IEC 61784-3

Edition 2.0 2010-06

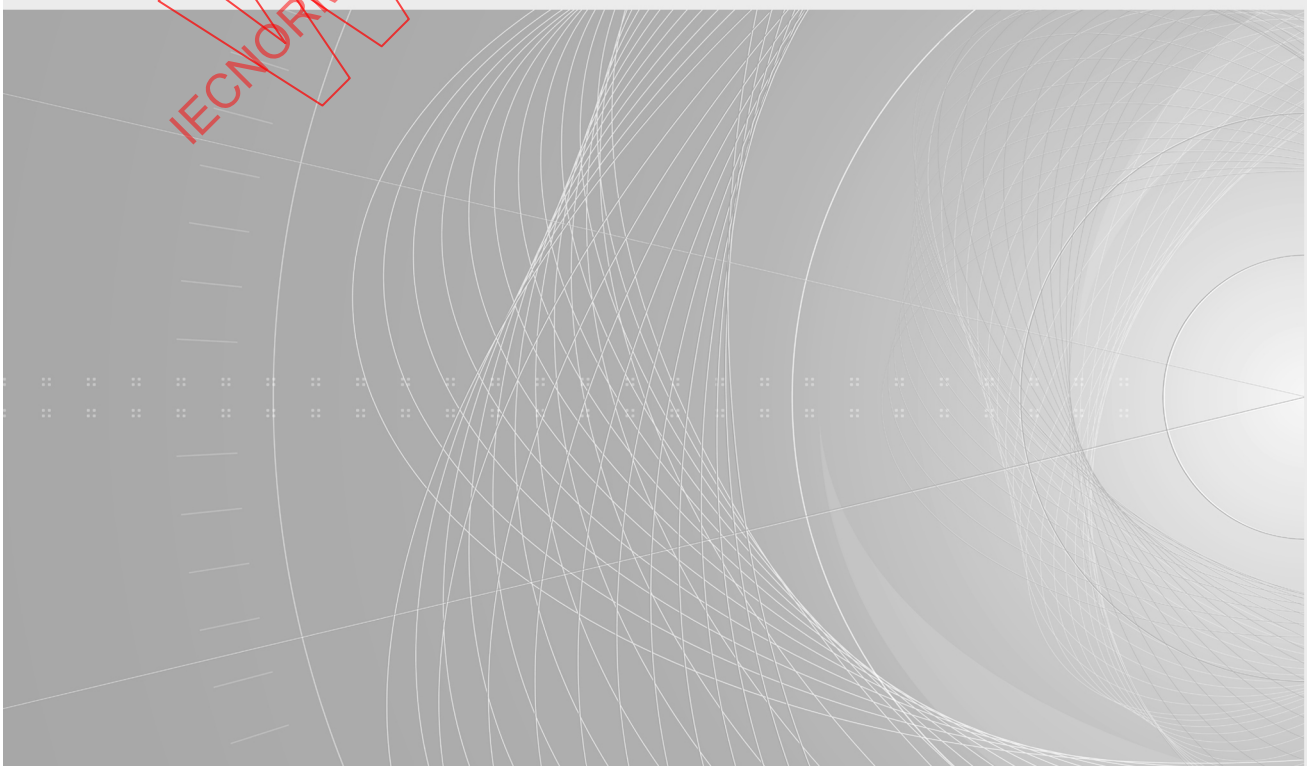
INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions

Réseaux de communication industriels – Profils – Partie 3: Bus de terrain de sécurité fonctionnelle – Règles générales et définitions de profils



IEC 61784-3:2010

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland
Email: inmail@iec.ch
Web: 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.

- Catalogue of IEC publications: www.iec.ch/searchpub
The IEC on-line Catalogue enables you to search by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, withdrawn and replaced publications.
- IEC Just Published: www.iec.ch/online_news/justpub
Stay up to date on all new IEC publications. Just Published details twice a month all new publications released. Available on-line and also by email.
- Electropedia: www.electropedia.org
The world's leading online dictionary of electronic and electrical terms containing more than 20 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary online.
- Customer Service Centre: www.iec.ch/webstore/custserv
If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us:
Email: csc@iec.ch
Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00

A propos de la CEI

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

A propos des publications CEI

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

- Catalogue des publications de la CEI: www.iec.ch/searchpub/cur_fut-f.htm
Le Catalogue en-ligne de la CEI vous permet d'effectuer des recherches en utilisant différents critères (numéro de référence, texte, comité d'études,…). Il donne aussi des informations sur les projets et les publications retirées ou remplacées.
- Just Published CEI: www.iec.ch/online_news/justpub
Restez informé sur les nouvelles publications de la CEI. Just Published détaille deux fois par mois les nouvelles publications parues. Disponible en-ligne et aussi par email.
- Electropedia: www.electropedia.org
Le premier dictionnaire en ligne au monde de termes électroniques et électriques. Il contient plus de 20 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans les langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International en ligne.
- Service Clients: www.iec.ch/webstore/custserv/custserv_entry-f.htm
Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions, visitez le FAQ du Service clients ou contactez-nous:
Email: csc@iec.ch
Tél.: +41 22 919 02 11
Fax: +41 22 919 03 00

IEC 61784-3

Edition 2.0 2010-06

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions

Réseaux de communication industriels – Profils – Partie 3: Bus de terrain de sécurité fonctionnelle – Règles générales et définitions de profils

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

PRICE CODE XA
CODE PRIX

ICS 25.040.40; 35.100.05

ISBN 978-2-88912-810-5

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES –

Part 3: Functional safety fieldbuses – General rules and profile definitions

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.

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

This second edition cancels and replaces the first edition published in 2007. This edition constitutes a technical revision. The main changes with respect to the previous edition are listed below:

– clarifications and additional explanations for requirements, updated references;
– updates of definitions and requirements in relation with the new edition of IEC 61508;
– addition of a new informative Annex D providing an assessment guideline;
– updates in parts for CPF 1, CPF 2, CPF 3, CPF 6 (details provided in the parts);
– addition of new parts for CPF 8, CPF 12, CPF 13, CPF 14;
– in CPF parts, addition of an annex to provide information about test laboratories for testing and validating conformance of FSCP products.

This bilingual version published in 2011-12, corresponds to the English version published in 2010-07.

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

FDIS	Report on voting
65C/591A/FDIS	65C/603/RVD

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

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

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

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

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

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

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

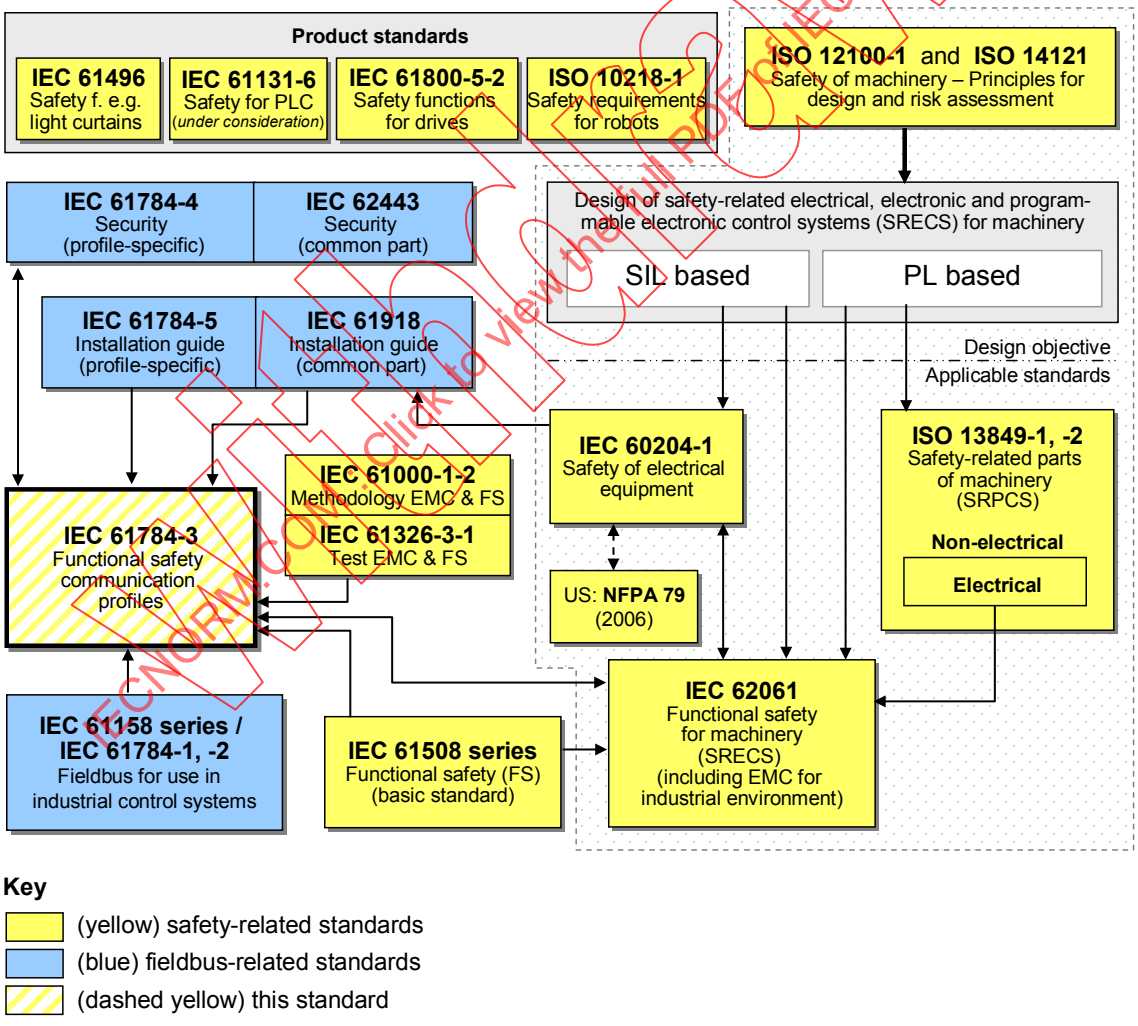
0 Introduction

0.1 General

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

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

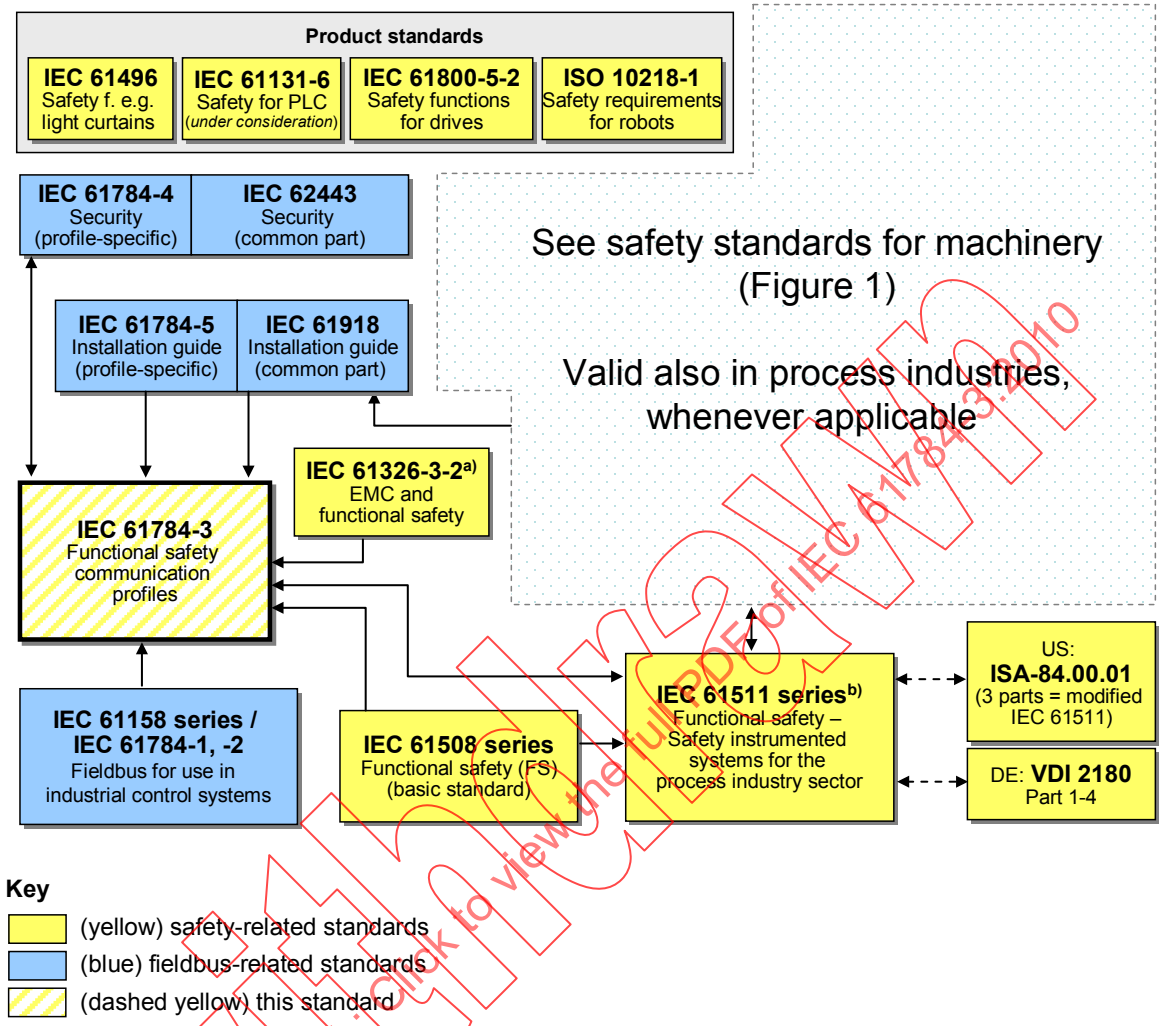
Figure 1 shows the relationships between this standard and relevant safety and fieldbus standards in a machinery environment.



NOTE Subclauses 6.7.6.4 (high complexity) and 6.7.8.1.6 (low complexity) of IEC 62061 specify the relationship between PL (Category) and SIL.

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

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



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

[b] EN ratified.

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

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

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

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

This standard describes:

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

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

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

0.2 Patent declaration

The International Electrotechnical Commission (IEC) draws attention to the fact that it is claimed that compliance with this document may involve the use of patents concerning functional safety communication profiles for families 1, 2, 3, 6, 12, 13 and 14 given in IEC 61784-3-1, IEC 61784-3-2, IEC 61784-3-3, IEC 61784-3-6, IEC 61784-3-12, IEC 61784-3-13 and IEC 61784-3-14.

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

The holders of these patent rights have assured 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 statements of the holders of these patent rights are registered with IEC.

NOTE Patent details and corresponding contact information are provided in IEC 61784-3-1, IEC 61784-3-2, IEC 61784-3-3, IEC 61784-3-6, IEC 61784-3-12, IEC 61784-3-13 and IEC 61784-3-14.

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES –

Part 3: Functional safety fieldbuses – General rules and profile definitions

1 Scope

This part of the IEC 61784-3 series explains some common principles than can be used in the transmission of safety-relevant messages among participants within a distributed network using fieldbus technology in accordance with the requirements of IEC 61508 series[1] for functional safety. These principles can be used in various industrial applications such as process control, manufacturing automation and machinery.

This part[2] and the IEC 61784-3-x parts specify several functional safety communication profiles based on the communication profiles and protocol layers of the fieldbus technologies in IEC 61784-1, IEC 61784-2 and the IEC 61158 series.

NOTE 1 Other safety-related communication systems meeting the requirements of IEC 61508 series may exist that are not included in this standard.

NOTE 2 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.

All systems are exposed to unauthorized access at some point of their life cycle. Additional measures need to be considered in any safety-related application to protect fieldbus systems against unauthorized access. The IEC 62443 series will address many of these issues; the relationship with the IEC 62443 series is detailed in a dedicated subclause of this part.

NOTE 3 Additional profile specific requirements for security may also be specified in IEC 61784-4[3] [10].

NOTE 4 Implementation of a functional safety communication profile according to this part in a device is not sufficient to qualify it as a safety device, as defined in IEC 61508 series.

NOTE 5 The resulting SIL claim of a system depends on the implementation of the selected functional safety communication profile within this system.

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 (all parts), *Industrial communication networks – Fieldbus specifications*

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*

---

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

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

3 Proposed new work item under consideration.

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

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

IEC 61508-1:2010[4], *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements*

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

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

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

IEC 61784-3-1, *Industrial communication networks – Profiles – Part 3-1: Functional safety fieldbuses – Additional specifications for CPF 1*

IEC 61784-3-2, *Industrial communication networks – Profiles – Part 3-2: Functional safety fieldbuses – Additional specifications for CPF 2*

IEC 61784-3-3, *Industrial communication networks – Profiles – Part 3-3: Functional safety fieldbuses – Additional specifications for CPF 3*

IEC 61784-3-6, *Industrial communication networks – Profiles – Part 3-6: Functional safety fieldbuses – Additional specifications for CPF 6*

IEC 61784-3-8[5], *Industrial communication networks – Profiles – Part 3-8: Functional safety fieldbuses – Additional specifications for CPF 8*

IEC 61784-3-12[5], *Industrial communication networks – Profiles – Part 3-12: Functional safety fieldbuses – Additional specifications for CPF 12*

IEC 61784-3-13[5], *Industrial communication networks – Profiles – Part 3-13: Functional safety fieldbuses – Additional specifications for CPF 13*

IEC 61784-3-14[5], *Industrial communication networks – Profiles – Part 3-14: Functional safety fieldbuses – Additional specifications for CPF 14*

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

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*

---

4 To be published.

5 To be published.

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

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
absolute time stamp
time stamp referenced to a global time which is common for a group of devices using a *fieldbus*
[IEC 62280-2, modified]

3.1.1.2
availability
probability for an automated system that for a given period of time there are no unsatisfactory system conditions such as loss of production

3.1.1.3
black channel
communication channel without available evidence of design or validation according to IEC 61508

3.1.1.4
bridge
abstract device that connects multiple network segments along the data link layer

3.1.1.5
communication channel
logical connection between two end-points within a *communication system*

3.1.1.6
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

3.1.1.7
connection
logical binding between two application objects within the same or different devices

3.1.1.8
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 [29], [30][6].

6 Figures in square brackets refer to the bibliography.

3.1.1.9
diversity
different means of performing a required function

NOTE Diversity may be achieved by different physical methods or different design approaches.

[IEC 61508-4:2010[7]]

3.1.1.10
error
discrepancy between a computed, observed or measured value or condition and the true, specified or theoretically correct value or condition

[IEC 61508-4:2010], [IEC 61158]

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

NOTE 2 Errors do not necessarily result in a *failure* or a *fault*.

3.1.1.11
failure
termination of the ability of a functional unit to perform a required function or operation of a functional unit in any way other than as required

NOTE 1 The definition in IEC 61508-4 is the same, with additional notes.

[IEC 61508-4:2010, modified], [ISO/IEC 2382-14.01.11, modified]

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

3.1.1.12
fault
abnormal condition that may cause a reduction in, or loss of, the capability of a functional unit to perform a required function

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

[IEC 61508-4:2010, modified], [ISO/IEC 2382-14.01.10, modified]

3.1.1.13
fieldbus
communication system based on serial data transfer and used in industrial automation or process control applications

3.1.1.14
fieldbus system
system using a *fieldbus* with connected devices

3.1.1.15
frame
denigrated synonym for DLPDU

3.1.1.16
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

---

7 To be published.

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

NOTE 2 See also [29], [30].

3.1.1.17
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/TR 62210, modified]

3.1.1.18
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

3.1.1.19
master
active communication entity able to initiate and schedule communication activities by other stations which may be masters or slaves

3.1.1.20
message
ordered series of octets intended to convey information
[ISO/IEC 2382-16.02.01, modified]

3.1.1.21
message sink
part of a *communication system* in which *messages* are considered to be received
[ISO/IEC 2382-16.02.03]

3.1.1.22
message source
part of a *communication system* from which *messages* are considered to originate
[ISO/IEC 2382-16.02.02]

3.1.1.23
nuisance trip
spurious trip with no harmful effect

NOTE Internal abnormal errors can be caused in communication systems such as wireless transmission, for example by too many retries in the presence of interferences.

3.1.1.24
performance level (PL)
discrete level used to specify the ability of safety-related parts of control systems to perform a safety function under foreseeable conditions
[ISO 13849-1]

3.1.1.25
protective extra-low-voltage (PELV)
electrical circuit in which the voltage cannot exceed a.c. 30 V r.m.s., 42,4 V peak or d.c. 60 V in normal and single-fault condition, except earth faults in other circuits

NOTE A PELV circuit is similar to an SELV circuit that is connected to protective earth.

[IEC 61131-2]

3.1.1.26
redundancy
existence of means, in addition to the means which would be sufficient for a functional unit to perform a required function or for data to represent information

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

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

3.1.1.27
relative time stamp
time stamp referenced to the local clock of an entity

NOTE In general, there is no relationship to clocks of other entities.

[IEC 62280-2, modified]

3.1.1.28
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]

3.1.1.29
risk
combination of the probability of occurrence of harm and the severity of that harm

NOTE For more discussion on this concept see Annex A of IEC 61508-5:2010[8].

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

3.1.1.30
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

3.1.1.31
safety connection
connection that utilizes the safety protocol for communications transactions

3.1.1.32
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.

8 To be published.

3.1.1.33
safety device
device designed in accordance with IEC 61508 and which implements the functional safety communication profile

3.1.1.34
safety extra-low-voltage (SELV)
electrical circuit in which the voltage cannot exceed a.c. 30 V r.m.s., 42,4 V peak or d.c. 60 V in normal and single-fault condition, including earth faults in other circuits

NOTE An SELV circuit is not connected to protective earth.

[IEC 61131-2]

3.1.1.35
safety function
function to be implemented by an E/E/PE safety-related system or other risk reduction measures, that is intended to achieve or maintain a safe state for the EUC, in respect of a specific hazardous event

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

[IEC 61508-4:2010, modified]

3.1.1.36
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 5.2.4 and addressed by the functional safety communication profiles defined in this part.

3.1.1.37
safety integrity level (SIL)
discrete level (one out of a possible four), corresponding to a range of safety integrity values, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest

NOTE 1 The target failure measures (see IEC 61508-4:2010, 3.5.17) for the four safety integrity levels are specified in Tables 2 and 3 of IEC 61508-1:2010[9].

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

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

[IEC 61508-4:2010]

3.1.1.38
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 5.3 and 5.4.

9 To be published.

3.1.1.39
safety-related application
programs designed in accordance with IEC 61508 to meet the SIL requirements of the application

3.1.1.40
safety-related system
system performing *safety functions* according to IEC 61508

3.1.1.41
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

3.1.1.42
spurious trip
trip caused by the safety system without a process demand

3.1.1.43
time stamp
time information included in a *message*

3.1.1.44
white channel
communication channel in which all relevant hardware and software components are designed, implemented and validated according to IEC 61508

3.1.2 CPF 1: Additional terms and definitions

None required for this part.

3.1.3 CPF 2: Additional terms and definitions

None required for this part.

3.1.4 CPF 3: Additional terms and definitions

None required for this part.

3.1.5 CPF 6: Additional terms and definitions

None required for this part.

3.1.6 CPF 8: Additional terms and definitions

None required for this part.

3.1.7 CPF 12: Additional terms and definitions

None required for this part.

3.1.8 CPF 13: Additional terms and definitions

None required for this part.

3.1.9 CPF 14: Additional terms and definitions

None required for this part.

3.2 Symbols and abbreviated terms

3.2.1 Common symbols and abbreviated terms

CP	Communication Profile	[IEC 61784-1]
CPF	Communication Profile Family	[IEC 61784-1]
CRC	Cyclic Redundancy Check	
DLL	Data Link Layer	[ISO/IEC 7498-1]
DLPDU	Data Link Protocol Data Unit	
EMC	Electromagnetic Compatibility	
EMI	Electromagnetic Interference	
EUC	Equipment Under Control	[IEC 61508-4:2010]
E/E/PE	Electrical/Electronic/Programmable Electronic	[IEC 61508-4:2010]
FAL	Fieldbus Application Layer	[IEC 61158-5]
FCS	Frame Check Sequence	
FS	Functional Safety	
FSCP	Functional Safety Communication Profile	
MTBF	Mean Time Between Failures	
MTTF	Mean Time To Failure	
NSR	Non Safety Relevant	
PDU	Protocol Data Unit	[ISO/IEC 7498-1]
PELV	Protective Extra Low Voltage	
PES	Programmable Electronic System	[IEC 61508-4:2010]
PFD	Probability of dangerous Failure on Demand	[IEC 61508-6:2010[10]]
PFH	Average frequency of dangerous failure [h^{-1}] per hour	[IEC 61508-6:2010]
PhL	Physical Layer	[ISO/IEC 7498-1]
PL	Performance Level	[ISO 13849-1]
PLC	Programmable Logic Controller	
SCL	Safety Communication Layer	
SELV	Safety Extra Low Voltage	
SIL	Safety Integrity Level	[IEC 61508-4:2010]
SR	Safety Relevant	

3.2.2 CPF 1: Additional symbols and abbreviated terms

SIS	Safety Instrumented Systems

3.2.3 CPF 2: Additional symbols and abbreviated terms

CIP™	Common Industrial Protocol (application framework shared among CPF 2 communication profiles)

3.2.4 CPF 3: Additional symbols and abbreviated terms

DP	Decentralized Peripherals

[10] To be published.

3.2.5 CPF 6: Additional symbols and abbreviated terms

None required for this part.

3.2.6 CPF 8: Additional symbols and abbreviated terms

ASE Application Service Element

SASE Safety Application Service Element

3.2.7 CPF 12: Additional symbols and abbreviated terms

FSoE Failsafe over CPF 12

3.2.8 CPF 13: Additional symbols and abbreviated terms

None required for this part.

3.2.9 CPF 14: Additional symbols and abbreviated terms

IP Internet Protocol

UDP User Datagram Protocol

4 Conformance

Each functional safety communication profile within this standard is based on communication profiles of IEC 61784-1 or IEC 61784-2 and protocol layers of the IEC 61158 series.

A statement of conformance to a Functional Safety Communication Profile (FSCP) of this standard shall be stated as either

conformance to IEC 61784-3:20xx FSCP n/m <Type>

or

conformance to IEC 61784-3 (Ed.2.0) FSCP n/m <Type>

where the Type within the angle brackets < > is optional and the angle brackets are not to be included.

Alternatively, a statement of conformance may be stated as either

conformance to IEC 61784-3-N:20xx

or

conformance to IEC 61784-3-N (Ed.2.0)

where N is the family number assigned to the corresponding CPF.

Conformance to a IEC 61784-3-N part means that all mandatory requirements of the corresponding FSCP(s) for the particular device, system or application shall be fulfilled.

Product standards shall not include any Conformity Assessment aspects (including QM provisions), either normative or informative, other than provisions for product testing (evaluation and examination).

5 Basics of safety-related fieldbus systems

5.1 Safety function decomposition

According to IEC 61508 a risk analysis will define safety functions. These safety functions can be decomposed to parts that contribute to the overall safety function (for example, Sensor(s) – Safety communication channel – PES(s) – Safety communication channel – Actuator(s)).

The communication system itself in this standard performs transmission of safety data. It is highly recommended that the safety communication channel does not consume more than 1 % of the maximum PFD or PFH of the target SIL for which the functional safety communication profile is designed (see Figure 3).

EXAMPLE

In Figure 3, the PFH of the safety function is PFH_{sensor} + PFH_{PES} + $PFH_{actuator}$ + 2 x $PFH_{safety\ communication\ channel}$.

