# IEC 61784-3

Edition 1.0 2007-12

# INTERNATIONAL STANDARD

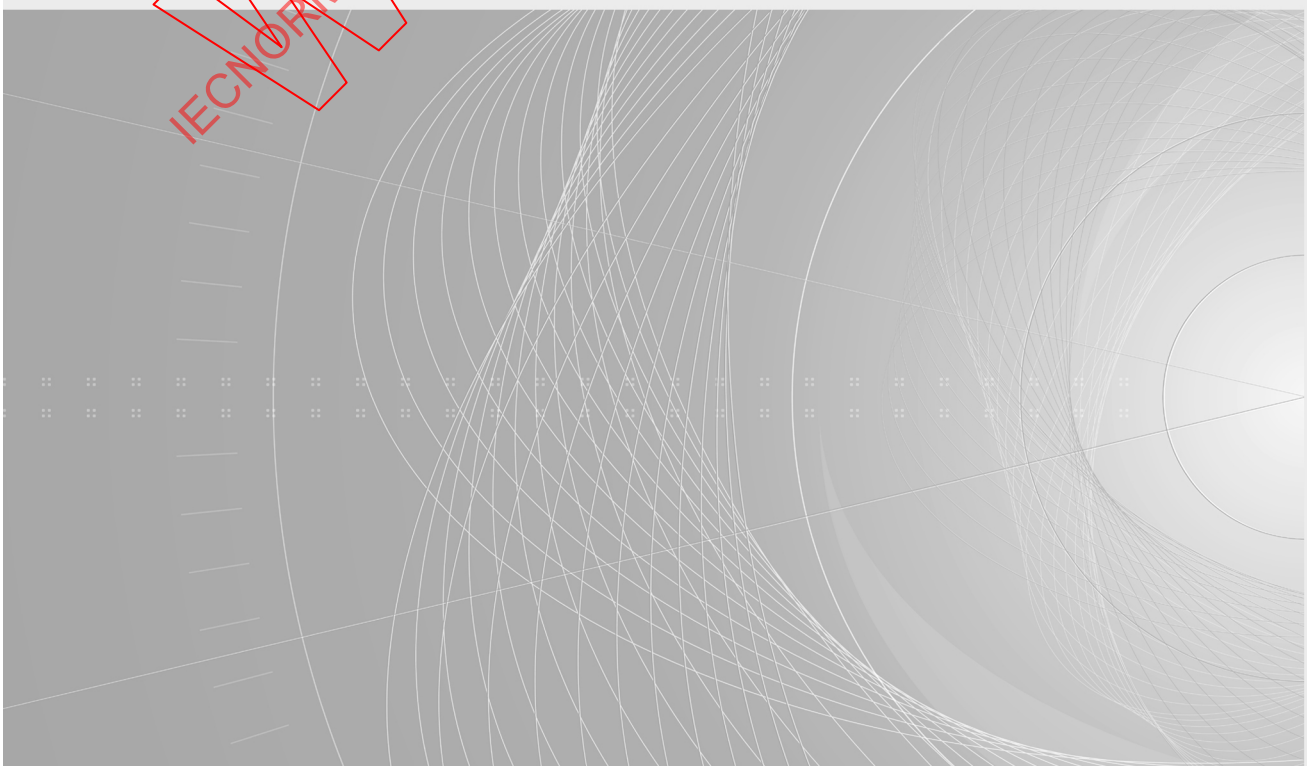
# NORME INTERNATIONALE

colour inside

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

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





IEC 61784-3:2007

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
info@iec.ch
www.iec.ch

## About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

## About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

**Useful links:**

IEC publications search - www.iec.ch/searchpub

The advanced search enables you to find IEC publications by a variety of criteria (reference number, text, technical committee,…).
It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

Stay up to date on all new IEC publications. Just Published details all new publications released. Available on-line and also once a month by email.

Electropedia - www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 30 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary (IEV) on-line.

Customer Service Centre - webstore.iec.ch/csc

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: csc@iec.ch.

## A propos de la CEI

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

## A propos des publications CEI

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

**Liens utiles:**

Recherche de publications CEI - www.iec.ch/searchpub

La recherche avancée vous permet de trouver des publications CEI en utilisant différents critères (numéro de référence, texte, comité d'études,…).
Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

Just Published CEI - webstore.iec.ch/justpublished

Restez informé sur les nouvelles publications de la CEI. Just Published détaille les nouvelles publications parues. Disponible en ligne et aussi une fois par mois par email.

Electropedia - www.electropedia.org

Le premier dictionnaire en ligne au monde de termes électroniques et électriques. Il contient plus de 30 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans les langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (VEI) en ligne.

Service Clients - webstore.iec.ch/csc

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: csc@iec.ch.

# IEC 61784-3

Edition 1.0 2007-12

# INTERNATIONAL STANDARD

# NORME INTERNATIONALE

colour inside

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

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



INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

PRICE CODE
CODE PRIX X

ICS 35.100.05 25.040.40

ISBN 978-2-83220-535-8

# 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 provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with an IEC Publication.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

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 and 6 given in IEC 61784-3-1, IEC 61784-3-2, IEC 61784-3-3 and IEC 61784-3-6.

IEC takes no position concerning the evidence, validity and scope of these patent rights.The holders of these patent rights have assured the IEC that they are willing to negotiate licences under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the 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 and IEC 61784-3-6.

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 bilingual version (2012-12) corresponds to the monolingual English version, published in 2007-12.

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

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

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

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

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

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

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

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

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

# INTRODUCTION

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

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

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

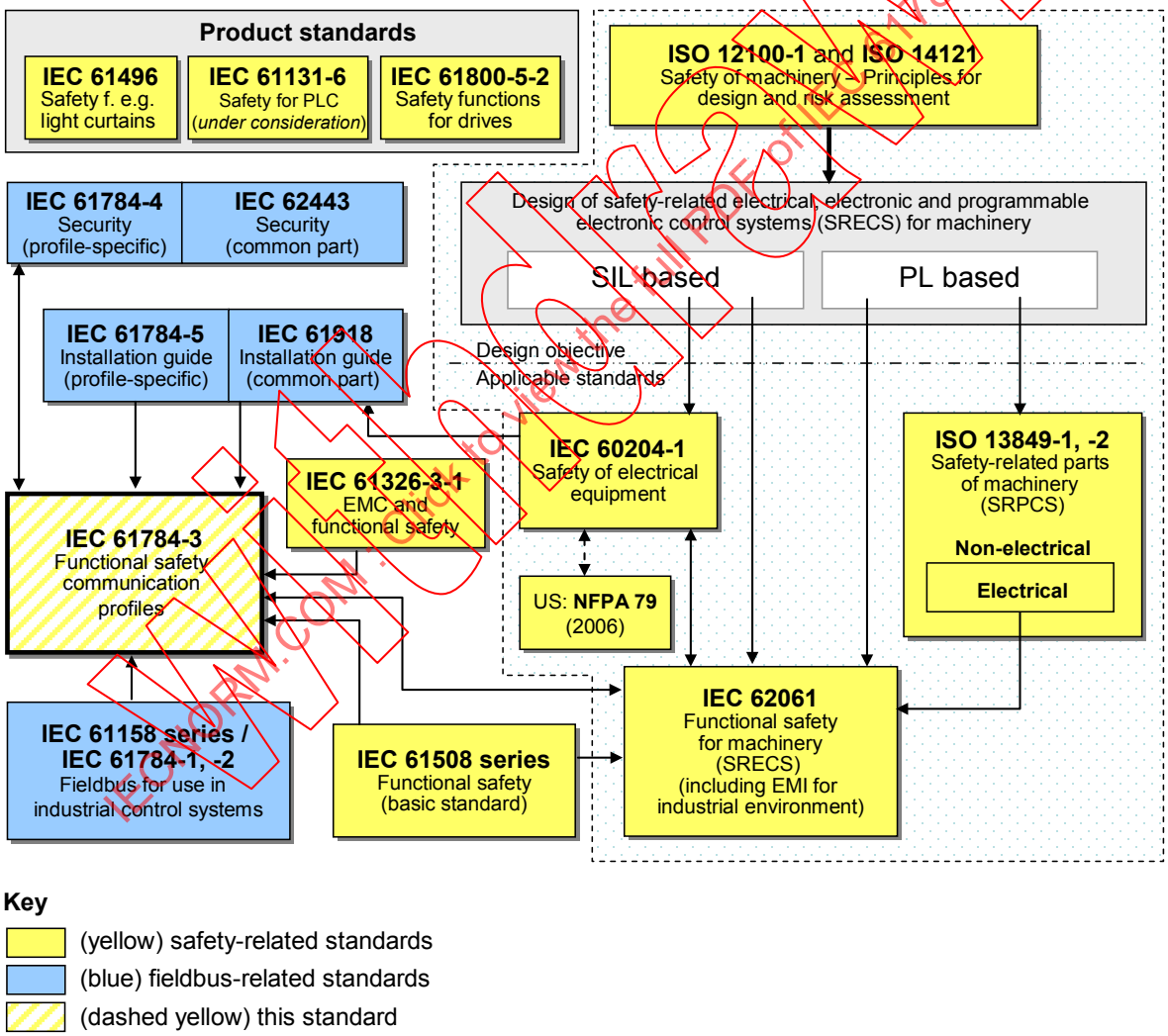
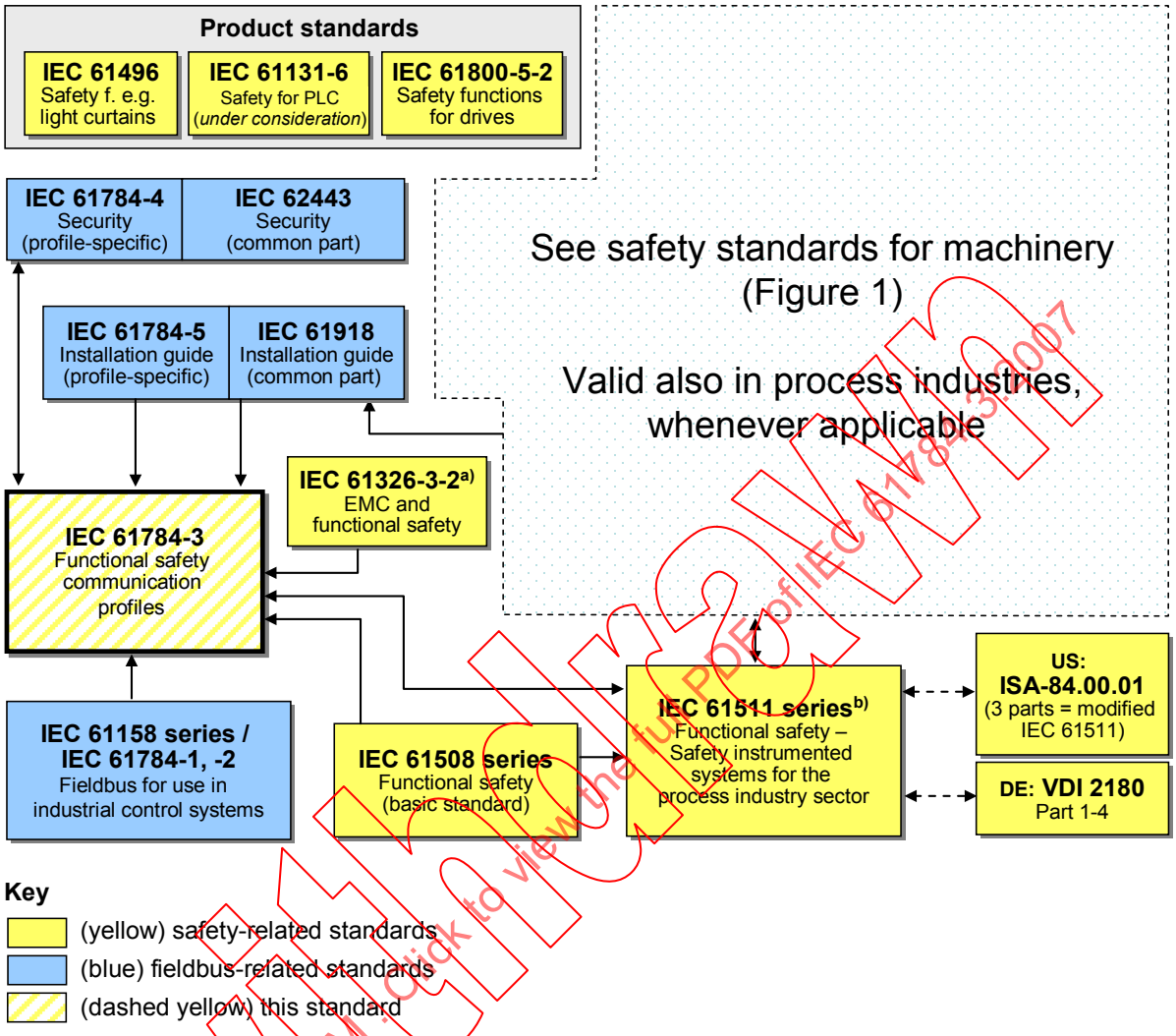



