IEC 61784-3

Edition 3.1 2017-08
CONSOLIDATED VERSION

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

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

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

IEC 61784-3:2016-05+AMD1:2017-08 CSV(en-fr)

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

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

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

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

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

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 It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and also once a month by email.

Electropedia - www.electropedia.org
The world's leading online dictionary of electronic and electrical terms containing 20 000 terms and definitions in English and French, with equivalent terms in 16 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

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

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

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

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

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

Recherche de publications IEC - www.iec.ch/searchpub
La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études,…). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

IEC Just Published - webstore.iec.ch/justpublished
Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et aussi une fois par mois par email.

Electropedia - www.electropedia.org
Le premier dictionnaire en ligne de termes électroniques et électriques. Il contient 20 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans 16 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

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

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

IEC 61784-3

Edition 3.1 2017-08
CONSOLIDATED VERSION

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

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

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

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 25.040.40; 35.100.05

ISBN 978-2-8322-4712-9

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

IEC 61784-3

Edition 3.1 2017-08
CONSOLIDATED VERSION

REDLINE VERSION

VERSION REDLINE

colour inside

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

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

IEC 61784-3:2016-05+AMD1:2017-08 CSV(en-fr)

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES –

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

FOREWORD

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

This consolidated version of the official IEC Standard and its amendment has been prepared for user convenience.

IEC 61784-3 edition 3.1 contains the third edition (2016-05) [documents 65C/840/FDIS and 65C/848/RVD] and its amendment 1 (2017-08) [documents 65C/879/FDIS and 65C/886/RVD].

In this Redline version, a vertical line in the margin shows where the technical content is modified by amendment 1. Additions are in green text, deletions are in strikethrough red text. A separate Final version with all changes accepted is available in this publication.

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

This third edition constitutes a technical revision.

This edition includes the following significant technical changes with respect to the previous edition:

- clarifications and additional explanations for requirements, updated references;
- deletion of technical overviews of profiles (Clauses 6 to 13), and associated dedicated subclauses for terms, definitions, symbols and abbreviations;
- addition of profiles for Communication Profile Families 8, 17 and 18 (Clauses 10, 14, 15);
- clarifications of models in Annex A;
- Annex B changed from informative to normative;
- addition of a new informative Annex E describing models for explicit and implicit FSCP mechanisms;
- addition of a new informative Annex F introducing an extended model for estimation of the total residual error rate;
- updates in parts for CPF 1, CPF 2, CPF 3, CPF 8, CPF 13 (details provided in the parts);
- addition of a new part for CPF 17.

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

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

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

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

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

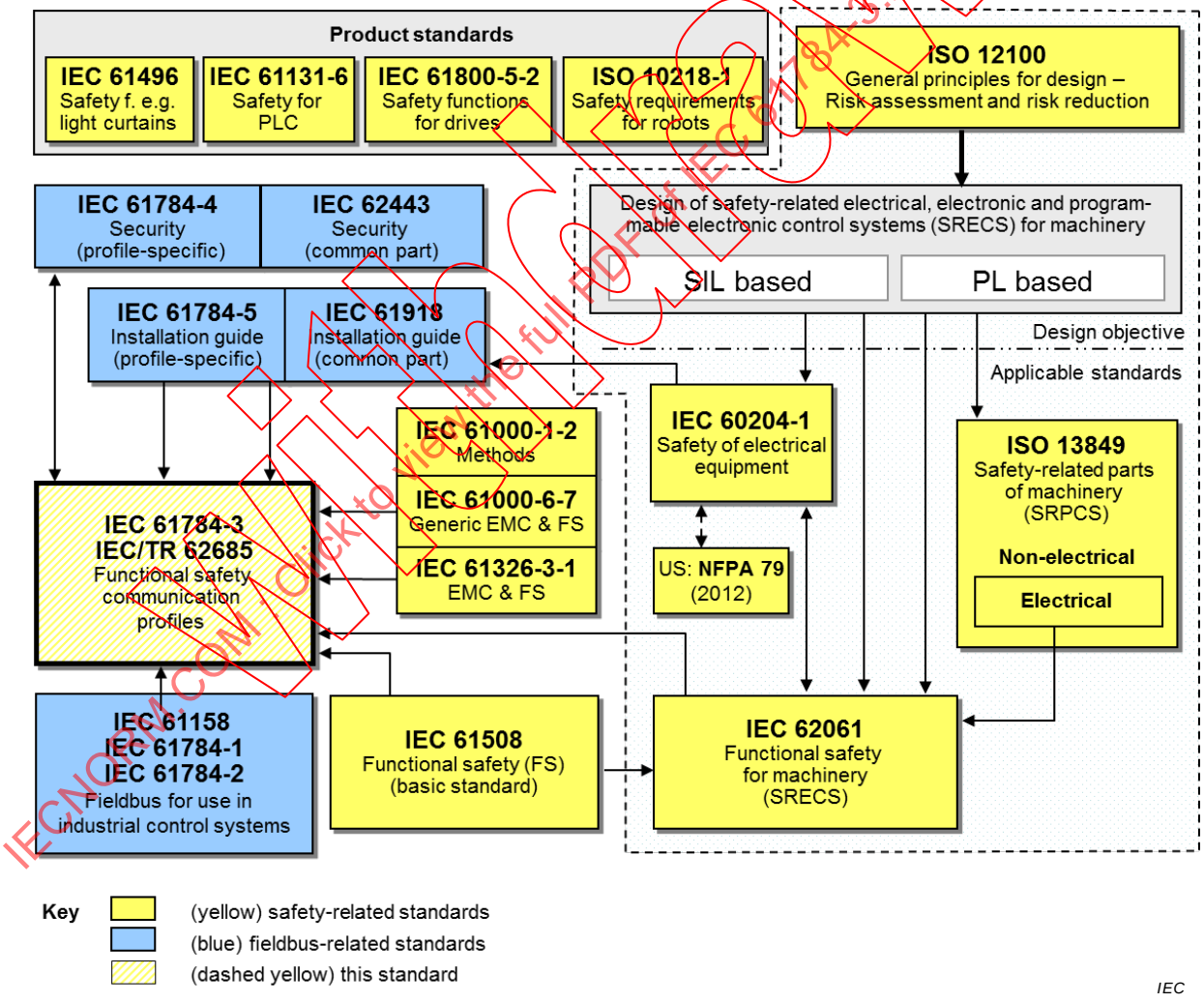
0 Introduction

0.1 General

The IEC 61158 fieldbus standard together with its companion standards IEC 61784-1 and IEC 61784-2 defines a set of communication protocols that enable distributed control of automation applications. Fieldbus technology is now considered well accepted and well proven. Thus fieldbus enhancements continue to emerge, addressing applications for areas such as real time, safety-related and security-related applications.

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

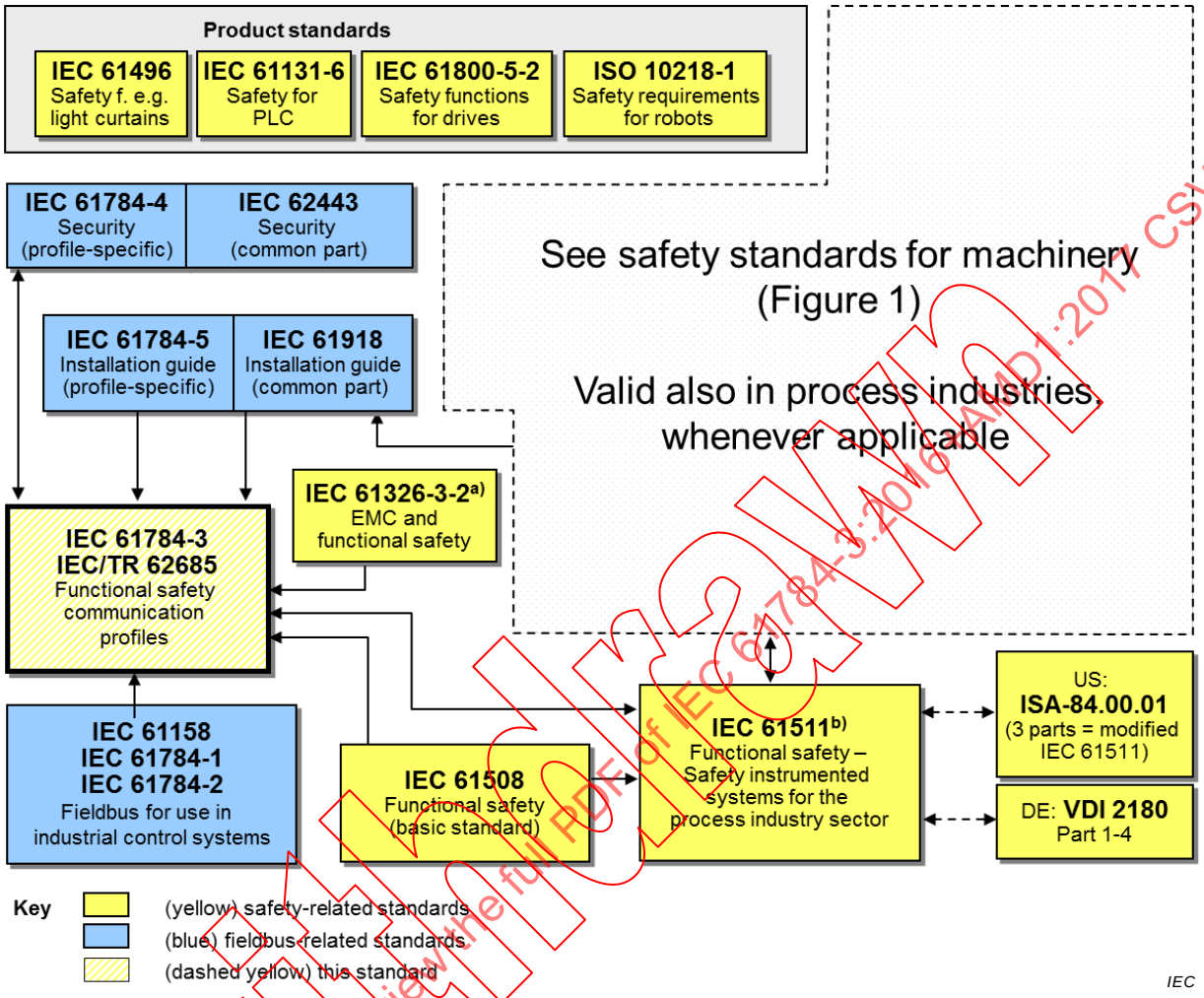
Figure 1 shows the relationships between this standard and relevant safety and fieldbus standards in a machinery environment.



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

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

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



[a] For specified electromagnetic environments; otherwise IEC 61326-3-1 or IEC 61000-6-7.

[b] EN ratified.

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

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

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

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

This standard describes:

- basic principles for implementing the requirements of IEC 61508 series for safety-related data communications, including possible transmission faults, remedial measures and considerations affecting data integrity;
- functional safety communication profiles for several communication profile families in IEC 61784-1 and IEC 61784-2, including safety layer extensions to the communication service and protocols sections of the IEC 61158 series.

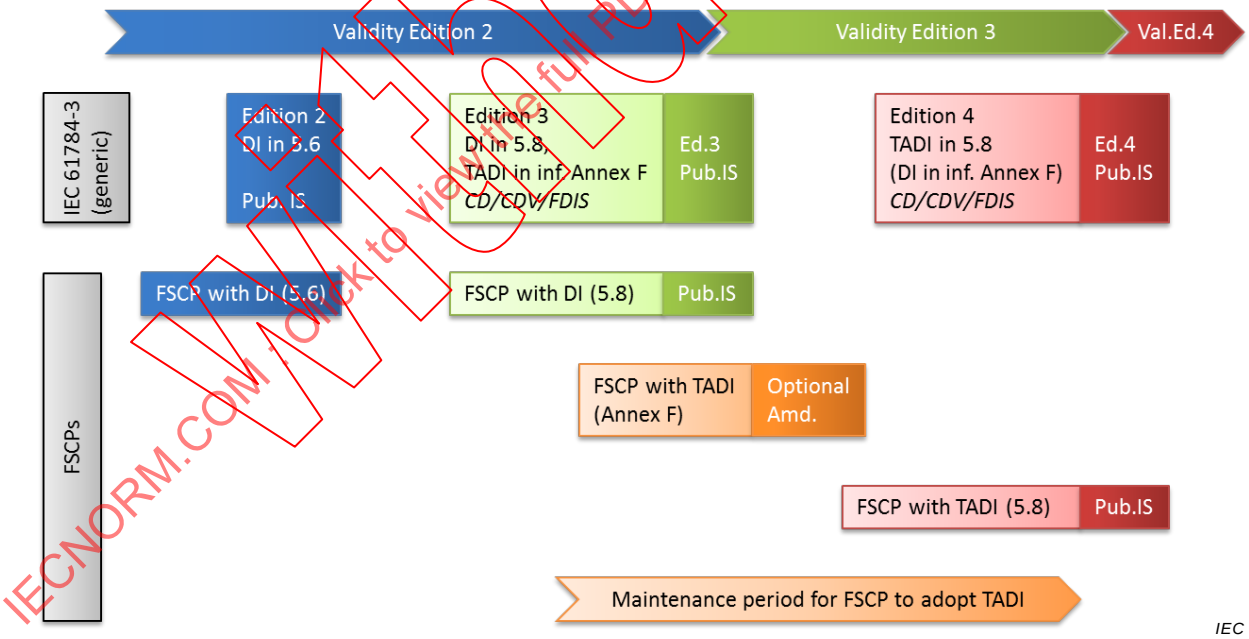
0.2 Transition from Edition 2 to extended assessment methods in Edition 3

This edition of the generic part of the standard includes additional extended models for future use when estimating the total residual error rate for an FSCP. This value can be used to determine if the FSCP meets the requirements of functional safety applications up to a given SIL. These extended models for qualitative and quantitative safety determination methods are detailed in Annex E and Annex F.

However, because of the typical duration of the assessment process, the FSCPs published prior to or concurrently with this new edition of the generic part can only be assessed using the methods from previous editions, based on data integrity considerations specified in 5.8.

The validity schema in Figure 3 shows how to handle the transition from original assessment methods of Edition 2 (specified in 5.8) to extended assessment methods in Edition 3 (currently specified in Annex F). According to this schema, the FSCPs are exempt from a new assessment according to Annex F until Edition 4, where the contents of current Annex F will replace the current 5.8.

NOTE However, a particular FSCP can achieve an earlier assessment and publish an adequate amendment.



Key

DI Data Integrity

TADI Timeliness, Authenticity, Data Integrity

Figure 3 – Transition from Edition 2 to Edition 3 assessment methods

0.3 Patent declaration

The International Electrotechnical Commission (IEC) draws attention to the fact that it is claimed that compliance with this document may involve the use of patents concerning functional safety communication profiles for families 1, 2, 3, 6, 8, 12, 13, 14, 17 and 18 given in IEC 61784-3-1, IEC 61784-3-2, IEC 61784-3-3, IEC 61784-3-6, IEC 61784-3-8, IEC 61784-3-12, IEC 61784-3-13, IEC 61784-3-14, IEC 61784-3-17 and IEC 61784-3-18.

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

NOTE Patent details and corresponding contact information are provided in IEC 61784-3-1, IEC 61784-3-2, IEC 61784-3-3, IEC 61784-3-6, IEC 61784-3-8, IEC 61784-3-12, IEC 61784-3-13, IEC 61784-3-14, IEC 61784-3-17 and IEC 61784-3-18.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights other than those identified above. IEC shall not be held responsible for identifying any or all such patent rights.

ISO (www.iso.org/patents) and IEC (http://patents.iec.ch) maintain on-line data bases of patents relevant to their standards. Users are encouraged to consult the data bases for the most up to date information concerning patents.

INTRODUCTION to the Amendment

This Amendment 1 discusses the concepts of implicit data safety mechanisms for use in functional safety communications protocols (FSCPs) as specified in IEC 61784-3:2016.

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 that can be used in the transmission of safety-relevant messages among participants within a distributed network which use fieldbus technology in accordance with the requirements of IEC 61508 series[1] for functional safety. These principles are based on the black channel approach. They can be used in various industrial applications such as process control, manufacturing automation and machinery.

This part[2] and the IEC 61784-3-x parts specify several functional safety communication profiles based on the communication profiles and protocol layers of the fieldbus technologies in IEC 61784-1, IEC 61784-2 and the IEC 61158 series. These functional safety communication profiles use the black channel approach, as defined in IEC 61508. These functional safety communication profiles are intended for implementation in safety devices exclusively.

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

NOTE 2 It does not cover electrical safety and intrinsic safety aspects. Electrical safety relates to hazards such as electrical shock. Intrinsic safety relates to hazards associated with potentially explosive atmospheres.

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

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

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

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

---

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

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

3 Proposed new work item under consideration.

IEC 61010-2-201:2013, *Safety requirements for electrical equipment for measurement, control and laboratory use – Part 2-201: Particular requirements for control equipment*

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*

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

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

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

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

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

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

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

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

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

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

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

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

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

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

IEC 61784-3-17[4], *Industrial communication networks – Profiles – Part 3-17: Functional safety fieldbuses – Additional specifications for CPF 17*

IEC 61784-3-18, *Industrial communication networks – Profiles – Part 3-18: Functional safety fieldbuses – Additional specifications for CPF 18*

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

IEC 61918:2013, *Industrial communication networks – Installation of communication networks in industrial premises*

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

3 Terms, definitions, symbols, abbreviated terms and conventions

3.1 Terms and definitions

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

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

3.1.1
absolute time stamp
time stamp referenced to a global time which is common for a group of devices using a *fieldbus*

[SOURCE: IEC 62280:2014, 3.1.1, modified – use devices and fieldbus]

3.1.2
active network element
network element containing electrically and/or optically active components that allows extension of the network

Note 1 to entry: Examples of active network elements are repeaters and switches.

[SOURCE: IEC 61918:2013, 3.1.2]

3.1.3
availability
probability for an automated system that for a given period of time there are no unsatisfactory system conditions such as loss of production

3.1.4
bit error probability
Pe
probability for a given bit to be received with the incorrect value

3.1.5
black channel
defined communication system containing one or more elements without evidence of design or validation according to IEC 61508

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

4 To be published

3.1.6
bridge
abstract device that connects multiple network segments along the data link layer

3.1.7
closed communication system
fixed number or fixed maximum number of participants linked by a communication system with well-known and fixed properties, and where the risk of unauthorized access is considered negligible

[SOURCE: IEC 62280:2014, 3.1.6, modified – transmission replaced by communication]

3.1.8
communication channel
logical connection between two end-points within a *communication system*

3.1.9
communication system
arrangement of hardware, software and propagation media to allow the transfer of *messages* (ISO/IEC 7498-1 application layer) from one application to another

3.1.10
connection
logical binding between two application objects within the same or different devices

3.1.11
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 to entry: 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 to entry: See also [28], [29][5].

3.1.12
defined communication system
defined channel
fixed number or fixed maximum number of participants linked by a fieldbus based communication system with well-known and fixed properties, such as installation conditions, electromagnetic immunity, industrial (active) network elements, and where the risk of unauthorized access is reduced to a tolerated level according to the lifecycle model of IEC 62443, using for example zones and conduits

3.1.13
diversity
different means of performing a required function

Note 1 to entry: Diversity may be achieved by different physical methods or different design approaches.

[SOURCE: IEC 61508-4:2010, 3.3.7]

5 Figures in square brackets refer to the bibliography.

3.1.14
error
discrepancy between a computed, observed or measured value or condition and the true, specified or theoretically correct value or condition

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

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

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

3.1.15
explicit code
code for safety measure that is actually transmitted within the SPDU and is known to the sender and receiver

3.1.16
failure
termination of the ability of a functional unit to perform a required function or operation of a functional unit in any way other than as required

Note 1 to entry: Failure may be due to an *error* (for example, problem with hardware/software design or message disruption).

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

3.1.17
fault
abnormal condition that may cause a reduction in, or loss of, the capability of a functional unit to perform a required function

Note 1 to entry: IEC 60050-191:1990, 191-05-01 defines "fault" as a state characterized by the inability to perform a required function, excluding the inability during preventive maintenance or other planned actions, or due to lack of external resources.

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

3.1.18
fieldbus
communication system based on serial data transfer and used in industrial automation or process control applications

3.1.19
fieldbus system
system using a *fieldbus* with connected devices

3.1.20
DLPDU
DEPRECATED: frame
Data Link Protocol Data Unit

3.1.21
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 to entry: An FCS can be derived using for example a CRC or other hash function.

Note 2 to entry: See also [28], [29].

Note 3 to entry: This note applies to the French language only.

3.1.22
hash function
(mathematical) function that maps values from a (possibly very) large set of values into a (usually) smaller range of values

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

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

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

3.1.23
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

3.1.24
implicit code
code for safety measure that is not transmitted within the SPDU but is known to the sender and receiver

3.1.25
master
active communication entity able to initiate and schedule communication activities by other stations which may be masters or slaves

3.1.26
message
ordered series of octets intended to convey information

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

3.1.27
message sink
part of a *communication system* in which *messages* are considered to be received

[SOURCE: ISO/IEC 2382-16:1996, 16.02.03]

3.1.28
message source
part of a *communication system* from which *messages* are considered to originate

[SOURCE: ISO/IEC 2382-16:1996, 16.02.02]

3.1.29
nuisance trip
spurious trip with no harmful effect

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

3.1.30
performance level
PL
discrete level used to specify the ability of safety-related parts of control systems to perform a safety function under foreseeable conditions

[SOURCE: ISO 13849-1:2015, 3.1.23]

3.1.31
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 1 to entry: A PELV circuit incorporates a connection to protective earth. Without the protective earth connection or if there is a fault in the protective earth connection, the circuit voltages are not controlled.

[SOURCE: IEC 61010-2-201:2013, 3.109, modified – deletion of "circuit" from term, and deletion of second note to entry]

3.1.32
redundancy
existence of more than one means for performing a required function or for representing information

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

3.1.33
relative time stamp
time stamp referenced to the local clock of an entity

Note 1 to entry: In general, there is no relationship to clocks of other entities.

[SOURCE: IEC 62280:2014, 3.1.43]

3.1.34
reliability
probability that an automated system can perform a required function under given conditions for a given time interval (t1,t2)

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

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

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

Note 4 to entry: Reliability differs from availability.

[SOURCE: IEC TR 62059-11:2002, 3.17, modified – use of "automated system" instead of "item" and addition of two notes]

3.1.35
residual error probability
RP
probability of an error undetected by the SCL safety measures

Note 1 to entry: This note applies to the French language only.

3.1.36
residual error rate
statistical rate at which the SCL safety measures fail to detect errors

3.1.37
risk
combination of the probability of occurrence of harm and the severity of that harm

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

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

3.1.38
safety communication channel
SC
communication channel starting at the top of the SCL of the source and ending at the top of the SCL of the sink

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

3.1.39
safety communication layer
SCL
communication layer above the FAL that includes all necessary additional measures to ensure safe transmission of data in accordance with the requirements of IEC 61508

Note 1 to entry: This note applies to the French language only.

3.1.40
safety connection
connection that utilizes the safety protocol for communications transactions

3.1.41
safety data
data transmitted across a safety network using a safety protocol

Note 1 to entry: The Safety Communication Layer does not ensure safety of the data itself, only that the data is transmitted safely.

3.1.42
safety device
device designed in accordance with IEC 61508 and which implements the functional safety communication profile

3.1.43
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

[SOURCE: IEC 61010-2-201:2013, 3.110, modified – deletion of "circuit" from term, and deletion of note to entry]

3.1.44
safety function
function to be implemented by an E/E/PE safety-related system or other risk reduction measures, that is intended to achieve or maintain a safe state for the EUC, in respect of a specific hazardous event

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

3.1.45
safety function response time
worst case elapsed time following an actuation of a safety sensor connected to a fieldbus, until the corresponding safe state of its safety actuator(s) is achieved in the presence of errors or failures in the safety function

Note 1 to entry: This concept is introduced in 5.2.4 and addressed by the functional safety communication profiles defined in this part.

3.1.46
safety integrity level
SIL
discrete level (one out of a possible four), corresponding to a range of safety integrity values, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest

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

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

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

Note 4 to entry: This note applies to the French language only.

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

3.1.47
safety measure
measure to control possible communication *errors* that is designed and implemented in compliance with the requirements of IEC 61508

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

Note 2 to entry: Communication *errors* and related safety measures are detailed in 5.3 and 5.4.

3.1.48
safety PDU
SPDU
PDU transferred through the safety communication channel

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

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

Note 3 to entry: This note applies to the French language only.

3.1.49
safety-related application
programs designed in accordance with IEC 61508 to meet the SIL requirements of the application

3.1.50
safety-related system
system performing *safety functions* according to IEC 61508

3.1.51
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

3.1.52
spurious trip
trip caused by the safety system without a process demand

3.1.53
time stamp
time information included in a *message*

3.1.54
uniform distribution
probability distribution where all values from a finite set are equally likely to occur

Note 1 to entry: For a field of bit length i the probability of occurrence of a particular field value is 2^{-i} since the sum of all probabilities of occurrence is equal to 1.

3.1.55
white channel
defined communication system in which all relevant hardware and software elements are designed, implemented and validated according to IEC 61508

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

3.1.56
explicit data
data that is transmitted

3.1.57
implicit data
additional data that is not transmitted but is known to the sender and receiver

[SOURCE: IEC 62280:2014, 3.1.25]

3.2 Symbols and abbreviated terms

3.2.1 Abbreviated terms

A-code	Authenticity code	
BSC	Binary Symmetric Channel	
CP	Communication Profile	[IEC 61784-1]
CPF	Communication Profile Family	[IEC 61784-1]
CRC	Cyclic Redundancy Check	
DLL	Data Link Layer	[ISO/IEC 7498-1]
DLPDU	Data Link Protocol Data Unit	
EMC	Electromagnetic Compatibility	
EMI	Electromagnetic Interference	
EUC	Equipment Under Control	[IEC 61508-4:2010]
E/E/PE	Electrical/Electronic/Programmable Electronic	[IEC 61508-4:2010]
FAL	Fieldbus Application Layer	[IEC 61158-5]
FCS	Frame Check Sequence	

FIT	Failure In Time (equals 10^{-9} failure per hour)	
FS	Functional Safety	
FSCP	Functional Safety Communication Profile	
IACS	Industrial Automation and Control System	
MTBF	Mean Time Between Failures	
MTTF	Mean Time To Failure	
NSR	Non Safety Related	
PDU	Protocol Data Unit	[ISO/IEC 7498-1]
~~Pe~~	~~Bit error probability~~	
PELV	Protective Extra Low Voltage	
PES	Programmable Electronic System	[IEC 61508-4:2010]
PFD_{avg}	Average probability of dangerous Failure on Demand	[IEC 61508-4:2010]
PFH	Average frequency of dangerous failure [h^{-1}] per hour	[IEC 61508-4:2010]
PhL	Physical Layer	[ISO/IEC 7498-1]
PL	Performance Level	[ISO 13849-1]
PLC	Programmable Logic Controller	
~~RP~~	~~Residual Error Probability~~	
SCL	Safety Communication Layer	
SELV	Safety Extra Low Voltage	
SIS	Safety Instrumented Systems	
SL	Security Level	[IEC 62443]
SMS	Security Management System	[IEC 62443]
SPDU	Safety PDU	
SR	Safety Related	
T-code	Timeliness code	

3.2.2 Symbols

A_k	Weight distribution of the code: number of valid codewords having k bits set to “one”
e	Bit length of explicit data
err_{impl}	Bitwise disjunction of $impl_S$ and $impl_R$
expl	Explicit data
$expl_R$	Explicit data in the receiver
$expl_S$	Explicit data in the sender
FCS_C	Frame check sequence calculated in the receiver
FCS_R	Frame check sequence received
FCS_S	Frame check sequence sent
i	Bit length of implicit data
ID	Incorrect delivery
$impl_R$	Implicit data in the receiver
$impl_S$	Implicit data in the sender
n	Bit length of SPDU
P_e	Bit error probability
P_{ID}	Probability of incorrect delivery

r Bit length of FCS (degree of generator polynomial)

RP Residual error probability

4 Conformance

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

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

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

or

conformance to IEC 61784-3 (Ed.3.0) FSCP n/m <Type>

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

Alternatively, a statement of conformance may be stated as either

conformance to IEC 61784-3-N:20xx

or

conformance to IEC 61784-3-N (Ed.3.0)

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

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

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

5 Basics of safety-related fieldbus systems

5.1 Safety function decomposition

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

The communication system itself in this standard performs transmission of safety data. To simplify system calculations, it is recommended that one logical connection of safety communication channels of a safety function does not consume more than 1 % of the maximum PFH or PFD_{avg} of the target SIL for which the functional safety communication profile is designed (see Figure 4 and 5.8.2).

If this value of 1 % for one logical connection cannot be guaranteed by a given FSCP, the safety manual for this FSCP shall provide additional guidance on the calculations of the PFH or PFD_{avg}.

The overall PFH and PFD_{avg} of each safety device shall incorporate the PFH and PFD_{avg} of the logical connection. The PFD_{avg} shall be provided if the FSCP is also used for low demand mode applications according to IEC 61508.

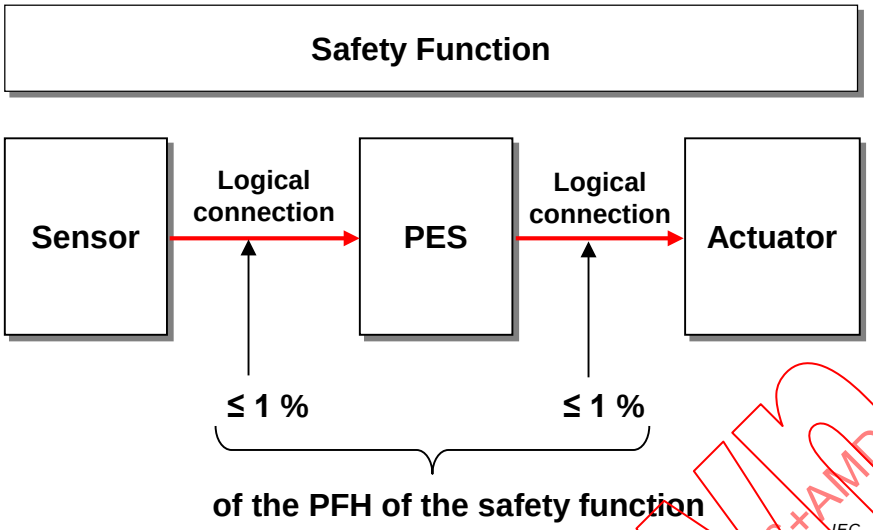


Figure 4 – Safety communication as a part of a safety function

Alternatively, the PFH / PFD_{avg} of the communication can be calculated for the whole safety function. In this case, the PFH / PFD_{avg} of the safety communication needs to be considered only once.

5.2 Communication system

5.2.1 General

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

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 5 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 5.

The safety communication layer includes suitable services and protocol to encode safety data into safety PDUs and pass them to the black channel and to receive safety PDUs from the black channel and decode them to extract safety data.

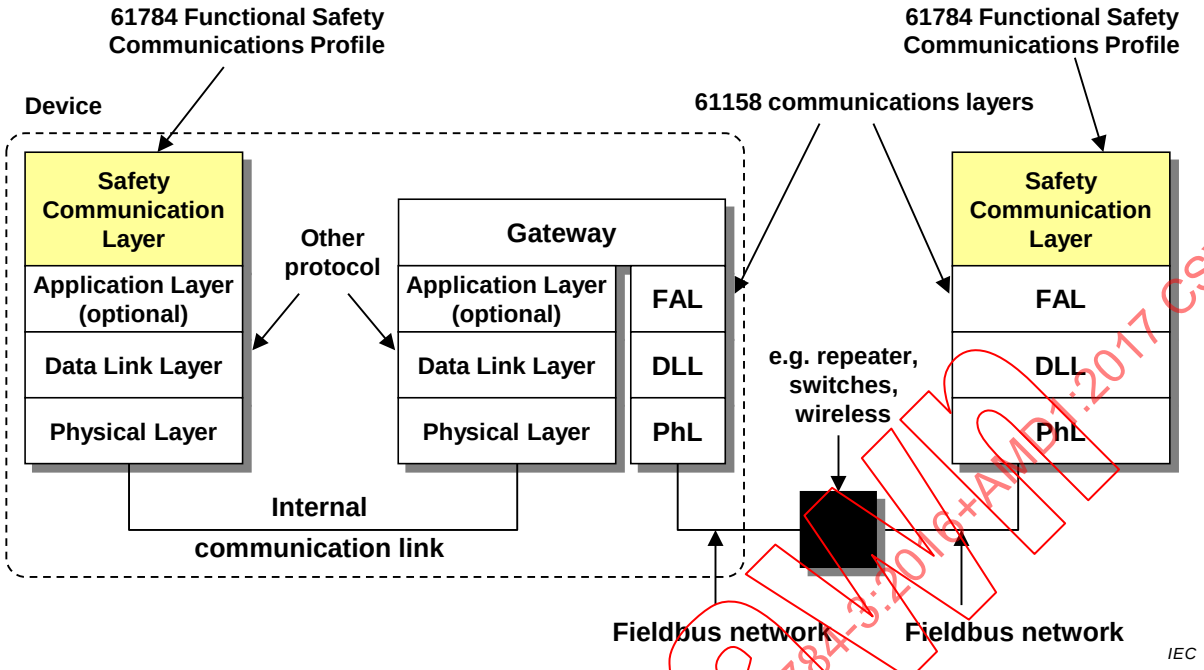


Figure 5 – Example model of a functional safety communication system

While implementation of the Fieldbus Application Layer (FAL) is required for functional safety communication systems according to this standard, the Application Layer may be omitted for communication links internal to a device (for example with a gateway).

Functions that are not safety-related may bypass the SCL and access the FAL directly.

5.2.3 Communication channel types

IEC 61508 uses the concepts of the so called “black channel” or “white channel” to define the requirements of the base fieldbus for transmission of safety data. This standard specifies functional safety communication profiles that use the black channel approach.

In this context, a safety communication channel is defined to start at the top of the safety communication layer of the source and stop at the top of the safety communication layer of the sink (see Figure 5). The black channel includes everything between the safety communication layers.

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, until 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.

Calculation of the safety function response time is specified in the profile specific parts of IEC 61784-3.

Empirical measurements may only serve as a plausibility check of the worst case calculation.

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

Figure 6 shows an example of typical components making up a safety function response time.

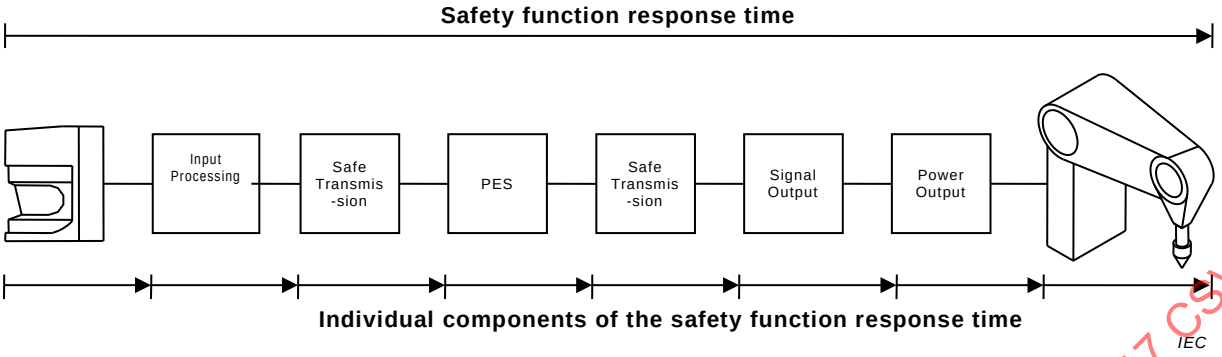


Figure 6 – Example of safety function response time components

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

Subclauses 5.3.2 to 5.3.9 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 will 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 can 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, messages are repeated.

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.

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 This “incorrect sequence” error is also referred to as “out-of-sequence” error.

NOTE 2 Fieldbus systems can contain elements that store messages (for example FIFOs in switches, bridges, routers) or use protocols that can alter the sequence (for example by allowing messages with high priority to overtake those with lower priority).

NOTE 3 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 can be reported for each sequence.

5.3.5 Loss

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

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)..

5.3.7 Insertion

Due to a fault or interference, a message is received 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 related message may be received by a safety related participant, which then treats it as safety related.

NOTE Communication systems used for safety-related applications can 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 related message is delivered to the incorrect safety related participant, which then treats reception as correct. This includes the so-called loopback error case, where the sender receives back its own sent message.

5.4 Deterministic remedial measures

5.4.1 General

Subclauses 5.4.2 to 5.4.9 list 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 Relative time stamps and absolute time stamps can be used.

Time stamping requires the time base to be synchronized. For safety applications, synchronization shall be regularly monitored, and the probability of this mechanism failing shall be included in the assessment of the overall safety function.

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 sends 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 related participant.

5.4.6 Feedback message

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

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

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

5.4.7 Data integrity assurance

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

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

If a hash function is used, it shall not include error correction mechanisms.

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 related (SR) and non-safety related (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.

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

5.5 Typical 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. Typical relationships are shown in Table 1, actual relationships shall be specified by each FSCP. Each safety measure can provide protection against one or more errors in the transmission. It shall be demonstrated that there is at least one corresponding safety measure or combination of safety measures for the defined possible errors in accordance with Table 1.

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

A safety measure shall only be listed in the corresponding table for a given FSCP if this measure takes effect before the guaranteed fieldbus safety response time.

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

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

NOTE Table adapted from IEC 62280:2014, Table 1.

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

[b] Required in all cases.

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

[d] Effective only if feedback message includes original data or information about the original data, and if the receiver only acts on the data after acknowledge of the feedback message.

[e] Effective only if the sequence numbers or time stamps of the source entities are different.

5.6 Communication phases

An FSCP shall be designed so that either a safe state or a sufficient residual error rate at the receiver side can be achieved according to IEC 61508 within each and every communication phase of the safety network, including:

- setup or change of the safety network (configuration and parameterization);
- start-up with initialization (e.g. connection establishment);
- operation (safety data exchange);
- warm-start after transition from a fault;
- shutdown.

Figure 7 shows a conceptual FSCP protocol model. An FSCP shall not return directly to correct FSCP communication after a fault, but first go through warm start or new initialization phases, depending on the FSCP.

NOTE In case of faults, the FSCP can take care of application requirements such as an operator acknowledge prior to a machine start.

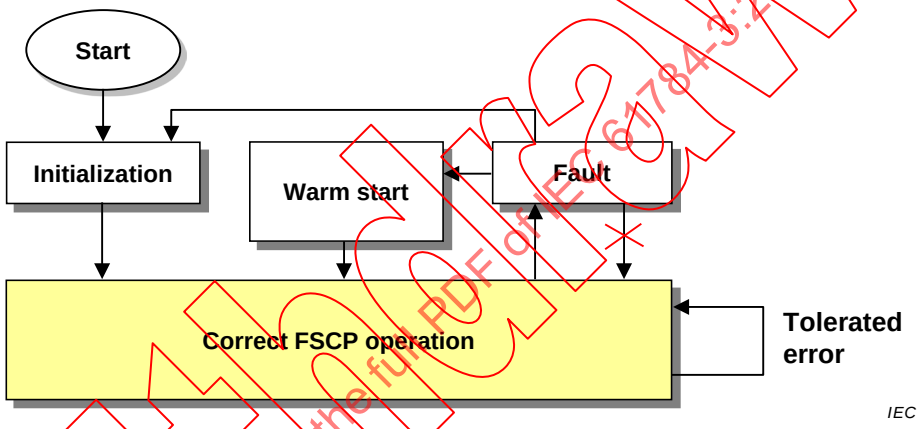


Figure 7 – Conceptual FSCP protocol model

5.7 FSCP implementation aspects

All FSCP technical measures shall be implemented within the SCL in devices designed in accordance with IEC 61508 and shall meet the target SIL.

Some protocol measures depend on the manner they are implemented in a particular safety device. Figure 8 shows the separation between FSCP implementation aspects and its deterministic and probabilistic aspects.

An example of an implementation aspect is a dependency on the failure rate of real-time clocks, watchdogs or microcontrollers. These aspects require quantitative safety assessments according to IEC 61508 to determine their relevance to the individual considerations of generic safety properties.

This standard does not consider implementation aspects, except when an implementation aspect is required by an FSCP and that aspect can affect the FSCPs residual error rate. Generic safety properties are considered based on logical connections between SCL end-points (using only basic assumptions on the black channel performance as stated in the safety manuals of the individual FSCPs).

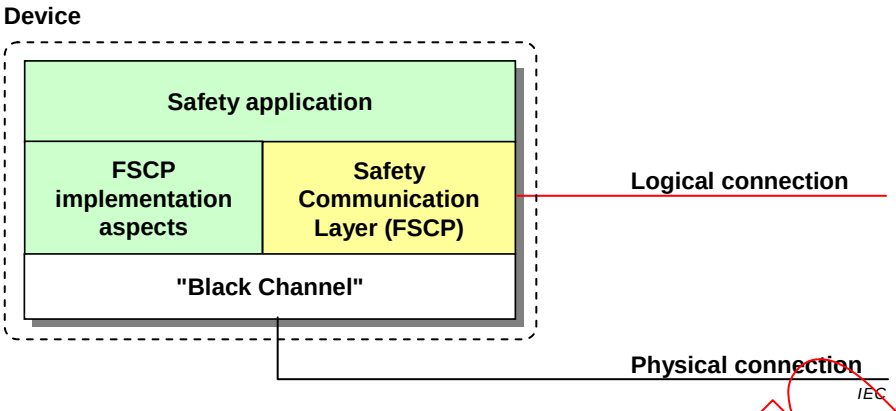


Figure 8 – FSCP implementation aspects

5.8 Data integrity considerations

5.8.1 Calculation of the residual error rate

Even when the messages are arriving in a correct (deterministic) manner the SPDU 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 fieldbus DLL shall not use the same hash function as the superimposed safety communication layer unless special care is taken for those cases. The safety code shall be functionally independent from the transmission code.

EXAMPLE When CRC is used as the hash function, the fieldbus DLL 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 sample rate of SPDUs. In case of calculation of PFH / PFD_{avg} per safety function, one shall take into account for the assessment the maximum number of information sinks (m) that is permitted in a single safety function.

Equations (1) and (2) shown below shall be used to calculate the residual error rates resulting from R_{SC} (Pe), unless the underlying model does not apply, or if another method may be more relevant. Items of the equations are specified in Table 2.

$$\lambda_{SC}(Pe) = R_{SC}(Pe) \times v \quad (1)$$

$$\lambda_{SCL}(Pe) = \lambda_{SC}(Pe) \times m \quad (2)$$

NOTE These equations assume cyclic sampling of SPDUs by the SCL.

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

Equation items	Definition
λ_{SC} (Pe)	Residual error rate per hour of the safety communication channel with respect to the bit error probability (see 3.1.36)
λ_{SCL} (Pe)	Residual error rate per hour of the safety communication layer with respect to the bit error probability (see 3.1.36)
Pe	Bit error probability (see Clause B.3)
R_{SC} (Pe)	Residual error probability of the safety communication channel with respect to the bit error probability (see 3.1.35)
v	Maximum sample rate of SPDUs per hour
m	Maximum number of logical connections that is permitted in a single safety function (see Figure 9 and Figure 10)

The number m of logical connections depends on the individual safety function application. Figure 9 and Figure 10 illustrate how this number can be determined.

The figures show the physical connections with possible network elements such as repeaters, switches, or wireless links and the logical connections between the subsystems involved in the safety function.

The logical connections can be based on single cast or multicast communications.

Figure 9 shows an example 1 of an application where m = 4. In this application, all three drives are considered to be hazardous at a single point in time according to the risk analysis.

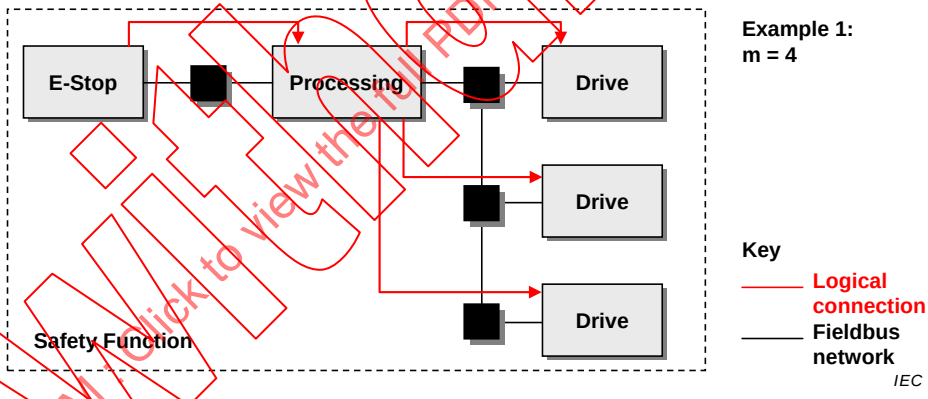


Figure 9 – Example application 1 (m=4)

Figure 10 shows an example 2 of an application where m = 2. In this application, only one of the drives is considered to be hazardous at a single point in time according to the risk analysis.

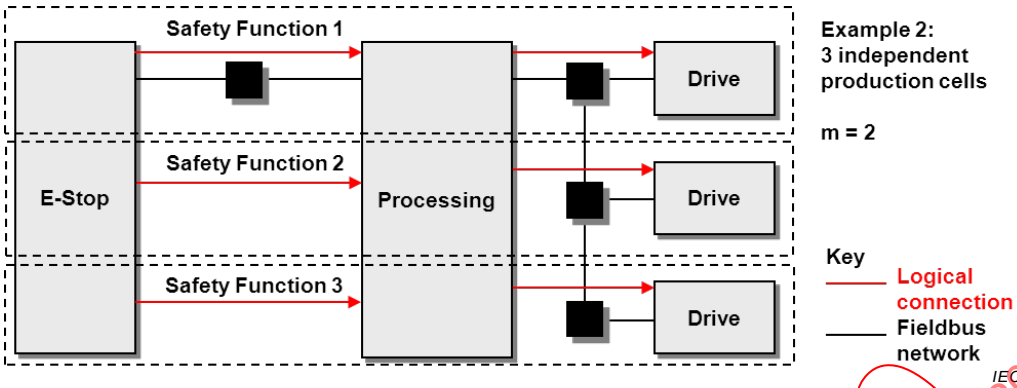


Figure 10 – Example application 2 (m = 2)

5.8.2 Total residual error rate and SIL

A functional safety communication system shall provide a residual error rate in accordance with this standard. Table 3 and Table 4 show the typical relationships between residual error rate and SIL, based on the assumption that the functional safety communication system contributes no more than 1 % per logical connection of the safety function.

Both low demand and high demand mode systems shall have a defined safety function response time, so a necessary rate of SPDUs shall be guaranteed. The PFH for a certain SIL shall be provided in all cases, while the PFD_{avg} is optional.

Table 3 – Typical relationship of residual error rate to SIL

Applicable for safety functions up to SIL	Average frequency of a dangerous failure for the safety function (PFH)	Maximum permissible residual error rate for one logical connection of the safety function (λ_{SC} (Pe))
4	$< 10^{-8}$/h	$< 10^{-10}$/h
3	$< 10^{-7}$/h	$< 10^{-9}$/h
2	$< 10^{-6}$/h	$< 10^{-8}$/h
1	$< 10^{-5}$/h	$< 10^{-7}$/h

Table 4 – Typical relationship of residual error on demand to SIL

Applicable for safety functions up to SIL	Average probability of a dangerous failure on demand for the safety function (PFDavg)	Maximum permissible residual error probability for one logical connection of the safety function
4	$< 10^{-4}$	$< 10^{-6}$
3	$< 10^{-3}$	$< 10^{-5}$
2	$< 10^{-2}$	$< 10^{-4}$
1	$< 10^{-1}$	$< 10^{-3}$

5.9 Relationship between functional safety and security

Security threat and risk assessment is necessary for safety-related applications. Requirements for security are detailed in the IEC 62443 series.

Security means protection against unacceptable intentional (cyber) attacks or unintentional changes of an industrial automation and control system (IACS).

Security concepts in IEC 62443 follow a similar life cycle concept as IEC 61508, starting with a security threat and risk assessment and the assignment of target Security Levels. However, due to the nature of the threats caused by individuals, IEC 62443 emphasizes primarily on issues such as policies and procedures for a Security Management System (SMS) established by plant owners and suppliers within their organization. One major issue of the SMS is maintenance of the security system to counter degradation, for example via monitoring, periodic assessments, or software patches.

IEC 62443 then specifies technologies and methods to achieve a secure system by partitioning the architecture of an IACS into zones and conduits. The plant owner or integrator is provided with appropriate countermeasures and technologies to achieve the target Security Level and its seven foundational requirements (vector) for the zones and conduits.

IEC 62443 also addresses the requirements to secure system components.

IEC 62443 allows designers to choose where to implement the security countermeasures with respect to safety devices.

NOTE Additional profile specific requirements can also be specified in IEC 61784-4.

Figure 11 shows an example of the zones and conduits partitioning of an IACS with functional safety islands.

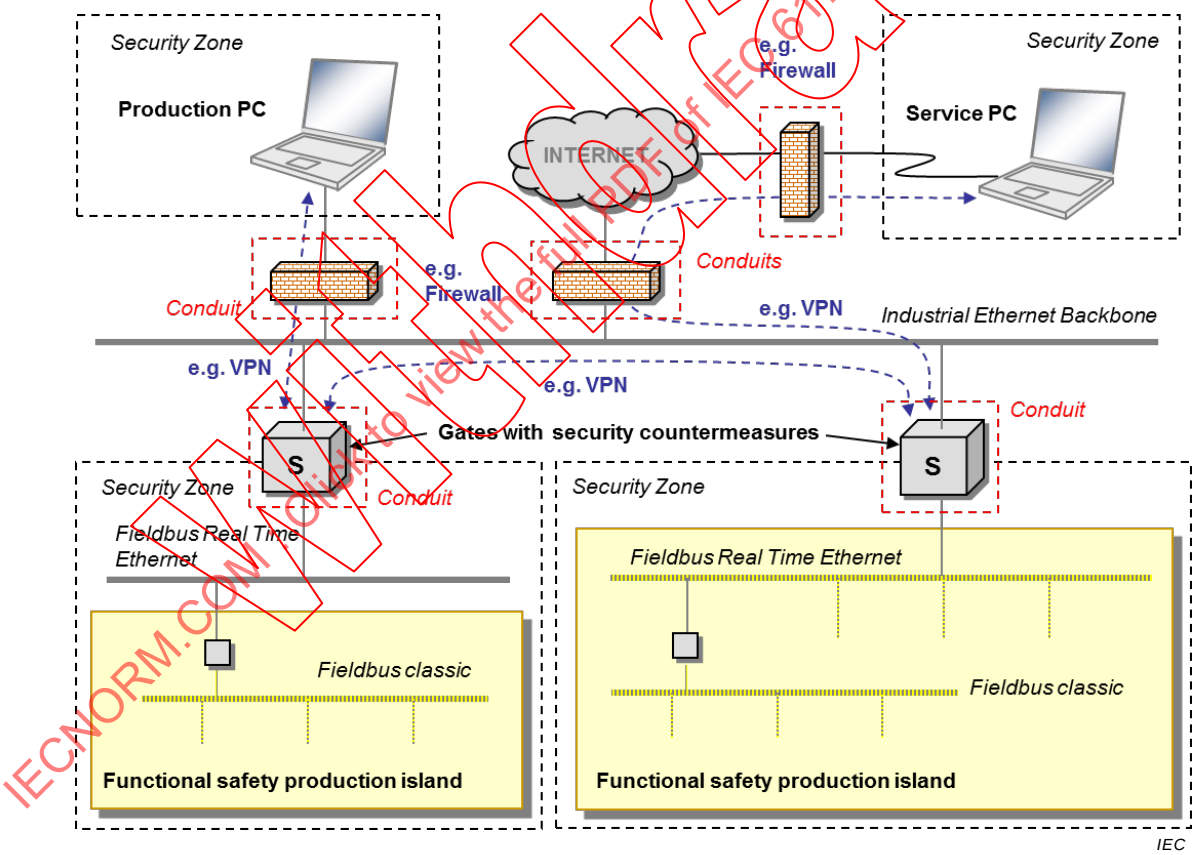


Figure 11 – Zones and conduits concept for security according to IEC 62443

5.10 Boundary conditions and constraints

5.10.1 Electrical safety

Electrical safety is a precondition for a functional safety communication system. Therefore, all safety devices connected to it shall conform to the relevant IEC electrical safety standards (for example SELV/PELV as specified in IEC 61010-2-201). The Safety Manual shall specify

the constraints required of the devices connected in a functional safety communication system, whether safety devices or non-safety devices, including active network elements.