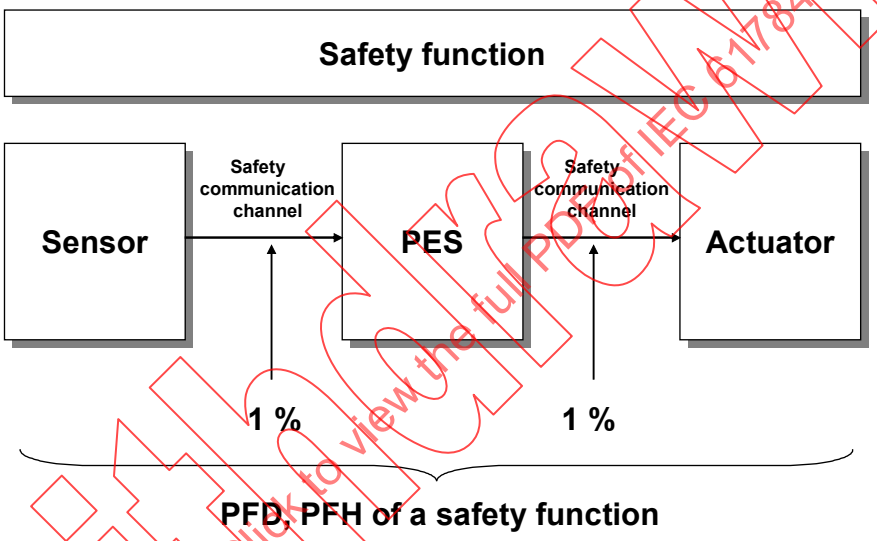


Figure 3 – Safety communication as a part of a safety function

5.2 Communication system

5.2.1 General

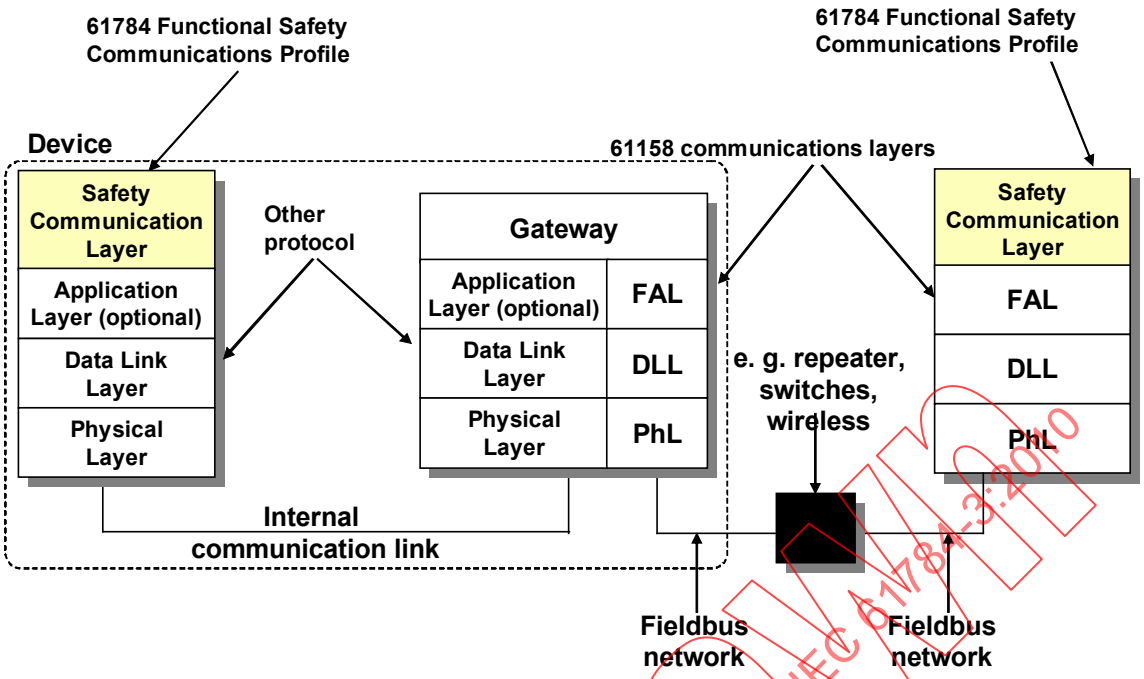
The following information is used to provide a common understanding of technology and terms.

NOTE Most of the information is derived from the Principles for Test and Certification of Bus Systems for Safety Relevant Communication of the German Institute for occupational safety and health [28].

5.2.2 IEC 61158 fieldbuses

While IEC 61508 is not restricting the use of communication technologies, this standard focuses on the use of fieldbus based functional safety communication systems. Figure 4 shows an example model of the use of functional safety communications with a fieldbus based on the black channel approach.

When using IEC 61158 based fieldbus structures without modifications in the definition of each communication layer, all the measures necessary to implement transmission of safety data in accordance with the requirements of IEC 61508 shall be performed by an additional “safety communication layer”, positioned as shown in Figure 4.



NOTE 1 Implementation of the Fieldbus Application Layer (FAL) is required, while the AL may be omitted for communication links internal to a device.

NOTE 2 Functions of the user layer that are not safety-related may bypass the SCL and access the FAL directly.

Figure 4 – Example model of a functional safety communication system

5.2.3 Communication channel types

IEC 61508 uses the concept of the so called “black channel” or “white channel” to define the requirements of the base fieldbus for transmission of safety data. Whether a communication channel is white or black is determined by where the safety measures are accomplished with respect to the base fieldbus. This standard specifies functional safety communication profiles that use the black channel approach.

In this context, a safety communication channel is defined to start at the top of the safety communication layer of the source and stop at the top of the safety communication layer of the sink (see Figure 4).

5.2.4 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 analogue signal crossing a threshold or a digital signal changing state.

Figure 5 shows an example of typical components making up a safety function response time.

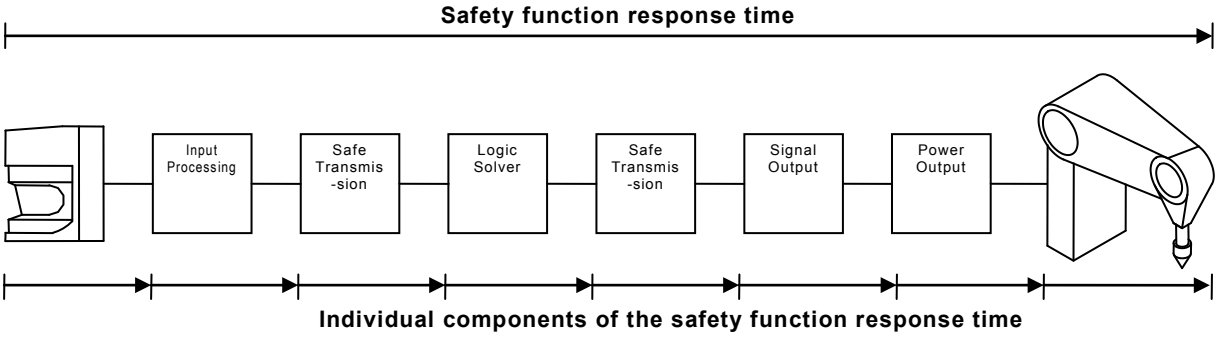


Figure 5 – Example of safety function response time components

Individual functional safety communication profiles may have a different set of components, but all relevant components shall be accounted for in the safety function response time.

5.3 Communication errors

5.3.1 General

The following subclauses specify possible communication errors. Additional notes are provided to indicate the typical behaviour of a black channel.

5.3.2 Corruption

Messages may be corrupted due to errors within a bus participant, due to errors on the transmission medium, or due to message interference.

NOTE 1 Message error during transfer is a normal event for any standard communication system, such events are detected at receivers with high probability by use of a hash function and the message is ignored.

NOTE 2 Most communication systems include protocols for recovery from message errors, so these messages should not be classed as 'Loss' until recovery or repetition procedures have failed or are not used.

NOTE 3 If the recovery or repetition procedures take longer than a specified deadline, a message is classed as 'Unacceptable delay'

NOTE 4 In the very low probability event that multiple errors result in a new message with correct message structure (for example addressing, length, hash function such as CRC, etc), the message will be accepted and processed further. Evaluations based on a message sequence number or a time stamp may result in fault classifications such as Unintended repetition, Incorrect sequence, Unacceptable delay, Insertion.

5.3.3 Unintended repetition

Due to an error, fault or interference, old not updated messages are repeated at an incorrect point in time.

NOTE 1 Repetition by the sender is a normal procedure when an expected acknowledgment/response is not received from a target station, or when a receiver station detects a missing message and asks for it to be resent.

In some cases, the lack of response can be detected and the message repeated with minimal delay and no loss of sequence, in other cases the repetition occurs at a later time and arrives out of sequence with other messages.

NOTE 2 Some fieldbuses use redundancy to send the same message multiple times or via multiple alternate routes to increase the probability of good reception.

5.3.4 Incorrect sequence

Due to an error, fault or interference, the predefined sequence (for example natural numbers, time references) associated with messages from a particular source is incorrect.

NOTE 1 Fieldbus systems may contain elements that store messages (for example FIFOs in switches, bridges, routers) or may use protocols that may alter the sequence (for example by allowing messages with high priority to overtake those with lower priority).

NOTE 2 When multiple sequences are active, such as messages from different source entities or reports relating to different object types, these sequences are monitored separately and errors may be reported for each sequence.

5.3.5 Loss

Due to an error, fault or interference, a message is not received or not acknowledged.

5.3.6 Unacceptable delay

Messages may be delayed beyond their permitted arrival time window, for example due to errors in the transmission medium, congested transmission lines, interference, or due to bus participants sending messages in such a manner that services are delayed or denied (for example FIFOs in switches, bridges, routers).

NOTE In underlying fieldbuses using scheduled or cyclic scans, message errors may be recovered in the following several ways:

a) immediate repetition;

b) repetition using spare time at the end of the cycle;

c) treat the message as lost and wait for the next cycle to receive the next value.

In case a) all the following messages in that cycle are slightly delayed, while in case b) only the resent message gets a delay.

Cases a) and b) are not normally classed as an Unacceptable delay.

Case c) would be classed as an Unacceptable delay unless the cycle repetition interval is short enough to ensure that delays between cycles are not significant and the next cyclic value can be accepted as a replacement for the missed previous value.

5.3.7 Insertion

Due to a fault or interference, a message is inserted that relates to an unexpected or unknown source entity.

NOTE These messages are additional to the expected message stream, and because they do not have expected sources, they cannot be classified as Correct, Unintended repetition, or Incorrect sequence.

5.3.8 Masquerade

Due to a fault or interference, a message is inserted that relates to an apparently valid source entity, so a non-safety relevant message may be received by a safety relevant participant, which then treats it as safety relevant.

NOTE Communication systems used for safety-related applications may use additional checks to detect Masquerade, such as authorised source identities and pass-phrases or cryptography.

5.3.9 Addressing

Due to a fault or interference, a safety relevant message is sent to the wrong safety relevant participant, which then treats reception as correct.

5.4 Deterministic remedial measures

5.4.1 General

This subclause lists measures commonly used to detect deterministic errors and failures of a communication system, as contrasted to stochastic errors like message corruption due to electromagnetic interference.

5.4.2 Sequence number

A sequence number is integrated into messages exchanged between message source and message sink. It may be realised as an additional data field with a number that changes from one message to the next in a predetermined way.

5.4.3 Time stamp

In most cases the content of a message is only valid at a particular point in time. The time stamp may be a time, or time and date, included in a message by the sender.

NOTE 1 Relative time stamps and absolute time stamps may be used.

NOTE 2 Time stamping implicitly requires the time base to be synchronized. For safety applications, synchronization needs to be monitored.

5.4.4 Time expectation

During the transmission of a message, the message sink checks whether the delay between two consecutively received messages exceeds a predetermined value. In this case, an error has to be assumed.

EXAMPLE

Time-slot-oriented access method:

The exchange of messages takes place within fixed cycles and predetermined time slots for every participant.

Optionally: Every participant shall send his data within its time slot even if there is no value change (this is an example of cyclic communication).

To identify a participant who did not transmit within its associated time slot, a source identification is added.

5.4.5 Connection authentication

Messages may have a unique source and/or destination identifier that describes the logical address of the safety relevant participant.

5.4.6 Feedback message

The message sink returns a feedback message to the source to confirm reception of the original message. This feedback message has to be processed by the safety communication layers.

NOTE 1 Some fieldbus specifications use the term “echo” or "receipt" as a synonym.

NOTE 2 This returned feedback message may contain for example only a short acknowledge, or may also contain the original data, or other information enabling the source to check the correct reception.

5.4.7 Data integrity assurance

The safety-related application process shall not trust the data integrity assurance methods if they are not designed from the point of view of functional safety. Therefore, redundant data is included in a message to permit data corruptions to be detected by redundancy checks.

NOTE Communication systems used for safety-related applications may use methods such as cryptography to ensure data integrity, as an alternative to typical methods such as CRCs.

5.4.8 Redundancy with cross checking

In safety-related fieldbus applications, the safety data may be sent twice, within one or two separate messages, using identical or different integrity measures, independent from the underlying fieldbus.

NOTE Additional redundant functional safety communication models are described in Annex A.

In addition to this, the transmitted safety data is cross-checked for validity over the fieldbus or over a separate connection source/sink unit. If a difference is detected, an error shall have taken place during the transmission, in the processing unit of the source or the processing unit of the sink.

When redundant media are used, then common mode protection should be considered using suitable measures (for example diversity, time skewed transmission).

5.4.9 Different data integrity assurance systems

If safety relevant (SR) and non-safety relevant (NSR) data are transmitted via the same bus, different data integrity assurance systems or encoding principles may be used (different hash functions, for example different CRC generator polynomials and algorithms), to make sure that NSR messages cannot influence any safety function in an SR receiver.

NOTE Having an additional data integrity assurance system for SR messages and none for NSR messages is acceptable.

5.5 Relationships between errors and safety measures

The safety measures outlined in 5.4 can be related to the set of possible errors, defined in 5.3. This relationship is shown in Table 1. Each safety measure can provide protection against one or more errors in the 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 1.

Actual protection of a measure against errors depends on the specific implementation of this measure.

NOTE A safety measure can only be listed in the corresponding Table for a given FSCP if this measure takes effect before the guarantied fieldbus safety response time.

Table 1 – Overview of the effectiveness of the various measures on the possible errors

Communication errors	Safety measures							
	Sequence number (see 5.4.2)	Time stamp (see 5.4.3)	Time expectation (see 5.4.4)	Connection authentication (see 5.4.5)	Feedback message (see 5.4.6)	Data integrity assurance (see 5.4.7)	Redundancy with cross checking (see 5.4.8)	Different data integrity assurance systems (see 5.4.9)
Corruption (see 5.3.2)					X [d]	X	Only for serial bus [c]	
Unintended repetition (see 5.3.3)	X	X					X	
Incorrect sequence (see 5.3.4)	X	X					X	
Loss (see 5.3.5)	X				X		X	
Unacceptable delay (see 5.3.6)		X	X [b]					
Insertion (see 5.3.7)	X			X [a]	X		X	
Masquerade (see 5.3.8)				X	X			X
Addressing (see 5.3.9)				X				

NOTE Table adapted from IEC 62280-2 [15] and [28].

[a] Only for sender identification. Detects only insertion of an invalid source.

[b] Required in all cases.

[c] This measure is only comparable with a high quality data assurance mechanism if a calculation can show that the residual error rate Λ reaches the values required in 5.4.9 when two messages are sent through independent transceivers.

[d] Effective only if feedback message includes original data or information about the original data.

5.6 Data integrity considerations

5.6.1 Calculation of the residual error rate

Even when the messages are arriving in a correct (deterministic) manner the safety data still may be corrupted. Thus data integrity assurance is a fundamental component of the safety communication layer to reach a required safety integrity level. Suitable hash functions like parity bits, cyclic redundancy check (CRC), message repetition, and similar forms of message redundancy shall be applied.

The communication channel shall not use the same hash function as the superimposed safety communication layer (see also IEC 62280-1) unless special care is taken for those cases. The safety code shall be functionally independent from the transmission code.

NOTE 1 When CRC is used as the hash function, the communication channel shall not use the same CRC polynomial as the superimposed safety communication layer.

All these methodologies provide a means of achieving low residual error rates. All measures of data integrity assurance shall be implemented within the superimposed parts (safety communication layer) of the controls designed to the required SIL claim.

A supplier may choose various calculation methods for providing estimates for the data integrity mechanisms of fieldbus networks. The results of these calculations may lead to either more effort in the design of hardware and software to provide integrity or more effort in the calculation and proof of the reliability of the overall control system.

The residual error rate is calculated from the residual error probability of the superimposed (safety) data integrity assurance mechanism and the transmission rate of safety messages. In addition, one shall take into account for the assessment the maximum number of information sinks (m) that is permitted in a single safety function.

The Equation (1) shown below shall be used to calculate the residual error rate resulting from RSL (Pe), unless the underlying model does not apply, or if another method may be more relevant. Items of the equation are specified in Table 2.

$$\Lambda_{SL}\,(Pe) = R_{SL}\,(Pe) \times v \times m \qquad (1)$$

NOTE 2 This equation assumes cyclic transmission of safety messages.

Table 2 – Definition of items used for calculation of the residual error rate

Equation items	Definition
Λ_{SL} (Pe)	Residual error rate per hour of the safety communication layer with respect to the bit error probability
Pe	Bit error probability. Unless a better error probability can be proven, a value of 10^{-2} shall be used [a]
R_{SL} (Pe)	Residual error probability of a safety message
v	Maximum number of safety messages per hour
m	Maximum number of information sinks that is permitted in a single safety function (see Figure 6)
[a] A Bit Error Probability (Pe) of 10^{-4} in the presence of continuous electromagnetic interference would lead to a stop of communication (nuisance trip) in case of cyclic data exchange (e.g. watchdog time expires after too many retries). Through correct installation (e.g. shielding, equipotential bonding), these nuisance trips normally can be mitigated. The design of a safety layer cannot be based on such an assumption, as single burst interferences with many perturbed bits are common in industrial environments. In order to detect these kind of disturbances, the error detection mechanisms shall be powerful enough to achieve the required Residual Error Probability RSL (Pe) at a 100 times higher Pe, that is 10^{-2}.	

Figure 6 shows an example of an application where m = 4.

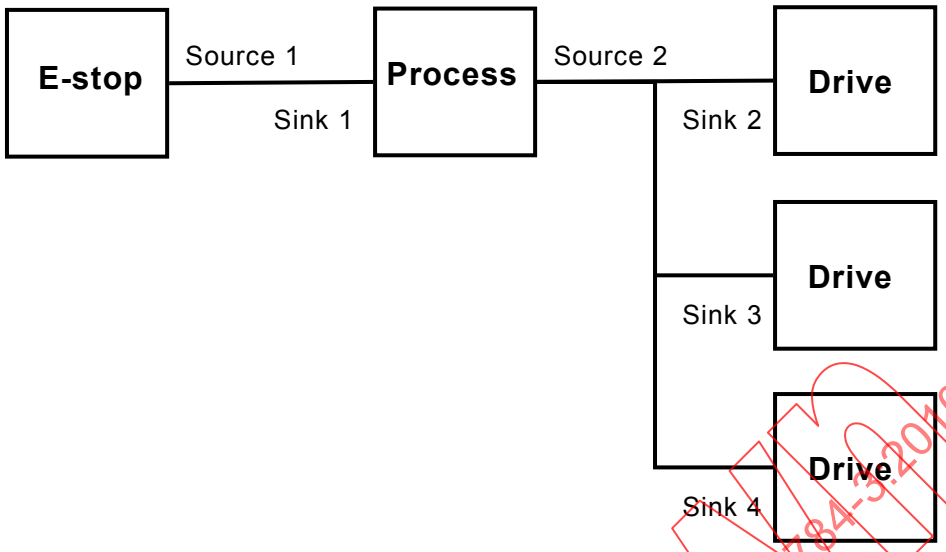


Figure 6 – Example application

5.6.2 Residual error rate and SIL

A functional safety communication system shall provide a residual error rate as specified in Table 3.

Both low demand and high demand mode systems shall have a defined safety function response time, so a necessary number of safety messages per second shall be guaranteed. The calculation of the error rate is based on high demand mode, and is therefore also applicable to the low demand mode.

Table 3 – Relationship of residual error rate to SIL level

Applicable for safety functions up to SIL	Probability of a dangerous failure per hour for the functional safety communication system	Maximum permissible residual error rate for the functional safety communication system
4	$< 10^{-10}$ / h	$\Lambda < 10^{-10}$ / h
3	$< 10^{-9}$ / h	$\Lambda < 10^{-9}$ / h
2	$< 10^{-8}$ / h	$\Lambda < 10^{-8}$ / h
1	$< 10^{-7}$ / h	$\Lambda < 10^{-7}$ / h
NOTE Values in this table are based on the assumption that the functional safety communication system contributes no more than 1 % of the total failures of the safety function.		

5.7 Relationship between functional safety and security

NOTE 1 Security threat and risk assessment is normally necessary for safety-related applications to protect against intentional attacks or unintentional changes. Security can be achieved by establishing appropriate security policies and measures such as physical (for example mechanical, electronic) or organizational measures.

When an application requires electronic security measures, the security shall be implemented within the black channel. The security function can be implemented either within the devices, or at external access points. Some requirements for security will be detailed in the IEC 62443 series.

NOTE 2 Additional profile specific requirements may also be specified in IEC 61784-4 [10].

5.8 Boundary conditions and constraints

5.8.1 Electrical safety

Electrical safety is a precondition for a functional safety communication system. Therefore, all devices connected to it shall conform to the relevant SELV/PELV IEC specifications (for example IEC 61131-2).

NOTE 1 Required additions to the installation guidelines (for example cables, cable installation, shields, grounding, potential balancing) are specified in IEC 61918 and IEC 61784-5.

NOTE 2 Requirements for power supplies (for example single fault prove, use of separate power supplies, SELV/PELV, country specific current limitations, etc) are specified in IEC 61918 and IEC 61784-5.

NOTE 3 Requirements for the standard bus devices (for example assessment) are specific to the functional safety communication profiles.

5.8.2 Electromagnetic compatibility (EMC)

IEC 61508 requires "Increase of interference immunity", but does not specify how to achieve this. Functional safety communication profiles in this standard will use for that purpose the increased test levels and corresponding performance criteria specified in IEC 61326-3-1. IEC 61326-3-2 may be used as an exception, if the intended application exactly matches the specific scope and pre-conditions of IEC 61326-3-2.

NOTE Certain applications may require higher levels than those specified in IEC 61326-3-1, according to Safety Requirements Specification (SRS).

5.9 Installation guidelines

The requirements for installation of equipment using the communication technologies specified in this standard are specified in IEC 61918 and the profile specific parts of IEC 61784-5, as well as any relevant additional standards required by the individual profiles.

Non-compliant devices on the bus could seriously disrupt operation, and thus compromise availability (because of spurious trips, including nuisance trips), subsequently causing the safety feature to be disabled by the user.

Therefore, it is strongly recommended that all products connected to the fieldbus in a safety-related application (even the standard ones) provide an appropriate conformity assessment to the relevant fieldbus protocol (for example manufacturer declaration or third-party assessment).

NOTE Additional details may be provided in the technology-specific parts of this standard if relevant.

5.10 Safety manual

According to IEC 61508-2, device suppliers shall provide a safety manual. A description of the minimum information required by the profile to be included in the safety manual is provided in the relevant profile specific parts.

5.11 Safety policy

Users of this standard shall take into account the following constraints to avoid misunderstanding, wrong expectations or legal actions regarding safety-related developments and applications.

NOTE 1 This includes for example use for training, seminars, workshops and consultancy.

The use of communication technologies specified in this standard in a device does not ensure that all necessary technical, organizational and legal requirements related to safety-related applications of the device have been fulfilled in accordance with the requirements of IEC 61508.

For a device based on this standard to be suitable for use in safety-related applications, appropriate functional safety management life-cycle processes according to the relevant safety standards and relevant legislation/regulations shall be observed. This shall be assessed in accordance with the independence and competence requirements of IEC 61508-1.

In the context of hardware safety integrity, the highest safety integrity level that can be claimed for a safety function is limited by the hardware safety integrity constraints which shall be achieved by implementing Route 1_H of IEC 61508-2, based on hardware fault tolerance and safe failure fraction concepts (to be implemented at system or subsystem level).

The manufacturer of a device using communication technologies specified in this standard is responsible for the correct implementation of the standard, the correctness and completeness of the device documentation and information.

It is strongly recommended that implementers of a specific profile comply with the appropriate conformance tests and validations provided by the related technology-specific organization. Information about test laboratories which can provide conformance tests and validations in accordance with the requirements in this clause can be found in Annex B of each individual profile part.

NOTE 2 These requirements and recommendations are included because incorrect implementations could lead to serious injury or loss of life.

6 Communication Profile Family 1 (FOUNDATION™ Fieldbus) – Profiles for functional safety

6.1 Functional Safety Communication Profile 1/1

Communication Profile Family 1 (commonly known as FOUNDATION™ Fieldbus[11]) 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™[11]) is based on the CP 1/1 basic profile in IEC 61784-1 and the safety communication layer specifications defined in IEC 61784-3-1.

6.2 Technical overview

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

NOTE These safety-related applications are also called safety instrumented systems (SIS) (see IEC 61511 [9]).

The FSCP 1/1 safety communication layer specified in IEC 61784-3-1 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 IEC 61784-3-1 is only applicable to CP 1/1 as described in IEC 61784-1.

IEC 61784-3-1 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 IEC 61784-3-1 is defined in Figure 7.

---

11 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 standard 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 of Fieldbus Foundation.

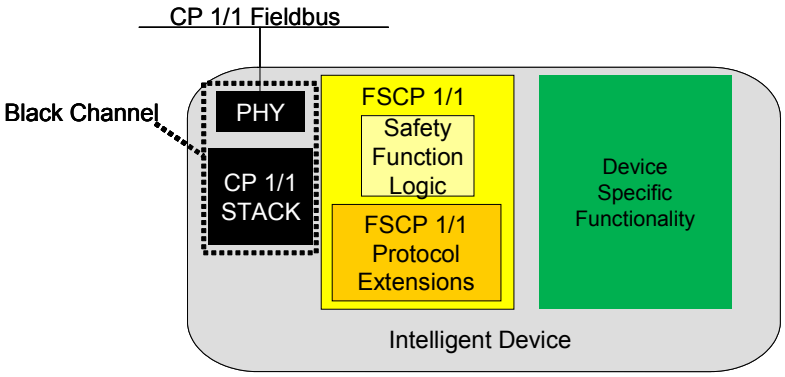


Figure 7 – Scope of FSCP 1/1

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 assessment 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.

Additional information is provided in IEC 61784-3-1.

7 Communication Profile Family 2 (CIP™) – Profiles for functional safety

7.1 Functional Safety Communication Profile 2/1

Communication Profile Family 2 (commonly known as CIP™[12]) defines communication profiles based on IEC 61158-2 Type 2, IEC 61158-3-2, IEC 61158-4-2, IEC 61158-5-2, and IEC 61158-6-2.

The basic profiles CP 2/1, CP 2/2, and CP 2/3 are defined in IEC 61784-1 and IEC 61784-2. The CPF 2 functional safety communication profile FSCP 2/1 (CIP Safety™[12]) is based on the CPF 2 basic profiles in IEC 61784-1 and IEC 61784-2 and the safety communication layer specifications defined in IEC 61784-3-2.

7.2 Technical overview

FSCP 2/1 is based on the producer/consumer model of CPF 2. The pairing of producers and consumers is an important part of the relationship that provides the high integrity needed for safety-related applications.

