécurité complète entre le capteur et l'actionneur doit être prise en compte. La liaison de bus de terrain est conçue pour ne pas consommer plus de 1% du budget PFD.



Légende

Anglais	Français
Remote I/O	E/S distant
Programmable electronics	Electronique programmable
Input Devices	Appareils d'entrée
Output Devices	Appareils de sortie

Figure 8 – Protocole FSCP 1/1 dans l'architecture de système

NOTE La figure indique une disposition centrale de l'électronique programmable, divers autres emplacements dans le PES étant toutefois possibles.

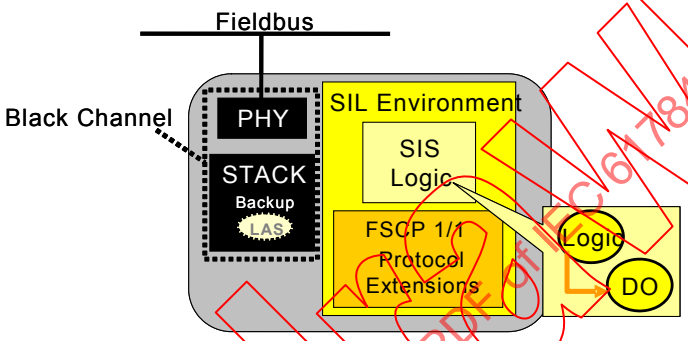
5.4.1.2 Topologie de liaison H1 simple

Une fonction de sécurité consiste en une liaison H1 simple. La liaison fait partie intégrante du canal noir. Les appareils de sécurité et les appareils H1 non relatifs à la sécurité sont mis en réseau de manière identique.

5.4.2 Architecture des appareils

5.4.2.1 Généralités

Le concept de canal noir permet à la pile câblée de communication (y compris ASIC et MAU) et de logiciel de communication de ne pas être validée, tandis que les communications de protocole FSCP 1/1 analysent et l'application de blocs de fonctions opère dans un environnement SIL composé de logiciel et de matériel SIL. La couche de communication de sécurité est l'interface entre le processus d'application SIL et l'entité de communication de canal noir non validée, tel qu'illustré à la Figure 9.



Légende

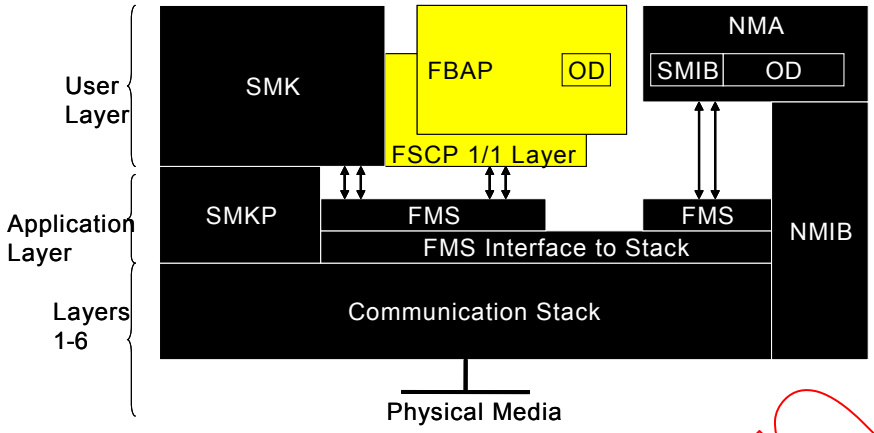
Anglais	Français
Fieldbus	Bus de terrain
Black Channel	Canal noir
PHY	PHYSIQUE
STACK	PILE
Backup	De secours
SIL Environment	Environnement SIL
SIS Logic	Logique SIS
Logic	Logique
Protocol Extensions	Extensions de protocole

Figure 9 – Appareil H1 FSCP 1/1

Une attention toute particulière est à porter à la mise en œuvre du concept de canal noir, afin de s'assurer que le matériel et le logiciel non SIL n'influencent pas le matériel et le logiciel SIL.

5.4.2.2 Architecture des appareils H1

Les processus d'application sont relatifs à la sécurité et exécutés dans un environnement SIL. L'entité de communications comprend la pile de communication, ainsi que les FMS, NMA et NMIB non validés. L'entité de communication, ainsi que les SMK et SMKP, font partie intégrante du canal noir. Leur relation est illustrée à la Figure 10.



Légende

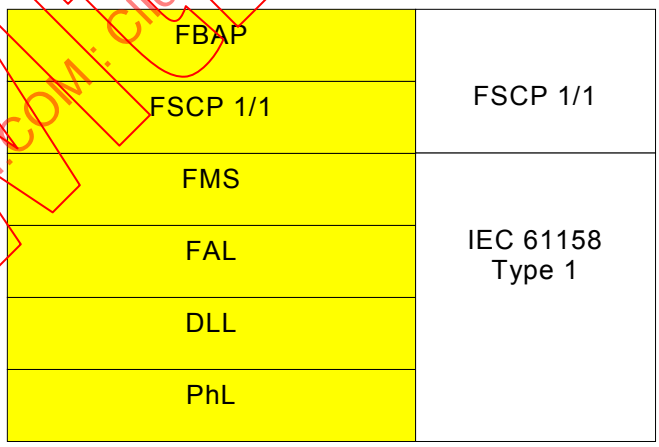
Anglais	Français
User Layer	Couche utilisateur
Application Layer	Couche application
Layers	Couches
FSCP 1/1 Layer	Couche FSCP 1/1
FMS Interface to Stack	Interface FMS vers la pile
Communication Stack	Pile de communication
Physical Media	Supports physiques

Figure 10 – Couches de protocole FSCP 1/1

5.5 Relations avec la FAL (et DLL, PhL)

5.5.1 Généralités

La Figure 11 illustre la relation entre le FSCP 1/1 et les autres couches du type 1 de la CEI 61158.



Légende

Anglais	Français
IEC 61158 Type 1	Type 1 défini dans la CEI 61158

Figure 11 - Relation entre le FSCP 1/1 et les autres couches du type 1 de la CEI 61158

5.5.2 Types de données

Le protocole FSCP 1/1 utilise les types de données de base énumérés dans le Tableau 3 selon le CPF 1 spécifié dans la CEI 61784-1.