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

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

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

5.10.2 Electromagnetic compatibility (EMC)

Safety devices shall comply with the increased test levels and durations, as well as corresponding performance criteria specified in IEC 61326-3-1 or the generic standard IEC 61000-6-7. 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 can require higher levels than those specified in IEC 61326-3-1, according to Safety Requirements Specification (SRS).

5.11 Installation guidelines

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

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

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

NOTE Additional details can be provided in the technology-specific parts of the IEC 61784-3 sub-series if relevant.

5.12 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.

5.13 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 communication technologies specified in this standard shall only be implemented in devices designed in accordance with the requirements of IEC 61508.

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

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

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

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

It is strongly recommended that implementers of a specific profile comply with the appropriate conformance tests and validations provided by the related technology-specific organization.

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

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

Communication Profile Family 1 (commonly known as FOUNDATION™ Fieldbus[6]) 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™[6]) 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.

7 Communication Profile Family 2 (CIP™) and Family 16 (SERCOS®) – Profiles for functional safety

Communication Profile Family 2 (commonly known as CIP™[7]) 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.

Communication Profile Family 16 (commonly known as SERCOS®[8]) defines a communication profile CP 16/3 based on IEC 61158-3-19, IEC 61158-4-19, IEC 61158-5-19, and IEC 61158-6-19.

---

6 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 and compliance with conditions for their use (such as testing and validation).

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

8 SERCOS® is a trade name of SERCOS International e.V. This information is given for the convenience of users of this International Standard and does not constitute an endorsement by IEC of the trademark holder or any of its products. Compliance to this standard does not require use of the trade name SERCOS®. Use of the trade

The basic profiles CP 2/1, CP 2/2, CP 2/3 and CP 16/3 are defined in IEC 61784-1 and IEC 61784-2. The CPF 2 functional safety communication profile FSCP 2/1 (CIP Safety™[7]) is based on the CPF 2 basic profiles in IEC 61784-1 and IEC 61784-2, the CP 16/3 basic profile in IEC 61784-2, and the safety communication layer specifications defined in IEC 61784-3-2.

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

Communication Profile Family 3 (commonly known as PROFIBUS™, PROFINET™[9]) 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™[9]) 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.

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

Communication Profile Family 6 (commonly known as INTERBUS®[10]) 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™[10]) 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 5.

Table 5 – 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.

name SERCOS® requires permission of the trade name holder and compliance with conditions for its use (such as testing and validation).

9 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 trade names for PROFIBUS™, PROFINET™ or PROFIsafe™. Use of the registered trade names for PROFIBUS™, PROFINET™ or PROFIsafe™ requires permission of PNO and compliance with conditions for their use (such as testing and validation).

10 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 and compliance with conditions for their use (such as testing and validation).

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

10.1 Functional Safety Communication Profile 8/1

Communication Profile Family 8 (commonly known as CC-Link™[11]) defines communication profiles based on IEC 61158-2 Type 18, IEC 61158-3-18, IEC 61158-4-18, IEC 61158-5-18, and IEC 61158-6-18.

The basic profiles CP 8/1, CP 8/2, and CP 8/3 are defined in IEC 61784-1. The CPF 8 functional safety communication profile FSCP 8/1 (CC-Link Safety™[11]) is based on the CPF 8 basic profiles in IEC 61784-1 and the safety communication layer specifications defined in IEC 61784-3-8.

10.2 Functional Safety Communication Profile 8/2

Communication Profile Family 8 also defines communication profiles based on IEC 61158-5-23 and IEC 61158-6-23.

The basic profiles CP 8/4 and CP 8/5 (commonly known as CC-Link IE™[12]) are defined in IEC 61784-2. The CPF 8 functional safety communication profile FSCP 8/2 (CC-Link IE™ Safety communication function) is based on the CPF 8 basic profiles in IEC 61784-2 and the safety communication layer specifications defined in IEC 61784-3-8.

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

Communication Profile Family 12 (commonly known as EtherCAT™[13]) defines communication profiles based on IEC 61158-2 Type 12, IEC 61158-3-12, IEC 61158-4-12, IEC 61158-5-12 and IEC 61158-6-12.

The basic profiles CP 12/1 and CP 12/2 are defined in IEC 61784-2. The CPF 12 functional safety communication profile FSCP 12/1 (Safety-over-EtherCAT™[13]) is based on the CPF 12 basic profiles in IEC 61784-2 and the safety communication layer specifications defined in IEC 61784-3-12.

---

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

12 CC-Link IE™ is a trade name of the non-profit organization CC-Link Partner Association. This information is given for the convenience of users of this International Standard and does not constitute an endorsement by IEC of the trade name holder or any of its products. Compliance to this standard does not require use of the trade name CC-Link IE™. Use of the trade name CC-Link IE™ requires permission of CC-Link Partner Association and compliance with conditions for its use (such as testing and validation).

13 EtherCAT™ and Safety-over-EtherCAT™ are trade names of Beckhoff, Verl. This information is given for the convenience of users of this International Standard and does not constitute an endorsement by IEC of the trade name holder or any of its products. Compliance to this standard does not require use of the trade names EtherCAT™ or Safety-over-EtherCAT™ Use of the trade names EtherCAT™ or Safety-over-EtherCAT™ requires permission of Beckhoff, Verl and compliance with conditions for their use (such as testing and validation).

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

Communication Profile Family 13 (commonly known as Ethernet POWERLINK™[14]) defines communication profiles based on IEC 61158-3-13, IEC 61158-4-13, IEC 61158-5-13, and IEC 61158-6-13.

The basic profile CP 13/1 is defined in IEC 61784-2. The CPF 13 functional safety communication profile FSCP 13/1 (openSAFETY™[14]) is based on the CPF 13 basic profiles in IEC 61784-2 and the safety communication layer specifications defined in IEC 61784-3-13.

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

Communication Profile Family 14 (commonly known as EPA®[15]) defines communication profiles based on IEC 61158-3-14, IEC 61158-4-14, IEC 61158-5-14, and IEC 61158-6-14.

The basic profiles CP 14/1 and CP 14/2 are defined in IEC 61784-2. The CPF 14 functional safety communication profile FSCP 14/1 (EPASafety®[15]) is based on the CPF 14 basic profiles in IEC 61784-2 and the safety communication layer specifications defined in IEC 61784-3-14.

14 Communication Profile Family 17 (RAPIEnet™) – Profiles for functional safety

Communication Profile Family 17 (commonly known as RAPIEnet™[16]) defines a communication profile based on IEC 61158-3-21, IEC 61158-4-21, IEC 61158-5-21, and IEC 61158-6-21.

The basic profile CP 17/1 is defined in IEC 61784-2. The CPF 17 functional safety communication profile FSCP 17/1 (RAPIEnet Safety™[16]) is based on the CPF 17 basic profile in IEC 61784-2 and the safety communication layer specifications defined in IEC 61784-3-17.

---

14 Ethernet POWERLINK™ and openSAFETY™ are trade names of the non-profit organization Ethernet POWERLINK™ Standardization Group (EPSG). This information is given for the convenience of users of this International Standard and does not constitute an endorsement by IEC of the trade name holder or any of its products. Compliance to this standard does not require use of the trade names Ethernet POWERLINK™ or openSAFETY™. Use of the trade names Ethernet POWERLINK™ or openSAFETY™ requires permission of Ethernet POWERLINK™ Standardization Group (EPSG) and compliance with conditions for their use (such as testing and validation).

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

16 RAPIEnet™ and RAPIEnet Safety™ are trade names of the non-profit organization RAPIEnet Association. This information is given for the convenience of users of this International Standard and does not constitute an endorsement by IEC of the trade name holder or any of its products. Compliance with this standard does not require use of the registered trade names for RAPIEnet™ or RAPIEnet Safety™. Use of the registered trade names for RAPIEnet™™ or RAPIEnet Safety™ requires permission of RAPIEnet Association and compliance with conditions for their use (such as testing and validation).

15 Communication Profile Family 18 (SafetyNET p™ Fieldbus) – Profiles for functional safety

Communication Profile Family 18 (commonly known as SafetyNET p™[17]) defines communication profiles based on IEC 61158-3-22, IEC 61158-4-22, IEC 61158-5-22 and IEC 61158-6-22.

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

17 SafetyNET p is a trade name of the Pilz GmbH & Co. KG. 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 profile does not require use of the trade name SafetyNET p. Use of the trade name SafetyNET p requires permission of the trade name holder and compliance with conditions for its use (such as testing and validation).

Annex A
(informative)

Example functional safety communication models

A.1 General

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

Some examples are listed in Clauses A.2 to A.5 – other models may be used.

NOTE Implementation structures in these examples are based on redundant safety communication layers, in accordance with IEC 61508 examples.

A.2 Model A (single message, channel and FAL, redundant SCLs)

Model A shown in Figure A.1 serves as the base reference model for the other models. Only one fieldbus is used as the communication channel.

Two SCLs operate independently to generate two SPDUs from the same safety data. The SPDUs are cross-checked before one of them is transferred using a single fieldbus message. The received SPDU is independently decoded and safety checked by the two receiving SCLs and cross-checked. Both safety communication layers are involved in the production of the message.

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

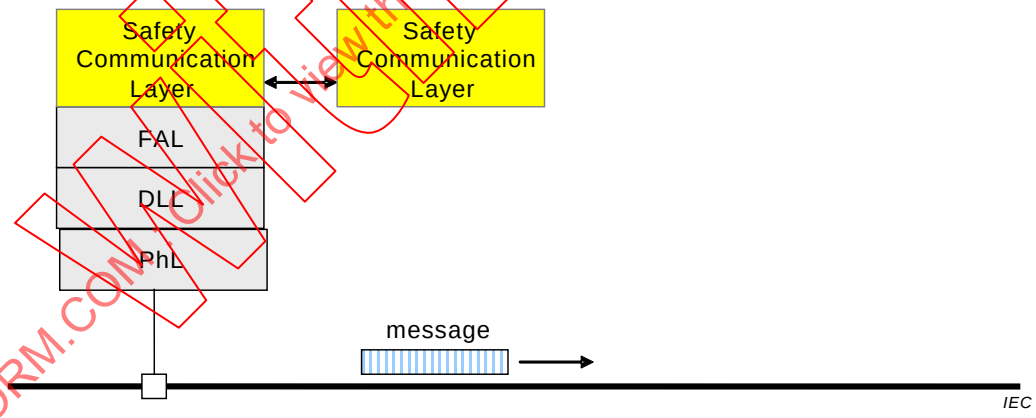


Figure A.1 – Model A

A.3 Model B (full redundancy)

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

Each SCL generates an SPDU from the same safety data and sends it on the attached fieldbus. The messages from both safety communication channels are safety-checked and cross-checked.

Transmission layers and transmission media may be of different types.

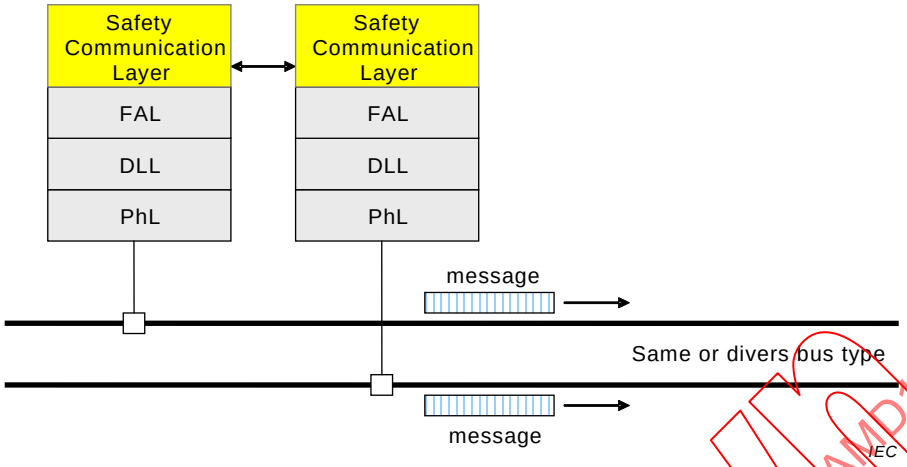


Figure A.2 – Model B

A.4 Model C (redundant messages, FALs and SCLs, single channel)

Model C in Figure A.3 shows a system with full redundancy of the fieldbus device components and only one transmission medium.

Two SCLs generate SPDUs from the same safety data. The SPDUs are sent at different times on the same fieldbus using different messages. The messages from both safety communication channels are safety-checked by both and cross-checked.

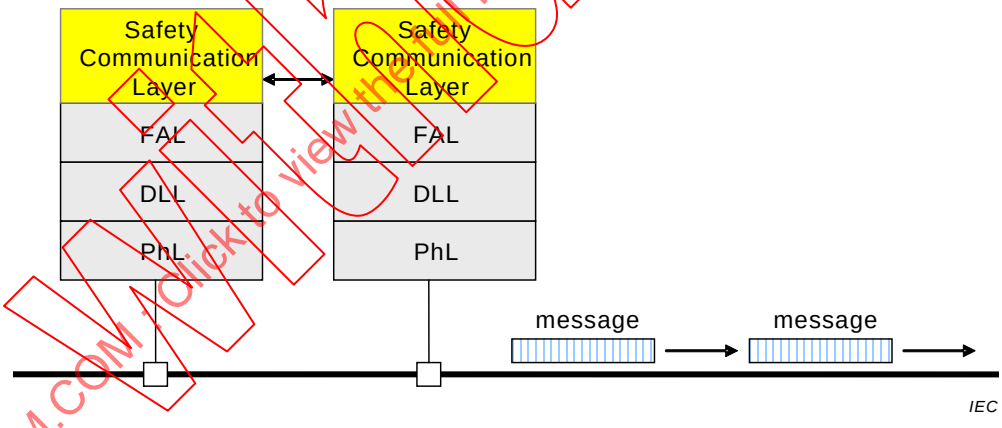


Figure A.3 – Model C

A.5 Model D (redundant messages and SCLs, single channel and FAL)

Model D in Figure A.4 shows a system with dual safety communication layers while the transmission layers exist only once.

Two SCLs generate SPDUs from the same safety data. The SPDUs are sent at different times on the same fieldbus using different messages. Alternatively the two SPDUs can be sent as separate fields in the same message.

The messages from both safety communication layers are safety-checked independently and cross-checked.

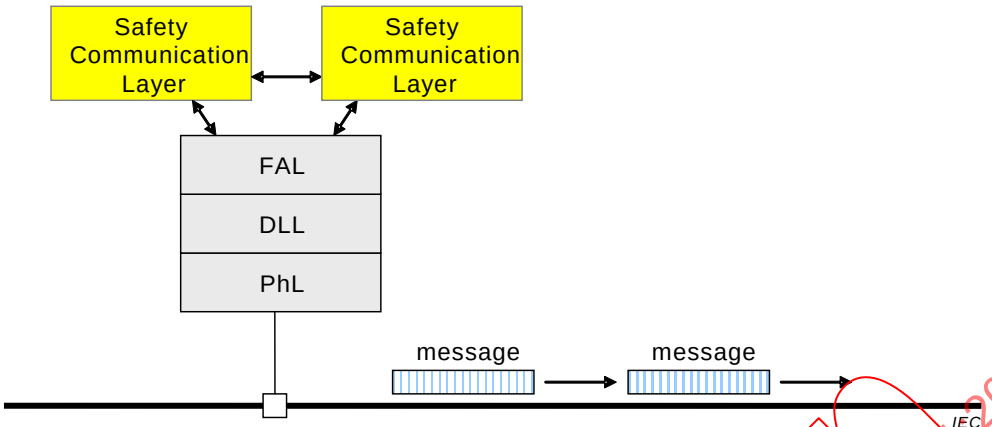


Figure A.4 – Model D

Annex B
(normative)

Safety communication channel model using CRC-based error checking

B.1 Overview

This annex contains a black channel model for data integrity calculations. Use of this model is recommended, unless a different model can be proven more applicable for a particular FSCP.

B.2 Channel model for calculations

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

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

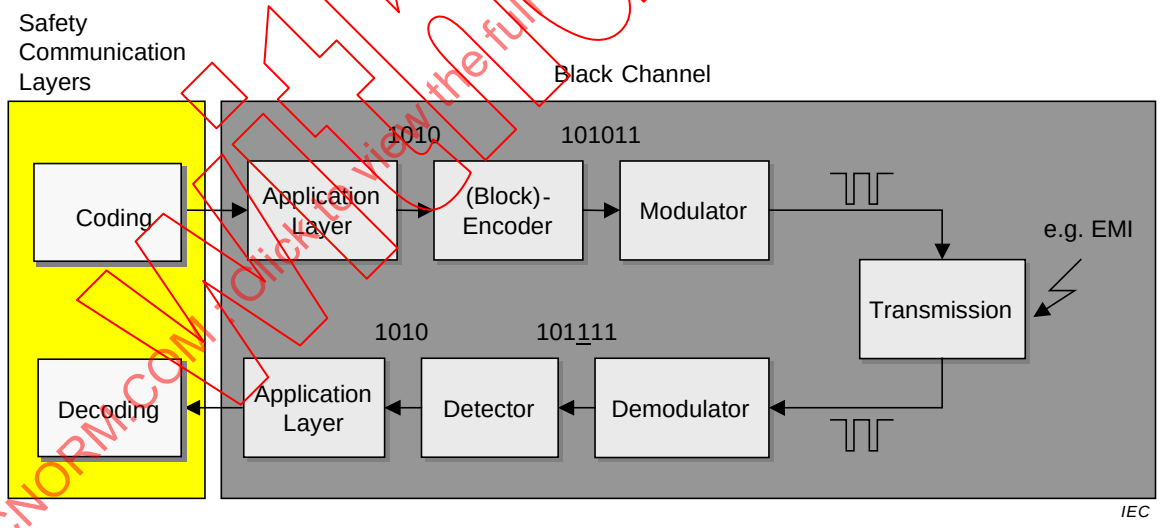


Figure B.1 – Communication channel with perturbation

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

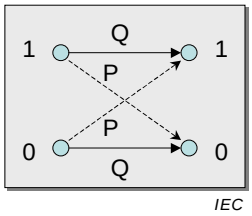


Figure B.2 – Binary symmetric channel (BSC)

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

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

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

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

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

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

B.3 Bit error probability Pe

A Bit Error Probability (Pe) of 10^{-4} in the presence of continuous electromagnetic interference would lead to a stop of communication (nuisance trip) in case of cyclic data exchange (e.g. watchdog time expires after too many retries). Through correct installation (e.g. shielding, equipotential bonding), these nuisance trips normally can be mitigated.

The design of a safety layer assuming a Pe of 10^{-4} is not recommended, as single burst interferences with many corrupted bits are common in industrial environments.

In order to detect these kinds of disturbances, the error detection mechanisms should be powerful enough to achieve the required total Residual Error Probability at a 100 times higher Pe than 10^{-4}, that is 10^{-2}.

Therefore, unless a better (lower) error probability can be proven, a maximum value of 10^{-2} shall be used for the bit error probability.

B.4 Cyclic redundancy checking

B.4.1 General

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

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

where

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

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

P_e is the bit error probability.

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

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

The function (curve) of this approximation Equation (B.4) may deliver smaller (better) residual error probability values than exact calculations (see for example [31]). 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.

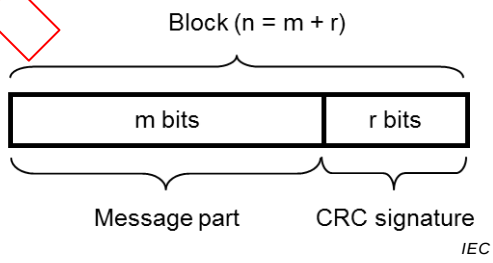


Figure B.3 – Example of a block with a message part and a CRC signature

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

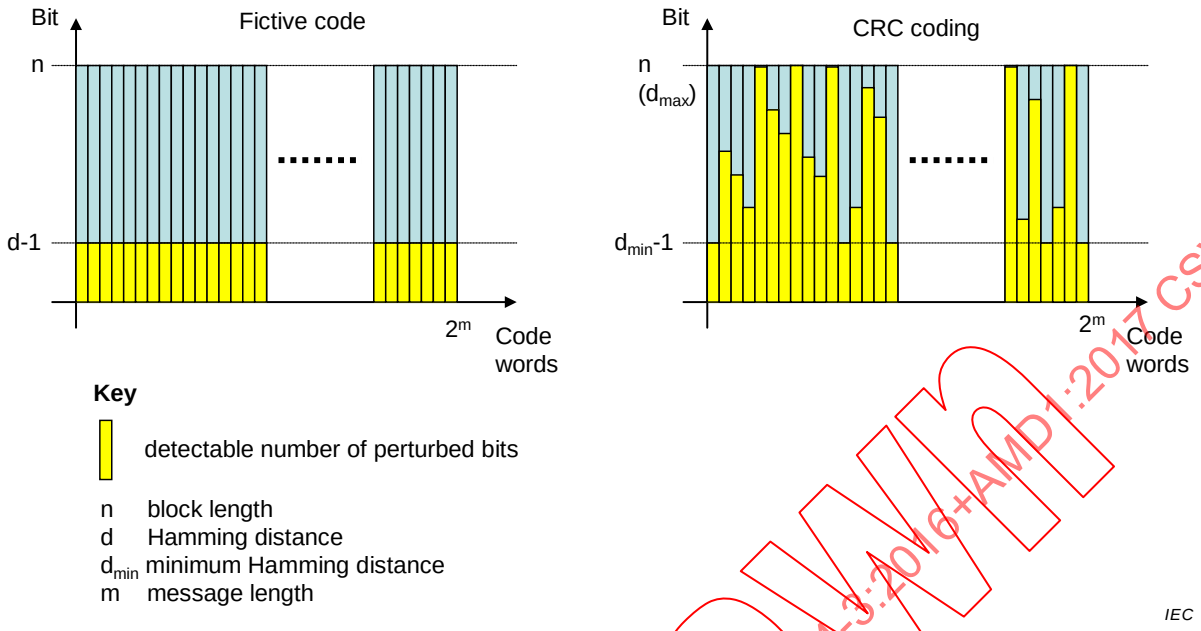


Figure B.4 – Block codes for error detection

Usually the CRC mechanism provides better residual error probability with smaller block bit length n. Thus a dependency exists between block bit 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 bit length n

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

B.4.2 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 [29], [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.

NOTE More information can be found in [32].

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

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

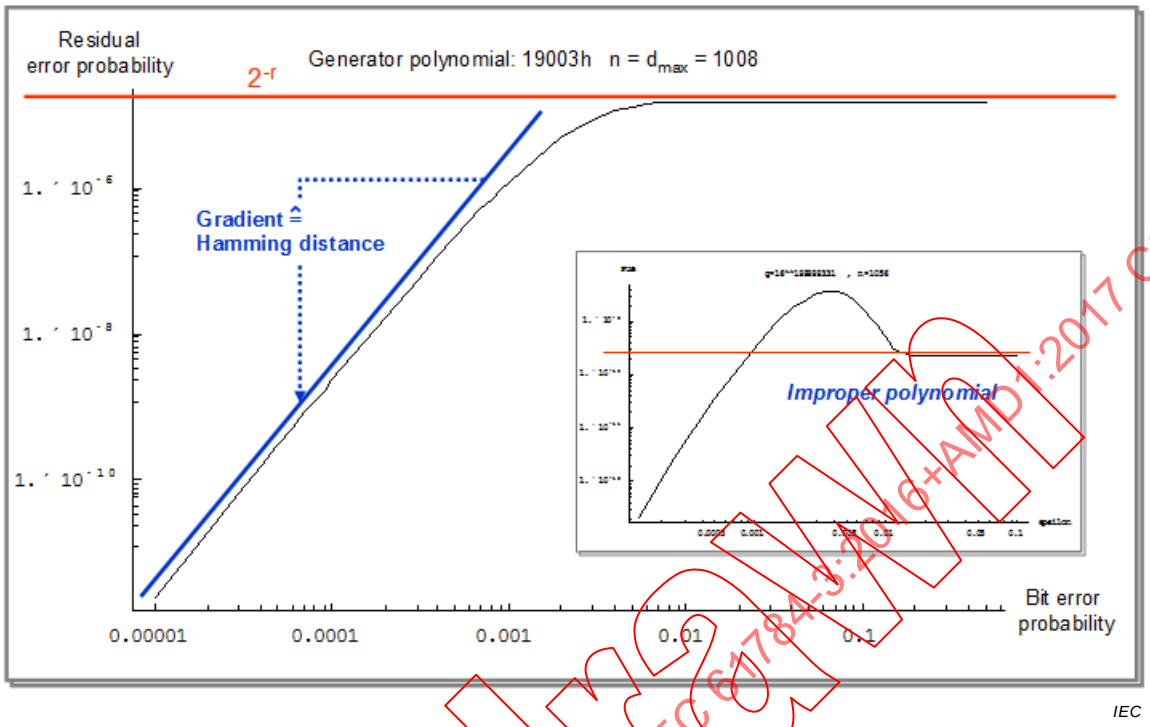


Figure B.5 – Proper and improper CRC polynomials

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

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

Annex C
(informative)

Structure of technology-specific parts

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

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

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

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

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

5.5	Relationships with FAL (and DLL, PhL)	May include existing diagnostics, expected services, constraints (for example, “to be used in conjunction with FSCP x/y”)
5.5.1	Data Types	List of the IEC 61158 data types used by the profile
6	Safety communication layer services	May include application objects used, diagnostic services
7	Safety communication layer protocol	First subclause is listed below, others may be added as needed. May include specific time mechanisms , state machines, sequence charts, reaction on power off/power down, diagnostic protocol and corresponding diagnosis
7.1	Safety PDU format	Includes detailed definition of safety PDU (message) formats. Will include several subclauses to specify the various format elements (for example safety CRC specification)
8	Safety communication layer management	Includes specifications for the following aspects of parameterization: – safe parameter data supplied by another safety device (for example a parameter server) – safe parameter data supplied by a tool (for example device description) (including any required measure to secure the storage, handling and transfer)
9	System requirements	First subclauses are listed below, others may be added as needed
9.1	Indicators and switches	Specifications for device indicators and switch function and behaviour
9.2	Installation guidelines	Detailed clause references within IEC 61918 or other relevant documents
9.3	Safety function response time	Calculations and related examples of reaction times relevant for the technology (for example worst case reaction time of safety loop)
9.4	Duration of demands	Specifications for the duration of demands within devices
9.5	Constraints for calculation of system characteristics	Includes black channel retries, number of telegram per second, number of message sinks
9.6	Maintenance	Specifications for system behaviour in case of device repair and replacement
9.7	Safety manual	If relevant, includes the minimum information required by the profile to be included in the safety manual
9.8	Wireless transmission channels	This subclause is optional. If relevant,it includes specific requirements when using wireless transmission
9.9	Conformance classes	This subclause is optional. If relevant, it includes additional conformance requirements for the base fieldbus protocol
10	Assessment	Include information on assessment requirements
Annex A (informative)	Additional information for functional safety communication profiles of CPF X	Mandatory informative annex used to provide additional non-normative information on the protocol. If there is none, then this will contain the following sentence: “There is no additional information for this FSCP”.

A.1	Hash function calculation	For example algorithms for CRC calculation
	Bibliography	Bibliographic references relevant for this part

Annex D
(informative)

Assessment guideline

D.1 Overview

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

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

The documentation that is provided for the test or assessment shall specify the exact operating conditions according to 5.10.2. No deviation from these conditions is permitted under any circumstances.

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

NOTE IEC TR 62685 is a companion guideline which provides information about additional assessment aspects of safety devices for functional safety communication, such as test beds, proof of increased interference immunity (EMC for functional safety), electrical safety, and other environmental requirements.

D.2 Channel types

D.2.1 General

Clause D.2 defines two general types of safety communication concepts, the black channel and the white channel approach. This guideline covers both safety communication concepts.

D.2.2 Black channel

According to definition 3.1.5, black channel type safety communication requires only evidence of design or validation of the safety communication layer (SCL) according to IEC 61508. It is possible for a safety device designer to use a pre-assessed and approved hardware/software component, which provides the functions of the particular SCL. If the designer implements this component in its specified manner, a safety assessment of the component itself according to IEC 61508 can be omitted. Thus, efforts can be reduced to the assessment of the safety-related technology of the device and the correct implementation of the SCL component.

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

D.2.3 White channel

According to definition 3.1.55, white channel type safety communication requires all relevant hardware and software components to be designed, implemented and validated according to IEC 61508. Due to the large variety of possible solutions this guideline only provides help on how to proceed with the aspects of data integrity assurance.

NOTE Further information can be found in IEC 62280.

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

D.3 Data integrity considerations for white channel approaches

D.3.1 General

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

D.3.2 Models B and C

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

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

NOTE 2 Equations in this Subclause D.3.2 can also be applied to black channel systems.

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

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

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

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

NOTE 3 This equation can only be applied for proper polynomials (see B.4.2), see [31].

An analysis according to D.3.3 together with a calculation using Equation (D.2) is required for a complete evaluation of the residual error probability in case of a white channel solution.

NOTE 4 See IEC 62280 for more information.

The calculation of $\Lambda_{SCL}(P_e)$ is carried out along the lines of 5.8.1 (Equation (1)).

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

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

D.3.3 Models A and D

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

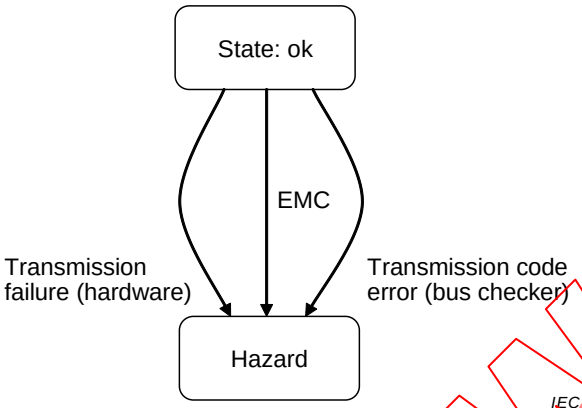


Figure D.1 – Basic Markov model

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

In this case a Markov analysis can be expressed by three fundamental transition possibilities (Figure D.1):

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

NOTE 1 This Markov analysis is derived from IEC 62280.

The residual error probability R_{AD} of the system is the summation of the individual probabilities (Equation (D.2)). The calculation of $\Lambda_{SCL}(p_e)$ is carried out along the lines of 5.8.1 with the residual error probability:

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

where

R_{AD} is the residual error probability of the system for models A and D;

R_{HW} is the residual error probability for faults resulting from hardware failures;

R_{EMC} is the residual error probability for faults resulting from electromagnetic interferences;

R_{TC} is the residual error probability for faults resulting from failures of bus checking mechanisms.

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

NOTE 2 See IEC 62280 for more information.

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

D.4 Verification of safety measures

D.4.1 General

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

D.4.2 Implementation

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

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

D.4.3 "De-energize to trip" principle

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

Assessment: See 5.4.4.

D.4.4 Safe state

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

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

D.4.5 Transmission errors

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

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

D.4.6 Safety reaction and response times

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

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

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

D.4.7 Combination of measures

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

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

D.4.8 Absence of interference

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

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

D.4.9 Additional fault causes (white channel)

In addition to the already described methods for the estimation of residual errors using the BSC model, further fault causes need to be considered and controlled, such as "synchronisation slip errors" within the physical and data link layers.

NOTE Details can be found in IEC 62280 or [28].

Assessment: This assessment is outside the scope of this standard.

D.4.10 Reference test beds and operational conditions

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

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

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

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

D.4.11 Conformance tester

Conformance to a particular FSCP should be tested by a profile conformance tester defined by the technology-specific organization related to the individual FSCP.

NOTE Conformance testing includes both positive and negative tests.

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

Annex E
(informative)

Examples of implicit vs. explicit FSCP safety measures

E.1 General

The examples provided in E.2 to E.7 illustrate the concepts of explicit and implicit safety measures.

E.2 Example fieldbus message with safety PDUs

Figure E.1 shows safety PDUs embedded in a fieldbus message during transmission.

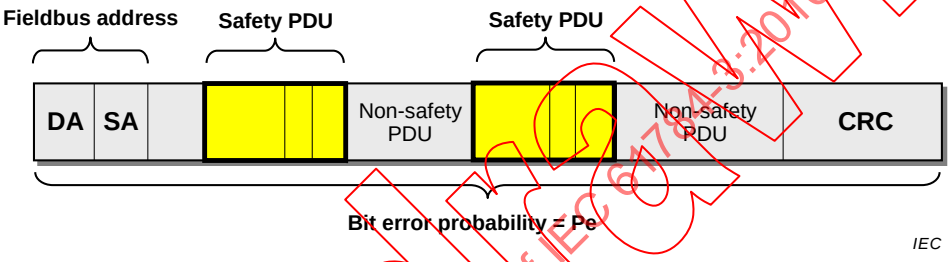


Figure E.1 – Example safety PDUs embedded in a fieldbus message

E.3 Model with completely explicit safety measures

Figure E.2 shows the model and the safety checking of a safety PDU with completely explicit safety measures for timeliness and authenticity.

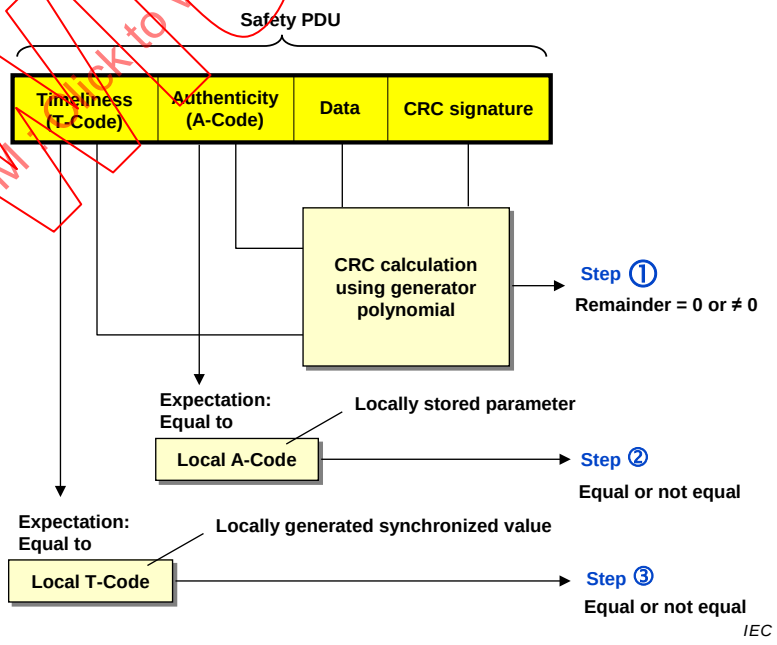


Figure E.2 – Model with completely explicit safety measures

Checking is done according to the following steps:

Step ①	Remainder ≠ 0	→	Any error detected
	Remainder = 0	→	Data correct or incorrect with RR_I according to F.5.2.2
Step ②	Not equal	→	Any error detected
	Equal	→	Authenticity correct or incorrect with RR_A according to F.5.2.3
Step ③	Not equal	→	Any error detected
	Equal	→	Timeliness correct or incorrect with RR_T according to F.5.2.4

E.4 Model with explicit A-code and implicit T-code safety measures

Figure E.3 shows the model and the safety checking of a safety PDU with explicit safety measure for Authenticity and implicit safety measure for Timeliness.

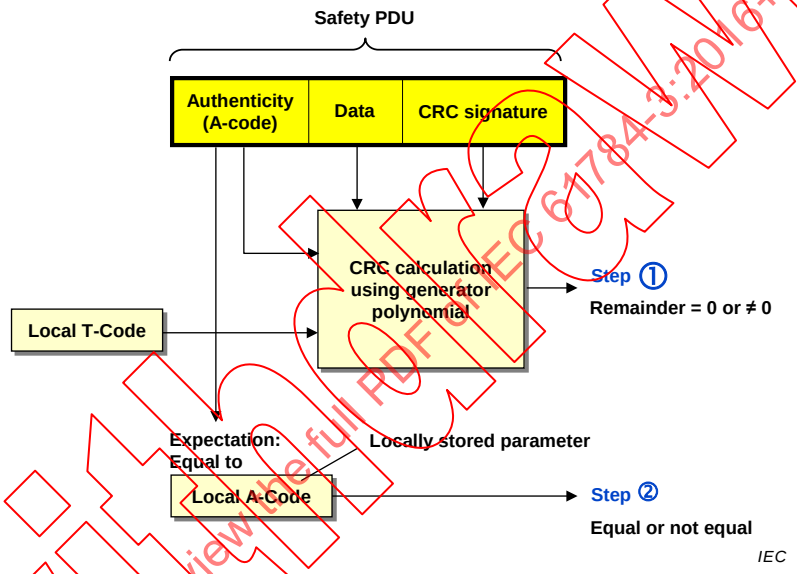


Figure E.3 – Model with explicit A-code and implicit T-code safety measures

Checking is done according to the following steps:

Step ①	Remainder ≠ 0	→	Any error detected
	Remainder = 0	→	Data and Timeliness correct or incorrect with certain RR
Step ②	Not equal	→	Any error detected
	Equal	→	Authenticity correct or incorrect with RR_A according to F.5.2.3

E.5 Model with explicit T-code and implicit A-code safety measures

Figure E.4 shows the model and the safety checking of a safety PDU with explicit safety measure for Timeliness and implicit safety measure for Authenticity.

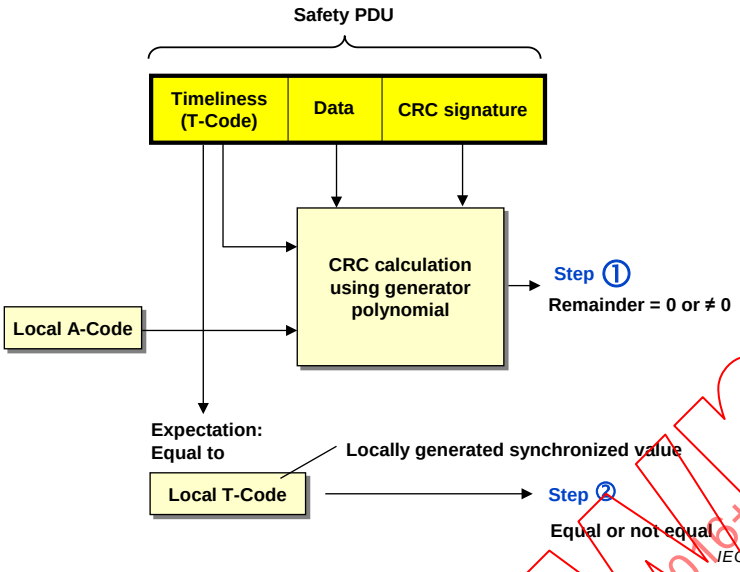


Figure E.4 – Model with explicit T-code and implicit A-code safety measures

Checking is done according to the following steps:

Step ①	Remainder ≠ 0	→	Any error detected
	Remainder = 0	→	Data and Authenticity correct or incorrect with certain RR
Step ②	Not equal	→	Any error detected
	Equal	→	Timeliness correct or incorrect with RR_T according to F.5.2.4

E.6 Model with split explicit and implicit safety measures

Figure E.5 shows the model and the safety checking of a safety PDU with split explicit and implicit safety measures for timeliness and implicit measures for authenticity.

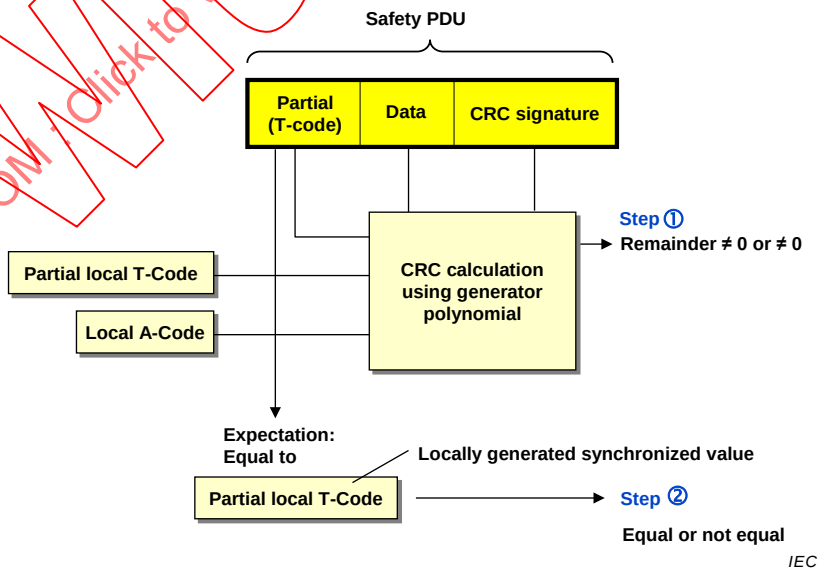


Figure E.5 – Model with split explicit and implicit safety measures

Checking is done according to the following steps:

Step ① Remainder ≠ 0 → Any error detected
Remainder = 0 → Data, Authenticity and Timeliness correct or incorrect with certain RR

Step ② Not equal → Any error detected
Equal → Timeliness correct or incorrect with certain RR

E.7 Model with completely implicit safety measures

Figure E.6 shows the model and the safety checking of a safety PDU with implicit safety measure for both Authenticity and Timeliness.

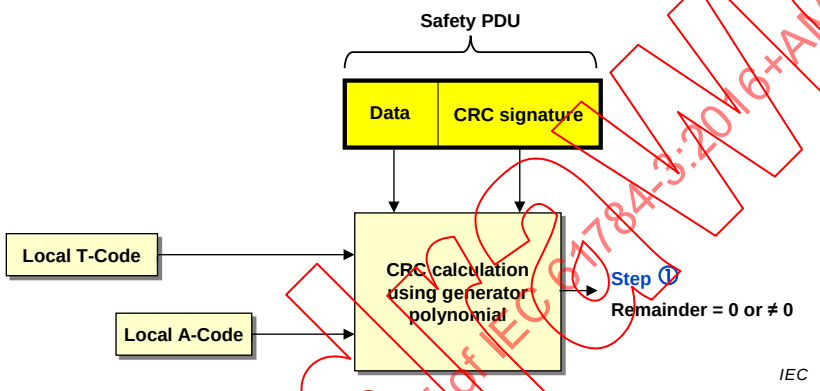


Figure E.6 – Model with completely implicit safety measures

Checking is done according to the following step:

Step ① Remainder ≠ 0 → Any error detected
Remainder = 0 → Data, Authenticity and Timeliness correct or incorrect with certain RR

E.8 Addition to Annex B – impact of implicit codes on properness

The presence of bit errors combined with an erroneous implicit code can influence the properness of the CRC polynomial. As a consequence, the application of implicit codes for safety measures leads to additional effort.

Due to the various possible approaches generic formulae cannot be provided. It is up to the individual FSCP to prove sufficient residual error probabilities.

Annex F
(informative)

Extended models for estimation of the total residual error rate

F.1 Applicability

This Annex F specifies additional extended models for estimating the total residual error rate for an FSCP, for the purpose of assessing this FSCP. These models are intended to replace the models currently specified in 5.8 in the subsequent editions of this standard.

Accordingly, the FSCPs are exempt from a new assessment according to this Annex F until Edition 4, where the contents of current Annex F will replace the current 5.8.

F.2 General models for black channel communications

All FSCPs make a fundamental assumption that all functional safety communications take place through a black channel (see 5.2.3).

To properly quantify the residual error of the safety measures, it is important to first constrain the model for the black channel with respect to the FSCP SCL. This allows the proper definition of the type of messages and the types and rates of errors that the designer of FSCP SCL shall consider with the safety measures.

Figure F.1 shows a black channel that contains different types of communication: Fieldbus messages with safety and non-safety PDUs.

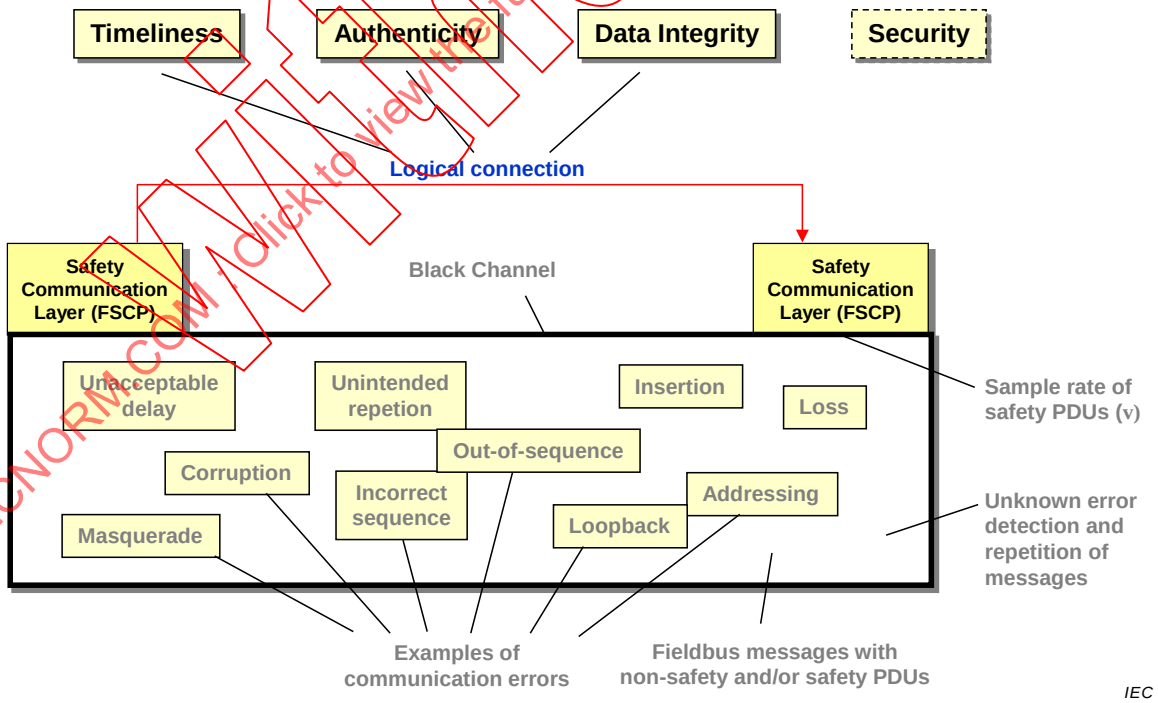


Figure F.1 – Black channel from an FSCP perspective

The black channel includes the underlying fieldbus communication layers below the SCL, as well as any additional communication between the FAL and the SCL within a device.

Errors in the black channel can be generated from several sources:

- bit corruption of messages in the transmission medium; or
- random hardware faults and systematic faults of electronic equipment and software in the black channel.

The frequency of the exchange of messages within the black channel can be different from the frequency at which the SCL is sampling and processing safety PDUs.

F.3 Identification of generic safety properties

Table 1 lists possible discrete safety measures, which alone or in combinations contribute to the following generic safety properties for messages (see Figure F.1):

- data integrity;
- authentication (including masquerade rejection);
- timeliness.

The correct delivery of the content of messages from a message source to the configured message sink(s) is the property of data integrity. The delivery of messages from a correct message source to the configured associated message sink(s) is the property of authentication. The rejection of random bits at a message sink that happen to appear proper is the property of masquerade rejection. Up-to-date delivery of messages between a message source and a message sink within a configured time frame is the property of timeliness.

NOTE Security is an additional known property which is beyond the scope of this standard. Security issues are addressed in IEC 62443.

Another generic safety aspect that shall be considered is the configuration and/or parameterization of the FSCP (see Clause F.12).

A fault in any of these generic safety measures may result in a hazardous state or unintended start-up.

A supplier of an FSCP shall provide proof of a sufficient overall residual error rate taking into account all three generic safety properties as specified in Clause F.10.

F.4 Assumptions for residual error rate calculations

Annex F specifies examples of the types of formulae employed in the calculation of residual error rate, based on assumptions that are taken regarding both black channel and SCL. Alternative formulae shall be employed for cases where these assumptions can be shown not suitable for a given SCL type.

The following general assumptions are valid for all formulae defined in Annex F:

a) assuming a failure rate of an average black channel device to be 100 FIT, it is expected that the SCL shall assume a black channel failure rate 10 000 times this value. Therefore failure rate for electronic equipment is better than 10^{-3}/h (10^{6} FIT) for each active network element or fieldbus part of a safety device;

NOTE 1 Once any device fails, failure could become continuous until it is detected and corrected. This includes permanent, intermittent and transient errors.

NOTE 2 A failure rate less conservative than 10^{-3} can be assumed for an FSCP, if this FSCP drives its safety function to safe state when it detects one or more dangerous black channel failures (see Fault state in Figure 7), if it only returns to operation when it is repaired, and if it can be proven that a failure rate of 10^{-3} would therefore render the safety communication channel inoperable.

b) the presence of store and forward devices is considered, when relevant for the FSCP;

c) safety PDU hash function is different from the one used by the underlying fieldbus DLL (this can be ensured by design or administrative procedures);

d) safety PDU hash function is a CRC which does not include error correction mechanisms;

e) black channel PDU hash function may include error correction mechanisms;

f) each logical connection is assigned a unique authentication code;

g) whenever fixed worst case values are used in the formulae for error or event occurrence probabilities or rates (state of the art), FSCPs may specify instead their own values if sufficient proof is provided;

h) whenever a single mechanism is used to detect multiple types of errors, then these error types shall be considered both individually and in combination when calculating the residual error probability.

F.5 Residual error rates

F.5.1 Explicit and implicit mechanisms

The explicit mechanism includes data corresponding to FSCP safety measures such as sequence number, time stamp and connection authentication in the safety PDU.

The implicit mechanism does not actually transmit all data corresponding to safety measures, but uses them to calculate the overall CRC signature, based on the assumption that the receiver has equivalent knowledge.

NOTE Implicit mechanism is typically used to accommodate limited systems with fixed black channel message sizes or slow transmission rates.

The FSCPs specified in the IEC 61784-3 series can be classified into explicit, implicit and partly explicit/implicit categories (see examples in Annex E). Due to the various possible approaches generic formulae cannot be provided for the implicit category. It is up to the individual FSCP to prove sufficient residual error probabilities. Therefore, this Annex F only deals with the explicit category.

F.5.2 Residual error rate calculations

F.5.2.1 General

Subclauses F.5.2.4 to F.5.2.5 show example equations for the calculation of residual error rates for the explicit FSCP category depending on the lengths of sequence numbers, time stamps and connection authentication data. Specific FSCPs may provide their own equations as applicable.

An SCL may restrict certain fields to only certain values. This is represented by the uniqueness coefficient of limited fields (RP_U) which is included in the residual error rate calculations where appropriate. It is given by Equation (F.1).

$$RP_U = \frac{V_{A1}}{V_{R1}} \times \frac{V_{A2}}{V_{R2}} \times \ldots \times \frac{V_{AN}}{V_{RN}} \qquad \text{(F.1)}$$

where

RP_U is the residual error probability for other fields of uniqueness that distinguish a properly formatted safety PDU;

V_{AN} is the number of values accepted by a sink in data field N;

V_{RN} is the number of values representing the total range for data field N.

F.5.2.2 Contribution of data integrity errors (RR_I)

An example for the calculation of the residual error rate for Data Integrity RR_I is shown in Equation (F.2).

$$RR_I = RP_I \times v \times RP_U \times RP_{FSCP} \quad (F.2)$$

where

RR_I is the residual error rate for Data Integrity;

RP_I is the residual error probability for Data Integrity;

v is the maximum number of SPDU samples by the SCL ("sample rate") per hour;

RP_U is the residual error probability for other fields of uniqueness that distinguish a properly formatted safety PDU;

RP_{FSCP} is the residual error probability for other measures unique to the FSCP.

F.5.2.3 Contribution of authenticity errors (RR_A)

There are three factors for this residual rate:

a) a misdirected PDU;

b) an undetected data corruption error, and;

c) the error must result in a match of the authentication code.