The FSCP 2/1 safety communication layer is specified using a Safety Validator object. This object is responsible for managing the FSCP 2/1 safety connections and serves as the interface between the safety-related application objects and the link layer connections, as shown in Figure 8. The Safety Validator ensures the integrity of the safety data transfers.

12 CIP™ (Common Industrial Protocol) and CIP Safety™ are trade names of the non-profit organization ODVA, Inc. This information is given for the convenience of users of this International Standard and does not constitute an endorsement by IEC of the trade name holder or any of its products. Compliance to this standard does not require use of the trade names CIP™ or CIP Safety™. Use of the trade names CIP™ or CIP Safety™ requires permission of ODVA.

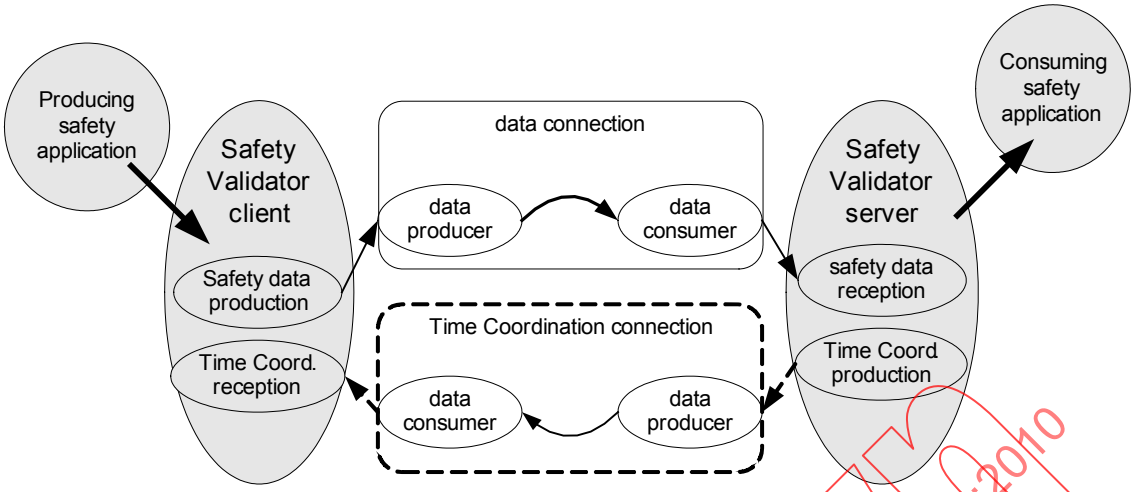


Figure 8 – Relationship of Safety Validators

The integrity of the safety data transfers is ensured as follows:

- the producing safety-related application uses an instance of a client Safety Validator to produce safety data and ensure time coordination;
- the client uses a link data producer to transmit the data and a link consumer to receive time coordination messages;
- the consuming safety-related application uses a server Safety Validator to receive and check data;
- the server uses a link consumer to receive data and a link producer to transmit time coordination messages.

FSCP 2/1 utilizes the black channel concept. The link producers and consumers have no knowledge of the safety packet and implement no safety function. The responsibility for high-integrity transfer and checking of safety data lies within the Safety Validators.

FSCP 2/1 uses the following measures to ensure the integrity of safety messaging:

- time stamp;
- connection authentication;
- data integrity assurance;
- redundancy with cross checking;
- different data integrity assurance systems.

Messages are produced with a timestamp that allows the consumer to verify the age of data being sent. Identification is encoded into each safety-related message to ensure that the correct consumer is using the message. All safety-related messages use a unique CRC. Safety-related data is sent redundantly. Diverse measures for producing safety-related messages are used to ensure that standard CPF 2 messages are not interpreted as safety messages.

Additional information is provided in IEC 61784-3-2.

8 Communication Profile Family 3 (PROFIBUS™, PROFINET™) – Profiles for functional safety

8.1 Functional Safety Communication Profile 3/1

Communication Profile Family 3 (commonly known as PROFIBUS™, PROFINET™[13]) defines communication profiles based on IEC 61158-2 Type 3, IEC 61158-3-3, IEC 61158-4-3, IEC 61158-5-3, IEC 61158-5-10, IEC 61158-6-3, and IEC 61158-6-10.

The basic profiles CP 3/1 and CP 3/2 are defined in IEC 61784-1; CP 3/4, CP 3/5 and CP 3/6 are defined in IEC 61784-2. The CPF 3 functional safety communication profile FSCP 3/1 (PROFIsafe™[13]) is based on the CPF 3 basic profiles in IEC 61784-1 and IEC 61784-2 and the safety communication layer specifications defined in IEC 61784-3-3.

8.2 Technical overview

FSCP 3/1 is based on the cyclic data exchange of a (bus) controller with its associated (field) devices using a one-to-one communication relationship (Figure 9). One controller can operate any mix of standard and safety devices connected to the network. Assigning safety tasks and standard tasks to different controllers also is possible. Any so-called acyclic communications between devices and controllers or supervisors such as programming devices are intended for configuration, parameterisation, diagnosis, and maintenance purposes.

For the realisation of FSCP 3/1, the following four measures have been chosen:

— (virtual) consecutive numbering;

— watchdog time monitoring with acknowledgement;

— codename per communication relationship;

— cyclic redundancy checking for data integrity.

13 PROFIBUS™, PROFINET™ and PROFIsafe™ are trade names of the non-profit organization PROFIBUS Nutzerorganisation e.V. (PNO). This information is given for the convenience of users of this International Standard and does not constitute an endorsement by IEC of the trade name holder or any of its products. Compliance to this standard does not require use of the registered logos for PROFIBUS™, PROFINET™ or PROFIsafe™. Use of the registered logos for PROFIBUS™, PROFINET™ or PROFIsafe™ requires permission of PNO.

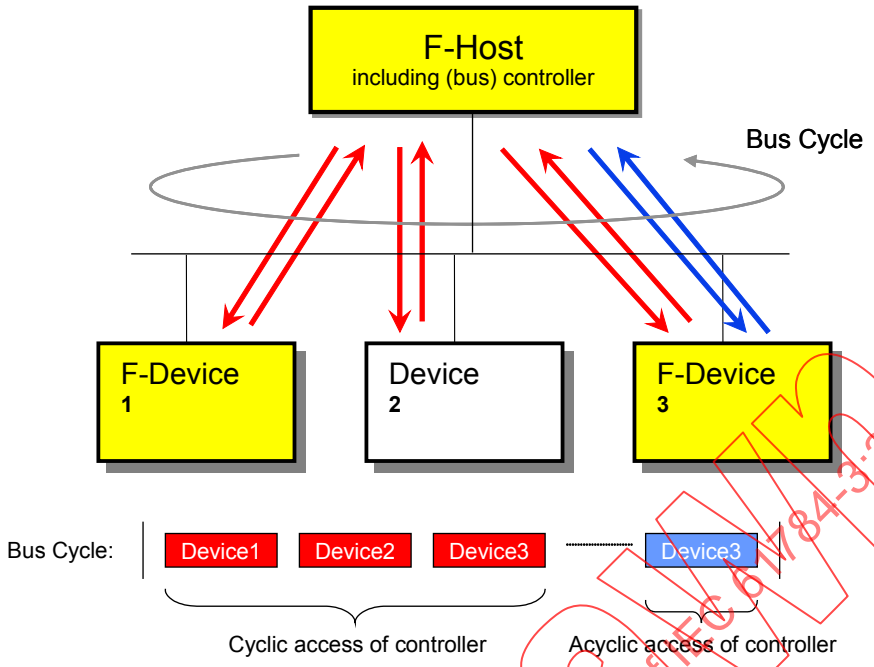


Figure 9 – Basic communication preconditions for FSCP 3/1

The consecutive numbering uses a range that is big enough to secure any malfunction caused by message storing network elements. Every safety device returns a message with a safety PDU for acknowledgement even if there are no process data. A separate watchdog timer on both the sender and the receiver side is used for each one-to-one communication relationship. The unique codename per communication relationship is established for authentication reasons and is encoded within an initial CRC signature value for the cyclically calculated and transmitted CRC2 signature (Figure 10).

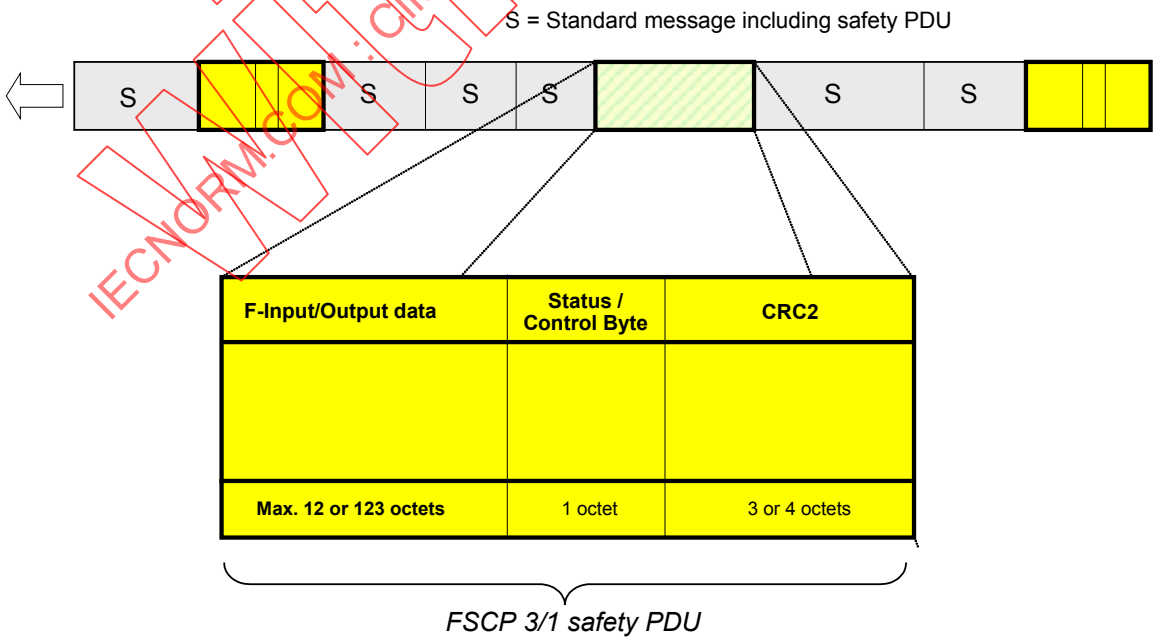


Figure 10 – Structure of a FSCP 3/1 safety PDU

FSCP 3/1 provides two operational modes: V1- and V2-mode. While the measures of the V1-mode are sufficient for the safe data transmission on pure CP 3/1 networks, the more

"generous" features of Ethernet / CP 3/4 to CP 3/6 such as wider address space and buffering switch components are requiring some extensions to the FSCP 3/1 protocol thus leading to the V2-mode. The V1-mode is restricted to CP 3/1 whereas the V2-mode is required for CP 3/4 to CP 3/6 and/or CP 3/1. IEC 61784-3-3 only describes the details of the extended functionality of the so-called V2-mode. Safe communication between PROFINET CBA components (see CP 3/3) is not yet defined. Figure 11 provides an overview on FSCP 3/1 within the CP 3/1 and CP 3/4 to CP 3/6 architectures.

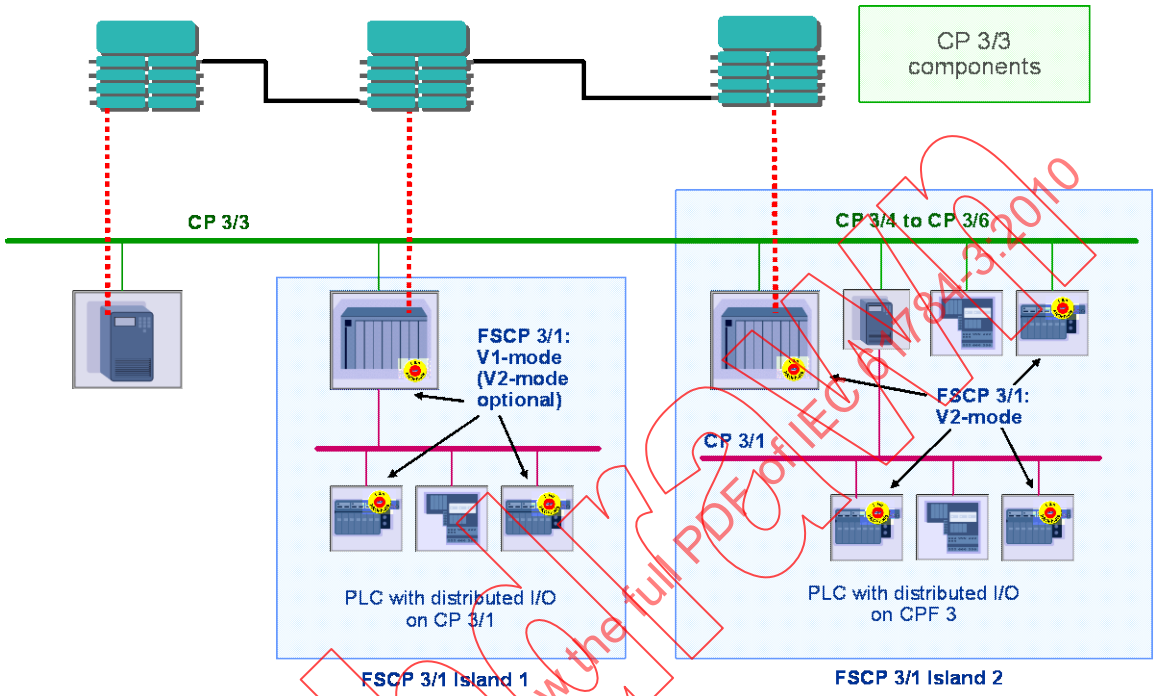


Figure 11 – Safe communication modes

Additional information is provided in IEC 61784-3-3.

9 Communication Profile Family 6 (INTERBUS®) – Profiles for functional safety

9.1 Functional Safety Communication Profile 6/7

Communication Profile Family 6 (commonly known as INTERBUS®[14]) defines communication profiles based on IEC 61158-2 Type 8, IEC 61158-3-8, IEC 61158-4-8, IEC 61158-5-8, and IEC 61158-6-8.

The basic profiles CP 6/1, CP 6/2, CP 6/3 are defined in IEC 61784-1. The CPF 6 functional safety communication profile FSCP 6/7 (INTERBUS Safety™[14]) is based on the CPF 6 basic profiles in IEC 61784-1 and the safety communication layer specifications defined in IEC 61784-3-6.

The profiles CP 6/1, CP 6/2 and CP 6/3 contain optional services, which are specified by profile identifiers. The suitable profile identifiers for CP 6/7 are shown in Table 4.

---

14 INTERBUS® and INTERBUS Safety™ are trade names of Phoenix Contact GmbH & Co. KG, control of trade name use is given to the non profit organization INTERBUS Club. This information is given for the convenience of users of this International Standard and does not constitute an endorsement by IEC of the trade name holder or any of its products. Compliance to this standard does not require use of the trade names INTERBUS® or INTERBUS Safety™. Use of the trade names INTERBUS® or INTERBUS Safety™ requires permission of the INTERBUS Club.

Table 4 – Overview of profile identifier usable for FSCP 6/7

Profile	Master		Slave		
	Cyclic	Cyclic and non cyclic	Cyclic	Non cyclic	Cyclic and non cyclic
Profile 6/1	618	619	611	—	613
Profile 6/2	—	629	—	—	623
Profile 6/3	—	639	—	—	633

The safety communication layer specification given in IEC 61784-3-6 fully applies.

9.2 Technical overview

FSCP 6/7 uses the existing conveyance path for cyclic transmission of data (for process data). This is in principle a master slave concept with a physical ring topology and logical one-to-one relationships between one master and each of its slaves (Figure 12). The data is transmitted via a PDU – commonly known as summation frame – from which each slave extracts its output data and insert its input data.

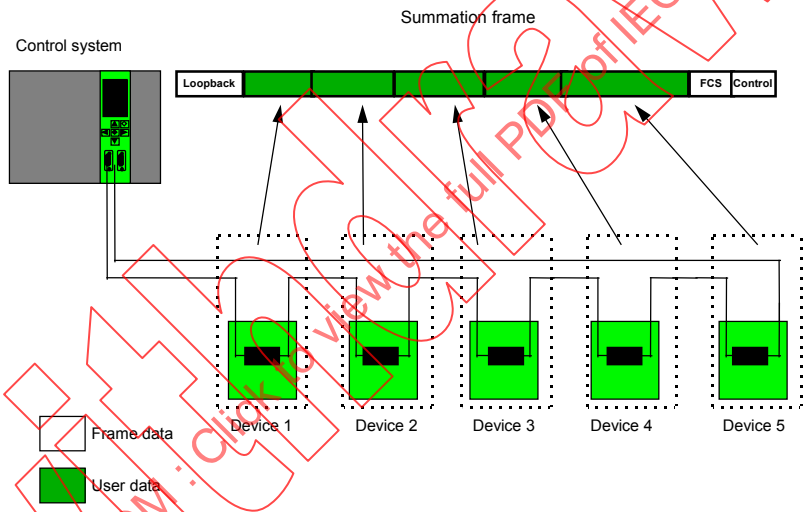


Figure 12 – FSCP 6/7 communication preconditions

The safety communication layer of FSCP 6/7 provides the following safety measures to realize its safety communication layer:

- sequence number;
- time stamp;
- connection authentication;
- cyclic redundancy checking for safety data integrity.

Sequence numbering uses the range from 001 to 111 without 000. The connection authentication (sender/receiver information) consists of 7 bits so that up to 126 slaves can be integrated in the safety fieldbus. Safety data can be conveyed from the safety master to each safety slave and from each safety slave to the safety master within a single data cycle. A separate watchdog timer in each safety output slave ensures a safety function response time for each safety function and can be widely parameterized. The watchdog timer can be adjusted for each safety output channel of a safety output slave.

The safety communication layer of FSCP 6/7 can be used for safety functions up to SIL 3. Therefore the safety fieldbus consumes at a maximum 1 % of the overall PFH. Within the

safety fieldbus $\Lambda < 10^{-7}$ is achieved. An integrated watchdog timer providing the time expectation of each output channel on each safety output slave ensures a functional safety response time. The functional safety response time comprises the fieldbus transmission time from a safety input slave to the master and from the master to the safety output slave including also possible repetitions of the safety PDU due to transmission errors, the processing time on each safety slave (input and output) and the processing time within the PES (usually realized as a safety PLC with an integrated master) and the stopping time of a machine. If the configured time of the integrated watchdog timer of a specific output channel of a safety output slave is exceeded, the corresponding output channel is set to its safe state which is usually the powerless state.

The structure of the safety PDU comprises the safety measures (sequence number, time stamp, connection authentication, CRC) and the safety data. The safety data and the safety measures for each safety slave will be integrated in the summation frame.

Additional information is provided in IEC 61784-3-6.

10 Communication Profile Family 8 (CC-Link™) – Profiles for functional safety

10.1 Functional Safety Communication Profile 8/1

Communication Profile Family 8 (commonly known as CC-Link™[15]) defines communication profiles based on IEC 61158-2 Type 18, IEC 61158-3-18, IEC 61158-4-18, IEC 61158-5-18, and IEC 61158-6-18.

The basic profiles CP 8/1, CP 8/2, and CP 8/3 are defined in IEC 61784-1. The CPF 8 functional safety communication profile FSCP 8/1 (CC-Link Safety™[15]) is based on the CPF 8 basic profiles in IEC 61784-1 and the safety communication layer specifications defined in IEC 61784-3-8.

10.2 Technical overview

FSCP 8/1 is a protocol for communicating safety-relevant data such as emergency stop signals among participants within a distributed network using fieldbus technology in accordance with the requirements of IEC 61508 for functional safety. This protocol may be used in various applications such as process control, manufacturing automation and machinery.

The FSCP 8/1 protocol is designed to support Safety Integrity Level SIL3 (IEC 61508) using CPF 8 by additionally specifying mechanisms for the implementation of sequence number, time expectation, connection authentication, feedback message, data integrity assurance and different data integrity assurance safety measures.

SCL capabilities for FSCP 8/1 are provided with the introduction of safety application service elements (SASE). These SASEs are used in place of their corresponding application service elements (ASEs) as specified in IEC 61784-3-8. However, since they inherit directly from the parent classes defined for CPF 8, these SASEs specify required additions to CPF 8 for functional safety using a black channel approach.

Additional information is provided in IEC 61784-3-8.

---

15 CC-Link™ and CC-Link Safety™ are trade names of the non-profit organization CC-Link Partner Association. This information is given for the convenience of users of this International Standard and does not constitute an endorsement by IEC of the trade name holder or any of its products. Compliance to this standard does not require use of the trade names CC-Link™ or CC-Link Safety™. Use of the trade names CC-Link™ or CC-Link Safety™ requires permission of CC-Link Partner Association.

11 Communication Profile Family 12 (EtherCAT™) – Profiles for functional safety

11.1 Functional Safety Communication Profile 12/1

Communication Profile Family 12 (commonly known as EtherCAT™[16]) defines communication profiles based on IEC 61158-2 Type 12, IEC 61158-3-12, IEC 61158-4-12, IEC 61158-5-12 and IEC 61158-6-12.

The basic profiles CP 12/1 and CP 12/2 are defined in IEC 61784-2. The CPF 12 functional safety communication profile FSCP 12/1 (Safety-over-EtherCAT™[16]) is based on the CPF 12 basic profiles in IEC 61784-2 and the safety communication layer specifications defined in IEC 61784-3-12.

11.2 Technical overview

FSCP 12/1 describes a protocol for transferring safety data up to SIL3 between FSCP 12/1 devices. Safety PDUs are transferred by a subordinate fieldbus that is not included in the safety considerations, since it can be regarded as a black channel. The Safety PDU exchanged between two communication partners is regarded by the subordinate fieldbus as process data that are exchanged cyclically.

FSCP 12/1 uses a unique master/slave relationship between the FSoE Master and an FSoE Slave; it is called FSoE Connection (Figure 13).In the FSoE Connection each device only returns its own new message once a new message has been received from the partner device. The complete transfer path between FSoE Master and FSoE Slave is monitored by a separate watchdog timer on both devices in each FSoE Cycle.

The FSoE Master can handle more than one FSoE Connection to support several FSoE Slaves.

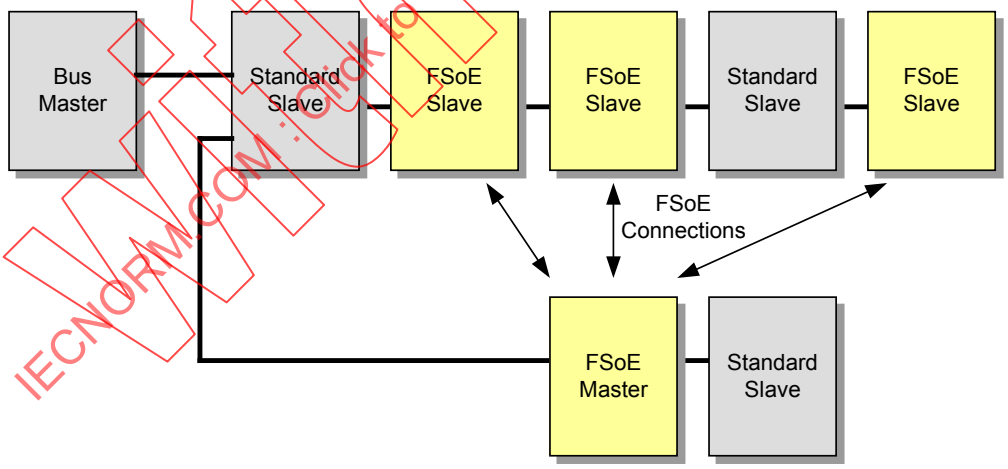


Figure 13 – Basic FSCP 12/1 system

The integrity of the safety data transfers is ensured as follows:

— session-number for detecting buffering of a complete startup sequence;

16 EtherCAT™ and Safety-over-EtherCAT™ are trade names of Beckhoff, Verl. This information is given for the convenience of users of this International Standard and does not constitute an endorsement by IEC of the trade name holder or any of its products. Compliance to this standard does not require use of the trade names EtherCAT™ or Safety-over-EtherCAT™ Use of the trade names EtherCAT™ or Safety-over-EtherCAT™ requires permission of Beckhoff, Verl.

— sequence number for detecting interchange, repetition, insertion or loss of whole messages;

— unique connection identification for safely detecting misrouted messages via a unique address relationship;

— watchdog monitoring for safely detecting of not allowed delays on the communication path;

— cyclic redundancy checking for data integrity for detecting message corruption from source to sink.

State transitions are initiated by the FSoE Master and acknowledged by the FSoE Slave. The FSoE state machine also involves exchange and checking of information for the communication relation.

Additional information is provided in IEC 61784-3-12.

12 Communication Profile Family 13 (Ethernet POWERLINK™) – Profiles for functional safety

12.1 Functional Safety Communication Profile 13/1

Communication Profile Family 13 (commonly known as Ethernet POWERLINK[17]) defines communication profiles based on IEC 61158-3-13, IEC 61158-4-13, IEC 61158-5-13, and IEC 61158-6-13.

The basic profile CP 13/1 is defined in IEC 61784-2. The CPF 13 functional safety communication profile FSCP 13/1 (Ethernet POWERLINK safety[17]) is based on the CPF 13 basic profiles in IEC 61784-2 and the safety communication layer specifications defined in IEC 61784-3-13.

12.2 Technical overview

Functional Safety Communication Profile FSCP 13/1 is designed to provide fieldbus communication for functional safety applications in the microsecond range.

FSCP 13/1 services and protocol specify safety data communication between safety devices. FSCP 13/1 protocol technology is designed to provide SIL 3 safety function according to IEC 61508.

The following services are defined:

— network configuration;

— network management (booting, runtime diagnosis);

— exchange of spontaneous data; and

— exchange of synchronous data.

Synchronous data communication between safety devices is modelled according to the publisher subscriber model (see Figure 14), whereas spontaneous data communication uses the client server model (see Figure 15).

---

17 Ethernet POWERLINK and Ethernet POWERLINK safety are trade names of the non-profit organization Ethernet POWERLINK Standardization Group (EPSG). This information is given for the convenience of users of this International Standard and does not constitute an endorsement by IEC of the trade name holder or any of its products. Compliance to this standard does not require use of the trade names Ethernet POWERLINK or Ethernet POWERLINK safety. Use of the trade names Ethernet POWERLINK or Ethernet POWERLINK safety requires permission of Ethernet POWERLINK Standardization Group (EPSG).

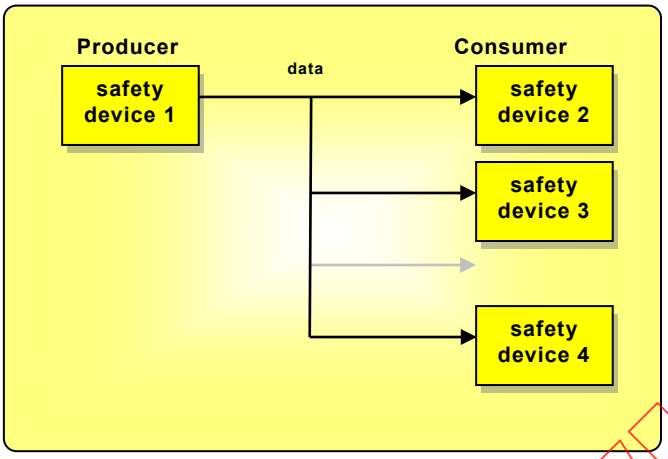


Figure 14 – Producer consumer example

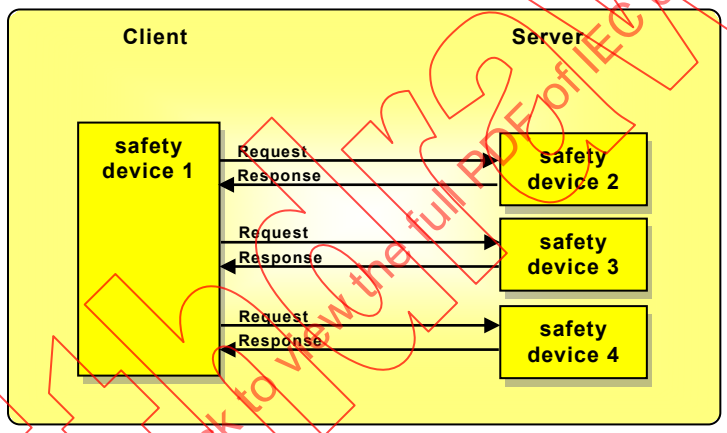


Figure 15 – Client server example

Additional information is provided in IEC 61784-3-13.