Tableau 3 – Types de données utilisés dans le protocole FSCP 1/1

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

6 Services de la couche de communication de sécurité

6.1 Processus d'Application (AP)

6.1.1 Présentation générale

Les fonctions de sécurité et non relatives à la sécurité peuvent être affectées aux mêmes processus d'application, ou à des processus différents, d'un appareil. Le processus d'application relatif aux fonctions de sécurité exige un environnement SIL et ne fait pas partie intégrante du canal noir.

La couche FSCP 1/1 est indépendante du processus d'application et peut par conséquent être utilisée avec le processus d'application des blocs de fonctions ou un autre type de processus d'application.

6.1.2 Objets visibles de réseau

Le processus d'application accède à la couche application de la pile de communication du canal noir, non de manière directe, mais par l'intermédiaire de la couche FSCP 1/1.

6.1.3 Interface de couche application

Le même ensemble de services de messages fourni par la FMS pour les objets non relatifs à la sécurité est également fourni par la couche de communication de sécurité pour les objets de même nature.

6.1.4 Dictionnaire d'objets

La prise en charge du canal noir ne nécessite aucune modification du dictionnaire d'objets de bus de terrain.

6.1.5 Répertoire de programmes d'application

La prise en charge du canal noir ne nécessite aucune modification du répertoire de programmes d'application.

6.2 Processus d'application de blocs de fonctions

6.2.1 Généralités

Les blocs de fonctions simples ont été définis et sont adaptés à des applications relatives à la sécurité. Un FBAP contenant des objets de sécurité opèrera dans un environnement SIL.

L'utilisation des blocs de fonctions est facultative. Un hôte ne mettra probablement pas en œuvre de blocs de fonctions.

6.2.2 Modèle de blocs de fonctions

6.2.2.1 Comptage des données périmées

La vérification de comptage des données périmées de bout en bout, basée sur la désadaptation des numéros de séquences, contrôle les anomalies de programmation et d'exécution de la chaîne logique jusqu'au bloc de fonctions de sortie. Un temporisateur de données périmées en aval du bloc de fonctions de sortie contrôle les anomalies de programmation et d'exécution du bloc de fonctions de sortie proprement dit. La sortie passe à l'état d'anomalie en l'absence de toute actualisation du bloc de fonctions de sortie dans le délai fixé, en raison d'une erreur de programmation ou d'exécution. L'utilisation d'un temporisateur de données périmées en aval du bloc de fonctions de sortie est une mesure de sécurité indépendante du SMK non SIL qui vérifie la bonne exécution des blocs de fonctions. Les sorties ne sont pas diffusées vers le canal noir en cas de non-fonctionnement d'un bloc. L'absence d'édition constitue une anomalie contrôlée en aval, la désadaptation des numéros de séquence occasionnant par ailleurs une action préconfigurée en réaction à un état d'anomalie. Le numéro de séquence propre à la liaison utilisée dans le protocole FSCP 1/1 est calculé à partir du numéro de macro cycle, sur la base du temps de liaison des données, et change par conséquent pour tout nouveau PDU fourni au canal noir. En cas de mauvais comportement du canal noir, ce dernier éditant par ailleurs des données anciennes, le numéro de séquence ne correspond pas et permet ainsi de détecter ce type d'anomalies en aval.

Le mécanise de comptage des données périmées de bout en bout détecte des anomalies telles que: interruption d'exécution des blocs de fonctions, exécution dans un ordre erroné, au mauvais moment ou avec une gigue trop importante. Ces anomalies peuvent être occasionnées par des erreurs de programmation, des anomalies du bloc de fonctions proprement dit ou présenter une durée plus longue que le temps d'exécution des blocs de fonctions le plus défavorable prévu.

6.2.2.2 Simulation

Le système d'interdiction d'écriture dans le bloc de ressources et la protection contre la simulation sont désactivés pour permettre une simulation. La réactivation du système d'interdiction d'écriture entraîne la désactivation automatique de la simulation. De plus, l'activation de la simulation est nécessaire pour intégrer la mémoire non volatile. La mise sous tension provoque toujours la désactivation de la simulation.

L'activation de la simulation provoque le déclenchement d'une alarme de fonctionnement non relative à la sécurité. L'hôte est tenu d'effectuer un contrôle régulier afin de déterminer toute activation effective de la simulation dans l'un des appareils.

6.2.2.3 Système d'interdiction d'écriture

Un système d'interdiction d'écriture protège la configuration des périphériques. Le réglage du système d'interdiction d'écriture dans le bloc de ressources de l'appareil de sécurité entraîne la désactivation de tous les systèmes d'écriture dans ledit bloc, ce qui comprend la MIB mais exclut le système d'interdiction d'écriture proprement dit. Le contenu protégé de la MIB comprend l'objet (blocs, liaisons, VCR), l'adresse, les paramètres et l'étiquette d'identification des périphériques.

Un bloc de fonctions du verrou de sécurité intégré à chaque appareil de sécurité est capable d'écrire des données dans le paramètre de l'appareil d'interdiction d'écriture, dans le bloc de ressources du même appareil. Le bloc de fonctions du verrou de sécurité comporte une entrée de système d'interdiction d'écriture qui accepte une liaison de blocs de fonctions de sécurité. Ceci permet d'activer ou de désactiver à distance les systèmes d'écriture vers plusieurs appareils, et ce, à partir d'un poste central. Le bloc de fonctions du verrou de sécurité peut activer et désactiver le système d'interdiction d'écriture dans l'appareil à l'aide d'un commutateur à clé placé sur un bloc de fonctions DI. La Figure 12 présente l'architecture de ce verrou.

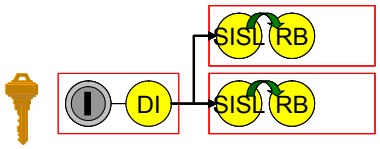


Figure 12 – Système d'interdiction d'écriture à clé

L'écriture d'un paramètre dans le bloc de fonctions du verrou de sécurité permet également d'activer et de désactiver le système d'interdiction d'écriture. L'existence de mots de passe appropriés dans l'hôte permet habituellement de protéger l'écriture de ce paramètre. La Figure 13 présente l'architecture de ce verrou.