An example for the calculation of the residual error rate for Authenticity RR_A is shown in Equation (F.3).

$$RR_A = RP_I \times 2^{-LA} \times R_A \times RP_{FSCP} \quad (F.3)$$

where

RR_A is the residual error rate for Authenticity regarding misdirected safety PDUs;

RP_I is the residual error probability for Data Integrity;

LA is the bit length of the connection authentication;

R_A is the rate of occurrence for misdirected safety PDUs;

RP_{FSCP} is the residual error probability for other measures unique to the FSCP.

NOTE The use of 2^{-LA} assumes uniform distribution of error patterns in the A-code.

F.5.2.4 Contribution of timeliness errors (RR_T)

An example for the calculation of the residual error rate for Timeliness RR_T is shown in Equation (F.4).

$$RR_T = 2^{-LT} \times w \times R_T \times RP_{FSCP} \quad (F.4)$$

where

RR_T is the residual error rate for Timeliness;

LT is the bit length of the sequence number;

w is the range of values (window) of accepted time stamps or sequence numbers for receiving safety PDUs;

R_T is the rate of occurrence for incorrect sequence safety PDUs (value cannot exceed v, as specified in F.5.2.2);

RP_{FSCP} is the residual error probability for other measures unique to the FSCP.

F.5.2.5 Contribution of masquerade errors (RR_M)

An example for the calculation of the residual error rate for Masquerade RR_M is shown in Equation (F.5).

$$RR_M = 2^{-LA} \times 2^{-LT} \times w \times 2^{-r} \times RP_U \times 2^{-LR} \times R_m \quad (F.5)$$

where

RR_M is the residual error rate for Masquerade;

LA is the bit length of the connection authentication;

LT is the bit length of the sequence number;

w is the range of values (window) of accepted time stamps or sequence numbers for receiving safety PDUs;

r is the bit length of the CRC signature (in case two CRCs with independent polynomials are used, r is the sum of the two corresponding bit lengths);

RP_U is the residual error probability for other fields of uniqueness that distinguish a properly formatted safety PDU;

LR is the bit length of the repeated portion of the safety PDU (for redundancy with cross-checking, otherwise LR = 0);

R_m is the rate of occurrence for masqueraded safety PDUs.

F.6 Data integrity

F.6.1 Probabilistic considerations

The generic safety property data integrity requires the detection of the following communication error according to Table 1:

- corruption (see 5.3.2).

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 and/or data repetition, and similar forms of redundancy shall be applied.

If the residual error probability of the data integrity measures is dependent on the safety data values, then the worst case values shall be considered.

When using cyclic redundancy check (CRC) as hash function, the designer of an FSCP shall prevent or consider the possibility of the "black channel" using the same polynomial. This can be achieved using various methodologies.

EXAMPLES

Possible methodologies include:

– measures allowing only specific combinations of FSCP and CPs;

– appropriate measures in the design of the SCL;

– calculations of the residual error rate using 0,5 as value for Pe.

F.6.2 Deterministic considerations

In addition to random bit patterns, the following specific error patterns shall be evaluated: completely inverted data, completely "0" or "1" data sets, synchronisation slip errors and burst errors.

F.7 Authenticity

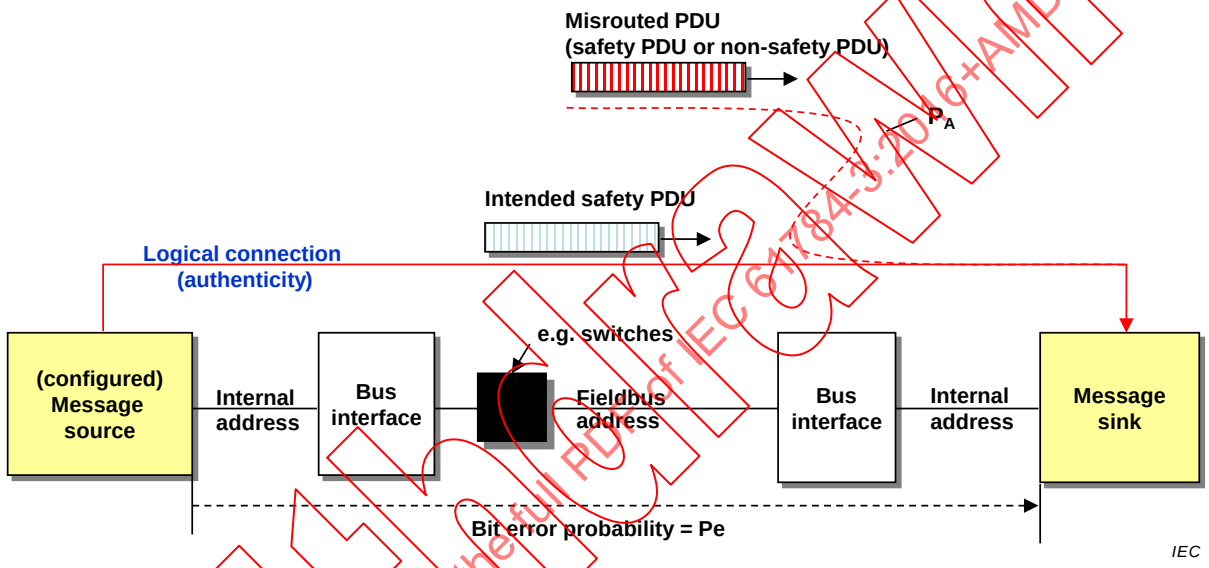
F.7.1 General

The generic safety property authenticity requires the detection of the following communication errors according to Table 1:

- addressing (see 5.3.9);
- insertion (see 5.3.7).

The FSCP shall meet the following requirement (see Figure F.2):

- the message sink shall only process safety data in correctly addressed messages received from an authenticated message source.



Key

PA Probability of an authenticity error for logical connections

Figure F.2 – Model for authentication considerations

These requirements shall be met during all communication phases in 5.6 for which connection authentication is relevant (FSCP dependant). Exclusions shall be documented in the safety manual.

Authentication prevents the processing of safety data in a received message that passes all other checks but is not a valid message for this receiver.

NOTE

Possible stochastic causes for incorrect authenticity include but are not limited to:

– Falsification of an address within the message or an error within an internal communication link (see Figure F.3) regardless whether it is related to a non-safety or safety address mechanism.

– Disturbed or erroneously operating protocol stacks/layers within the black channel.

– Disturbed or erroneously operating routing devices, for example switches or routers.

– Disturbed or erroneously operating gateways, for example bus couplers.

– Disturbed or erroneously operating black channel devices mirroring messages (“loopback error”) or redirect messages by other means.

– The authentication mechanism within the message sink is not sufficient to differentiate between messages from different message sources.

Figure F.3 shows possible addressing errors due to corrupted addresses within the fieldbus communication system or possible internal addressing errors (for example due to corrupted pointers within modular remote I/O devices).

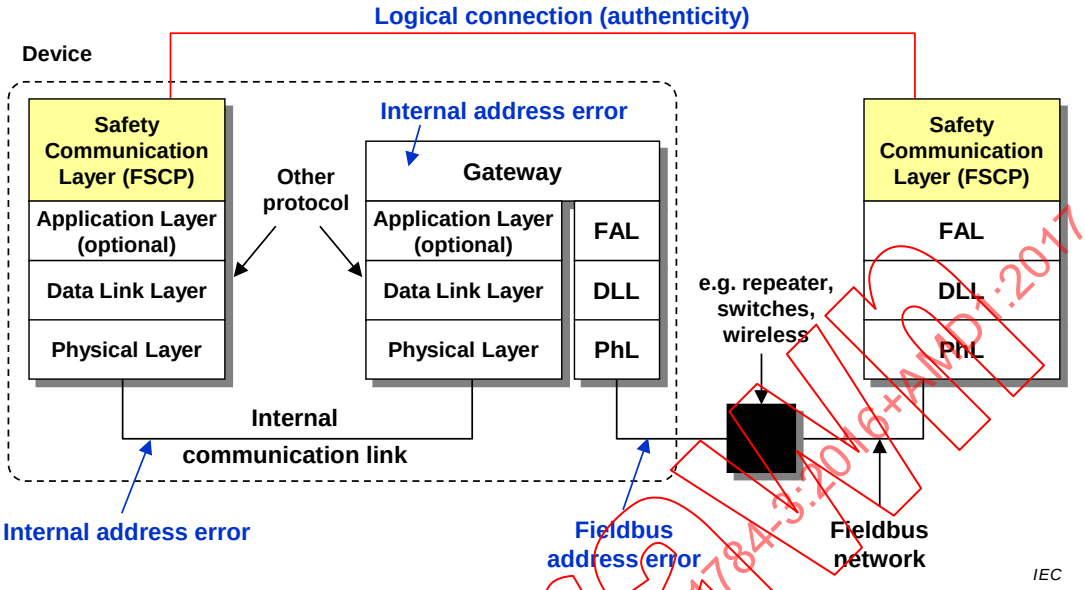


Figure F.3 – Fieldbus and internal address errors

Additional systematic causes for incorrect authenticity may be identified within configuration and parameterization procedures as shown in F.12. Additional organizational measures may be required to control these systematic error causes.

A connection authentication can be used to uniquely and unambiguously identify one of the following:

- a single message source or message sink;
- a single connection between a message source and a message sink;
- a multiple connection between a message source and multiple message sinks in case of multicast;
- a group connection between multiple message sources and sinks.

Several methods are available to avoid authentication errors.

EXAMPLES

– A unique connection authentication (e.g. “connection ID") that is transmitted with each and every FSCP message.

– A locally stored unique connection authentication (e.g. "connection ID") that is encrypted via hash functions such as CRC signatures and transmitted to the message sink. This encryption is usually part of the overall data integrity measures of FSCPs according to 5.9.

F.7.2 Residual error rate for authenticity (RR_A)

The residual error rate RR_A for the generic safety property authenticity shall be calculated from a message sink perspective as shown in Figure F.2.

In accordance with Clause F.4 bullet a), a value of 10^{-3}/h per device shall be assumed for the rate of occurrence for misdirected safety PDUs (R_A), unless otherwise specified.

It is further assumed that R_A shall have the value of v (SPDU sample rate) after the first occurrence of a misdirected safety PDU, until the system is repaired.

The residual error rate RR_A shall be sufficient for all communication phases in 5.6 for which connection authentication is relevant (FSCP dependant).

The technical measures for the authentication can be supplemented by organizational measures, which shall be practical for the user to perform (see Clause F.12).

F.8 Timeliness

F.8.1 General

The generic safety property timeliness requires the detection of the following communication errors according to Table 1:

- unacceptable delay (see 5.3.6);
- unintended repetition (see 5.3.3);
- incorrect sequence (see 5.3.4);
- loss (see 5.3.5).

The FSCP shall meet the following requirements:

- the message sink processes up-to-date messages;
- the message sink monitors the operational status of the safety layer of the message source.

NOTE 1 Depending on unidirectional or bidirectional communication, a device can provide a message source and a message sink at the same time.

The technical measures for timeliness can be supplemented by organizational measures.

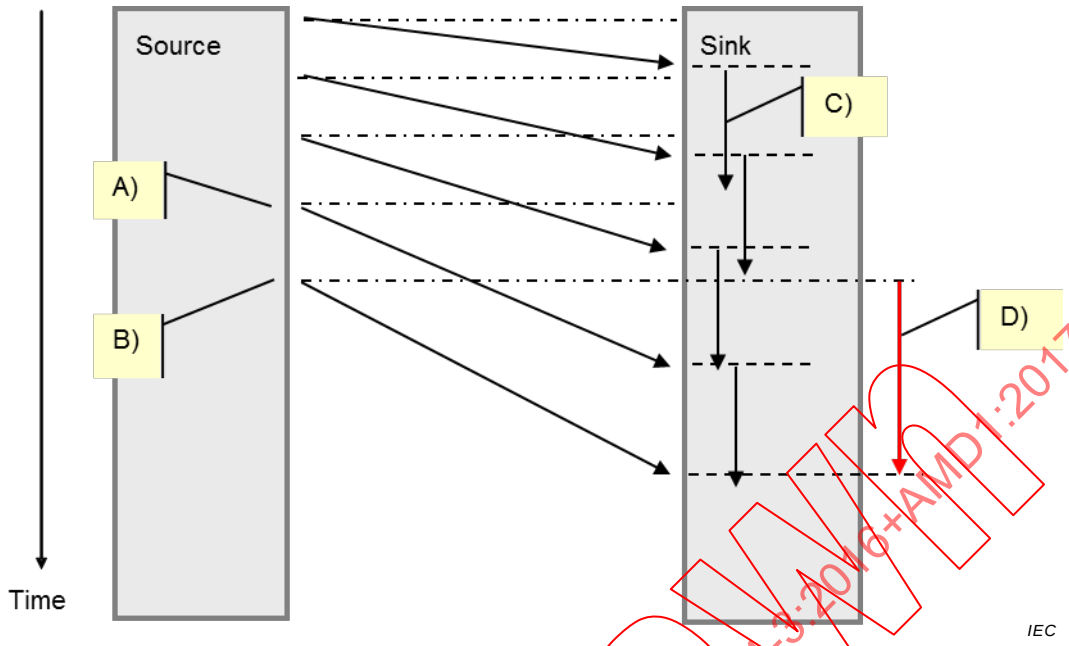
Typical causes for non-timely communication which shall be considered during the design of the FSCP are variable performances of the black channel.

EXAMPLES

Variations in black channel performance can result from:

– insufficient throughput (e.g. bandwidth, traffic);
– loss of communication (temporary or total);
– varying latency;
– slowly increasing latency (see Figure F.4);
– different latency for each message source / sink pair;
– variations in synchronization clock times at message source or message sink; or
– any combination of these.

Figure F.4 shows an example of a slowly increasing message latency of the black channel.



Key

A) Message departure times do not correlate with the message reception times

B) Message departure time is earlier than message reception time of the previous message

C) Timeout check in sink

D) A message sink cannot determine the message departure times out of the message reception times and the intervals. The message delay can be larger than the timeout without being detected!

Figure F.4 – Example of slowly increasing message latency

Another issue that shall be considered is the unintended transmission from memory of messages or parts of messages.

EXAMPLES

– Active network elements such as switches, routers (see Figure 5).

– Communication devices outside the defined communication system (e.g. the Internet or introduced via wireless communication links).

– Multi-path communication (e.g. the Internet).

Figure F.5 shows an example of unintended transmission from memory due to an active network element failing as follows: "queue-jumping" in a revolving memory where the send pointer passes the receive pointer, which will cause emptying/sending of the whole queue of a switch.

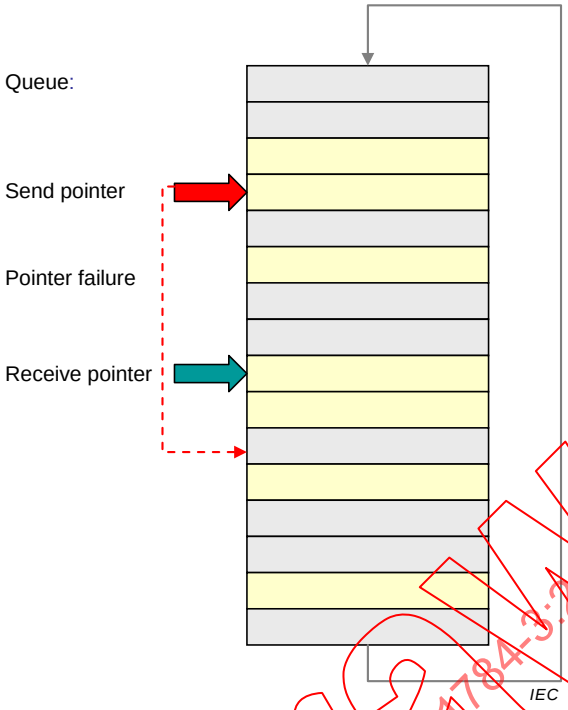


Figure F.5 – Example of an active network element failure

NOTE 2 Black channel can include other types of storage elements than switches.

Several methods are available to detect errors from unintended transmission from memory.

EXAMPLES

– Cyclic communication with monitoring of latencies.
– Synchronized clocks in all devices and time stamping of SPDUs.
– Sufficiently ranged sequence numbering of SPDUs.

In each case, time precision and ranges shall meet the requirements arising from:

- the intended safety application timing issues;
- potential storage of messages inside or outside the system.

The error rate for time bases exceeding specified safety limits shall be determined during the design and implementation assessments according to IEC 61508.

NOTE 3 Use of a synchronized time base throughout the safety network is part of implementation aspects.

F.8.2 Residual error rate for timeliness (RR_T)

In a safety-related network with message storing elements (see Figure F.5), in accordance with Clause F.4 bullet a), a value of 10^{-3}/h per storing element shall be assumed for the rate of timeliness errors (R_T), unless otherwise specified.

The series of unintended transmission from memory of SPDUs shall be assumed to be not more than 65 000.

F.9 Masquerade

F.9.1 General

The safety property masquerade rejection requires the detection of the following communication error according to Table 1:

- masquerade (see 5.3.8).

In general, non-safety PDUs (masquerade) are more likely to be detected by the SCL since they have to fulfill all the preconditions (Timeliness, Authenticity, and Data Integrity).

F.9.2 Other terms used to calculate residual error rate for masquerade rejection (RR_M)

In accordance with Clause F.4 bullet a), a value of 10^{-3}/h per device shall be assumed for the rate of occurrence for masqueraded safety PDUs (R_m), unless otherwise specified.

F.10 Calculation of the total residual error rates

F.10.1 Based on the summation of the residual error rates

The total residual error rate λ_{SC} for the safety communication channel is the sum of the individual residual error rates RR_T, RR_A, RR_I and RR_M as shown in Equation (F.6).

$$\lambda_{SC} = RR_T + RR_A + RR_I + RR_M \qquad \text{(F.6)}$$

where

λ_{SC} is the total residual error rate per hour for the safety communication channel;

RR_T is the residual error rate per hour for Timeliness (see F.5.2.4);

RR_A is the residual error rate per hour for Authenticity (see F.5.2.3);

RR_I is the residual error rate per hour for Data Integrity (see F.5.2.2);

RR_M is the residual error rate per hour for Masquerade (see F.5.2.5).

The residual error rate of the SCL is calculated from the total residual error rate λ_{SC} of the safety communication channels and the maximum number of logical connections (m) that is permitted in a single safety function as shown in Equation (F.7) and in Figure F.6 and Figure F.7.

$$\lambda_{SCL} = \lambda_{SC} \times m \qquad \text{(F.7)}$$

where

λ_{SCL} is the residual error rate per hour of the SCL;

λ_{SC} is the residual error rate per hour per logical connection (see Equation (F.6));

m is the maximum number of logical connections (m) that is permitted in a single safety function.

NOTE This equation assumes cyclic sampling of SPDUs and assumes the worst case that each safety PDU passed over from the black channel can be erroneous.

The number m of logical connections depends on the individual safety function application. Figure F.6 and Figure F.7 illustrate how this number can be determined.

The figures show the physical connections with possible network components such as repeaters, switches, or wireless links and the logical connections between the subsystems involved in the safety function.

The logical connections can be based on single cast or multicast communications.

Figure F.6 shows an example 1 of an application where m = 4. In this application, all three drives are considered to be hazardous at a single point in time according to the risk analysis.

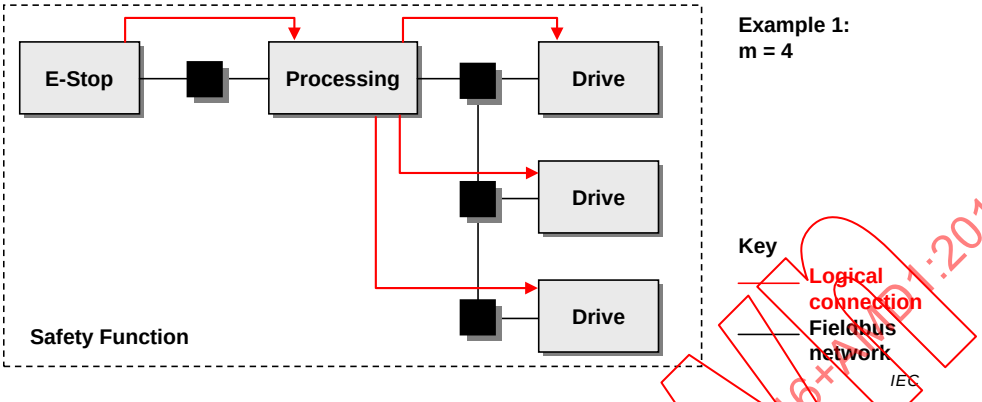


Figure F.6 – Example application 1 (m = 4)

Figure F.7 shows an example 2 of an application where m = 2. In this application, only one of the drives is considered to be hazardous at a single point in time according to the risk analysis.

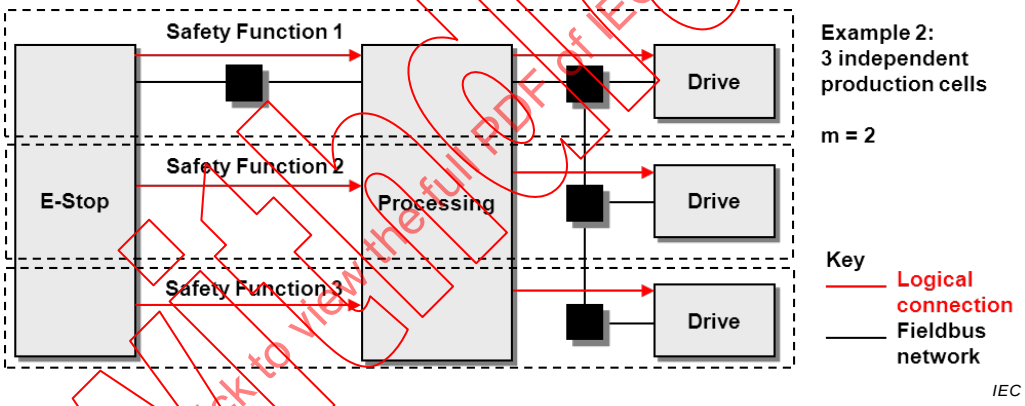


Figure F.7 – Example application 2 (m = 2)

F.10.2 Based on other quantitative proofs

The summation of the residual error rates of the generic safety properties as shown in F.10.1 is an acceptable method to calculate the total residual error rate for a given FSCP.

It is possible to use combined mathematical methods for the calculations taking into account cross effects of the individual safety measures and thus achieve better residual error rates.

It is also possible to use directly the methods of the IEC 61508 and to determine the Safe Failure Fraction and the Diagnostic Coverage of the FSCP.

F.11 Total residual error rate and SIL

A functional safety communication system shall provide a residual error rate in accordance with this standard. Table F.1 and Table F.2 show the typical relationships between residual error rate and SIL, based on the assumption that the functional safety communication system contributes no more than 1 % per logical connection of the safety function.

Both low demand and high demand mode systems shall have a defined safety function response time, so a necessary rate of SPDUs shall be guaranteed. The PFH for a certain SIL shall be provided in all cases, while the PFD_{avg} is optional.

Table F.1 – Typical relationship of residual error rate to SIL

Applicable for safety functions up to SIL	Average frequency of a dangerous failure for the safety function (PFH)	Maximum permissible residual error rate for one logical connection of the safety function (λ_{SC} (Pe))
4	$< 10^{-8}$/ h	$< 10^{-10}$ / h
3	$< 10^{-7}$ / h	$< 10^{-9}$ / h
2	$< 10^{-6}$ / h	$< 10^{-8}$ / h
1	$< 10^{-5}$ / h	$< 10^{-7}$ / h

Table F.2 – Typical relationship of residual error on demand to SIL

Applicable for safety functions up to SIL	Average probability of a dangerous failure on demand for the safety function (PFDavg)	Maximum permissible residual error probability for one logical connection of the safety function
4	$< 10^{-4}$	$< 10^{-6}$
3	$< 10^{-3}$	$< 10^{-5}$
2	$< 10^{-2}$	$< 10^{-4}$
1	$< 10^{-1}$	$< 10^{-3}$

F.12 Configuration and parameterization for an FSCP

F.12.1 General

Correct configuration and parameterization of the safety devices and their SCL during the different phases is essential for functional safety. The engineering of safety functions using an FSCP usually comprises configuration, parameterization, and programming activities as shown in the example of Figure F.8.

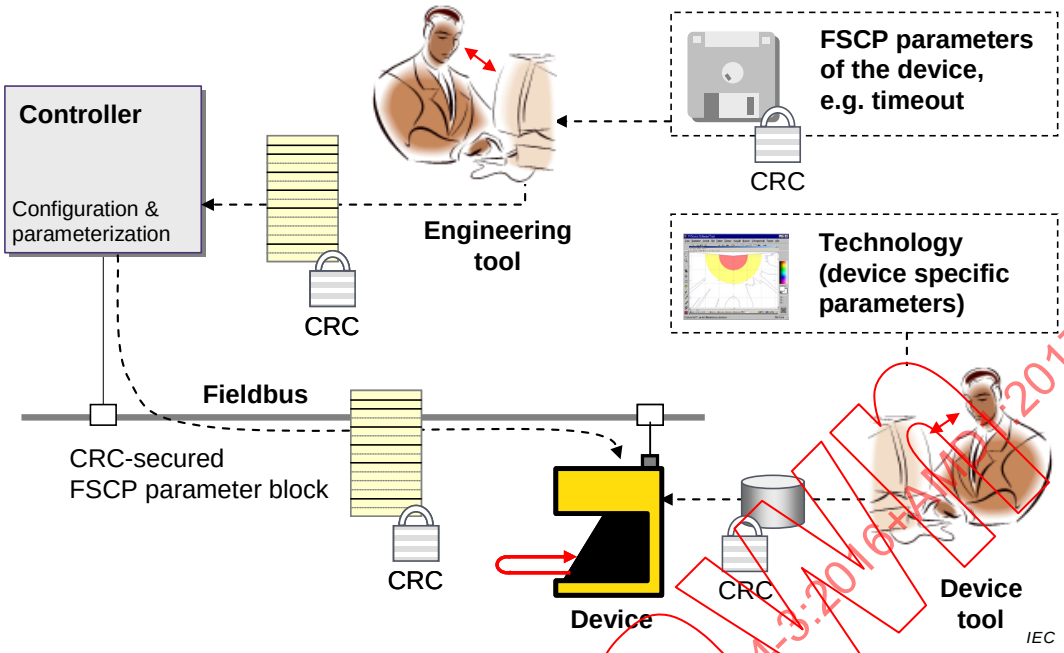


Figure F.8 – Example of configuration and parameterization procedures for FSCP

Configuration requires an engineering tool to set-up the fieldbus network structure, to connect the field devices and to assign values to the black channel layer parameters as well as to the FSCP parameters such as connection authentication, timeout, SIL claim, etc. Usually, the field devices provide a data sheet in electronic form stored within a file that can be imported into the engineering tool.

After a configuration session, the configuration data including parameter values are downloaded to the fieldbus controller to set-up communication. The field device related part of the configuration and parameter data is downloaded to the particular field device prior to cyclic process data exchange.

More complex safety devices may require a dedicated tool for the configuration or parameterization of the technology specific safety device application.

NOTE 1 Relevant information can be found in IEC 62061:2005, 6.11.2.3 and ISO 13849-1:2015, 4.6.4.

NOTE 2 Aspects of incorrect configuration and parameterization include but are not limited to:

– human errors resulting in the entry of incorrect initialization and parameter values;
– data corruption during storage;
– incorrect addressing during download;
– data corruption during download;
– inconsistent update of safety devices;
– connection of identical "safety islands" (serial machines);
– systematic errors while working with engineering tools due to specific computer settings (for example differences between displayed and stored values);
– unrecognized changes within the technology specific safety parameters of the safety device be it stochastic or intentional;
– use of safety devices previously installed in other safety functions.

An FSCP shall specify methods to protect against stochastic errors in the safety configuration and parameters.

EXAMPLES

– Incorrect addressing.

– Data corruption.

– Unrecognized changes.

The above requirements shall be considered by the designer of the FSCP for all relevant communication phases (see 5.6).

Several methods are available to avoid incorrect configuration and parameterization.

EXAMPLES

– CRC signatures across configuration and parameter data.

– Correlation between safety technology parameters and FSCP parameters.

Stochastic configuration and parameterization errors during operation can be prevented by the generic safety measures.

Systematic configuration and parameterization errors can only be safely prevented by verification and validation. The safety manuals shall provide the necessary instructions.

NOTE 3 Relevant information can be found in IEC 62061:2005, 6.11.2.3 and ISO 13849-1:2015, 4.6.4.

F.12.2 Configuration and parameterization change rate

Unless otherwise specified, the configuration and parameterization change rate for calculations shall be assumed as 1 per day.

F.12.3 Residual error rate for configuration and parameterization

The residual error rate RR_{CP} for the stochastic configuration and parameterization errors during onetime operations such as download can be calculated using the residual error probability of the chosen CRC signature (see B.4.2) multiplied by the change rate from F.12.2.

Annex G
(informative)

Implicit data safety mechanisms for IEC 61784-3 functional safety communication profiles (FSCPs)

G.1 Overview

Annex G discusses the concepts of implicit data safety mechanisms for use in functional safety communications protocols (FSCPs) as specified in this standard. Implicit data is that which is not explicitly transmitted in a PDU. Instead, the implicit data values are known by both the sender (source) and the receiver (sink). Implicit data values are validated by the value of one or more transmitted frame check sequence(s) (FCS) which are calculated using an overall data string comprised of the implicit data string appended with the explicit data string. Because the implicit data is not transmitted, the load on the transmission media is reduced.

Today, the FSCPs that use implicit data mechanisms do so in order to communicate complete or partial timeliness codes (T-codes) and/or authenticity codes (A-codes), see Annex E. These FSCPs also use cyclic redundancy check (CRC) algorithms for the frame check sequence (FCS) exclusively. Therefore, Annex G is limited to the analysis of implicitly transmitted T-codes and A-codes using CRC-algorithms.

According to Clause E.8, with regard to implicit data, "Due to the various possible approaches generic formulae cannot be provided. It is up to the individual FSCP to prove sufficient residual error probabilities." In the hope of advancing IEC 61784-3 for the next edition and beyond, the subject of this new Annex G is to improve the understanding of formulating models for the residual error probabilities of FSCPs using CRC-algorithms to implicitly transmit T-codes and A-codes when a single FCS code is used by the protocol.

Presented in Annex G are two formulae examples, applicable for two special cases, and from which a better understanding is promoted for the development of additional (specific and general) formulae.

Also presented is a summation method generally applicable when conditional weight distributions for implicit data error patterns are known and can be quantified in a way either leading to a closed-form solution, or suitable for iterative summation with a reasonably bounded execution time.

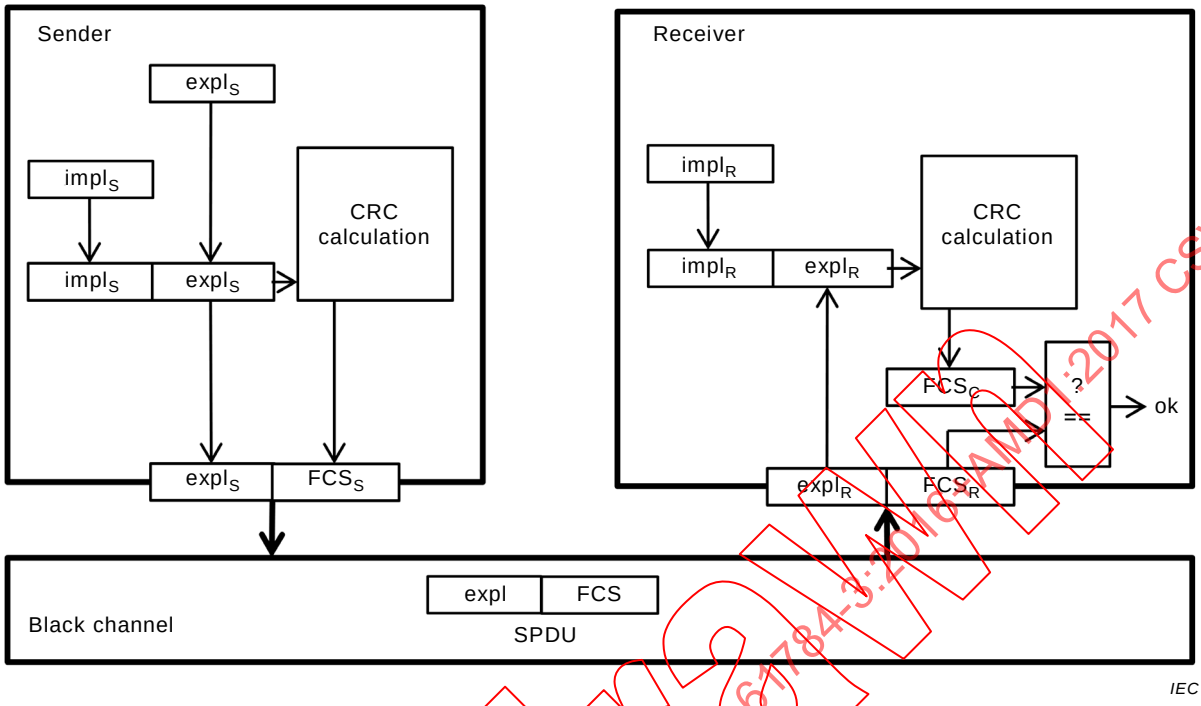
G.2 Basic principles

Calculations in Annex G also use the binary symmetric channel (BSC) model as specified in Annex B.

NOTE 1 Although it does not take into account burst errors, the BSC model with a sufficiently conservative bit error probability is so far the most practical known for use in probability calculations needed for the determination of the FSCP residual error rate.

Figure G.1 shows the basic principle of an FSCP using single FCS protection mechanisms involving implicit data. In the sender, a CRC-checksum over the implicit data $impl_S$ concatenated with the explicit data $expl_S$ is generated, resulting in a frame check sequence FCS_S. When multiple FCS codes are used in an FCSP format, the calculation shall be done for each FCS code. While $expl_S$ and FCS_S are explicitly transmitted over the black channel, $impl_S$ is not transmitted, but impacts the value of the FCS_S. Therefore, it can only contain data whose value is already known to the receiver. Implicit data is used to detect e.g. SPDUs which were misdirected in either space (“authentication error”) or time (“timeliness error”). This is accomplished by deriving the implicit data from the A-code (e.g. connection identifier) and/or the T-code (e.g. sequence number) of an SPDU.

NOTE 2 Initialization details are addressed in F.12.1.



Key Symbols are specified in 3.2.2

Figure G.1 – FSCP with implicit transmission of authenticity and/or timeliness codes

When the SPDU comprising expl and FCS is delivered to the FSCP-layer in the receiver, it may contain transmission errors, i.e. the value delivered may differ from the value sent. For discrimination, the symbols expl$_R$ and FCS$_R$ are used in the receiver.

The expected value of the implicit data is called impl$_R$. In the error free case, this expectation is identical to impl$_S$. In case of, for example, a misdirected SPDU, impl$_R$ and impl$_S$ may differ.

The receiver generates one or more frame check sequence(s) FCS$_C$ by building a CRC-checksum over the concatenation of impl$_R$ and expl$_R$. When each FCS$_C$ is identical to its corresponding FCS$_R$, it is assumed that no error occurred. Otherwise an error has been detected.

The lengths of the bitstrings for a single FCS are defined as follows:

r length of FCS (degree of generator-polynomial);

i length of implicit data (it is assumed that i ≥ r);

e length of explicit data;

n length of SPDU, with n = e + r.

G.3 Problem statement: constant values for implicit data

In FSCPs using implicit data, the CRC-check in the receiver is used for both the detection of data integrity errors as well as the detection of mis-directed or mis-timed SPDUs. Therefore, it may happen that the CRC-mechanism becomes “overburdened” by multiple simultaneous errors, resulting in an increase of the overall residual error probability. This is exemplified in the following scenario in Figure G.2.

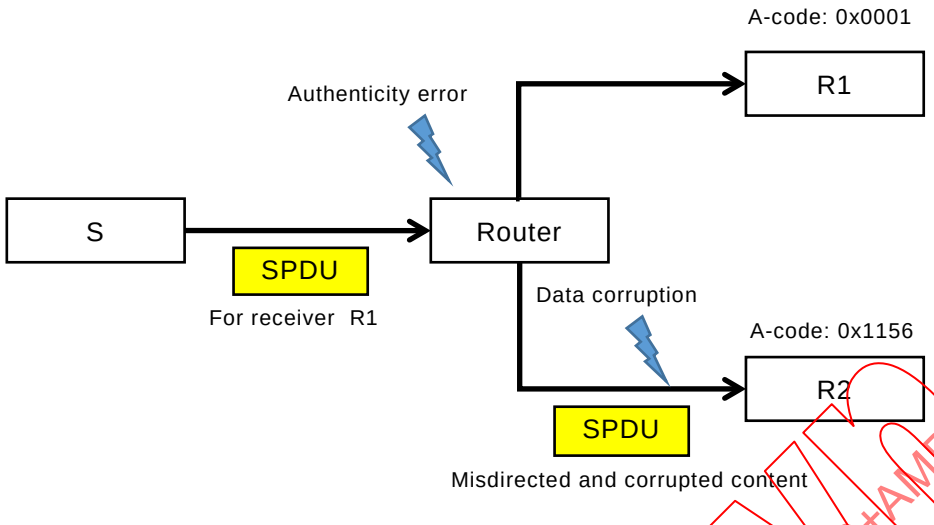


Figure G.2 – Example of an incorrect transmission with multiple error causes

The scenario assumes a sender S sending SPDUs to receiver R1 and receiver R2, using a black channel containing a router. The implicit data used comprises a single field containing an authenticity-code (A-code) of length 16 bits, identifying the receiver (see Figure E.4). For each SPDU sent from S to R1, the A-code of R1 is used as implicit data, and similarly the A-code of R2 for SPDUs sent from S to R2. It is further assumed that the following errors can occur during the transmission of an SPDU.

a) Authenticity error: Due to a fault within the router, the SPDU is delivered to the incorrect receiver (receiver R2 instead of receiver R1 or vice versa). Thus, the implicit authenticity code $impl_S$ used to calculate the FCS_S in the sender is unequal to the expected authenticity code $impl_R$ in the receiver.

b) Data corruption: Due to for example interference or noise on the transmission media, the content of the SPDU is corrupted (expl and/or FCS).

It is further assumed that the black channel itself does not detect any of these errors. Therefore, the errors, and possibly a combination of errors shall be detected by the check within the safety layer of the receiver. The error pattern err_{impl} caused by the authenticity error is defined by the bit-wise exclusive disjunction (XOR) of the A-codes in use. In this case with only two receivers, this error pattern is constant. The error pattern err_{expl} is defined as the bit-wise exclusive disjunction (XOR) of $expl_S$ and $expl_R$. It is modelled by a BSC (see Annex B).

Figure G.3 shows the residual error probabilities for different parameters when using the proper generator polynomial $x^{16}+x^{14}+x^{11}+x^{10}+x^9+x^7+x^5+x^3+x+1$ (0x14EAB) of degree 16.

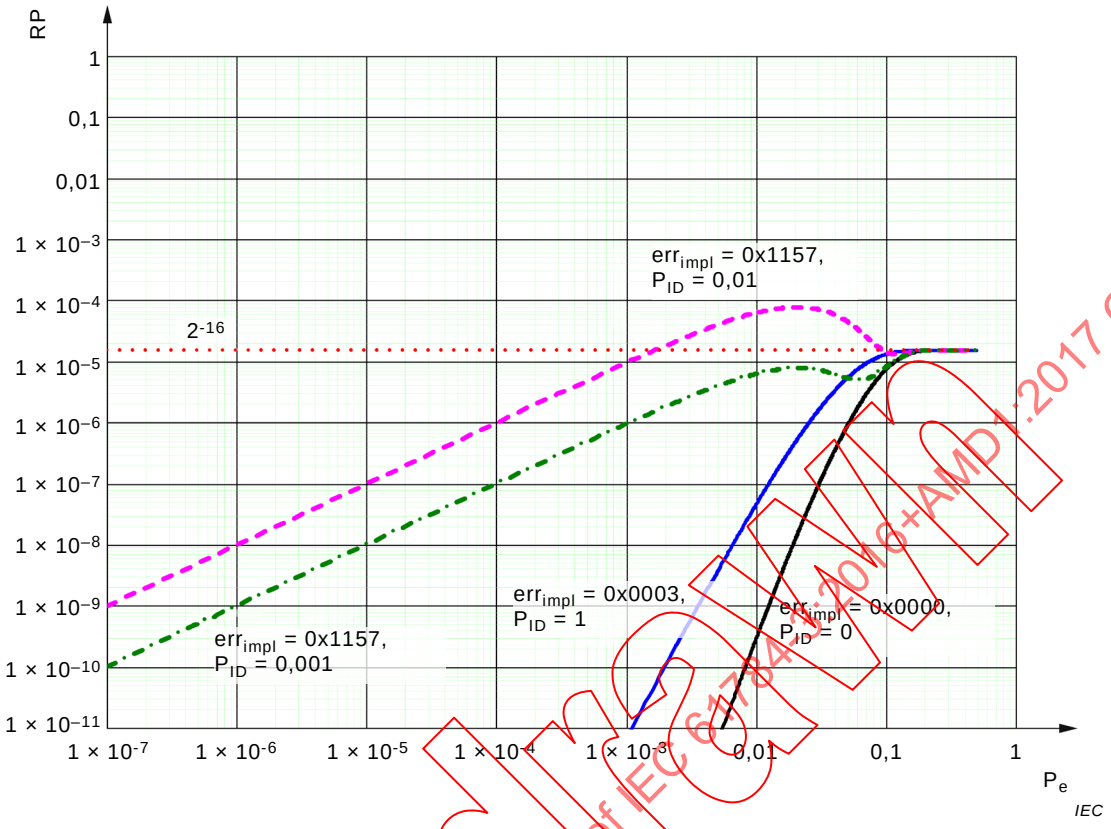


Figure G.3 – Impact of errors in implicit data on the residual error probability

Figure G.3 is based on data which was generated by a brute force algorithm checking all possible error patterns. In addition to the generator polynomial, the following input data was used in the algorithm:

P_{ID} probability of incorrect delivery (here: addressing error);

err_{impl} constant error pattern caused by an addressing error (bitwise disjunction of the A-codes).

It is important to note that the residual error probability does not only depend on p and P_{ID}, but also on the constant err_{impl} and hence on the values of the A-codes chosen during commissioning.

The curve for $P_{ID} = 0$ (solid black) proves the properness of the generator polynomial. In this case of no errors in implicit data, the residual error probability is always below the limit 2^{-16} and the curve is monotonically increasing.

The dashed purple curve and the dotted-dashed green curve show the characteristics when using A-codes resulting in an err_{impl} of 0x1157 (for example the A-codes 0x0001 and 0x1156). The residual error probability is no longer monotonically increasing but has a maximum greater than 2^{-16}. For $P_{ID} = 10^{-3}$, the corresponding curve (dotted-dashed green) does not pass the limit of 2^{-16}. However, if P_{ID} is set to 10^{-2} (dashed purple), the maximum is greater (worse) than the limit 2^{-16}. As a consequence the limit 2^{-r} cannot be used as an approximation even if the generator polynomial has proven properness for the case $P_{ID} = 0$.

The green and purple curve is only observed for certain rare values of err_{impl}. For most other values of err_{impl}, the curves are below the limit even for a probability of occurrence $P_{ID} = 1$. As an example, the curve for err_{impl} = 0x0003 (e.g. A-codes equal to 0x0001 and 0x0002) shows this characteristics (solid blue).

Conclusion: When using implicit transmission mechanisms, the residual error probability is not necessarily bounded by 2^{-r}. This bound is only valid if the FSCP provides additional mechanisms such as the ones shown in the following clauses.

NOTE Improper bounding of an FCS would not necessarily lead to insufficient residual error when other FSCP specific protocol measures are combined in the error detection scheme.

G.4 RP for FSCPs with random, uniformly distributed err_{impl}

G.4.1 General

Clause G.4 investigates the case of a random err_{impl} taking each possible value with equal probability ("uniform distribution"). As seen in Clause G.3 where err_{impl} is constant, this assumption is not always justified and shall be provably guaranteed by the design of the respective FSCP.

As already defined earlier, err_{impl} is the bitwise exclusive disjunction (XOR) between the implicit data $impl_S$ used in the sender of the erroneous packet, and the expected value for the implicit data $impl_R$ in the receiver. Clearly, if $impl_S$ and $impl_R$ are uniformly distributed, independent random variables, also err_{impl} is uniformly distributed, i.e. takes each possible value with equal possibility. However, because errors can be assumed to happen at 'random' points of time, it is also possible to achieve a uniformly distributed err_{impl} if $impl_S$ and $impl_R$ are non-random variables. In order to validate whether err_{impl} follows a uniform distribution, statistical checks such as the Chi-Square-Test or the Kolmogoroff-Smirnoff-Test can be used, (see for example [35]).

NOTE 1 err_{impl} being a uniformly distributed random variable, it does not require that all possible values are observed with equal frequency during a finite interval of time. It is therefore not always possible to evaluate a random number generator by simply counting the number of occurrences within a limited time interval.

Depending on the design of the FSCP, there are two reasonable variants of the assumption "err_{impl} is uniformly distributed":

a) err_{impl} takes each value out of $[0;2^i-1]$ with probability 2^{-i};

b) err_{impl} takes each value out of $[1;2^i-1]$ with probability $1/(2^i-1)$.

NOTE 2 There is a slight difference in the two variants: in the second variant, a value of $err_{impl} = 0$ means that the SPDU was delivered correctly, as an incorrectly delivered SPDU will always result in a value $err_{impl} \neq 0$. In the first variant, a value of $err_{impl} = 0$ does not necessarily imply a correct delivery.

In the second case, measures shall be implemented to ensure that each SPDU is assigned a unique value for implicit data. Hence, the error pattern in case of a misdirected SPDU can never become zero. In the first case, no such measures are implemented and hence the error pattern 'zero' may occur. Clearly, such an error cannot be detected in the receiver unless there are additional detectable data integrity errors or other FSCP specific checks.

In the following, the two variants are shown separately.

Other and perhaps more detailed models are beyond the scope of this document. For example, it is possible to eliminate data error patterns with demonstrated certainty of detection by the CRC polynomial.

EXAMPLE Examples of these data error patterns include: Hamming distances less than the minimum Hamming distance for the CRC polynomial over the data block length; burst errors of length r; odd number of bit errors; and others.

Subclause G.4.2 shows an example where the implicit data field is at least as long as the FCS and the implicit data values are randomly generated in such a way that A-codes are not guaranteed unique for each endpoint, T-codes are not guaranteed unique for each SPDU time, and the combinations of A-code and T-code are not guaranteed unique.

Subclause G.4.3 shows an example where the implicit data field is exactly as long as the FCS and A-codes and T-codes are guaranteed unique for each endpoint and SPDU time. In actual application, additional terms may be necessary to account for exceptions such as T-code wrap around.

Clause G.5 shows a summation method for general applicability when conditional weight distributions for implicit data error patterns are known and can be quantified.

G.4.2 Uniform distribution within the interval [0;2^i-1], i ≥ r

This case applies in particular to FSCPs that use random number generators to derive implicit data values.

At a coarse-grained level, two main types of errors can be discriminated:

- Incorrect content of an SPDU, i. e. data integrity errors;
- Incorrect delivery of an SPDU, i.e. the SPDU is delivered to the wrong receiver or at the wrong instance of time.

In combination, the following disjoint cases can be discriminated:

- Case 1. CC: No error (correct delivery, and correct explicit data);
- Case 2. IC: Incorrect delivery, and correct explicit data;
- Case 3. CI: Correct delivery, and incorrect explicit data;
- Case 4. II: Incorrect delivery, and incorrect data.

The residual error probabilities RP_2, RP_3, and RP_4 for each of the cases 2, 3, and 4 are calculated from the following parameters:

P_{ID} is the "probability of incorrect delivery", i.e. the probability that due to for example an authenticity or timeliness error an SPDU is erroneously delivered to the FSCP;

NOTE 1 The event "incorrect delivery" can result in an $err_{impl} \neq 0$. However, due to the uniform distribution within [0;2^r-1] the case $err_{impl} = 0$ can also occur.

P_{IED} is the probability of incorrect explicit data, i.e. the probability that data corruption occurs;

P_{IC} is the probability that an error is not detected in the receiver under the condition that case 2 occurs;

P_{CI} is the probability that an error is not detected in the receiver under the condition that case 3 occurs;

P_{II} is the probability that an error is not detected in the receiver under the condition that case 4 occurs;

RP_I is the residual error probability for data corruption as defined in Annex F.

R_{CRC} is the residual error probability for CRC polynomials as defined in Equation B.3.

NOTE 2 $RP_I \leq R_{CRC}$ because other safety measures than CRC can further reduce the value of RP_I.

r is the length of the FCS, identical to the degree of the CRC polynomial;

i is the length of the implicit data, with i ≥ r;

n is the number of bits of the SPDU.

Because the events IC, CI, and II are disjoint, the overall residual error probability can be obtained by building the sum of the respective RP_x values.

In general, RP_x is calculated by:

RP_x = P("error case x takes place") × P("error case x is not detectable").

This leads to the formulae for cases 2, 3 and 4 detailed in the following paragraphs.

Case 2 (IC)

$RP_2 = P_{ID} \times (1 - P_{IED}) \times P_{IC}$
$= P_{ID} \times (1 - P_{IED}) \times 2^{-r}$

Explanations on P_{IC}:

- If i > r, this probability is 2^{-r}, because
  - by assumption, the bitwise disjunction of $impl_S$ and $impl_R$ is uniformly distributed in the interval $[0;2^i-1]$;
  - therefore, the bitwise disjunction of $FCS_S = FCS_R$ and FCS_C is uniformly distributed in the interval $[0;2^r-1]$;
  - therefore, the probability that the bitwise disjunction of FCS_R and FCS_C equals zero is 2^{-r};
  - therefore, the probability that FCS_R is equal to FCS_C is 2^{-r}.
- If i = r, this probability is 2^{-r}, because
  - FCS_R is equal to FCS_C, if and only if $err_{impl} = 0$, because the length of err_{impl} does not exceed the degree of the CRC polynomial. CRC-codes detect all burst errors of length less than or equal to r;
  - the probability that $err_{impl} = 0$ is 2^{-r} because of the uniform distribution in the interval $[0;2^r-1]$.

Case 3 (CI)

$RP_3 = (1-P_{ID}) \times P_{IED} \times P_{CI}$
$= (1-P_{ID}) \times RP_I$
$\leq (1-P_{ID}) \times 2^{-r}$ for proper polynomials.

Case 4 (II)

$RP_4 = P_{ID} \times P_{IED} \times P_{II}$
$= P_{ID} \times P_{IED} \times 2^{-r}$

Explanations:

- Due to the assumptions, err_{impl} takes all values from $[0;2^i-1]$ with equal probability.
- Hence, each bit of err_{impl} takes the value 0 or 1 with equal probability 0,5.
- Because CRC-codes are linear codes, and because $|err_{impl}| \geq r$, each bit of err_{impl} determines the result of one bit in the bitwise exclusive disjunction of FCS_R and FCS_C.
- Hence, the bits in the bitwise exclusive disjunction of FCS_R and FCS_C can be treated as independent random variables, each taking the values 0 and 1 with equal probability 0,5.
- The bitwise exclusive disjunction of FCS_R and FCS_c is a uniformly distributed random variable, taking all values from $[0;2^r-1]$ with equal probability.
- The probability that the bitwise exclusive disjunction of FCS_R and FCS_C equals zero is 2^{-r}.
- The probability that FCS_C is identical to FCS_R is 2^{-r}.

In summary, the residual error probability of an FSCP using implicit mechanisms for the detection of timeliness and authenticity error (guaranteeing that the error in the implicit data is uniformly distributed in the interval $[0;2^i-1]$ can be calculated using the following formula:

$$RP_{TOTAL} = RP2 + RP3 + RP4$$
$$= (P_{ID} \times (1 - P_{IED}) \times 2^{-r}) + ((1-P_{ID}) \times P_{IED} \times P_{CI}) + (P_{ID} \times P_{IED} \times 2^{-r})$$
$$= (P_{ID} \times 2^{-r}) + ((1-P_{ID}) \times P_{IED} \times P_{CI})$$
$$= (P_{ID} \times 2^{-r}) + ((1-P_{ID}) \times RP_I)$$

Explanation:

- Cases 2 to 4 are disjoint events.