13 Communication Profile Family 14 (EPA®) – Profiles for functional safety

13.1 Functional Safety Communication Profile 14/1

Communication Profile Family 14 (commonly known as EPA®[18]) defines communication profiles based on IEC 61158-3-14, IEC 61158-4-14, IEC 61158-5-14, and IEC 61158-6-14.

The basic profiles CP 14/1 and CP 14/2 are defined in IEC 61784-2. The CPF 14 functional safety communication profile FSCP 14/1 (EPASafety®[18]) is based on the CPF 14 basic profiles in IEC 61784-2 and the safety communication layer specifications defined in IEC 61784-3-14.

---

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

13.2 Technical overview

EPASafety describes the safe communication specification used to connect safety field devices and controllers in EPA systems. It is a supplementary technology based on EPA protocol specified in IEC 61158 and IEC 61784-2 to reduce the failure or error probability of the data transmission between safety transmitters, actuators and field controllers to the level required by the relevant standards, or better.

EPA communication is based on black channel principle as shown in Figure 16. Black channel includes non safety-relevant devices such as wires, fibre optics, repeater, barrier, power supplies, ASIC, communication stack, EPA bridge, interface. Communication stack includes the following layers: physical, data link, network (IP), transport (UDP) and application.

During data transfer in black channel, faults or errors maybe occur with the following reasons:

— random fault;

— standard hardware failure/fault;

— system failure caused by standard hardware or software components.

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

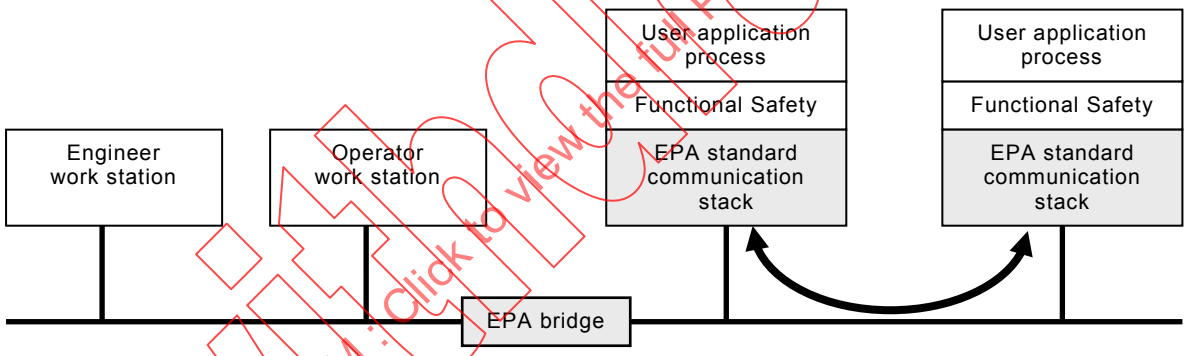


Figure 16 – FSCP 14/1 safety communication architecture

Additional information is provided in IEC 61784-3-14.

Annex A
(informative)

Example functional safety communication models

A.1 General

This annex considers various models of implementation structure for safety fieldbus devices. These models provide different fault detection mechanisms. Models shown below are only intended to illustrate possible implementation structures. IEC 61508 should be used for overall system design.

Some examples are listed in the following subclauses – other models may be used.

A.2 Model A

Model A shown in Figure A.1 serves as the base reference model for the other models. Only one channel is connected to the bus.

Data from both safety communication layers are safety-checked and cross-checked. Both safety communication layers are involved in the production of the message. If cross-checking shows discrepancy, an appropriate action is initiated to maintain safety.

NOTE The implementation can be realized via hardware and/or software diversity.

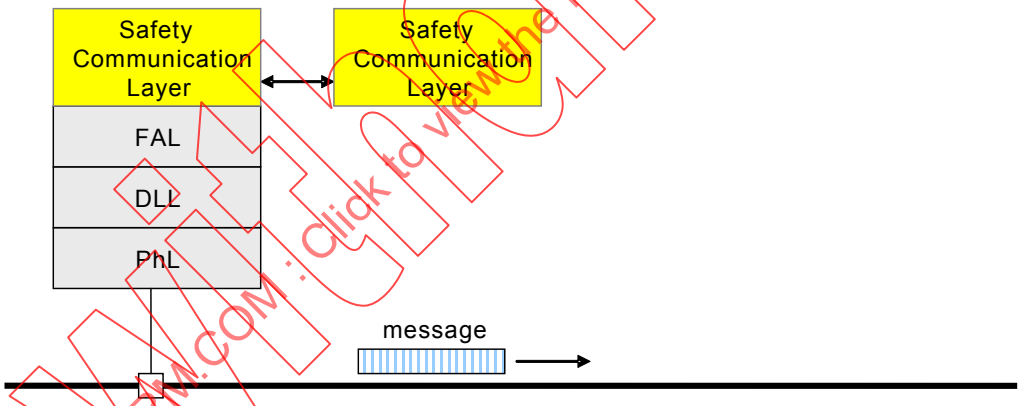


Figure A.1 – Model A

A.3 Model B

Model B in Figure A.2 shows a system where all safety communication layers, transmission layers and transmission media exist twice.

The messages from both safety communication channels are safety-checked and cross-checked. If cross-checking shows discrepancy, an appropriate action is initiated to maintain safety.

NOTE Transmission layers and transmission media may be of different types.

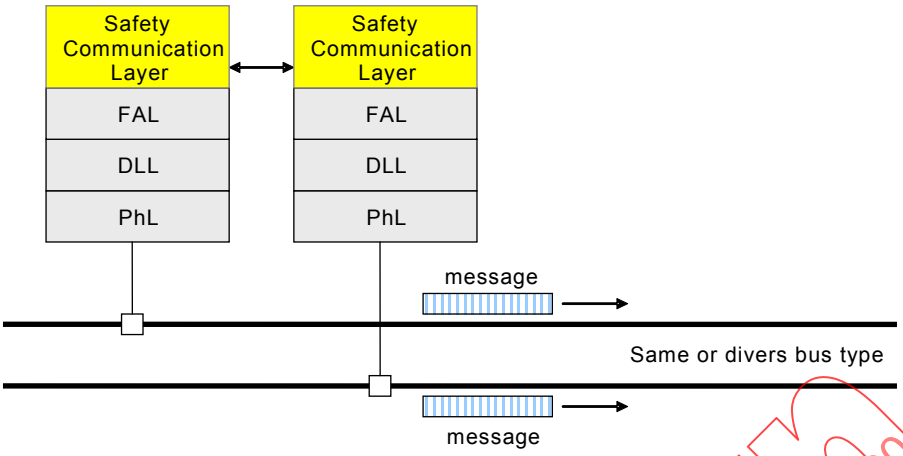


Figure A.2 – Model B

A.4 Model C

Model C in Figure A.3 describes a redundancy approach similar to Model B. This model uses only one transmission medium.

The messages from both safety communication channels are safety-checked and cross-checked. If cross-checking shows discrepancy, an appropriate action is initiated to maintain safety.

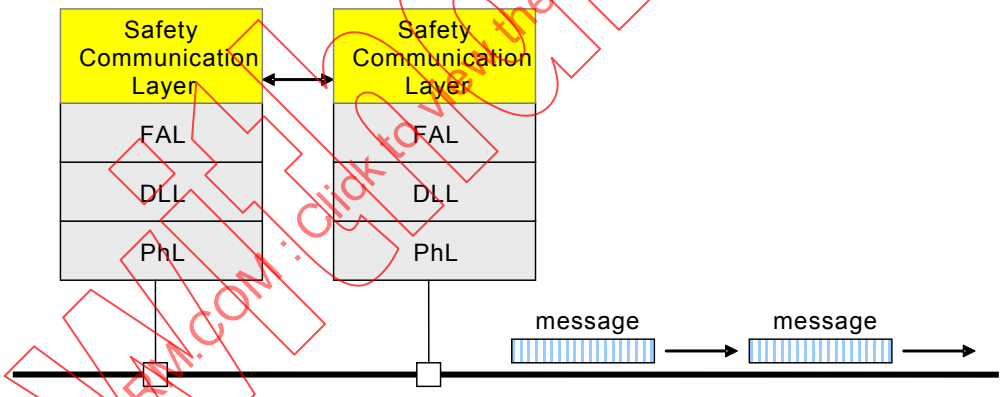


Figure A.3 – Model C

A.5 Model D

Model D in Figure A.4 shows a system with dual safety communication layers while the transmission layers exist only once. Both safety communication layers access the transmission layers independently. The safety data may be transmitted by one or two messages.

The messages from both safety communication layers are safety-checked and cross-checked. If cross-checking shows discrepancy, an appropriate action is initiated to maintain safety.

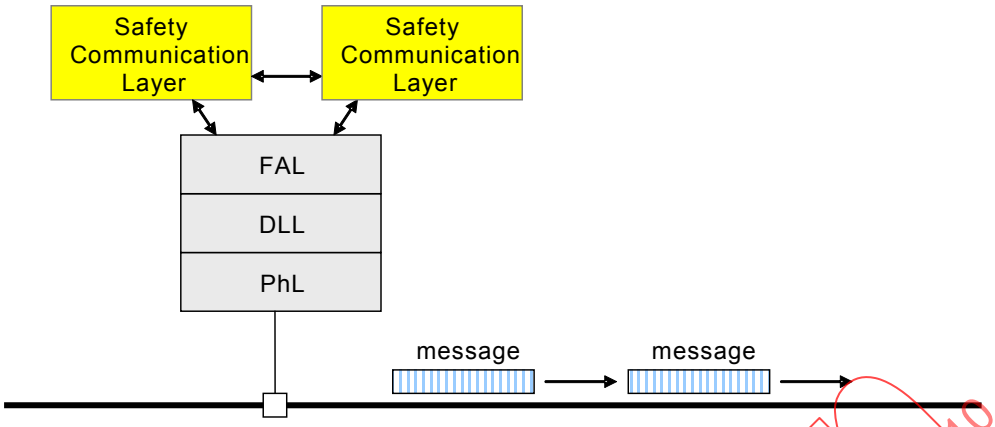


Figure A.4 – Model D

Annex B
(informative)

A safety communication channel model using CRC-based error checking

B.1 Overview

This annex contains a model for benchmarking purposes which has been used by some assessment bodies.

NOTE The considerations in the following subclauses do not cover all the possible failures and errors of black channel transmission systems. Additional requirements can be found in Clause 7 of IEC 62280-1:2002.

B.2 Channel model for calculations

The model shown in Figure B.1 is used to calculate/evaluate in a first step the probability for a certain number of perturbed bits within the safety communication layer. The various considerations on specific errors within the black channel are not covered here.

The model assumes independent error detection mechanisms are used by both the black channel and the safety communication layer. Whenever the error detection mechanism of the black channel fails, the error detection mechanism of the safety communication layer shall be good enough alone to provide the necessary residual error rate. A functioning error detection mechanism within the black channel will filter out certain bit error patterns and thus the error detection mechanism of the safety communication layer has to take into account a certain bit error model. The following basic equations can be used for simplified assessments of residual error rates or as a basis for more sophisticated approaches.

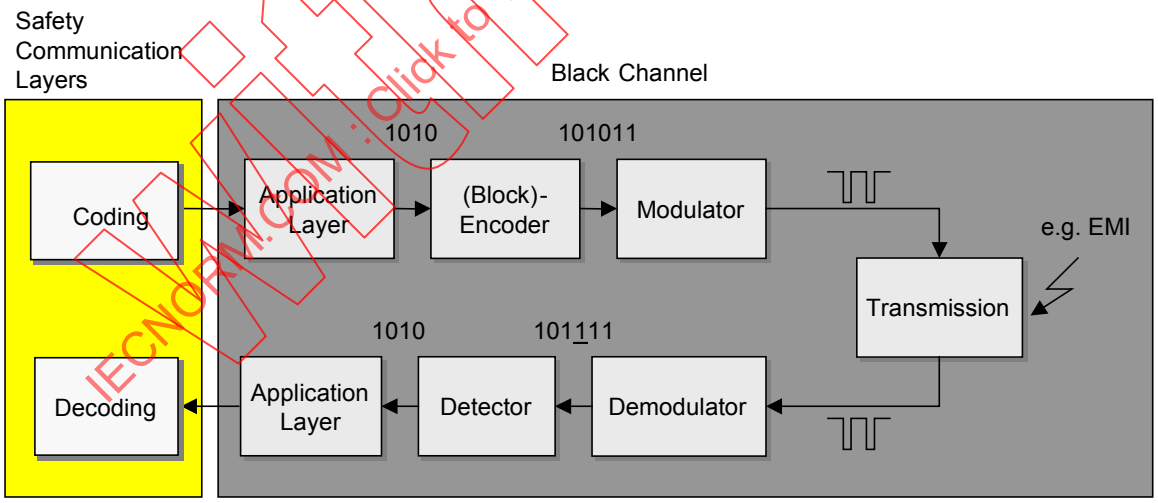


Figure B.1 – Communication channel with perturbation

A binary channel is called symmetric when the probabilities P for both directions of perturbation for a bit cell are equal: 1→0 and 0→1 (see Figure B.2). Furthermore it is assumed all bit cells have the same bit error probability $P_e = P$.

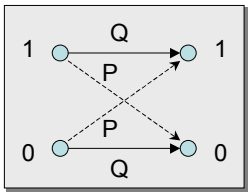


Figure B.2 – Binary symmetric channel (BSC)

Usually safety data are transmitted in blocks of a certain length n. In this case the error probability for a number of k perturbed bits (in a block of length n) can be calculated with the Equation (B.1) shown below.

$$P_n(k) = \binom{n}{k} \times P_e^k \times (1 - P_e)^{n-k} \qquad \text{(B.1)}$$

In case the block contains a fictive coding to detect error patterns up to d-1 such as shown in Figure B.4 with a Hamming distance d, an upper limit residual error probability $R_{WC}(P_e)$ can be calculated with the Equation (B.2) shown below.

NOTE A coding with this feature does not exist in reality, thus it is called fictive.

$$R_{UL}(P_e) = \sum_{k=d}^{n} \binom{n}{k} \times P_e^k \times (1 - P_e)^{n-k} \qquad \text{(B.2)}$$

However, this simplified equation does not take into account that even a simple parity bit (Hamming distance d=2) allows more error patterns to be detected than just 1 bit. For exact calculations the sum of all individual undetectable error patterns shall be used if there is no other method or approximation available.

B.3 Cyclic redundancy checking

B.3.1 General

The residual error rate, which is based on the detection using a CRC-mechanism for BSC, can be calculated using the Equation (B.3) below (residual error probability for CRC polynomials).

$$R_{CRC}(P_e) = \sum_{i=1}^{n} A_i \times P_e^i \times (1 - P_e)^{n-i} \qquad \text{(B.3)}$$

where

A_i is the distribution factor of the code (determined either by computer simulation or a mathematical analysis);

n is the number of bits in the block, including its CRC signature;

P_e is the bit error probability.

Investigations for the method of cyclic redundancy checking (CRC) have shown that for the particular class of so-called proper CRC polynomials a weighting factor 2^{-r} is applicable within the equation to build an approximation (see Equation (B.4) below – residual error probability approximation for CRC polynomials).

$$R_{CRC}(P_e) \approx 2^{-r} \times \sum_{k=d_{min}}^{n} \binom{n}{k} \times P_e^k \times (1-P_e)^{n-k} \qquad \text{(B.4)}$$

The function (curve) of this approximation Equation (B.4) may deliver smaller (better) residual error probability values than exact calculations. For a high bit error probability (close to 0,5), the worst case value is 2^{-r}.

The value r represents the number of CRC bits added to the message part as a CRC signature to provide error detection, as shown in Figure B.3.

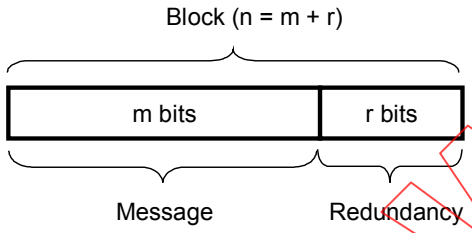


Figure B.3 – Example of a block with message and CRC bits (redundancy code)

Figure B.4 illustrates the background for the Equations (B.2) and (B.4).

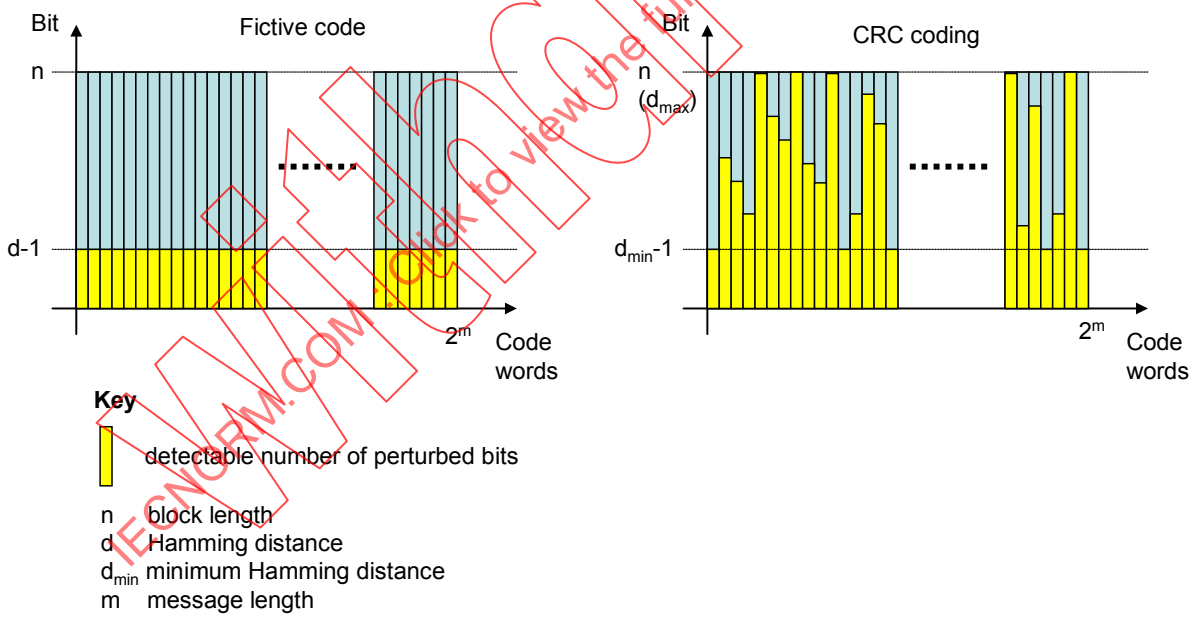


Figure B.4 – Block codes for error detection

Usually the CRC mechanism provides better residual error probability with smaller block length n. Thus a dependency exists between block length n and the minimum Hamming distance d_{min} for a given proper CRC polynomial (see Table B.1).

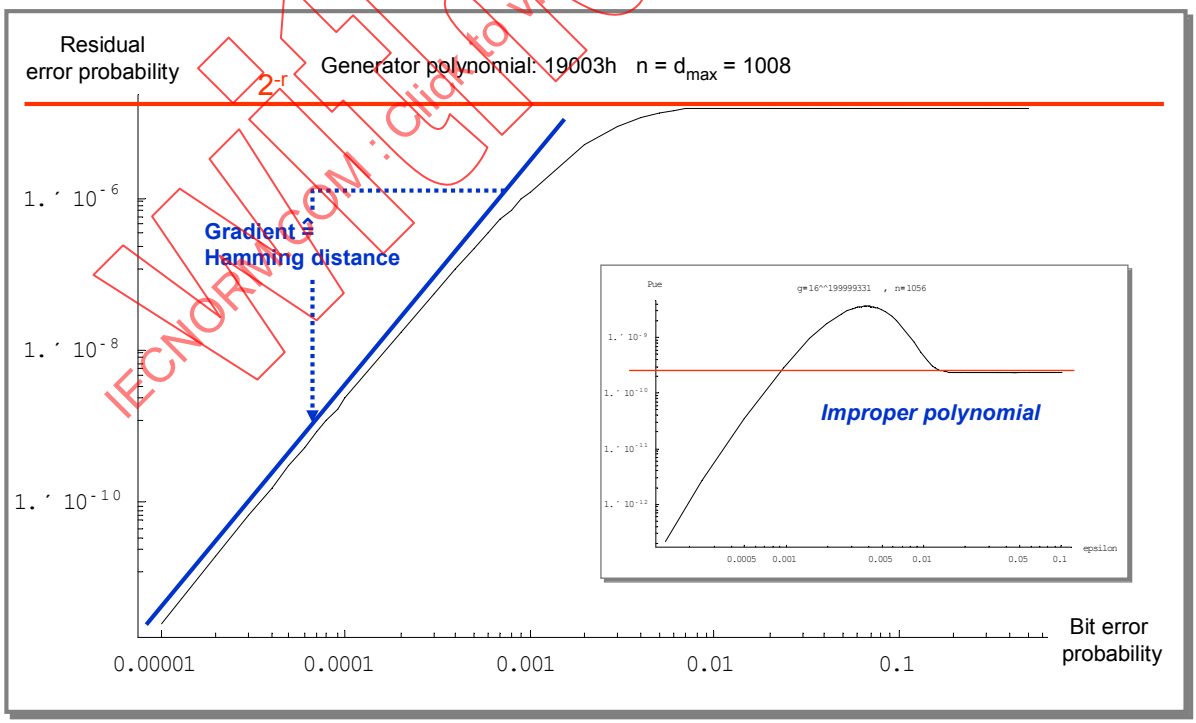
Table B.1 – Example dependency d_{min} and block length n

d_{min}	d_{max} = n
12	17
8	18…22
6	23…130
4	131 … 258
2	≥ 259

B.3.2 Considerations concerning CRC polynomials

Proper CRC polynomials are characterized by a monotonic ascending slope of the residual error probability function over the bit error probability. Figure B.5 illustrates the difference between a proper and an improper CRC polynomial. It is highly recommended to deploy only those proper CRC polynomials in order to simplify the proof of sufficient residual error rates. Several ways are known in science for the calculation of such functions, for example [30], [36] and [37]. Whether or not the polynomial is proper has to be checked for all the intended safety block sizes (see Table B.1). Improper polynomials may show a better residual error probability at high bit error probabilities (2^{-r}) than with smaller bit error probabilities (>2^{-r}). When using improper CRC polynomials, the worst case value (>2^{-r}) shall be used, whereas with proper polynomials it is sufficient to use 2^{-r} for an estimate of the residual error probability.

In some cases a particular function (curve) of a chosen CRC generator polynomial may deliver smaller (better) residual error probability values up to the required bit error probability limit of 10^{-2}. In these cases it is highly recommended to use the worst case values 2^{-r} or >2^{-r}, respectively, as only messages with high-order bit errors (non equally distributed bit errors) may reach the safety communication layer.



n = number of bits in a block including CRC signature r.

Figure B.5 – Proper and improper CRC polynomials

The gradient of the slope is a measure for the minimum Hamming distance of the particular CRC polynomial and block size.

CRC coding offers good protection against burst type electromagnetic interference. Any burst error up to the size of the CRC signature in bits will be detected.

Annex C
(informative)

Structure of technology-specific parts

All technology-specific parts of this standard will be numbered according to their CPF number in IEC 61784-1 or IEC 61784-2.

EXAMPLE The technology-specific part containing specifications for the functional safety communication profiles of CPF 33 would be numbered IEC 61784-3-33.

All technology-specific parts will have the same general structure, to facilitate comparison between the different technologies. This structure is detailed in Table C.1.

Table C.1 – Common subclause structure for technology-specific parts

Clause and subclause No.	Title	Contents
	Introduction	This introduction is the same for all parts of IEC 61784-3
1	Scope	This scope is standardized for all parts of IEC 61784-3
2	Normative references	Normative documents for this part
3	Terms, definitions, symbols, abbreviated terms and conventions	—
3.1	Terms and definitions	—
3.1.1	Common terms and definitions	Common terms used in this part
3.1.2	CPF X: Additional terms and definitions	Technology-specific terms used in this part
3.2	Symbols and abbreviated terms	—
3.2.1	Common symbols and abbreviated terms	Common symbols used in this part
3.2.2	CPF X: Additional symbols and abbreviated terms	Technology-specific symbols used in this part
3.3	Conventions	Conventions which are used to describe the various elements of the safety communication layer (for example state tables, sequence diagrams)
4	Overview of FSCP X/1 (Safetyname™)	Overview of the functional safety communication profile, and relevant introductory material (including objectives and motivations for the technology)
5	General	—
5.1	External documents providing specifications for the profile	List of the reference documents required by the technologies, especially those that could not be listed in Clause 2 (because they are not "official" standards such as IEC or ISO, for example consortia documents), and thus were included in Bibliography, together with all "informative only" documents
5.2	Safety functional requirements	May include description of safe states (see IEC 61508-1:2010, 7.10.2.6)
5.3	Safety measures	May include measures to be considered from 5.4
5.4	Safety communication layer structure	May include decomposition of the SCL
5.5	Relationships with FAL (and DLL, PhL)	May include existing diagnostics, expected services, constraints (for example, “to be used in conjunction with FSCP x/y”)
5.5.1	Data Types	List of the IEC 61158 data types used by the profile
6	Safety communication layer	May include application objects used, diagnostic services

Clause and subclause No.	Title	Contents
	services	
7	Safety communication layer protocol	First subclause is listed below, others may be added as needed. May include specific time mechanisms , state machines, sequence charts, reaction on power off/power down, diagnostic protocol and corresponding diagnosis
7.1	Safety PDU format	Includes detailed definition of safety PDU (message) formats. Will include several subclauses to specify the various format elements (for example safety CRC specification)
8	Safety communication layer management	Includes specifications for the following aspects of parameterization: - safe parameter data supplied by another safety device (for example a parameter server) - safe parameter data supplied by a tool (for example device description) (including any required measure to secure the storage, handling and transfer)
9	System requirements	First subclauses are listed below, others may be added as needed
9.1	Indicators and switches	Specifications for device indicators and switch function and behaviour
9.2	Installation guidelines	Detailed clause references within IEC 61918 or other relevant documents
9.3	Safety function response time	Calculations and related examples of reaction times relevant for the technology (for example worst case reaction time of safety loop)
9.4	Duration of demands	Specifications for the duration of demands within devices
9.5	Constraints for calculation of system characteristics	Includes black channel retries, number of telegram per second, number of message sinks
9.6	Maintenance	Specifications for system behaviour in case of device repair and replacement
9.7	Safety manual	If relevant, includes the minimum information required by the profile to be included in the safety manual
9.8	Wireless transmission channels	This subclause is optional. If relevant, include specific requirements when using wireless transmission
9.9	Conformance classes	This subclause is optional. If relevant, include additional conformance requirements for the base fieldbus protocol
10	Assessment	Include information on assessment requirements
Annex A (informative)	Additional information for functional safety communication profiles of CPF X	Mandatory informative annex used to provide additional non-normative information on the protocol. If there is none, then this will contain the following sentence: “There is no additional information for this FSCP”.
A.1	Hash function calculation	For example algorithms for CRC calculation
Annex B (informative)	Information for assessment of the functional safety communication profiles of CPF X	Mandatory informative annex used to provide information about test laboratories which test and validate the conformance of FSCP X/1 products with IEC 61784-3-X
	Bibliography	Bibliographic references relevant for this part

Annex D
(informative)

Assessment guideline

D.1 Overview

This guideline is intended for the assessment and test of communication systems for the transmission of safety-related messages. The safety communication may take place between various processing units of a safety control system and/or between intelligent safety sensors/actuators and processing units of a safety control system.