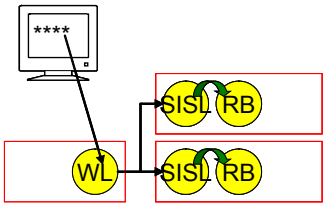


Figure 13 – Système d'interdiction d'écriture à mots de passe

6.2.2.4 Déclenchement et réinitialisation

Pour le bloc de fonctions de sortie FSCP 1/1, la configuration de l'état d'anomalie peut être la suivante: mise hors tension pour déclenchement ou mise en tension pour déclenchement. La dernière valeur affectée peut également être conservée. Si le statut de l'entrée cascade d'un bloc de fonctions de sortie est « Incorrect », par exemple suite à la perte d'une communication, ce caractère incorrect se traduit également par un sous-statut non spécifique « Incorrect » de la sortie de réaction de ce même bloc. La sortie physique peut déclencher, sur injonction authentique du processus du résolveur logique, une erreur d'exécution de bloc de fonctions logique, de communication ou amont, et ce, par l'intervention de l'opérateur ou suite à une panne de périphérique.

Il existe une différence entre l'action préconfigurée en réaction à un état d'anomalie, en réponse à une injonction du processus, une erreur d'exécution de blocs de fonctions de communication ou aval et un déclenchement dû à une anomalie de périphérique et d'alimentation. Suite à une injonction du processus, le bloc de fonctions de sortie agit sur son signal d'entrée, où zéro (0) désigne toujours une action préconfigurée en réaction à un état d'anomalie, et un (1) désigne toujours une autorisation (OK) de fonctionnement. Pour l'état « mise en tension pour déclenchement », le signal est inversé dans le bloc de fonctions de sortie. Suite à une erreur de communication, le bloc de fonctions de sortie n'entreprend aucune action jusqu'à l'expiration du temps d'exécution de l'état d'anomalie, puis il conserve sa dernière position ou adopte la valeur d'anomalie établie par l'option d'état d'anomalie et la valeur d'état d'anomalie.

En fonctionnement normal, le bloc de fonctions de sortie est en mode cascade. Par défaut, le mode demeure en cascade sur une injonction du processus. La sortie peut, de manière facultative, être verrouillée dans son état d'anomalie pour l'injonction du processus et pour l'erreur de communication. Lors de l'activation de l'option d'état d'anomalie du type verrou et d'une injonction du processus ou de l'occurrence d'une erreur de communication, le bloc de fonctions DO passe en mode neutralisation locale (LO). Même en cas de suppression de la condition d'injonction ou d'anomalie, la sortie conserve son état d'anomalie jusqu'à réinitialisation par l'utilisateur. Un résolveur logique peut contrôler l'accès de la sortie de réaction du bloc de fonctions de sortie, et signaler le cas échéant tout statut « Incorrect ». Si cet accès est verrouillé, l'opérateur le déverrouille, soit par la suppression de l'état d'anomalie du bloc de ressources, soit par l'entrée de réinitialisation du bloc de fonctions de sortie. La configuration éventuelle d'un appareil pour un état d'anomalie de mise hors tension peut s'opérer, par exemple, par l'ouverture ou la fermeture d'une soupape. Le Tableau 4 énumère les exemples de comportement possible.

Si le statut d'entrée est Incorrect ou Correct: État d'anomalie initié (Bad or Good::Initiate-fault-state), la sortie exécute également une action préconfigurée en réaction à un état d'anomalie.

Tableau 4 – Comportement d'états d'anomalie

Condition	Exemple	Retard d'état d'anomalie DO	Option d'état d'anomalie DO	Verrou d'état d'anomalie DO	Remarque
Statut incorrect, erreur d'exécution de communication ou de bloc de fonctions amont	Statut incorrect de l'entrée en cascade en raison d'une défaillance CRC de la couche de communication de sécurité, d'une désadaptation des numéros de séquence ou d'une erreur de comparaison de la contre-vérification de redondance	Oui	Mis en tension		
Mise hors tension					
Maintien	Mode LO facultatif				
État d'anomalie initié	Réception de sous-statut d'un autre bloc de fonctions ou résolveur logique	Oui	Mis en tension		
Mise hors tension					
Maintien	Mode LO facultatif				
Intervention de l'opérateur	Définir l'état d'anomalie à partir du bloc de ressources	Non	Mis en tension		
Mise hors tension					
Maintien	Mode LO en continu				
Injonction du processus provenant du résolveur logique	L'entrée en cascade discrète est nulle (0)	Non	Non	Mode LO facultatif	Habituellement mode CAS
Défaillance du canal noir	Erreur de synchronisation temporelle	Oui	Mis en tension		
Mise hors tension					
Maintien	Mode LO facultatif				

Sous réserve de la suppression de la condition d'exécution de l'action préconfigurée en réaction à un état d'anomalie, l'utilisateur peut réinitialiser la sortie verrouillée à l'aide du paramètre d'état d'anomalie de libération dans le bloc de ressources ou d'une entrée d'état d'anomalie de libération dans le bloc de fonctions de sortie proprement dit.

6.2.3 Processus d'Application

6.2.3.1 Généralités

Des blocs de fonctions FSCP 1/1 standard ont été définis. Les fabricants peuvent créer des blocs de fonctions de sécurité améliorés et personnalisés. Des numéros de profils compris dans une gamme spécifiée permettent d'identifier tous les blocs FSCP 1/1. Ceci permet à l'hôte d'interagir avec les blocs FSCP 1/1 si nécessaire.

6.2.3.2 Types de blocs

6.2.3.2.1 Généralités

Des blocs de fonctions standard et un bloc de ressources supplémentaires ont été créés pour le protocole FSCP 1/1/. Les numéros de profils compris dans une gamme spécifiée permettent d'identifier les blocs de fonctions FSCP 1/1 standard. Les blocs de fonctions FSCP 1/1 comportent un nombre réduit d'options de modes et de paramètres admis par rapport à leurs blocs homologues réguliers. Le mode manuel est admis uniquement lorsque le système d'interdiction d'écriture de l'appareil n'est pas activé, le même principe s'appliquant au mode automatique pour les blocs de fonctions de sortie. En cas de déverrouillage des systèmes d'écriture des périphériques, les modes des blocs de fonctions passent en modes fonctionnement automatique et en cascade respectivement.

Un comportement d'état d'anomalie est obligatoire dans les blocs de fonctions de sortie de sécurité.