In case of a proper polynomial, the following applies:

$$RP_{TOTAL} = RP2 + RP3 + RP4$$
$$= (P_{ID} \times (1 - P_{IED}) \times 2^{-r}) + ((1-P_{ID}) \times P_{IED} \times P_{CI}) + (P_{ID} \times P_{IED} \times 2^{-r})$$
$$\leq (P_{ID} \times (1 - P_{IED}) \times 2^{-r}) + ((1-P_{ID}) \times 2^{-r}) + (P_{ID} \times P_{IED} \times 2^{-r})$$
$$\leq 2^{-r}$$

Explanations:

- Cases 2 to 4 are disjoint events.
- This upper bound of RP_{TOTAL} is independent of the values of P_{IED} and P_{ID}.

G.4.3 Uniform distribution in the interval [1;2^r-1], i = r

For this variant, it is assumed i = r, i.e. the length of the implicit data is exactly the degree of the CRC polynomial, and that err_{impl} is uniformly distributed within the interval [1;2^r-1]. In contrast to the variant shown in G.4.2, err_{impl} is always unequal to 0 in case of an incorrect delivery.

The following cases of error combinations can be discriminated:

- Case 1. CC: No error (correct delivery, and correct explicit data);
- Case 2. IC: Incorrect delivery, and correct explicit data;
- Case 3. CI: Correct delivery, and incorrect explicit data;
- Case 4. II: Incorrect delivery, and incorrect data.

The residual error probabilities RP_2, RP_3, and RP_4 for each of the cases 2, 3, and 4 are calculated from the following parameters:

P_{ID} is the "probability of incorrect delivery", i.e. the probability that due to for example an authenticity or timeliness error an SPDU is erroneously delivered to the FSCP;

NOTE Due to the uniform distribution within [1;2^r-1], $err_{impl} \neq 0$ is guaranteed. Hence, the event "incorrect delivery" is equivalent to the event "incorrect implicit data" in this case.

P_{IED} is the probability of incorrect explicit data, i.e. the probability that data corruption occurs;

P_{IC} is the probability that an error is not detected in the receiver under the condition that case 2 occurs;

P_{CI} is the probability that an error is not detected in the receiver under the condition that case 3 occurs;

P_{II} is the probability that an error is not detected in the receiver under the condition that case 4 occurs;

$P_{EIC}(i)$ is the probability that the error pattern in the explicit data err_{expl} complements the error pattern in the implicit data err_{impl} making the error undetectable, under the condition that "err_{impl} = i";

r is the length of the implicit data and the length of the FCS (degree of the CRC polynomial);

n is the number of bits in the SPDU.

Because the events IC, CI, and II are disjoint, the overall residual error probability can be obtained by building the sum of the respective RP_x values.

In general, RP_x is calculated by:

RP_x = P("error case x takes place") × P("error case x is not detectable").

This leads to the formulae for cases 2, 3 and 4 detailed in the following paragraphs.

Case 2 (IC)

$RP_2 = P_{ID} \times (1 - P_{IED}) \times P_{IC}$

$= 0$

Explanation:

- Errors of type 2 are always detected, because the length of err_{impl} does not exceed r. CRC-codes detect all burst errors of length less than or equal to r. Hence P_{IC} is equal to 0 in this case.

Case 3 (CI)

$RP_3 = (1-P_{ID}) \times P_{IED} \times P_{CI}$

$= (1-P_{ID}) \times RP_I$

$\leq (1-P_{ID}) \times 2^{-r}$ for proper polynomials.

Case 4 (II)

$RP_4 = P_{ID} \times P_{IED} \times P_{II}$

$\approx P_{ID} \times P_{IED} \times 2^{-r}$

Explanations:

- $P_{II} = \sum_{i=1}^{2^r-1} P\{err_{impl} = i\} \times P_{EIC}(i)$

$= \sum_{i=1}^{2^r-1} \frac{1}{2^r-1} \times P_{EIC}(i)$

$= \frac{1}{2^r-1} \times \sum_{i=1}^{2^r-1} P_{EIC}(i)$

$= \frac{1}{2^r-1}$ (because for all possible err_{expl} there is exactly one matching err_{impl})

$\approx 2^{-r}$

In summary, the residual error probability of an FSCP using implicit mechanisms for the detection of timeliness and authenticity error guaranteeing that the error in the implicit data is uniformly distributed in the interval $[1;2^r-1]$, can be calculated using the following formula:

RP_{TOTAL} = RP2 + RP3 + RP4

$= (P_{ID} \times (1 - P_{IED}) \times 2^{-r}) + ((1-P_{ID}) \times P_{IED} \times P_{CI}) + (P_{ID} \times P_{IED} \times 2^{-r})$

$= (P_{ID} \times 2^{-r}) + ((1-P_{ID}) \times P_{IED} \times P_{CI})$

$= (P_{ID} \times 2^{-r}) + ((1-P_{ID}) \times RP_I)$

Explanation:

- Cases 2 to 4 are disjoint events.

G.5 General case

The calculations presented in G.4.2 and G.4.3 are only valid under the assumption of a uniform distribution of err_{impl} and with certain restrictions on the length of the implicit data field. In the general case, RP_{TOTAL} can be calculated as follows, if the conditional weight distribution of the code is known for each possible value of err_{impl}.

$$RP_{TOTAL} = P_{ID} \times \sum_{j=0}^{2^i-1} P\{ err_{impl} = j\} \times P\{ FCS_C = FCS_R \mid err_{impl} = j\} + (1-P_{ID}) \times P_{re}^{CRC, BSC}$$

where

$P\{ err_{impl} = j\}$ is the probability that the error pattern in implicit data has the value j (under the condition that there is a misdirected SPDU);

$P\{ FCS_C = FCS_R \mid err_{impl} = j\}$ is the probability that no error is indicated for the given CRC-polynomial and code length, under the condition that the error pattern in implicit data has the value j;

$P_{re}^{CRC, BSC}$ is the residual error probability for the given CRC-polynomial and code length without implicit data.

$P_{re}^{CRC, BSC}$ and $P\{ FCS_C = FCS_R \mid err_{impl} = j\}$ are given by:

$$P_{re}^{CRC,BSC} = \sum_{k=1}^{n} A_k(err_{impl} = 0) \times P_e^k \times (1-P_e)^{n-k}$$

$$P\{ FCS_C = FCS_R \mid err_{impl} = j\} = \sum_{k=0}^{n} A_k(err_{impl} = j) \times P_e^k \times (1-P_e)^{n-k}$$

where

$A_k(err_{impl} = j)$ is the weight distribution of the code under the condition that the error pattern in the implicit data takes the value j.

Explanations:

- $P\{ FCS_C = FCS_R \mid err_{impl} = 0\} = P_{re}^{CRC, BSC} + (1-P_e)^n$.

G.6 Calculation of P_{ID}

If both the T-code and the A- code are implicit, P_{ID} can be calculated as follows:

$$P_{ID} = \min\left(\frac{R_T + R_A}{\nu}, 1\right)$$

where

P_{ID} is the probability that due to for example an authenticity or timeliness error an SPDU is erroneously delivered to the FSCP;

R_T is the rate of occurrence for incorrect sequence safety PDUs (see F.5.2.4);

R_A is the rate of occurrence for misdirected safety PDUs (see F.5.2.3);

v is the maximum number of SPDU samples by the SCL ("sample rate") per hour (see F.5.2.2).

Explanation:

- Due to approximation, $R_T + R_A$ may become greater than one. In this case, the value 1 shall be used for P_{ID}.

If only the T-code is implicit, P_{ID} can be calculated as follows:

$$P_{ID} = \frac{R_T}{v}$$

If only the A-code is implicit, P_{ID} can be calculated as follows:

$$P_{ID} = \frac{R_A}{v}$$

Calculation of the total residual error rate

According to F.10.1, the total residual error rate is calculated by (see Equation (F.6)):

$$\lambda_{SC} = RR_T + RR_A + RR_I + RR_M$$

Alternatively, the following formula can be used:

$$\lambda_{SC} = v \times RP_{TOTAL}$$

Bibliography

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

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

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

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

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

[5] IEC 61131-2:2007, *Programmable controllers – Part 2: Equipment requirements and tests*

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

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

[8] IEC 61496-1, *Safety of machinery – Electro-sensitive protective equipment – Part 1: General requirements and tests*

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

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

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

[12] IEC 61784-4[18], *Industrial communication networks – Profiles – Part 4: Secure communications for fieldbuses*

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

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

[15] IEC 62061:2005, *Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems*

[18] Proposed new work item under consideration.

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

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

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

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

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

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

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

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

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

[25] ISO 13849-1:2015, *Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design*

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

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

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

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

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

[31] J. WOLF, A. MICHELSON, A. LEVESQUE, *On the probability of undetected error for linear block codes*, February 1982, IEEE Transactions on Communications, Volume 30, Issue 2

[32] S. LEUNG-YAN-CHEONG AND M. HELLMAN, *Concerning a bound on undetected error probability*, March 1976, IEEE Transactions on Information Theory, Volume 22, Issue 2

[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, Issue 6

[35] D. KNUTH, *The Art of Computer Programming, Volume 2: Seminumerical Algorithms*, 3rd Edition, Addison-Wesley, 1997

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

RÉSEAUX DE COMMUNICATION INDUSTRIELS – PROFILS –

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

AVANT-PROPOS

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

Cette version consolidée de la Norme IEC officielle et de son amendement a été préparée pour la commodité de l'utilisateur.

L'IEC 61784-3 édition 3.1 contient la troisième édition (2016-05) [documents 65C/840/FDIS et 65C/848/RVD] et son amendement 1 (2017-08) [documents 65C/879/FDIS et 65C/886/RVD].

Dans cette version Redline, une ligne verticale dans la marge indique où le contenu technique est modifié par l'amendement 1. Les ajouts sont en vert, les suppressions sont en rouge, barrées. Une version Finale avec toutes les modifications acceptées est disponible dans cette publication.

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

Cette troisième édition constitue une révision technique.

Cette édition inclut les modifications techniques majeures suivantes par rapport à l'édition précédente:

- clarifications et explications complémentaires des exigences, références actualisées;
- suppression des présentations techniques de profils (Articles 6 à 13) et paragraphes dédiés associés à des termes, définitions, symboles et abréviations;
- ajout de profils pour les familles de profils de communication 8, 17 et 18 (Articles 10, 14, 15);
- clarifications des modèles de l'Annexe A;
- modification de l'Annexe B informative qui devient normative;
- ajout d'une nouvelle Annexe E informative pour décrire les modèles des mécanismes FSCP explicites et implicites;
- ajout d'une nouvelle Annexe F informative qui introduit un modèle étendu pour l'estimation du taux total d'erreurs résiduelles;
- actualisations des parties pour les CPF 1, CPF 2, CPF 3, CPF 8, CPF 13 (détails fournis dans les parties);
- ajout d'une nouvelle partie pour CPF 17.

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

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

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

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

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

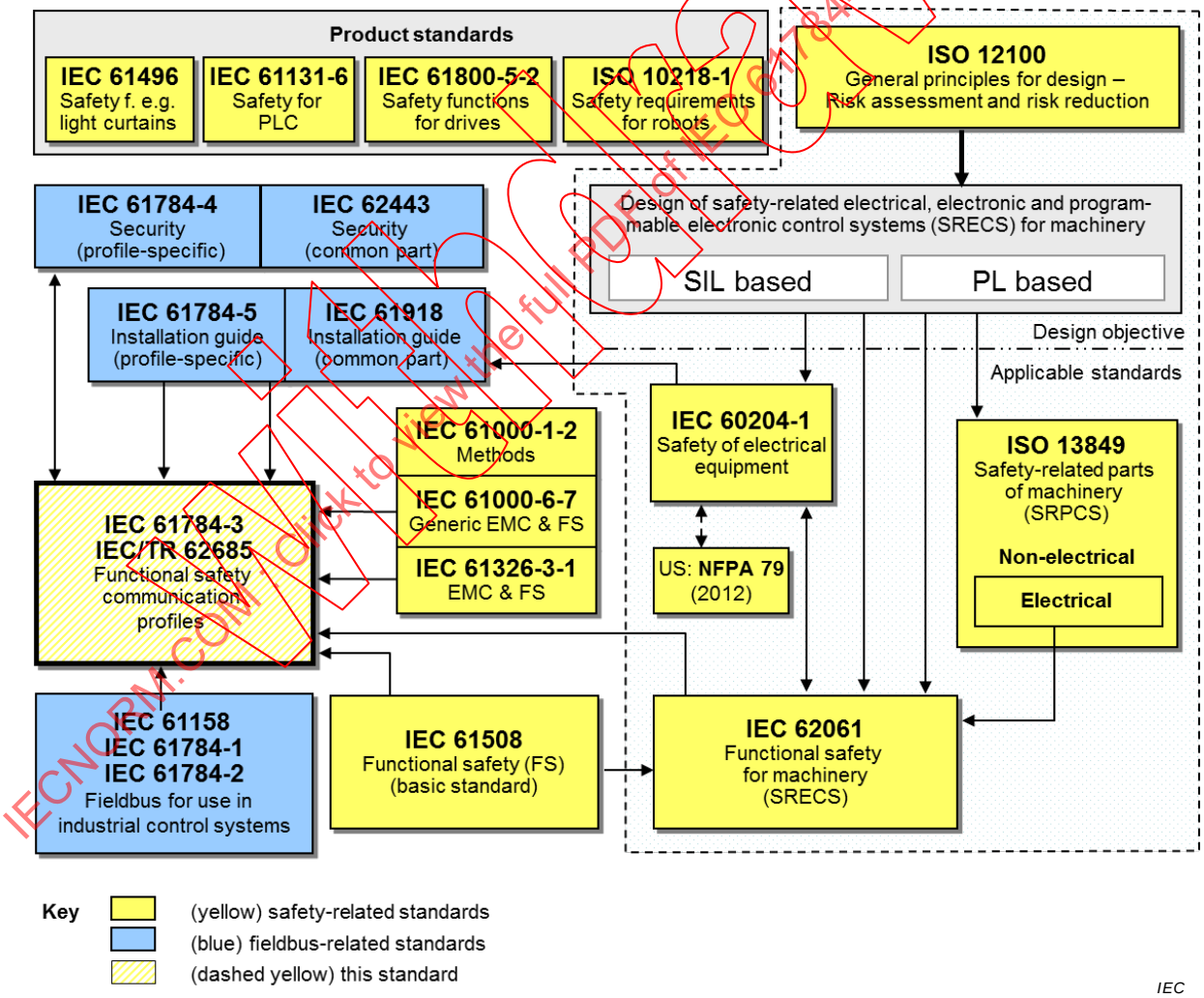
0 Introduction

0.1 Généralités

L'IEC 61158, relative aux bus de terrain, ainsi que ses normes associées IEC 61784-1 et IEC 61784-2, définit un ensemble de protocoles de communication qui assurent la commande répartie d'applications automatisées. La technologie de bus de terrain est désormais reconnue et bien éprouvée. Les améliorations des bus de terrain se poursuivent; elles couvrent des applications pour des domaines comme les applications en temps réel relatives à la sécurité et à la sûreté.

Cette norme définit les principes applicables aux communications de sécurité fonctionnelle en référence à la série IEC 61508; elle spécifie plusieurs couches de communication de sécurité (profils et protocoles correspondants) en fonction des profils de communication et des couches de protocole de l'IEC 61784-1, l'IEC 61784-2 et de la série IEC 61158. Elle ne couvre pas les aspects relatifs à la sécurité électrique et à la sécurité intrinsèque.

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

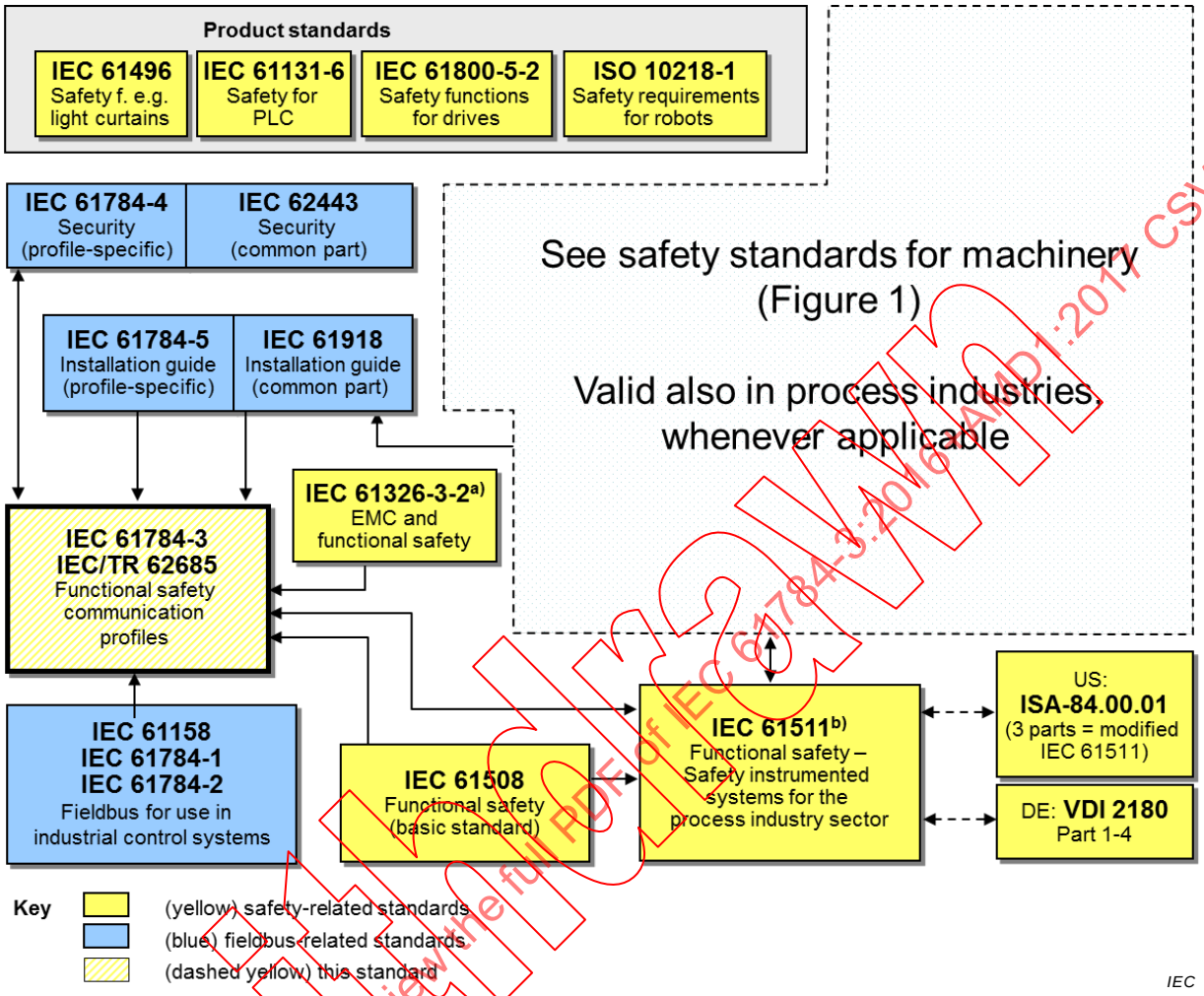


Anglais	Français
Product standards	Normes de produits
Safety function, e.g. light curtains	Fonction de sécurité, par exemple rideaux de lumière
Safety for PLC	Sécurité relative aux automates programmables
Safety functions for drives	Fonctions de sécurité applicables aux entraînements
Safety requirements for robots	Exigences de sécurité applicables aux robots
General principles for design – Risk assessment and risk reduction	Principes généraux de conception – Appréciation du risque et réduction du risque
Security (profile-specific)	Sécurité (spécifique au profil)
Security (common part)	Sécurité (partie commune)
Design of safety-related electrical, electronic and programmable electronic control systems (SRECS) for machinery	Conception des systèmes de commande électriques, électroniques et électroniques programmables relatifs à la sécurité pour les machines
SIL based	Basé sur SIL
PL based	Basé sur PL
Installation guide (profile-specific)	Guide d'installation (spécifique au profil)
Installation guide (common part)	Guide d'installation (partie commune)
Design objective	Objectif de conception
Applicable standards	Normes applicables
Methods	Méthodes
Generic EMC & FS	CEM & FS génériques
EMC & FS	CEM & FS
Safety of electrical equipment	Sécurité des équipements électriques
Safety-related parts of machinery	Sécurité des machines – Parties des systèmes de commande relatives à la sécurité
Non-electrical	Non électrique
Electrical	Electrique
Functional safety communication profiles	Profils de communication de sécurité fonctionnelle
Fieldbus for use in industrial control systems	Bus de terrain pour utilisation dans des systèmes de commande industriels
Functional safety (FS) (basic standard)	Sécurité fonctionnelle (FS) (norme de base)
Functional safety for machinery	Sécurité fonctionnelle des machines
Key	Légende
(yellow) safety-related standards	(jaune) normes relatives à la sécurité
(blue) fieldbus-related standards	(bleu) normes relatives au bus de terrain
(dashed yellow) this standard	(jaune pointillé) la présente norme

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

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

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



Anglais	Français
Product standards	Normes de produits
Safety function, e.g. light curtains	Fonction de sécurité, par exemple rideaux de lumière
Safety for PLC	Sécurité relative aux automates programmables
Safety functions for drives	Fonctions de sécurité applicables aux entraînements
Safety requirements for robots	Exigences de sécurité applicables aux robots
Security (profile-specific)	Sûreté (spécifique au profil)
Security (common part)	Sûreté (partie commune)
Installation guide (profile-specific)	Guide d'installation (spécifique au profil)
Installation guide (common part)	Guide d'installation (partie commune)
See safety standards for machinery (Figure 1)	Voir normes de sécurité pour les machines (Figure 1)
Valid also in process industries, whenever applicable	Valable également dans les industries de transformation, le cas échéant
Functional safety communication profiles	Profils de communication de sécurité fonctionnelle
EMC and functional safety	CEM et sécurité fonctionnelle
Fieldbus for use in industrial control systems	Bus de terrain pour utilisation dans des systèmes de commande industriels
Functional safety (basic standard)	Sécurité fonctionnelle (norme de base)

Anglais	Français
Functional safety–safety instrumented systems for the process industry sector	Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur des industries de transformation
3 parts = modified IEC 61511	3 parties = IEC 61511 modifiée
Part 1 – 4	Parties 1 à 4
Key	Légende
(yellow) safety-related standards	(jaune) normes relatives à la sécurité
(blue) fieldbus-related standards	(bleu) normes relatives au bus de terrain
(dashed yellow) this standard	(jaune pointillé) la présente norme

[a] Pour des environnements électromagnétiques spécifiés; sinon, l'IEC 61326-3-1 ou l'IEC 61000-6-7.

[b] EN ratifiée.

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

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

Les couches de communication de sécurité spécifiées dans la présente norme permettent de garantir cette assurance de sorte qu'un bus de terrain puisse être utilisé dans des applications qui nécessitent une sécurité fonctionnelle jusqu'au niveau d'intégrité de sécurité (SIL) spécifié par son profil de communication de sécurité fonctionnelle correspondant.

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

La présente norme décrit:

- les principes de base de la mise en œuvre des exigences de la série IEC 61508 pour les communications de données relatives à la sécurité, y compris les anomalies de transmission potentielles, les mesures correctives et des considérations relatives à l'intégrité des données;
- les profils de communication de sécurité fonctionnelle pour plusieurs familles de profils de communication dans les IEC 61784-1 et IEC 61784-2, y compris les extensions de la couche de sécurité aux sections relatives au service et aux protocoles de communication de la série IEC 61158.

0.2 Transition de l'édition 2 aux méthodes d'évaluation étendue de l'édition 3

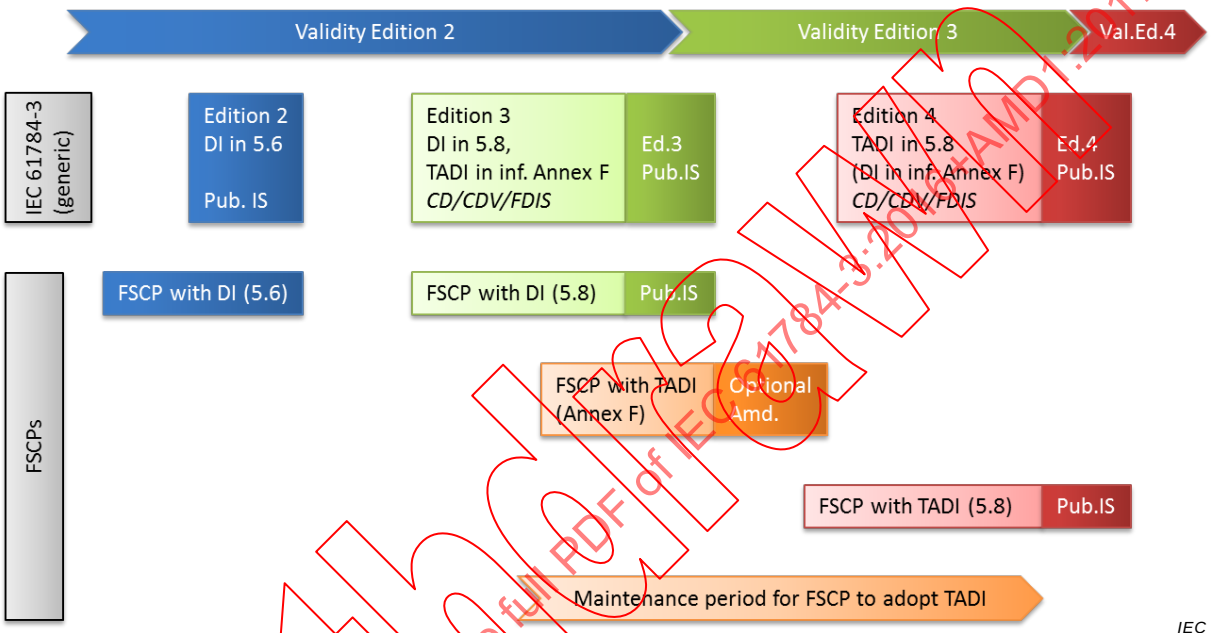
Cette édition de la partie générique de la norme comprend des modèles étendus supplémentaires pour une utilisation ultérieure lors de l'estimation du taux total d'erreurs résiduelles pour un FSCP. Cette valeur peut être utilisée pour déterminer si le FSCP satisfait aux exigences des applications de sécurité fonctionnelle jusqu'à un SIL donné. Ces modèles étendus pour les méthodes qualitatives et quantitatives de détermination de sécurité sont détaillés à l'Annexe E et à l'Annexe F.

Toutefois, en raison de la durée typique du processus d'évaluation, les Profils de Communication de Sécurité Fonctionnelle publiés avant ou en même temps que cette nouvelle édition de la partie générique ne peuvent être évalués qu'en fonction des méthodes

des éditions précédentes, sur la base des considérations relatives à l'intégrité des données détaillées en 5.8.

Le schéma de validité de la Figure 3 présente le procédé de gestion de la transition des méthodes d'évaluation d'origine de l'édition 2 (détaillé en 5.8) aux méthodes d'évaluation étendue de l'édition 3 (actuellement spécifiées à l'Annexe F). Conformément à ce schéma, les Profils de Communication de Sécurité Fonctionnelle sont exemptés d'une nouvelle évaluation conformément à l'Annexe F jusqu'à l'édition 4, lorsque le contenu de l'Annexe F actuelle remplacera le 5.8 actuel.

NOTE Un FSCP peut cependant réaliser une évaluation antérieure et publier un amendement approprié.



Anglais	Français
Validity edition	Edition de validité
(generic)	(générique)
DI in ...	DI en ...
... in inf. Annex F	... à l'Annexe F inf.
... with DI	... avec DI
... with TADI	... avec TADI
Optional amd.	Amd. facultatif
Maintenance period for FSCP to adopt TADI	Période de maintenance permettant au FSCP d'adopter TADI

Légende

DI Data Integrity (Intégrité des données)

TADI Timeliness, Authenticity, Data Integrity (Opportunité, Authenticité, Intégrité des données)

Figure 3 – Transition de l'édition 2 aux méthodes d'évaluation de l'édition 3

0.3 Déclaration de brevet

La commission électrotechnique internationale (IEC) attire l'attention sur le fait qu'il est déclaré que la conformité aux dispositions du présent document peut impliquer l'utilisation de brevets qui intéressent les profils de communication de sécurité fonctionnelle pour les familles 1, 2, 3, 6, 8, 12, 13, 14, 17 et 18 de l'IEC 61784-3-1, l'IEC 61784-3-2,

l'IEC 61784-3-3, l'IEC 61784-3-6, l'IEC 61784-3-8, l'IEC 61784-3-12, l'IEC 61784-3-13, l'IEC 61784-3-14, l'IEC 61784-3-17 et l'IEC 61784-3-18.

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

Les détenteurs de ces droits de propriété ont donné l'assurance à l'IEC qu'ils consentent à négocier des licences avec des demandeurs du monde entier, sans frais ou à des termes et conditions raisonnables et non discriminatoires. A ce propos, les énoncés des détenteurs de ces droits de propriété sont enregistrés à l'IEC.

NOTE Les détails relatifs aux brevets et les informations relatives aux coordonnées correspondantes sont fournis dans l'IEC 61784-3-1, l'IEC 61784-3-2, l'IEC 61784-3-3, l'IEC 61784-3-6, l'IEC 61784-3-8, l'IEC 61784-3-12, l'IEC 61784-3-13, l'IEC 61784-3-14, l'IEC 61784-3-17 et l'IEC 61784-3-18.

L'attention est attirée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété intellectuelle autres que ceux identifiés ci-dessus. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et de ne pas avoir signalé leur existence.

L'ISO (www.iso.org/patents) et l'IEC (http://patents.iec.ch) maintiennent à disposition des bases de données en ligne des droits de propriété relatifs à leurs normes. Les utilisateurs sont encouragés à consulter ces bases de données pour obtenir les informations les plus récentes concernant les droits de propriété.

INTRODUCTION à l'Amendement

Le présent Amendement 1 traite des concepts de mécanismes de sécurité reposant sur des données implicites destinés à être utilisés dans les protocoles de communication de sécurité fonctionnelle (FSCP, *functional safety communications protocols*) spécifiés dans l'IEC 61784-3:2016.

RÉSEAUX DE COMMUNICATION INDUSTRIELS – PROFILS –

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

1 Domaine d'application

La présente partie de la série IEC 61784-3 définit des principes communs qui peuvent être appliqués pour la transmission des messages relatifs à la sécurité entre les participants d'un réseau réparti, à l'aide de la technologie de bus de terrain conformément aux exigences de la série IEC 61508[1] sur la sécurité fonctionnelle. Ces principes peuvent s'appuyer sur le principe de canal noir. Ils peuvent être utilisés dans différentes applications industrielles, par exemple la commande de processus, l'usinage automatique et les machines.

La présente partie[2] et les parties IEC 61784-3-x spécifient plusieurs profils de communication de sécurité fonctionnelle basés sur les profils de communication et les couches de protocole des technologies des bus de terrain de l'IEC 61784-1, de l'IEC 61784-2 et de la série IEC 61158. Ces profils de communication de sécurité fonctionnelle utilisent le principe de canal noir, comme défini dans l'IEC 61508. Ces profils de communication de sécurité fonctionnelle sont destinés à être exclusivement mis en œuvre dans des appareils de sécurité.

NOTE 1 Il peut exister d'autres systèmes de communication relatifs à la sécurité qui satisfont aux exigences de la série IEC 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 comme les chocs électriques. La sécurité intrinsèque concerne les dangers associés aux atmosphères explosibles.

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

NOTE 3 Des exigences spécifiques au profil peuvent également être spécifiées dans l'IEC 61784-4[3].

NOTE 4 La mise en œuvre du profil de communication de sécurité fonctionnelle, conforme à la présente partie, dans un appareil normal ne suffit pas à le qualifier d'appareil de sécurité, comme défini dans la série IEC 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 suivants sont cités en référence de manière normative, en intégralité ou en partie, dans le présent document et sont indispensables pour son application. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

---

1 Dans les pages suivantes de la présente norme, "IEC 61508" remplace "série IEC 61508".

2 Dans les pages suivantes de la présente norme, "la présente partie" remplace "cette partie de la série IEC 61784-3".

3 Proposition d'un nouveau sujet de travail à l'étude.

IEC 61000-6-7, *Compatibilité électromagnétique (CEM) – Partie 6-7: Normes génériques – Exigences d'immunité pour les équipements visant à exercer des fonctions dans un système lié à la sécurité (sécurité fonctionnelle) dans des sites industriels*

IEC 61010-2-201:2013, *Règles de sécurité pour appareils électriques de mesurage, de régulation et de laboratoire – Partie 2-201: Exigences particulières pour les équipements de commande*

IEC 61158 (toutes les parties), *Réseaux de communication industriels – Spécifications des bus de terrain*

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

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

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

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

IEC 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, *Réseaux de communication industriels – Profils – Part 1: Profils de bus de terrain*

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

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

IEC 61784-3-2, *Réseaux de communication industriels – Profils – Partie 3-2: Bus de terrain de sécurité fonctionnelle – Spécifications supplémentaires pour CPF 2*

IEC 61784-3-3, *Réseaux de communication industriels – Profils – Partie 3-3: Bus de terrain de sécurité fonctionnelle – Spécifications supplémentaires pour CPF 3*

IEC 61784-3-6, *Réseaux de communication industriels – Profils – Partie 3-6: Bus de terrain de sécurité fonctionnelle – Spécifications supplémentaires pour CPF 6*

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

IEC 61784-3-12, *Réseaux de communication industriels – Profils – Partie 3-12: Bus de terrain de sécurité fonctionnelle – Spécifications supplémentaires pour CPF 12*

IEC 61784-3-13, *Réseaux de communication industriels – Profils – Partie 3-13: Bus de terrain de sécurité fonctionnelle – Spécifications supplémentaires pour CPF 13*

IEC 61784-3-14, *Réseaux de communication industriels – Profils – Partie 3-14: Bus de terrain de sécurité fonctionnelle – Spécifications supplémentaires pour CPF 14*

IEC 61784-3-17[4], *Réseaux de communication industriels – Profils – Partie 3-17: Bus de terrain de sécurité fonctionnelle – Spécifications supplémentaires pour CPF 17*

IEC 61784-3-18, *Réseaux de communication industriels – Profils – Partie 3-18: Bus de terrain de sécurité fonctionnelle – Spécifications supplémentaires pour CPF 18*

IEC 61784-5 (toutes les parties), *Réseaux de communication industriels – Profils – Partie 5: Installation des bus de terrain*

IEC 61918:2013, *Réseaux de communication industriels – Installation de réseaux de communication dans des locaux industriels*

IEC 62443 (toutes les parties), *Réseaux industriels de communication – Sécurité dans les réseaux et les systèmes*

3 Termes, définitions, symboles, abréviations et conventions

3.1 Termes et définitions

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

NOTE Les italiques sont utilisés dans les définitions pour mettre en évidence les termes définis en 3.1.

3.1.1
date absolue
date référencée par rapport à un temps global, commun à un groupe d'appareils utilisant un *bus de terrain*

[SOURCE: IEC 62280:2014, 3.1.1, modifié – utilisation d'appareils et de bus de terrain]

3.1.2
élément de réseau actif
élément de réseau contenant des composants actifs du point de vue électrique et/ou optique et permettant d'étendre le réseau

Note 1 à l'article: Les répéteurs et les commutateurs sont des exemples d'éléments de réseau actif.

[SOURCE: IEC 61918:2013, 3.1.2]

3.1.3
disponibilité
probabilité, pour un système automatisé, qu'il ne se produise pas de condition opérationnelle non satisfaisante, par exemple la perte de production, pendant une période donnée

3.1.4
probabilité d'erreurs sur les éléments binaires
Pe
probabilité de réception d'un bit donné avec la valeur incorrecte

4 A publier

3.1.5
canal noir
système de communication défini qui contient un ou plusieurs éléments sans preuve de conception ou de validation conformément à l'IEC 61508

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

3.1.6
pont
appareil abstrait qui relie plusieurs segments de réseau le long de la couche de liaison de données

3.1.7
système de communication fermé
nombre fixe ou nombre maximal fixe d'éléments reliés par un système de communication dont les propriétés sont connues et fixées et où le risque d'accès non autorisé est considéré comme négligeable

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

3.1.8
canal de communication
connexion logique entre deux points limites d'un *système de communication*

3.1.9
système de communication
ensemble de matériels, de logiciels et de supports de propagation qui permet la transmission de *messages* (ISO/IEC 7498-1, couche d'application) d'une application à une autre

3.1.10
connexion
liaison logique entre objets applicatifs au sein du même appareil ou d'appareils différents

3.1.11
contrôle de redondance cyclique
CRC
<valeur> donnée redondante déduite et enregistrée ou transmise simultanément d'un bloc de données afin de détecter toute corruption des données

<méthode> procédure utilisée pour calculer les données redondantes

Note 1 à l'article: Les termes "code CRC" et "signature CRC", ainsi que les étiquettes comme CRC1, CRC2, peuvent également être utilisés dans la présente norme pour se référer aux données redondantes.

Note 2 à l'article: Voir également [28], [29][5].

3.1.12
système de communication défini
canal défini
nombre fixe ou nombre maximal fixe d'éléments reliés par un système de communication à bus de terrain, dont les propriétés sont connues et fixées, par exemple les conditions d'installation, l'immunité électromagnétique, les éléments (actifs) de réseau industriel, et où le risque d'accès non autorisé est réduit à un niveau tolérable conformément au modèle de cycle de vie de l'IEC 62443, en utilisant par exemple des zones et des conduits

5 Les chiffres entre crochets se réfèrent à la bibliographie.

3.1.13
diversité
moyens différents pour réaliser une fonction requise

Note 1 à l'article: La diversité peut être réalisée en utilisant des méthodes physiques ou des approches conceptuelles différentes.

[SOURCE: IEC 61508-4:2010, 3.3.7]

3.1.14
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 à l'article: Les erreurs peuvent être causées par des erreurs de conception du matériel/logiciel et/ou des informations altérées du fait d'un brouillage électromagnétique et/ou autres effets.

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

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

3.1.15
code explicite
code de mesure de sécurité réellement transmis dans le SPDU et connu de l'émetteur et du destinataire

3.1.16
défaillance
cessation de l'aptitude d'une unité fonctionnelle à accomplir une fonction requise ou à fonctionner comme prévu

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

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

3.1.17
anomalie
condition anormale qui peut entraîner une réduction de capacité ou la perte de capacité d'une unité fonctionnelle à accomplir une fonction requise

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

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

3.1.18
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

3.1.19
système de bus de terrain
système qui utilise un *bus de terrain* avec des appareils reliés

3.1.20
DLPDU
DÉCONSEILLÉ: trame
Data Link Protocol Data Unit (Unité de données de protocole de liaison de données)

3.1.21
Séquence de contrôle de trame
FCS
données redondantes issues d'un bloc de données d'une DLPDU (trame), qui utilisent une fonction de hachage et enregistrées ou transmises avec le bloc de données, afin de déterminer l'altération des données

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

Note 2 à l'article: Voir également [28], [29].

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

3.1.22
fonction de hachage
fonction (mathématique) de mise en correspondance des valeurs d'un ensemble (éventuellement) très grand de valeurs en une plage de valeurs (habituellement) plus petite

Note 1 à l'article: Les fonctions de hachage peuvent être utilisées pour déterminer l'altération des données.

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

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

3.1.23
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

3.1.24
code implicite
code de mesure de sécurité qui n'est pas transmis dans le SPDU, mais qui est connu de l'émetteur et du destinataire

3.1.25
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

3.1.26
message
série ordonnée d'octets, destinée à véhiculer des informations

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

3.1.27
collecteur de messages
partie d'un *système de communication* destiné à recevoir des *messages*

[SOURCE: ISO/IEC 2382-16:1996, 16.02.03]

3.1.28
source de messages
partie d'un *système de communication* destiné à envoyer des *messages*

[SOURCE: ISO/IEC 2382-16:1996, 16.02.02]

3.1.29
déclenchement de nuisance
déclenchement parasite sans effet préjudiciable

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

3.1.30
niveau de performances
PL
niveau discret utilisé pour spécifier la capacité des parties relatives à la sécurité des systèmes de commande à accomplir une fonction de sécurité dans des conditions prévisibles

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

[SOURCE: ISO 13849-1:2015, 3.1.23, traduction française modifiée – amélioration]

3.1.31
très basse tension de protection
TBTP
circuit électrique dans lequel la tension ne peut pas dépasser 30 V eff. c.a., 42,4 V crête ou 60 V c.c. en conditions normales et en conditions de défaut isolé, sauf en conditions de défauts de terre dans d'autres circuits

Note 1 à l'article: Un circuit TBTP comprend un raccordement à un conducteur de protection. En l'absence de raccordement à un conducteur de protection, ou si une défaillance existe au niveau du raccordement, les tensions ne sont pas corrigées.

[SOURCE: IEC 61010-2-201:2013, 3.109, modifié – suppression de "circuit" dans le terme, et suppression de la seconde note à l'article]

3.1.32
redondance
existence de plusieurs moyens pour accomplir une fonction requise ou pour représenter des informations

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

3.1.33
date relative
date référencée par rapport à l'horloge locale d'une entité

Note 1 à l'article: En général, il n'y a pas de relation avec les horloges des autres entités.

[SOURCE: IEC 62280:2014, 3.1.43]

3.1.34
fiabilité
probabilité pour qu'un système automatisé puisse accomplir une fonction requise, dans des conditions données, pendant un intervalle de temps donné (t1, t2)

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

Note 2 à l'article: Le terme "fiabilité" est aussi employé pour désigner l'aptitude caractérisée par cette probabilité.

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

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

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

3.1.35
probabilité d'erreurs résiduelles
RP
probabilité de non-détection d'une erreur par les mesures de sécurité SCL

Note 1 à l'article: L'abréviation «RP» est dérivée du terme anglais développé correspondant «residual error probability».

3.1.36
taux d'erreurs résiduelles
taux statistique de défaut de détection d'erreurs par les mesures de sécurité SCL

3.1.37
risque
combinaison de la probabilité d'un dommage et de sa gravité

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

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

3.1.38
canal de communication de sécurité
SC
canal de communication qui débute au sommet de la SCL de la source et qui se termine au sommet de la SCL du collecteur

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

3.1.39
couche de communication de sécurité
SCL
couche de communication située au-dessus de la FAL qui comprend toutes les mesures supplémentaires nécessaires qui permettent d'assurer la transmission de données en toute sécurité conformément aux exigences de l'IEC 61508

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

3.1.40
connexion de sécurité
connexion qui utilise le protocole de sécurité pour des transactions de communications

3.1.41
données de sécurité
données transmises par un réseau de sécurité qui utilise un protocole de sécurité

Note 1 à l'article: La couche de communication de sécurité ne garantit pas la sécurité des données proprement dites, mais uniquement la transmission en toute sécurité de ces dernières.

3.1.42
appareil de sécurité
appareil conçu conformément à l'IEC 61508 et qui met en œuvre le profil de communication de sécurité fonctionnelle

3.1.43
très basse tension de sécurité
TBTS
circuit électrique dans lequel la tension ne peut pas dépasser 30 V eff. c.a., 42,4 V crête ou 60 V c.c. en conditions normales et en conditions de défaut isolé, y compris en conditions de défauts de terre dans d'autres circuits

[SOURCE: IEC 61010-2-201:2013, 3.110, modifié — suppression de "circuit" dans le terme, et suppression de la note à l'article]

3.1.44
fonction de sécurité
fonction à réaliser par un système E/E/PE relatif à la sécurité ou par un dispositif externe de réduction de risque, prévue pour assurer ou maintenir un état de sécurité de l'EUC par rapport à un événement dangereux spécifique

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

3.1.45
temps de réponse de la fonction de sécurité
temps écoulé dans le cas le plus défavorable à la suite de l'activation d'un capteur de sécurité relié à un bus de terrain, avant que ne soit atteint l'état de sécurité correspondant de ses actionneurs de sécurité, du fait d'erreurs ou de défaillances dans la fonction de sécurité

Note 1 à l'article: Ce concept, introduit en 5.2.4, est traité dans le cadre des profils de communication de sécurité fonctionnelle définis dans la présente partie.

3.1.46
niveau d'intégrité de sécurité
SIL
niveau discret (parmi quatre possibles) correspondant à une gamme de valeurs d'intégrité de sécurité, où le niveau 4 d'intégrité de sécurité possède le plus haut degré d'intégrité et le niveau 1 possède le plus bas

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

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

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

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

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

3.1.47
mesure de sécurité
mesure permettant de contrôler les *erreurs* de communication éventuelles, qui est conçue et mise en œuvre conformément aux exigences de l'IEC 61508

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

Note 2 à l'article: Les *erreurs* de communication et les mesures de sécurité associées sont détaillées en 5.3 et 5.4.

3.1.48
PDU de sécurité
SPDU
PDU transféré via le canal de communication de sécurité

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

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

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

3.1.49
application relative à la sécurité
programmes conçus conformément à l'IEC 61508 pour satisfaire aux exigences SIL de l'application

3.1.50
système relatif à la sécurité
système qui exécute les *fonctions de sécurité* conformément à l'IEC 61508

3.1.51
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

3.1.52
déclenchement parasite
déclenchement provoqué par le système de sécurité sans injonction du processus

3.1.53
horodatage
information temporelle incluse dans un *message*

3.1.54
répartition uniforme
loi de probabilité où toutes les valeurs d'un ensemble fini sont également susceptibles de se produire

Note 1 à l'article: Pour un champ de longueur de bit i, la probabilité d'occurrence d'une valeur de champ particulier est égale à 2^{-i} étant donné que la somme de toutes les probabilités d'occurrence est égale à 1.

3.1.55
canal blanc
système de communication défini dans lequel tous les éléments pertinents du matériel et des logiciels sont conçus, mis en œuvre et validés conformément à l'IEC 61508

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

3.1.56
données explicites
données qui sont transmises

3.1.57
données implicites
données additionnelles qui ne sont pas transmises, mais sont connues de l'émetteur et du récepteur

[SOURCE: IEC 62280:2014, 3.1.25]

3.2 Symboles et abréviations

3.2.1 Abréviations

BSC	Binary Symmetric Channel (Canal symétrique binaire)	
Code A	Code d'authenticité	
Code T	Code d'opportunité	
CP	Communication Profile (Profil de communication)	[IEC 61784-1]
CPF	Communication Profile Family (Famille de profils de communication)	[IEC 61784-1]
CRC	Contrôle de redondance cyclique	
DLL	Data Link Layer (Couche de liaison de données)	[ISO/IEC 7498-1]
DLPDU	Data Link Protocol Data Unit (Unité de données de protocole de liaison de données)	
CEM	Compatibilité électromagnétique	
EMI	Electromagnetic Interference (Brouillage électromagnétique)	
EUC	Equipment Under Control (Equipement commandé)	[IEC 61508-4:2010]
E/E/PE	Electrique/électronique/électronique programmable	[IEC 61508-4:2010]
FAL	Fieldbus Application Layer (Couche d'application de bus de terrain)	[IEC 61158-5]
FCS	Frame Check Sequence (Séquence de contrôle de trame)	
FIT	Failure In Time (Intensité de défaillance) (équivaut à 10^{-9} de défaillance par heure)	
FS	Functional Safety (Sécurité fonctionnelle)	
FSCP	Functional Safety Communication Profile (Profil de communication de sécurité fonctionnelle)	
IACS	Industrial Automation and Control System (Automatisation Industrielle et système de commande)	
MTBF	Mean Time Between Failures (Temps moyen de bon fonctionnement)	
MTTF	Mean Time To Failure (Durée moyenne de fonctionnement avant défaillance)	
NSR	Non Safety Related (Non relatif à la sécurité)	
PDU	Protocol Data Unit (Unité de données de protocole)	[ISO/IEC 7498-1]
~~Pe~~	~~Bit error probability (Probabilité d'erreurs sur les éléments binaires)~~	
TBTP	Très basse tension de protection	
PES	Programmable Electronic System (Système électronique programmable)	[IEC 61508-4:2010]
PFD_{avg}	Probabilité moyenne de défaillance dangereuse en cas de sollicitation	[IEC 61508-4:2010]
PFH	Fréquence moyenne de défaillance dangereuse [h^{-1}] par heure	[IEC 61508-4:2010]
PhL	Couche physique	[ISO/IEC 7498-1]
PL	Niveau de performances	[ISO 13849-1]
PLC	Programmable Logic Controller (Automate programmable)	
~~RP~~	~~Residual Error Probability (Probabilité d'erreurs résiduelles)~~	

SCL	Safety Communication Layer (Couche de communication de sécurité)	
TBTS	Très basse tension de sécurité	
SIS	Safety Instrumented Systems (Systèmes de sécurité instrumentés)	
SL	Security Level (Niveau de sécurité)	[IEC 62443]
SMS	Security Management System (Système de gestion de sécurité)	[IEC 62443]
SPDU	Safety PDU (PDU de sécurité)	
SR	Safety Related (Relatif à la sécurité)	

3.2.2 Symboles

A_k	Répartition du poids du code: nombre de mots de code valides à k bits définis sur "un"
e	Longueur binaire des données explicites
err_{impl}	Disjonction bit à bit de $impl_S$ et $impl_R$
expl	Données explicites
$expl_R$	Données explicites côté récepteur
$expl_S$	Données explicites côté émetteur
FCS_C	Séquence de contrôle de trame calculée au niveau du récepteur
FCS_R	Séquence de contrôle de trame reçue
FCS_S	Séquence de contrôle de trame émise
i	Longueur binaire des données implicites
ID	Remise incorrecte (*Incorrect Delivery*)
$impl_R$	Données implicites côté récepteur
$impl_S$	Données implicites côté émetteur
n	Longueur binaire du SPDU
P_e	Probabilité d'erreurs sur les éléments binaires
P_{ID}	Probabilité de remise incorrecte
r	Longueur binaire de la FCS (degré de polynôme générateur)
RP	Probabilité d'erreurs résiduelles

4 Conformité

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

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

une conformité à l'IEC 61784-3:20xx FSCP n/m <Type>

ou

une conformité à l'IEC 61784-3 (Ed.3.0) FSCP n/m <Type>

où le Type entre les crochets obliques < > est facultatif et les crochets obliques ne doivent pas être inclus.

En variante, une déclaration de conformité peut être présentée comme

une conformité à l'IEC 61784-3-N:20xx

ou

une conformité à l'IEC 61784-3-N (Ed.3.0)

où N est le numéro de famille attribué à la CPF correspondante.

La conformité à une partie IEC 61784-3-N implique que toutes les exigences obligatoires des FSCP correspondants applicables à l'appareil, au système ou à l'application spécifiques 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

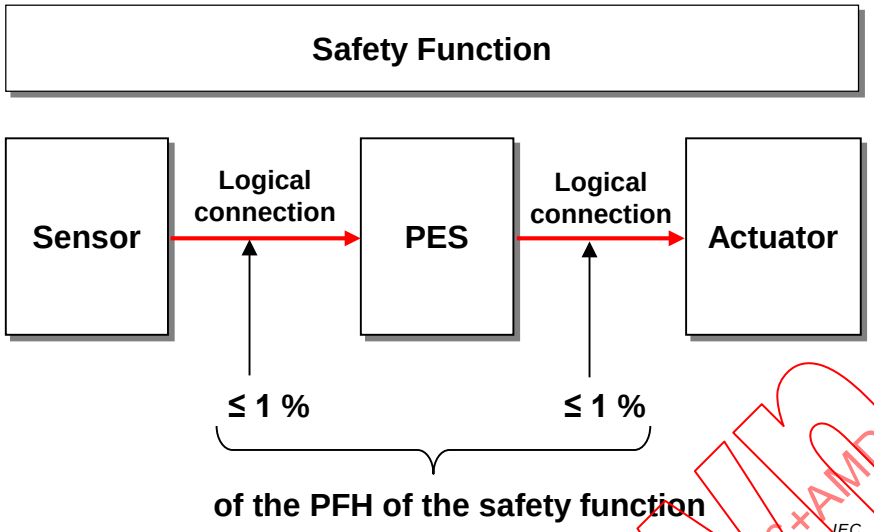
5.1 Décomposition d'une fonction de sécurité

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

Le système de communication proprement dit, défini dans la présente norme, transmet les données de sécurité. Pour simplifier les calculs de système, il est recommandé qu'une connexion logique aux canaux de communication de sécurité d'une fonction de sécurité ne consomme pas plus de 1 % de la PFH ou de la PFD_{avg} maximale du SIL cible pour lequel le profil de communication de sécurité fonctionnelle est conçu (voir la Figure 4 et 5.8.2).