**Figure 1 – Relationships of IEC 61784-3 with other standards (machinery)**

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




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

b EN ratified.

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



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

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

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

This standard describes:

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

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

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

# INDUSTRIAL COMMUNICATION NETWORKS – PROFILES

## Part 3: 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 for functional safety. These principles can be used in various industrial applications such as process control, manufacturing automation and machinery.

This part[1] 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. IEC 62443 will address many of these issues; the relationship with IEC 62443 is detailed in a dedicated subclause of this part.

NOTE 3 Additional profile specific requirements for security may also be specified in the future IEC 61784-4.

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*[2]

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

---

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

2 To be published.

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

IEC 61508-1, *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 61784-5 (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*

## 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

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

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

**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 [26], [27] [3].

**3.1.1.9**
**diversity**
different means of performing a required function

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

[IEC 61508-4:1998]

**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

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

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

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

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

**3.1.1.11**
**failure**
termination of the ability of a functional unit to perform a required function

[3] Figures in square brackets refer to the bibliography.

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

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

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

**3.1.1.12**
**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 preventative maintenance or other planned actions, or due to lack of external resources.

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

**3.1.1.13**
**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

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

NOTE 2 See also [26], [27].

**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 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**
**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]

**3.1.1.25**
**redundancy**
existence of means, in addition to the means which would be sufficient for a functional unit to perform a required function or for data to represent information

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

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

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

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

**3.1.1.26**
**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]

**3.1.1.27**
**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]

**3.1.1.28**
**risk**
combination of the probability of occurrence of harm and the severity of that harm
[IEC 61508-4:1998]

**3.1.1.29**
**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

**3.1.1.30**
**safety connection**
connection that utilizes the safety protocol for communications transactions

**3.1.1.31**
**safety data**
data transmitted across a safety network using a safety protocol

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

**3.1.1.32**
**safety device**
device designed in accordance with IEC 61508 and which implements the functional safety communication profile

**3.1.1.33**
**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]

**3.1.1.34**
**safety function**
function to be implemented by an E/E/PE safety-related system, other technology *safety-related system* or external risk reduction facilities, which is intended to achieve or maintain a safe state for the EUC, in respect of a specific hazardous event
[IEC 61508-4:1998]

**3.1.1.35**
**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.

**3.1.1.36**
**safety integrity level (SIL)**
discrete level (one out of a possible four) for specifying the safety integrity requirements of the *safety functions* to be allocated to the E/E/PE safety-related systems, where safety

integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest

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

[IEC 61508-4:1998]

**3.1.1.37**
**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.

**3.1.1.38**
**safety-related application**
programs designed in accordance with IEC 61508 to meet the SIL requirements of the application

**3.1.1.39**
**safety-related system**
system performing *safety functions* according to IEC 61508

**3.1.1.40**
**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

**3.1.1.41**
**spurious trip**
trip caused by the safety system without a process demand

**3.1.1.42**
**time stamp**
time information included in a *message*

**3.1.1.43**
**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.

## 3.2 Symbols and abbreviated terms

### 3.2.1 Common symbols and abbreviated terms

| | | |
|---|---|---|
| CP | Communication Profile | [IEC 61784-1] |
| CPF | Communication Profile Family | [IEC 61784-1] |
| CRC | Cyclic Redundancy Check | |
| DLL | Data Link Layer | [ISO/IEC 7498-1] |
| DLPDU | Data Link Protocol Data Unit | |
| EMI | Electro-Magnetic Interference | |
| EUC | Equipment Under Control | [IEC 61508-4:1998] |
| FAL | Fieldbus Application Layer | [IEC 61158-5] |
| FCS | Frame Check Sequence | |
| FSCP | Functional Safety Communication Profile | |
| HD | Hamming Distance | |
| E/E/PE | Electrical/Electronic/Programmable Electronic | [IEC 61508-4:1998] |
| NSR | Non Safety Relevant | |
| PDU | Protocol Data Unit | [ISO/IEC 7498-1] |
| PELV | Protective Extra Low Voltage | |
| PES | Programmable Electronic System | [IEC 61508-4:1998] |
| PFD | Average Probability of Failure on Demand | [IEC 61508-6:1998] |
| PFH | Probability of Failure per Hour | [IEC 61508-6:1998] |
| PhL | Physical Layer | [ISO/IEC 7498-1] |
| PLC | Programmable Logic Controller | |
| SCL | Safety Communication Layer | |
| SELV | Safety Extra Low Voltage | |
| SIL | Safety Integrity Level | [IEC 61508-4:1998] |
| 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 |

### 3.2.5 CPF 6: Additional symbols and abbreviated terms

None required for this part.

# 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 61784-3:200x FSCP n/m <Type>

or

conformance to IEC 61784-3 (Ed.1.0) 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:200x

or

conformance to IEC 61784-3-N (Ed.1.0)

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

The IEC 61508 is defining 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 $PFH_{safety\ communication\ channel}$.

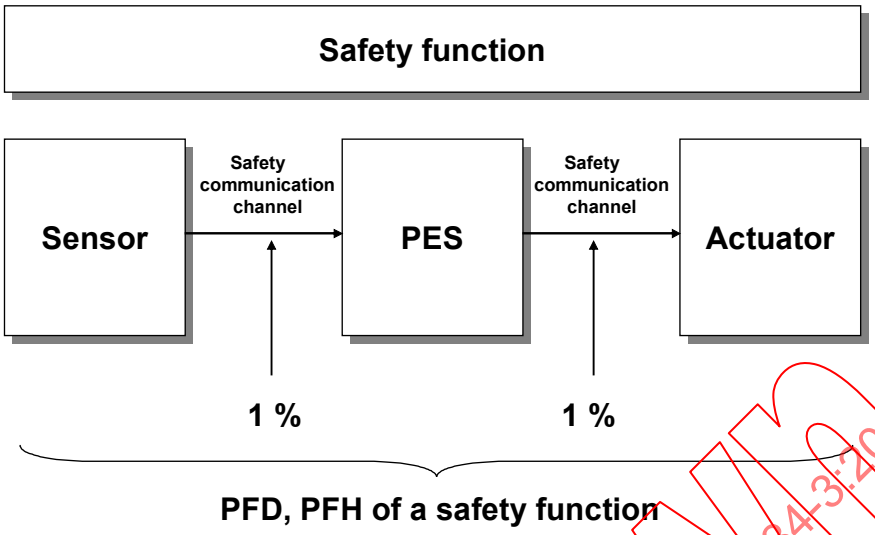



**Figure 3 – Safety communication as a part of a safety function**

## 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 [25].

### 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.

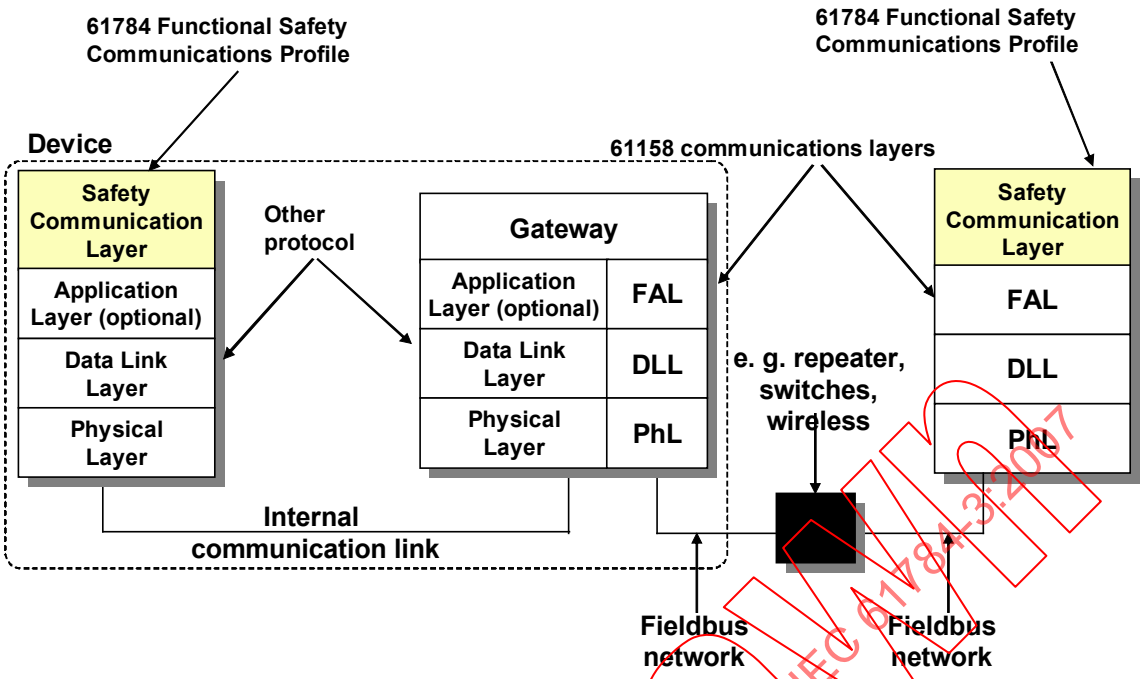



**Figure 4 – Example model of a functional safety communication system**

### 5.2.3 Communication channel types

IEC 61508 series [4] will 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.

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.