It is highly recommended to use this guideline when assessing a particular safety communication profile or communication system as well as safety-related devices using these profiles.

The documentation that is provided for the test or assessment shall specify the exact operating conditions according to 5.8.2. No deviation from these conditions is permitted under any circumstances.

If a safety communication system is an integral part of a safety-related device for which a product standard exists (for example IEC 61496-1 [5]), then this product and the related safety communication components shall meet the requirements to the extent that is mentioned in the scope of the relevant standard, or as defined in a specific safety communication profile within the IEC 61784-3 series.

D.2 Channel types

D.2.1 General

This part defines two general types of safety communication concepts, the black channel and the white channel approach. This guideline covers both safety communication concepts.

D.2.2 Black channel

According to definition 3.1.1.3, black channel type safety communication requires only evidence of design or validation of the safety communication layer (SCL) according to IEC 61508. It is possible for a safety device designer to use a preassessed and approved hardware/software component, which provides the functions of the particular SCL. If the designer implements this component in its specified manner, a safety assessment of the component itself according to IEC 61508 can be omitted. Thus, efforts can be reduced to the assessment of the safety-related technology of the device and the correct implementation of the SCL component.

Assessment: Check of documentation and implementation within the system as specified; validation and verification of the calculations provided by the manufacturer; verification of the parameters that are necessary for these calculations.

D.2.3 White channel

According to definition 3.1.1.44, white channel type safety communication requires all relevant hardware and software components to be designed, implemented and validated according to IEC 61508. Due to the large variety of possible solutions this guideline only provides help on how to proceed with the aspects of data integrity assurance. Further information can be found in IEC 62280-1.

Normally, individual white channel approaches can be evaluated using one of the models outlined in Annex A.

D.3 Data integrity considerations for white channel approaches

D.3.1 General

For data integrity considerations two classes of white channels can be identified as described in D.3.2 and D.3.3.

D.3.2 Model B and C

This approach considers each channel of the bus communication system not to be safe. The protocol layers are redundant and two messages are sent. Hereby the data integrity measures of the bus communication system are used completely. Sufficient error detection is not possible if one of the two channels fails. Due to their architecture, some known bus communication systems enable the other participants to check each message and thus already detect the majority of the error possibilities.

NOTE 1 Model B and C can be realized both as white or black channel solutions.

NOTE 2 Equations in this subclause may also be applied to black channel systems.

The following approach is based on the concept "redundancy with cross checking", as described in 5.4.8. This means, in case of twofold transfer of the safety message and bit by bit comparison within the receiver it is a precondition for an undetected error that both messages are corrupted equally. With the help of the BSC model, the residual error probability can be calculated along the lines of Annex B. The probability for a particular bit error combination within each message is the same in this case and thus the expression is squared. The possibilities for bit error combinations are in accordance with those of a single message (binomial coefficients).

NOTE 3 FSCPs should adjust the individual measures such that a maximum of independence can be assumed. Otherwise, it is necessary to use more complex equations considering the dependency.

When assuming data integrity assurance via CRC signature the same factor 2^{-r} is effective (see Annex B) and Equation (D.1) provides an estimate on the residual error probability.

$$R_{EMC}(P_e) \approx 2^{-r} \times \sum_{k=d_{min}}^{n} \binom{n}{k} \times \left(P_e^{\,k} \times (1-P_e)^{n-k} \right)^2 \quad \text{(D.1)}$$

NOTE 4 This equation can only be applied for proper polynomials (see B.3.2).

An analysis according to D.3.3 together with a calculation using Equation (D.2) is required for a complete evaluation of the residual error probability in case of a white channel solution. IEC 62280-1 should be considered to the extent to which it is applicable.

The calculation of $\Lambda_{SL}(P_e)$ is carried out along the lines of 5.6.1 (Equation (1)).

The complete safety assessment shall be accomplished according to IEC 61508 (for example Failure Mode and Effect Analysis, Safe Failure Fraction, Common Cause Errors).

Assessment: Check of documentation and implementation within the system as specified; validation and verification of the calculations provided by the manufacturer; verification of the parameters that are necessary for these calculations.

D.3.3 Model A and D

This approach relies on the error detection measures of existing bus transmission channels and supplements these with additional measures in the superimposed safety communication layer to reach the desired SIL.

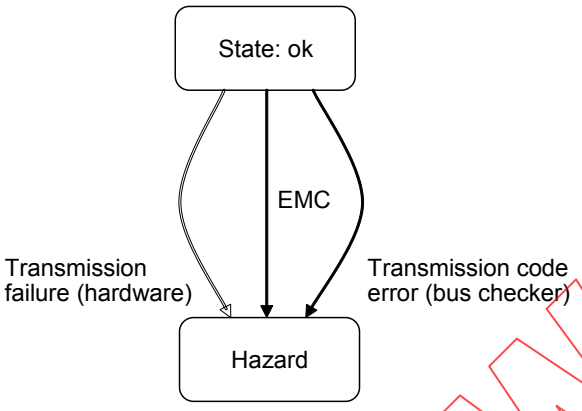


Figure D.1 – Basic Markov model

Within this approach due to safety hazards through failures of the bus protocol circuits their hardware fault tolerance needs to be considered and thus their life expectancy.

In this case a Markov analysis can be put down to three fundamental transition possibilities (Figure D.1) according to IEC 62280-1:

- undetected faulty messages that are caused by actual hardware failures in the transmission layers that result in passing of corrupted messages (R_{HW});
- faulty messages with undetected bit errors caused by electromagnetic interferences (EMC) that occur as part of normal operation (R_{EMC});
- undetected faulty messages that are caused by failures in the corresponding bus checking part of the transmission channel (R_{TC}).

The residual error probability R_{AD} of the system is the summation of the individual probabilities (Equation (D.2). The calculation of $\Lambda_{SL}(p_e)$ is carried out along the lines of 5.6.1 with the residual error probability:

$$R_{AD} = R_{HW} + R_{EMC} + R_{TC} \qquad \text{(D.2)}$$

The complete safety assessment shall be accomplished according to IEC 61508 (e.g. Failure Mode and Effect Analysis, Safe Failure Fraction, Common Cause Errors). IEC 62280-1 should be considered to the extent to which it is applicable.

Assessment: Check of documentation and implementation within the system as specified; validation and verification of the calculations provided by the manufacturer; verification of the parameters that are necessary for these calculations.

D.4 Verification of safety measures

D.4.1 General

This part of the assessment guideline specifies the verification requirements for a particular safety communication profile.

D.4.2 Implementation

Messages to be transmitted safely shall be generated in a safe manner (in line with the required SIL). The transmission medium (e.g. bus line including interface ASICs) in itself is considered not safe. The safety measures are within the sole responsibility of the processing units of message source and message sink. This concerns white and black channel solutions.

Assessment: The requirements of IEC 61508 or other additional standards such as IEC 61784-3 shall be considered and checked. These requirements are beyond the scope of this assessment guideline and are defined normatively.

D.4.3 "De-energize to trip" principle

A time expectation mechanism (e.g. watchdog timer) shall be used in all cases.

Assessment: See 5.4.4.

D.4.4 Safe state

A mechanism for error detection and reaction shall be provided at the receiver that is responsible to establish a safety-related reaction to achieve a safe state, within the process fault tolerance time.

Assessment: Check of documentation and implementation, measurement of the reaction time for the safety device using safety communication at worst case conditions of the system (e.g. in the presence of errors or failures).

D.4.5 Transmission errors

When transmission errors according to 5.3 occur, a defined fault reaction shall be initiated (e.g. stop demand).

Assessment: Check of documentation, implementation, calculation if necessary, and functional test; extended functional tests along the line of IEC 61508.

D.4.6 Safety reaction and response times

The maximum safety function response time specified by the manufacturer and the time required to complete a safety-related reaction shall not be exceeded, even in the presence of errors and failures.

NOTE In some bus systems, the transmission rate and the reaction or response times depend on the number of participants. If transmission rate and reaction or response times are safety-related, it may be necessary to limit the number of participants.

Assessment: Check of documentation and implementation; measurement of the reaction and/or response times at worst case conditions for the particular system. The manufacturer or the safety communication profile shall provide the definition of the number and timing of errors to be considered.

D.4.7 Combination of measures

For the transmission of safety-related messages over bus systems a combination of measures from those quoted in 5.4 shall be implemented in such a manner that each error described in 5.3 is detected within the process fault tolerance time. Table 1 assists in choosing the appropriate individual measures.

Assessment: All the technical measures in use shall be verified for completeness according to Table 1. Implementation of the measures shall be according to the required SIL.

D.4.8 Absence of interference

It shall be proved that non-safety-related communication participants do not interfere with safety communication participants.

Assessment: Checking of the documentation and implementation shall include specific functional tests and those with impact of for example personal computer (PC) simulation such as traffic burden or stimulated address changes.

D.4.9 Additional fault causes (white channel)

In addition to the already described methods for the estimation of residual errors using the BSC model, further fault causes need to be considered and controlled. Details can be found in IEC 62280-1 or [29].

Assessment: All the technical measures in use shall be verified against the requirements in IEC 62280-1.

D.4.10 Reference test beds and operational conditions

As far as feasible, all parts of a safety communication system should be tested together. Otherwise, parts of a safety communication system are tested separately. In the second case, reference systems (test beds) and/or simulators should be defined by the particular safety communication profile and implemented using a particular variety of different devices from different suppliers where possible.

The test bed should take into account worst case conditions, for example connection length or number of devices. Signals that are required for the safety function shall be simulated or otherwise imposed.

Relevant operational modes shall be defined for use during testing, such as cyclic data exchange of process values or acyclic data exchange of parameterization data.

Assessment: Test and inspections according to the definitions of the particular FSCP or the specifications of the manufacturer of the EUT.

D.4.11 Conformance tester

Conformance to a particular FSCP should be tested by a profile conformance tester defined and provided by the individual FSCP.

NOTE Conformance testing includes both positive and negative tests.

Assessment: Test and inspections according to the definitions of the particular FSCP.

Bibliography

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

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

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

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

[4] IEC 61131-6[19], *Programmable controllers – Part 6: Functional safety*

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

[6] IEC 61508-4:2010[20], *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations*

[7] IEC 61508-5:2010[20], *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 5: Examples of methods for the determination of safety integrity levels*

[8] IEC 61508-6:2010[20], *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3*

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

[10] IEC 61784-4[21], *Industrial communication networks – Profiles – Part 4: Secure communications for fieldbuses*

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

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

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

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

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

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

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

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

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

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

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

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

---

19 In preparation.

20 To be published.

21 Proposed new work item under consideration.

[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] EN 954-1:1996[22], *Safety of machinery – Safety related parts of control systems – General principles for design*

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

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

[28] GS-ET-26[23], *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*")

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

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

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

[32] *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.

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

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

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

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

[37] 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

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

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

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

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

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

RÉSEAUX DE COMMUNICATION INDUSTRIELS – PROFILS –

Partie 3: Bus de terrain de sécurité fonctionnelle – Règles générales et définitions de profils

AVANT-PROPOS

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

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

Cette seconde édition annule et remplace la première édition parue en 2007. Cette édition constitue une révision technique. Les principales modifications par rapport à l'édition précédente sont énumérées ci-dessous:

– clarifications et explications complémentaires des exigences, références actualisées;
– actualisations des définitions et exigences par rapport à la nouvelle édition de la CEI 61508;
– ajout d'une nouvelle Annexe D informative fournissant une ligne directrice relative à l'évaluation.
– actualisations des parties pour les CPF 1, CPF 2, CPF 3, CPF 6 (détails fournis dans les parties);

– ajout de nouvelles parties pour les CPF 8, CPF 12, CPF 13, CPF 14;
– dans les parties CPF, ajout d'une annexe afin de fournir des informations concernant les laboratoires d'essais, en vue d'une vérification par des essais et d'une validation de la conformité des produits FSCP.

La présente version bilingue, correspond à la version anglaise monolingue publiée en 2010-07.

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

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

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

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

Une liste de toutes les parties de la série CEI 61784-3, publiée 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.

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

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

IMPORTANT – Le logo "couleur" figurant sur la page de garde de la présente publication indique qu'elle comporte des couleurs considérées comme utiles pour la bonne compréhension de son contenu. Il convient par conséquent que les utilisateurs impriment le présent document avec une imprimante couleur.

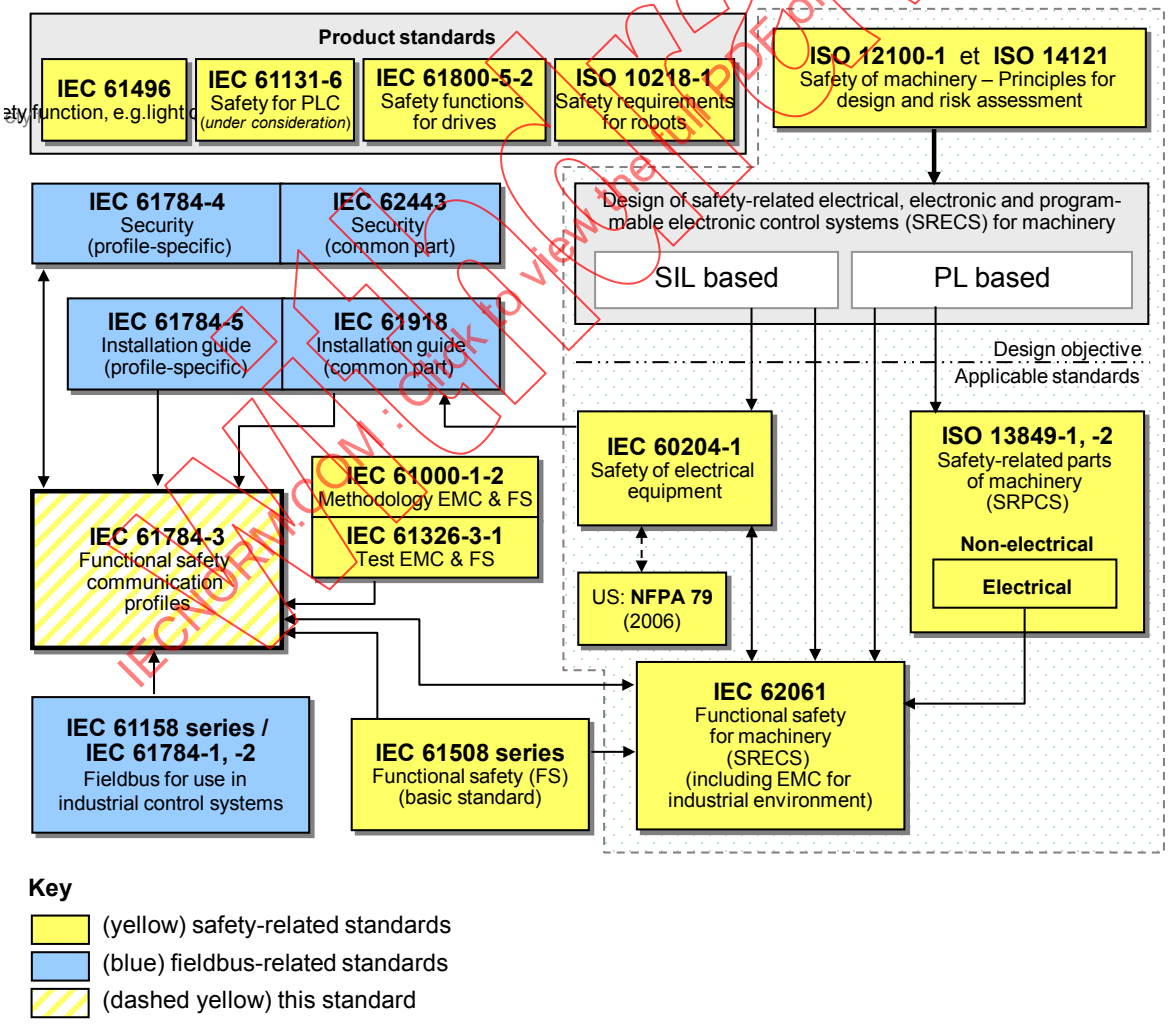
0 Introduction

0.1 Généralités

La 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 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.



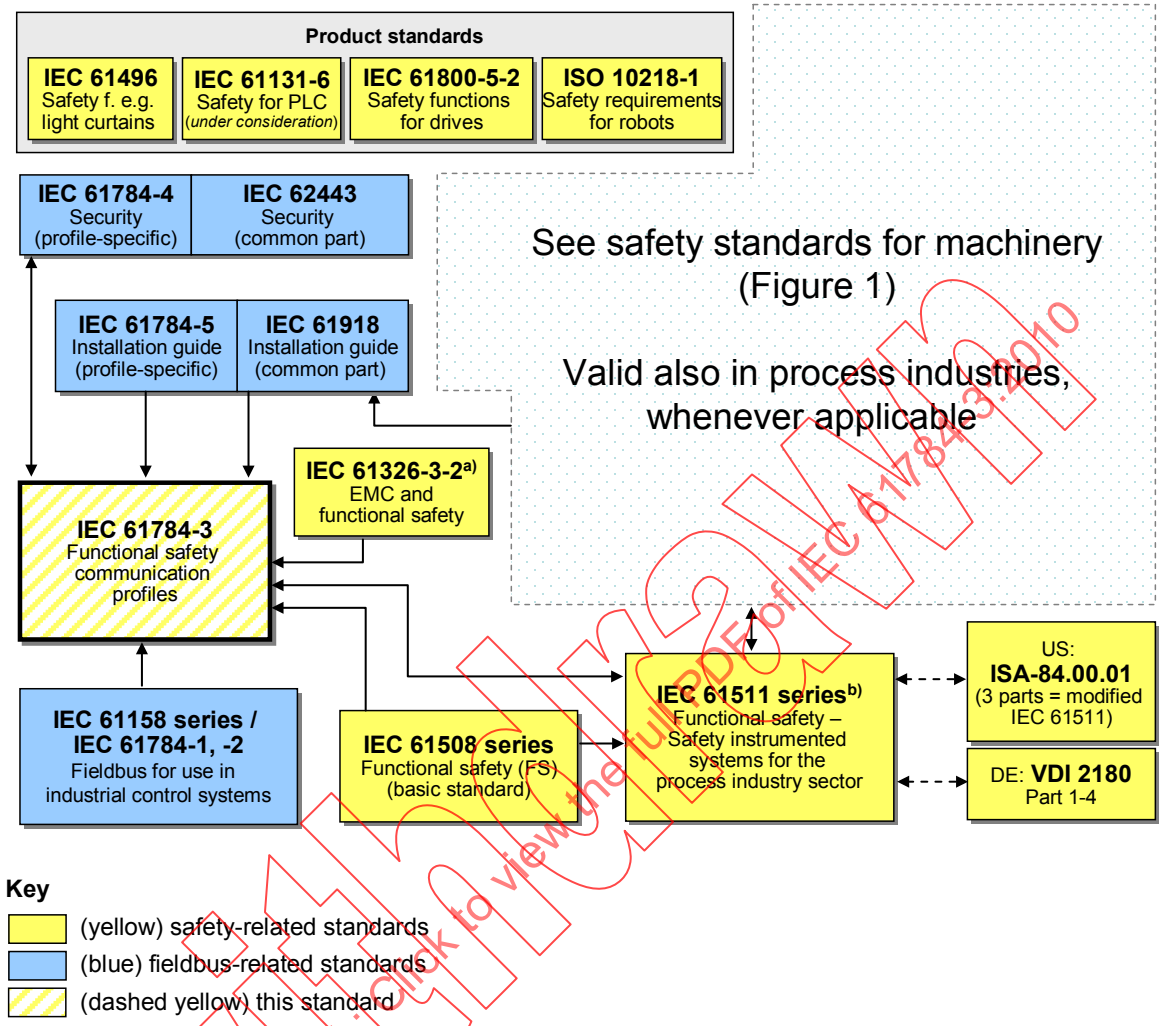
Légende

Anglais	Français
Product standards	Normes de produits
Safety function, e.g. light curtains	Fonction de sécurité, par exemple barrières photo électriques
Safety for PLC (under consideration)	Sécurité relative aux automates programmables (à l'étude)
Safety functions for drives	Fonctions de sécurité applicables aux entraînements
Safety requirements for robots	Exigences de sécurité applicables aux robots
Safety of machinery – principles for design and risk assessment	Sécurité des machines – principes généraux de conception et d'appréciation du risque
Security (profile-specific)	Sûreté (spécifique au profil)
Security (common part)	Sûreté (partie commune)
Design of safety-related electrical, electronic and programmable electronic control systems 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	Electrique
Methodology EMC & functional safety	Méthodologie en matière de compatibilité électromagnétique & sécurité fonctionnelle
Test EMC & functional safety	Essai CEM et sécurité fonctionnelle
Functional safety communication profiles	Profils de communication de sécurité fonctionnelle
IEC 61158 series / IEC 61784-1,-2 Fieldbus for use in industrial control systems	Série CEI 61158 / CEI 61784-1,-2 Bus de terrain pour utilisation dans des systèmes de commande industriels
IEC 61508 series, Functional safety (basic standard)	Série CEI 61508 Sécurité fonctionnelle (norme de base)
Functional safety for machinery (SRECS) including EMC 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

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

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

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



Légende

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

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

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

b EN ratifiée.

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

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

La sécurité des couches de communication spécifiées dans la présente norme garantissent qu'un bus de terrain peut être utilisé dans des applications nécessitant une sécurité fonctionnelle jusqu'au niveau d'intégrité de sécurité (SIL) spécifié par son profil de communication correspondant.

Le niveau d'intégrité de sécurité SIL qui en résulte pour un système dépend de la mise en œuvre du profil de communication de sécurité fonctionnelle retenu au sein du système – la mise en œuvre du profil de communication de sécurité fonctionnelle dans un dispositif normal ne suffit pas pour le qualifier de dispositif de sécurité.

La présente norme décrit:

— les principes de base de la 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 ce qui concerne l'intégrité des données.

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

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

0.2 Déclaration de droits de propriété

La commission électrotechnique internationale (CEI) attire l'attention sur le fait qu'il est déclaré que la conformité avec le présent document peut impliquer l'utilisation de brevets concernant les profils de communication de sécurité fonctionnelle pour les familles 1, 2, 3, 6, 12, 13 et 14 donnés dans la CEI 61784-3-1, CEI 61784-3-2, CEI 61784-3-3, CEI 61784-3-6, CEI 61784-3-12, CEI 61784-3-13 et CEI 61784-3-14.

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 les demandeurs du monde entier, en des termes et à des conditions raisonnables et non discriminatoires. A ce propos, la déclaration des détenteurs de ces droits de propriété est enregistrée à la CEI.

NOTE Les détails relatifs aux brevets et l'information personne-ressource correspondante sont fournis dans les CEI 61784-3-1, CEI 61784-3-2, CEI 61784-3-3, CEI 61784-3-6, CEI 61784-3-12, CEI 61784-3-13 et CEI 61784-3-14.

RÉSEAUX DE COMMUNICATION INDUSTRIELS – PROFILS –

Partie 3: Bus de terrain de sécurité fonctionnelle – Règles générales et définitions de profils

1 Domaine d'application

La présente partie de la série CEI 61784-3 définit des principes communs pouvant être appliqués pour la 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[1] concernant la sécurité fonctionnelle. Ces principes peuvent être utilisés dans diverses applications industrielles, telles que la commande de processus, l'usinage automatique et les machines.

La présente partie[2] et les parties CEI 61784-3-x spécifient plusieurs profils de communication de sécurité fonctionnelle basés sur les profils de communication et les couches du protocole des technologies des bus de terrain de la CEI 61784-1, la CEI 61784-2 et la série CEI 61158.

NOTE1 Il peut exister d'autres systèmes de communication relatifs à la sécurité qui satisfont aux exigences de la série CEI 61508 et ne sont pas inclus dans la présente norme.

NOTE 2 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.

Tous les systèmes sont exposés à un accès non autorisé à un certain moment de leur cycle de vie. Des mesures supplémentaires doivent être prises en compte dans toute application nécessitant un niveau de sécurité afin de protéger les systèmes ayant des bus de terrain contre tout accès non autorisé. La série CEI 62443 traite bon nombre de ces questions; la relation avec la série CEI 62443 est détaillée dans un paragraphe dédié de la présente partie.

NOTE 3 Des exigences supplémentaires spécifiques au profil et concernant la sécurité peuvent également être spécifiées dans la CEI 61784-4[3] [10].

NOTE 4 La mise en œuvre du profil de communication de sécurité fonctionnelle, conforme à la présente partie, dans un dispositif normal ne suffit pas à le qualifier de dispositif de sécurité, tel que défini dans la série CEI 61508.

NOTE 5 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.

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, P*rogrammable controllers – Part 2: Equipment requirements and tests* (disponible uniquement en anglais)

---

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

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

3 Proposition d'un nouveau sujet d'études soumise à examen.

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

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

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

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

CEI 61508-1:2010[4], *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 1: Exigences générales*

CEI 61508-2, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 2: Exigences pour les systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité*

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

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

IEC 61784-3-1, *Industrial communication networks – Profiles – Part 3-1: Functional safety fieldbuses – Additional specifications for CPF 1* (disponible uniquement en anglais)

IEC 61784-3-2, *Industrial communication networks – Profiles – Part 3-2: Functional safety fieldbuses – Additional specifications for CPF 2* (disponible uniquement en anglais)

IEC 61784-3-3, *Industrial communication networks – Profiles – Part 3-3: Functional safety fieldbuses – Additional specifications for CPF 3* (disponible uniquement en anglais)

IEC 61784-3-6, *Industrial communication networks – Profiles – Part 3-6: Functional safety fieldbuses – Additional specifications for CPF 6* (disponible uniquement en anglais)

IEC 61784-3-8[5], *Industrial communication networks – Profiles – Part 3-8: Functional safety fieldbuses – Additional specifications for CPF 8* (disponible uniquement en anglais)

IEC 61784-3-12[5], *Industrial communication networks – Profiles – Part 3-12: Functional safety fieldbuses – Additional specifications for CPF 12* (disponible uniquement en anglais)

IEC 61784-3-13[5], *Industrial communication networks – Profiles – Part 3-13: Functional safety fieldbuses – Additional specifications for CPF 13* (disponible uniquement en anglais)

IEC 61784-3-14[5], *Industrial communication networks – Profiles – Part 3-14: Functional safety fieldbuses – Additional specifications for CPF 14* (disponible uniquement en anglais)

---

4 A publier.

5 A publier.

IEC 61784-5 (all parts), *Industrial communication networks – Profiles – Part 5: Installation of fieldbuses – Installation profiles for CPF x* (disponible uniquement en anglais)

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

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*

IEC 62443 (all parts), *Industrial communication networks – Network and system security* (disponible uniquement en anglais)

3 Termes, définitions, symboles, abréviations et conventions

3.1 Termes et définitions

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

3.1.1 Termes et définitions communs

3.1.1.1
date (horodatage) absolue
date référencée par rapport à un temps global, commun à un groupe de dispositifs utilisant un *bus de terrain*

[CEI 62280-2, modifiée]

3.1.1.2
disponibilité
probabilité, pour un système automatisé, que pendant une période donnée il n'y ait pas de conditions opérationnelles insatisfaisantes, telles que des pertes de production

3.1.1.3
canal noir
canal de communication sans preuve existante de conception ou de validation conformément à la CEI 61508

3.1.1.4
pont
dispositif abstrait qui relie des segments de réseau multiples le long de la couche de liaison de données

3.1.1.5
canal de communication
connexion logique entre deux points limites d'un *système de communication*

3.1.1.6
système de communication
ensemble de matériels, logiciels et médias de propagation permettant la transmission de *messages* d'une application à une autre (ISO/CEI 7498, couche d'application)

3.1.1.7
connexion
liaison logique entre deux objets d'application d'un même dispositif ou de dispositifs différents

3.1.1.8
contrôle de redondance cyclique (CRC[6])
<valeur> donnée redondante déduite et enregistrée ou transmise simultanément par 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 [29], [30]][7].