Si cette valeur de 1 % pour une connexion logique ne peut pas être garantie par un FSCP donné, le manuel de sécurité de ce FSCP doit fournir des lignes directrices supplémentaires sur les calculs de la PFH ou de la PFD_{avg}.

La PFH et la PFD_{avg} globales de chaque appareil de sécurité doivent comprendre la PFH et la PFD_{avg} de la connexion logique. La PFD_{avg} doit être fournie si le FSCP est également utilisé pour les applications en mode à faible sollicitation conformes à l'IEC 61508.



Anglais	Français
Safety function	Fonction de sécurité
Sensor	Capteur
Logical connection	Connexion logique
Actuator	Actionneur
of the PFH of the safety function	de la PFH de la fonction de sécurité

Figure 4 – Communication de sécurité comme partie intégrante d'une fonction de sécurité

D'autre part, la PFH/PFD_{avg} de la communication peut être calculée pour l'ensemble de la fonction de sécurité. Dans ce cas, la PFH/PFD_{avg} de la communication de sécurité n'est à prendre compte qu'une seule fois.

5.2 Système de communication

5.2.1 Généralités

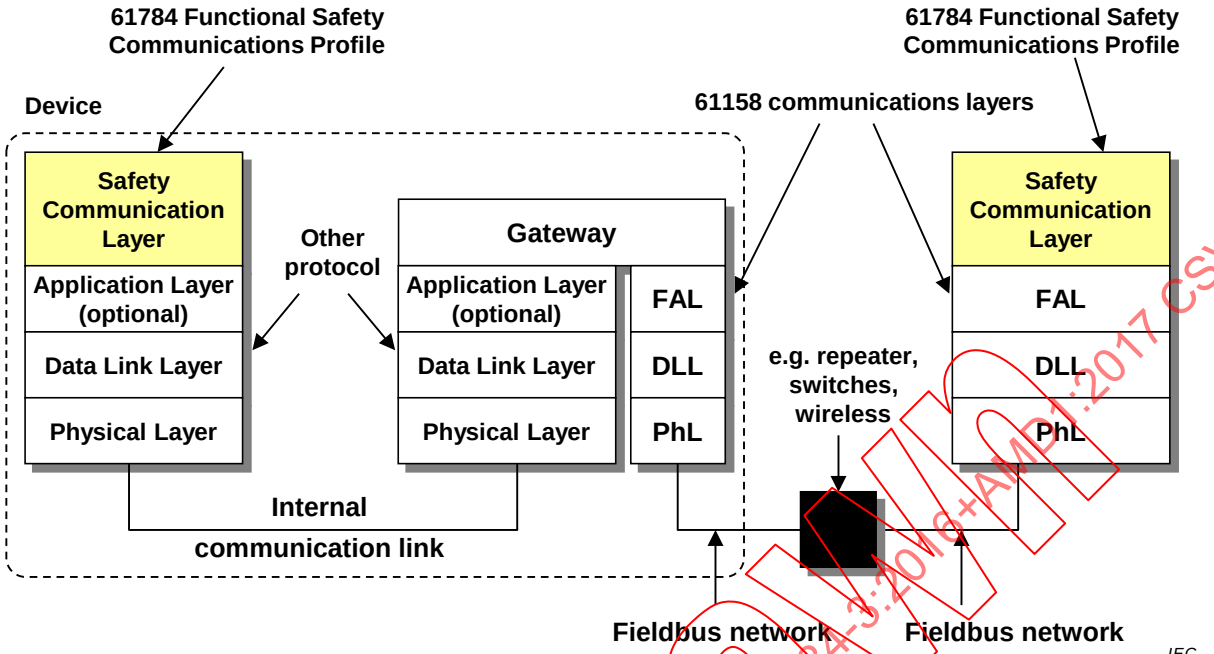
Les informations suivantes permettent une compréhension commune de la technologie et des termes employés.

5.2.2 Bus de terrain définis dans l'IEC 61158

Même si l'IEC 61508 ne limite pas l'utilisation des technologies de communication, la présente norme se concentre sur l'utilisation des systèmes de communication de sécurité fonctionnelle basés sur les bus de terrain. La Figure 5 présente un exemple de modèle d'utilisation de communications de sécurité fonctionnelle avec un bus de terrain qui s'appuie sur le principe du canal noir.

Lors de l'utilisation des structures de bus de terrain basées sur l'IEC 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 l'IEC 61508 doivent être effectuées par une "couche de communication de sécurité" supplémentaire, positionnée comme illustré à la Figure 5.

La couche de communication de sécurité inclut des services et un protocole adaptés pour coder les données de sécurité en PDU de sécurité, lesquels sont transmis au canal noir et reçus de ce dernier, puis les décoder pour en extraire les données de sécurité.



Anglais	Français
Functional Safety Communication Profile	Profil de communication de sécurité fonctionnelle
Device	Appareil
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 5 – Exemple de modèle d'un système de communication de sécurité fonctionnelle

Alors que la mise en œuvre de la couche d'application de bus de terrain (FAL) est exigée pour des systèmes de communication de sécurité fonctionnelle conformément à la présente norme, la couche d'application peut être omise pour les liaisons de communication internes à un appareil (avec une passerelle, par exemple).

Les fonctions non relatives à la sécurité peuvent contourner la SCL et accéder directement à la FAL.

5.2.3 Types de canaux de communication

L'IEC 61508 utilise les concepts appelés "canal noir" ou "canal blanc" pour définir les exigences du bus de terrain de base en vue de la transmission des données de sécurité. La présente norme spécifie les profils de communication de sécurité fonctionnelle qui appliquent la méthode du canal noir.

Dans ce contexte, un canal de communication de sécurité est défini comme issu 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 collecteur (voir la Figure 5). Le canal noir inclut tout ce qui se trouve entre les couches de communication de sécurité.

5.2.4 Temps de réponse de la fonction de sécurité

Le temps de réponse de la fonction de sécurité est le temps écoulé dans le cas le plus défavorable à la suite de l'activation d'un capteur de sécurité (interrupteur, transmetteur de pression, rideau de lumière, par exemple) relié à un bus de terrain, avant que ne soit atteint l'état de sécurité correspondant de ses actionneurs de sécurité (relais, soupape, entraînement, par exemple), du fait d'erreurs ou de défaillances dans la fonction de sécurité.

Le calcul du temps de réponse de la fonction de sécurité est spécifié dans les parties spécifiques au profil de l'IEC 61784-3.

Les mesures empiriques ne peuvent être utilisées que comme un contrôle de vraisemblance du calcul du cas le plus défavorable.

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 6 présente un exemple des composantes typiques d'un temps de réponse de la fonction de sécurité.

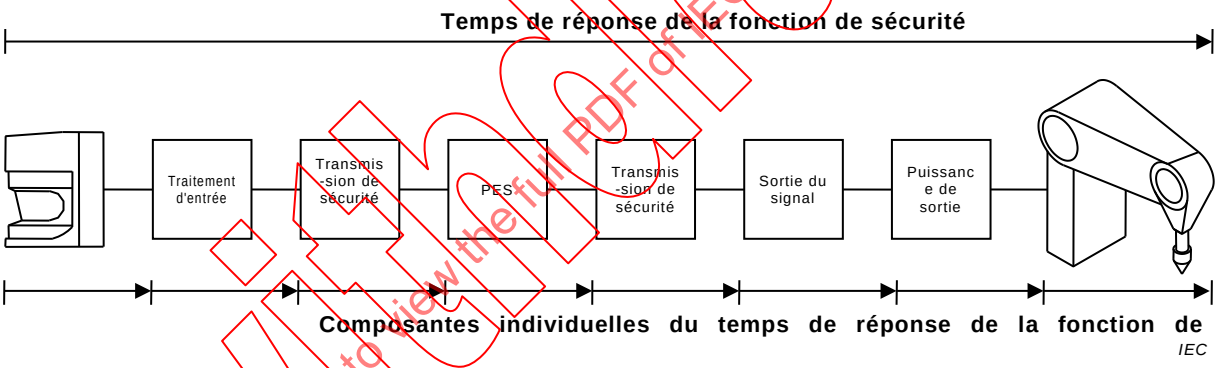


Figure 6 – Exemple des composantes du temps de réponse de la fonction de sécurité

Les profils individuels de communication de sécurité fonctionnelle 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 5.3.2 à 5.3.9 spécifient les erreurs de communication potentielles. Des notes supplémentaires sont fournies pour indiquer le comportement classique 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 entre les messages.

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

NOTE 2 La plupart des systèmes de communication comportent des protocoles de correction des erreurs de message. Ces messages ne sont pas classés comme une "perte" jusqu'à l'échec avéré des procédures de correction ou de répétition ou tant que lesdites procédures ne sont pas utilisées.

NOTE 3 Un message est classé comme un "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 plusieurs erreurs produisent un nouveau message dont la structure est correcte (adressage, longueur, fonction de hachage comme 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 anomalies, comme une répétition non prévue, une séquence incorrecte, un retard inacceptable, une insertion.

5.3.3 Répétition non prévue

Les messages sont répétés à la suite d'une erreur, d'une anomalie 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.

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 anomalie ou d'une perturbation.

NOTE 1 Cette erreur de "séquence correcte" est également appelée erreur "hors séquence".

NOTE 2 Les systèmes de bus de terrain peuvent contenir des éléments de stockage des messages (par exemple, FIFO au niveau des commutateurs, ponts, routeurs) ou appliquer des protocoles qui peuvent affecter la séquence (par exemple, en favorisant les messages à priorité élevée par rapport aux messages à priorité moins élevée).

NOTE 3 Lorsque plusieurs séquences sont actives, par exemple des messages en provenance de différentes entités sources ou des rapports relatifs à des types d'objets différents, ces séquences sont contrôlées séparément et des erreurs peuvent être signalées pour chaque séquence.

5.3.5 Perte

Un message ou un acquittement n'est pas reçu en raison d'une erreur, d'une anomalie ou d'une perturbation.

5.3.6 Retard inacceptable

Les messages peuvent être retardés au-delà de leur fenêtre temporelle d'arrivée admise, en raison, par exemple, 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 nature à retarder ou à refuser les services (FIFO au niveau des commutateurs, ponts, routeurs, par exemple).

5.3.7 Insertion

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

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

5.3.8 Déguisement

Une anomalie 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 le déguisement, par exemple les identités de sources autorisées, les expressions d'adaptation ou la cryptographie.

5.3.9 Adressage

En raison d'une anomalie ou d'une perturbation, un message relatif à la sécurité est délivré au participant relatif à la sécurité inapproprié, qui traite alors le message reçu comme un message correct. Cela inclut le cas appelé erreur de bouclage où l'émetteur du message reçoit en retour son propre message.

5.4 Mesures correctives déterministes

5.4.1 Généralités

Les mesures couramment appliquées pour détecter les erreurs déterministes et les défaillances d'un système de communication sont énumérées de 5.4.2 à 5.4.9, par opposition aux erreurs stochastiques comme la corruption de messages provoquée par un brouillage électromagnétique.

5.4.2 Numéro de séquence

Un numéro de séquence est intégré dans les messages échangés entre la source de messages et le collecteur de messages. 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 Horodatage

Dans la plupart des cas, le contenu d'un message n'est valide qu'à un moment particulier. L'horodatage peut être une heure ou une heure et une date, que l'émetteur a incluses dans un message.

NOTE Des horodatages relatifs et des horodatages absolus peuvent être utilisés.

L'horodatage exige la synchronisation de la base temporelle. Pour les applications de sécurité, la synchronisation doit être régulièrement surveillée et la probabilité de défaillance de ce mécanisme doit être incluse dans l'évaluation de l'ensemble de la fonction de sécurité.

5.4.4 Délai

Lors de la transmission d'un message, le collecteur de messages vérifie si le temps écoulé entre deux messages reçus de manière consécutive dépasse une valeur prédéterminée. L'existence d'une erreur est alors à envisager.

EXEMPLE

Méthode d'accès à intervalles de temps:

– l'échange de messages a lieu dans le cadre de cycles fixes et d'intervalles de temps prédéterminés pour chaque participant;
– chaque participant transmet 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 est ajoutée, 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 identifiant de source et/ou de destination unique qui décrit l'adresse logique du participant relatif à la sécurité.

5.4.6 Message en retour

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

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

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

5.4.7 Assurance d'intégrité des données

Le processus d'application relative à la sécurité ne doit pas se fier aux méthodes d'assurance d'intégrité des données si elles ne sont pas conçues en fonction de la sécurité fonctionnelle. Des données redondantes sont donc 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 comme la cryptographie pour assurer l'intégrité des données, comme variante aux méthodes typiques comme les CRC.

Si une fonction de hachage est utilisée, elle ne doit pas inclure des mécanismes de correction d'erreur.

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, via l'application de 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.

Les données de sécurité transmises font par ailleurs l'objet d'une contre-vérification pour déterminer leur validité sur le bus de terrain ou sur une unité source/collectrice 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 collecteur.

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.

Il est acceptable de disposer d'un système d'assurance d'intégrité des données supplémentaire pour les messages SR, et pas pour les messages NSR.

5.5 Relations typiques entre les erreurs et les mesures de sécurité

Les mesures de sécurité spécifiées en 5.4 peuvent être relatives à l'ensemble des erreurs possibles défini en 5.3. Les relations typiques sont présentées au Tableau 1. Chaque FSCP doit spécifier les relations réelles. 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 combinaison de mesures de sécurité correspondante pour les erreurs possibles définies conformément au Tableau 1.

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

Une mesure de sécurité ne doit figurer au tableau correspondant pour un FSCP donné que si elle est effective avant le temps de réponse de sécurité garanti du bus de terrain.

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

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

NOTE Tableau adapté du Tableau 1 de l'IEC 62280:2014.

[a] Uniquement pour l'identification de l'émetteur. Ne détecte que l'insertion d'une source non valide.

[b] Exigé dans tous les cas.

[c] Cette mesure n'est comparable qu'avec un mécanisme d'assurance des données de grande qualité si un calcul peut permettre de démontrer que le taux d'erreurs résiduelles Λ atteint les valeurs exigées en 5.4.9 lorsque deux messages sont envoyés par des émetteurs-récepteurs indépendants.

[d] Efficace uniquement si le message en retour contient les données d'origine ou des informations sur ces dernières et si le récepteur agit uniquement sur les données après acquittement du message en retour.

[e] Efficace uniquement si les numéros de séquence ou les horodatages des entités sources sont différents.

5.6 Phases de communication

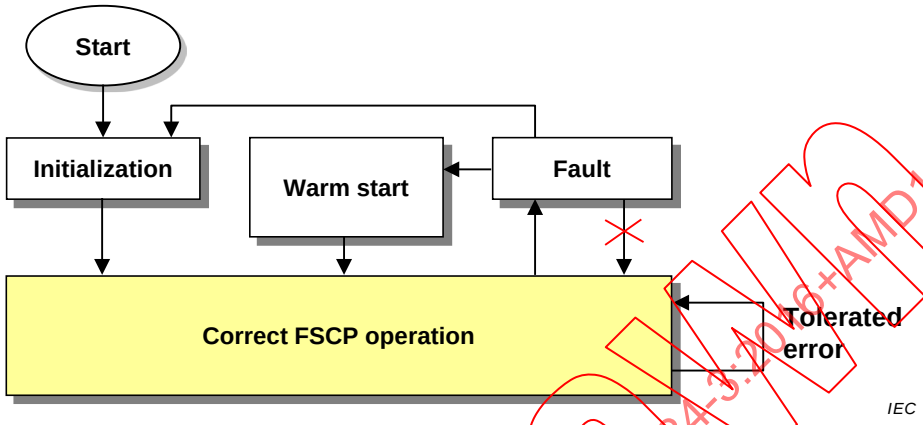
Un FSCP doit être conçu de sorte qu'un état de sécurité ou qu'un taux d'erreurs résiduelles suffisant du côté du récepteur puisse être atteint, conformément à l'IEC 61508, dans chacune des phases de communication du réseau de sécurité, y compris:

- installation ou modification du réseau de sécurité (configuration et paramétrage);
- démarrage avec initialisation (par exemple, établissement de connexion);
- fonctionnement (échange de données de sécurité);
- démarrage à chaud après une anomalie;

- arrêt.

La Figure 7 présente un modèle de protocole FSCP conceptuel. Un FSCP ne doit pas revenir directement pour corriger la communication FSCP après une anomalie, mais d'abord passer par un démarrage à chaud ou de nouvelles phases d'initialisation en fonction du FSCP.

NOTE En cas d'anomalies, le FSCP peut considérer les exigences de l'application comme un acquittement d'opérateur avant un démarrage de la machine.



Anglais	Français
Start	Démarrage
Tolerated error	Erreur tolérée
Correct FSCP operation	Fonctionnement correct du FSCP
Warm start	Démarrage à chaud
Fault	Anomalie
Initialization	Initialisation

Figure 7 – Modèle de protocole FSCP conceptuel

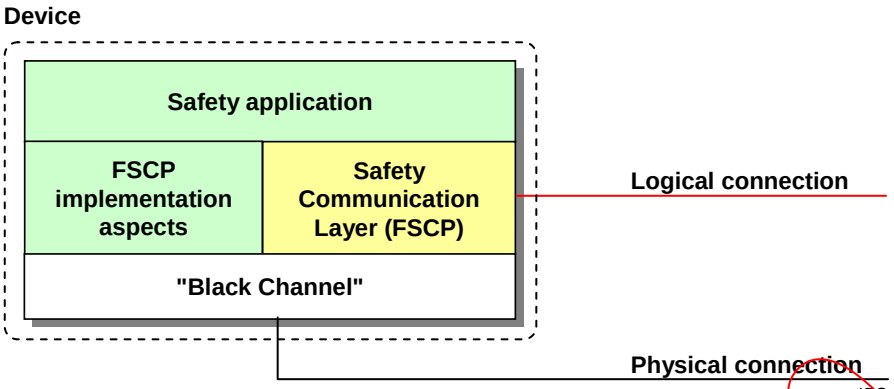
5.7 Aspects relatifs à la mise en œuvre du FSCP

Toutes les mesures techniques FSCP doivent être mises en œuvre dans la SCL des appareils conçus conformément à l'IEC 61508 et doivent satisfaire au SIL cible.

Certaines mesures du protocole dépendent de la manière dont elles sont mises en œuvre dans un appareil de sécurité particulier. La Figure 8 présente la séparation entre les aspects relatifs à la mise en œuvre du FSCP et ses aspects déterministes et probabilistes.

Un exemple d'aspect relatif à la mise en œuvre est une dépendance sur le taux de défaillance des horloges en temps réel, des chiens de garde ou des microcontrôleurs. Ces aspects exigent des évaluations quantitatives de sécurité conformes à l'IEC 61508 pour déterminer leur pertinence par rapport aux prises en compte individuelles des propriétés de sécurité génériques.

La présente norme ne considère pas les aspects relatifs à la mise en œuvre, sauf si un aspect relatif à la mise en œuvre est exigé par un FSCP et si cet aspect peut affecter le taux d'erreurs résiduelles du FSCP. Les propriétés de sécurité génériques sont prises en compte en fonction des connexions logiques entre les points d'extrémité SCL (qui n'utilisent que des hypothèses de base sur les performances du canal noir, comme indiqué dans les manuels de sécurité des FSCP individuels).



Anglais	Français
Safety application	Application de sécurité
FSCP implementation aspects	Aspects relatifs à la mise en œuvre du FSCP
Safety communication Layer	Couche de communication de sécurité
Black Channel	Canal noir
Device	Appareil
Logical connection	Connexion logique
Physical connection	Connexion physique

Figure 8 – Aspects relatifs à la mise en œuvre du FSCP

5.8 Considérations relatives à l'intégrité des données

5.8.1 Calcul du taux d'erreurs résiduelles

Le SPDU peut toujours être corrompu, même si les messages arrivent de manière correcte (déterministe). L'assurance d'intégrité des données est ainsi une composante fondamentale de la couche de communication de sécurité qui permet d'atteindre un niveau d'intégrité de sécurité exigé. Des fonctions de hachage appropriées, par exemple 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.

La DLL du bus de terrain ne doit pas utiliser la même fonction de hachage que celle de la couche de communication de sécurité superposée, 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.

EXEMPLE Lorsque le CRC est utilisé comme fonction de hachage, la DLL du bus de terrain 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 conformément à la revendication de SIL exigée.

Un fournisseur peut choisir différentes méthodes de calcul afin 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 taux d'erreurs résiduelles est calculé sur la base de la probabilité d'erreurs résiduelles du mécanisme d'assurance d'intégrité des données (de sécurité) superposées et de la fréquence d'échantillonnage des SPDU. En cas de calcul de la PFH/PFD_{avg} par fonction de sécurité,

l'évaluation du nombre maximal de collecteurs d'informations (m) admis dans une fonction de sécurité simple doit être prise en compte.

Les Equations (1) et (2) ci-dessous doivent servir au calcul des taux d'erreurs résiduelles qui résultent de R_{SC} (Pe), sauf si le modèle sous-jacent ne s'applique pas ou si une autre méthode peut se révéler plus appropriée. Les éléments des équations sont spécifiés au Tableau 2.

$$\lambda_{SC}\,(Pe) = R_{SC}\,(Pe) \times v \qquad (1)$$

$$\lambda_{SCL}\,(Pe) = \lambda_{SC}\,(Pe) \times m \qquad (2)$$

NOTE Ces équations partent de l'hypothèse d'un échantillonnage cyclique des SPDU par la SCL.

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

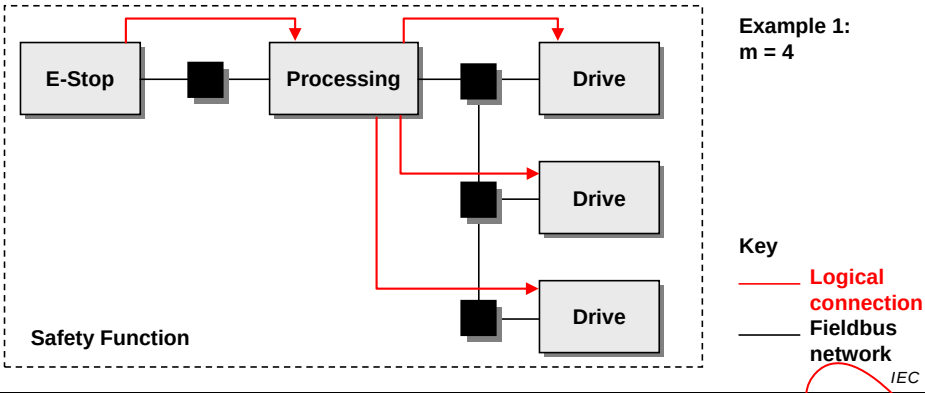
Eléments de l'équation	Définition
λ_{SC} (Pe)	Taux d'erreurs résiduelles par heure du canal de communication de sécurité par rapport à la probabilité d'erreurs sur les éléments binaires (voir 3.1.36)
λ_{SCL} (Pe)	Taux d'erreurs résiduelles par heure de la couche de communication de sécurité en fonction de la probabilité d'erreurs sur les éléments binaires (voir 3.1.36)
Pe	Probabilité d'erreurs sur les éléments binaires (voir Article B.3)
R_{SC} (Pe)	Probabilité d'erreurs résiduelles du canal de communication de sécurité en fonction de la probabilité d'erreurs sur les éléments binaires (voir 3.1.35)
v	Fréquence d'échantillonnage maximale des SPDU par heure
m	Nombre maximal de connexions logiques autorisé dans une seule fonction de sécurité (voir la Figure 9 et la Figure 10)

Le nombre m de connexions logiques dépend de l'application de la fonction de sécurité individuelle. La Figure 9 et la Figure 10 présentent la manière dont ce nombre peut être déterminé.

Les Figures présentent les connexions physiques avec d'éventuels éléments de réseau, des répéteurs, des commutateurs ou des liaisons sans fil par exemple et les connexions logiques entre les sous-systèmes impliqués dans la fonction de sécurité.

Les connexions logiques peuvent être basées sur des communications en diffusion unique ou en multidiffusion.

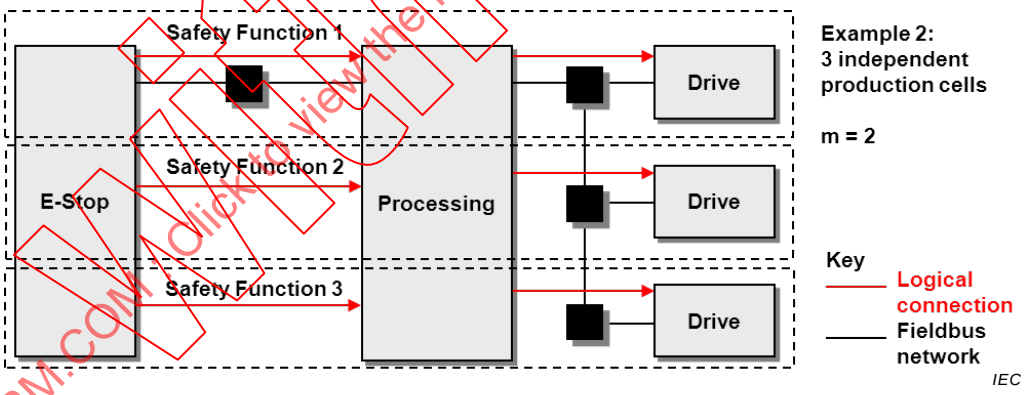
La Figure 9 donne un exemple 1 d'une application où m = 4. Dans cette application, les trois entraînements sont considérés comme dangereux à un seul moment conformément à l'analyse des risques.



Anglais	Français
E-Stop	E-interruption
Processing	Traitement
Drive	Entraînement
Key	Légende
Logical connection	Connexion logique
Safety function	Fonction de sécurité
Fieldbus network	Réseau de bus de terrain
Example 1	Exemple 1

Figure 9 – Exemple d'application 1 (m = 4)

La Figure 10 donne un exemple 2 d'une application où m = 2. Dans cette application, un seul des trois entraînements est considéré comme dangereux à un seul moment conformément à l'analyse des risques.



Anglais	Français
E-Stop	E-interruption
Processing	Traitement
Drive	entraînement
Key	légende
Logical connection	Connexion logique
Safety function	Fonction de sécurité
Fieldbus network	Réseau de bus de terrain
Example 2	Exemple 2
3 independent production cells	3 cellules de production indépendantes

Figure 10 – Exemple d'application 2 (m = 2)

5.8.2 Taux total d'erreurs résiduelles et SIL

Un système de communication de sécurité fonctionnelle doit fournir un taux d'erreurs résiduelles en conformité à la présente norme. Le Tableau 3 et le Tableau 4 présentent la relation typique entre le taux d'erreurs résiduelles et le SIL, en fonction du principe que la contribution du système de communication de sécurité fonctionnelle ne dépasse pas 1 % par connexion logique de la fonction de sécurité.

Un temps de réponse de la fonction de sécurité doit être défini pour les deux systèmes avec un mode de sollicitation faible et élevée. Un taux nécessaire de SPDU doit de ce fait être garanti. La PFH qui correspond à un certain SIL doit être fournie dans tous les cas; la PFD_{avg} est quant à elle facultative.

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

Applicable pour les fonctions de sécurité jusqu'au SIL	Fréquence moyenne d'une défaillance dangereuse pour la fonction de sécurité (PFH)	Taux d'erreurs résiduelles maximal admissible pour une connexion logique de la fonction de sécurité (λ_{sc} (Pe))
4	$< 10^{-8}$/h	$< 10^{-10}$/h
3	$< 10^{-7}$/h	$< 10^{-9}$/h
2	$< 10^{-6}$/h	$< 10^{-8}$/h
1	$< 10^{-5}$/h	$< 10^{-7}$/h

Tableau 4 – Relation typique entre l'erreur résiduelle et le SIL

Applicable pour les fonctions de sécurité jusqu'au SIL	Probabilité moyenne d'une défaillance dangereuse en cas de sollicitation pour la fonction de sécurité (PFDavg)	Probabilité d'erreurs résiduelles maximale admissible pour une connexion logique de la fonction de sécurité
4	$< 10^{-4}$	$< 10^{-6}$
3	$< 10^{-3}$	$< 10^{-5}$
2	$< 10^{-2}$	$< 10^{-4}$
1	$< 10^{-1}$	$< 10^{-3}$

5.9 Relation entre sécurité fonctionnelle et sûreté

L'évaluation de la menace pour la sûreté et des risques est nécessaire pour les applications relatives à la sécurité. Les exigences relatives à la sûreté sont détaillées dans la série IEC 62443.

La sûreté signifie la protection contre les (cyber)attaques délibérées inacceptables ou les changements intempestifs d'un système d'automatisation industrielle et système de commande (IACS).

Les concepts de sûreté de l'IEC 62443 suivent un concept de cycle de vie similaire à l'IEC 61508, commençant par une évaluation de la menace pour la sûreté et des risques et l'attribution des niveaux de sûreté cibles (SL). Toutefois, en raison de la nature des menaces causées par les individus, l'IEC 62443 met l'accent principalement sur des questions comme les politiques et les procédures d'un système de gestion de sûreté (SMS) établi par les propriétaires d'usines et les fournisseurs au sein de leur organisation. Un problème majeur du SMS est la maintenance du système de sûreté pour lutter contre la dégradation, par exemple via une surveillance, des évaluations périodiques ou des corrections de logiciels.

L'IEC 62443 spécifie ensuite les technologies et les méthodes qui permettent d'obtenir un système sécurisé par une division de l'architecture d'un IACS en zones et en conduits. Le propriétaire de l'usine ou l'intégrateur est muni des contre-mesures et des technologies

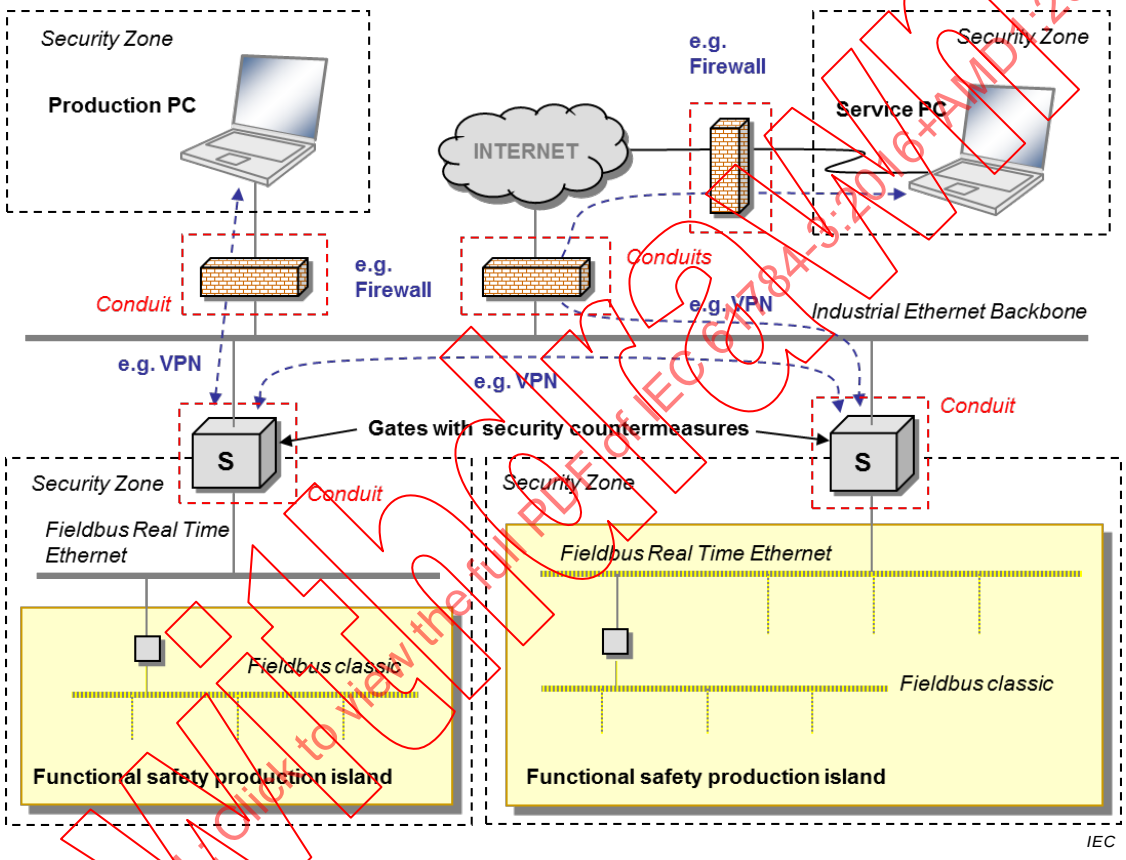
appropriées pour atteindre le niveau de sûreté cible et satisfaire à ses sept exigences fondamentales (vecteur) pour les zones et les conduits.

L'IEC 62443 traite également des exigences de sûreté des composants du système.

L'IEC 62443 permet aux concepteurs de choisir l'endroit de la mise en œuvre des contre-mesures de sûreté en ce qui concerne les appareils de sécurité.

NOTE Des exigences spécifiques au profil peuvent également être spécifiées dans l'IEC 61784-4.

La Figure 11 présente un exemple de division en zones et conduits d'un IACS avec îlots de sécurité fonctionnelle.



Anglais	Français
Firewall	Pare-feu
Conduit	Conduit
Industrial Ethernet Backbone	Dorsale Ethernet industriel
Gates with security countermeasures	Portes avec contre-mesures de sûreté
Security zone	Zone de sûreté
Fieldbus classic	Bus de terrain classique
Functional safety production island	Ilot de production de sécurité fonctionnelle
Fieldbus real time Ethernet	Ethernet de bus de terrain en temps réel

Figure 11 – Concept de zones et conduits pour la sûreté conformément à l'IEC 62443

5.10 Conditions aux limites et contraintes

5.10.1 Sécurité électrique

La sécurité électrique est une condition préalable à un système de communication de sécurité fonctionnelle. Tous les appareils de sécurité reliés doivent donc être conformes aux normes IEC de sécurité électrique applicables (par exemple, spécifications TBTS/TBTP de l'IEC 61010-2-201). Le manuel de sécurité doit spécifier les contraintes exigées des appareils reliés à un système de communication de sécurité fonctionnelle, qu'il s'agisse d'appareils relatifs à la sécurité ou d'appareils non relatifs à la sécurité, dont les éléments de réseau actifs.

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

NOTE 2 Les exigences sur les sources d'alimentation (démonstration d'anomalie simple, utilisation de sources d'alimentation distinctes, TBTS/TBTP, limitations de courant spécifiques au pays, etc.) sont spécifiées dans l'IEC 61918 et dans l'IEC 61784-5.

NOTE 3 Les exigences qui concernent les appareils de bus normaux (l'évaluation, par exemple) sont spécifiques aux profils de communication de sécurité fonctionnelle.

5.10.2 Compatibilité électromagnétique (CEM)

Les appareils de sécurité doivent être conformes aux niveaux d'essai renforcés et aux durées, ainsi qu'aux critères de performance correspondants spécifiés dans l'IEC 61326-3-1 ou dans la norme générique IEC 61000-6-7. L'IEC 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 l'IEC 61326-3-2.

NOTE Certaines applications peuvent exiger des niveaux plus élevés que ceux spécifiés dans l'IEC 61326-3-1, conformément à la spécification sur les exigences de sécurité (SRS).

5.11 Guide d'installation

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

La présence d'appareils 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 relative à la sécurité (même les produits normaux) permettent une évaluation de conformité appropriée du protocole de bus de terrain pertinent (par exemple, déclaration du fabricant ou évaluation par un tiers).

NOTE Des détails supplémentaires peuvent être fournis dans les parties spécifiques à la technologie de la sous-série IEC 61784-3 le cas échéant.

5.12 Manuel de sécurité

Conformément à l'IEC 61508-2, les fournisseurs d'appareils doivent fournir un manuel de sécurité. Les parties appropriées et spécifiques au profil décrivent les informations minimales exigées par le profil à inclure dans le manuel de sécurité.

5.13 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 sur les développements et les applications relatifs à la sécurité.

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

Les technologies de communication spécifiées dans la présente norme ne doivent être mises en œuvre que dans des appareils conçus conformément aux exigences de l'IEC 61508.

L'application à un appareil des technologies de communication spécifiées dans la présente norme ne garantit pas la satisafaction de toutes les exigences nécessaires sur le plan technique, organisationnel et juridique, relatives aux applications de sécurité de cet appareil, conformément aux exigences de l'IEC 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 appareil, 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 l'IEC 61508-1.

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

Le fabricant d'un appareil 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 à l'appareil.

Il est vivement recommandé que les mises en œuvre d'application d'un profil spécifique satisfassent aux essais de conformité et de validations correspondantes aux technologies de l'organisation.

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

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

La famille de profils de communication 1 (souvent appelée Fieldbus FOUNDATION™[6]) définit les profils de communication qui reposent sur l'IEC 61158-2 Type 1, l'IEC 61158-3-1, l'IEC 61158-4-1, l'IEC 61158-5-5, l'IEC 61158-5-9, l'IEC 61158-6-5 et l'IEC 61158-6-9.

Les profils de base CP 1/1, CP 1/2 et CP 1/3 sont définis dans l'IEC 61784-1. Le profil de communication de sécurité fonctionnelle CPF 1 FSCP 1/1 (FF-SIS™[6]) repose sur le profil de base CP 1/1 défini dans l'IEC 61784-1, ainsi que les spécifications de la couche de communication de sécurité définies dans l'IEC 61784-3-1.

---

6 Fieldbus FOUNDATION™ et FF-SIS™ sont des appellations commerciales de l'organisme à but non lucratif Fieldbus Foundation. Cette information est donnée à l'intention des utilisateurs de la présente Norme internationale et ne signifie nullement que l'IEC approuve ou recommande l'utilisation de produits de ces appellations commerciales. La conformité à la présente norme n'exige pas d'utiliser les appellations commerciales Foundation Fieldbus™ ou FF-SIS™. L'utilisation des appellations commerciales Fieldbus Foundation™ ou FF-SIS™ exige l'autorisation de la Fieldbus Foundation et la conformité aux conditions d'utilisation (essais et validation).

7 Famille de profils de communication 2 (CIP™) et Famille 16 (SERCOS®) – Profils de sécurité fonctionnelle

La famille de profils de communication 2 (souvent appelée CIP™[7]) définit les profils de communication qui reposent sur l'IEC 61158-2 Type 2, l'IEC 61158-3-2, l'IEC 61158-4-2, l'IEC 61158-5-2 et l'IEC 61158-6-2.

La famille de profils de communication 16 (souvent appelée SERCOS®[8]) définit un profil de communication CP 16/3 qui repose sur l'IEC 61158-3-19, l'IEC 61158-4-19, l'IEC 61158-5-19 et l'IEC 61158-6-19.

Les profils de base CP 2/1, CP 2/2, CP 2/3 et CP 16/3 sont définis dans l'IEC 61784-1 et dans l'IEC 61784-2. Le profil de communication de sécurité fonctionnelle CPF 2 FSCP 2/1 (CIP Safety™[7]) repose sur les profils de base CPF 2 définis dans l'IEC 61784-1 et l'IEC 61784-2, le profil de base CP 16/3 de l'IEC 61784-2 et les spécifications de la couche de communication de sécurité définies dans l'IEC 61784-3-2.

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

La famille de profils de communication 3 (souvent appelée PROFIBUS™, PROFINET™[9]) définit les profils de communication qui reposent sur l'IEC 61158-2 Type 3, l'IEC 61158-3-3, l'IEC 61158-4-3, l'IEC 61158-5-3, l'IEC 61158-5-10, l'IEC 61158-6-3 et l'IEC 61158-6-10.

Les profils de base CP 3/1 et CP 3/2 sont définis dans l'IEC 61784-1. CP 3/4, CP 3/5 et CP 3/6 sont définis dans l'IEC 61784-2. Le profil de communication de sécurité fonctionnelle CPF 3 FSCP 3/1 (PROFIsafe™[9]) repose sur les profils de base CPF 3 définis dans l'IEC 61784-1 et l'IEC 61784-2, ainsi que les spécifications de la couche de communication de sécurité définies dans l'IEC 61784-3-3.

---

7 CIP™ (Common Industrial Protocol) et CIP Safety™ désignent les appellations commerciales de l'organisme à but non lucratif ODVA, Inc. Cette information est donnée à l'intention des utilisateurs de la présente Norme internationale et ne signifie nullement que l'IEC approuve ou recommande le détenteur de la marque ou de l'un de ses produits. La conformité à la présente norme n'exige pas d'utiliser les appellations commerciales CIP™ ou CIP Safety™. L'utilisation des appellations commerciales CIP™ ou CIP Safety™ exige l'autorisation d'ODVA et la conformité aux conditions d'utilisation (essais et validation).

8 SERCOS® est une appellation commerciale de SERCOS International e.V. Cette information est donnée à l'intention des utilisateurs de la présente Norme internationale et ne signifie nullement que l'IEC approuve ou recommande le détenteur de la marque ou de l'un de ses produits. La conformité à la présente norme n'exige pas l'utilisation de l'appellation commerciale SERCOS®. L'utilisation de l'appellation commerciale SERCOS® exige l'autorisation de son détenteur et la conformité aux conditions d'utilisation (essais et validation).

9 PROFIBUS™, PROFINET™ et PROFIsafe™ désignent les appellations commerciales de l'organisme à but non lucratif PROFIBUS Nutzerorganisation e.V. (PNO). Cette information est donnée à l'intention des utilisateurs de la présente Norme internationale et ne signifie nullement que l'IEC approuve ou recommande l'utilisation de produits de ces appellations commerciales. La conformité à la présente norme n'exige pas d'utiliser les appellations commerciales PROFIBUS™, PROFINET™ ou PROFIsafe™. L'utilisation des appellations commerciales PROFIBUS™, PROFINET™ ou PROFIsafe™ exige l'autorisation de PNO et la conformité aux conditions d'utilisation (essais et validation).

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

La famille de profils de communication 6 (souvent appelée INTERBUS®[10]) définit les profils de communication qui reposent sur l'IEC 61158-2 Type 8, l'IEC 61158-3-8, l'IEC 61158-4-8, l'IEC 61158-5-8 et l'IEC 61158-6-8.

Les profils de base CP 6/1, CP 6/2 et CP 6/3 sont définis dans l'IEC 61784-1. Le profil de communication de sécurité fonctionnelle CPF 6 FSCP 6/7 (INTERBUS Safety™[10]) repose sur les profils de base CPF 6 définis dans l'IEC 61784-1 et les spécifications de la couche de communication de sécurité définies dans l'IEC 61784-3-6.

Les profils CP 6/1, CP 6/2 et CP 6/3 contiennent des services facultatifs, spécifiés par des identifiants de profil. Les identifiants de profil nécessaires pour CP 6/7 sont présentés au Tableau 5.

Tableau 5 – Présentation générale de l'identifiant de profil applicable au protocole FSCP 6/7

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

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

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

10.1 Profil de communication de sécurité fonctionnelle 8/1

La famille de profils de communication 8 (souvent appelée CC-Link™[11]) définit les profils de communication qui reposent sur l'IEC 61158-2 Type 18, l'IEC 61158-3-18, l'IEC 61158-4-18, l'IEC 61158-5-18 et l'IEC 61158-6-18.

Les profils de base CP 8/1, CP 8/2 et CP 8/3 sont définis dans l'IEC 61784-1. Le profil de communication de sécurité fonctionnelle CPF 8 FSCP 8/1 (CC-Link Safety™[11]) repose sur les profils de base CPF 8 définis dans l'IEC 61784-1 et les spécifications de la couche de communication de sécurité définies dans l'IEC 61784-3-8.

---

[10] INTERBUS® et INTERBUS Safety™ désignent les appellations commerciales de Phoenix Contact GmbH & Co. KG. Le contrôle de l'utilisation des appellations commerciales est confié à l'organisme à but non lucratif INTERBUS Club. Cette information est donnée à l'intention des utilisateurs de la présente Norme internationale et ne signifie nullement que l'IEC approuve ou recommande l'utilisation de produits de ces appellations commerciales. La conformité à la présente norme n'exige pas d'utiliser les appellations commerciales INTERBUS® ou INTERBUS Safety™. L'utilisation des appellations commerciales INTERBUS® ou INTERBUS Safety™ exige l'autorisation de INTERBUS Club et la conformité aux conditions d'utilisation (essais et validation).

[11] CC-Link™ et CC-Link Safety™ désignent les appellations commerciales de l'organisme à but non lucratif CC-Link Partner Association. Cette information est donnée à l'intention des utilisateurs de la présente Norme internationale et ne signifie nullement que l'IEC approuve ou recommande l'utilisation de produits de ces appellations commerciales. La conformité à la présente norme n'exige pas d'utiliser les appellations commerciales CC-Link™ ou CC-Link Safety™. L'utilisation des appellations commerciales CC-Link™ ou CC-Link Safety™ exige l'autorisation de CC-Link Partner Association et la conformité aux conditions d'utilisation (essais et validation).

10.2 Profil de communication de sécurité fonctionnelle 8/2

La famille de profils de communication 8 définit également des profils de communication basés sur l'IEC 61158-5-23 et l'IEC 61158-6-23.

Les profils de base CP 8/4 et CP 8/5 (souvent appelés CC-Link IE™[12]) sont définis dans l'IEC 61784-2. Le profil de communication de sécurité fonctionnelle CPF 8 FSCP 8/2 (fonction de communication de sécurité CC-Link IE™) repose sur les profils de base CPF 8 définis dans l'IEC 61784-2 et les spécifications de la couche de communication de sécurité définies dans l'IEC 61784-3-8.

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

La famille de profils de communication 12 (souvent appelée EtherCAT™[13]) définit les profils de communication qui reposent sur l'IEC 61158-2 Type 12, l'IEC 61158-3-12, l'IEC 61158-4-12, l'IEC 61158-5-12 et l'IEC 61158-6-12.

Les profils de base CP 12/1 et CP 12/2 sont définis dans l'IEC 61784-2. Le profil de communication de sécurité fonctionnelle CPF 12 FSCP 12/1 (Safety-over-EtherCAT™[13]) repose sur les profils de base CPF 12 définis dans l'IEC 61784-2 et les spécifications de la couche de communication de sécurité définies dans l'IEC 61784-3-12.

12 Famille de profils de communication 13 (Ethernet POWERLINK™) – Profils de sécurité fonctionnelle

La famille de profils de communication 13 (souvent appelée Ethernet POWERLINK™[14]) définit des profils de communication qui reposent sur l'IEC 61158-3-13, l'IEC 61158-4-13, l'IEC 61158-5-13 et l'IEC 61158-6-13.

Le profil de base CP 13/1 est défini dans l'IEC 61784-2. Le profil de communication de sécurité fonctionnelle CPF 13 FSCP 13/1 (openSAFETY™[14]) repose sur les profils de base CPF 13 définis dans l'IEC 61784-2 et les spécifications de la couche de communication de sécurité définies dans l'IEC 61784-3-13.

---

12 CC-Link IE™ est une appellation commerciale de l'organisme à but non lucratif CC-Link Partner Association. Cette information est donnée à l'intention des utilisateurs de la présente Norme internationale et ne signifie nullement que l'IEC approuve ou recommande l'utilisation de produits de ces appellations commerciales. La conformité à la présente norme n'exige pas d'utiliser l'appellation commerciale CC-Link IE™. L'utilisation de l'appellation commerciale CC-Link IE™ exige l'autorisation de CC-Link Partner Association et la conformité aux conditions d'utilisation (essais et validation).

13 EtherCAT™ et Safety-over-EtherCAT™ désignent les appellations commerciales de Beckhoff, Verl. Cette information est donnée à l'intention des utilisateurs de la présente Norme internationale et ne signifie nullement que l'IEC approuve ou recommande l'utilisation de produits de ces appellations commerciales. La conformité à la présente norme n'exige pas d'utiliser les appellations commerciales EtherCAT™ ou Safety-over-EtherCAT™. L'utilisation des appellations commerciales EtherCAT™ ou Safety-over-EtherCAT™ exige l'autorisation de Beckhoff, Verl et la conformité aux conditions d'utilisation (essais et validation).

14 Ethernet POWERLINK™ et openSAFETY™ sont des appellations commerciales de l'organisme à but non lucratif Ethernet POWERLINK™ Standardization Group (EPSG). Cette information est donnée à l'intention des utilisateurs de la présente Norme internationale et ne signifie nullement que l'IEC approuve ou recommande l'utilisation de produits de ces appellations commerciales. La conformité à la présente norme n'exige pas l'utilisation de l'appellation commerciale Ethernet POWERLINK™ ou openSAFETY™. L'utilisation des appellations commerciales Ethernet POWERLINK™ ou openSAFETY™ exige l'autorisation d'Ethernet POWERLINK™ Standardization Group (EPSG) et la conformité aux conditions d'utilisation (essais et validation).

13 Famille de profils de communication 14 (EPA®) – Profils de sécurité fonctionnelle

La famille de profils de communication 14 (souvent appelée EPA®[15]) définit des profils de communication qui reposent sur l'IEC 61158-3-14, l'IEC 61158-4-14, l'IEC 61158-5-14 et l'IEC 61158-6-14.

Les profils de base CP 14/1 et CP 14/2 sont définis dans l'IEC 61784-2. Le profil de communication de sécurité fonctionnelle CPF 14 FSCP 14/1 (EPASafety®[15]) repose sur les profils de base CPF 14 définis dans l'IEC 61784-2 et les spécifications de la couche de communication de sécurité définies dans l'IEC 61784-3-14.

14 Famille de profils de communication 17 (RAPIEnet™) – Profils de sécurité fonctionnelle

La famille de profils de communication 17 (souvent appelée RAPIEnet™[16]) définit un profil de communication qui repose sur l'IEC 61158-3-21, l'IEC 61158-4-21, l'IEC 61158-5-21 et l'IEC 61158-6-21.

Le profil de base CP 17/1 est défini dans l'IEC 61784-2. Le profil de communication de sécurité fonctionnelle CPF 17 FSCP 17/1 (RAPIEnet Safety™[16]) repose sur le profil de base CPF 17 défini dans l'IEC 61784-2 et les spécifications de la couche de communication de sécurité définies dans l'IEC 61784-3-17.

15 Famille de profils de communication 18 (Fieldbus SafetyNET p™) – Profils de sécurité fonctionnelle

La famille de profils de communication 18 (souvent appelée SafetyNET p™[17]) définit des profils de communication qui reposent sur l'IEC 61158-3-22, l'IEC 61158-4-22, l'IEC 61158-5-22 et l'IEC 61158-6-22.

Les profils de base CP 18/1 et CP 18/2 sont définis dans l'IEC 61784-2. Le profil de communication de sécurité fonctionnelle CPF 18 FSCP 18/1 repose sur les profils de base CPF 18 définis dans l'IEC 61784-2 et les spécifications de la couche de communication de sécurité définies dans l'IEC 61784-3-18.

---

15 EPA® et EPASafety® sont des appellations commerciales de Zhejiang SUPCON® Sci&Tech Group Co. Ltd. Chine. Cette information est donnée à l'intention des utilisateurs de la présente Norme internationale et ne signifie nullement que l'IEC approuve ou recommande l'utilisation de produits de ces appellations commerciales. La conformité à la présente norme n'exige pas d'utiliser les appellations commerciales EPA® ou EPASafety®. L'utilisation des appellations commerciales EPA® ou EPASafety® exige l'autorisation de SUPCON® et la conformité aux conditions d'utilisation (essais et validation).

16 RAPIEnet™ et RAPIEnet Safety™ désignent les appellations commerciales de l'organisme à but non lucratif RAPIEnet Association. Cette information est donnée à l'intention des utilisateurs de la présente Norme internationale et ne signifie nullement que l'IEC approuve ou recommande l'utilisation de produits de ces appellations commerciales. La conformité à la présente norme n'exige pas d'utiliser les appellations commerciales RAPIEnet™ ou RAPIEnet Safety™. L'utilisation des appellations commerciales RAPIEnet™ ou RAPIEnet Safety™ exige l'autorisation de RAPIEnet Association et la conformité aux conditions d'utilisation (essais et validation).

17 SafetyNET p est une appellation commerciale de Pilz GmbH & Co. KG. Cette information est donnée à l'intention des utilisateurs de la présente Norme internationale et ne signifie nullement que l'IEC approuve ou recommande l'utilisation de produits de ces appellations commerciales. La conformité à ce profil n'exige pas d'utiliser l'appellation commerciale SafetyNET p. L'utilisation de l'appellation commerciale SafetyNET p exige l'autorisation du détenteur de la marque et la conformité aux conditions d'utilisation (essais et validation).