4 Second edition in preparation.

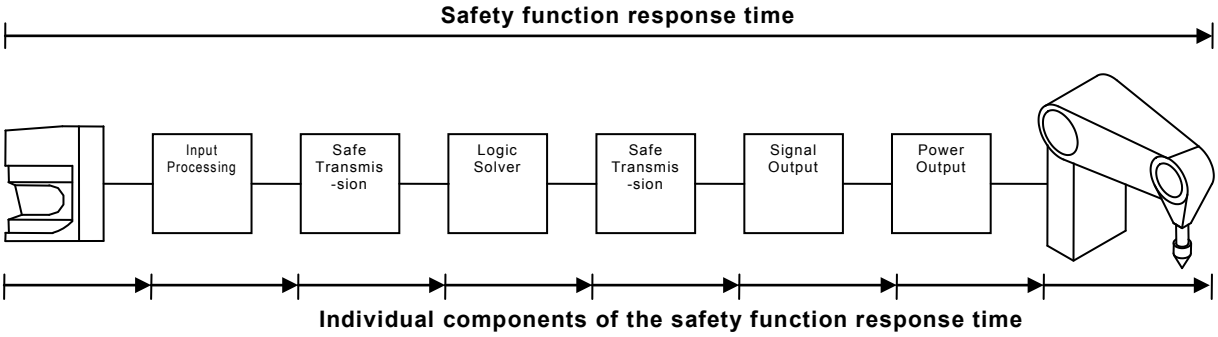



**Figure 5 – Example of safety function response time components**

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

EXAMPLE

This returned feedback message may contain only a short acknowledge, or may also contain the original data, thus enabling the source to check the correct reception by comparing sent and received data.

### 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.

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

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

| Communication errors | Safety measures | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | Sequence number | Time stamp | Time expectation | Connection authentication | Feedback message | Data integrity assurance | Redundancy with cross checking | Different data integrity assurance systems |
| Corruption (see 5.3.2) | | | | | X | X | Only for serial bus[d] | |
| 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[c] | | | | | |
| Insertion (see 5.3.7) | X | | | X[a,b] | X[a] | | X | |
| Masquerade (see 5.3.8) | | | | X[a] | X[a] | | | X |
| Addressing (see 5.3.9) | | | | X | | | | |

NOTE Table adapted from IEC 62280-2 and [25].

[a] Depends on application.

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

[c] Required in all cases.

[d] 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.



## 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 formula (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 formula are specified in Table 2.

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

NOTE 2 This formula assumes cyclic transmission of safety messages.

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

| Formula items | Definition |
|---|---|
| $\Lambda_{SL}$ (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 |
| $R_{SL}$ (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) |

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

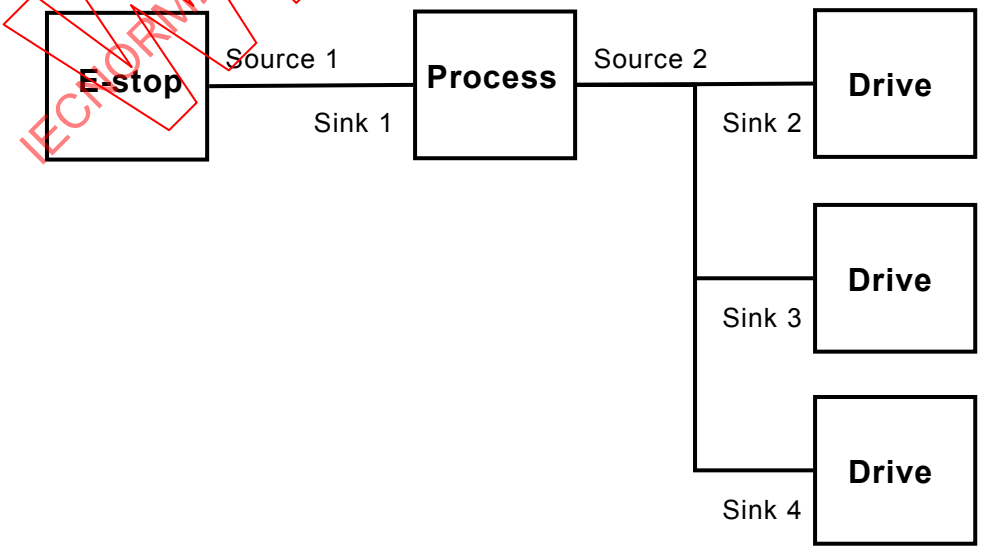



**Figure 6 – Example application**

### 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 future IEC 62443.

NOTE 2 Additional profile specific requirements may also be specified in the future IEC 61784-4.

## 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 certification) are specific to the functional safety communication profiles.

### 5.8.2 Electromagnetic compatibility (EMC)

IEC 61508 series 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 certificate).

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.

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 obtain the appropriate conformity assessment from the related technology-specific organization. This recommendation is included because incorrect implementations could lead to serious injury or loss of life.

NOTE 2 This standard would have made the above recommendation mandatory, except that IEC Directives (Ed.5) Part 2, 6.7, do not allow a standard to include such requirements.

# 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[5]) 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™[5]) 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 series.

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

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.

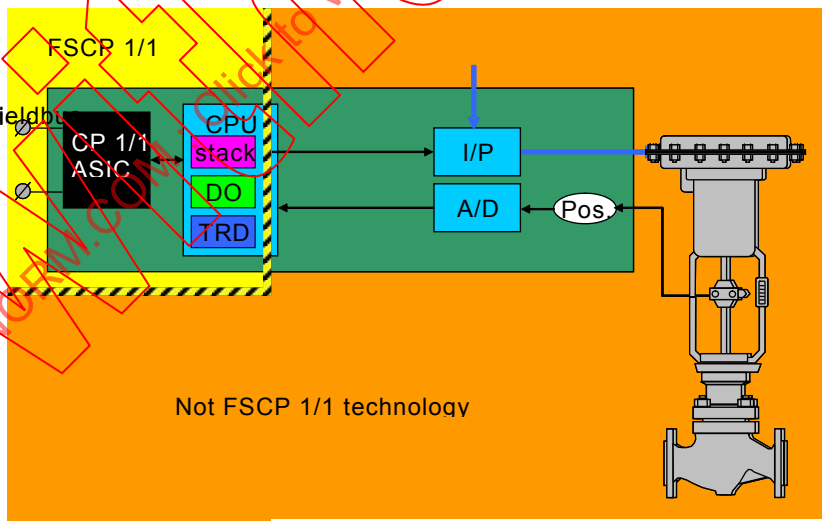



**Figure 7 – Scope of FSCP 1/1**

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 certification for the

5 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.

products, systems, and software. The user shall ascertain the suitability of use of all safety-related equipment in the safety function in accordance with IEC 61508 series.

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™[6]) 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™[6]) 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.

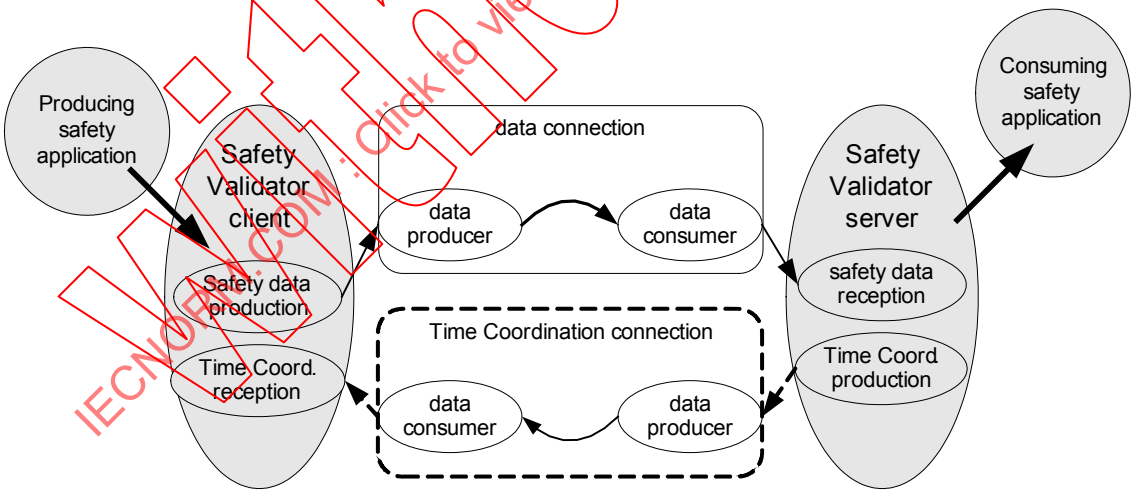



**Figure 8 – Relationship of Safety Validators**

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;

---

6 CIP™ (Common Industrial Protocol) and CIP Safety™ are trade names of the non-profit organization Open DeviceNet Vendor Association, Inc (ODVA). 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.

— 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™[7]) 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™[7]) 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.

---

7 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.

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.

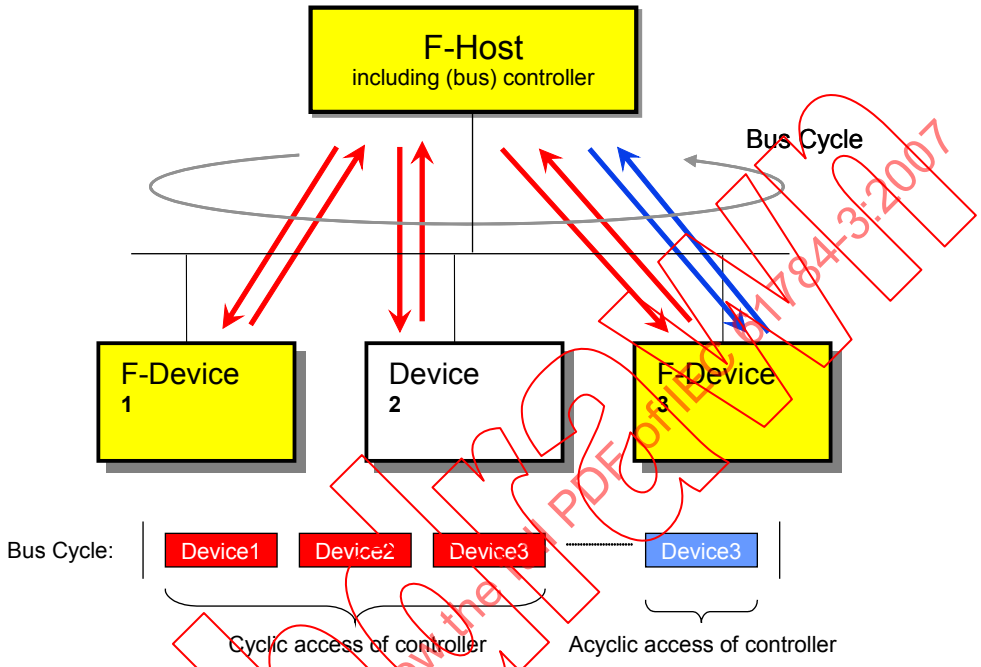



**Figure 9 – Basic communication preconditions for FSCP 3/1**

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).