3.1.1.9
diversité
moyens différents pour réaliser une fonction requise

NOTE La diversité peut être réalisée en utilisant des méthodes physiques ou des approches conceptuelles différentes.

[CEI 61508-4:2010[8]]

3.1.1.10
erreur
écart ou discordance entre une valeur ou une condition calculée, observée ou mesurée, et la valeur ou la condition vraie, prescrite ou théoriquement correcte

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

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

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

3.1.1.11
défaillance
cessation de l'aptitude d'une unité fonctionnelle à accomplir une fonction requise ou fonctionnement d'une unité fonctionnelle d'une toute autre manière que celle requise

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

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

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

3.1.1.12
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 61508-4:2010, modifiée], [ISO/CEI 2382-14.01.10, modifiée]

---

6 CRC = *Cyclic Redundancy Check*

7 Les chiffres entre crochets font référence à la bibliographie.

8 A publier.

3.1.1.13
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

3.1.1.14
système de bus de terrain
système utilisant un *bus de terrain* avec des dispositifs reliés

3.1.1.15
trame
synonyme discrédité de DLPDU

3.1.1.16
séquence de contrôle de trame (FCS[9])
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 [29], [30].

3.1.1.17
fonction de hachage
fonction (mathématique) de mise en correspondance des valeurs d'un ensemble (éventuellement) très grand de valeurs en une plage de valeurs (habituellement) plus petite

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

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

[CEI/TR 62210, modifiée]

3.1.1.18
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

3.1.1.19
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

3.1.1.20
message
série ordonnée d'octets destinée à communiquer des informations

[ISO/CEI 2382-16.02.01, modifiée]

3.1.1.21
récepteur de messages
partie d'un *système de communication* destiné à recevoir des *messages*

[ISO/CEI 2382-16.02.03]

9 FCS = *Frame Check Sequence*

3.1.1.22
source de messages
partie d'un *système de communication* destiné à envoyer des *messages*

[ISO/CEI 2382-16.02.02]

3.1.1.23
déclenchement de nuisance
déclenchement parasite sans effet préjudiciable

NOTE Les erreurs anormales internes peuvent être générées dans des systèmes de communication tels que des systèmes de transmission par ondes radioélectriques, par exemple, du fait d'un trop grand nombre de nouvelles tentatives en présence de perturbations.

3.1.1.24
niveau de performance (PL[10])
niveau discret utilisé pour spécifier la capacité des parties relatives à la sécurité des systèmes de commande à accomplir une fonction de sécurité dans des conditions prévisibles

[ISO 13849-1]

3.1.1.25
très basse tension de protection (TBTP)
circuit électrique dans lequel la tension ne peut pas dépasser 30 V eff. en c.a., 42,4 V crête ou 60 V en c.c. dans des conditions normales de simple défaut, à l'exception des défauts de terre dans d'autres circuits

NOTE Un circuit TBTP est similaire à un circuit TBTS relié à la terre de protection.

[CEI 61131-2]

3.1.1.26
redondance
existence de moyens supplémentaires à ceux qui se révèleraient suffisants pour qu'une unité fonctionnelle accomplisse une fonction requise ou que des données représentent une information

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

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

3.1.1.27
date (horodatage) relative
date référencée par rapport à l'horloge locale d'une entité

NOTE En général, il n'y a pas de relation avec les horloges des autres entités.

[CEI 62280-2, modifiée]

3.1.1.28
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.

[10] PL = Performance Level

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]

3.1.1.29
risque
combinaison de la probabilité d'occurrence d'un dommage ou d'un préjudice et de la gravité de ce dernier

NOTE Pour plus d'informations sur ce concept, se reporter à l'Annexe A de la CEI 61508-5:2010[11].

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

3.1.1.30
couche de communication de sécurité (SCL[12])
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

3.1.1.31
connexion de sécurité
connexion qui utilise le protocole de sécurité pour des transactions de communications

3.1.1.32
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.

3.1.1.33
dispositif de sécurité
dispositif conçu conformément à la CEI 61508 et qui met en œuvre le profil de communication de sécurité fonctionnelle

3.1.1.34
très basse tension de sécurité (TBTS)
circuit électrique dans lequel la tension ne peut pas dépasser 30 V eff. en c.a., 42,4 V crête ou 60 V en c.c. dans des conditions normales de défaut simple, y compris les défauts à la terre dans les autres circuits

NOTE Un circuit TBTS n'est pas relié à la terre de protection.

[CEI 61131-2]

3.1.1.35
fonction de sécurité
fonction qu'un système E/E/PE relatif à la sécurité ou d'autres mesures de réduction du risque doivent 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 spécifique dangereux

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

[CEI 61508-4:2210, modifiée]

---

11 A publier.

12 SCL = *Safety Communication Layer*

3.1.1.36
temps de réponse de la fonction de sécurité
dans le cas le plus défavorable temps écoulé 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 sur le canal de la fonction de sécurité

NOTE Ce concept est introduit en 5.2.4, et traité par les profils de communication de sécurité fonctionnelle définis dans la présente partie.

3.1.1.37
niveau d'intégrité de sécurité (SIL[13])
niveau discret (un sur quatre niveaux possibles), correspondant à une plage de valeurs d'intégrité de sécurité, où le niveau d'intégrité de sécurité 4 est le niveau le plus élevé et le niveau d'intégrité de sécurité 1 est le niveau le plus faible

NOTE 1 Les mesures de défaillance cible (voir la CEI 61508-4:2010, 3.5.17) applicables aux quatre niveaux d'intégrité de sécurité sont spécifiées dans les Tableaux 2 et 3 de la CEI 61508-1:2010[14].

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

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

[CEI 61508-4:2010]

3.1.1.38
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 en 5.3 et 5.4.

3.1.1.39
application relative à la sécurité
programmes conçus conformément à la CEI 61508 pour satisfaire aux exigences SIL de l'application

3.1.1.40
système relatif à la sécurité
système qui exécute les *fonctions de sécurité* conformément à la CEI 61508

3.1.1.41
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

3.1.1.42
déclenchement parasite
déclenchement provoqué par le système de sécurité sans injonction du processus

---

13 SIL = *Safety Integrity Level*

14 A publier.

3.1.1.43
datation (horodatage)
information temporelle incluse dans un *message*

3.1.1.44
canal blanc
canal de communication dans lequel tous les composants matériels et toutes les composantes logicielles sont conçus, mis en œuvre et validés conformément à la CEI 61508

3.1.2 CPF 1: Termes et définitions supplémentaires

Aucun requis pour la présente partie.

3.1.3 CPF 2: Termes et définitions supplémentaires

Aucun requis pour la présente partie.

3.1.4 CPF 3: Termes et définitions supplémentaires

Aucun requis pour la présente partie.

3.1.5 CPF 6: Termes et définitions supplémentaires

Aucun requis pour la présente partie.

3.1.6 CPF 8: Termes et définitions supplémentaires

Aucun requis pour la présente partie.

3.1.7 CPF 12: Termes et définitions supplémentaires

Aucun requis pour la présente partie.

3.1.8 CPF 13: Termes et définitions supplémentaires

Aucun requis pour la présente partie.

3.1.9 CPF 14: Termes et définitions supplémentaires

Aucun requis pour la présente partie.

3.2 Symboles et abréviations

3.2.1 Symboles et abréviations communs

CP	Profil de communication (*Communication Profile*)	[CEI 61784-1]
CPF	Famille de profils de communication (*Communication Profile Family)*	[CEI 61784-1]
CRC	Contrôle de redondance cyclique (*Cyclic Redundancy Check)*	
DLL	Couche de liaison de données (	[ISO/CEI 7498-1]
DLPDU	Ensemble (unité) de données de protocole de liaison de données (*Data Link Protocol Data Unit)*	
CEM	Compatibilité électromagnétique	
EMI	Perturbation électromagnétique (	
EUC	Equipement commandé (*Equipment Under Control)*	[CEI 61508-4:2010]
E/E/PE	Electrique/électronique/électronique programmable (	[CEI 61508-4:2010]
FAL	Couche Application du bus de terrain (*Fieldbus Application Layer*)	[CEI 61158-5]
FCS	Séquence de contrôle de trame (*Frame Check Sequence)*	

FS	Sécurité fonctionnelle (*Functional Safety)*	
FSCP	Profil de communication de sécurité fonctionnelle (*Functional Safety Communication Profile)*	
MTBF	Moyenne des temps de bon fonctionnement entre défaillances (*Mean Time Between Failures*)	
MTTF	Durée moyenne de fonctionnement avant défaillance (*Mean Time To Failure*)	
NSR	Non relatif à la sécurité (*Non Safety Relevant*)	
PDU	Ensemble (Unité) de données de protocole (*Protocol Data Unit*)	[ISO/CEI 7498-1]
TBTP	Très basse tension de protection	
PES	Système électronique programmable (*Programmable Electronic System*)	[CEI 61508-4:2010]
PFD	Probabilité de défaillance dangereuse sur sollicitation (*Probability of dangerous Failure on Demand*)	[CEI 61508-6:2010 [15]]
PFH	Fréquence moyenne de défaillance dangereuse [h^{-1}] par heure	[CEI 61508-6:2010]
PhL	Couche physique (*Physical Layer*)	[ISO/CEI 7498-1]
PL	Niveau de performance (*Performance Level*)	[ISO 13849-1]
PLC	Automate programmable (*Programmable Logic Controller*)	
SCL	Couche de communication de sécurité (*Safety Communication Layer*)	
TBTS	Très basse tension de sécurité	
SIL	Niveau d'intégrité de sécurité (*Safety Integrity Level*)	[CEI 61508-4:2010]
SR	Relatif à la sécurité (*Safety Relevant*)	

3.2.2 CPF 1: Symboles et abréviations supplémentaires

SIS	Systèmes instrumentés de sécurité (*Safety Instrumented Systems*)

3.2.3 CPF 2: Symboles et abréviations supplémentaires

CIP™	Protocole industriel commun (*Common Industrial Protocol*) (cadre d'application partagé parmi les profils de communication CPF-2)

3.2.4 CPF 3: Symboles et abréviations supplémentaires

DP	Périphériques décentralisés (*Decentralized Peripherals*)

3.2.5 CPF 6: Symboles et abréviations supplémentaires

Aucun requis pour la présente partie.

3.2.6 CPF 8: Symboles et abréviations supplémentaires

ASE	Elément de service d'application (*Application Service Element*)
SASE	Elément de service d'application de sécurité (*Safety Application Service Element*)

3.2.7 CPF 12: Symboles et abréviations supplémentaires

FSoE	A sécurité intégrée sur le CPF 12 (*Failsafe over CPF 12*)

3.2.8 CPF 13: Symboles et abréviations supplémentaires

Aucun requis pour la présente partie.

3.2.9 CPF 14: Symboles et abréviations supplémentaires

IP	Protocole Internet (*Internet Protocol*)
UDP	Protocole de datagrammes utilisateur (*User Datagram Protocol*)

15 A publier.

4 Conformité

Chaque profil de communication de sécurité fonctionnelle défini dans la présente norme est basé sur les profils de communication de la CEI 61784-1 ou CEI 61784-2 et les couches de protocole de la série CEI 61158.

Une déclaration de conformité à un protocole de communication de sécurité fonctionnelle (FSCP) défini dans la présente norme doit être présentée comme

une conformité au FSCP n/m <Type> défini dans la CEI 61784-3:20xx

ou

une conformité au FSCP n/m <Type> défini dans la CEI 61784-3 (Ed. 2.0)

où le Type placé entre parenthèses en chevron < > est facultatif, lesdites parenthèses devant être exclues.

En variante, une déclaration de conformité peut être présentée comme

une conformité à la CEI 61784-3-N:20xx

ou

une conformité à la CEI 61784-3-N (Ed.2.0)

où N est le numéro de famille attribué au CPF correspondant.

La conformité à une partie CEI 61784-3-N implique que toutes les exigences obligatoires du (des) FSCP correspondant(s) applicables au dispositif, au système ou à l'application particuliers doivent être satisfaites.

Les normes de produits ne doivent comporter aucun aspect relatif à l'évaluation de conformité (y compris les dispositions MQ), à titre normatif ou informatif, autre que les dispositions applicables aux essais des produits (évaluation et examen).

5 Principes des systèmes de bus de terrain relatifs à la sécurité

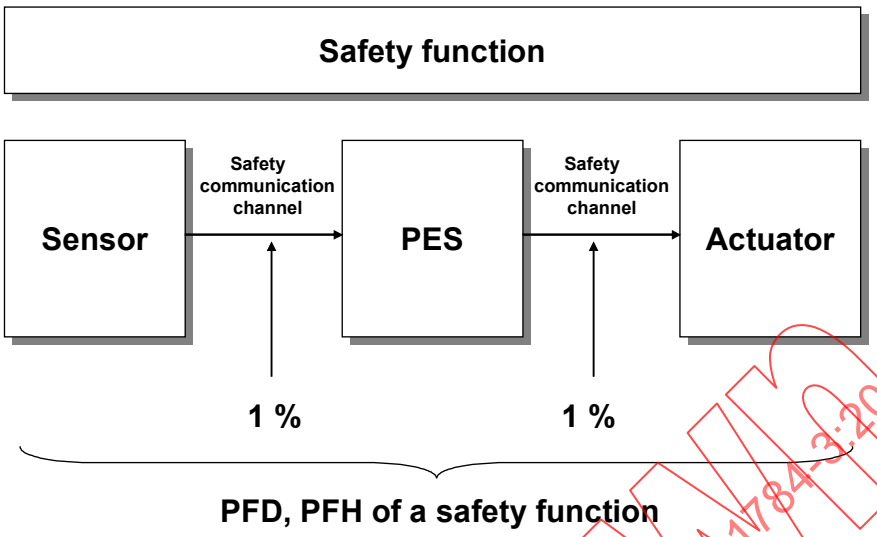
5.1 Décomposition des fonctions de sécurité

Conformément à la CEI 61508, une analyse des risques permettra de définir les fonctions de sécurité. Ces fonctions de sécurité peuvent être décomposées en parties contribuant à la fonction de sécurité globale (par exemple, capteur(s) – Canal de communication de sécurité – PES(s) - Canal de communication de sécurité – Actionneur(s)).

Le système de communication proprement dit, défini dans la présente norme, transmet les données de sécurité. Il est vivement recommandé que le canal de communication de sécurité ne consomme pas plus de 1% de la PFD ou de la PFH maximale du SIL concerné pour lequel le profil de communication de sécurité fonctionnelle est conçu (voir Figure 3).

EXEMPLE

A la Figure 3, la PFH de la fonction de sécurité est $PFH_{capteur}$ + PFH_{PES} + $PFH_{actionneur}$ + 2 x $PFH_{canal\ de\ communication\ de\ sécurité}$.



Légende

Anglais	Français
Safety function	Fonction de sécurité
Sensor	Capteur
Safety communication channel	Canal de communication de sécurité
PES	PES
Actuator	Actionneur
PFD, PFH of a safety function	PFD, PFH d'une fonction de sécurité

Figure 3 – Communication de sécurité comme partie intégrante d'une fonction de sécurité

5.2 Système de communication

5.2.1 Généralités

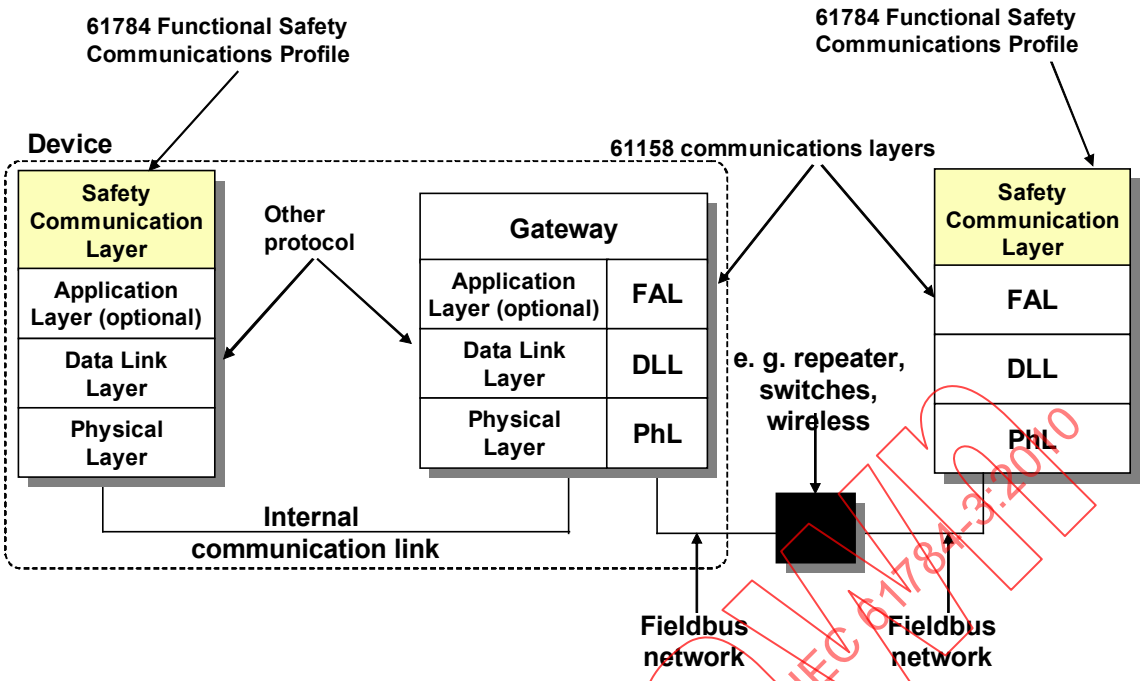
Les informations suivantes permettent une compréhension commune de la technologie et des termes employés.

NOTE Ces informations sont issues, en grande partie, des Principes d'essai et de certification des systèmes de bus pour la communication de sécurité (Principles for Test and Certification of Bus Systems for Safety Relevant Communication) de l'Institut allemand de la sécurité et de la santé au travail [28].

5.2.2 Bus de terrain définis dans la CEI 61158

Tandis que la CEI 61508 ne limite pas l'utilisation des technologies de communication, la présente norme cible l'utilisation des systèmes de communication de sécurité fonctionnelle basés sur les bus de terrain. La Figure 4 illustre un exemple de modèle d'utilisation des systèmes de communication avec un bus de terrain, fondée sur la méthode du canal noir.

Lors de l'utilisation des structures de bus de terrain basées sur la CEI 61158 sans modifier la définition de chaque couche de communication, toutes les mesures nécessaires à la transmission effective des données de sécurité conformément aux exigences de la CEI 61508 doivent être effectuées par une « couche de communication de sécurité » supplémentaire, positionnée tel qu'illustré à la Figure 4.



Légende

Anglais	Français
61784 Functional Safety Communication Profile	61784 Profil de Communication de Sécurité Fonctionnelle
Device	Dispositif
Communication layers	Couches de communication
Safety Communication Layer	Couche de Communication de Sécurité
Application Layer (optional)	Couche d'Application (facultatif)
Data Link Layer	Couche de Liaison de Données
Physical Layer	Couche Physique
Gateway	Passerelle
e.g. repeater, switches, wireless	par exemple, répéteur, commutateurs, sans fil
Internal communication link	Liaison de communication interne
Fieldbus network	Réseau de bus de terrain
Other protocol	Autre protocole

NOTE 1 La mise en œuvre de la couche d'application de bus de terrain (FAL) est requise, tandis que la couche d'application (AL) peut être omise pour les liaisons de communication internes à un dispositif.

NOTE 2 Les fonctions de la couche utilisateur non relatives à la sécurité peuvent contourner la SCL et accéder directement à la FAL.

Figure 4 – Exemple de modèle d'un système de communication de sécurité fonctionnelle

5.2.3 Types de canaux de communication

La CEI 61508 utilise un concept appelé « canal noir » ou « canal blanc » pour définir les exigences du bus de terrain de base en vue de la transmission des données de sécurité. Le point d'application des mesures de sécurité de base par rapport au bus de terrain permet de déterminer si un canal de communication est blanc ou noir. La présente norme spécifie les profils de communication de sécurité fonctionnelle qui appliquent la méthode du canal noir.

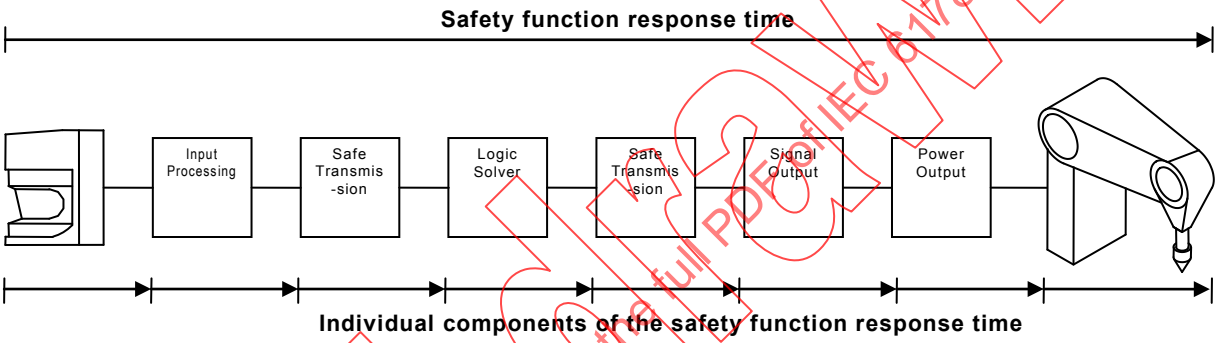
Dans ce contexte, un canal de communication de sécurité est défini comme partant du sommet de la couche de communication de sécurité de la source pour se terminer au sommet de la couche de communication de sécurité du récepteur (voir Figure 4).

5.2.4 Temps de réponse de la fonction de sécurité

Il s'agit du temps écoulé dans le cas le plus défavorable suite à l'activation d'un capteur de sécurité (par exemple, interrupteur, transmetteur de pression, rideau de lumière) relié à un bus de terrain, avant que ne soit atteint l'état de sécurité correspondant de son (ses) actionneur(s) de sécurité (par exemple relais, soupape, entraînement), du fait d'erreurs ou de défaillances avérées sur le canal de la fonction de sécurité

Un franchissement de seuil par des signaux analogiques ou un changement d'état de signaux numériques est à l'origine de la sollicitation (activation) d'une fonction de sécurité.

La Figure 5 illustre un exemple des composantes typiques constituant un temps de réponse de la fonction de sécurité.



Légende

Anglais	Français
Safety function response time	Temps de réponse de la fonction de sécurité
Input processing	Traitement des entrées
Safe transmission	Transmission de sécurité
Logic solver	Résolveur logique
Signal output	Sortie de signal
Power output	Puissance de sortie
Individual components of the safety function response time	Composantes individuelles du temps de réponse de la fonction de sécurité

Figure 5 – Exemple des composantes du temps de réponse de la fonction de sécurité

Les profils de communication de sécurité fonctionnelle individuels peuvent avoir un ensemble de composantes différentes, mais le temps de réponse de la fonction de sécurité doit tenir compte de toutes les composantes pertinentes.

5.3 Erreurs de communication

5.3.1 Généralités

Les paragraphes suivants spécifient les erreurs de communication potentielles. Des notes supplémentaires sont fournies pour indiquer le comportement typique d'un canal noir.

5.3.2 Corruption

Les messages peuvent être corrompus par des erreurs internes à un élément du bus de terrain, des erreurs sur le support de transmission ou des perturbations de communication.

NOTE 1 L'erreur de message en cours de transfert est un événement normal pour tout système de communication standard. Des événements de ce type sont détectés au niveau des récepteurs avec une probabilité élevée, grâce à une fonction de hachage, et le message est alors ignoré.

NOTE 2 La plupart des systèmes de communication comportent des protocoles de correction des erreurs de message. Il convient ainsi de ne pas classer ces messages comme une « perte » jusqu'à l'échec avéré des procédures de correction ou de répétition, ou tant que les dites procédures ne sont pas utilisées.

NOTE 3 Un message est classé comme « Retard inacceptable » si les procédures de correction ou de répétition durent plus longtemps qu'un délai spécifié.

NOTE 4 Dans le cas très peu probable où des erreurs multiples produisent un nouveau message de structure correcte (par exemple, adressage, longueur, fonction de hachage telle que CRC, etc.), le message est accepté et traité. Les évaluations basées sur un numéro de séquence de message ou un horodatage peuvent permettre une classification des défauts comme une répétition non prévue, une séquence incorrecte, un retard inacceptable, une insertion.

5.3.3 Répétition non prévue

Des messages anciens et non actualisés sont répétés à un moment inapproprié en raison d'une erreur, d'une panne ou d'une perturbation.

NOTE 1 La répétition par l'émetteur constitue une procédure normale lorsqu'une station cible ne transmet pas un acquittement/une réponse attendu(e), ou lorsqu'une station réceptrice détecte l'absence d'un message et demande sa retransmission.

Dans certains cas, il est possible de détecter l'absence de réponse et de répéter le message avec un retard minimal et aucune perte de séquence. Dans d'autres cas, la répétition se produit ultérieurement et hors séquence avec d'autres messages.

NOTE 2 Certains bus de terrain se servent de la redondance pour envoyer le même message plusieurs fois, ou par l'intermédiaire de plusieurs voies alternatives pour accroître la probabilité d'une bonne réception.

5.3.4 Séquence incorrecte

La séquence prédéfinie (par exemple, nombres naturels, références temporelles) associée aux messages d'une source particulière est incorrecte en raison d'une erreur, d'une panne ou d'une perturbation.

NOTE 1 Les systèmes de bus de terrain peuvent contenir des éléments de stockage des messages (par exemple, FIFO au niveau des commutateurs, ponts, routeurs) ou peuvent appliquer des protocoles susceptibles d'affecter la séquence (par exemple, en favorisant les messages à priorité élevée par rapport aux messages à priorité moins élevée).

NOTE 2 Lorsque des séquences multiples sont actives, telles que des messages en provenance de différentes entités sources ou des rapports relatifs à des types d'objet différents, ces séquences sont contrôlées séparément et des erreurs peuvent être signalées pour chaque séquence.

5.3.5 Perte

Un message n'est pas reçu ou reconnu en raison d'une erreur, d'une panne ou d'une perturbation.

5.3.6 Retard inacceptable

Les messages peuvent être retardés au-delà de leur fenêtre temporelle d'arrivée admise, par exemple, en raison d'erreurs sur le support de transmission, de lignes de transmission encombrées, de perturbations, ou de l'envoi de messages par des éléments du bus de terrain de telle manière que les services soient retardés ou refusés (par exemple, FIFO au niveau des commutateurs, passerelles, routeurs).