Annexe A
(informative)

Exemple de modèles de communication de sécurité fonctionnelle

A.1 Généralités

La présente Annexe A examine différents modèles de structure de mise en œuvre d'appareils de sécurité de bus de terrain. Ces modèles fournissent différents mécanismes de détection des anomalies. Les modèles présentés ci-dessous ne sont fournis qu'à titre d'illustration des structures de mise en œuvre possibles. Il convient d'utiliser l'IEC 61508 pour la conception globale du système.

Certains exemples sont cités dans les Articles A.2 à A.5. D'autres modèles peuvent par ailleurs être utilisés.

NOTE Les structures de mise en œuvre dans ces exemples sont basées sur des couches redondantes de communication de sécurité, conformément aux exemples de l'IEC 61508.

A.2 Modèle A (message unique, canal et FAL, SCL redondantes)

Le modèle A présenté à la Figure A.1 sert de modèle de référence de base pour les autres modèles. Un seul bus de terrain est utilisé en tant que canal de communication.

Deux SCL fonctionnent indépendamment pour générer deux SPDU à partir des mêmes données de sécurité. Les SPDU font l'objet d'une contre-vérification avant que l'un d'eux ne soit transféré à l'aide d'un message de bus de terrain unique. Le SPDU reçu est décodé indépendamment et contrôlé quant à la sécurité par les deux SCL de réception et fait l'objet d'une contre-vérification. Les deux couches de communication de sécurité sont impliquées dans la production du message.

NOTE La mise en œuvre peut être assurée par une diversité des matériels et/ou des logiciels.

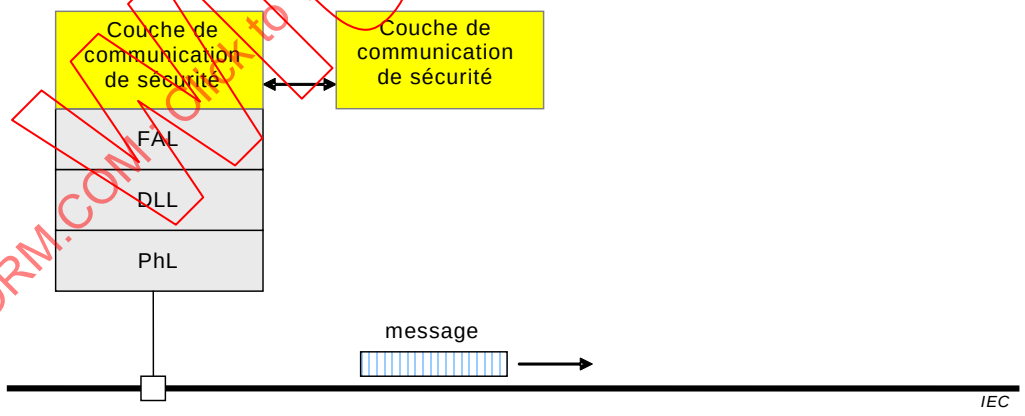


Figure A.1 – Modèle A

A.3 Modèle B (redondance complète)

Le modèle B de la Figure A.2 présente un système dans lequel les couches de communication de sécurité, les couches de transmission et les supports de transmission sont doublés.

Chaque SCL génère un SPDU à partir des mêmes données de sécurité et l'envoie sur le bus de terrain joint. Les messages des deux canaux de communication de sécurité sont vérifiés et contre-vérifiés.

Les couches et les supports de transmission peuvent être de types différents.

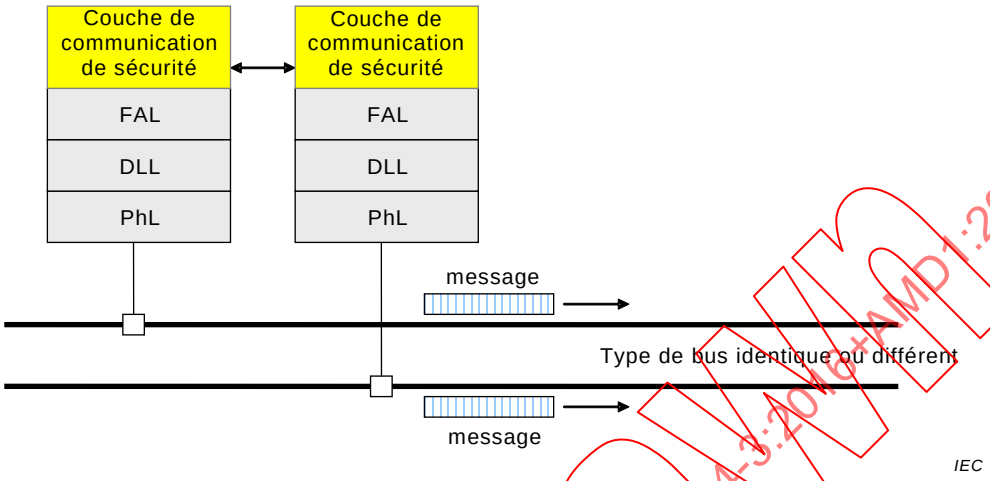


Figure A.2 – Modèle B

A.4 Modèle C (messages redondants, FAL et SCL, canal unique)

Le Modèle C de la Figure A.3 présente un système avec redondance complète des composants de l'appareil de bus de terrain et un seul support de transmission.

Deux SCL génèrent des SPDU à partir des mêmes données de sécurité. Les SPDU sont envoyés à des moments différents sur le même bus de terrain au moyen de messages différents. Les messages des deux canaux de communication de sécurité sont à la fois vérifiés et contre-vérifiés par ces deux canaux.

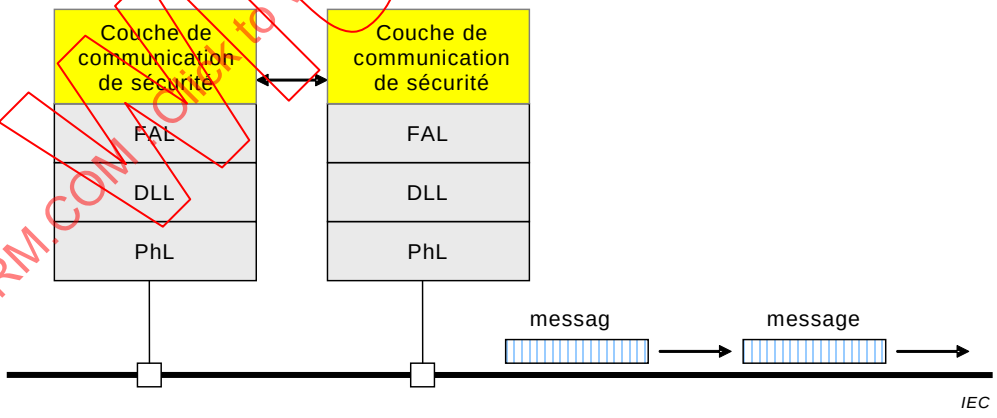


Figure A.3 – Modèle C

A.5 Modèle D (messages redondants et SCL, canal unique et FAL)

Le Modèle D de la Figure A.4 présente un système avec deux couches de communication de sécurité tandis que les couches de transmission n'existent qu'une seule fois.

Deux SCL génèrent des SPDU à partir des mêmes données de sécurité. Les SPDU sont envoyés à des moments différents sur le même bus de terrain au moyen de messages différents. D'autre part, les deux SPDU peuvent être envoyés comme des champs distincts dans le même message.

Les messages des deux couches de communication de sécurité sont indépendamment vérifiés et contre-vérifiés.

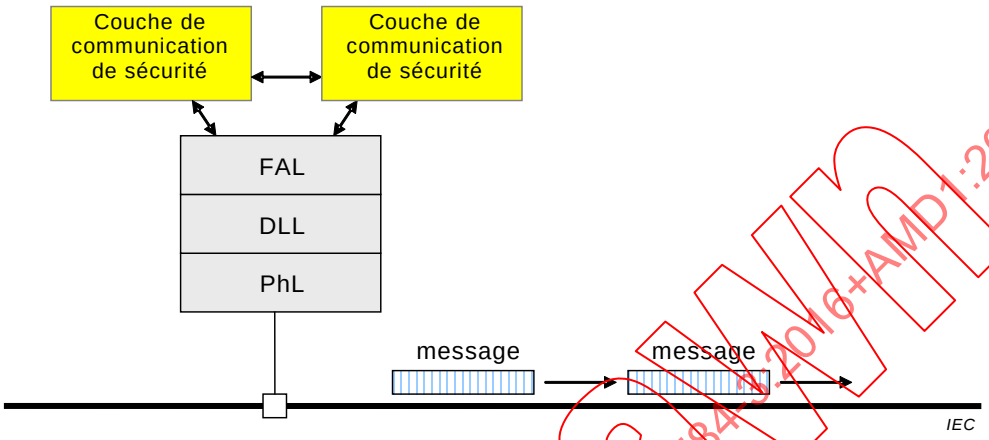


Figure A.4 – Modèle D

Annexe B
(normative)

Modèle de canal de communication de sécurité qui utilise le contrôle d'erreurs CRC

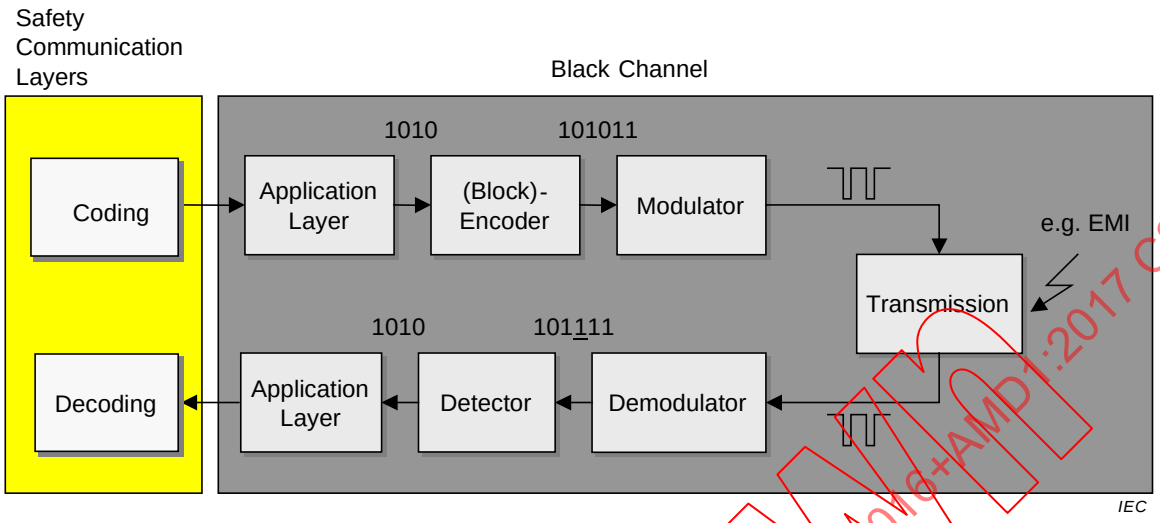
B.1 Vue d'ensemble

La présente Annexe B comporte un modèle de canal noir pour les calculs d'intégrité des données. L'utilisation de ce modèle est recommandée, sauf si l'application d'un modèle différent peut se révéler plus appropriée pour un FSCP particulier.

B.2 Modèle de canal pour calculs

Le modèle présenté à la Figure B.1 permet de calculer/d'évaluer en premier lieu la probabilité d'occurrence d'un certain nombre de bits perturbés au sein de la couche de communication de sécurité. Les différentes considérations relatives aux erreurs spécifiques qui se produisent sur le canal noir ne sont pas traitées dans la présente annexe.

Le modèle suppose que le canal noir et que la couche de communication de sécurité utilisent tous les deux des mécanismes de détection d'erreurs indépendants. En cas de défaillance du mécanisme de détection d'erreurs du canal noir, le mécanisme de même nature de la couche de communication de sécurité doit pouvoir à lui seul fournir le taux d'erreurs résiduelles nécessaire. Un mécanisme de détection d'erreurs fonctionnel au sein du canal noir élimine certaines configurations d'erreurs sur les bits; de ce fait, le mécanisme de détection d'erreurs de la couche de communication de sécurité est tenu de prendre en compte un certain modèle d'erreurs sur les bits. Les équations de base suivantes peuvent être utilisées pour des évaluations simplifiées des taux d'erreurs résiduelles ou comme base d'application de méthodes plus complexes.



Anglais	Français
Safety Communication Layers	Couches de communication de sécurité
Black Channel	Canal noir
Coding	Codage
Decoding	Décodage
Application Layer	Couche d'application
(Block)-Encoder	Codeur (de bloc)
Modulator	Modulateur
Detector	Détecteur
Demodulator	Démodulateur
e.g. EMI	Par exemple, EMI

Figure B.1 – Canal de communication avec perturbation

Un canal binaire est appelé canal symétrique lorsque les probabilités P relatives aux deux directions de perturbation pour un bit sont égales: 1→0 et 0→1 (voir la Figure B.2). Il est par ailleurs supposé que tous les paquets de bits ont la même probabilité d'erreurs sur les éléments binaires P_e = P.

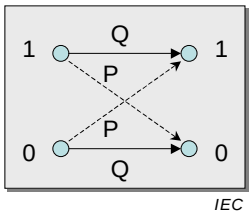


Figure B.2 – Canal symétrique binaire (BSC)

Les données de sécurité sont généralement transmises en blocs d'une certaine longueur binaire n. Dans ce cas, la probabilité d'erreurs pour un nombre k de bits perturbés (dans un bloc de longueur binaire n) peut être calculée à l'aide de l'Equation (B.1) indiquée ci-dessous.

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

Si le bloc contient un codage fictif qui permet de détecter les configurations d'erreurs jusqu'à d-1, comme illustré à la Figure B.4 avec une distance de Hamming d, une probabilité d'erreurs résiduelles de limite supérieure $R_{UL}(P_e)$ peut être calculée à l'aide de l'Equation (B.2) indiquée ci-dessous.

NOTE Un codage avec cette caractéristique n'existe pas dans la réalité, d'où l'appellation "fictif".

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

Cette équation simplifiée ne tient cependant pas compte du fait qu'un seul bit de parité (distance de Hamming d = 2) permet de détecter un plus grand nombre de configurations d'erreurs qu'un seul 1 bit. En l'absence de toute autre méthode ou de toute autre approximation, la somme de toutes les configurations d'erreurs individuelles non détectables doit être appliquée pour des calculs exacts.

B.3 Probabilité d'erreurs sur les éléments binaires Pe

Une probabilité d'erreurs sur les éléments binaires (Pe) de 10^{-4} en présence d'un brouillage électromagnétique continu entraînerait une interruption de la communication (déclenchement de nuisance) dans le cas d'un échange de données cycliques (par exemple, expiration du temps de fonctionnement du chien de garde après un nombre trop élevé de tentatives). Ces déclenchements de nuisance peuvent normalement être limités par une installation correcte (par exemple, blindage, liaison équipotentielle).

La conception d'une couche de sécurité avec un Pe de 10^{-4} n'est pas recommandée, dans la mesure où l'existence de brouillages par rafales simples avec de nombreux bits perturbés est commune dans les environnements industriels.

Pour pouvoir détecter ce type de perturbations, il convient que les mécanismes de détection d'erreurs soient suffisamment puissants pour obtenir la probabilité d'erreurs résiduelles totale exigée à un niveau de probabilité Pe 100 fois supérieur à 10^{-4}, c'est-à-dire 10^{-2}.

A moins de pouvoir démontrer une meilleure (plus faible) probabilité d'erreurs, une valeur maximale de 10^{-2} doit donc être utilisée pour la probabilité d'erreurs sur les éléments binaires.

B.4 Contrôle de redondance cyclique

B.4.1 Généralités

Le taux d'erreurs résiduelles, qui repose sur la détection au moyen d'un mécanisme CRC pour le BSC, peut être calculé à l'aide de l'Equation (B.3) ci-dessous (probabilité d'erreurs résiduelles pour les polynômes CRC).

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

où

A_i est le facteur de distribution du code (déterminé par une simulation sur ordinateur ou une analyse mathématique);

n est le nombre de bits dans le bloc, y compris sa signature CRC;

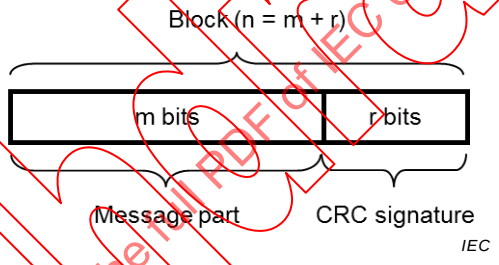
P_e est la probabilité d'erreurs sur les éléments binaires.

Les enquêtes sur la méthode de contrôle de redondance cyclique (CRC) ont montré que l'équation peut utiliser un facteur de pondération 2^{-r} pour la classe particulière appropriée des polynômes CRC et ce, pour obtenir une approximation (voir l'Equation (B.4) ci-dessous – approximation de probabilité d'erreurs résiduelles pour les polynômes CRC).

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

La fonction (courbe) de cette équation d'approximation (B.4) peut fournir de plus faibles (meilleures) valeurs de probabilité d'erreurs résiduelles que des calculs exacts (voir [31] pour un exemple). La valeur la plus défavorable est 2^{-r} pour une probabilité d'erreurs sur les éléments binaires élevée (proche de 0,5).

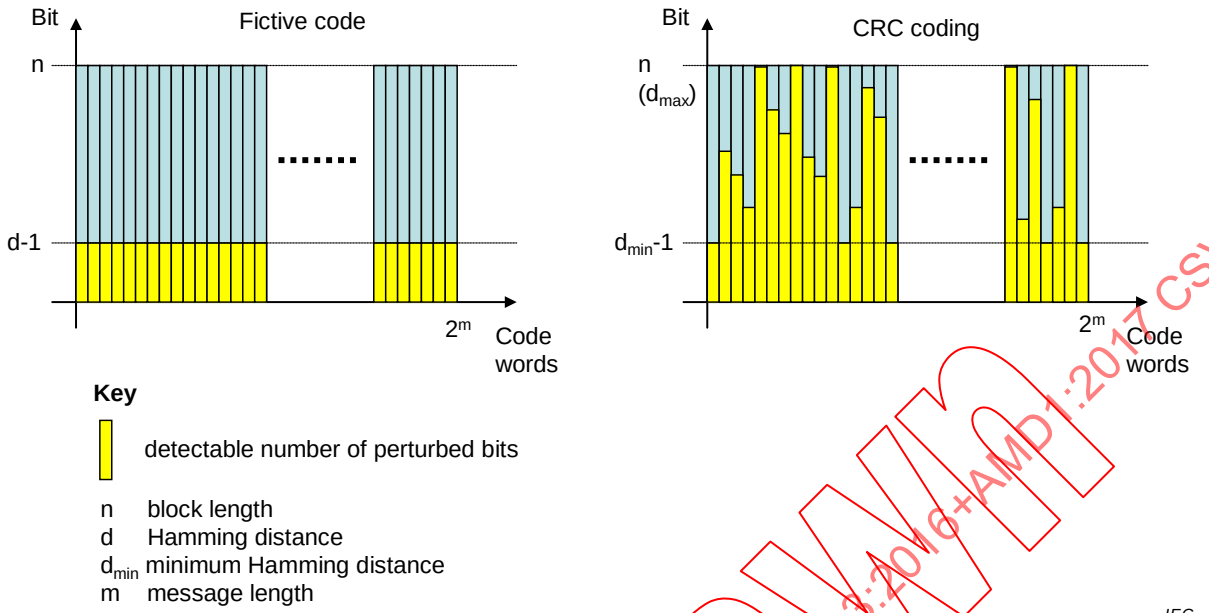
La valeur r représente le nombre de bits CRC ajoutés à la partie message sous forme de signature CRC pour permettre la détection d'erreurs, comme illustré dans la Figure B.3.



Anglais	Français
Block	Bloc
Message part	Partie Message
CRC signature	Signature CRC

Figure B.3 – Exemple de bloc avec une partie message et une signature CRC

La Figure B.4 présente le contexte d'utilisation des Equations (B.2) et (B.4).



Anglais	Français
Bit	Bit
Fictive code	Code fictif
CRC coding	Codage CRC
Code words	Mots de code
Key	Légende
detectable number of perturbed bits	nombre détectable de bits perturbés
block length	longueur de blocs
Hamming distance	distance de Hamming
minimum Hamming distance	distance de Hamming minimale
message length	longueur de message

Figure B.4 – Codes de blocs pour la détection d'erreurs

En règle générale, le mécanisme CRC fournit une meilleure probabilité d'erreurs résiduelles avec une plus petite longueur binaire de bloc n. Il existe ainsi une dépendance entre la longueur binaire de bloc n et la distance de Hamming minimale d_{min} pour un polynôme CRC approprié (voir le Tableau B.1).

Tableau B.1 – Exemple de dépendance d_{min} et de longueur binaire de bloc n

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

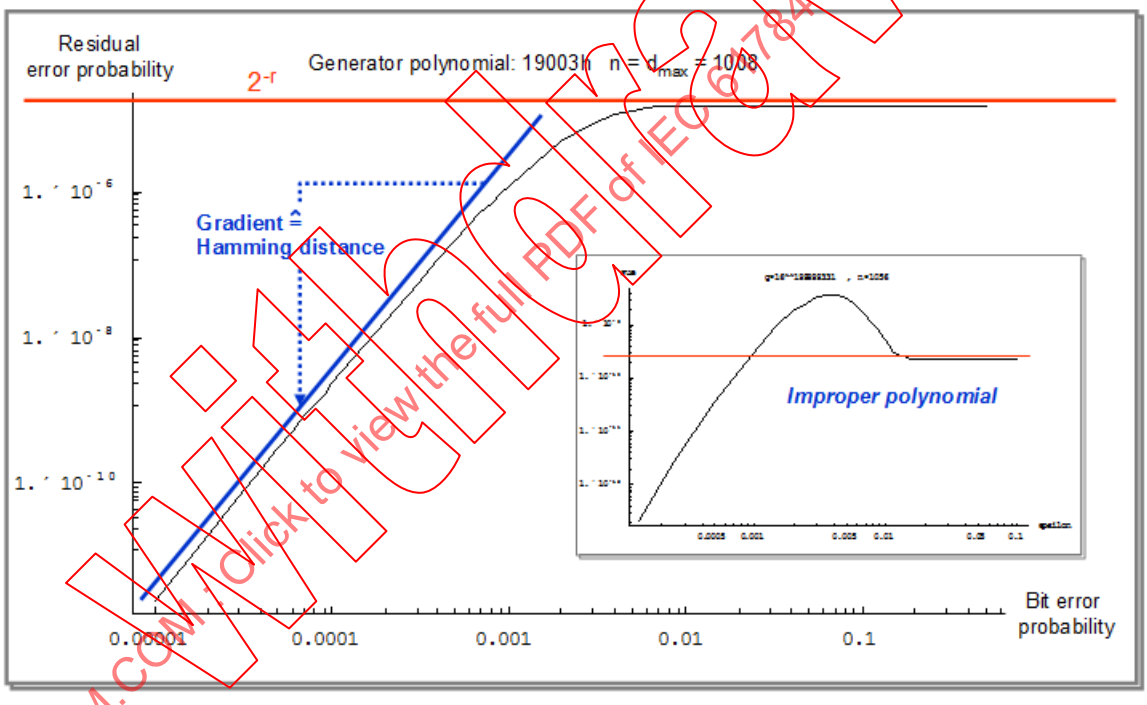
B.4.2 Considérations relatives aux polynômes CRC

Les polynômes CRC appropriés se caractérisent par une pente ascendante monotone de la fonction de probabilité d'erreurs résiduelles sur la probabilité d'erreurs sur les éléments binaires. La Figure B.5 présente la différence entre des polynômes CRC appropriés et

inappropriés. Il est vivement recommandé d'utiliser les seuls polynômes CRC appropriés afin de simplifier la démonstration des taux d'erreurs résiduelles suffisants. Plusieurs méthodes scientifiques de calcul de ce type de fonctions existent, [29], [33] et [34] par exemple. Il est nécessaire de vérifier pour toutes les longueurs de bloc de sécurité prévues si le polynôme est approprié ou non (voir le Tableau B.1). Des polynômes inappropriés peuvent présenter une meilleure probabilité d'erreurs résiduelles à des probabilités élevées d'erreurs sur les éléments binaires (2^{-r}) qu'avec des probabilités moins élevées d'erreurs sur les éléments binaires ($>2^{-r}$). En cas d'utilisation de polynômes CRC inappropriés, la valeur la plus défavorable ($>2^{-r}$) doit être utilisée, tandis que pour des polynômes appropriés, la valeur 2^{-r} est suffisante pour obtenir une estimation de la probabilité d'erreurs résiduelles.

NOTE Plus d'informations peuvent être trouvées en [32].

Dans certains cas, une fonction (courbe) particulière d'un polynôme générateur de CRC choisi peut fournir des valeurs de probabilité d'erreurs résiduelles moins élevées (meilleures) jusqu'à la limite de probabilité d'erreurs sur les éléments binaires exigée de 10^{-2}. Il est alors vivement recommandé d'appliquer les valeurs les plus défavorables 2^{-r} ou $> 2^{-r}$, respectivement, dans la mesure où seuls les messages avec des erreurs sur les éléments binaires de poids fort (erreurs sur les éléments binaires non réparties de manière égale) peuvent atteindre la couche de communication de sécurité.



Anglais	Français
Residual error probability	Probabilité d'erreurs résiduelles
Generator polynomial	Polynôme générateur
Gradient	Gradient
Hamming distance	Distance de Hamming
Improper polynomial	Polynôme inapproprié
Bit error probability	Probabilité d'erreurs sur les bits

n = nombre de bits dans un bloc, y compris la signature CRC r.

Figure B.5 – Polynômes CRC appropriés et inappropriés

Le gradient de la pente constitue une mesure de la distance de Hamming minimale des longueurs particulières du polynôme CRC et des blocs.

Le codage CRC assure une bonne protection contre le brouillage électromagnétique de type rafale. Tout paquet d'erreurs qui peut atteindre la longueur de la signature CRC en bits sera détecté.

Annexe C
(informative)

Structure des parties spécifiques à la technologie

Toutes les parties de la présente norme spécifiques à la technologie sont numérotées conformément à leur numéro CPF défini dans l'IEC 61784-1 ou l'IEC 61784-2.

EXEMPLE La partie spécifique à la technologie qui contient les spécifications sur les profils de communication de sécurité fonctionnelle du CPF 33 serait l'IEC 61784-3-33.

Toutes les parties spécifiques à la technologie ont la même structure générale, afin de faciliter la comparaison entre les différentes technologies. Cette structure est détaillée au Tableau C.1.

Tableau C.1 – Structure commune des paragraphes pour les parties spécifiques à la technologie

N° d'article et de paragraphe	Titre	Sommaire
	Introduction	Cette introduction est commune à toutes les parties de l'IEC 61784-3
1	Domaine d'application	Ce domaine d'application est normalisé pour toutes les parties de l'IEC 61784-3
2	Références normatives	Documents normatifs pour cette partie
3	Termes, définitions, symboles, abréviations et conventions	—
3.1	Termes et définitions	—
3.1.1	Termes et définitions communs	Termes communs utilisés dans la présente partie
3.1.2	CPF X: Termes et définitions supplémentaires	Termes spécifiques à la technologie utilisés dans la présente partie
3.2	Symboles et abréviations	—
3.2.1	Symboles et abréviations communs	Symboles communs utilisés dans la présente partie
3.2.2	CPF X: Symboles et abréviations supplémentaires	Symboles spécifiques à la technologie utilisés dans la présente partie
3.3	Conventions	Conventions qui permettent de décrire les différents éléments de la couche de communication de sécurité (par exemple, tables d'états, diagrammes séquentiels)
4	Présentation générale de FSCP X/1 (Safetyname™)	Présentation générale du profil de communication de sécurité fonctionnelle et des informations d'introduction pertinentes (y compris les objectifs et les motivations technologiques)
5	Généralités	—
5.1	Documents externes de spécifications applicables au profil	Liste des documents de référence exigés par les technologies, notamment ceux qui n'ont pu être énumérés à l'Article 2 (dans la mesure où il ne s'agit pas de normes "officielles" de l'IEC ou de l'ISO, par exemple documents des consortiums) et qui ont ainsi été inclus dans la bibliographie, accompagnés de tous les documents "exclusivement informatifs".
5.2	Exigences fonctionnelles de sécurité	Peut comporter la description des états de sécurité (voir IEC 61508-1:2010, 7.10.2.6)
5.3	Mesures de sécurité	Peut comporter les mesures de 5.4 à prendre en compte

N° d'article et de paragraphe	Titre	Sommaire
5.4	Structure de la couche de communication de sécurité	Peut comporter la décomposition de la SCL
5.5	Relations avec la FAL (et DLL, PhL)	Peut comporter les diagnostics existants, les services et les contraintes prévus (par exemple, "à utiliser conjointement avec FSCP x/y")
5.5.1	Types de données	Liste des types de données définis dans l'IEC 61158 utilisés par le profil
6	Services de la couche de communication de sécurité	Peut comporter les objets d'application utilisés, les services de diagnostic
7	Protocole de couche de communication de sécurité	Le premier paragraphe est énuméré ci-dessous, les autres peuvent être ajoutés si nécessaire Peut comporter les mécanismes temporels spécifiques, diagrammes d'états, organigrammes séquentiels, réaction à la mise sous tension et hors tension, protocole de diagnostic et diagnostic correspondant
7.1	Format PDU de sécurité	Comprend la définition détaillée des formats PDU de sécurité (message). Comportera plusieurs paragraphes afin de spécifier les différents éléments de format (par exemple, spécification du CRC de sécurité)
8	Gestion de la couche de communication de sécurité	Comprend les spécifications relatives aux aspects suivants du paramétrage: – données de paramétrage de sécurité fournies par un autre appareil de sécurité (un serveur de paramétrage, par exemple) – données de paramétrage de sécurité fournies par un outil (description de l'appareil, par exemple) (y compris toutes les mesures exigées pour protéger le stockage, la manutention et le transfert)
9	Exigences pour le système	Les premiers paragraphes sont énumérés ci-dessous; d'autres peuvent être ajoutés si nécessaire
9.1	Voyants et commutateurs	Spécifications relatives aux voyants des appareils, mais aussi au comportement et aux fonctions des commutateurs
9.2	Guide d'installation	Références d'articles détaillées de l'IEC 61918 ou autres documents pertinents
9.3	Temps de réponse de la fonction de sécurité	Calculs et exemples associés de temps de réaction pertinents pour la technologie (par exemple, temps de réaction le plus défavorable de la boucle de sécurité)
9.4	Durée des demandes	Spécifications relatives à la durée des demandes internes aux appareils
9.5	Contraintes liées au calcul des caractéristiques des systèmes	Comprend les tentatives de canal noir, le nombre de télégrammes par seconde et le nombre de collecteurs de messages
9.6	Maintenance	Spécifications relatives au comportement du système en cas de réparation et de remplacement des appareils
9.7	Manuel de sécurité	Le cas échéant, comprend les informations minimales exigées par le profil à inclure dans le manuel de sécurité
9.8	Canaux de transmission sans fil	Ce paragraphe est facultatif. Le cas échéant, il comprend les exigences spécifiques en cas de transmission sans fil
9.9	Classes de conformité	Ce paragraphe est facultatif. Le cas échéant, il comprend des exigences de conformité supplémentaires pour le protocole de bus de terrain de base
10	Evaluation	Comprend les informations sur les exigences d'évaluation
Annexe A (informative)	Informations supplémentaires pour les profils de communication de sécurité fonctionnelle de CPF X	Annexe informative obligatoire utilisée pour fournir des informations non normatives supplémentaires sur le protocole. En l'absence de ces informations, elle contiendra alors la phrase suivante: "Il n'existe aucune information supplémentaire sur ce FSCP".

N° d'article et de paragraphe	Titre	Sommaire
A.1	Calcul de la fonction de hachage	Par exemple, algorithmes pour le calcul CRC
	Bibliographie	Références bibliographiques pertinentes pour cette partie

Annexe D
(informative)

Lignes directrices pour l'évaluation

D.1 Vue d'ensemble

Ces lignes directrices sont destinées à l'évaluation et aux essais des systèmes de communication utilisés pour la transmission des messages relatifs à la sécurité. La communication de sécurité peut se produire entre différentes unités de traitement d'un système de commande de sécurité et/ou entre les capteurs/actionneurs intelligents de sécurité et les unités de traitement d'un système de commande de sécurité.

Il est vivement recommandé d'utiliser ces lignes directrices d'évaluation d'un profil de communication ou d'un système de communication de sécurité particulier, ainsi que des appareils relatifs à la sécurité qui utilisent ces profils.

Les documents fournis pour l'essai ou l'évaluation doivent spécifier les conditions de fonctionnement exactes conformément à 5.10.2. Aucun écart par rapport à ces conditions n'est admis, quelles que soient les circonstances.

Si un système de communication de sécurité fait partie intégrante d'un appareil relatif à la sécurité pour lequel il existe une norme de produits (par exemple, IEC 61496-1), ce produit et les composantes de communication de sécurité associées doivent satisfaire aux exigences du degré mentionné dans le domaine d'application de la norme correspondante ou comme défini dans un profil de communication de sécurité spécifique défini dans la série IEC 61784-3.

NOTE L'IEC TR 62685 est un guide d'accompagnement qui fournit des informations sur les aspects d'évaluation supplémentaires d'appareils de sécurité pour la communication de sécurité fonctionnelle, comme des bancs d'essai, la preuve de l'augmentation de l'immunité aux perturbations (CEM pour la sécurité fonctionnelle), la sécurité électrique et d'autres exigences environnementales.

D.2 Types de canaux

D.2.1 Généralités

L'Article D.2 définit deux types généraux de concepts de communication de sécurité: la méthode du canal noir et la méthode du canal blanc. Les présentes lignes directrices couvrent les deux concepts.

D.2.2 Canal noir

Conformément à la définition 3.1.5, la communication de sécurité de type canal noir n'exige que des preuves de conception ou de validation de la couche de communication de sécurité (SCL) conformément à l'IEC 61508. Le concepteur d'un appareil de sécurité peut utiliser un composant matériel/logiciel préalablement évalué et agréé, qui fournit les fonctions particulières de la SCL. Si le concepteur met en œuvre ce composant conformément à la méthode spécifiée, il peut se passer d'une évaluation de sécurité conformément à l'IEC 61508. Les efforts peuvent ainsi se réduire à l'évaluation de la technologie relative à la sécurité de l'appareil et à la mise en œuvre correcte de la composante SCL.

Evaluation: Vérification de la documentation et mise en œuvre dans le système comme spécifié; validation et vérification des calculs fournis par le fabricant; vérification des paramètres nécessaires pour ces calculs.

D.2.3 Canal blanc

Conformément à la définition 3.1.55, la communication de sécurité de type canal blanc exige que tous les composants matériels et logiciels soient conçus, mis en œuvre et validés conformément à l'IEC 61508. En raison du grand nombre de solutions possibles, les présentes lignes directrices n'apportent de l'aide que pour aborder les aspects liés à l'assurance d'intégrité des données.

NOTE Plus d'informations peuvent être trouvées dans l'IEC 62280.

Les méthodes individuelles du canal blanc peuvent en principe être évaluées par l'un des modèles présentés à l'Annexe A.

D.3 Considérations relatives à l'intégrité des données pour les méthodes du canal blanc

D.3.1 Généralités

En matière d'intégrité des données, deux classes de canaux blancs peuvent être identifiées, comme illustré en D.3.2 et en D.3.3.

D.3.2 Modèles B et C

Cette méthode considère qu'aucun des canaux du système de communication de bus n'est sécurisé. Les couches de protocole sont redondantes et deux messages sont transmis. Les mesures d'intégrité des données du système de communication de bus s'appliquent de ce fait dans leur intégralité. En cas de défaillance de l'un des deux canaux, une détection d'erreurs suffisante est impossible. Certains systèmes de communication de bus permettent, en raison de leur architecture, aux autres participants de vérifier chaque message et ainsi de détecter déjà le plus grand nombre de possibilités d'erreurs.

NOTE 1 Les modèles B et C peuvent tous deux être réalisés par une solution canal blanc ou une solution canal noir.

NOTE 2 Les équations utilisées dans le présent D.3.2 peuvent également s'appliquer aux systèmes du canal noir.

La méthode suivante repose sur le concept de "redondance avec contre-vérification", comme décrit en 5.4.8. Cela signifie, dans le cas d'un double transfert du SPDU et d'une comparaison bit par bit au niveau du récepteur, que la condition préalable à une erreur non détectée est la corruption identique des deux messages. La probabilité d'erreurs résiduelles peut être calculée conformément à l'Annexe B. La probabilité d'une combinaison d'erreurs particulière sur les bits dans chaque message est identique et dans ce cas l'expression est mise au carré. Les possibilités des combinaisons d'erreurs sur les bits sont conformes à celles d'un message unique (coefficients binomiaux).

Il convient que les FSCP ajustent les mesures individuelles de manière à pouvoir envisager une indépendance maximale. À défaut, il est nécessaire d'utiliser des équations plus complexes en fonction de de la dépendance.

Le même facteur 2^{-r} se révèle efficace (voir l'Annexe B) pour la détermination de l'assurance d'intégrité des données via une signature CRC; l'Equation (D.1) fournit par ailleurs une estimation de la probabilité d'erreurs résiduelles.

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

NOTE 3 Cette équation ne peut être appliquée que pour des polynômes appropriés (voir B.4.2). Voir [31].

Une analyse réalisée conformément à D.3.3 est exigée, accompagnée d'un calcul basé sur l'Equation (D.2) pour une évaluation complète de la probabilité d'erreurs résiduelles dans le cas d'une solution de canal blanc.

NOTE 4 Voir l'IEC 62280 pour plus d'informations.

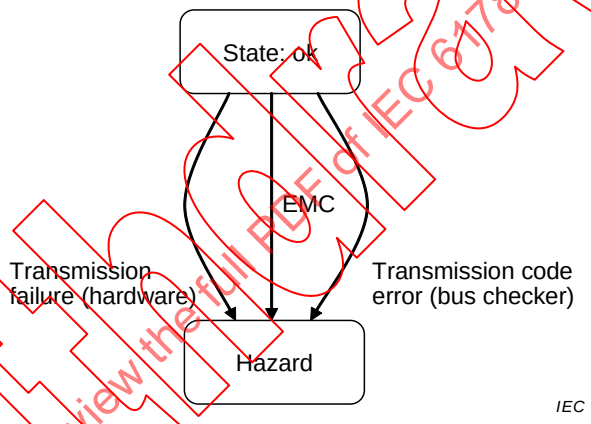
Le calcul de $\Lambda_{SCL}(P_e)$ s'inspire de 5.8.1 (Equation (1)).

L'évaluation de sécurité complète doit être effectuée conformément à l'IEC 61508 (par exemple, analyse du mode de défaillance et des effets, proportion de défaillances en sécurité, erreurs de cause commune).

Evaluation: Vérification de la documentation et mise en œuvre dans le système comme spécifié; validation et vérification des calculs fournis par le fabricant; vérification des paramètres nécessaires pour ces calculs.

D.3.3 Modèles A et D

Cette méthode repose sur les mesures de détection des erreurs des canaux de transmission des bus existants et complète ces dernières par des mesures supplémentaires applicables à la couche de communication de sécurité superposée pour atteindre le SIL souhaité.



Anglais	Français
State: ok	Etat: ok
EMC	CEM
Transmission failure (hardware)	Défaillance de transmission (matériel)
Transmission code error (bus checker)	Erreur de code de transmission (vérificateur de bus)
Hazard	Danger

Figure D.1 – Modèle de Markov de base

Dans cette méthode, les dangers pour la sécurité issus des défaillances des circuits de protocole de bus nécessitent de tenir compte de leur tolérance aux anomalies du matériel et de leur durée de vie prévue.

Dans ce cas, une analyse de Markov peut être exprimée par trois possibilités de transition fondamentales (Figure D.1):

- messages d'anomalies non détectés produits par des défaillances réelles du matériel dans les couches de transmission, qui aboutissent à la transmission de messages corrompus (R_{HW});
- messages défectueux accompagnés d'erreurs sur les bits non détectées provoquées par un brouillage électromagnétique (CEM) susceptible de se produire comme partie intégrante d'un fonctionnement normal (R_{EMC});

- messages d'anomalies non détectés provoqués par des défaillances dans la partie de vérification correspondante du bus du canal de transmission (R_{TC}).

NOTE 1 Cette analyse de Markov est déduite de l'IEC 62280.

La probabilité d'erreurs résiduelles R_{AD} du système est la somme des probabilités individuelles (Equation (D.2)). Le calcul de $\Lambda_{SCL}(p_e)$ s'inspire de 5.8.1 avec la probabilité d'erreurs résiduelles:

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

où

R_{AD} est la probabilité d'erreurs résiduelles du système pour les modèles A et D;

R_{HW} est la probabilité d'erreurs résiduelles pour les défauts qui résultent de défaillances matérielles;

R_{EMC} est la probabilité d'erreurs résiduelles pour les défauts qui résultent d'un brouillage électromagnétique;

R_{TC} est la probabilité d'erreurs résiduelles pour les défauts qui résultent de défaillances des mécanismes de vérification du bus.

L'évaluation de sécurité complète doit être effectuée conformément à l'IEC 61508 (par exemple, analyse du mode de défaillance et des effets, proportion de défaillances en sécurité, erreurs de cause commune).

NOTE 2 Voir l'IEC 62280 pour plus d'informations.

Evaluation: Vérification de la documentation et mise en œuvre dans le système comme spécifié; validation et vérification des calculs fournis par le fabricant; vérification des paramètres nécessaires pour ces calculs.

D.4 Vérification des mesures de sécurité

D.4.1 Généralités

Cette partie des lignes directrices d'évaluation spécifie les exigences de vérification pour un profil de communication de sécurité particulier.

D.4.2 Mise en œuvre

Les messages à transmettre en toute sécurité doivent être produits de la même manière (conformément au SIL exigé). Le support de transmission (par exemple, ligne de bus avec les ASIC d'interface) n'est pour sa part pas considéré comme sécurisé. Les mesures de sécurité relèvent de la seule responsabilité des unités de traitement de la source de messages et du collecteur de messages. Cela concerne les solutions de canal noir et de canal blanc.

Evaluation: Les exigences de l'IEC 61508 ou d'autres normes comme l'IEC 61784-3 doivent être prises en compte et vérifiées. Ces exigences ne relèvent pas du domaine d'application des présentes lignes directrices d'évaluation et sont définies de manière normative.

D.4.3 Principe de "mise hors tension pour déclenchement"

Un mécanisme de délai (par exemple, temporisateur) doit être utilisé dans tous les cas.

Evaluation: Voir 5.4.4.

D.4.4 Etat de sécurité

Un mécanisme de détection d'erreurs et de réaction doit être placé sur le récepteur chargé d'établir une réaction relative à la sécurité pour atteindre un état de sécurité dans le temps toléré pour les anomalies du processus.

Evaluation: Vérification de la documentation et de la mise en œuvre; mesure du temps de réaction de l'appareil de sécurité qui utilise une communication de sécurité dans les conditions les plus défavorables du système (par exemple, en présence d'erreurs ou de défaillances).

D.4.5 Erreurs de transmission

Lorsque des erreurs de transmission conformément à 5.3 se produisent, une réaction aux anomalies définies doit se déclencher (demande d'interruption, par exemple).

Evaluation: Vérification de la documentation, mise en œuvre, calcul si nécessaire et essai de fonctionnement; essais de fonctionnement étendus qui s'inspirent de l'IEC 61508.

D.4.6 Réaction de sécurité et temps de réponse

Le temps de réponse de la fonction de sécurité maximal spécifié par le fabricant et le temps exigé à une réaction totale relative à la sécurité ne doivent pas être dépassés, même en présence d'erreurs et de défaillances.

NOTE La vitesse de transmission et les temps de réaction ou de réponse de certains systèmes de bus dépendent du nombre de participants. Si une vitesse de transmission ou si le temps de réaction ou de réponse sont relatifs à la sécurité, une limitation du nombre de participants peut se révéler nécessaire.

Evaluation: Vérification de la documentation et mise en œuvre; mesure des temps de réaction et/ou de réponse dans les conditions les plus défavorables du système particulier. Le fabricant du profil de communication de sécurité doit définir le nombre et la synchronisation des erreurs à prendre en compte.

D.4.7 Combinaison des mesures

Dans le cas de la transmission des messages relatifs à la sécurité sur les systèmes de bus, les mesures issues de celles citées en 5.4 doivent être combinées de manière à détecter chaque erreur décrite en 5.3 dans le temps toléré pour le traitement des anomalies du processus. Le Tableau 1 facilite le choix des mesures individuelles appropriées.

Evaluation: L'exhaustivité de toutes les mesures techniques appliquées doit être vérifiée conformément au Tableau 1. La mise en œuvre de ces mesures doit être conforme au SIL exigé.

D.4.8 Absence de perturbations

Il doit être démontré que les participants à la communication non relative à la sécurité ne perturbent pas les participants de la communication de sécurité.

Evaluation: L'exhaustivité de toutes les mesures techniques appliquées doit être vérifiée conformément au Tableau 1. La mise en œuvre de ces mesures doit être conforme au SIL exigé.

D.4.9 Causes d'anomalies supplémentaires (canal blanc)

Outre les méthodes déjà décrites d'estimation des erreurs résiduelles qui utilisent le modèle BSC, d'autres causes d'anomalies, par exemple les erreurs de synchronisation de glissement dans les couches physiques et les couches de liaison de données, doivent être prises en compte et contrôlées.

NOTE Des détails sont fournis dans l'IEC 62280 ou en [28].

Evaluation: L'évaluation est hors du domaine d'application de la présente norme.

D.4.10 Bancs d'essai de référence et conditions de fonctionnement

Il convient, dans la mesure du possible, de soumettre à essai toutes les parties d'un système de communication de sécurité en même temps. Toutefois, si des parties d'un système de communication de sécurité sont soumises à essai séparément, il convient que le profil de communication de sécurité particulier définisse les systèmes de référence (bancs d'essai) et/ou les simulateurs, mais aussi que ceux-ci soient mis en œuvre, dans la mesure du possible, à l'aide de différents types d'appareils issus de différents fournisseurs.

Il convient que le banc d'essai tienne compte des conditions les plus défavorables, par exemple, longueur des connexions ou nombre d'appareils. Les signaux exigés pour la fonction de sécurité doivent être simulés ou générés d'une autre manière.

Les modes pertinents de fonctionnement doivent être définis pour une utilisation lors des essais, par exemple l'échange de données cycliques des valeurs du processus ou l'échange de données acycliques des données de paramétrage.

Evaluation: Essai et inspections conformes aux définitions du FSCP particulier ou aux spécifications du fabricant de l'EUT.

D.4.11 Appareil de vérification de conformité

Il convient de soumettre à essai la conformité à un FSCP particulier à l'aide d'un appareil de vérification de la conformité d'un profil défini par l'organisation relatif à la technologie liée au FSCP individuel.

NOTE Les essais de conformité incluent à la fois les essais positifs et les essais négatifs.

Evaluation: Essai et inspections conformes aux définitions du FSCP particulier.

Annexe E
(informative)

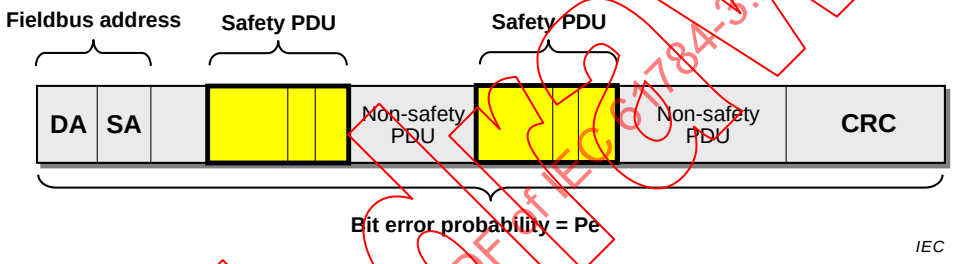
Exemples de mesures de sécurité de FSCP implicites et explicites

E.1 Généralités

Les exemples fournis de E.2 à E.7 illustrent les concepts de mesures de sécurité explicites et implicites.

E.2 Exemple de message de bus de terrain avec PDU de sécurité

La Figure E.1 présente des PDU de sécurité intégrés à un message de bus de terrain lors de la transmission.

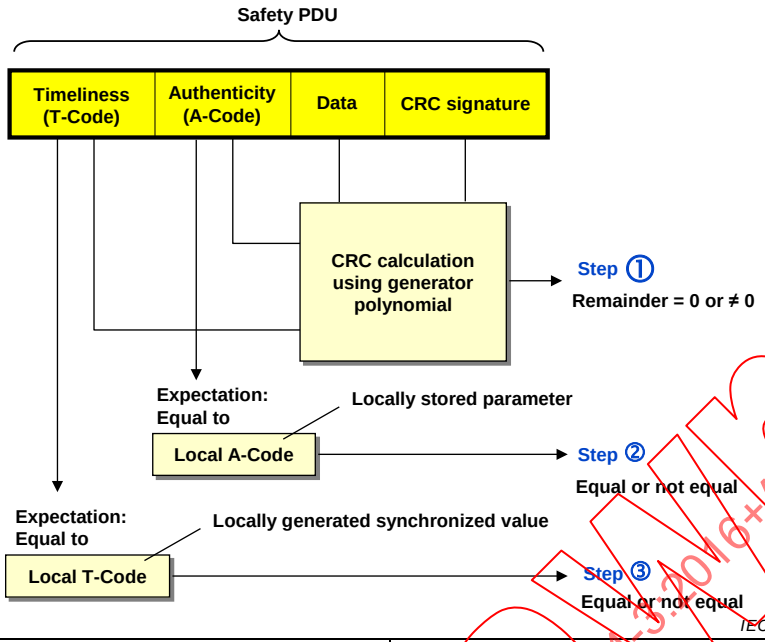


Anglais	Français
Fieldbus address	Adresse de bus de terrain
Safety PDU	PDU de sécurité
Non-safety PDU	PDU non relatif à la sécurité
Bit error probability	Probabilité d'erreurs sur les bits

Figure E.1 – Exemple de PDU de sécurité intégrés à un message de bus de terrain

E.3 Modèle avec mesures de sécurité totalement explicites

La Figure E.2 présente le modèle et la vérification de sécurité d'un PDU de sécurité avec des mesures de sécurité totalement explicites pour l'opportunité et l'authenticité.



Anglais	Français
CRC calculation using generator polynomial	Calcul de CRC à l'aide du polynôme générateur
Locally stored parameter	Paramètre stocké localement
Locally generated synchronized value	Valeur synchronisée générée localement
CRC signature	Signature CRC
Timeliness (T-code)	Opportunité (code T)
Authenticity (A-code)	Authenticité (code A)
Local A-code	Code A local
Local T-code	Code T local
Safety PDU	PDU de sécurité
Data	Données
Remainder	Reste
Expectation: equal to	Prévision: égal à
Step	Etape
Equal or not equal	Egal ou non égal

Figure E.2 – Modèle avec mesures de sécurité totalement explicites

La vérification est réalisée conformément aux étapes suivantes:

Etape ① Reste ≠ 0 → Toute erreur détectée

Reste = 0 → Données correctes ou incorrectes avec RR_I conformément à F.5.2.2

Etape ② Pas égal à → Toute erreur détectée

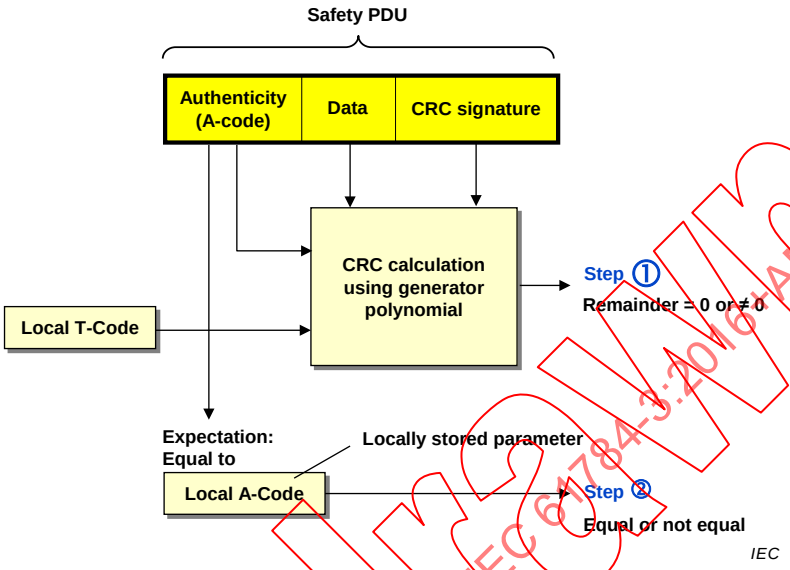
Egal à → Authenticité correcte ou incorrecte avec RR_A conformément à F.5.2.3

Etape ③ Pas égal à → Toute erreur détectée

Egal à → Opportunité correcte ou incorrecte avec RR_T conformément à F.5.2.4

E.4 Modèle avec mesures de sécurité explicites de code A et implicites de code T

La Figure E.3 présente le modèle et la vérification de sécurité d'un PDU de sécurité avec mesure de sécurité explicite pour l'authenticité et mesure de sécurité implicite pour l'opportunité.