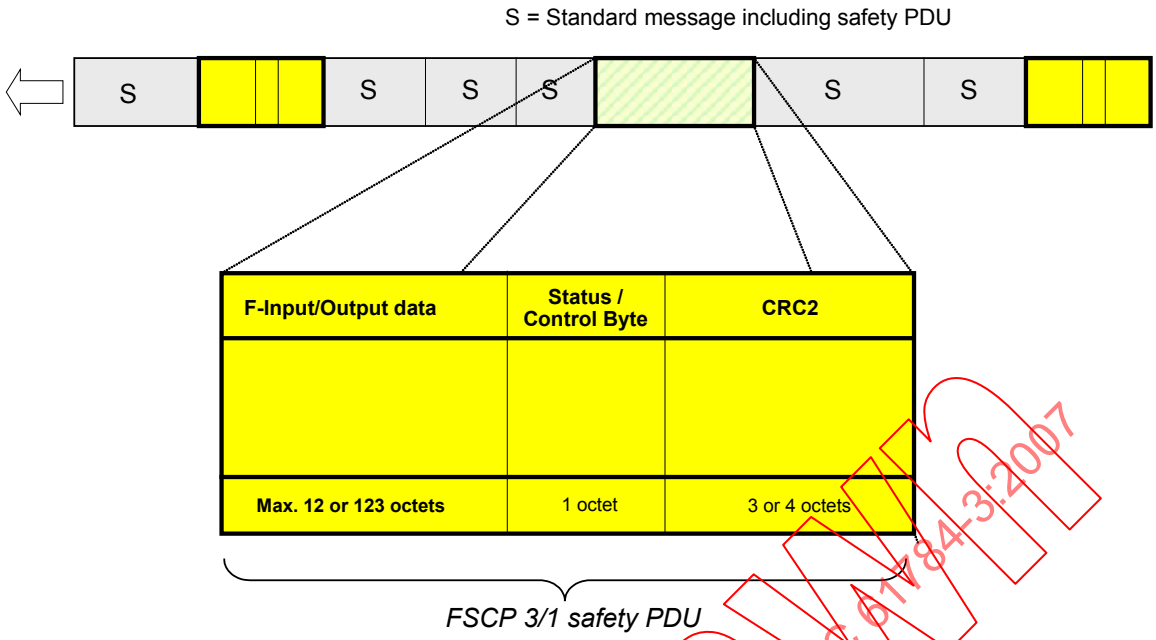



**Figure 10 – Structure of a FSCP 3/1 safety PDU**

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.

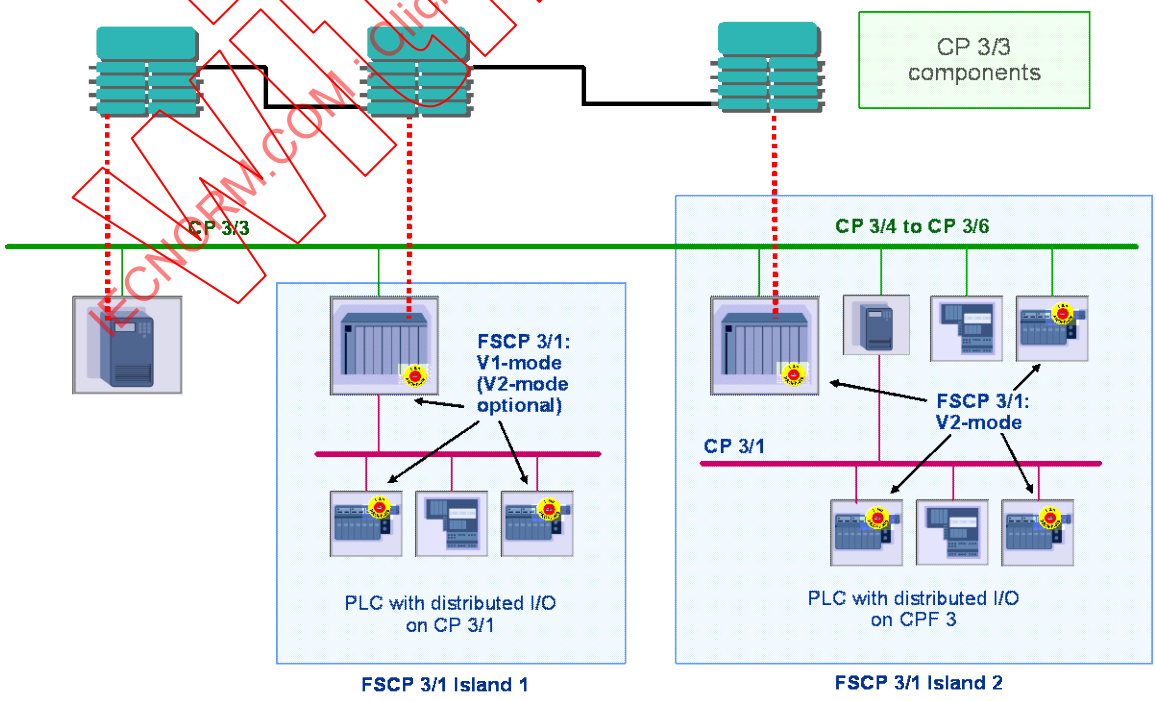



**Figure 11 – Safe communication modes**

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®[8]) 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™[8]) 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.

**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.



8 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.

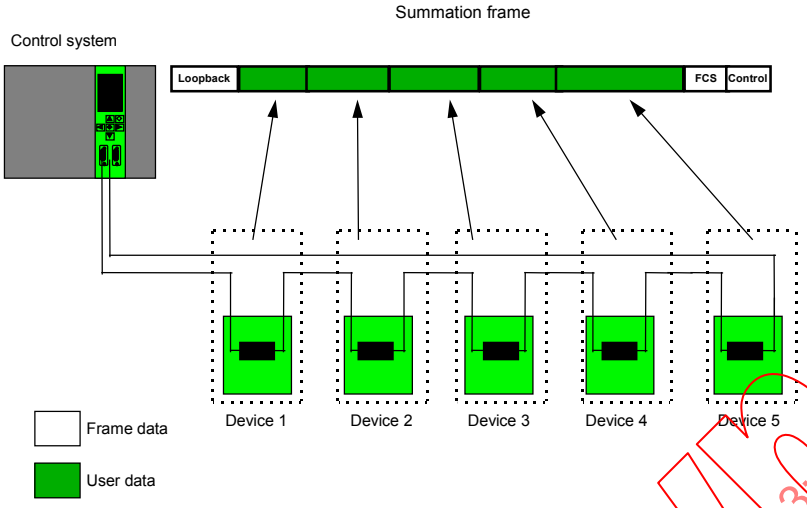



**Figure 12 – FSCP 6/7 communication preconditions**

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.

# 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 series 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.

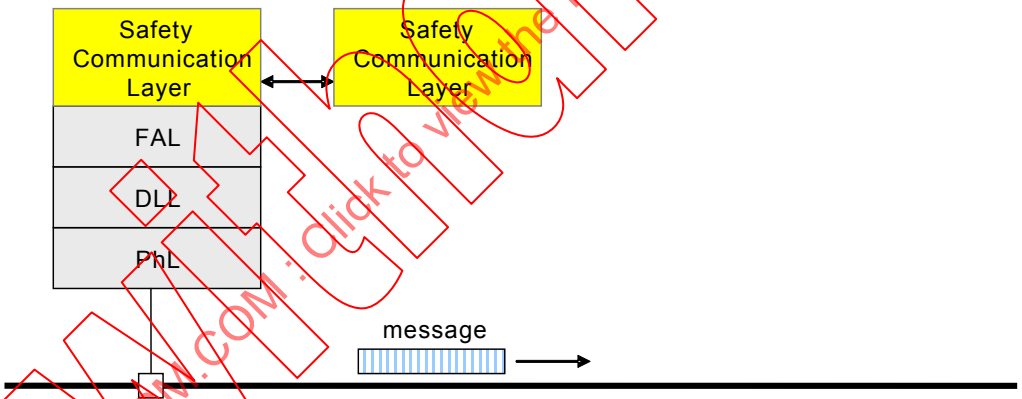



**Figure A.1 – Model A**



## 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.

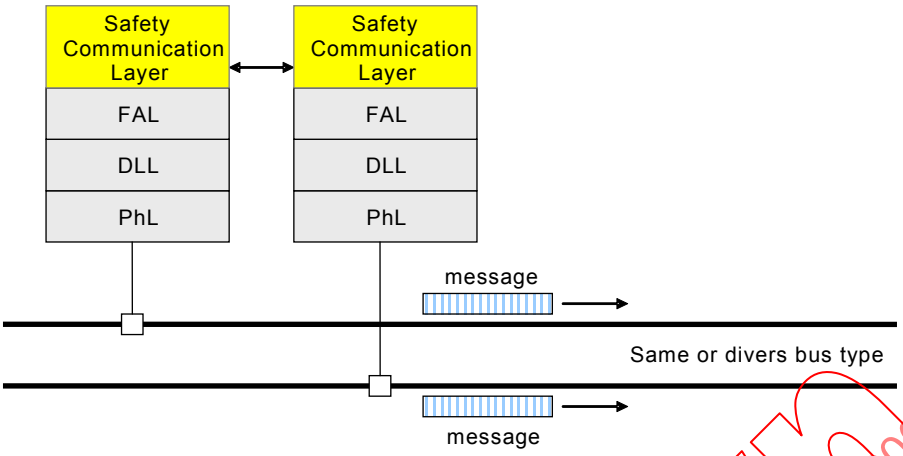



**Figure A.2 – Model B**

## 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.

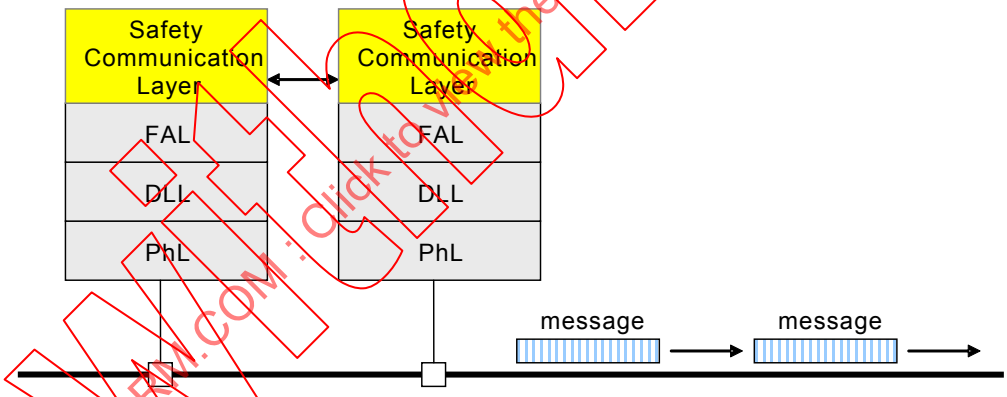



**Figure A.3 – Model C**



## 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.

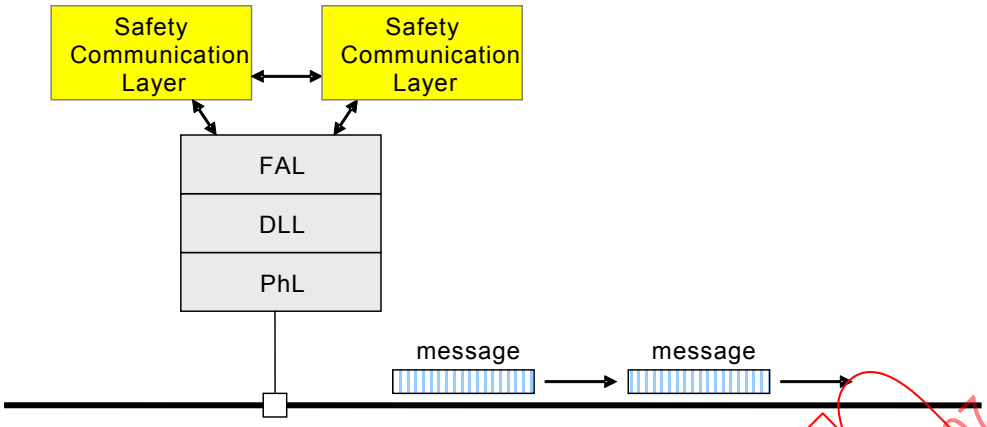



**Figure A.4 – Model D**

# 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 certification 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 formulas can be used for simplified assessments of residual error rates or as a basis for more sophisticated approaches.