NOTE Dans les bus de terrain sous-jacents qui utilisent des analyses programmées ou cycliques, les erreurs de message peuvent être corrigées comme suit:

a) répétition immédiate;

b) répétition utilisant le temps disponible à la fin du cycle;

c) traitement du message comme message perdu et attente du cycle suivant pour recevoir la valeur suivante.

Dans le cas a), tous les messages suivants dans le cycle concerné sont légèrement retardés, tandis que dans le cas b), seul le message retransmis connaît un retard.

Les cas a) et b) ne sont normalement pas classés comme « retard inacceptable ».

Le cas c) serait classé comme « retard inacceptable », à moins que l'intervalle de répétition de cycles ne soit suffisamment court pour assurer que les retards entre les cycles ne sont pas importants et que la valeur cyclique suivante peut être acceptée comme valeur de substitution de la valeur précédente manquante.

5.3.7 Insertion

Un message est inséré qui se rapporte à une entité source imprévue ou inconnue, en raison d'une panne ou d'une perturbation.

NOTE Ces messages s'ajoutent au flux de messages prévu, et ne peuvent être classés comme « corrects », « répétition non prévue », ou « séquence incorrecte » dans la mesure où ils ne comportent pas de source prévue.

5.3.8 Mascarade

Une panne ou une perturbation provoque l'insertion d'un message associé à une entité source apparemment valide; un message non relatif à la sécurité peut alors être reçu par un participant relatif à la sécurité, qui le traite alors comme un message relatif à la sécurité.

NOTE Les systèmes de communication utilisés pour les applications relatives à la sécurité peuvent recourir à des contrôles supplémentaires pour détecter la mascarade, tels que les identités de source autorisées, les expressions d'adaptation ou la cryptographie.

5.3.9 Adressage

En raison d'une panne ou d'une perturbation, un message relatif à la sécurité est envoyé au participant relatif à la sécurité inapproprié, qui traite alors le message reçu comme message correct.

5.4 Mesures correctives déterministes

5.4.1 Généralités

Le présent paragraphe énumère les mesures couramment appliquées pour détecter les erreurs déterministes et les défaillances d'un système de communication, par opposition aux erreurs stochastiques telles que la corruption de messages provoquée par des perturbations électromagnétiques.

5.4.2 Numéro de séquence

Un numéro de séquence est intégré dans les messages échangés entre la source et le récepteur du message. Il peut prendre la forme d'un champ de données supplémentaire dont le numéro varie d'un message à l'autre de manière prédéterminée.

5.4.3 Datation (horodatage)

Dans la plupart des cas, le contenu d'un message est valide uniquement à un moment particulier. La datation peut être une heure donnée ou une heure et une date données, incluse dans un message par l'émetteur.

NOTE 1 Des datations relatives et des datations absolues peuvent être utilisées.

NOTE 2 La datation exige de manière implicite la synchronisation de la base de temps. Il est nécessaire de contrôler la synchronisation pour des applications de sécurité.

5.4.4 Délai

Lors de la transmission d'un message, le récepteur du message vérifie si le temps écoulé entre deux messages reçus de manière consécutive dépasse une valeur prédéterminée. Dans ce cas, l'existence d'une erreur doit être envisagée.

EXEMPLE

Méthode d'accès à intervalles de temps (Time-slot-oriented):

L'échange de messages s'effectue dans le cadre de cycles fixes et d'intervalles de temps prédéterminés pour chaque participant.

Facultatif: Chaque participant doit transmettre ses données dans l'intervalle de temps qui lui est propre, même en sans variation de valeur (il s'agit d'un exemple de communication cyclique).

Une identification de la source complète le dispositif afin d'identifier un participant qui n'a pas transmis ses données dans l'intervalle de temps qui lui est associé.

5.4.5 Authentification de connexion

Les messages peuvent comporter un identificateur de source et/ou destination unique qui décrit l'adresse logique du participant relatif à la sécurité.

5.4.6 Message de réaction

Le destinataire du message renvoie un message de réaction à la source pour confirmer la réception du message d'origine. Ce message de réaction doit être traité par les couches de communication de sécurité.

NOTE 1 Certaines spécifications de bus de terrain utilisent le terme « écho » ou « réception » comme synonyme.

NOTE 2 Ce message de réaction renvoyé peut contenir, par exemple, uniquement un acquittement court, ou peut également contenir les données d'origine, ou toute autre information qui permet à la source de vérifier la bonne réception.

5.4.7 Assurance d'intégrité des données

Le processus d'application relatif à la sécurité ne doit pas se fier aux méthodes d'assurance d'intégrité des données si elles ne sont pas conçues en tenant compte de la sécurité fonctionnelle. Par conséquent, des données redondantes sont incluses dans un message afin de détecter les corruptions de données lors des contrôles de redondance .

NOTE Les systèmes de communication utilisés pour les applications relatives à la sécurité peuvent utiliser des méthodes telles que la cryptographie pour assurer l'intégrité des données, comme variante aux méthodes typiques telles que les CRC.

5.4.8 Redondance avec contre-vérification

Dans les applications de bus de terrain relatives à la sécurité, les données de sécurité peuvent être transmises à deux reprises, dans un ou deux messages séparés, en appliquant des mesures d'intégrité identiques ou différentes indépendantes du bus de terrain sous-jacent.

NOTE Les modèles de communication de sécurité fonctionnelle redondante supplémentaires sont décrits à l'Annexe A.

Par ailleurs, les données de sécurité transmises font l'objet d'une contre-vérification pour déterminer leur validité sur le bus de terrain ou sur une unité source/récepteur connectée séparément. La détection d'une différence signifie qu'une erreur a eu lieu au cours de la transmission, dans l'unité de traitement de la source ou du récepteur.

Lorsque des supports redondants sont utilisés, il convient d'envisager l'application d'une protection de mode commun avec utilisation de mesures appropriées (par exemple, diversité, transmission à décalage temporel.

5.4.9 Différents systèmes d'assurance d'intégrité des données

Si les données relatives à la sécurité (SR) et les données non relatives à la sécurité (NSR) sont transmises via le même bus, différents systèmes d'assurance d'intégrité des données ou différents principes de codage peuvent être utilisés (différentes fonctions de hachage, par exemple, différents polynômes et algorithmes générateurs de CRC), pour s'assurer que les messages NSR ne peuvent influencer aucune fonction de sécurité dans un récepteur SR.

NOTE La présence d'un système d'assurance d'intégrité des données supplémentaire pour les messages SR, et l'absence de ce même système pour les messages NSR est acceptable.

5.5 Relations entre les erreurs et les mesures de sécurité

Les mesures de sécurité spécifiées en 5.4 peuvent être associées à l'ensemble des erreurs possibles défini en 5.3. Cette relation est illustrée dans le Tableau 1. 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 1.

La protection réelle d'une mesure contre les erreurs dépend de la mise en œuvre spécifique de cette dernière.

NOTE Une mesure de sécurité ne peut être mentionnée dans le Tableau correspondant pour une FSCP donnée que si cette mesure est effective préalablement au temps de réponse de sécurité garanti du bus de terrain.

Tableau 1 – Présentation générale de l'efficacité des diverses mesures sur les erreurs possibles

Erreurs de communication	Mesures de sécurité							
	Numéro de séquence (voir 5.4.2)	Horodatage (voir 5.4.3)	Délai (voir 5.4.4)	Authentification de connexion (voir 5.4.5)	Message de réaction (voir 5.4.6)	Assurance d'intégrité des données (voir 5.4.7)	Redondance avec contre-vérification (voir 5.4.8)	Différents systèmes d'assurance d'intégrité des données (voir 5.4.9)
Corruption (voir 5.3.2)					X [d]	X	Uniquement pour un bus série [c]	
Répétition non prévue (voir 5.3.3)	X	X					X	
Séquence incorrecte (voir 5.3.4)	X	X					X	
Perte (voir 5.3.5)	X				X		X	
Retard inacceptable (voir 5.3.6)		X	X [b]					
Insertion (voir 5.3.7)	X			X [a]	X		X	
Déguisement (voir 5.3.8)				X	X			X
Adressage (voir 5.3.9)				X				

NOTE Tableau adapté de la CEI 62280-2 [15] et [28]].

a Uniquement pour l'identification de l'émetteur. Détecte uniquement l'insertion d'une source invalide.

b Requis dans tous les cas.

c Cette mesure est comparable uniquement avec un mécanisme d'assurance des données de grande qualité s'il est possible de démontrer par calcul que le taux d'erreurs résiduelles Λ atteint les valeurs requises en 5.4.9 lorsque deux messages sont transmis par des émetteurs-récepteurs indépendants.

d Efficace uniquement si le message de réaction comporte les données d'origine ou des informations concernant ces dernières.

5.6 Considérations concernant l'intégrité des données

5.6.1 Calcul du taux d'erreurs résiduelles

Les données de sécurité peuvent toujours être corrompues même lorsque les messages arrivent de manière correcte (déterministe). Ainsi, l'assurance d'intégrité des données est une composante fondamentale de la couche de communication de sécurité permettant d'atteindre un niveau d'intégrité de sécurité requis. Des fonctions de hachage appropriées telles que des bits de parité, un contrôle de redondance cyclique (CRC), la répétition des messages et des formes similaires de redondance de message doivent être appliquées.

Le canal de communication ne doit pas utiliser la même fonction de hachage que celle de la couche de communication de sécurité superposée (voir également CEI 62280-1), à moins que ces cas ne fassent l'objet d'une attention toute particulière. Le code de sécurité doit être fonctionnellement indépendant du code de transmission.

NOTE 1 Lorsque le CRC est utilisé comme fonction de hachage, le canal de communication ne doit pas utiliser le même polynôme CRC comme couche de communication de sécurité superposée.

Toutes ces méthodologies permettent d'obtenir des taux d'erreurs résiduelles faibles. Toutes les mesures d'assurance d'intégrité des données doivent être appliquées sur les parties superposées (couche de communication de sécurité) des commandes conçues selon la revendication SIL requise.

Un fournisseur peut choisir différentes méthodes de calcul lui permettant d'obtenir des estimations des mécanismes d'intégrité des données des réseaux de bus de terrain. Les résultats de ces calculs peuvent aboutir à une conception renforcée des matériels et logiciels afin d'assurer l'intégrité ou à un calcul et à une démonstration renforcés de la fiabilité du système de commande global.

Le calcul du taux d'erreurs résiduelles s'effectue sur la base de la probabilité d'erreur résiduelle du mécanisme d'assurance d'intégrité des données (de sécurité) superposées et de la vitesse de transmission des messages de sécurité. De plus, il doit être tenu compte de l'évaluation du nombre maximum de récepteurs d'informations (m) admis dans une fonction de sécurité simple.

L'équation (1) ci-dessous doit servir au calcul du taux d'erreurs résiduelles résultant de RSL (Pe), à moins que le modèle sous-jacent ne s'applique pas ou dans le cas où une autre méthode peut se révéler plus appropriée. Les éléments de l'équation sont spécifiés dans le Tableau 2.

$$\Lambda_{SL}(Pe) = R_{SL}(Pe) \times v \times m \qquad (1)$$

NOTE 2 Cette équation pose l'hypothèse d'une transmission cyclique des messages de sécurité.

Tableau 2 – Définition des éléments utilisés pour le calcul du taux d'erreurs résiduelles

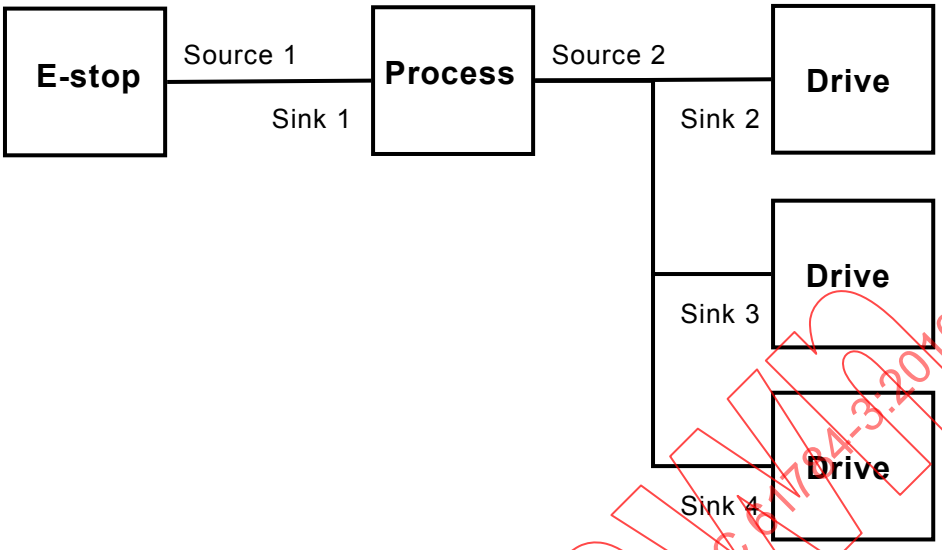
Eléments de l'équation	Définition
Λ_{SL} (Pe)	Taux d'erreurs résiduelles par heure de la couche de communication de sécurité eu égard à la probabilité d'erreurs bit
Pe	Probabilité d'erreurs bit. Une valeur de 10^{-2} doit être utilisée à moins qu'une meilleure probabilité d'erreur puisse être démontrée [a]
R_{SL} (Pe)	Probabilité d'erreur résiduelle d'un message de sécurité
v	Nombre maximum de messages de sécurité par heure
m	Nombre maximum de collecteurs d'informations admis dans une fonction de sécurité simple (voir Figure 6)

[a] Une probabilité d'erreur bit (Pe) de 10^{-4} en présence de perturbations électromagnétiques continues entraînerait une interruption de communication (déclenchement de nuisance) dans le cas d'un échange de données cyclique (par exemple, expiration du temps de fonctionnement du chien de garde après un nombre trop élevé de tentatives). Il est normalement possible de limiter ces déclenchements de nuisance par une installation correcte (par exemple, blindage, liaison équipotentielle).

Ce type d'hypothèse ne peut reposer sur la conception d'une couche de sécurité, dans la mesure où l'existence de brouillages par rafales simples comportant de nombreux bits perturbés est chose courante dans les environnements industriels

Pour pouvoir détecter ce type de perturbations, les mécanismes de détection d'erreurs doivent être suffisamment puissants pour obtenir la probabilité d'erreur résiduelle RSL (Pe) requise à un niveau de probabilité Pe 100 fois plus élevé, c'est-à-dire 10^{-2}.

La Figure 6 illustre un exemple d'application où m = 4.



Légende

Anglais	Français
E-stop	E-interruption
Source	Source
Sink	Récepteur
Process	Processus
Drive	Variateur

Figure 6 – Exemple d'application

5.6.2 Taux d'erreurs résiduelles et SIL

Un système de communication de sécurité fonctionnelle doit fournir un taux d'erreurs résiduelles tel que spécifié dans le Tableau 3.

Les deux systèmes avec un mode de sollicitation faible et élevée doivent avoir un temps de réponse de fonction de sécurité défini. Un nombre nécessaire de messages de sécurité par seconde doit de ce fait être garanti. Le calcul du taux d'erreur, basé sur un mode à sollicitation élevée est par conséquent également applicable au mode à faible sollicitation.

Tableau 3 – Relation entre le taux d'erreurs résiduelles et le niveau SIL

Applicable pour les fonctions de sécurité jusqu'au niveau SIL	Probabilité d'une défaillance dangereuse par heure pour le système de communication de sécurité fonctionnelle	Taux d'erreurs résiduelles maximal admissible pour le système de communication de sécurité fonctionnelle
4	$< 10^{-10}$ / h	$\Lambda < 10^{-10}$ / h
3	$< 10^{-9}$ / h	$\Lambda < 10^{-9}$ / h
2	$< 10^{-8}$ / h	$\Lambda < 10^{-8}$ / h
1	$< 10^{-7}$ /h	$\Lambda < 10^{-7}$ / h

NOTE Les valeurs données dans ce tableau sont basées sur l'hypothèse selon laquelle la contribution du système de communication de sécurité fonctionnelle au nombre total de défaillances de la fonction de sécurité ne dépasse pas 1%.

5.7 Relation entre sécurité fonctionnelle et sûreté

NOTE 1 L'évaluation de la menace pour la sécurité et des risques constitue une opération normalement nécessaire pour que les applications relatives à la sécurité assurent une protection contre les attaques délibérées ou les changements intempestifs. La mise en place de politiques et mesures de sûreté appropriées telles que des mesures physiques (par exemple, mécaniques, électroniques) ou organisationnelles permettent d'établir la sûreté.

Lorsqu'une application exige des mesures de sûreté électronique, cette sûreté doit être mise en œuvre dans le canal noir. La fonction de sûreté peut être mise en œuvre soit dans les dispositifs, soit aux points d'accès externes. Certaines exigences relatives à la sûreté seront décrites en détail dans la série CEI 62443.

NOTE 2 Des exigences supplémentaires spécifiques au profil peuvent également être précisées dans la CEI 61784-4 [10].

5.8 Conditions aux limites et contraintes

5.8.1 Sécurité électrique

La sécurité électrique est une condition préalable à un système de communication de sécurité fonctionnelle. Par conséquent, tous les dispositifs qui sont reliés doivent être conformes aux spécifications CEI TBTS/TBTP applicables (par exemple CEI 61131-2).

NOTE 1 Les ajouts nécessaires aux lignes directrices d'installation (par exemple, câbles, installation par câble, écrans, mise à la terre, équilibrage de potentiel) sont spécifiés dans la CEI 61918 et la CEI 61784-5.

NOTE 2 Les exigences concernant les sources d'alimentation (par exemple, démonstration de panne simple, utilisation d'alimentations distinctes, TBTS/TBTP, limitations de courant spécifiques au pays, etc.) sont spécifiées dans la CEI 61918 et la CEI 61784-5.

NOTE 3 Les exigences concernant les dispositifs de bus standard (par exemple, évaluation) sont spécifiques aux profils de communication de sécurité fonctionnelle.

5.8.2 Compatibilité électromagnétique (CEM)

La CEI 61508 exige une «Augmentation de l'immunité aux perturbations », mais ne précise pas la méthode à employer pour y parvenir. Les profils de communication de sécurité fonctionnelle décrits dans la présente norme utilisent à cette fin les niveaux d'essai renforcés et les critères de performance correspondants spécifiés dans la CEI 61326-3-1. La CEI 61326-3-2 peut être utilisée à titre d'exception, si l'application prévue correspond exactement au domaine d'application et conditions préalables spécifiques de la CEI 61326-3-2.

NOTE Certaines applications peuvent exiger des niveaux plus élevés que ceux spécifiés dans la CEI 613626-3-1, selon la Spécification sur les exigences de sécurité (SRS).

5.9 Lignes directrices d'installation

Les exigences concernant l'installation des matériels utilisant les technologies de communication spécifiées dans la présente norme sont spécifiées dans la CEI 61918 et les parties de la CEI 61784-5 spécifiques au profil, ainsi que les normes supplémentaires appropriées requises par les profils individuels.

La présence de dispositifs non conformes sur le bus pourrait interrompre le fonctionnement et compromettre de ce fait la disponibilité (en raison de déclenchements parasites, y compris les déclenchements commandés par la fonction de sécurité sans réel danger), provoquant ultérieurement la désactivation de la fonction de sécurité par l'utilisateur.

Il est ainsi vivement recommandé que tous les produits reliés au bus de terrain dans une application de sécurité (même les produits standard) permettent une évaluation de conformité appropriée du protocole de bus de terrain pertinent (par exemple, déclaration du fabricant ou évaluation par un tiers).

NOTE Des détails supplémentaires peuvent être fournis dans les parties spécifiques à la technologie de la présente norme le cas échéant.

5.10 Manuel de sécurité

Selon la CEI 61508-2, les fournisseurs de dispositifs doivent fournir un manuel de sécurité. Les parties appropriées et spécifiques au profil décrivent les informations minimales exigées que le manuel de sécurité doit contenir.

5.11 Politique de sécurité

Les utilisateurs de la présente norme doivent tenir compte des contraintes suivantes pour éviter tout malentendu, toutes fausses attendues ou toutes actions légales concernant les développements et les applications relatifs à la sécurité.

NOTE 1 Ceci inclut, par exemple, le recours à la formation, aux séminaires, ateliers et conseils.

L'application à un dispositif des technologies de communication spécifiées dans la présente norme ne garantit pas une réponse à toutes les exigences nécessaires sur le plan technique, organisationnel et juridique, associées aux applications de sécurité, conformément aux exigences de la CEI 61508.

Des processus appropriés de cycle de vie et de gestion de la sécurité fonctionnelle, conformes aux normes de sécurité et aux législations/réglementations applicables, doivent être respectés pour qu'un dispositif, basé sur la présente norme, puisse être utilisé dans les applications dites de sécurité. Cet aspect doit être évalué conformément aux exigences d'indépendance et de compétence spécifiées dans la CEI 61508-1.

Dans le contexte de l'intégrité de la sécurité du matériel, le niveau d'intégrité de sécurité le plus élevé qui peut être revendiqué pour une fonction de sécurité est limité par les contraintes d'intégrité de sécurité du matériel qui doivent être réalisées par l'application du parcours 1H spécifié dans la CEI 61508-2, sur la base des concepts de tolérance aux anomalies du matériel et de la part des défaillances en sécurité (à mettre en œuvre au niveau du système ou du sous-système).

Le fabricant d'un dispositif qui utilise les technologies de communication spécifiées dans la présente norme est chargé de l'application correcte de la norme, ainsi que de l'exactitude et de l'exhaustivité de la documentation et des informations relatives au dispositif.

Il est vivement recommandé que les mises en œuvre d'application d'un profil spécifique satisfassent aux essais de conformité et de validations correspondantes aux technologies de l'organisation. Les informations concernant les laboratoires d'essai qui peuvent fournir des essais de conformité et des validations conformément aux exigences du présent article sont spécifiées à l'Annexe B de chaque partie dédiée aux profils individuels.

NOTE 2 Ces exigences et recommandations sont incluses dans la mesure où des mises en œuvre incorrectes pourraient provoquer des blessures graves, voire le décès d'individus.

6 Famille de profils de communication 1 (FOUNDATION™ Fieldbus) - Profils de sécurité fonctionnelle

6.1 Profil de communication de sécurité fonctionnelle 1/1

La famille de profils de communication 1 (communément appelée FOUNDATION™[16] Fieldbus) 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™[16]) 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 CEI 61784-3-1.

6.2 Présentation générale d'ordre technique

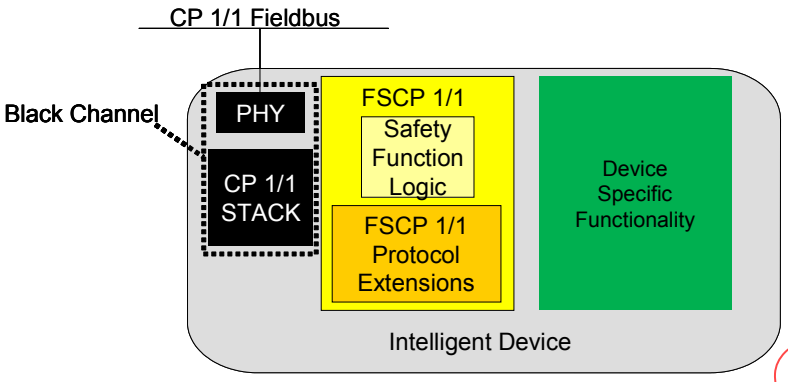
Certaines applications exigent un niveau d'intégrité de sécurité de un à quatre tel que défini dans la CEI 61508.

NOTE Ces applications relatives à la sécurité sont également appelées systèmes instrumentés de sécurité (SIS) (voir CEI 61151 [9]).

La couche de communication de sécurité FSCP 1/1 spécifiée dans la CEI 61784-3-1 permet d'utiliser des dispositifs 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 CEI 61784-3-1 s'applique uniquement au CP 1/1 tel que décrit dans la CEI 61784-1.

La CEI 61784-3-1 ne définit aucune exigence concernant les outils techniques ou la fonctionnalité de mesure interne des dispositifs. La couche de communication de sécurité garantit le téléchargement d'une configuration, créée à l'aide d'un outil technique, dans les dispositifs de sécurité sans que le protocole n'affecte le niveau d'intégrité de sécurité. Le domaine d'application de la CEI 61784-3-1 est défini à la Figure 7.

16 FOUNDATION™ Fieldbus et FF-SIS™ désignent les appellations commerciales de l'organisme sans but lucratif Fieldbus Foundation. Cette information est donnée à l'intention des utilisateurs de la présente Norme internationale et ne signifie nullement que la CEI approuve ou recommande le détenteur de la marque ou de l'un quelconque de ses produits.. La conformité à la présente norme n'exige pas 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.



Légende

Anglais	Français
Fieldbus	Bus de terrain
Black Channel	Canal noir
PHY	Physique
STACK	PILE
Safety Function Logic	Logique de fonction de sécurité
Protocol Extensions	Extensions de protocole
Device specific Functonality	Fonctionnalité spécifique au dispositif
Intelligent Device	Dispositif intelligent

Figure 7 – 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 l'évaluation 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 CEI 61508.

Des informations supplémentaires sont fournies dans la CEI 61784-3-1.

7 Famille de profils de communication 2 (CIP™) – Profils de sécurité fonctionnelle

7.1 Profil de communication de sécurité fonctionnelle 2/1

La famille de profils de communication 2 (communément appelée CIP™[17]) définit des profils de communication sur la base du Type 2 de la CEI 61158-2, de la CEI 61158-3-2, la CEI 61158-4-2, la CEI 61158-5-2 et la CEI 61158-6-2.

Les profils de base CP 2/1, CP 2/2 et CP 2/3 sont définis dans la CEI 61784-1 et la CEI 61784-2. Le profil de communication de sécurité fonctionnelle CPF 2 FSCP 2/1 (CIP Safety™[17]) est fondé sur les profils de base CPF 2 définis dans la CEI 61784-1 et la CEI 61784-2, ainsi que les spécifications de la couche de communication de sécurité définies dans la CEI 61784-3-2.

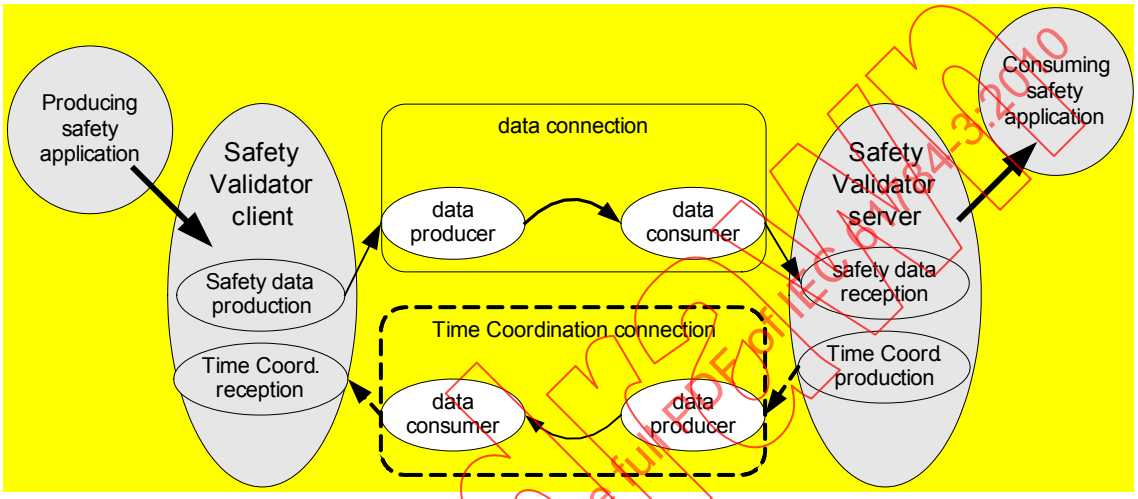
---

17 CIP™ (Common Industrial Protocol) et CIP Safety™ désignent les appellations commerciales de l'organisme sans but lucratif ODVA, Inc. Cette information est donnée à l'intention des utilisateurs de la présente Norme internationale et ne signifie nullement que la CEI approuve ou recommande le détenteur de la marque ou de l'un quelconque de ses produits.. La conformité à la présente norme n'exige pas l'emploi des appellations CIP™ ou CIP Safety™. L'emploi des appellations CIP™ ou CIP Safety™ exige l'autorisation de ODVA.