6.2.3.2.2 Bloc de ressources de l'appareil de sécurité

Le paramètre d'interdiction d'écriture du bloc de ressources comporte la fonction importante d'un mécanisme de verrouillage qui empêche toute écriture sur l'ensemble dudit bloc.

Le bloc de ressources de l'appareil de sécurité permet d'avoir accès aux statistiques actuelles de la couche de communication de sécurité. Les statistiques du protocole FSCP 1/1 consistent en un appareil de comptage du nombre d'anomalies CRC détectées de la couche de communication de sécurité.

Les statistiques de la couche de communication de sécurité comportent également un paramètre d'erreur du canal noir avec un drapeau indiquant l'occurrence d'une anomalie de synchronisation temporelle.

Le bloc de ressources de l'appareil de sécurité comporte un paramètre de déverrouillage de la protection en écriture de l'appareil. Le déverrouillage intervient préalablement à l'écriture des paramètres et d'autres objets. Le bloc de fonctions du verrou de sécurité simplifie le verrouillage et le déverrouillage des systèmes d'écriture dans plusieurs appareils.

Le bloc de ressources de l'appareil de sécurité comporte un paramètre de neutralisation de toutes les sorties déclenchées dont le verrouillage a été effectué dans des conditions d'état d'anomalie.

Le bloc de ressources de l'appareil de sécurité comporte un paramètre de durée de macro cycle, dans la mesure où les données du canal noir ne sont pas fiables.

Ce même bloc de ressources comporte des paramètres d'information de la révision du matériel et du micrologiciel, ainsi que des sommes de contrôle pour le micrologiciel et la configuration.

6.2.3.2.3 Blocs de fonctions supplémentaires

6.2.3.2.3.1 Généralités

Les applications de sécurité requièrent des entrées, des sorties et des éléments logiques. Un nouvel ensemble de blocs de fonctions de sécurité fournissant ces capacités est par conséquent fourni. Les nouveaux blocs de fonctions de sécurité comportent:

- une entrée analogique de sécurité;
- une entrée discrète de sécurité;
- un verrou de sécurité;
- une sortie discrète de sécurité;
- une logique de sécurité;
- un comparateur analogique de sécurité.

La fonctionnalité des blocs de fonctions SR-AI, SR-DI et SR-DO est réduite par comparaison avec celle de leurs homologues réguliers, de manière à simplifier la certification par les

ingénieurs d'application, à réduire les erreurs et à faciliter la vérification par les utilisateurs. La simplification comprend un nombre restreint de modes pris en charge et l'absence de toute alarme.

6.2.3.2.3.2 Blocs de fonctions de sortie de sécurité

Les blocs de fonctions de sortie de sécurité ont leur importance dans la mesure où ils sont présents lors de l'exécution de l'action préconfigurée en réaction à un état d'anomalie. Outre l'action préconfigurée en réaction à un état d'anomalie exécutée à réception de la valeur d'injonction du processus au niveau de l'entrée en cascade, le bloc de fonctions de sortie exécute également ce type d'action en réaction à un statut incorrect, un état d'anomalie initié, une erreur d'exécution de bloc de fonctions en amont et une communication périmée. Le transducteur de sortie se déclenche suite à la défaillance de son bloc de fonctions de sortie associé dans la fonction de sécurité à exécuter. Le transducteur de sortie contrôle, par déclenchement, les anomalies de programmation et de communication de la fonction de sécurité, si celle-ci n'a pas été actualisée avec de nouvelles données dans le paramétrage du temporisateur des données périmées. Lorsque le bloc de fonctions de sortie exécute une action préconfigurée en réaction à un état d'anomalie sur injonction authentique du processus, ou suite à une anomalie de statut ou de communication, le mode reste par défaut en cascade. Les blocs de fonctions de sortie de sécurité comportent une fonctionnalité facultative permettant le verrouillage des sorties déclenchées. Une sortie de réaction du bloc de fonctions de sortie indique l'état « Incorrect: statut non spécifique » si l'entrée en cascade comporte une communication incorrecte. Le statut reflète également les autres anomalies de la sortie. Une alarme non relative à la sécurité peut le cas échéant être émise en cas d'état d'anomalie si l'appareil la prend en charge. Le statut de réaction et les détails d'alarme indiquent si l'état d'anomalie est une injonction authentique du processus ou résulte d'une anomalie. Le paramètre de mode du bloc de fonctions de sortie permet de déterminer si la sortie présente un état d'anomalie, au moyen d'une communication FSCP 1/1. Il est possible de neutraliser une sortie verrouillée individuelle en utilisant un paramètre d'entrée de réinitialisation dans chaque bloc de fonctions de sortie. L'entrée de réinitialisation accepte une liaison de blocs de fonctions de sécurité, permettant ainsi la réinitialisation de l'état d'anomalie à distance et par le biais des éléments logiques d'un autre bloc de fonctions. Toutes les sorties déclenchées peuvent être neutralisées par un paramètre contenu dans le bloc de ressources.

Il est prévu de mettre en œuvre les diagnostics des soupapes de deuxième niveau, tels que les essais de frappe partielle, réaction de position analogique sur les soupapes discrètes et alarmes d'écart de position, dans les blocs de transducteurs par des moyens spécifiques au fournisseur. Les équipes futures de création de profils de blocs de transducteurs peuvent définir des paramètres standard pour ces appareils.

6.2.3.2.3.3 Bloc de fonctions du verrou de sécurité

Le bloc de fonctions du verrou de sécurité déverrouille le système de protection en écriture sur la base des entrées de liaison, activant le verrouillage et le déverrouillage centraux de plusieurs appareils.

Le bloc de ressources est déverrouillé avant l'écriture des paramètres. Ceci équivaut à une clé de verrouillage installée sur un pupitre de sécurité. En raison du grand nombre potentiel d'appareils de sécurité, installés souvent dans des zones dangereuses non pratiques, voire inaccessibles, une communication FSCP 1/1 permet le verrouillage et le déverrouillage. La présence d'un système d'interdiction d'écriture souple est obligatoire dans le bloc de ressources de sécurité.