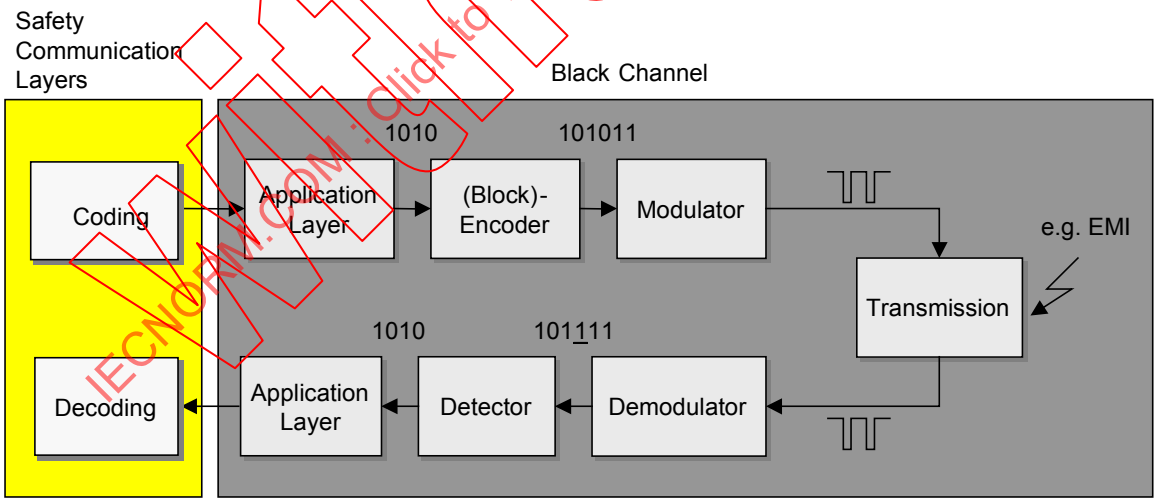



**Figure B.1 – Communication channel with perturbation**

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.

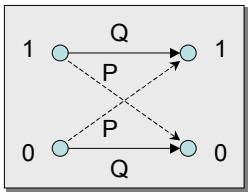



**Figure B.2 – Binary symmetric channel (BSC)**

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 formula (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 formula (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 formula 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 formula (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 formula to build an approximation (see formula (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 formula (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.

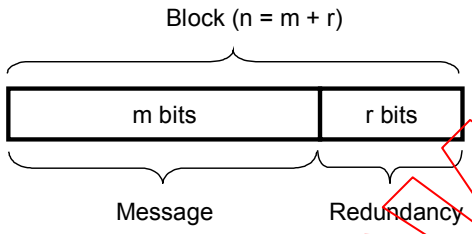



**Figure B.3 – Example of a block with message and CRC bits (redundancy code)**

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

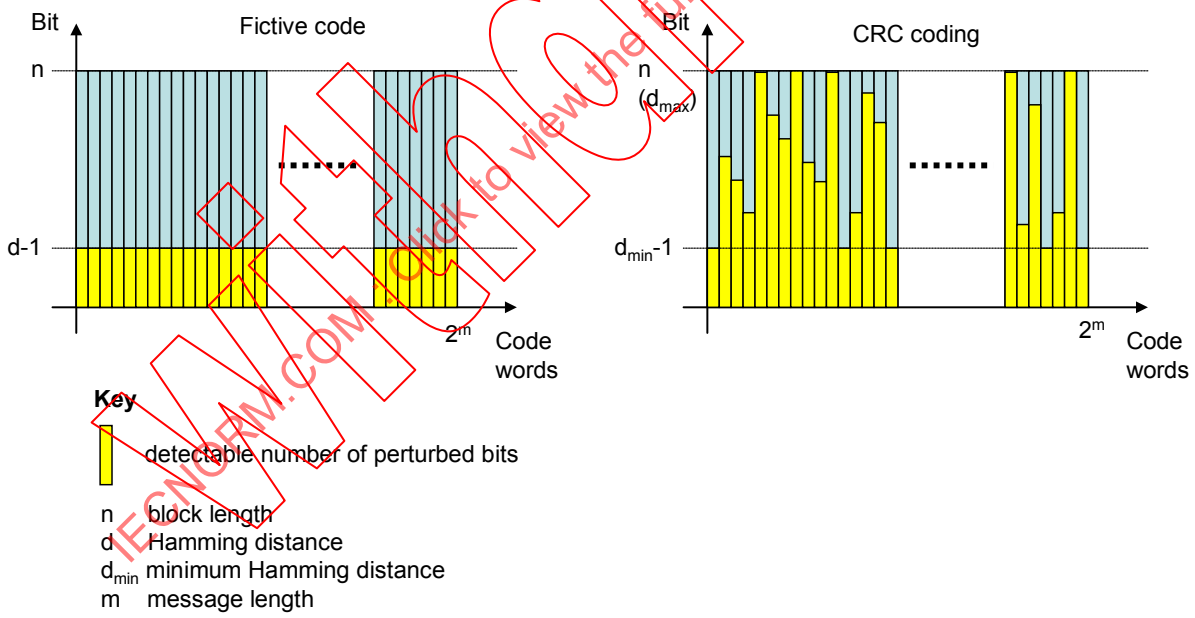



**Figure B.4 – Block codes for error detection**

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).

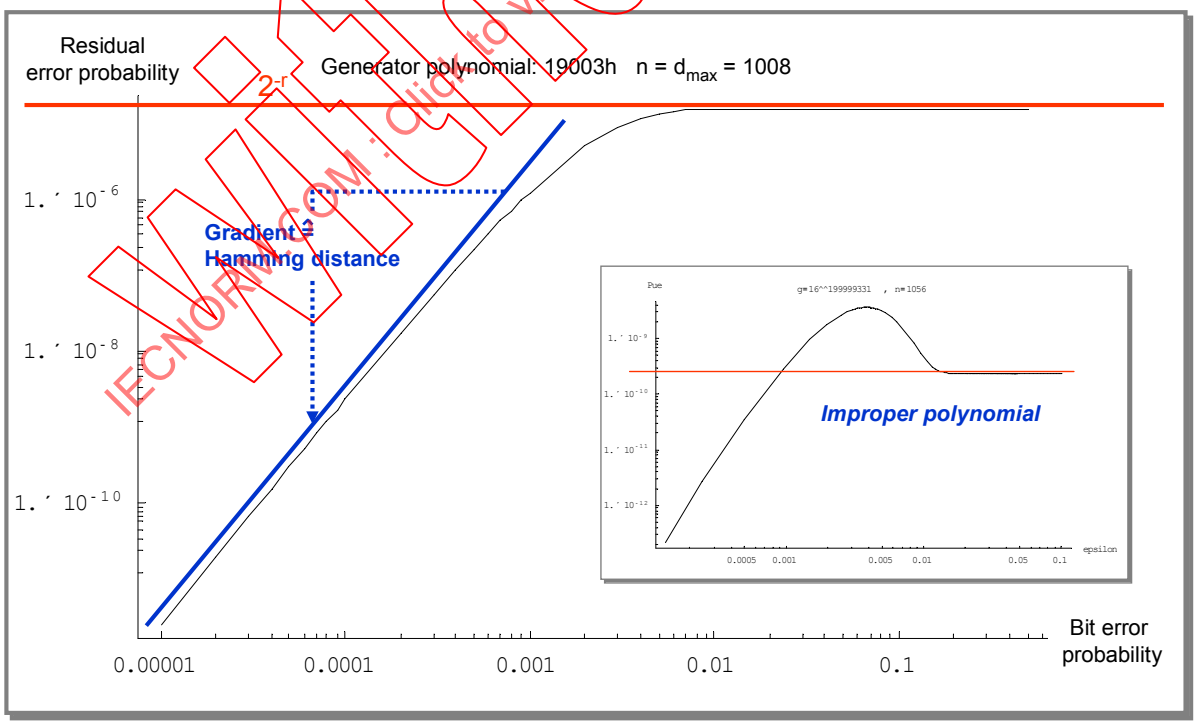
**Table B.1 – Example dependency $d_{min}$ and block length n**

| $d_{min}$ | $d_{max}$ = 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 [27], [33] and [34]. 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 61508-2:2000, 7.2.3) |
| 5.3 | Safety measures | May include measures to be considered from IEC 61784-3, 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 |

| Clause and subclause No. | Title | Contents |
|---|---|---|
| 6 | Safety communication layer services | May include application objects used, diagnostic services |
| 7 | Safety communication layer protocol | First subclause is listed below, others may be added as needed.<br>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.<br>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:<br>- safe parameter data supplied by another safety device (for example a parameter server)<br>- safe parameter data supplied by a tool (for example device description)<br>(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 | Certification | Include information on certification requirements |
| Annex A (informative) | Additional information for functional safety communication profiles of CPF X | Informative annexes may be used to provide additional non-normative information |
| A.1 | Hash function calculation | For example algorithms for CRC calculation |
| | Bibliography | Bibliographic references relevant for this part |

# Bibliography


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

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

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

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

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

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

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

[7] IEC 61784-4, *Industrial communication networks – Profiles – Part 4: Secure communications for fieldbuses*[9]

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

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

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

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

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

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

[14] IEC 62443, *Security for industrial process measurement and control – Network and system security*[9]

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

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

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

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

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

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

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

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

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




9 In preparation.

10 Under consideration.

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

[25] GS-ET-26; *Grundsatz für die Prüfung und Zertifizierung von Bussystemen für die Übertragung sicherheitsrelevanter Nachrichten*, May 2002. HVBG, Gustav-Heinemann-Ufer 130, D-50968 Köln ("*Principles for Test and Certification of Bus Systems for Safety relevant Communication*")[11]

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

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

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

[29] *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

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

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

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

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

[34] 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



[11] 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 COMMUNICATIONS 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.
9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de la CEI peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. La CEI ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et de ne pas avoir signalé leur existence.

La 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, et 6 donnés dans la CEI 61784-3-1, la CEI 61784-3-2, la CEI 61784-3-3 et la CEI 61784-3-6.

La CEI ne prend pas position quant à la preuve, à la validité et à la portée de ces droits de propriété. Le détenteur de ces droits de propriété a donné l'assurance à la CEI qu'il consent à négocier des licences avec des demandeurs du monde entier, à des termes et conditions raisonnables et non discriminatoires. A ce propos, la déclaration du détenteur des droits de propriété est enregistrée à la CEI.