7.2 Présentation générale d'ordre technique

Le FSCP 2/1 est basé sur le modèle producteur/consommateur de CPF 2. L'association des producteurs et des consommateurs constitue un élément important de la relation qui garantit la haute intégrité nécessaire aux applications relatives à la sécurité.

La couche de communication de sécurité FSCP 2/1 est spécifiée à l'aide d'un objet de validation de sécurité. Cet objet est chargé de la gestion des connexions de sécurité FSCP 2/1 et constitue l'interface entre les objets d'application relatifs à la sécurité et les connexions de couches de liaison, tel qu'illustré à la Figure 8. L'objet de validation de sécurité garantit l'intégrité des transferts des données de sécurité.



Légende

Anglais	Français
Producing safety application	Production d'application de sécurité
Safety Validator client	Objet de validation de sécurité client
Safety data production	Production des données de sécurité
Time Coordination reception	Réception du signal de coordination temporelle
data connection	connexion de données
data producer	producteur de données
data consumer	consommateur des données
Time Coordination production	Production du signal de coordination temporelle
Safety Validator server	Objet de validation de sécurité serveur
Safety data reception	Réception des données de sécurité
Time Coordination production	Production de la coordination temporelle
Consuming safey application	Application de sécurité consommatrice

Figure 8 – Relation des objets de validation de sécurité

L'intégrité des transferts de données de sécurité est assurée comme suit:

— l'application relative à la sécurité productrice utilise une instance d'objet de validation de sécurité client pour générer des données de sécurité et assurer la coordination temporelle;

— le client utilise une liaison producteur de données pour transmettre les données et une liaison consommateur pour recevoir des messages de coordination temporelle;

— l'application relative à la sécurité des données consommées utilise un objet de validation de sécurité serveur pour recevoir et vérifier les données;

— le serveur utilise une liaison consommateur pour recevoir les données et une liaison producteur pour transmettre des messages de coordination temporelle.

Le FSCP 2/1 utilise le concept de canal noir. Les liaisons producteurs et consommateurs de données n'ont aucune connaissance des trames de données de sécurité et ne mettent en œuvre aucune fonction de sécurité. Les objets de validation de sécurité sont responsables du transfert à haute intégrité et du contrôle des données de sécurité.

Le FSCP 2/1 applique les mesures suivantes pour assurer l'intégrité des messages de sécurité:

— datation (horodatage);

— authentification de connexion;

— assurance d'intégrité des données;

— redondance avec contre-vérification;

— différents systèmes d'assurance d'intégrité des données.

Les messages sont produits avec une datation qui permet au consommateur de vérifier l'âge des données transmises. L'identification fait l'objet d'un codage dans chaque message relatif à la sécurité afin de s'assurer que le bon consommateur utilise le message. Tous les messages relatifs à la sécurité utilisent un CRC unique. La transmission des données relatives à la sécurité est redondante. Diverses mesures de production de messages relatifs à la sécurité permettent de s'assurer que les messages CPF 2 standard ne sont pas interprétés comme des messages de sécurité.

Des informations supplémentaires sont fournies dans la CEI 61784-3-2.

8 Famille de profils de communication 3 (PROFIBUS™, PROFINET™) – Profils de sécurité fonctionnelle

8.1 Profil de communication de sécurité fonctionnelle 3/1

La famille de profils de communication 3 (communément appelée PROFIBUS™, PROFINET™[18]) définit des profils de communication sur la base du Type 3 de la CEI 61158-2, de la CEI 61158-3-3, la CEI 61158-4-3, la CEI 61158-5-3, la CEI 61158-5-10, la CEI 61158-6-3 et la CEI 61158-6-10.

Les profils de base CP 3/1 et CP 3/2 sont définis dans la CEI 61784-1; CP 3/4, CP 3/5 et CP 3/6 sont définis dans la CEI 61784-2. Le profil de communication de sécurité fonctionnelle CPF 3 FSCP 3/1 (PROFIsafe™[18]) est fondé sur les profils de base CPF 3 définis dans la CEI 61784-1 et la CEI 61784-2, ainsi que les spécifications de la couche de communication de sécurité définies dans la CEI 61784-3-3.

8.2 Présentation générale d'ordre technique

Le FSCP 3/1 est basé sur l'échange de données cycliques d'un contrôleur (de bus) avec ses dispositifs (de terrain) associés grâce à une relation de communication « one to one » (Figure 9). Un contrôleur peut utiliser toute combinaison de dispositifs standards et de sécurité reliés

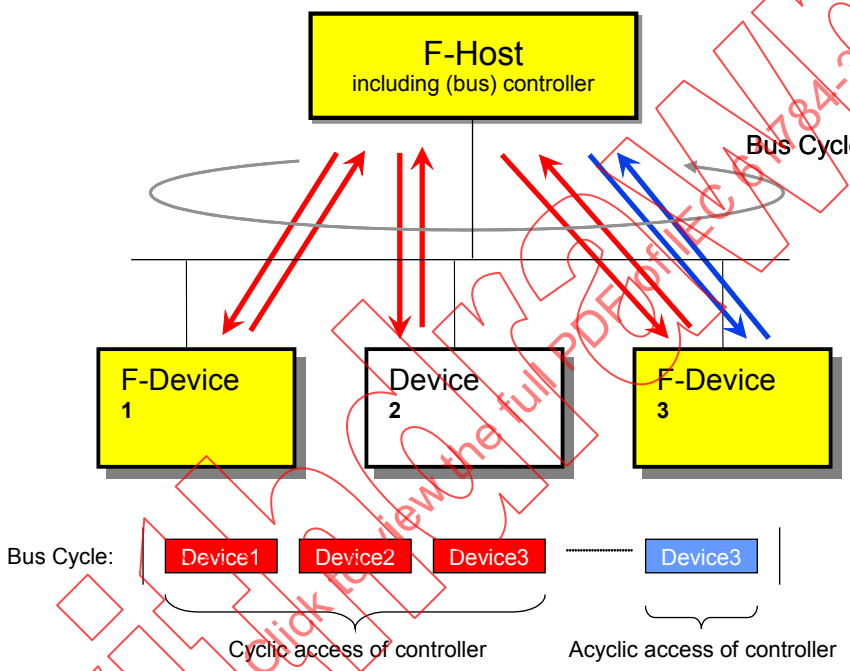
---

18 PROFIBUS™, PROFINET™ et PROFIsafe™ désignent les appellations commerciales de l'organisme sans but lucratif PROFIBUS Nutzerorganisation e.V. (PNO). Cette information est donnée à l'intention des utilisateurs de la présente Norme internationale et ne signifie nullement que la CEI approuve ou recommande le détenteur de la marque ou de l'un quelconque de ses produits. La conformité à la présente norme n'exige pas l'emploi des logos déposés pour PROFIBUS™, PROFINET™ ou PROFIsafe™. L'emploi des logos déposés pour PROFIBUS™, PROFINET™ ou PROFIsafe™ exige l'autorisation de PNO.

au réseau. Il est également possible d'affecter des tâches de sécurité et des tâches normales à différents contrôleurs. Les communications dites acycliques entre les dispositifs et les contrôleurs ou les superviseurs tels que les dispositifs de programmation, sont prévues à des fins de configuration, paramétrage, diagnostic et maintenance.

Les quatre mesures suivantes ont été retenues pour réaliser le protocole FSCP 3/1:

— numérotation consécutive (virtuelle);
— contrôle du temps de fonctionnement du chien de garde avec acquittement;
— nom de code par relation de communication;
— contrôle de redondance cyclique pour l'intégrité des données.

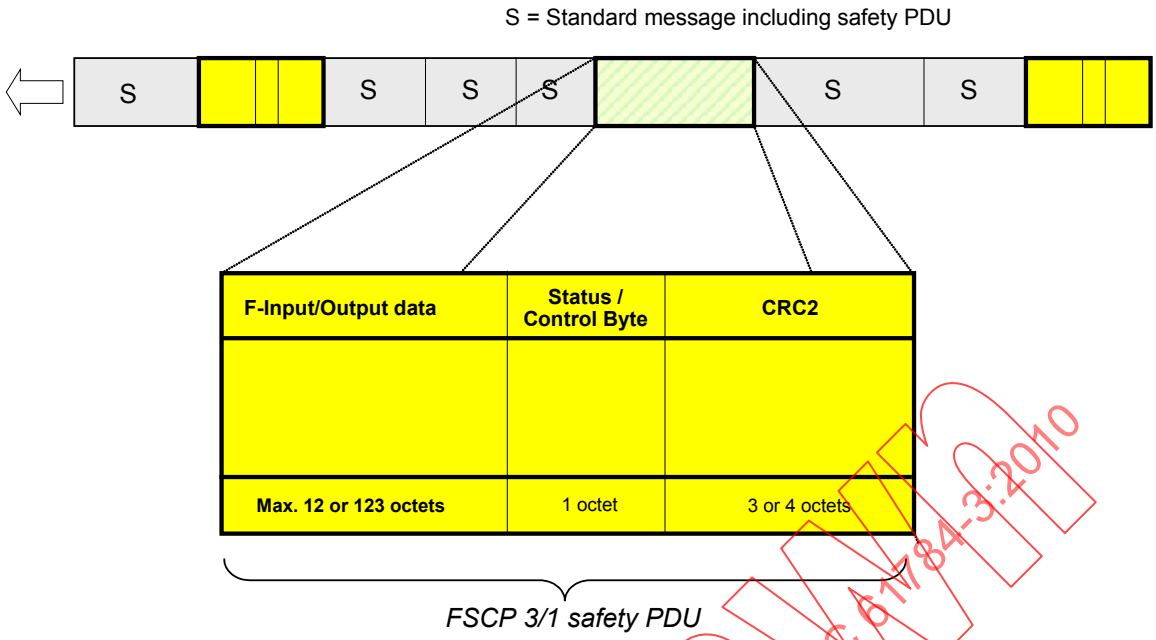


Légende

Anglais	Français
F-Host including (bus) controller	F-Hôte y compris le contrôleur (de bus)
Bus Cycle	Cycle du bus
F-Device	Dispositif F
Device	Dispositif
Cyclic access of controller	Accès cyclique du contrôleur
Acyclic access of controller	Accès acyclique du contrôleur

Figure 9 – Conditions préalables de communication de base pour le protocole FSCP 3/1

La numérotation consécutive utilise une plage suffisamment grande pour sécuriser tout dysfonctionnement provoqué par les éléments de réseau de stockage des messages. Chaque dispositif de sécurité renvoie un message contenant un PDU de sécurité pour acquittement, y compris en l'absence de données du processus. Un temporisateur séparé placé à la fois du côté émetteur et récepteur est utilisé pour chaque relation de communication « one to one ». Le nom de code unique par relation de communication est établi pour des raisons d'authentification, son codage étant constitué d'une valeur de signature CRC initiale pour la signature CRC2 calculée et transmise de manière cyclique (Figure 10).

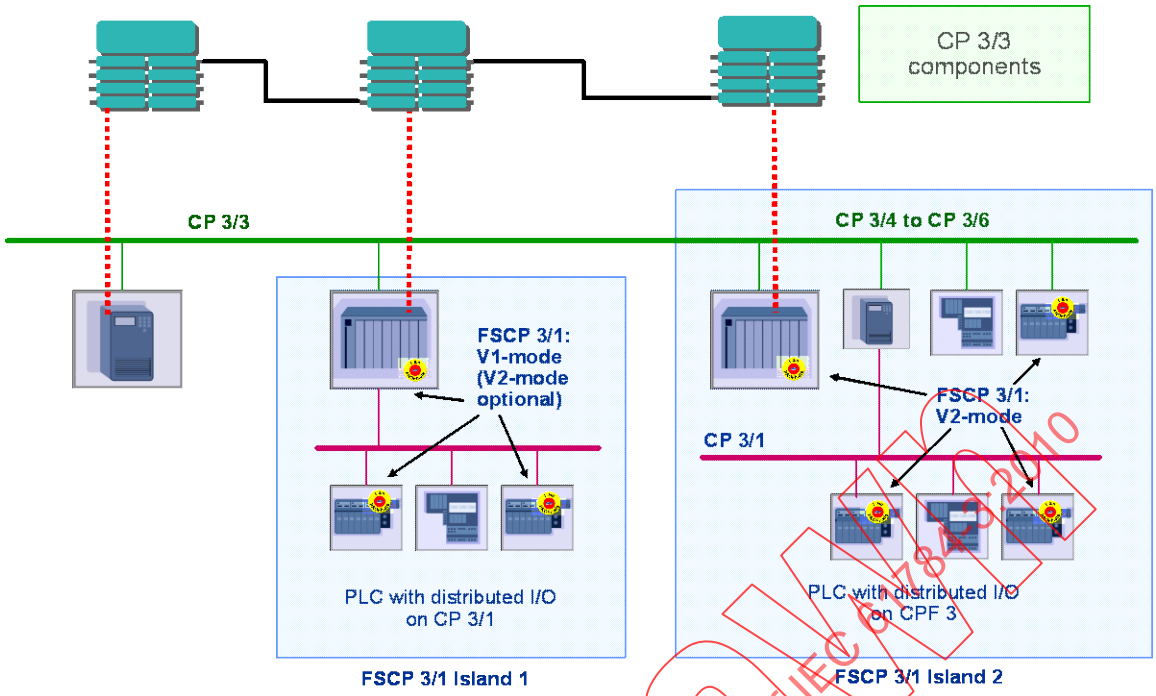


Légende

Anglais	Français
Standard message including safety PDU	Message standard y compris le PDU de sécurité
F-Input/Output data	Données d'entrée/sortie F
Status / Control Byte	Statut / octet de contrôle
Max. 12 or 123 octets	12 ou 123 octets au maximum
or	ou
Safety PDU	PDU de sécurité

Figure 10 – Structure d'un PDU de sécurité FSCP 3/1

Le FSCP 3/1 fournit deux modes de fonctionnement: les modes V1 et V2. Alors que les mesures du mode V1 permettent une transmission des données en toute sécurité sur de véritables réseaux CP 3/1, les caractéristiques plus « généreuses » d' Ethernet / CP 3/4 à CP 3/6, telles qu'un plus large espace d'adressage et des composants de commutation de stockage exigent certaines extensions au protocole FSCP 3/1, conduisant ainsi au mode V2. Le mode V1 est limité au protocole CP 3/1, tandis que le mode V2 est requis pour les protocoles CP 3/4 à C/P 3/6 et/ou CP 3/1. La CEI 61784-3-3 décrit uniquement les détails de la fonctionnalité étendue du mode dit V2. Une communication sécurisée entre les composantes PROFINET CBA (voir CP 3/3) n'est pas encore définie. La Figure 11 présente de manière générale le protocole FSVP 3/1 dans le cadre des architectures CP 3/1 et CP 3/4 à CP 3/6.



Légende

Anglais	Français
components	composants
CP 3/4 to CP 3/6	CP 3/4 à CP 3/6
V1 mode	Mode V1
V2 mode optional	Mode V2 facultatif
PLC with distributed I/O on CP 3/1	PLC avec répartition E/S sur CP 3/1
PLC with distributed I/O on CP 3	PLC avec répartition E/S sur CP 3
FSCP 3/1 Island 1	Ilôt FSCP 3/1

Figure 11 – Modes de communication sécurisée

Des informations supplémentaires sont fournies dans la CEI 61784-3-3.

9 Famille de profils de communication 6 (INTERBUS®) – Profils de sécurité fonctionnelle

9.1 Profil de communication de sécurité fonctionnelle 6/7

La famille de profils de communication 6 (communément appelée INTERBUS®[19]) définit des profils de communication sur la base du Type 8 de la CEI 61158-2, de la CEI 61158-3-8, la CEI 61158-4-8, la CEI 61158-5-8 et la CEI 61158-6-8.

Les profils de base CP 6/1, CP 6/2, CP 6/3 sont définis dans la CEI 61784-1. Le profil de communication de sécurité fonctionnelle CPF 6 FSCP 6/7 (INTERBUS Safety™[19]) est fondé sur les profils de base CPF 6 définis dans la CEI 61784-1, ainsi que les spécifications de la couche de communication de sécurité définies dans la CEI 61784-3-6.

19 INTERBUS® et INTERBUS Safety™ désignent les appellations commerciales de Phoenix Contact GmbH & Co. KG. Le contrôle de l'emploi des appellations commerciales est confié à l'organisme sans but lucratif INTERBUS Club. Cette information est donnée à l'intention des utilisateurs de la présente Norme internationale et ne signifie nullement que la CEI approuve ou recommande le détenteur de la marque ou de l'un quelconque de ses produits. La conformité à la présente norme n'exige pas l'emploi des appellations INTERBUS® ou INTERBUS Safety™. L'emploi des appellations INTERBUS® ou INTERBUS Safety™ exige l'autorisation de INTERBUS Club.

Les profils CP 6/1, CP 6/2 et CP 6/3 contiennent des services facultatifs, spécifiés par des identificateurs de profil. Les identificateurs de profil nécessaires pour le protocole CP 6/7 sont présentés dans le Tableau 4.

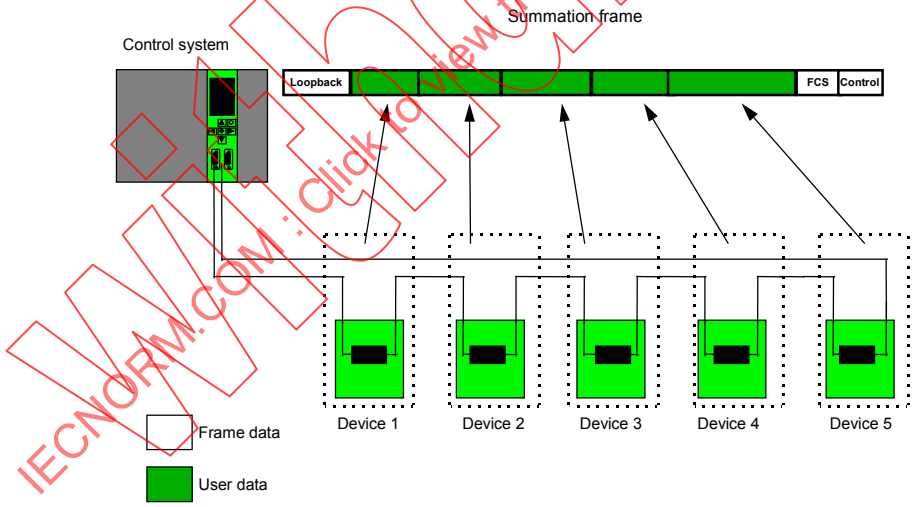
Tableau 4 – Présentation générale de l'identificateur de profil applicable au protocole FSCP 6/7

Profil	Maître		Esclave		
	Cyclique	Cyclique et non cyclique	cyclique	Non cyclique	Cyclique et non cyclique
Profil 6/1	618	619	611	—	613
Profil 6/2	—	629	—	—	623
Profil 6/3	—	639	—	—	633

La spécification de la couche de communication de sécurité donnée dans la CEI 61784-3-6 s'applique dans son intégralité.

9.2 Présentation générale d'ordre technique

Le FSCP 6/7 utilise la voie de transport existante pour la transmission cyclique des données (pour les données du processus). Il s'agit, en principe, d'un concept maître-esclave avec une topologie en anneau physique et l'existence de relations logiques « one to one » entre un maître et chacun de ses esclaves (Figure 12). La transmission des données s'effectue via un PDU – communément appelé trame unique– à partir duquel chaque esclave extrait ses données de sortie et insère ses données d'entrée.



Légende

Anglais	Français
Summation frame	Trame unique
Control system	Système de commande
Loopback	Bouclage
Control	Commande
Frame data	Données de trame
Device	Dispositif
User data	Données utilisateur

Figure 12 – Conditions préalables de communication FSCP 6/7

La couche de communication de sécurité du FSCP 6/7 fournit les mesures de sécurité suivantes pour sa réalisation:

— numéro de séquence;

— datation (horodatage);

— authentification de connexion;

— contrôle de redondance cyclique pour l'intégrité des données de sécurité.

La numérotation de séquence utilise une plage comprise entre 001 et 111 sans 000. L'authentification de connexion (informations émetteur/récepteur) est codée sur 7 bits, de sorte qu'il est possible de connecter un nombre maximal de 126 esclaves sur le bus de terrain de sécurité. Le transfert des données de sécurité peut s'effectuer entre le maître de sécurité et chaque esclave de sécurité correspondant, et entre chaque esclave de sécurité et le maître de sécurité correspondant dans un cycle de données unique. Un temporisateur séparé placé sur chaque esclave de sortie de sécurité garantit un temps de réponse pour chaque fonction de sécurité, son paramétrage est possible sur une large échelle . Le temporisateur peut être adapté pour chaque canal de sortie de sécurité d'un esclave de sortie.

La couche de communication de sécurité de FSCP 6/7 peut être utilisée pour des fonctions de sécurité jusqu'au niveau SIL 3. Par conséquent, le bus de terrain de sécurité consomme au maximum 1% du PFH global. On obtient $\Lambda < 10^{-7}$ dans le bus de terrain de sécurité. Un temporisateur intégré fournissant le délai de chaque canal de sortie de chaque esclave de sortie de sécurité correspondant, garantit un temps de réponse de sécurité fonctionnelle. Le temps de réponse de sécurité fonctionnelle comprend le temps de transmission du bus de terrain entre un esclave d'entrée de sécurité et le maître, et entre le maître et l'esclave de sortie de sécurité, y compris également les répétitions éventuelles du PDU de sécurité en raison des erreurs de transmission, le temps de traitement de chaque esclave de sécurité (entrée et sortie) et le temps de traitement du système PES (généralement réalisé par un PLC de sécurité avec un maître intégré) et le temps d'arrêt d'une machine. Si le temps configuré du temporisateur intégré du canal de sortie spécifique d'un esclave de sortie de sécurité est écoulé, le canal de sortie correspondant est réglé sur son état de sécurité, qui est habituellement l'état hors tension.

La structure du PDU de sécurité comprend les mesures de sécurité (numéro de séquence, datation, authentification de connexion, CRC) et les données de sécurité. Les données et les mesures de sécurité pour chaque esclave de sécurité sont intégrées dans la trame unique.

Des informations supplémentaires sont fournies dans la CEI 61784-3-6.

10 Famille de profils de communication 8 (CC-Link™) – Profils de sécurité fonctionnelle

10.1 Profil de communication de sécurité fonctionnelle 8/1

La famille de profils de communication 18 (communément appelée CC-Link™[20]) définit des profils de communication sur la base du Type 18 de la CEI 61158-2, de la CEI 61158-3-18, la CEI 61158-4-18, la CEI 61158-5-18 et la CEI 61158-6-18.

Les profils de base CP 8/1, CP 8/2 et CP 8/3 sont définis dans la CEI 61784-1. Le profil de communication de sécurité fonctionnelle CPF 8 FSCP 8/1 (CC-Link Safety™[20]) est fondé sur

20 CC-Link™ et CC-Link Safety™ désignent les appellations commerciales de l'organisme sans but lucratif CC-Link Partner Association. Cette information est donnée à l'intention des utilisateurs de la présente Norme internationale et ne signifie nullement que la CEI approuve ou recommande le détenteur de la marque ou de l'un quelconque de ses produits. La conformité à la présente norme n'exige pas l'emploi des appellations CC-Link™ or CC-Link Safety™. L'emploi des appellations CC-Link™ ou CC-Link Safety™ exige l'autorisation de la CC-Link Partner Association.

les profils de base CPF 8 définis dans la CEI 61784-1, ainsi que les spécifications de la couche de communication de sécurité définies dans la CEI 61784-3-8.

10.2 Présentation générale d'ordre technique

Le FSCP 8/1 est un protocole de communication de données relatives à la sécurité tel que les signaux d'arrêt d'urgence entre les participants d'un réseau réparti, en utilisant la technologie de bus de terrain conformément aux exigences de la CEI 61508 concernant la sécurité fonctionnelle. Ce protocole peut être utilisé dans diverses applications telles que la commande de processus, l'usinage automatique et les machines.

Le protocole FSCP 18/1 est conçu de manière à prendre en charge le niveau d'intégrité de sécurité SIL 3 (CEI 61508) qui utilise CPF 8, en spécifiant par ailleurs des mécanismes de mise en œuvre des numéros de séquence, délai, authentification de connexion, message de réaction, assurance d'intégrité des données et différentes mesures de sécurité dédiées à ladite assurance.

L'introduction des éléments de service d'application de sécurité (SASE) fournit les capacités SCL du protocole FSCP 8/1. Ces SASE se substituent à leurs éléments de service d'application (ASE) correspondants, tel que spécifié dans la CEI 61784-3-8. Cependant, dans la mesure où ces SASE proviennent directement des classes de parent définies pour le CPF 8, ils spécifient les ajouts nécessaires à ce dernier en vue d'une sécurité fonctionnelle, en appliquant la méthode du canal noir.

Des informations supplémentaires sont fournies dans la CEI 61784-3-8.

11 Famille de profils de communication 12 (EtherCAT™) – Profils de sécurité fonctionnelle

11.1 Profil de communication de sécurité fonctionnelle 12/1

La famille de profils de communication 12 (communément appelée EtherCAT™[21]) définit des profils de communication sur la base du Type 12 de la CEI 61158-2, de la CEI 61158-3-12, la CEI 61158-4-12, la CEI 61158-5-12 et la CEI 61158-6-12.

Les profils de base CP 12/1 et CP 12/2 sont définis dans la CEI 61784-2. Le profil de communication de sécurité fonctionnelle CPF 12 FSCP 12/1 (Safety-over-EtherCAT™) est fondé sur les profils de base de CPF 12 définis dans la CEI 61784-2, ainsi que les spécifications de la couche de communication de sécurité définies dans la CEDI 61784-3-12.

11.2 Présentation générale d'ordre technique

Le protocole FSCP 12/1 décrit un protocole de sécurité qui permet le transfert de données de sécurité jusqu'au niveau SIL3 entre les dispositifs de Type FSCP 12/1. Les PDU de sécurité sont transférés par un bus de terrain subordonné non pris en compte dans les considérations de sécurité, étant donné qu'il peut être considéré comme un canal noir. Les PDU de sécurité échangés entre deux partenaires de communication sont considérés comme des données du processus cyclique échangées par le bus de terrain subordonné.

Le protocole FSCP 12/1 utilise une relation maître/esclave unique entre le maître FSoE et un esclave de même nature, appelée connexion FSoE (Figure 13). Dans ce type de connexion, chaque dispositif renvoie uniquement son propre message à la réception d'un nouveau

---

21 EtherCAT™ et Safety-over-EtherCAT™ désignent les appellations commerciales de Beckhoff, Verl. Cette information est donnée à l'intention des utilisateurs de la présente Norme internationale et ne signifie nullement que la CEI approuve ou recommande le détenteur de la marque ou de l'un quelconque de ses produits. La conformité à la présente norme n'exige pas l'emploi des appellations EtherCAT™ ou Safety-over-EtherCAT™. L'emploi des appellations EtherCAT™ ou Safety-over-EtherCAT™ exige l'autorisation de Beckhoff, Verl.