6.2.3.2.4 Objet de liaison de sécurité

Il comporte les extensions du protocole FSCP 1/1. Un objet de liaison différent de stockage des informations supplémentaires est utilisé pour les liaisons de blocs de fonctions FSCP 1/1. L'objet de liaison de sécurité contient la clé de connexion et la limite de comptage des données périmées de bout en bout requises pour les applications de sécurité. Des chaînes de fonctions de sécurité indépendantes multiples peuvent exister sur le même réseau ou le même appareil ou résolveur logique. La défaillance d'une chaîne de fonctions de sécurité ne doit pas nécessiter un arrêt des autres chaînes de fonctions de sécurité sur le même bus ou dans les mêmes appareils ou résolveur logique. Pour assurer l'interopérabilité avec des

matériels existants dans des applications non relatives à la sécurité, il est obligatoire qu'un appareil prenne également en charge l'objet de liaison non relatif à la sécurité.

6.2.3.2.5 Temporisateur de données périmées

Le mécanisme de comptage des données périmées de bout en bout reçoit les erreurs d'exécution des blocs de fonctions jusqu'à, mais non compris, le bloc de fonctions de sortie. Un second mécanisme, le temporisateur de données périmées, déclenche la sortie si le bloc de transducteurs de sortie n'est pas actualisé par le bloc de fonctions de sortie en temps utile, tel que suite à une défaillance d'exécution des blocs de fonctions de sortie. La configuration du temps d'exécution des données périmées de sortie s'effectue par le bloc de fonctions de sortie. Le temps d'exécution des données périmées ne doit pas être confondu avec le temps d'exécution de l'état d'anomalie.

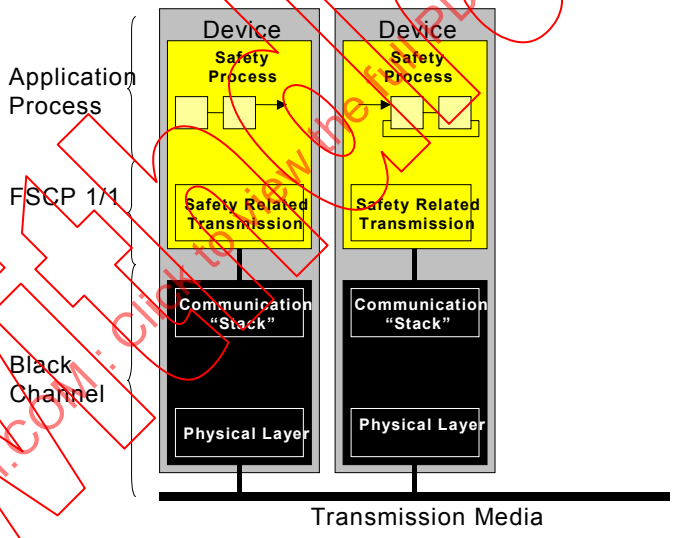
De façon similaire, un mécanisme spécifique au fabricant contrôle l'exécution des autres blocs, y compris les blocs de transducteurs.

EXEMPLE Une exécution incorrecte du bloc de transducteurs d'entrée signifie un statut de sortie incorrect des blocs de fonctions d'entrée.

6.3 Communications entre appareils

6.3.1 Généralités

La communication FSCP 1/1 est prise en charge pour les communications éditeur/abonné et client/serveur, mais non pour la diffusion des rapports. Un appareil de sécurité peut continuer à utiliser la VCR de diffusion des rapports pour la transmission des alarmes, le mécanisme n'étant toutefois pas fiable. La Figure 14 illustre cette communication.



Légende

Anglais	Français
Device	Appareil
Application Process	Processus d'application
Safety Process	Processus de sécurité
Safety Related Transmission	Transmission relative à la sécurité
Black Channel	Canal noir
Communication stack	Pile de communication
Physical Layer	Couche physique
Transmission Media	Supports de transmission

Figure 14 – Exemple de communication FSCP 1/1

6.3.2 Client/serveur

Un appareil de sécurité prend en charge la lecture et l'écriture client/serveur. L'utilisateur utilise la relation client/serveur pour l'écriture des paramètres. Il convient que l'utilisateur effectue un essai de fonctionnement tel que défini dans la série CEI 61508 après que des changements ont été apportés.

La VCR client/serveur n'est pas déterministe et sa synchronisation n'est pas véritablement effective. Les VCR client/serveur ne conviennent pas à la trajectoire d'arrêt.

L'écriture des paramètres et des objets est possible, mais les communications FSCP 1/1 sont requises avant tout pour activer les écritures. Le bloc de ressources comprend un système d'interdiction d'écriture qui protège tous les objets dudit bloc. L'utilisateur est tenu d'effectuer un essai de démonstration après un changement de configuration. Les communications FSCP 1/1 permettent alors de désactiver l'écriture ultérieure.

Les requêtes de lecture et les réponses d'écriture utilisent le protocole CP 1/1 régulier. Les requêtes d'écriture et les réponses de lecture utilisent le protocole FSCP 1/1. Un objet de liaison client/serveur (avec clé de connexion, etc.) doit être créé pour chaque client (interface) auquel la lecture/l'écriture d'un appareil sont autorisées. Chaque message est soumis à un CRC. La clé de connexion est incluse comme partie intégrante de l'en-tête virtuel, utilisé dans le calcul du CRC.

Les liaisons FSCP 1/1 des blocs de fonctions FSCP 1/1 sont configurées dans les objets de liaison de sécurité. Le protocole FSCP 1/1 est une extension du PDU, mais non un nouveau type de données.

Le protocole FSCP 1/1 utilise une transmission redondante, ce qui signifie une double transmission et une contre-vérification à l'extrémité de réception des données, du numéro de séquence et du CRC.

6.3.3 Editeur/abonné

Les liaisons FSCP 1/1 des blocs de fonctions FSCP 1/1 sont configurées dans les objets de liaison de sécurité. Le protocole FSCP 1/1 est une extension du PDU, mais non un nouveau type de données. Outre le CRC de la couche de communication de sécurité, le PDU de sécurité édité comporte également un numéro de séquence qui permet aux abonnés de contrôler les anomalies supplémentaires.

Le protocole FSCP 1/1 utilise une transmission redondante, ce qui signifie une double transmission et une contre-vérification à l'extrémité de réception des données, du numéro de séquence et du CRC.

6.3.4 Diffusion de rapports

Il n'existe pas d'extension de protocole FSCP 1/1 pour la VCR de diffusion de rapports. Par conséquent, cette dernière n'est pas fiable. Un appareil de sécurité peut émettre des alarmes de non-sécurité.