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

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

La présente version bilingue (2012-12) correspond à la version anglaise monolingue publiée en 2007-12.

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

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

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

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

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

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

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

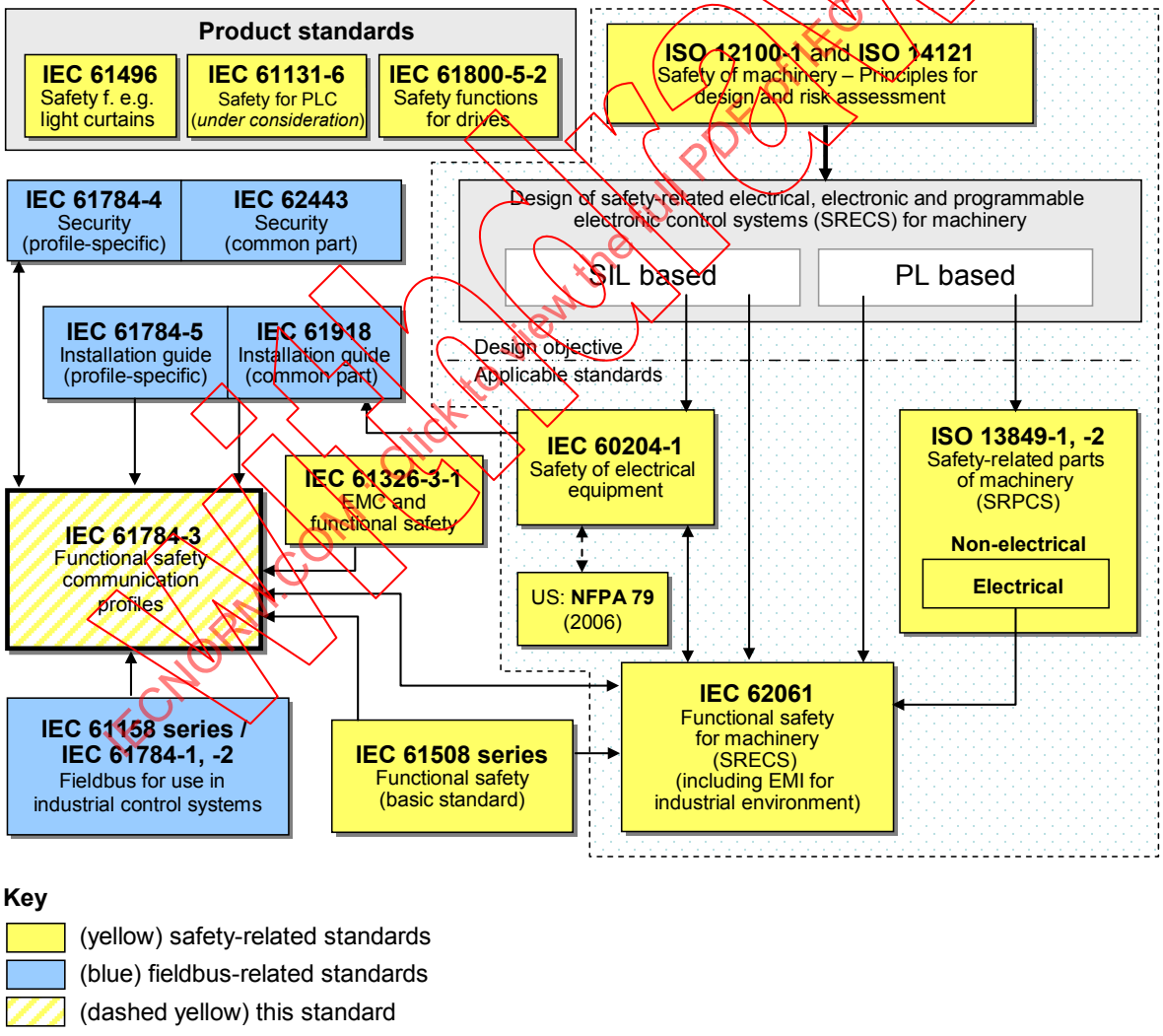
**IMPORTANT – Le logo "colour inside" qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une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

# INTRODUCTION

La 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.





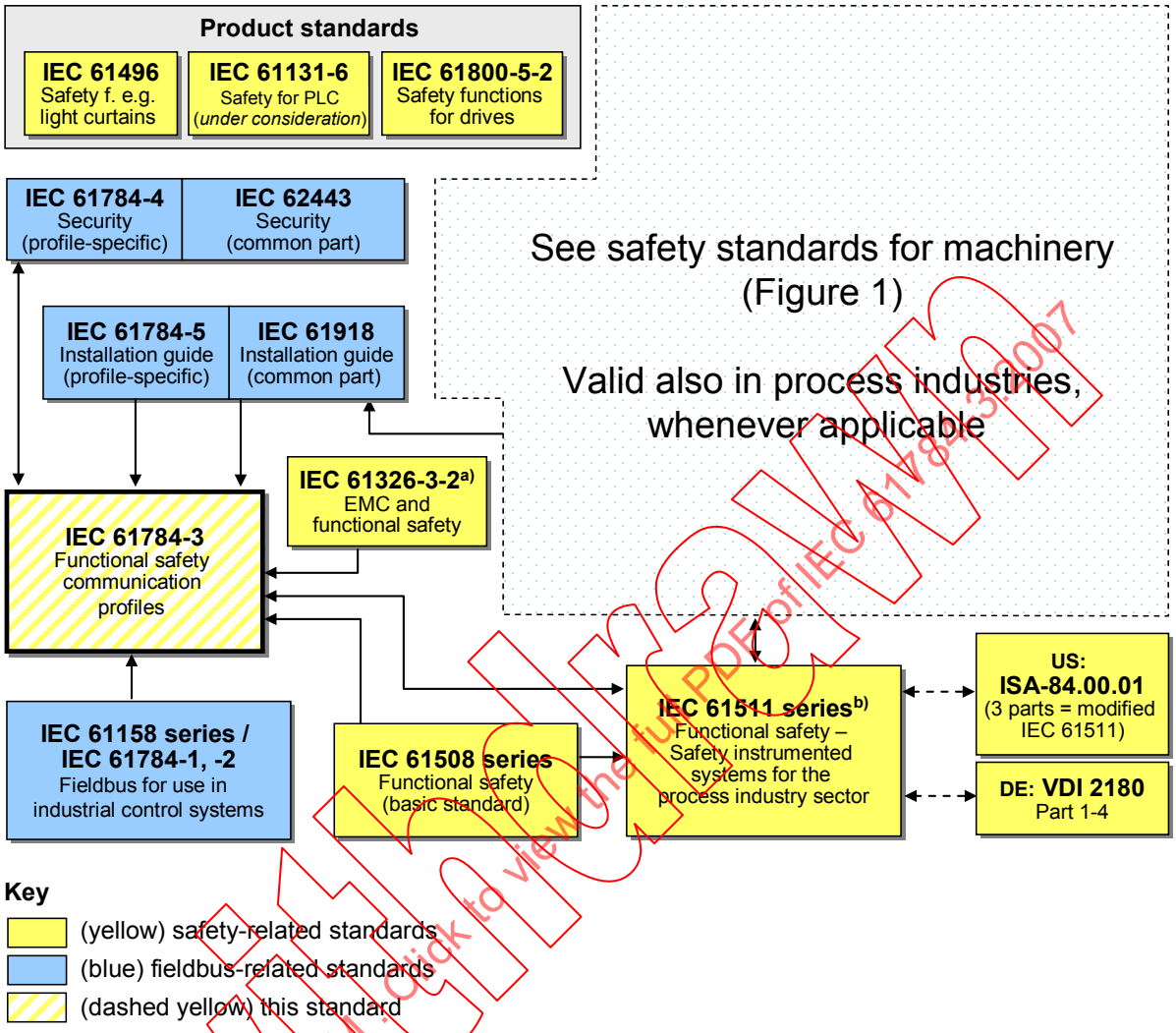

| Anglais | Français |
|---|---|
| Product standards | Normes de produits |
| Safety function, e.g. light curtains | Fonction de sécurité, par exemple barrières photo électriques |

| Anglais | Français |
|---|---|
| Safety for PLC (under consideration) | Sécurité relative aux automates programmables (à l'étude) |
| Safety functions for drives | Fonctions de sécurité applicables aux entraînements |
| Safety requirements for robots | Exigences de sécurité applicables aux robots |
| Safety of machinery - … 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 system (SRECS) for machinery | Conception des systèmes de commande électriques, électroniques et électroniques programmables relatifs à la sécurité pour les machines |
| SIL based | Basé sur SIL |
| PL based | Basé sur PL |
| Installation guide (profile-specific) | Guide d'installation (spécifique au profil) |
| Installation guide (common part) | Guide d'installation (partie commune) |
| Design objective | Objectif de conception |
| Applicable standards | Normes applicables |
| 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 |
| EMC and functional safety | Compatibilité électromagnétique et sécurité fonctionnelle |
| Functional safety communication profiles | Profils de communication de sécurité fonctionnelle |
| IEC 61158 series / Fieldbus for use in industrial control systems | Série CEI 61158 / Bus de terrain pour utilisation dans des systèmes de commande industriels |
| IEC 61508 series, Functional safety (basic standard) | Série CEI 61508, Sécurité fonctionnelle (norme de base) |
| Functional safety for machinery (SRECS) (including EMI for industrial environment) | Sécurité fonctionnelle des systèmes de commande électriques, électroniques et électroniques programmables (y compris les interférences électromagnétiques dans l'environnement industriel) |
| Key | Légende |
| (yellow) safety-related standards | (jaune) normes relatives à la sécurité |
| (blue) fieldbus-related standards | (bleu) normes relatives au bus de terrain |
| (dashed) yellow) this standard | (jaune pointillé) la présente norme |
| IEC | CEI |



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

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






| 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 |
| EMC and functional safety | CEM et sécurité fonctionnelle |

| Anglais | Français |
|---|---|
| IEC 61158 series Fieldbus for use in industrial control systems | Série CEI 61158, Bus de terrain pour utilisation dans des systèmes de commande industriels |
| IEC 61508 series, Functional safety (basic standard) | Série CEI 61508, Sécurité fonctionnelle (norme de base) |
| IEC 61511 series Functional safety – safety instrumented systems for the process industry sector | Série CEI 61511, Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur des industries de transformation |
| (3 parts = modified IEC 61511) | (3 parties = CEI 61511 modifiée) |
| Part 1 –4 | Parties 1 à 4 |
| Key | Légende |
| (yellow) safety-related standards | (jaune) normes relatives à la sécurité |
| (blue) fieldbus-related standards | (bleu) normes relatives au bus de terrain |
| (dashed) yellow) this standard | (jaune pointillé) la présente norme |
| IEC | CEI |

[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 industriels)**

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 la confiance nécessaire 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.

Les couches de communication de sécurité 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.

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

La présente norme décrit:

— les principes de base de la mise en œuvre des exigences de la 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 dans la CEI 61784-1 et la CEI 61784-2;

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

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

NOTE 1 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 nécessitent d'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 CEI 62443 traite bon nombre de ces questions; la relation avec la 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 future CEI 61784-4.