Anglais	Français
CRC calculation using generator polynomial	Calcul de CRC à l'aide du polynôme générateur
Locally stored parameter	Paramètre stocké localement
CRC signature	Signature CRC
Authenticity (A-code)	Authenticité (code A)
Local A-code	Code A local
Local T-code	Code T local
Safety PDU	PDU de sécurité
Data	Données
Remainder	Reste
Expectation: equal to	Prévision: égal à
Step	Etape
Equal or not equal	Egal ou non égal

Figure E.3 – Modèle avec mesures de sécurité explicites de code A et mesures de sécurité implicites de code T

La vérification est réalisée conformément aux étapes suivantes:

Etape ① Reste ≠ 0 → Toute erreur détectée

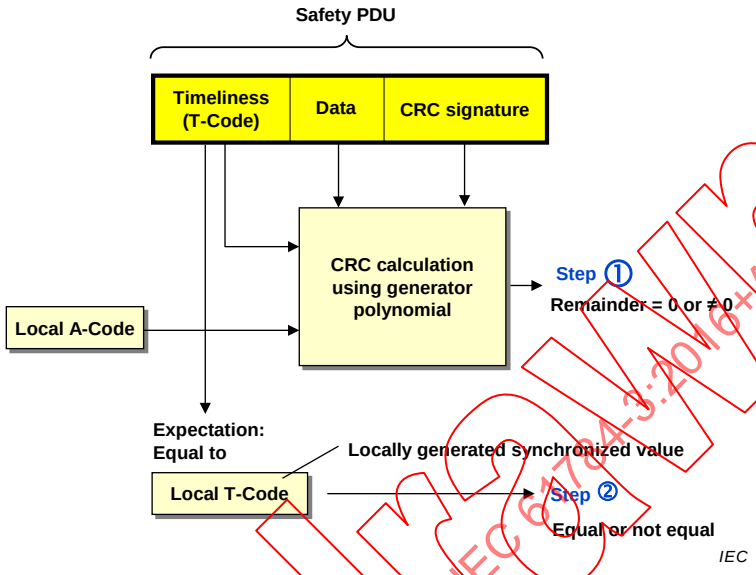
Reste = 0 → Données et opportunité correctes ou incorrectes avec RR

Etape ② Pas égal à → Toute erreur détectée

Egal à → Authenticité correcte ou incorrecte avec RR_A conformément à F.5.2.3

E.5 Modèle avec mesures de sécurité explicites de code T et implicites de code A

La Figure E.4 présente le modèle et la vérification de sécurité d'un PDU de sécurité avec mesure de sécurité explicite pour l'opportunité et mesure de sécurité implicite pour l'authenticité.



Anglais	Français
CRC calculation using generator polynomial	Calcul de CRC à l'aide du polynôme générateur
Locally generated synchronized value	Valeur synchronisée générée localement
CRC signature	Signature CRC
Timeliness (T-code)	Opportunité (code T)
Local A-code	Code A local
Local T-code	Code T local
Safety PDU	PDU de sécurité
Data	Données
Remainder	Reste
Expectation: equal to	Prévision: égal à
Step	Etape
Equal or not equal	Egal ou non égal

Figure E.4 – Modèle avec mesures de sécurité explicites de code T et mesures de sécurité implicites de code A

La vérification est réalisée conformément aux étapes suivantes:

Etape ① Reste ≠ 0 → Toute erreur détectée

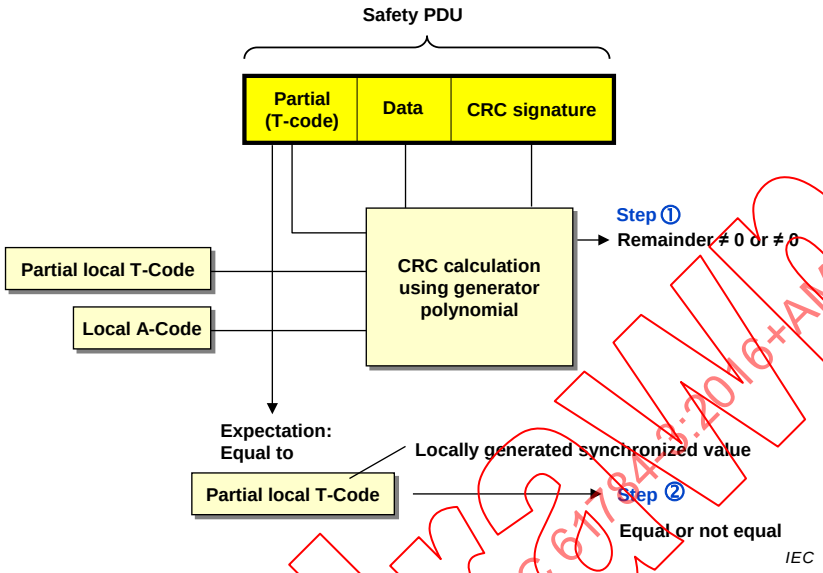
Reste = 0 → Données et authenticité correctes ou incorrectes avec RR

Etape ② Pas égal à → Toute erreur détectée

Egal à → Opportunité correcte ou incorrecte avec RR_T conformément à F.5.2.4

E.6 Modèle avec mesures de sécurité explicites et implicites divisées

La Figure E.5 présente le modèle et la vérification de sécurité d'un PDU de sécurité avec mesures de sécurité explicites et implicites divisées pour l'opportunité et mesures implicites pour l'authenticité.



Anglais	Français
CRC calculation using generator polynomial	Calcul de CRC à l'aide du polynôme générateur
Locally generated synchronized value	Valeur synchronisée générée localement
CRC signature	Signature CRC
Partial (T-code)	Partiel (code T)
Local A-code	Code A local
Partial local T-code	Code T local partiel
Safety PDU	PDU de sécurité
Data	Données
Remainder	Reste
Expectation: equal to	Prévision: égal à
Step	Etape
Equal or not equal	Egal ou non égal

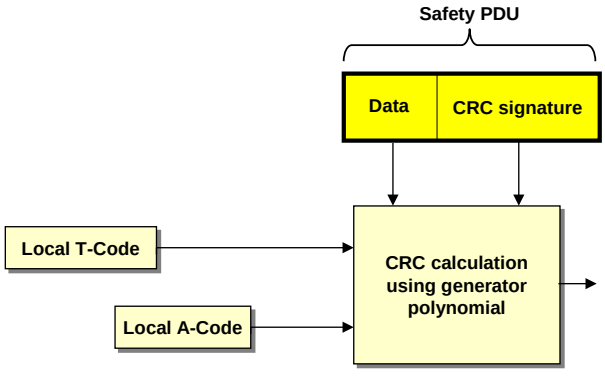
Figure E.5 – Modèle avec mesures de sécurité explicites et implicites divisées

La vérification est réalisée conformément aux étapes suivantes:

Etape ①	Reste ≠ 0	→	Toute erreur détectée
	Reste = 0	→	Données, Authenticité et Opportunité correctes ou incorrectes avec RR
Etape ②	Pas égal à	→	Toute erreur détectée
	Egal à	→	Opportunité correcte ou incorrecte avec RR

E.7 Modèle avec mesures de sécurité totalement implicites

La Figure E.6 présente le modèle et la vérification de sécurité d'un PDU de sécurité avec mesure de sécurité implicite pour l'authenticité et l'opportunité.



Anglais	Français
CRC calculation using generator polynomial	Calcul de CRC à l'aide du polynôme générateur
CRC signature	Signature CRC
Local A-code	Code A local
Local T-code	Code T local
Safety PDU	PDU de sécurité
Data	Données
Remainder	Reste
Step	Etape

Figure E.6 – Modèle avec mesures de sécurité totalement implicites

La vérification est réalisée conformément à l'étape suivante:

Etape ① Reste ≠ 0 → Toute erreur détectée

Reste = 0 → Données, Authenticité et Opportunité correctes ou incorrectes avec RR

E.8 Ajout à l'Annexe B – Influence des codes implicites sur l'exactitude

La présence d'erreurs sur les éléments binaires associées à un code implicite erroné peut influencer l'exactitude du polynôme de CRC. L'application de codes implicites pour les mesures de sécurité donne donc lieu à un effort supplémentaire.

En raison de la diversité des méthodes possibles, aucune formule générique ne peut être fournie. Il incombe au FSCP individuel de démontrer des probabilités d'erreurs résiduelles suffisantes.

Annexe F
(informative)

Modèles étendus pour l'estimation du taux total d'erreurs résiduelles

F.1 Applicabilité

La présente Annexe F spécifie des modèles étendus supplémentaires pour l'estimation du taux total d'erreurs résiduelles pour un FSCP, afin d'évaluer ce FSCP. Ces modèles sont destinés à remplacer les modèles actuellement définis en 5.8 dans les éditions ultérieures de la présente norme.

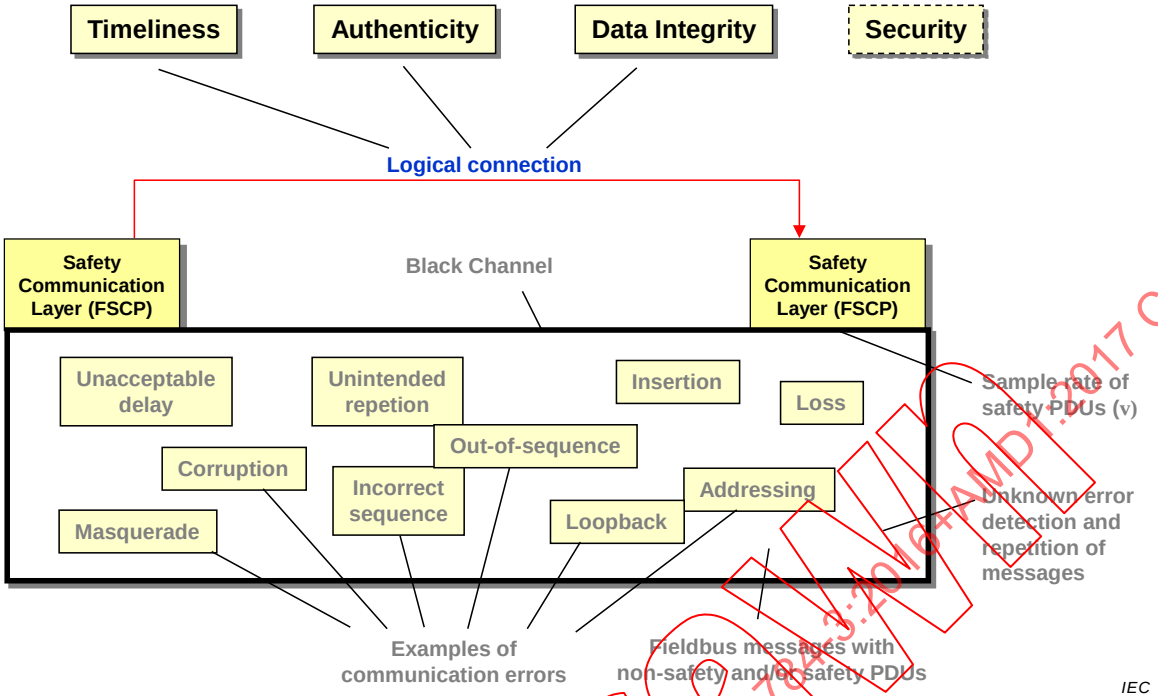
Les FSCP sont donc exemptés d'une nouvelle évaluation, conformément à la présente Annexe F, jusqu'à l'édition 4, où le contenu de l'actuelle Annexe F remplacera l'actuel 5.8.

F.2 Modèles généraux pour les communications du canal noir

Tous les FSCP partent du principe que toutes les communications de sécurité fonctionnelle sont établies par un canal noir (voir 5.2.3).

Pour quantifier convenablement l'erreur résiduelle des mesures de sécurité, il est important en premier lieu de contraindre le modèle pour le canal noir en fonction de la SCL du FSCP. Cela permet de définir correctement le type de messages, ainsi que les types et les taux d'erreurs que le concepteur de la SCL du FSCP doit prendre en compte avec les mesures de sécurité.

La Figure F.1 présente un canal noir qui contient différents types de communications: messages de bus de terrain avec PDU de sécurité et PDU non relatif à la sécurité.



Anglais	Français
Timeliness	Opportunité
Authenticity	Authenticité
Data Integrity	Intégrité des données
Security	Sécurité
Logical connection	Connexion logique
Safety communication Layer (FSCP)	Couche de communication de sécurité (FSCP)
Black channel	Canal noir
masquerade	déguisement
corruption	corruption
Unaccepted delay	Retard inacceptable
Unintended repetition	Répétition non prévue
Loopback	Bouclage
Addressing	Adressage
Examples of communication errors	Exemples d'erreurs de communication
Fieldbus messages with non-safety and/or safety PDU	Messages de bus de terrain avec PDU non relatif à la sécurité et/ou PDU de sécurité
Unknown error detection and repetition of messages	Détection d'erreur inconnue et répétition de messages
Sample rate of safety PDUs	Fréquence d'échantillonnage de PDU de sécurité
insertion	insertion
loss	perte
Out-of sequence	Hors séquence
Incorrect sequence	Séquence incorrecte

Figure F.1 – Canal noir du point de vue d'un FSCP

Le canal noir comprend les couches sous-jacentes de communication de bus de terrain en dessous de la SCL, ainsi que toute communication supplémentaire entre la FAL et la SCL dans un appareil.

Les erreurs dans le canal noir peuvent être générées à partir de plusieurs sources:

- corruption de bits de messages dans le support de transmission; ou
- anomalies aléatoires du matériel et erreurs systématiques du matériel électronique et des logiciels dans le canal noir.

La fréquence de l'échange de messages dans le canal noir peut être différente de la fréquence à laquelle la SCL échantillonne et traite les PDU de sécurité.

F.3 Identification des propriétés de sécurité générique

Le Tableau 1 énumère les éventuelles mesures de sécurité discrètes, qui, seules ou en combinaison, contribuent aux propriétés de sécurité générique suivantes pour les messages (voir la Figure F.1):

- intégrité des données;
- authentification (y compris le rejet de déguisement);
- opportunité.

La remise correcte du contenu des messages issus d'une source de messages aux collecteurs de messages configurés est la propriété d'intégrité des données. La remise des messages issus d'une source de messages correcte aux collecteurs de messages configurés associés est la propriété d'authentification. Le rejet de bits aléatoires au niveau d'un collecteur de messages dont l'occurrence semble correcte est la propriété du rejet de déguisement. La remise en temps voulu de messages entre une source de messages et un collecteur de messages dans un intervalle de temps configuré est la propriété d'opportunité.

NOTE La sécurité est une autre propriété connue qui ne relève pas du domaine d'application de la présente norme. Les questions relatives à la sécurité sont traitées dans l'IEC 62443.

Un autre aspect de sécurité générique qui doit être pris en compte est la configuration et/ou le paramétrage du FSCP (voir l'Article F.12).

Une anomalie dans l'une de ces mesures de sécurité générique peut conduire à un état dangereux ou à un démarrage intempestif.

Le fournisseur d'un FSCP doit fournir la preuve d'un taux total d'erreurs résiduelles suffisant en fonction des trois propriétés de sécurité générique spécifiées à l'Article F.10.

F.4 Hypothèses pour les calculs de taux d'erreurs résiduelles

L'Annexe F donne des exemples des types de formules utilisés pour le calcul du taux d'erreurs résiduelles, sur la base des hypothèses formulées en ce qui concerne le canal noir et la SCL. D'autres formules doivent être utilisées dans les cas où ces hypothèses peuvent s'avérer inadaptées à un type donné de SCL.

Les hypothèses générales suivantes sont valides pour toutes les formules définies à l'Annexe F:

a) en supposant que le taux de défaillance d'un appareil de canal noir moyen s'élève à 100 FIT, la SCL doit partir du principe qu'un taux de défaillance de canal noir est égal à 10 000 fois cette valeur. Le taux de défaillance du matériel électronique est donc supérieur à 10^{-3}/h (10^{6} FIT) pour chaque élément de réseau actif ou partie de bus de terrain d'un appareil de sécurité;

NOTE 1 L'éventuelle défaillance d'un appareil peut devenir continue tant qu'elle n'a pas été détectée et corrigée. Cela inclut les erreurs permanentes, intermittentes et transitoires.

NOTE 2 Un taux de défaillance moins prudent que 10^{-3} peut être supposé pour un FSCP, si ce FSCP passe sa fonction de sécurité à l'état sûr en cas de détection d'une ou de plusieurs défaillances dangereuses de canal noir (voir l'état d'anomalie à la Figure 7), s'il ne reprend son fonctionnement qu'après avoir été réparé et s'il peut être démontré qu'un taux de défaillance de 10^{-3} rendrait donc inopérant le canal de communication de sécurité.

b) la présence d'appareils de stockage et de retransmission est prise en compte, si cela s'avère pertinent pour le FSCP;

c) la fonction de hachage du PDU de sécurité est différente de celle utilisée par la DLL du bus de terrain sous-jacent (cela peut être garanti par la conception ou des procédures administratives);

d) la fonction de hachage du PDU de sécurité est un CRC qui ne comprend pas de mécanisme de correction d'erreurs;

e) la fonction de hachage du PDU du canal noir peut comporter des mécanismes de correction d'erreurs;

f) il est attribué à chaque connexion logique un code d'authentification unique;

g) chaque fois que les valeurs fixes les plus défavorables sont utilisées dans les formules de probabilités d'erreurs ou d'événements (état de l'art), les FSCP peuvent spécifier leurs propres valeurs si une preuve suffisante est fournie;

h) chaque fois qu'un seul mécanisme est utilisé pour détecter plusieurs types d'erreurs, ces types d'erreurs doivent être pris en compte aussi bien individuellement qu'en combinaison lors du calcul de la probabilité d'erreurs résiduelles.

F.5 Taux d'erreurs résiduelles

F.5.1 Mécanismes explicites et implicites

Le mécanisme explicite comprend des données qui correspondent aux mesures de sécurité de FSCP, par exemple le numéro de séquence, l'horodatage et l'authentification de la connexion dans le PDU de sécurité.

Le mécanisme implicite ne transmet pas réellement toutes les données qui correspondent aux mesures de sécurité, mais les utilise pour calculer la signature CRC complète, conformément à l'hypothèse que le récepteur dispose de connaissances équivalentes.

NOTE Le mécanisme implicite est généralement utilisé pour accueillir des systèmes limités avec des messages de canal noir à taille fixe ou à taux de transmission lente.

Les FSCP spécifiés dans la série IEC 61784-3 peuvent être classés en catégorie explicite, implicite et partiellement explicite/implicite (voir les exemples à l'Annexe E). En raison de la diversité des méthodes possibles, aucune formule générique ne peut être fournie pour la catégorie implicite. Il incombe au FSCP individuel de démontrer des probabilités d'erreurs résiduelles suffisantes. La présente Annexe F ne traite donc que de la catégorie explicite.

F.5.2 Calculs de taux d'erreurs résiduelles

F.5.2.1 Généralités

Des exemples d'équations pour le calcul des taux d'erreurs résiduelles sont donnés de F.5.2.4 à F.5.2.5 pour la catégorie FSCP explicite en fonction des longueurs des numéros de séquence, des horodatages et des données d'authentification de connexion. Des FSCP spécifiques peuvent fournir leurs équations, le cas échéant.

Une SCL peut limiter certains champs à seulement certaines valeurs. Cela est représenté par le coefficient d'unicité des champs limités (RP_U) inclus dans les calculs du taux d'erreurs résiduelles, le cas échéant. Il est donné par l'Équation (F.1).

$$RP_U = \frac{V_{A1}}{V_{R1}} \times \frac{V_{A2}}{V_{R2}} \times \ldots \times \frac{V_{AN}}{V_{RN}} \qquad (F.1)$$

où

RP_U est la probabilité d'erreurs résiduelles pour d'autres champs d'unicité qui distinguent un PDU de sécurité convenablement formaté;

V_{AN} est le nombre de valeurs accepté par un collecteur dans le champ de données N;

V_{RN} est le nombre de valeurs qui représente la plage totale du champ de données N.

F.5.2.2 Contribution des erreurs d'intégrité des données (RR_I)

Un exemple de calcul du taux d'erreurs résiduelles pour l'intégrité des données RR_I est présenté dans l'Equation (F.2).

$$RR_I = RP_I \times v \times RP_U \times RP_{FSCP} \qquad (F.2)$$

où

RR_I est le taux d'erreurs résiduelles pour l'intégrité des données;

RP_I est la probabilité d'erreurs résiduelles pour l'intégrité des données;

v est le nombre maximal d'échantillons de SPDU produit par la SCL (fréquence d'échantillonnage) par heure;

RP_U est la probabilité d'erreurs résiduelles pour d'autres champs d'unicité qui distinguent un PDU de sécurité convenablement formaté;

RP_{FSCP} est la probabilité d'erreurs résiduelles pour d'autres mesures uniques au FSCP.

F.5.2.3 Contribution des erreurs d'authenticité (RR_A)

Trois facteurs expliquent ce taux résiduel:

a) un PDU mal acheminé;

b) une erreur non détectée de corruption de données et;

c) l'erreur doit donner lieu à une mise en correspondance du code d'authentification.

Un exemple de calcul du taux d'erreurs résiduelles pour l'authenticité RR_A est présenté dans l'Equation (F.3).

$$RR_A = RP_I \times 2^{-LA} \times R_A \times RP_{FSCP} \qquad (F.3)$$

où

RR_A est le taux d'erreurs résiduelles pour l'authenticité pour les PDU de sécurité mal acheminés;

RP_I est la probabilité d'erreurs résiduelles pour l'intégrité des données;

LA est la longueur binaire de l'authentification de la connexion;

R_A est le taux d'occurrence des PDU de sécurité mal acheminés;

RP_{FSCP} est la probabilité d'erreurs résiduelles pour d'autres mesures uniques au FSCP.

NOTE L'utilisation de 2^{-LA} suppose une répartition uniforme des configurations d'erreurs dans le code A.

F.5.2.4 Contribution des erreurs d'opportunité (RR_T)

Un exemple de calcul du taux d'erreurs résiduelles pour l'opportunité RR_T est présenté dans l'Equation (F.4).

$$RR_T = 2^{-LT} \times w \times R_T \times RP_{FSCP} \quad (F.4)$$

où

RR_T est le taux d'erreurs résiduelles pour l'opportunité;

LT est la longueur binaire du numéro de séquence;

w est la plage de valeurs (fenêtre) des horodatages acceptés ou des numéros de séquence pour la réception de PDU de sécurité;

R_T est le taux d'occurrence des PDU de sécurité à séquence incorrecte (la valeur ne peut pas dépasser v, comme indiqué en F.5.2.2);

RP_{FSCP} est la probabilité d'erreurs résiduelles pour d'autres mesures uniques au FSCP.

F.5.2.5 Contribution des erreurs de déguisement (RR_M)

Un exemple de calcul du taux d'erreurs résiduelles pour le déguisement RR_M est présenté dans l'Equation (F.5).

$$RR_M = 2^{-LA} \times 2^{-LT} \times w \times 2^{-r} \times RP_U \times 2^{-LR} \times R_m \quad (F.5)$$

où

RR_M est le taux d'erreurs résiduelles pour le déguisement;

LA est la longueur binaire de l'authentification de la connexion;

LT est la longueur binaire du numéro de séquence;

w est la plage de valeurs (fenêtre) des horodatages acceptés ou des numéros de séquence pour la réception de PDU de sécurité;

r est la longueur binaire de la signature CRC (si deux CRC avec polynômes indépendants sont utilisés, r est la somme des deux longueurs binaires correspondantes);

RP_U est la probabilité d'erreurs résiduelles pour d'autres champs d'unicité qui distinguent un PDU de sécurité convenablement formaté;

LR est la longueur binaire de la partie répétée du PDU de sécurité (pour la redondance avec contre-vérification, autrement LR = 0);

R_m est le taux d'occurrence pour les PDU de sécurité déguisés.

F.6 Intégrité des données

F.6.1 Considérations probabilistes

L'intégrité des données de propriété de sécurité générique exige de détecter l'erreur de communication suivante, conformément au Tableau 1:

- la corruption (voir 5.3.2).

L'assurance d'intégrité des données est une composante fondamentale de la couche de communication de sécurité pour atteindre un niveau d'intégrité de sécurité exigé. Les fonctions de hachage appropriées comme les bits de parité, le contrôle de redondance cyclique (CRC), la répétition de messages et/ou de données et des formes similaires de redondance doivent être appliquées.

Si la probabilité d'erreurs résiduelles des mesures d'intégrité des données dépend des valeurs de données de sécurité, les valeurs des cas les plus défavorables doivent être prises en compte.

Lors de l'application du contrôle de redondance cyclique (CRC) en tant que fonction de hachage, le concepteur d'un FSCP doit empêcher ou envisager l'éventualité que le canal noir utilise le même polynôme. Cela peut être accompli à l'aide de méthodologies.

EXEMPLES

Les éventuelles méthodologies comprennent:

– des mesures n'autorisant que des combinaisons spécifiques de FSCP et de CP;
– des mesures appropriées dans la conception de la SCL;
– des calculs du taux d'erreurs résiduelles avec 0,5 comme valeur de Pe.

F.6.2 Considérations déterministes

Outre les configurations de bits aléatoires, les configurations d'erreurs spécifiques suivantes doivent être évaluées: les données totalement inversées, les ensembles de données totalement "0" ou "1", les erreurs de glissement de synchronisation et les erreurs en rafale.

F.7 Authenticité

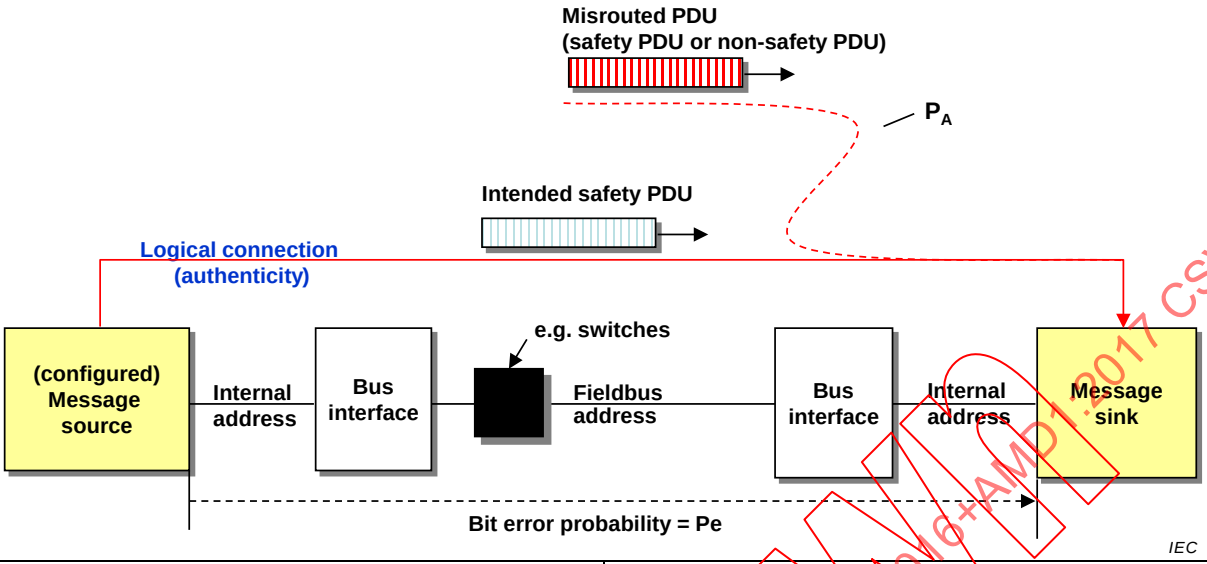
F.7.1 Généralités

L'authenticité de la propriété de sécurité générique exige de détecter les erreurs de communication suivantes, conformément au Tableau 1:

- l'adressage (voir 5.3.9);
- l'insertion (voir 5.3.7).

Le FSCP doit satisfaire à l'exigence suivante (voir Figure F.2):

- le collecteur de messages ne doit traiter que les données de sécurité intégrées à des messages correctement adressés et issus d'une source de messages authentifiée.



Anglais	Français
Misrouted PDU (safety PDU or non-safety PDU)	PDU mal acheminé (PDU de sécurité ou PDU non relatif à la sécurité)
Intended safety PDU	PDU de sécurité prévu
Logical connection (authenticity)	Connexion logique (authenticité)
(configured) Message source	Source de message (configurée)
Internal address	Adresse interne
Bus interface	Interface de bus
e.g. switches	Par exemple, commutateurs
Fieldbus address	Adresse de bus de terrain
Message sink	Collecteur de messages
Bit error probability	Probabilité d'erreurs sur les bits

Légende

PA Probabilité d'une erreur d'authenticité pour connexions logiques

Figure F.2 – Modèle pour la prise en compte de l'authentification

Ces exigences doivent être satisfaites durant toutes les phases de communication indiquées en 5.6 pour lesquelles l'authentification de connexion est pertinente (dépendant du FSCP). Les exclusions doivent être documentées dans le manuel de sécurité.

L'authentification empêche le traitement des données de sécurité dans un message reçu qui satisfait à tous les autres contrôles, mais qui ne constitue pas un message valide pour ce récepteur.

NOTE

Les éventuelles causes stochastiques de l'authenticité incorrecte incluent, sans toutefois s'y limiter:

– la falsification d'une adresse dans le message ou une erreur dans une liaison de communication interne (voir la Figure F.3), indépendamment du fait qu'elle soit liée à un mécanisme d'adressage non relatif à la sécurité ou relatif à la sécurité.

– les piles/couches de protocoles perturbées ou erronées dans le canal noir.

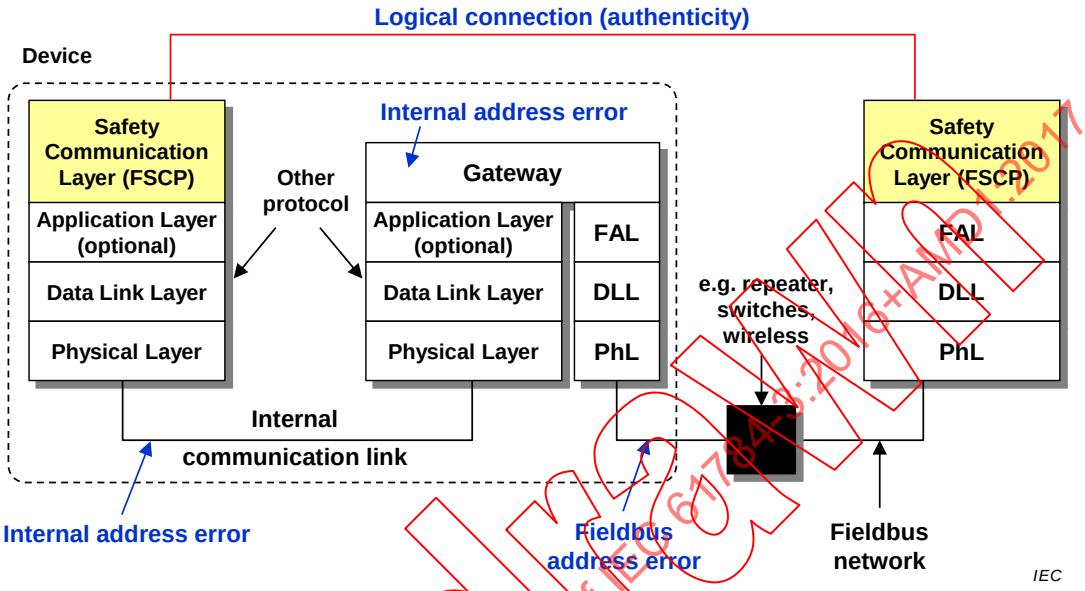
– les appareils de routage perturbés ou erronés, commutateurs ou routeurs par exemple.

– les passerelles perturbées ou erronées, coupleurs de bus par exemple.

– les messages en miroir d'appareils de canal noir perturbés ou erronés ("erreur de bouclage") ou les messages réacheminés par d'autres moyens.

– le mécanisme d'authentification contenu dans le collecteur de messages ne suffit pas pour faire la distinction entre les messages issus de différentes sources de messages.

La Figure F.3 présente les éventuelles erreurs d'adressage dues à des adresses corrompues au sein du système de communication de bus de terrain ou les éventuelles erreurs d'adressage internes (en raison de pointeurs corrompus au sein d'appareils E/S distants modulaires, par exemple).



Anglais	Français
Logical connection (Authenticity)	Connexion logique (Authenticité)
Device	Appareil
Safety communication layer (FSCP)	Couche de communication de sécurité (FSCP)
Application layer (optional)	Couche d'application (facultative)
Data link layer	Couche de liaison de données
Physical layer	Couche physique
Other protocol	Autre protocole
Internal address error	Erreur d'adresse interne
Gateway	Passerelle
Internal communication link	Liaison de communication Interne
Fieldbus address error	Erreur d'adresse de bus de terrain
Fieldbus network	Réseau de bus de terrain
e.g. repeater, switches, wireless	Par exemple, répéteur, commutateurs, sans fil

Figure F.3 – Bus de terrain et erreurs d'adresse internes

Des causes systématiques supplémentaires d'authenticité incorrecte peuvent être identifiées dans les procédures de configuration et de paramétrage, comme indiqué en F.12. Des mesures organisationnelles supplémentaires peuvent être exigées pour contrôler ces causes d'erreurs systématiques.

Une authentification de la connexion peut être utilisée pour identifier de manière unique et sans ambiguïté l'un des éléments suivants:

- une source de messages unique ou un collecteur de messages;
- une seule connexion entre une source de messages et un collecteur de messages;
- une connexion multiple entre une source de messages et plusieurs collecteurs de messages en cas de multidiffusion;

- une connexion de groupe entre plusieurs sources de messages et collecteurs de messages.

Plusieurs méthodes disponibles permettent d'éviter les erreurs d'authentification.

EXEMPLES

– Une authentification unique de connexion (par exemple, "Identifiant de connexion") qui est transmise avec chaque message FSCP.

– Une authentification unique de connexion stockée localement (par exemple, "Identifiant de connexion") cryptée par l'intermédiaire des fonctions de hachage comme les signatures CRC et transmise au collecteur de messages. Ce cryptage fait généralement partie des mesures d'intégrité des données totales des FSCP conformément à 5.9.

F.7.2 Taux d'erreurs résiduelles pour l'authenticité (RR_A)

Le taux d'erreurs résiduelles RR_A pour l'authenticité de la propriété de sécurité générique doit être calculé du point de vue du collecteur de messages, comme illustré à la Figure F.2.

Conformément à l'Article F.4 point a), une valeur de 10^{-3}/h par appareil doit être supposée pour le taux d'occurrence de PDU de sécurité mal acheminés (R_A), sauf spécification contraire.

Il est en outre supposé que R_A doit avoir la valeur de v (fréquence d'échantillonnage de SPDU) après la première occurrence d'un PDU de sécurité mal acheminé, jusqu'à ce que le système soit réparé.

Le taux d'erreurs résiduelles RR_A doit être suffisant pour toutes les phases de communication indiquées en 5.6 auxquelles se rapporte l'authentification de connexion (dépendant du FSCP).

Les mesures techniques d'authentification peuvent être complétées par des mesures organisationnelles, qui doivent être pratiquées dans le but de faciliter leur exécution par l'utilisateur (voir l'Article F.12).

F.8 Opportunité

F.8.1 Généralités

L'opportunité de la propriété de sécurité générique exige de détecter les erreurs de communication suivantes, conformément au Tableau 1:

- retard inacceptable (voir 5.3.6);
- répétition non prévue (voir 5.3.3);
- séquence incorrecte (voir 5.3.4);
- perte (voir 5.3.5).

Le FSCP doit satisfaire aux exigences suivantes:

- Le collecteur de messages traite des messages mis à jour;
- Le collecteur de messages surveille l'état de fonctionnement de la couche de sécurité de la source de messages.

NOTE 1 Selon qu'une communication est unidirectionnelle ou bidirectionnelle, un appareil peut fournir une source de messages et un collecteur de messages simultanément.

Les mesures techniques de l'opportunité peuvent être complétées par des mesures organisationnelles.

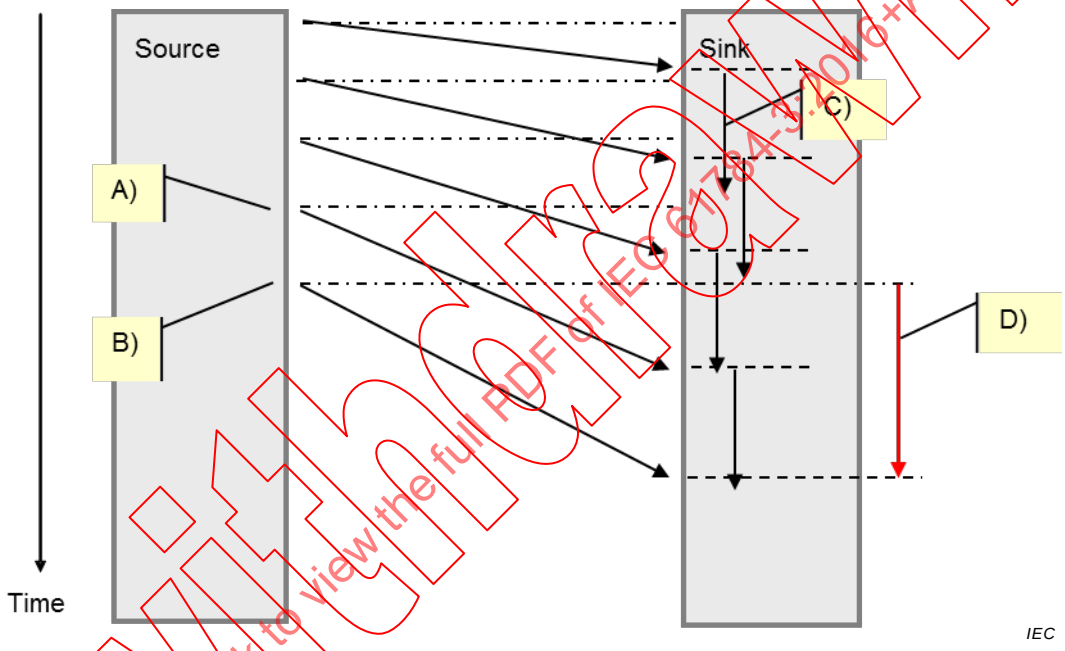
Les causes typiques de communications non opportunes qui doivent être prises en compte lors de la conception du FSCP sont des performances variables du canal noir.

EXEMPLES

Les variations de performances du canal noir peuvent être le résultat de:

– Débit insuffisant (par exemple, bande passante, trafic);
– Perte de la communication (temporaire ou totale);
– Temps de latence variable;
– latence en croissance progressive (voir Figure F.4);
– latence différente pour chaque paire de source de messages/collecteur de messages;
– Variations des temps de synchronisation d'horloge à la source de messages ou au collecteur de messages; ou
– une combinaison de ces éléments.

La Figure F.4 présente un exemple de latence de message du canal noir en croissance progressive.



Anglais	Français
Sink	Collecteur
Time	Durée

Légende

A) Les heures de départ des messages ne sont pas en concordance avec les heures de réception des messages.

B) L'heure de départ du message est antérieure à l'heure de réception du message précédent.

C) Un contrôle de temporisation a lieu dans le collecteur.

D) Un collecteur de messages ne peut pas déterminer les heures de départ des messages, les heures de réception des messages et les intervalles. Le retard du message peut être plus important que la temporisation, mais ne pas être détecté!

Figure F.4 – Exemple de latence de message en croissance progressive

Une autre question doit être examinée: la transmission imprévue à partir de la mémoire de messages ou de parties de messages.

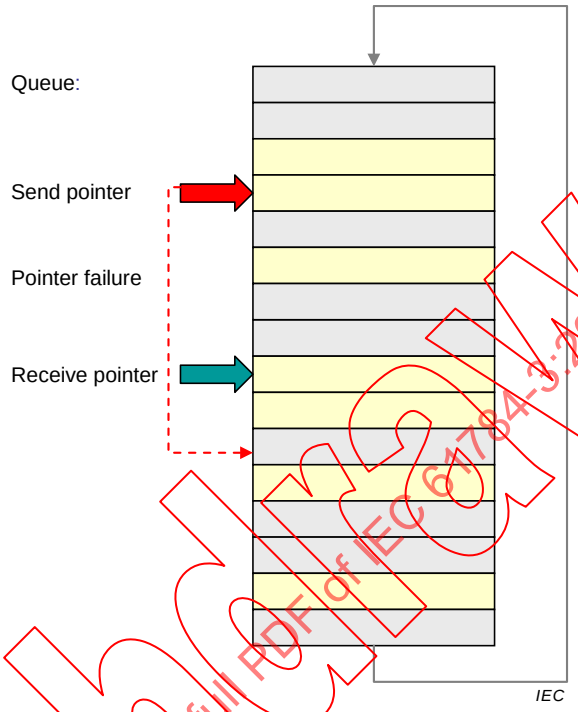
EXEMPLES

– Des éléments de réseau actifs, par exemple les commutateurs, les routeurs (voir la Figure 5).

– Les appareils de communication en dehors du système de communication défini (Internet ou introduits par des liaisons de communication sans fil, par exemple).

– la communication multi-itinéraire (par exemple Internet).

La Figure F.5 présente un exemple de transmission imprévue à partir de la mémoire due à la défaillance d'un élément de réseau actif, comme suit: "resquillage" dans une mémoire tournante où le pointeur d'émission dépasse le pointeur de réception, ce qui entraîne la vidange/l'envoi de l'ensemble de la file d'attente d'un commutateur.



Anglais	Français
Receive pointer	Pointeur de réception
Queue	File d'attente
Pointer failure	Défaillance de pointeur
Send pointer	Pointeur d'émission

Figure F.5 – Exemple de défaillance d'un élément de réseau actif

NOTE 2 Le canal noir peut inclure d'autres types d'éléments de stockage que les commutateurs.

Plusieurs méthodes permettent de détecter les erreurs résultant d'une transmission imprévue à partir de la mémoire.

EXEMPLES

– La communication cyclique avec surveillance de latences.

– Horloges synchronisées dans tous les appareils et horodatages des SPDU.

– Numérotation suffisamment ordonnée de la séquence de SPDU.

Dans chaque cas, la précision et les plages temporelles doivent satisfaire aux exigences découlant:

- des questions prévisionnelles de synchronisation de l'application de sécurité;
- du stockage potentiel de messages à l'intérieur ou à l'extérieur du système.

Le taux d'erreur pour les bases de temps dépassant les limites de sécurité spécifiées doit être déterminé au cours des évaluations de conception et de mise en œuvre conformément à la norme IEC 61508.

NOTE 3 L'utilisation d'une base de temps synchronisée à travers le réseau de sécurité fait partie des aspects de mise en œuvre.

F.8.2 Taux d'erreurs résiduelles pour l'opportunité (RR_T)

Dans un réseau relatif à la sécurité avec des éléments de stockage de messages (voir la Figure F.5), conformément à l'Article F.4 point a), une valeur de 10^{-3}/h par élément de stockage doit être supposée pour le taux d'erreurs d'opportunité (R_T), sauf spécification contraire.

La série de transmission imprévue à partir de la mémoire de SPDU doit être supposée ne pas être supérieure à 65 000.

F.9 Déguisement

F.9.1 Généralités

La propriété de sécurité de rejet de déguisement nécessite la détection de l'erreur de communication ci-après, conformément au Tableau 1:

- déguisement (voir 5.3.8).

En général, les PDU non relatifs à la sécurité (déguisement) sont plus susceptibles d'être détectés par la SCL, car ils ont à remplir toutes les conditions préalables (opportunité, authenticité et intégrité des données).

F.9.2 Autres termes utilisés pour calculer le taux d'erreurs résiduelles pour le rejet de déguisement (RR_M)

Conformément à l'Article F.4 point a), une valeur de 10^{-3}/h par appareil doit être supposée pour le taux d'occurrence de PDU de sécurité déguisés (R_m), sauf spécification contraire.

F.10 Calcul du taux total d'erreurs résiduelles

F.10.1 Sur la base de la somme des taux d'erreurs résiduelles

Le taux total d'erreurs résiduelles λ_{SC} pour le canal de communication de sécurité est la somme des taux individuels d'erreurs résiduelles RR_T, RR_A, RR_I et RR_M, comme indiqué dans l'Equation (F.6).

$$\lambda_{SC} = RR_T + RR_A + RR_I + RR_M \qquad \text{(F.6)}$$

où

λ_{SC} est le taux total d'erreurs résiduelles par heure pour le canal de communication de sécurité;

RR_T est le taux d'erreurs résiduelles par heure pour Opportunité (voir F.5.2.4);

RR_A est le taux d'erreurs résiduelles par heure pour Authenticité (voir F.5.2.3);

RR_I est le taux d'erreurs résiduelles par heure pour Intégrité des données (voir F.5.2.2);

RR_M est le taux d'erreurs résiduelles par heure pour le déguisement (voir F.5.2.5)

Le taux d'erreurs résiduelles de la SCL est calculé à partir du taux total d'erreurs résiduelles λ_{SC} des canaux de communication de sécurité et du nombre maximal de connexions logiques (m) autorisé dans une seule fonction de sécurité, comme indiqué dans l'Equation (F.7), ainsi que dans la Figure F.6 et la Figure F.7.

$$\lambda_{SCL} = \lambda_{SC} \times m \qquad \text{(F.7)}$$

où

λ_{SCL} est le taux d'erreurs résiduelles par heure de la SCL;

λ_{SC} est le taux d'erreurs résiduelles par heure par connexion logique (voir l'Equation (F.6))

m est le nombre maximal de connexions logiques (m) autorisé dans une seule fonction de sécurité.

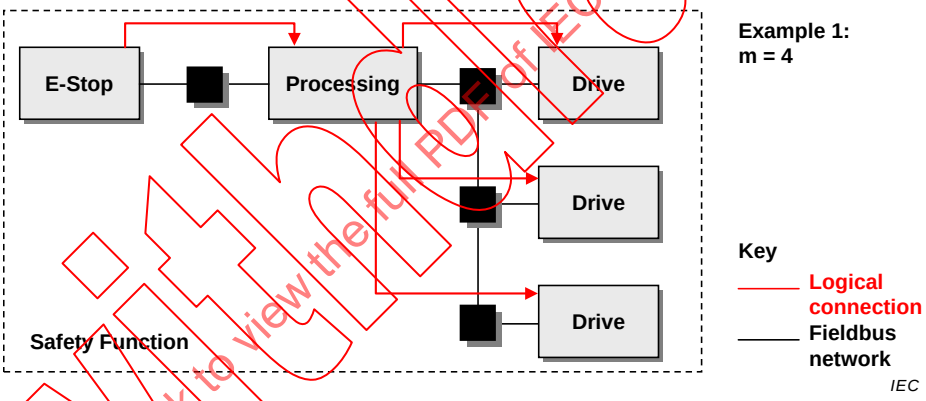
NOTE Cette équation suppose un échantillonnage cyclique de SPDU et le cas le plus défavorable dans lequel chaque PDU de sécurité transmis par le canal noir peut être erroné.

Le nombre m de connexions logiques dépend de l'application de la fonction de sécurité individuelle. La Figure F.6 et la Figure F.7 présentent la manière dont ce nombre peut être déterminé.

Les figures illustrent les connexions physiques avec d'éventuels composants réseaux, comme des répéteurs, des commutateurs ou des liaisons sans fil, ainsi que les connexions logiques entre les sous-systèmes impliqués dans la fonction de sécurité.

Les connexions logiques peuvent être basées sur des communications en diffusion unique ou en multidiffusion.

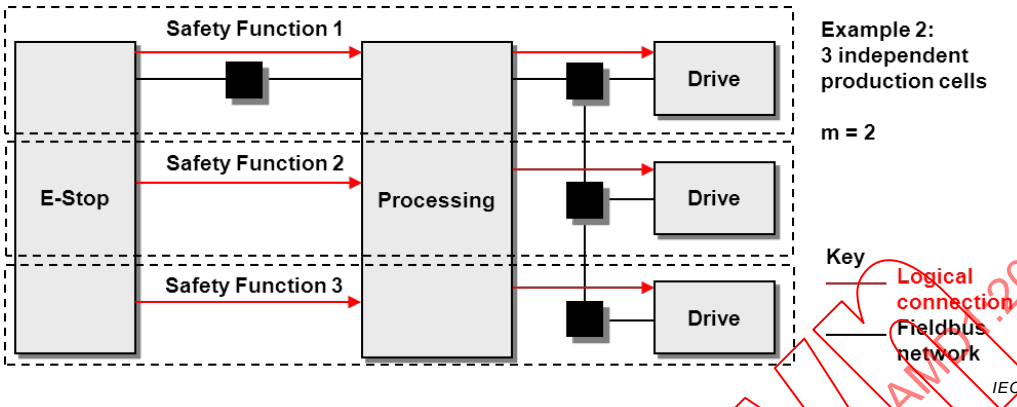
La Figure F.6 donne un exemple 1 d'une application où m = 4. Dans cette application, les trois entraînements sont considérés comme dangereux à un seul moment conformément à l'analyse des risques.



Anglais	Français
E-Stop	E-interruption
Processing	Traitement
Drive	Entraînement
Example 1	Exemple 1
Key	Légende
Logical connection	Connexion logique
Safety function	Fonction de sécurité
Fieldbus network	Réseau de bus de terrain

Figure F.6 – Exemple d'application 1 (m = 4)

La Figure F.7 donne un exemple 2 d'une application où m = 2. Dans cette application, un seul des trois entraînements est considéré comme dangereux à un seul moment conformément à l'analyse des risques.



Anglais	Français
Safety function	Fonction de sécurité
E-Stop	E-interruption
Processing	Traitement
Drive	Entraînement
Example 2: 3 independent production cells	Exemple 2: 3 cellules de production indépendantes
Key	Légende
Logical connection	Connexion logique
Fieldbus network	Réseau de bus de terrain

Figure F.7 – Exemple d'application 2 (m = 2)

F.10.2 Sur la base d'autres preuves quantitatives

La somme des taux d'erreurs résiduelles des propriétés de sécurité générique, comme illustré en F.10.1, est une méthode acceptable de calcul du taux total d'erreurs résiduelles pour un FSCP donné.

Il est possible d'utiliser des méthodes mathématiques combinées pour les calculs prenant en compte les effets croisés des mesures de sécurité individuelles et ainsi obtenir de meilleurs taux d'erreurs résiduelles.

Il est également possible d'utiliser directement les méthodes de l'IEC 61508 et de déterminer la proportion de défaillances en sécurité et la couverture de diagnostic du FSCP.

F.11 Taux total d'erreurs résiduelles et SIL

Un système de communication de sécurité fonctionnelle doit fournir un taux d'erreurs résiduelles en conformité à la présente norme. Le Tableau F.1 et le Tableau F.2 présentent la relation typique entre le taux d'erreurs résiduelles et le SIL, en fonction du principe que la contribution du système de communication de sécurité fonctionnelle ne dépasse pas 1 % par connexion logique de la fonction de sécurité.

Un temps de réponse de la fonction de sécurité doit être défini pour les deux systèmes avec un mode de sollicitation faible et élevée. Un taux nécessaire de SPDU doit de ce fait être garanti. La PFH qui correspond à un certain SIL doit être fournie dans tous les cas; la PFD_{avg} est quant à elle facultative.