6.3.5 Opération FBAP dans un appareil de liaison

La méthode d'accès d'un processus d'application dans un appareil de liaison est identique à celle d'un FBAP FSCP 1/1.

6.3.6 Communications de protocole de noyau de gestion de système (SMKP)

Le SMKP fait partie intégrante du canal noir. Des moyens spécifiques au fabricant permettent de contrôler les anomalies de l'interface locale entre le SMKP et le processus d'application.

6.4 Profils

6.4.1 Généralités

Un profil est un sous-ensemble, une sélection, choisi à partir d'une spécification générale plus importante. Un profil FSCP 1/1 est ainsi une version limitée de la fonctionnalité FSCP 1/1 complète. De nouveaux profils sont créés pour le protocole FSCP 1/1.

6.4.2 Profil FSCP 1/1

6.4.2.1 Généralités

Les appareils FSCP 1/1 H1 peuvent également être répertoriés en classes établies sur leurs capacités. Les appareils FSCP 1/1 H1 appartiennent à un ou plusieurs des ensembles de classes présentés ci-dessous:

- Appareils de terrain FSCP 1/1 H1 – appareils de commande reposant sur des liaisons H1;
- Appareils hôtes FSCP 1/1 – exécutent l'interface utilisateur et fonctions de configuration – résolveur logique avec outil de configuration.

6.4.2.2 Paramétrage des blocs

L'écriture de tous les paramètres des blocs de sécurité est possible en utilisant la VCR client/serveur non FSCP 1/1, préalablement à la création de l'objet de liaison client/serveur FSCP 1/1, ou la VCR client/serveur FSCP 1/1 une fois que l'objet de liaison client/serveur FSCP 1/1 a été créé. Le protocole FSCP 1/1 nécessite le « déverrouillage » du bloc de ressources préalablement à l'écriture de tout élément du bloc de ressources. Il convient d'effectuer un essai de fonctionnement après que des changements ont été apportés.

6.4.2.3 Verrouillage du paramétrage des blocs

Le bloc de ressources est à déverrouiller avant l'écriture des paramètres. Ceci équivaut à une clé de verrouillage installée sur un pupitre relatif à la sécurité. En raison du grand nombre potentiel d'appareils de sécurité, installés souvent dans des zones dangereuses, voire inaccessibles, une communication FSCP 1/1 permet le verrouillage et le déverrouillage. La présence d'un système d'interdiction d'écriture souple est obligatoire dans le bloc de ressources de sécurité.

L'une des nombreuses mises en œuvre réalisables associées prend la forme d'un bloc de fonctions qui, en cas d'activation d'une entrée, procède à l'écriture du paramètre d'interdiction d'écriture dans l'appareil afin d'activer la configuration. Un bloc de fonctions est prévu à cet effet.

6.4.2.4 Authentification de l'utilisateur

Le logiciel hôte est tenu de s'assurer que l'accès à la programmation et au paramétrage est permis aux seuls utilisateurs autorisés.

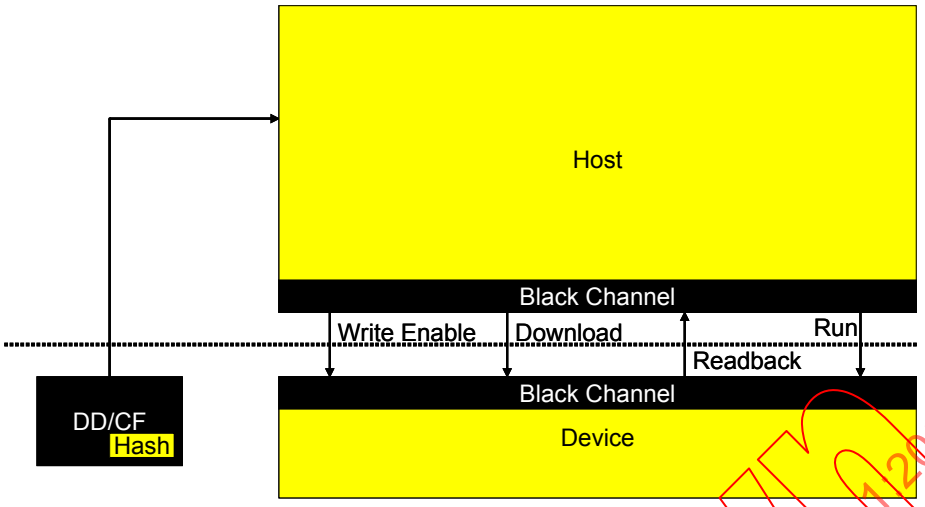
6.4.2.5 Verrouillage de programmation

Il est nécessaire de déverrouiller le bloc de ressources préalablement à toute modification des objets. Ceci équivaut à une clé de verrouillage installée sur un pupitre relatif à la sécurité. En raison du grand nombre potentiel d'appareils de sécurité, installés souvent dans des zones dangereuses, voire inaccessibles, une communication FSCP 1/1 permet le verrouillage et le déverrouillage. Le verrouillage de programmation est basé sur le paramètre d'interdiction d'écriture de ressource dans le bloc de même nature. L'écriture des objets autres que des blocs, tels que des objets de liaison, est possible uniquement lorsque le bloc de ressources est déverrouillé.

Il convient d'effectuer les modifications de programmes avec le processus interrompu (les appareils exécutant toutefois toujours les blocs), lorsque l'hôte communique avec les appareils.

6.5 Descriptions d'appareils

Les descriptions d'appareils font partie intégrante de l'outil de configuration Un hachage MD5 est généré pour chacun des fichiers DD et de capacité afin d'assurer l'intégrité du fichier. Le hachage MD5 des fichiers DD/CF est archivé avec un mot clé spécial dans le fichier de capacités FSCP 1/1. Ceci est illustré à la Figure 15.



Légende

Anglais	Français
Host	Hôte
Black Channel	Canal noir
Write Enable	Activation Ecriture
Download	Téléchargement
Run	Exécution
Readback	Relecture
Hash	Hachage
Device	Appareil

Figure 15 – Exemple de description d'appareils

6.6 Formats de fichiers communs

Les fichiers de capacité font partie intégrante de l'outil de configuration. Le mécanisme de hachage est décrit pour le fichier DD et est identique pour le fichier CF.