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

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

---

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

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*[2]

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*[2]

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

CEI 61508-1, *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*

IEC 61784-1, *Industrial communication networks – Profiles – Part 1: Fieldbus profiles* (disponible uniquement en anglais)

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

IEC 61784-3-1, *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 61784-5 (toutes les parties), *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*

## 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.

---

2 A publier.

### 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

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

**3.1.1.3**
**canal noir**
*canal de communication* sans preuve existante de conception ou de validation conformément à la série 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 (la couche d'application est définie dans l'ISO/CEI 7498)

**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 – *cyclic redundancy check*)**
<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 [26], [27][3].

**3.1.1.9**
**diversité**
moyens différents pour réaliser une fonction requise



---

3 Les chiffres entre crochets font référence à la bibliographie.

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

[CEI 61508-4:1998]

**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

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

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

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

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

**3.1.1.11**
**défaillance**
cessation de l'aptitude d'une unité fonctionnelle à accomplir une fonction requise

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

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

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

**3.1.1.12**
**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 61508-4:1998], [ISO/CEI 2382-14.01.10]

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

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

NOTE 2 Voir également [26], [27].

**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 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]

**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**
**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]

**3.1.1.25**
**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

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

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

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

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

**3.1.1.26**
**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]

**3.1.1.27**
**fiabilité**
probabilité qu'un système automatisé puisse accomplir une fonction requise, dans des conditions données, pendant un intervalle de temps donné (t1, t2)

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

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

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

NOTE 4 La fiabilité est différente de la disponibilité.

[CEI 62059-11, modifiée]

**3.1.1.28**
**risque**
combinaison de la probabilité d'occurrence d'un dommage ou d'un préjudice et de la gravité de ce dernier

[CEI 61508-4:1998]

**3.1.1.29**
**couche de communication de sécurité (SCL - *safety communication layer*)**
couche de communication qui comprend toutes les mesures nécessaires permettant d'assurer la transmission de données en toute sécurité conformément aux exigences de la CEI 61508

**3.1.1.30**
**connexion de sécurité**
connexion qui utilise le protocole de sécurité pour des transactions de communications

**3.1.1.31**
**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.

**3.1.1.32**
**dispositif de sécurité**
dispositif conçu conformément à la CEI 61508 et qui met en œuvre le profil de communication de sécurité fonctionnelle

**3.1.1.33**
**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]

**3.1.1.34**
**fonction de sécurité**
fonction à réaliser par un système E/E/PE relatif à la sécurité, par un *système relatif à la sécurité* basé sur une autre technologie, ou par un dispositif externe de réduction de risque, prévue pour assurer ou maintenir un état de sécurité de l'équipement commandé (EUC) par rapport à un événement dangereux spécifique

[CEI 61508-4:1998]

**3.1.1.35**
**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.

**3.1.1.36**
**niveau d'intégrité de sécurité (SIL - *safety integrity level*)**
niveau discret (parmi quatre possibles), permettant de spécifier les exigences concernant l'intégrité de sécurité des *fonctions de sécurité* à allouer aux systèmes E/E/PE relatifs à la sécurité. Le niveau d'intégrité de sécurité 4 est le niveau le plus élevé et le niveau 1 est le niveau de plus faible

NOTE Les mesures cibles des défaillances pour les quatre niveaux d'intégrité de sécurité sont indiquées dans les Tableaux 2 et 3 de la CEI 61508-1.

[CEI 61508-4:1998]

**3.1.1.37**
**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.

**3.1.1.38**
**application relative à la sécurité**
programmes conçus conformément à la CEI 61508 pour satisfaire aux exigences SIL de l'application

**3.1.1.39**
**système relatif à la sécurité**
système qui exécute les *fonctions de sécurité* conformément à la CEI 61508

**3.1.1.40**
**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

**3.1.1.41**
**déclenchement parasite**
déclenchement provoqué par le système de sécurité sans injonction du processus

**3.1.1.42**
**datation (horodatage)**
information temporelle incluse dans un *message*

**3.1.1.43**
**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.

## 3.2 Symboles et abréviations

### 3.2.1 Symboles et abréviations communs

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

### 3.2.2 CPF 1: Symboles et abréviations supplémentaires

| | |
|---|---|
| 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.

## 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 de la 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 61784-3:200x

ou

une conformité au FSCP n/m <Type> défini dans la CEI 61784-3 (Ed.1.0)

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:200x

ou

une conformité à la CEI 61784-3-N (Ed.1.0)

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

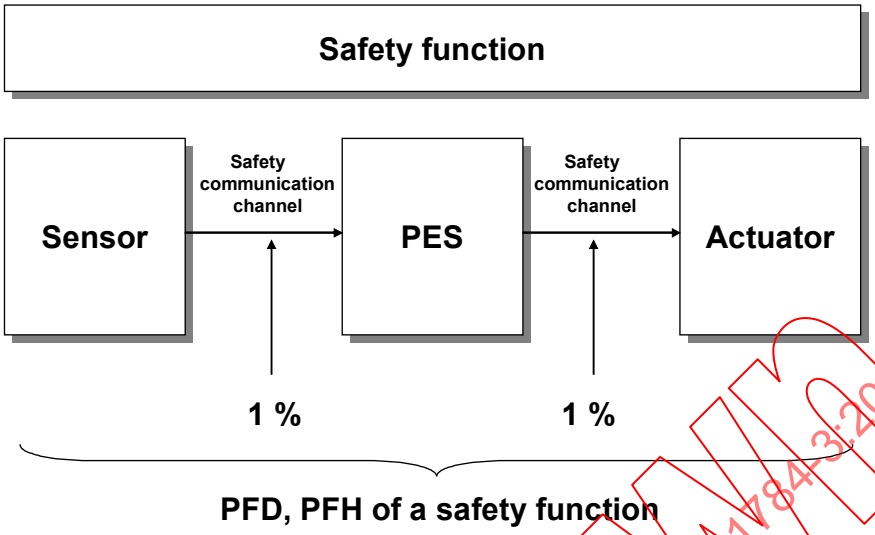
### 5.1 Décomposition des fonctions de sécurité

La CEI 61508 définit des 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 $PFH_{capteur} + PFH_{PES} + PFH_{actionneur} + 2 \times PFH_{canal\ de\ communication\ de\ sécurité}$.




**Légende**

| Anglais | Français |
|---|---|
| Safety function | Fonction de sécurité |
| sensor | Capteur |
| Safety communication channel | Canal de communication de sécurité |
| 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

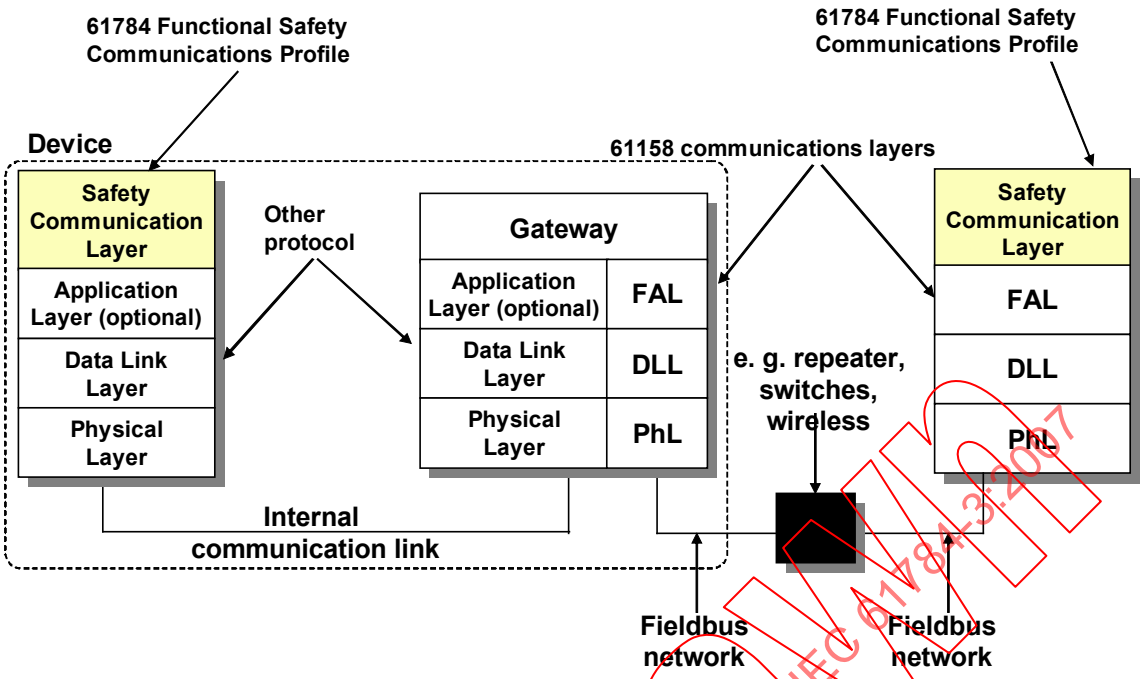
Les informations suivantes permettent une compréhension commune de la technologie et des termes employés.

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 [25].

### 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 de sécurité fonctionnelle 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 |
|---|---|
| Functional Safety Communication Profile | 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 |

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



### 5.2.3 Types de canaux de communication

La série CEI 61508[4] 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.

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).

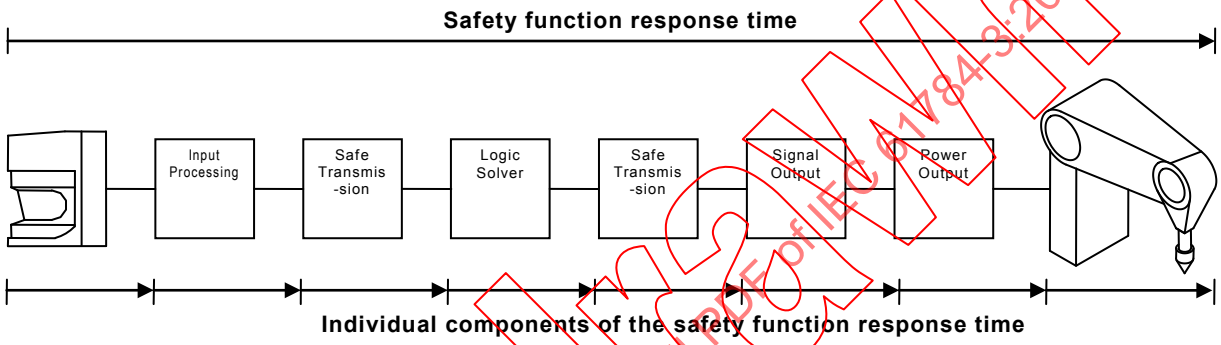
4 Deuxième édition en préparation.

### 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, ponts, 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, il est nécessaire d'envisager l'existence d'une erreur.

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 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 de 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 est tenu d'être traité par les couches de communication de sécurité.

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

EXEMPLE

Ce message de réaction renvoyé peut contenir uniquement un acquittement court, ou peut également contenir les données d'origine, qui permet à la source de vérifier la bonne réception par la comparaison des données transmises et des données reçues.

### 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 doit avoir 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.