Le résumé du hachage MD5 des fichiers DD et CFF est archivé en fin de fichier CFF.

Le fichier de capacités contient des paramètres d'information des taux de défaillance de l'appareil. Il existe également des paramètres pour le niveau de conception des produits, c'est-à-dire l'évitement des anomalies obtenu (par exemple, au cours du processus de conception, il est possible de respecter les exigences relatives à un appareil SIL 2, même si les taux de défaillance sont corrects pour le niveau SIL 3).

6.7 Informations de configuration

6.7.1 Présentation générale

La configuration FSCP 1/1 est dans une large mesure identique à la configuration non relative à la sécurité, avec toutefois l'ajout de paramètres d'écriture de blocs de fonctions de sécurité tels que le temporisateur de données périmées, la limite de comptage des données périmées de bout en bout et le macro cycle. Les liaisons de blocs de fonctions FSCP 1/1 utilisent l'objet de liaison de sécurité lorsqu'il est nécessaire de définir la clé de connexion. Il est prévu que l'outil de configuration gère automatiquement la configuration de la clé de connexion et le macro cycle. Aucune modification des blocs de fonctions n'est admise une fois qu'un appareil est opérationnel.

6.7.2 Configuration de niveau 1: définition des appareils du fabricant

Les questions liées à la mise en œuvre et applicables aux appareils de sécurité incluent les mesures de séparation physique ou logique des fonctions de sécurité (processus d'application et couche de communication de sécurité) et non fiables (pile de canal noir) visant à s'assurer de l'absence de perturbations. Des VFD identiques ou différentes peuvent

comporter des applications de blocs de fonctions pour des applications relatives et non relatives à la sécurité.

6.7.3 Configuration de niveau 2: définition de réseau

La configuration du canal noir n'est pas modifiée.

6.7.4 Configuration de niveau 3: définition d'une application répartie

Un objet de liaison spécial est utilisé pour les blocs de fonctions de sécurité. Le temps de propagation prévu du canal doit être calculé.

L'utilisateur définit le temps de sécurité du processus. La configuration du macro cycle, des limites de comptage des données périmées de bout en bout et du temporisateur de données périmées est à effectuer en conséquence.

6.7.5 Configuration de niveau 4: Configuration des appareils

Le paramètre du bloc de ressources doit permettre de définir le temps de macro cycle.

7 Protocole de couche de communication de sécurité

7.1 Format PDU de sécurité

7.1.1 Généralités

Le protocole FSCP 1/1 contrôle les défaillances de communication. Ce protocole s'applique au protocole de communication FMS. Des moyens spécifiques au fabricant permettent de contrôler les anomalies au niveau de l'interface locale entre le processus d'application et le SMK, ainsi que la SMIB dans le NMA. Le protocole FSCP 1/1 s'applique aux communications FMS sur le bus de terrain.

7.1.2 CRC de couche de communication de sécurité

Le contrôle de redondance cyclique permet de contrôler les défaillances de corruption de données dans la communication de bus de terrain. Les données sont transmises avec une somme de contrôle CRC calculée pour chaque PDU de sécurité. Le CRC de couche de communication de sécurité est défini par CCITT 32 V.42 et l'ISO/CEI 8802-3 (IEEE 802.3). Il s'agit d'un polynôme de 32 bits dont le calcul s'effectue comme suit:

$(x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1)$.

La couche de communication de sécurité du récepteur recalcule la somme de contrôle des données reçues et compare le résultat avec la somme de contrôle reçue. Les messages corrompus sont rejetés.

7.1.3 Contrôle de la synchronisation temporelle par le canal noir

Le numéro de séquence est basé sur le nombre de macro cycles déduit du temps de liaison de données pour chaque édition. Le numéro de séquence est effectivement une sorte de datation. Tous les appareils placés sur le réseau H1 comportent un macro cycle à sens commun. Les appareils placés sur un réseau H1 reposent ainsi sur un temps à sens commun établi sur un mécanisme de synchronisation temporelle à fonctionnement correct. Un temps synchronisé est requis pour garantir une exécution synchrone des blocs de fonctions et des communications, garantissant par ailleurs le temps de réponse de fonction de sécurité le plus court possible. Le mécanisme de synchronisation temporelle corrige le temps et la fréquence de liaison de données, et se trouve dans le canal noir. Son contrôle est toutefois assuré par la couche de communication de sécurité. La couche de communication de sécurité comporte une source de temps de sécurité indépendante et détecte toute perte de synchronisation temporelle dans le canal noir, par comparaison de la fréquence de l'horloge FSCP 1/1 avec la fréquence de l'horloge de canal noir, avec synchronisation de l'horloge. Si l'écart est supérieur à une valeur admise, le réglage sur « statut incorrect » des entrées et sorties de blocs de fonctions déclenche une action préconfigurée en réaction à un état d'anomalie. Le bloc de ressources comporte un paramètre d'erreur de canal noir avec drapeau d'erreur de synchronisation temporelle.

La répartition temporelle entre le maître (LAS) et les autres appareils peut être altérée par des retards de mise en file d'attente de communication, simplement comme d'autres éditions de liaison. Le canal noir local comporte une fonction de mesure du retard de cycle par l'intermédiaire du canal noir, afin de compenser les retards de mise en file d'attente. Cette opération est effectuée de manière régulière et comprend le démarrage et les modifications LAS. Il ne s'agit pas d'une fonction de sécurité. Il s'agit d'une fonction destinée à éviter les déclenchements parasites, assurant ainsi une plus grande disponibilité.

Le moniteur de synchronisation temporelle par le canal noir contrôle les anomalies telles que:

- temps LAS rapide, lent ou saut;
- anomalie de mise en file d'attente (éditeur/abonné ou répartition du temps)
- redémarrage d'appareils;
- redémarrage de la fonction de sécurité;
- basculement LAS;
- redémarrage LAS;
- corruption de programmation (LAS ou appareil de terrain);
- démarrage initial (configuration) (identique au redémarrage de la fonction de sécurité);
- communication (répartition du temps perdu, données contraintes ou édition).

7.1.4 Numéro de séquence

Pour les VCR éditeur/abonné, le numéro de séquence pour chaque édition est basé sur le nombre de macro cycles calculé par la couche de communication de sécurité à partir du temps de liaison des données au début de chaque macro cycle. La fonction de contrôle de la synchronisation temporelle par le canal noir dans la couche de communication de sécurité s'assure du caractère correct du temps de liaison de données. Le numéro de séquence éditeur/abonné est effectivement une datation. Tous les appareils placés sur le réseau H1 comportent un macro cycle à sens commun. Il peut ne pas y avoir de sous-programmes, c'est-à-dire que les blocs de fonctions ne peuvent être exécutés qu'une seule fois par macro cycle. En fonctionnement normal, le numéro de séquence augmente de un pour chaque nouvelle édition de liaison. Le numéro de séquence est inclus dans le message et comparé par rapport à un numéro de séquence prévu dans la couche de communication de sécurité à l'extrémité de réception. En cas de dépassement d'une différence admise maximale, cela confère un statut incorrect à l'entrée du bloc de fonctions, de sorte que le processus d'application connaît le caractère périmé des données.

Si des erreurs de communication, l'exécution des blocs de fonctions, des anomalies de programmation ou tout autre facteur remettent en cause le temps de réponse global entre le capteur et l'actionneur, la sortie exécute l'action préconfigurée en réaction à un état d'anomalie. En présence d'une chaîne de blocs de fonctions associés constituant une fonction de sécurité, plusieurs comptages des données périmées de liaison individuels pourraient s'ajouter à un temps de réponse long avant détection. Le diagnostic des comptages des données périmées s'effectue de bout en bout de préférence à un comptage des données périmées par liaison tel qu'utilisé pour les communications non FSCP 1/1. Il s'agit effectivement d'une mesure du délai de propagation. Le temps de réponse maximal entre le capteur et l'actionneur admis par l'application (exprimé en unités de macro cycle) doit être configuré dans la limite de comptage des données périmées de bout en bout de l'objet de liaison. En cas de dépassement de la limite de comptage des données périmées de bout en bout, la couche de communication de sécurité règle le statut d'entrée du bloc de fonctions sur BAD («Incorrect »). Les comptages des données périmées sont propagés en aval et cumulés, étant donné que la couche de communication de sécurité déduit le numéro de séquence du nombre de macro cycles uniquement lorsque les sorties des blocs de fonctions ont été actualisées, et chaque bloc de fonctions individuel actualise uniquement sa sortie si les conditions d'entrée sont correctes (l'édition ultérieure provoquant ainsi la génération du numéro de séquence). En d'autres termes, lorsque toutes les liaisons fonctionnent et lorsque tous les blocs de fonctions opèrent comme il convient, le numéro de séquence (basé sur le nombre de macro cycles au niveau du capteur) propagé de bout en bout est adapté au macro cycle (numéro de séquence prévu) dans la soupape. Lorsque ce numéro est comparé au

macro cycle de l'appareil de sortie, il indique le nombre total de communications et d'exécutions manquées dans la chaîne des blocs de fonctions qui constituent la fonction de sécurité. Ceci entraîne un temps de réponse défavorable de bien plus courte durée. Les critères de rafraîchissement avec ou non une nouvelle sortie sont spécifiques aux blocs de fonctions. Un nouveau numéro de séquence est généré uniquement par la couche de communication de sécurité au moment de l'édition du message. Certains blocs de fonctions peuvent exiger de toutes les entrées utilisées qu'elles soient actuelles, tandis que d'autres blocs de fonctions peuvent présenter une capacité élective exigeant uniquement d'un certain nombre des entrées utilisées qu'elles soient actuelles.

La couche FSCP 1/1 exige un compteur de numéros de séquence pour chaque VCR client/serveur. Le numéro de séquence client/serveur est augmenté de un pour chaque nouvelle transaction. Pour chaque VCR client-serveur, la connexion est abandonnée si le numéro de séquence est hors synchronisation. Les numéros de séquence sont réinitialisés à chaque établissement d'une nouvelle connexion.

7.1.5 En-tête virtuel

L'en-tête de protocole, tel que l'adresse, dans la trame de canal noir n'est pas protégé par le CRC de la couche de communication de sécurité, et les applications relatives à la sécurité ne peuvent par conséquent pas s'y fier. Il est de ce fait nécessaire d'utiliser un mécanisme différent qui permet d'identifier de manière unique la relation source-destination dans le message FSCP 1/1, avec toutefois une protection assurée par le CRC de la couche de communication de sécurité. La clé de connexion est utilisée à cette fin. La transmission de la clé de connexion dans chaque message créerait cependant une surcharge système. Pour réduire cette surcharge, le CRC de la couche de communication de sécurité est calculé sur la base des données de sécurité et un en-tête virtuel incluant la clé de connexion et l'index d'objet. Le CRC de la couche de communication de sécurité au niveau du destinataire échoue si la clé de connexion est erronée, bien que la clé de connexion ne soit pas transmise sur le bus. L'objet de liaison de sécurité comporte la clé de connexion qui permet de calculer le CRC.

7.1.6 Clé de connexion

Le protocole comporte un mécanisme qui permet d'identifier de manière unique les messages FSCP 1/1, le déguisement procuré par un message FSCP 1/1 étant ainsi différent de celui procuré par un autre message FSCP 1/1: une clé de connexion de 32 bits unique permet d'identifier les liaisons des blocs de fonctions FSCP 1/1. La clé de connexion est administrée par l'hôte et inscrite (écriture) dans les objets de liaison de sécurité. La clé de connexion fait partie intégrante de l'en-tête virtuel intégré dans le CRC de la couche de communication de sécurité, mais n'est pas communiquée. L'abonné ou le serveur n'effectue aucun contrôle explicite de tout défaut d'adaptation de la clé de connexion. Un défaut d'adaptation occasionne toutefois une erreur de CRC de la couche de communication de sécurité. A savoir, une erreur de CRC de la couche de communication de sécurité peut indiquer une corruption des données ou un défaut d'adaptation de la clé de connexion.

7.1.7 Redondance et contre-vérification

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

Une mise en œuvre possible est que chaque contrôleur d'un appareil comportant deux microcontrôleurs redondants élabore son message de transmission de manière totalement indépendante. L'interface du canal noir rassemble les deux messages de données indépendants, qui sont alors transmis comme une seule trame. Inversement, à réception, les deux messages de données indépendants dans la trame en provenance du canal noir sont dégroupés selon leurs microcontrôleurs respectifs, qui effectuent alors la contre-vérification.