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

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

| Erreurs de communication | Mesures de sécurité | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | Numéro de séquence | Datation (horodatage) | Délai | Authentification de connexion | Message de réaction | Assurance d'intégrité des données | Redondance avec contre-vérification | Différents systèmes d'assurance d'intégrité des données |
| Corruption (voir 5.3.2) | | | | | X | X | Uniquement pour un bus de série [d] | |
| 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 [c] | | | | | |
| Insertion (voir 5.3.7) | X | | | X [a,b] | X [a] | | X | |
| Mascarade (voir 5.3.8) | | | | X [a] | X [a] | | | X |
| Adressage (voir 5.3.9) | | | | X | | | | |

NOTE Tableau adapté de la CEI 62280-2 et [25].

[a] Dépend de l'application.

[b] Uniquement pour l'identification de l'émetteur. Détecte uniquement l'insertion d'une source invalide.

[c] Requis dans tous les cas.

[d] 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.



## 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'erreurs résiduelles 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 maximal de récepteurs d'informations (m) admis dans une fonction de sécurité simple.

La formule (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 la formule sont spécifiés dans le Tableau 2.

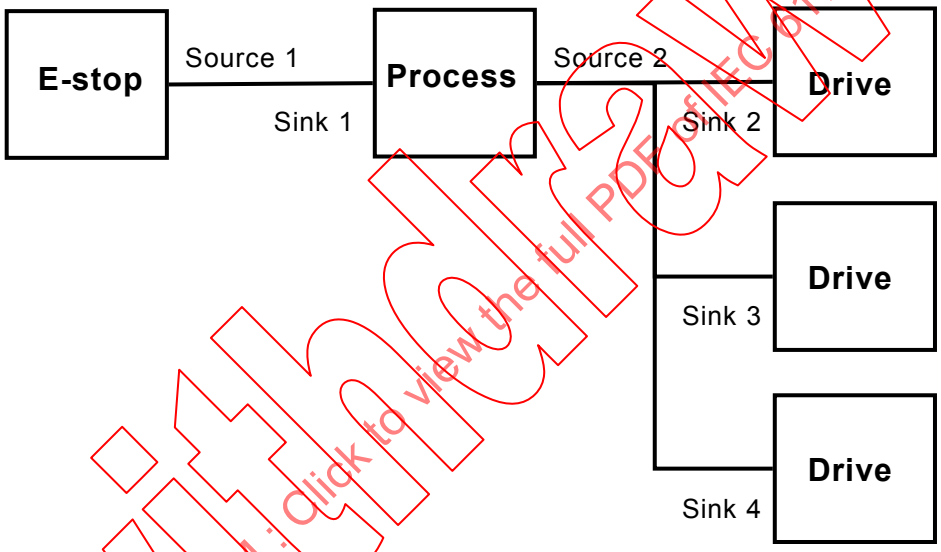
$$\Lambda_{SL}\,(Pe) = R_{SL}\,(Pe) \times v \times m \qquad (1)$$

NOTE 2 Cette formule 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 la formule | Définition |
|---|---|
| $\Lambda_{SL}$ (Pe) | Taux d'erreurs résiduelles par heure de la couche de communication de sécurité eu égard à la probabilité d'erreurs sur les bits |
| Pe | Probabilité d'erreurs sur les bits. Une valeur de $10^{-2}$ doit être utilisée à moins qu'une meilleure probabilité d'erreur puisse être démontrée |
| $R_{SL}$ (Pe) | Probabilité d'erreurs résiduelles d'un message de sécurité |
| v | Nombre maximal de messages de sécurité par heure |
| m | Nombre maximal de récepteurs d'informations admis dans une fonction de sécurité simple (voir Figure 6 ) |

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 sûreté 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 de mesures de sûreté appropriées telles que des mesures physiques (par exemple, mécaniques, électroniques) ou organisationnelles permet 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 future CEI 62443.

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

## 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, certification) sont spécifiques aux profils de communication de sécurité fonctionnelle.

### 5.8.2 Compatibilité électromagnétique (CEM)

La série 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 aux conditions préalables spécifiques de la CEI 61326-3-2.

NOTE Certaines applications peuvent exiger des niveaux plus élevés que ceux spécifiés dans la CEI 61326-3-1, 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 de nuisance), 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 standards) permettent une évaluation de conformité appropriée du protocole de bus de terrain pertinent (par exemple, déclaration du fabricant ou certificat fourni 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 à inclure dans le manuel de sécurité.

### 5.11 Politique de sécurité

Les utilisateurs de la présente norme doivent tenir compte des contraintes suivantes pour éviter tout malentendu, toutes fausses attentes 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, aux ateliers et aux 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.

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 ingénieurs d'application d'un profil spécifique obtiennent l'évaluation de conformité appropriée de l'organisation associée spécifique aux technologies. Cette recommandation est incluse dans la mesure où des mises en œuvre incorrectes pourraient provoquer des blessures graves, voire le décès d'individus.

NOTE 2 La présente norme aurait rendu obligatoire la recommandation ci-dessus, sauf que les Directives CEI (Ed.5) Parties 2, 6.7, ne permettent pas à une norme d'inclure ce type d'exigences.

# 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™ Fieldbus[5]) définit des profils de communication sur la base du type 1 de la CEI 61158-2, de la CEI 61158-3-1, de la CEI 61158-4-1, de la CEI 61158-5-5, de la CEI 61158-5-9, de la CEI 61158-6-5 et de 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™[5]) 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 série CEI 61508.

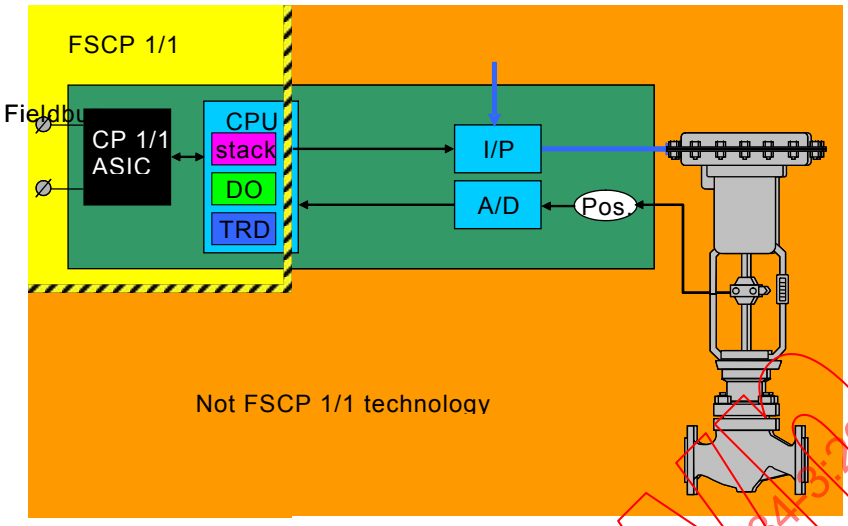
NOTE Ces applications relatives à la sécurité sont également appelées systèmes instrumentés de sécurité (SIS) (voir CEI 61511).

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.



5 FOUNDATION™ Fieldbus et FF-SIS™ désignent les appellations commerciales de l'organisme à but non lucratif Fieldbus Foundation. Ces informations sont données pour des raisons de commodité aux utilisateurs de la présente norme internationale et ne constituent en aucun cas un entérinement par la CEI du détenteur de la marque ou de l'un 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 |
| Stack | PILE |
| Not FSCP 1/1 technology | Technologie autre que technologie FSCP 1/1 |

**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 la certification de la sécurité fonctionnelle des produits, systèmes et logiciels. L'utilisateur doit déterminer l'aptitude à l'emploi de tous les matériels relatifs à la sécurité dans la fonction de sécurité conformément à la série CEI 61508.

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™[6]) définit des profils de communication sur la base du type 2 de la CEI 61158-2, de la CEI 61158-3-2, de la CEI 61158-4-2, de la CEI 61158-5-2 et de la CEI 61158-6-2.

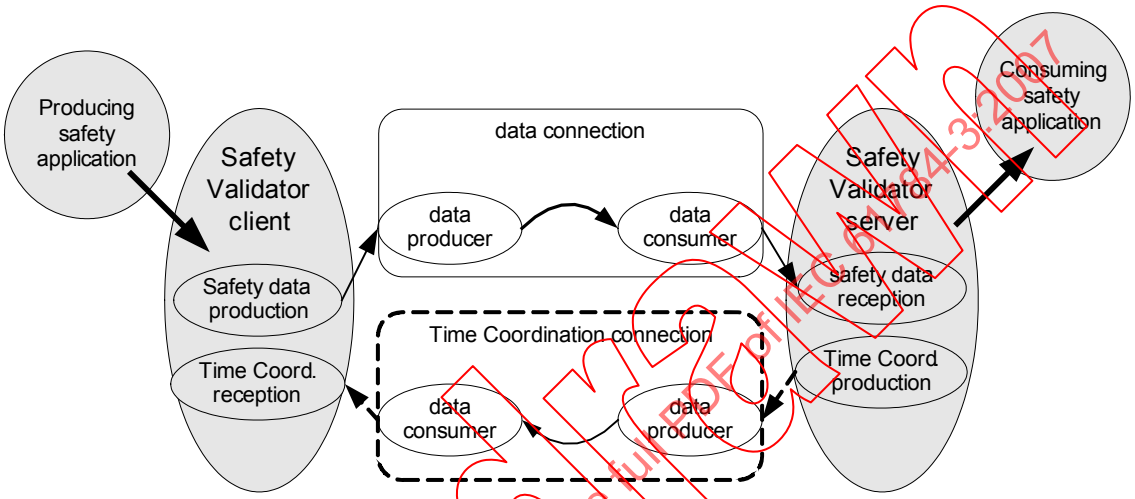
Les profils de base CP 2/1, CP 2/2 et CP 2/3 sont définis dans la CEI 61784-1 et la CEI 61784-2. Le profil de communication de sécurité fonctionnelle CPF 2 FSCP 2/1 (CIP Safety™[6]) est fondé sur les profils de base de CPF 2 définis dans la CEI 61784-1 et la CEI 61784-2, ainsi que les spécifications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

6 CIP™ (Common Industrial Protocol) et CIP Safety™ désignent les appellations commerciales de l'organisme à but non lucratif Open DeviceNet Vendor Association, Inc (ODVA). Ces informations sont données pour des raisons de commodité aux utilisateurs de la présente norme internationale et ne constituent en aucun cas un entérinement par la CEI du détenteur de la marque ou de l'un 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 de 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 de données |
| Time Coordination connection | Connexion 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 safety 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 standards 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™[7]) définit des profils de communication sur la base du type 3 de la CEI 61158-2, de la CEI 61158-3-3, de la CEI 61158-4-3, de la CEI 61158-5-3, de la CEI 61158-5-10, de la CEI 61158-6-3 et de 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™[7]) est fondé sur les profils de base de 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 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

---

7 PROFIBUS™, PROFINET™ et PROFIsafe™ désignent les appellations commerciales de l'organisme à but non lucratif PROFIBUS Nutzerorganisation e.V. (PNO). Ces informations sont données pour des raisons de commodité aux utilisateurs de la présente norme internationale et ne constituent en aucun cas un entérinement par la CEI du détenteur de la marque ou de l'un 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.