Tableau F.1 – Relation typique entre le taux d'erreurs résiduelles et le SIL

Applicable pour les fonctions de sécurité jusqu'au SIL	Fréquence moyenne d'une défaillance dangereuse pour la fonction de sécurité (PFH)	Taux d'erreurs résiduelles maximal admissible pour une connexion logique de la fonction de sécurité (λ_{SC} (Pe))
4	$< 10^{-8}$/h	$< 10^{-10}$/h
3	$< 10^{-7}$/h	$< 10^{-9}$/h
2	$< 10^{-6}$/h	$< 10^{-8}$/h
1	$< 10^{-5}$/h	$< 10^{-7}$/h

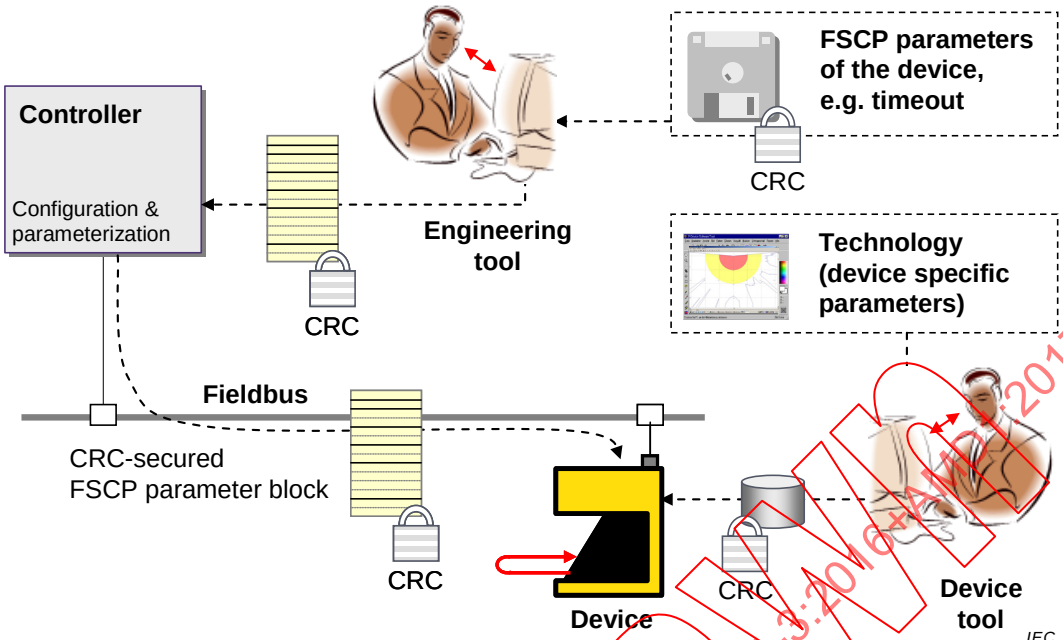
Tableau F.2 – Relation typique entre l'erreur résiduelle et le SIL

Applicable pour les fonctions de sécurité jusqu'au SIL	Probabilité moyenne d'une défaillance dangereuse en cas de sollicitation pour la fonction de sécurité (PFDavg)	Probabilité d'erreurs résiduelles maximale admissible pour une connexion logique de la fonction de sécurité
4	$< 10^{-4}$	$< 10^{-6}$
3	$< 10^{-3}$	$< 10^{-5}$
2	$< 10^{-2}$	$< 10^{-4}$
1	$< 10^{-1}$	$< 10^{-3}$

F.12 Configuration et paramétrage pour un FSCP

F.12.1 Généralités

La configuration et le paramétrage corrects des appareils de sécurité et de leur SCL au cours des différentes phases sont essentiels pour la sécurité fonctionnelle. L'ingénierie des fonctions de sécurité qui utilisent un FSCP comprend généralement la configuration, le paramétrage et des activités de programmation, comme illustré dans l'exemple de la Figure F.8.



Anglais	Français
Controller Configuration & parameterization	Contrôleur Configuration et paramétrage
CRC-secured	CRC sécurisé
Engineering tool	Outil technique
Technology (device specific parameters)	Technologie (paramètres spécifiques à l'appareil)
FSCP parameters of the device, e.g. timeout	Paramètres FSCP de l'appareil, par exemple, temporisation
Device tool	Outil d'appareil
Device	Appareil
Fieldbus	Bus de terrain
FSCP parameter block	Bloc de paramètres FSCP

Figure F.8 – Exemple de procédures de configuration et de paramétrage pour FSCP

La configuration nécessite d'utiliser un outil technique pour mettre en place la structure du réseau de bus de terrain, relier les appareils de terrain et attribuer des valeurs aux paramètres de la couche du canal noir, ainsi qu'aux paramètres FSCP comme l'authentification de connexion, la temporisation, la revendication de SIL, etc. Les appareils de terrain fournissent généralement une fiche technique sous forme électronique stockée dans un fichier qui peut être importé dans l'outil technique.

Après une session de configuration, les données de configuration, y compris les valeurs des paramètres, sont téléchargées sur le contrôleur de bus de terrain pour établir la communication. La partie des données de configuration et de paramétrage relative à l'appareil de terrain est téléchargée sur l'appareil de terrain spécifique avant l'échange de données cycliques de processus.

Les appareils de sécurité plus complexes peuvent exiger d'utiliser un outil dédié pour la configuration ou le paramétrage de l'application de l'appareil de sécurité spécifique à la technologie.

NOTE 1 Des informations pertinentes peuvent être consultées dans l'IEC 62061:2005, 6.11.2.3 et l'ISO 13849-1:2015, 4.6.4.

NOTE 2 Les aspects relatifs à la configuration et au paramétrage incorrects comprennent, sans toutefois s'y limiter:

– les erreurs humaines donnant lieu à l'entrée de valeurs d'initialisation et de paramètres incorrectes;
– la corruption des données lors du stockage;
– l'adressage incorrect lors du téléchargement;
– la corruption des données lors du téléchargement;
– la mise à jour irrégulière des appareils de sécurité;
– la connexion des "îlots de sécurité" identiques (machines en série);
– les erreurs systématiques au cours des opérations réalisées avec des outils techniques en raison des paramètres informatiques spécifiques (par exemple, les différences entre les valeurs affichées et enregistrées);
– les changements non reconnus dans les paramètres de sécurité spécifiques à la technologie de l'appareil de sécurité, qu'ils soient stochastiques ou délibérés;
– l'utilisation d'appareils de sécurité précédemment installés dans d'autres fonctions de sécurité.

Un FSCP doit spécifier les méthodes de protection contre les erreurs stochastiques dans la configuration et les paramètres de sécurité.

EXEMPLES

– Adressage incorrect.
– Corruption des données.
– Changements non reconnus.

Les exigences ci-dessus doivent être prises en compte par le concepteur du FSCP pour toutes les phases de communication applicables (voir 5.6).

Plusieurs méthodes disponibles permettent d'éviter une mauvaise configuration et un mauvais paramétrage:

EXEMPLES

– Signatures CRC dans les données de configuration et de paramétrage.
– Corrélation entre les paramètres technologiques de sécurité et les paramètres FSCP.

Les erreurs stochastiques de configuration et de paramétrage au cours du fonctionnement peuvent être évitées par des mesures de sécurité générique.

Les erreurs systématiques de configuration et de paramétrage ne peuvent être évitées en toute sécurité que par la vérification et la validation. Les manuels de sécurité doivent donner les instructions nécessaires.

NOTE 3 Des informations pertinentes peuvent être consultées dans l'IEC 62061:2005, 6.11.2.3 et l'ISO 13849-1:2015, 4.6.4.

F.12.2 Fréquence de modification de la configuration et du paramétrage

Sauf spécification contraire, la fréquence de modification de la configuration et du paramétrage pour les calculs doit être supposée de 1 par jour.

F.12.3 Taux d'erreurs résiduelles pour la configuration et le paramétrage

Le taux d'erreurs résiduelles RR_{CP} pour les erreurs stochastiques de configuration et de paramétrage au cours des opérations ponctuelles comme le téléchargement peut être calculé à l'aide de la probabilité d'erreurs résiduelles de la signature CRC choisie (voir B.4.2) multipliée par la fréquence de modification spécifiée en F.12.2.

Annexe G
(informative)

Mécanismes de sécurité reposant sur des données implicites pour les profils de communication de sécurité fonctionnelle (FSCP) définis dans l'IEC 61784-3

G.1 Vue d'ensemble

L'Annexe G traite des concepts de mécanismes de sécurité reposant sur des données implicites destinés à être utilisés dans les protocoles de communication de sécurité fonctionnelle (FSCP) spécifiés dans la présente norme. Les données implicites sont les données qui ne sont pas explicitement transmises dans un PDU. Au lieu de cela, les valeurs des données implicites sont connues à la fois de l'émetteur (source) et du récepteur (collecteur). Les valeurs des données implicites sont validées par la valeur d'une ou plusieurs séquences de contrôle de trame (FCS, *Frame Check Sequence*) calculées à l'aide d'une chaîne de données globale constituée de la chaîne de données implicites à laquelle est accolée la chaîne de données explicites. Les données implicites n'étant pas transmises, la charge sur le support de transmission s'en trouve réduite.

Aujourd'hui, les FSCP qui utilisent des mécanismes reposant sur des données implicites s'en servent pour communiquer des codes d'opportunité (codes T) complets ou partiels et/ou des codes d'authenticité (codes A), voir l'Annexe E. Ces FSCP utilisent également des algorithmes de contrôle de redondance cyclique (CRC) exclusivement pour la séquence de contrôle de trame (FSC). Par conséquent, l'Annexe G est limitée à l'analyse des codes A et des codes T transmis implicitement à l'aide d'algorithmes de CRC.

Conformément à l'Article E.8, concernant les données implicites, "En raison de la diversité des méthodes possibles, aucune formule générique ne peut être fournie. Il incombe au FSCP individuel de démontrer des probabilités d'erreurs résiduelles suffisantes." Dans la perspective de faire évoluer l'IEC 61784-3 pour la prochaine édition et les suivantes, cette nouvelle Annexe G a pour objet d'approfondir la compréhension des modèles de formulation pour les probabilités d'erreurs des FSCP utilisant des algorithmes de CRC afin d'assurer la transmission implicite de codes T et de codes A lorsqu'un code FCS unique est utilisé par le protocole.

L'Annexe G propose deux exemples de formules applicables pour deux cas spécifiques, qui permettent de mieux comprendre les modèles de formulation afin de développer de nouvelles formules (spécifiques et générales).

Elle propose également une méthode d'addition généralement applicable lorsque les répartitions du poids conditionnel pour les configurations d'erreurs dans les données implicites sont connues et peuvent être quantifiées de manière à obtenir une solution en forme fermée, ou bien de manière adaptée à une addition itérative avec un temps d'exécution aux limites raisonnables.

G.2 Principes de base

Les calculs donnés dans l'Annexe G utilisent également le modèle de canal symétrique binaire (BSC, *binary symmetric channel*) spécifié dans l'Annexe B.

NOTE 1 Bien qu'il ne tienne pas compte des erreurs en rafale, le modèle BSC avec une probabilité d'erreurs sur les éléments binaires estimée suffisante est le moyen le plus pratique actuellement connu pour réaliser les calculs de probabilités nécessaires à déterminer le taux d'erreurs résiduelles du FSCP.

La Figure G.1 représente le principe de base d'un FSCP utilisant des mécanismes de protection FCS simples impliquant des données implicites. Côté émetteur, une somme de

contrôle CRC sur les données implicites $impl_S$ concaténées avec les données explicites $expl_S$ est générée, formant ainsi une séquence de contrôle de trame FCS_S. Lorsque plusieurs codes FCS sont utilisés dans un format FSCP, le calcul doit être réalisé pour chaque code FCS. Lorsque $expl_S$ et FCS_S sont transmis explicitement par le canal noir, $impl_S$ n'est pas transmise, mais influe sur la valeur de FCS_S. Par conséquent, elle ne peut contenir que des données dont la valeur est déjà connue du récepteur. Des données implicites sont utilisées pour détecter, par exemple, des SPDU mal acheminés dans l'espace ("erreur d'authentification") ou le temps ("erreur d'opportunité"). Cette opération est accomplie par dérivation des données implicites à partir du code A (par exemple, un identifiant de connexion) et/ou le code T (par exemple, un numéro de séquence) d'un SPDU.

NOTE 2 Les détails d'initialisation font l'objet du F.12.1.

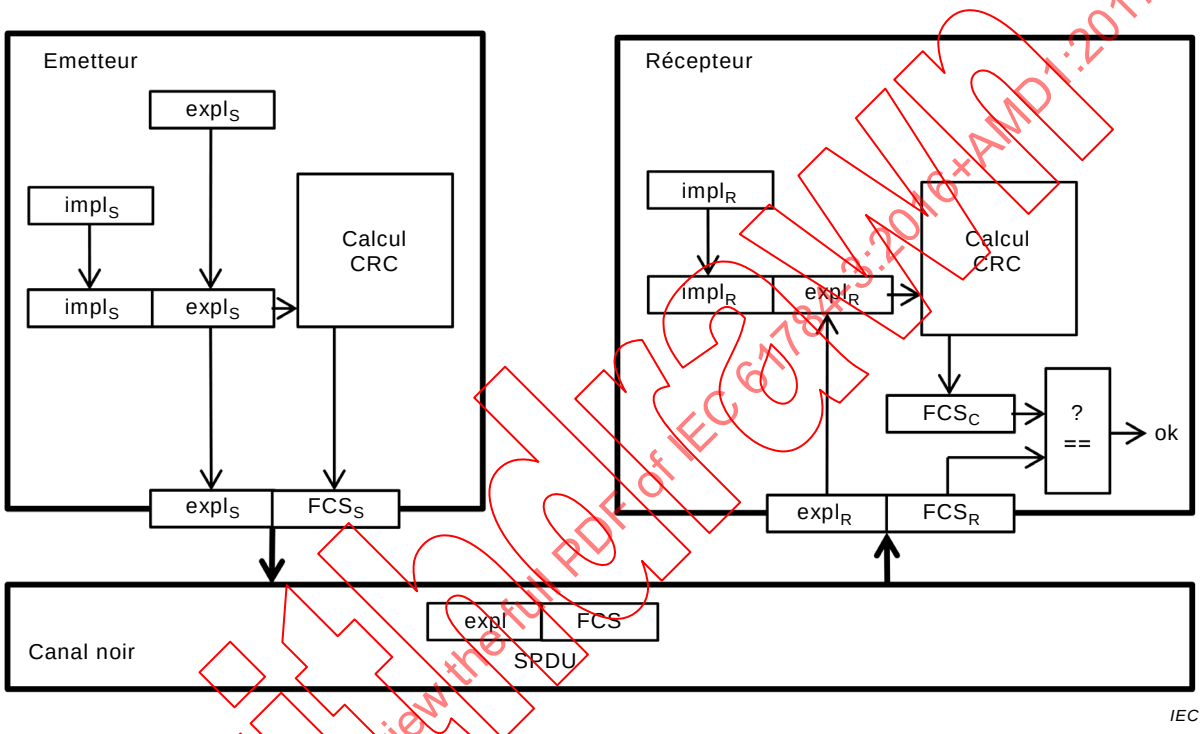


Figure G.1 – FSCP à transmission implicite de codes d'authenticité et/ou d'opportunité

Lorsque le SPDU comprenant expl et FCS est transmis à la couche FSCP dans le récepteur, elle peut contenir des erreurs de transmission, c'est-à-dire que la valeur d'arrivée peut différer de la valeur envoyée. A des fins de distinction, les symboles $expl_R$ et FCS_R sont utilisés dans le récepteur.

La valeur attendue des données implicites est appelée $impl_R$. En cas d'absence d'erreur, cette valeur est identique à $impl_S$. En cas, par exemple, d'erreur d'acheminement d'un SPDU, $impl_R$ et $impl_S$ peuvent différer.

Le récepteur génère une ou plusieurs séquences de contrôle de trame FCS_C en créant une somme de contrôle CRC pour la concaténation de $impl_R$ et $expl_R$. Lorsque chaque FCS_C est identique à la valeur FCS_R correspondante, l'hypothèse selon laquelle aucune erreur ne s'est produite est retenue. Autrement, une erreur a été détectée.

Les longueurs des chaînes de bits pour un FCS unique sont définies comme suit:

r longueur de la FCS (degré de polynôme générateur);

i longueur des données implicites (l'hypothèse retenue est: i ≥ r);

e longueur des données explicites;

n longueur du SPDU, avec n = e + r.

G.3 Enoncé du problème: valeurs constantes pour les données implicites

Dans les FSCP utilisant des données implicites, le contrôle CRC côté récepteur est utilisé pour la détection d'erreurs concernant l'intégrité des données, l'acheminement ou encore l'opportunité des SPDU. Par conséquent, il peut arriver que le mécanisme de CRC soit "surchargé" par de multiples erreurs simultanées, ce qui conduit à une augmentation de la probabilité globale d'erreurs résiduelles. Un exemple de ce cas est représenté dans le scénario suivant, à la Figure G.2.

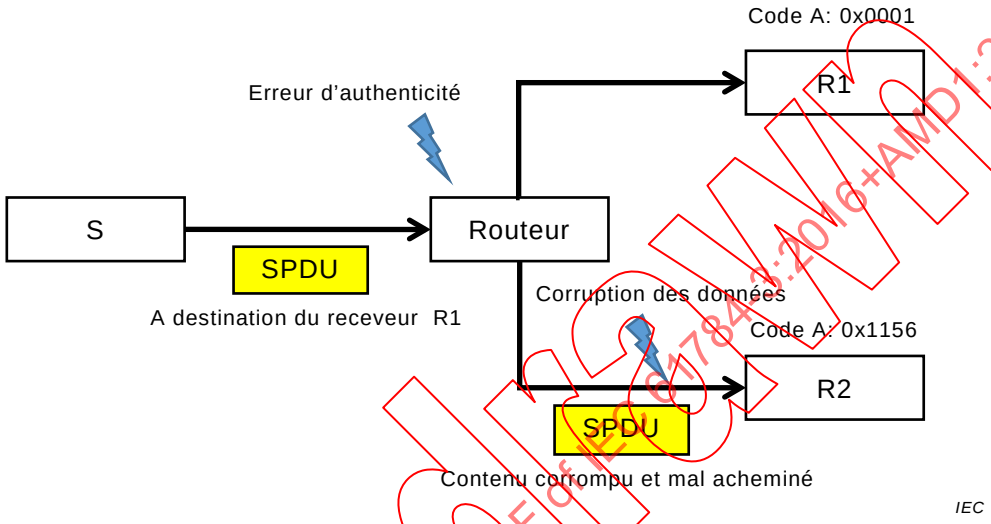


Figure G.2 – Exemple de transmission incorrecte due à des causes d'erreur multiples

Le scénario prend l'hypothèse d'un émetteur S envoyant des SPDU à un récepteur R1 et à un récepteur R2 via un canal noir contenant un routeur. Les données implicites utilisées comportent un champ unique contenant un code d'authenticité (code A) de 16 bits, identifiant le récepteur (voir Figure E.4). Pour chaque SPDU transmis de S à R1, le code A de R1 est utilisé comme donnée implicite, de la même manière que le code A de R2 pour les SPDU transmis de S à R2. De plus, il est pris pour hypothèse que les erreurs suivantes peuvent se produire lors de la transmission d'un SPDU.

a) Erreur d'authenticité: En raison d'une anomalie dans le routeur, le SPDU est transmis au mauvais récepteur (soit le récepteur R2 au lieu du récepteur R1, ou inversement). Ainsi, le code d'authenticité implicite $impl_S$ utilisé pour calculer le FCS_S côté émetteur n'est pas égal au code d'authenticité attendu $impl_R$ côté récepteur.

b) Corruption des données: En raison, par exemple, d'interférences ou de bruits sur le support de transmission, le contenu du SPDU est corrompu (expl et/ou FCS).

De plus, il est pris pour hypothèse que le canal noir lui-même ne détecte aucune de ces erreurs. Par conséquent, les erreurs, et potentiellement une combinaison d'erreurs, doivent être détectées par la vérification réalisée dans la couche de sécurité du récepteur. La configuration d'erreur err_{impl} provoquée par l'erreur d'authenticité est définie par la disjonction exclusive (XOR) bit à bit des codes A utilisés. Dans le cas représenté, à deux récepteurs seulement, cette configuration d'erreur est constante. La configuration d'erreur err_{expl} est définie comme la disjonction exclusive (XOR) bit à bit de $expl_S$ et $expl_R$. Elle est modélisée par un BSC (voir l'Annexe B).

La Figure G.3 représente les probabilités d'erreurs résiduelles pour différents paramètres lors de l'utilisation du polynôme générateur exact $x^{16}+x^{14}+x^{11}+x^{10}+x^9+x^7+x^5+x^3+x+1$ (0x14EAB) de degré 16.

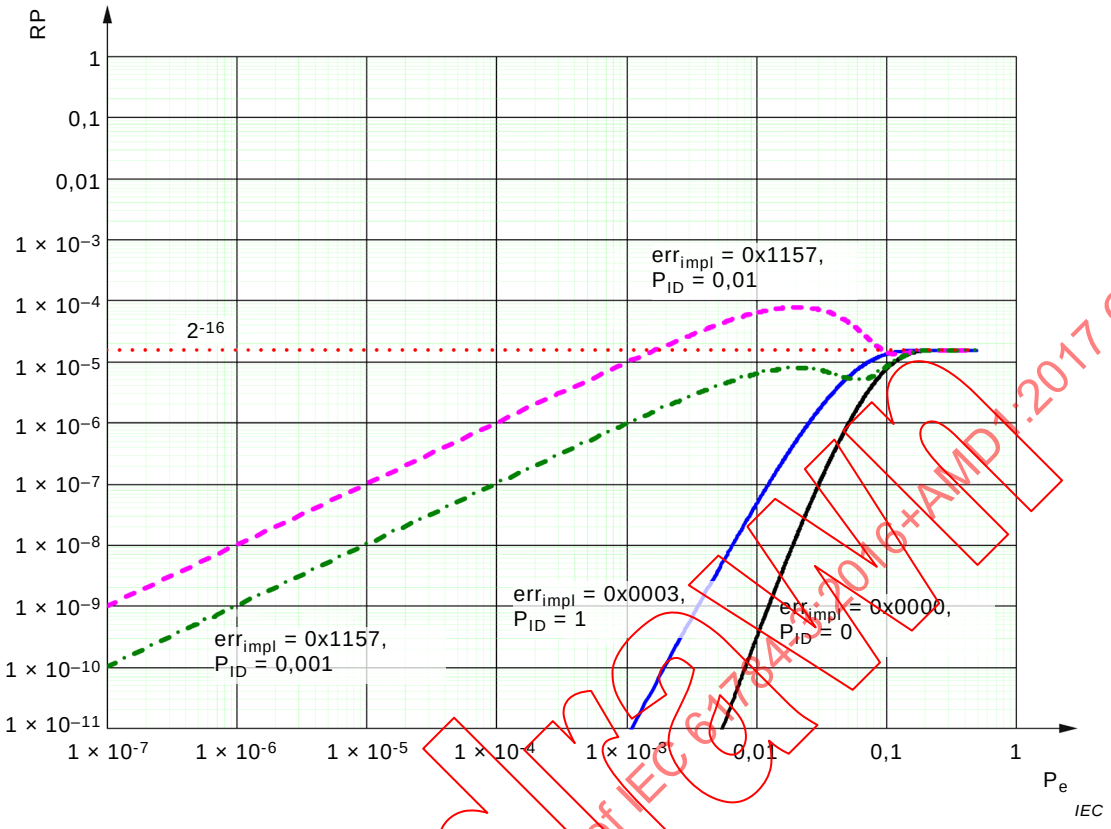


Figure G.3 – Influence des erreurs dans les données implicites sur la probabilité d'erreurs résiduelles

La Figure G.3 s'appuie sur des données générées par un algorithme exhaustif de vérification de toutes les configurations d'erreur possible. En plus du polynôme générateur, les données d'entrée suivantes ont été utilisées dans l'algorithme:

P_{ID} probabilité de remise incorrecte (ici: erreur d'adressage);

err_{impl} configuration d'erreur constante provoquée par une erreur d'adressage (disjonction bit à bit des codes A).

Il est important de noter que la probabilité d'erreurs résiduelles ne dépend pas seulement de p et de P_{ID}, mais également de la constance de la variable err_{impl}, et donc des valeurs des codes A choisies pendant la mise en service.

La courbe correspondant à P_{ID} = 0 (noir continu) démontre l'exactitude du polynôme générateur. Dans ce cas où aucune erreur n'est détectée dans les données implicites, la probabilité d'erreurs résiduelles est toujours inférieure à la limite de 2^{-16} et la courbe augmente de façon monotone.

La courbe en tirets violets et la courbe en pointillés verts représentent les caractéristiques associées à une utilisation de codes A résultant en une variable err_{impl} de 0x1157 (par exemple, les codes A 0x0001 et 0x1156). La probabilité d'erreurs résiduelles n'augmente plus de manière monotone mais présente une valeur maximale supérieure à 2^{-16}. Pour $P_{ID}=10^{-3}$, la courbe (pointillés verts) ne dépasse pas la limite de 2^{-16}. Cependant, si P_{ID} est défini sur 10^{-2} (tirets violets), la valeur maximale est supérieure à la limite 2^{-16} (soit un cas défavorable). Par conséquent, la limite 2^{-r} ne peut pas être utilisée comme approximation même si l'exactitude du polynôme générateur a été démontrée pour le cas P_{ID} = 0.

Les courbes verte et violette sont observées seulement pour certaines valeurs rares de err_{impl}. Pour la plupart des autres valeurs de err_{impl}, les courbes se situent en dessous de la limite, même pour une probabilité d'occurrence P_{ID} = 1. Par exemple, la courbe correspondant

à err_{impl} = 0x0003 (par exemple, codes A égaux à 0x0001 et 0x0002) représente ces caractéristiques (bleu continu).

Conclusion: Lorsque des mécanismes de transmission implicites sont utilisés, la probabilité d'erreurs résiduelles n'est pas nécessairement limitée par 2^{-r}. Cette limite est valide seulement si le FSCP fournit des mécanismes supplémentaires tels que ceux indiqués dans les articles suivants.

NOTE La limitation incorrecte d'un FCS n'entraînerait pas nécessairement une erreur résiduelle insuffisante lorsque d'autres mesures de protocole spécifiques au FSCP sont associées dans le schéma de détection d'erreurs.

G.4 RP pour les FSCP avec une variable err_{impl} aléatoire et uniformément répartie

G.4.1 Généralités

L'Article G.4 examine le cas d'une variable err_{impl} aléatoire en accordant une probabilité égale à chaque valeur possible ("répartition uniforme"). Comme indiqué dans l'Article G.3, où err_{impl} est constante, cette hypothèse n'est pas toujours justifiée et doit être garantie de manière démontrable par la conception du FSCP correspondant.

Comme défini ci-dessus, err_{impl} est la disjonction exclusive (XOR) bit à bit entre les données implicites $impl_S$ utilisées côté émetteur du paquet erroné et la valeur attendue pour les données implicites $impl_R$ côté récepteur. Clairement, si $impl_S$ et $impl_R$ sont uniformément distribuées, des variables aléatoires indépendantes, soit err_{impl}, sont uniformément réparties, c'est-à-dire qu'elles adoptent chaque valeur possible selon une possibilité égale. Cependant, dans la mesure où l'hypothèse selon laquelle les erreurs se produisent à des points "aléatoires" dans le temps peut être retenue, il est également possible d'assurer la répartition uniforme de err_{impl} si $impl_S$ et $impl_R$ sont des variables non aléatoires. Afin de confirmer si err_{impl} adopte une répartition uniforme, des vérifications statistiques telles que le test du khi carré ou le test de Kolmogoroff-Smirnoff peuvent être utilisées (voir par exemple [35]).

NOTE 1 La variable err_{impl} étant répartie de manière uniforme, elle ne requiert pas que toutes ses valeurs possibles soient observées à fréquence égale pendant un intervalle de temps fini. Par conséquent, il n'est pas toujours possible d'évaluer un générateur de nombres aléatoires par simple décompte du nombre d'occurrences dans un intervalle de temps limité.

En fonction de la conception du FSCP, il existe deux variantes raisonnables de l'hypothèse "err_{impl} est uniformément répartie":

a) err_{impl} adopte chaque valeur hors de l'intervalle $[0;2^i-1]$ selon une probabilité de 2^{-i};

b) err_{impl} adopte chaque valeur hors de l'intervalle $[1;2^i-1]$ selon une probabilité de $1/(2^i-1)$.

NOTE 2 Il existe une légère différence entre les deux variantes: dans la seconde variante, la valeur err_{impl} = 0 indique que le SPDU a été transmis correctement, car une erreur de remise de SPDU se traduit systématiquement par une valeur $err_{impl} \neq 0$. Dans la première variante, la valeur err_{impl} = 0 n'implique pas nécessairement une remise correcte.

Dans le second cas, des mesures doivent être mises en œuvre pour garantir qu'une valeur unique pour les données implicites soit attribuée à chaque SPDU. Par conséquent, la configuration d'erreur en cas de SPDU mal acheminé ne peut jamais être égale à zéro. Dans le premier cas, aucune mesure de ce type n'est mise en œuvre, la configuration d'erreur "zéro" peut donc se produire. Clairement, une telle erreur ne peut pas être détectée côté récepteur à moins qu'il n'existe des erreurs d'intégrité de données détectables supplémentaires ou d'autres vérifications spécifiques aux FSCP.

Les deux variantes sont représentées séparément ci-après.

Les autres modèles, potentiellement plus détaillés, se situent hors du domaine d'application du présent document. Par exemple, il est possible d'éliminer des configurations d'erreur dans les données avec une certitude de détection démontrée à l'aide du polynôme de CRC.

EXEMPLE Les distances de Hamming inférieures aux distances de Hamming minimales pour le polynôme de CRC sur la longueur du bloc de données, les erreurs en rafale de longueur r, un nombre impair d'erreurs dans les bits, etc., sont des exemples de ces configurations d'erreur dans les données.

Le Paragraphe G.4.2 donne un exemple dans lequel le champ des données implicites est au moins aussi long que le FCS et les valeurs des données implicites sont générées aléatoirement de telle sorte que l'unicité des codes A n'est pas garantie pour chaque point d'extrémité, que l'unicité des codes T n'est pas garantie pour chaque temps de SPDU, et que l'unicité des combinaisons de codes A et de codes T n'est pas garantie.

Le Paragraphe G.4.3 donne un exemple dans lequel le champ des données implicites est exactement aussi long que la FCS et l'unicité des codes A et des codes T est garantie pour chaque point d'extrémité et chaque temps de SPDU. En application réelle, des termes supplémentaires peuvent être nécessaires pour tenir compte des exceptions, par exemple un bouclage de code T.

L'Article G.5 donne une méthode d'addition généralement applicable lorsque les répartitions du poids conditionnel pour les configurations d'erreurs dans les données implicites sont connues et peuvent être quantifiées.

G.4.2 Répartition uniforme dans l'intervalle [0;2^i-1], i ≥ r

Ce cas s'applique en particulier aux FSCP qui utilisent des générateurs de nombres aléatoires pour dériver des valeurs de données implicites.

A un niveau de granularité grossière, deux types principaux d'erreurs peuvent être distingués:

- contenu incorrect d'un SPDU, c'est-à-dire erreurs d'intégrité des données;
- remise incorrecte d'un SPDU, c'est-à-dire que le SPDU est transmis au mauvais récepteur ou à la mauvaise instance temporelle.

En combinant ces deux types, les cas distincts suivants peuvent être distingués:

- Cas 1. CC: Aucune erreur (remise correcte, et données explicites correctes);
- Cas 2. IC: Remise incorrecte, et données explicites correctes;
- Cas 3. CI: Remise correcte, et données explicites incorrectes;
- Cas 4. II: Remise incorrecte, et données explicites incorrectes.

Les probabilités d'erreurs résiduelles RP_2, RP_3, et RP_4, pour chacun des cas 2, 3 et 4, sont calculées à partir des paramètres suivants:

P_{ID} est la "probabilité de remise incorrecte", c'est-à-dire la probabilité qu'un SPDU soit transmis de manière erronée au FSCP en raison, par exemple, d'une erreur d'authenticité ou d'opportunité;

NOTE 1 L'évènement de "remise incorrecte" peut se traduire par $err_{impl} \neq 0$. Cependant, en raison de la répartition uniforme dans l'intervalle [0;2^r-1], le cas où $err_{impl} = 0$ peut également se produire.

P_{IED} est la probabilité de données explicites incorrectes, c'est-à-dire la probabilité qu'une corruption des données se produise;

P_{IC} est la probabilité qu'une erreur ne soit pas détectée au niveau du récepteur à condition que le cas 2 se produise;

P_{CI} est la probabilité qu'une erreur ne soit pas détectée au niveau du récepteur à condition que le cas 3 se produise;

P_{II} est la probabilité qu'une erreur ne soit pas détectée au niveau du récepteur à condition que le cas 4 se produise;

RP_I est la probabilité d'erreur résiduelle pour la corruption des données telle que définie à l'Annexe F.

R_{CRC} est la probabilité d'erreur résiduelle pour les polynômes CRC tels que définis dans l'Equation B.3.

NOTE 2 $RP_I \leq R_{CRC}$ car d'autres mesures de sécurité que le CRC peuvent réduire davantage la valeur de RP_I.

r est la longueur de la FCS, identique au degré du polynôme de CRC;

i est la longueur des données implicites, avec $i \geq r$;

n est le nombre de bits du SPDU.

Les évènements IC, CI et II étant distincts, la probabilité globale d'erreurs résiduelles peut être calculée en faisant la somme de leurs valeurs RP_x respectives.

En général, RP_x est calculée comme suit:

RP_x = P("l'erreur x a lieu") × P("l'erreur x n'est pas détectable").

Ce calcul donne les formules pour les cas 2, 3 et 4 décrits dans les alinéas suivants.

Cas 2 (IC)

$RP_2 = P_{ID} \times (1 - P_{IED}) \times P_{IC}$
$= P_{ID} \times (1 - P_{IED}) \times 2^{-r}$

Explication de P_{IC}:

- Si i > r, la probabilité de ce cas est de 2^{-r}, car
  - par hypothèse, la disjonction bit à bit de $impl_S$ et $impl_R$ est uniformément répartie dans l'intervalle $[0;2^i-1]$;
  - par conséquent, la disjonction bit à bit de $FCS_S = FCS_R$ et FCS_C est uniformément répartie dans l'intervalle $[0;2^r-1]$;
  - par conséquent, la probabilité que la disjonction bit à bit de FCS_R et FCS_C soit égale à zéro est de 2^{-r};
  - par conséquent, la probabilité que FCS_R soit égal à FCS_C est de 2^{-r}.
- Si i = r, la probabilité de ce cas est de 2^{-r}, car
  - FCS_R est égal à FCS_C, si et seulement si $err_{impl} = 0$, car la longueur de err_{impl} ne dépasse pas le degré du polynôme de CRC. Les codes CRC détectent toutes les erreurs en rafale de longueur inférieure ou égale à r;
  - La probabilité que $err_{impl} = 0$ est de 2^{-r} en raison de la répartition uniforme dans l'intervalle $[0;2^r-1]$.

Cas 3 (CI)

$RP_3 = (1-P_{ID}) \times P_{IED} \times P_{CI}$
$= (1-P_{ID}) \times RP_I$
$\leq (1-P_{ID}) \times 2^{-r}$ pour les polynômes exacts.

Cas 4 (II)

$RP_4 = P_{ID} \times P_{IED} \times P_{II}$
$= P_{ID} \times P_{IED} \times 2^{-r}$

Explication:

- Par hypothèse, err_{impl} adopte toutes les valeurs de l'intervalle $[0;2^i-1]$ selon une égale probabilité.

- Par conséquent, chaque bit de err_{impl} adopte la valeur 0 ou 1 selon une égale probabilité de 0,5.
- Puisque les codes CRC sont des codes linéaires, et que $|err_{impl}| \geq r$, chaque bit de err_{impl} détermine le résultat d'un bit dans la disjonction exclusive bit à bit de FCS_R et FCS_C.
- Par conséquent, les bits de la disjonction exclusive bit à bit de FCS_R et FCS_C peuvent être traités comme des variables aléatoires indépendantes, chacune adoptant les valeurs 0 et 1 selon une égale probabilité de 0,5.
- La disjonction exclusive bit à bit de FCS_R et FCS_C est une variable aléatoire uniformément répartie, adoptant toutes les valeurs de l'intervalle $[0;2^r-1]$ selon une probabilité égale.
- La probabilité que la disjonction bit à bit de FCS_R et FCS_C soit égale à zéro est de 2^{-r}.
- La probabilité que FCS_C soit identique à FCS_R est de 2^{-r}.

En résumé, la probabilité d'erreurs résiduelles d'un FSCP utilisant des mécanismes implicites pour la détection d'erreurs d'opportunité et d'authenticité (garantissant que l'erreur dans les données implicites est uniformément répartie dans l'intervalle $[0;2^i-1]$ peut être calculée à l'aide de la formule suivante:

$$\begin{aligned} RP_{TOTAL} &= RP2 + RP3 + RP4 \\ &= (P_{ID} \times (1 - P_{IED}) \times 2^{-r}) + ((1-P_{ID}) \times P_{IED} \times P_{CI}) + (P_{ID} \times P_{IED} \times 2^{-r}) \\ &= (P_{ID} \times 2^{-r}) + ((1-P_{ID}) \times P_{IED} \times P_{CI}) \\ &= (P_{ID} \times 2^{-r}) + ((1-P_{ID}) \times RP_I) \end{aligned}$$

Explication:

- Les cas 2 à 4 sont des évènements distincts.

En cas de polynôme exact, ce qui suit s'applique:

$$\begin{aligned} RP_{TOTAL} &= RP2 + RP3 + RP4 \\ &= (P_{ID} \times (1 - P_{IED}) \times 2^{-r}) + ((1-P_{ID}) \times P_{IED} \times P_{CI}) + (P_{ID} \times P_{IED} \times 2^{-r}) \\ &\leq (P_{ID} \times (1 - P_{IED}) \times 2^{-r}) + ((1-P_{ID}) \times 2^{-r}) + (P_{ID} \times P_{IED} \times 2^{-r}) \\ &\leq 2^{-r} \end{aligned}$$

Explication:

- Les cas 2 à 4 sont des évènements distincts.
- Cette limite supérieure de RP_{TOTAL} est indépendante des valeurs de P_{IED} et P_{ID}.

G.4.3 Répartition uniforme dans l'intervalle $[1;2^r-1]$, i = r

Pour cette variante, il est pris pour hypothèse que i = r, c'est-à-dire que la longueur des données implicites correspond exactement au degré du polynôme de CRC, et que err_{impl} est uniformément répartie dans l'intervalle $[1;2^r-1]$. Contrairement à la variante donnée en G.4.2, err_{impl} est toujours différent de 0 en cas de remise incorrecte.

Les cas de combinaisons d'erreurs suivants peuvent être distingués:

- Cas 1. CC: Aucune erreur (remise correcte, et données explicites correctes);
- Cas 2. IC: Remise incorrecte, et données explicites correctes;
- Cas 3. CI: Remise correcte, et données explicites incorrectes;
- Cas 4. II: Remise incorrecte, et données explicites incorrectes.

Les probabilités d'erreurs résiduelles RP_2, RP_3, et RP_4 pour chacun des cas 2, 3 et 4 sont calculées à partir des paramètres suivants:

P_{ID} est la "probabilité de remise incorrecte", c'est-à-dire la probabilité qu'un SPDU soit transmis de manière erronée au FSCP en raison, par exemple, d'une erreur d'authenticité ou d'opportunité;

NOTE En raison de la répartition uniforme dans $[1;2^r-1]$, $err_{impl} \neq 0$ est garantie. Par conséquent, l'évènement de "remise incorrecte" est, dans ce cas, équivalent à l'évènement de "données implicites incorrectes".

P_{IED} est la probabilité de données explicites incorrectes, c'est-à-dire la probabilité qu'une corruption des données se produise;

P_{IC} est la probabilité qu'une erreur ne soit pas détectée au niveau du récepteur à condition que le cas 2 se produise;

P_{CI} est la probabilité qu'une erreur ne soit pas détectée au niveau du récepteur à condition que le cas 3 se produise;

P_{II} est la probabilité qu'une erreur ne soit pas détectée au niveau du récepteur à condition que le cas 4 se produise;

$P_{EIC}(i)$ est la probabilité que les configurations d'erreurs dans les données explicites err_{expl} complètent les configurations d'erreurs dans les données implicites err_{impl} rendant l'erreur indétectable, à condition que "$err_{impl} = i$";

r est la longueur des données implicites et la longueur de la FCS (degré du polynôme de CRC);

n est le nombre de bits du SPDU.

Les évènements IC, CI et II étant distincts, la probabilité globale d'erreurs résiduelles peut être calculée en faisant la somme de leurs valeurs RP_x respectives.

En général, RP_x est calculée comme suit:

RP_x = P("l'erreur x a lieu") × P("l'erreur x n'est pas détectable").

Ce calcul donne les formules pour les cas 2, 3 et 4 décrits dans les alinéas suivants.

Cas 2 (IC)

$RP_2 = P_{ID} \times (1 - P_{IED}) \times P_{IC}$
$= 0$

Explication:

- Les erreurs de type 2 sont toujours détectées, car la longueur de err_{impl} ne dépasse pas r. Les codes CRC détectent toutes les erreurs en rafale de longueur inférieure ou égale à r. Par conséquent, P_{IC} est égal à 0 dans ce cas.

Cas 3 (CI)

$RP_3 = (1-P_{ID}) \times P_{IED} \times P_{CI}$
$= (1-P_{ID}) \times RP_I$
$\leq (1-P_{ID}) \times 2^{-r}$ pour les polynômes exacts.

Cas 4 (II)

$RP_4 = P_{ID} \times P_{IED} \times P_{II}$
$\approx P_{ID} \times P_{IED} \times 2^{-r}$

Explication:

- $P_{II} = \sum_{i=1}^{2^r-1} P\{err_{impl} = i\} \times P_{EIC}(i)$

$= \sum_{i=1}^{2^r-1} \frac{1}{2^r-1} \times P_{EIC}(i)$

$= \frac{1}{2^r-1} \times \sum_{i=1}^{2^r-1} P_{EIC}(i)$

$= \frac{1}{2^r-1}$ (car pour toutes les valeurs possibles de err_{expl} il y a exactement une valeur err_{impl} correspondante)

$\approx 2^{-r}$

En résumé, la probabilité d'erreurs résiduelles d'un FSCP utilisant des mécanismes implicites pour la détection d'erreurs d'opportunité et d'authenticité garantissant que l'erreur dans les données implicites est uniformément répartie dans l'intervalle [1;2^r-1] peut être calculée à l'aide de la formule suivante:

RP_{TOTAL} = RP2 + RP3 + RP4

$= (P_{ID} \times (1 - P_{IED}) \times 2^{-r}) + ((1-P_{ID}) \times P_{IED} \times P_{CI}) + (P_{ID} \times P_{IED} \times 2^{-r})$

$= (P_{ID} \times 2^{-r}) + ((1-P_{ID}) \times P_{IED} \times P_{CI})$

$= (P_{ID} \times 2^{-r}) + ((1-P_{ID}) \times RP_I)$

Explication:

- Les cas 2 à 4 sont des évènements distincts.

G.5 Cas général

Les calculs présentés en G.4.2 et G.4.3 sont valides seulement dans l'hypothèse d'une répartition uniforme de err_{impl} et sous certaines restrictions concernant la longueur du champ de données implicites. Dans le cas général, RP_{TOTAL} peut être calculé comme suit, si la répartition du poids conditionnel du code est connue pour chaque valeur possible de err_{impl}.

$$RP_{TOTAL} = P_{ID} \times \sum_{j=0}^{2^r-1} P\{ err_{impl} = j\} \times P\{ FCS_C = FCS_R \mid err_{impl} = j\} + (1 - P_{ID}) \times P_{re}^{CRC, BSC}$$

où

$P\{ err_{impl} = j\}$ est la probabilité que la configuration d'erreur dans les données implicites ait la valeur j (à condition qu'il existe un SPDU mal acheminé);

$P\{ FCS_C = FCS_R \mid err_{impl} = j\}$ est la probabilité qu'aucune erreur ne soit indiquée pour le polynôme de CRC donné et la longueur de code donnée, à condition que la configuration d'erreur dans les données implicites ait la valeur j;

$P_{re}^{CRC, BSC}$ est la probabilité d'erreurs résiduelles pour le polynôme de CRC et la longueur de code sans données implicites.

$P_{re}^{CRC,\,BSC}$ et $P\{FCS_C = FCS_R \mid err_{impl} = j\}$ sont donnés par:

$$P_{re}^{CRC,BSC} = \sum_{k=1}^{n} A_k(err_{impl} = 0) \times P_e^k \times (1 - P_e)^{n-k}$$

$$P\{FCS_C = FCS_R \mid err_{impl} = j\} = \sum_{k=0}^{n} A_k(err_{impl} = j) \times P_e^k \times (1 - P_e)^{n-k}$$

où

$A_k(err_{impl} = j)$ est la répartition du poids du code à la condition que la configuration d'erreur dans les données implicites adopte la valeur j.

Explication:

- $P\{FCS_C = FCS_R \mid err_{impl} = 0\} = P_{re}^{CRC,\,BSC} + (1\text{-}P_e)^n$.

G.6 Calcul de P_{ID}

Si le code T et le code A sont tous deux implicites, P_{ID} peut être calculé comme suit:

$$P_{ID} = \min\left(\frac{R_T + R_A}{v}, 1\right)$$

où

P_{ID} est la probabilité qu'un SPDU soit transmis de manière erronée au FSCP en raison, par exemple, d'une erreur d'authenticité ou d'opportunité;

R_T est le taux d'occurrence des PDU de sécurité à séquence incorrecte (voir F.5.2.4);

R_A est le taux d'occurrence des PDU de sécurité mal acheminés (voir F.5.2.3);

v est le nombre maximal d'échantillons de SPDU produit par la SCL ("fréquence d'échantillonnage") par heure (voir F.5.2.2).

Explication:

- En raison de l'approximation, $R_T + R_A$ peut devenir supérieur à un. Dans ce cas, la valeur 1 doit être utilisée pour P_{ID}.

Si seul le code T est implicite, P_{ID} peut être calculé comme suit:

$$P_{ID} = \frac{R_T}{v}$$

Si seul le code A est implicite, P_{ID} peut être calculé comme suit:

$$P_{ID} = \frac{R_A}{v}$$

Calcul du taux total d'erreurs résiduelles

Conformément à F.10.1, le taux total d'erreurs résiduelles est calculé comme suit (voir l'Equation (F.6)):

$$\lambda_{SC} = RR_T + RR_A + RR_I + RR_M$$

Sinon, la formule suivante peut être utilisée:

$$\lambda_{SC} = \nu \times RP_{TOTAL}$$

Bibliographie

[1] IEC 60050 (toutes les parties), *Vocabulaire Electrotechnique International* (disponible à l'adresse <http://www.electropedia.org/)

NOTE Voir également le dictionnaire multilingue de l'IEC – Electricité, électronique et télécommunications (disponible sur CD-ROM et à l'adresse <http://www.electropedia.org>).

[2] IEC 60050-191:1990, *Vocabulaire Electrotechnique International – Chapitre 191: Sûreté de fonctionnement et qualité de service*

[3] IEC 60204-1, *Sécurité des machines – Equipement électrique des machines – Partie 1: Règles générales*

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

[5] IEC 61131-2:2007, *Automates programmables – Partie 2: Exigences et essais des équipements*

[6] IEC 61131-6, *Automates programmables – Partie 6: Sécurité fonctionnelle*

[7] IEC 61496 (toutes les parties), *Sécurité des machines – Equipements de protection électrosensibles*

[8] IEC 61496-1, *Sécurité des machines – Equipements de protection électro-sensibles – Partie 1: Exigences générales et essais*

[9] IEC 61508-4:2010, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 4: Définitions et abréviations*

[10] IEC 61508-5:2010, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 5: Exemples de méthodes pour la détermination des niveaux d'intégrité de sécurité*

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

[12] IEC 61784-4[18], *Industrial communication networks – Profiles – Part 4: Secure communications for fieldbuses* (disponible en anglais seulement)

[13] IEC 61800-5-2, *Entraînements électriques de puissance à vitesse variable – Partie 5-2: Exigences de sécurité – Fonctionnelle*

[14] IEC TR 62059-11:2002, *Equipements de comptage de l'électricité – Sûreté de fonctionnement – Partie 11: Concepts généraux*

[15] IEC 62061:2005, *Sécurité des machines – Sécurité fonctionnelle des systèmes de commande électriques, électroniques et électroniques programmables relatifs à la sécurité*

[18] Proposition d'un nouveau sujet de travail à l'étude.

[16] IEC TR 62210:2003, *Power system control and associated communications – Data and communication security* (disponible en anglais seulement)

[17] IEC 62280:2014, *Applications ferroviaires – Systèmes de signalisation, de télécommunication et de traitement – Communication de sécurité dans les systèmes de transmission*

[18] IEC TR 62685, *Réseaux de communication industriels – Profils – Lignes directrices pour l'évaluation des appareils de sécurité utilisant les profils de communication pour la sécurité fonctionnelle (FSCP) de l'IEC 61784-3*

[19] ISO/IEC Guide 51:2014, *Aspects liés à la sécurité – Principes directeurs pour les inclure dans les normes*

[20] ISO/IEC 2382-16:1996, *Technologies de l'information – Vocabulaire – Partie 16: Théorie de l'information*

[21] ISO/IEC 7498-1, *Technologies de l'information – Interconnexion de systèmes ouverts (OSI) – Modèle de référence de base: Le modèle de base*

[22] ISO 10218-1, *Robots et dispositifs robotiques – Exigences de sécurité pour les robots industriels – Partie 1: Robots*

[23] ISO 12100, *Sécurité des machines – Principes généraux de conception – Appréciation du risque et réduction du risque*

[24] ISO 13849 (toutes les parties), *Sécurité des machines – Parties des systèmes de commande relatives à la sécurité*

[25] ISO 13849-1:2015, *Sécurité des machines – Parties des systèmes de commande relatives à la sécurité – Partie 1: Principes généraux de conception*

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

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

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

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

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

[31] J. WOLF, A. MICHELSON, A. LEVESQUE, *On the probability of undetected error for linear block codes*, February 1982, IEEE Transactions on Communications, Volume 30, Issue 2

[32] S. LEUNG-YAN-CHEONG AND M. HELLMAN, *Concerning a bound on undetected error probability*, March 1976, IEEE Transactions on Information Theory, Volume 22, Issue 2

[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, Issue 6

[35] D. KNUTH, *The Art of Computer Programming, Volume 2: Seminumerical Algorithms*, 3rd Edition, Addison-Wesley, 1997

IEC 61784-3

Edition 3.1 2017-08
CONSOLIDATED VERSION

FINAL VERSION

VERSION FINALE

colour inside

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

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

IEC 61784-3:2016-05+AMD1:2017-08 CSV(en-fr)

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES –

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

FOREWORD

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

This consolidated version of the official IEC Standard and its amendment has been prepared for user convenience.

IEC 61784-3 edition 3.1 contains the third edition (2016-05) [documents 65C/840/FDIS and 65C/848/RVD] and its amendment 1 (2017-08) [documents 65C/879/FDIS and 65C/886/RVD].

This Final version does not show where the technical content is modified by amendment 1. A separate Redline version with all changes highlighted is available in this publication.

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

This third edition constitutes a technical revision.

This edition includes the following significant technical changes with respect to the previous edition:

- clarifications and additional explanations for requirements, updated references;
- deletion of technical overviews of profiles (Clauses 6 to 13), and associated dedicated subclauses for terms, definitions, symbols and abbreviations;
- addition of profiles for Communication Profile Families 8, 17 and 18 (Clauses 10, 14, 15);
- clarifications of models in Annex A;
- Annex B changed from informative to normative;
- addition of a new informative Annex E describing models for explicit and implicit FSCP mechanisms;
- addition of a new informative Annex F introducing an extended model for estimation of the total residual error rate;
- updates in parts for CPF 1, CPF 2, CPF 3, CPF 8, CPF 13 (details provided in the parts);
- addition of a new part for CPF 17.

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

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

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

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

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

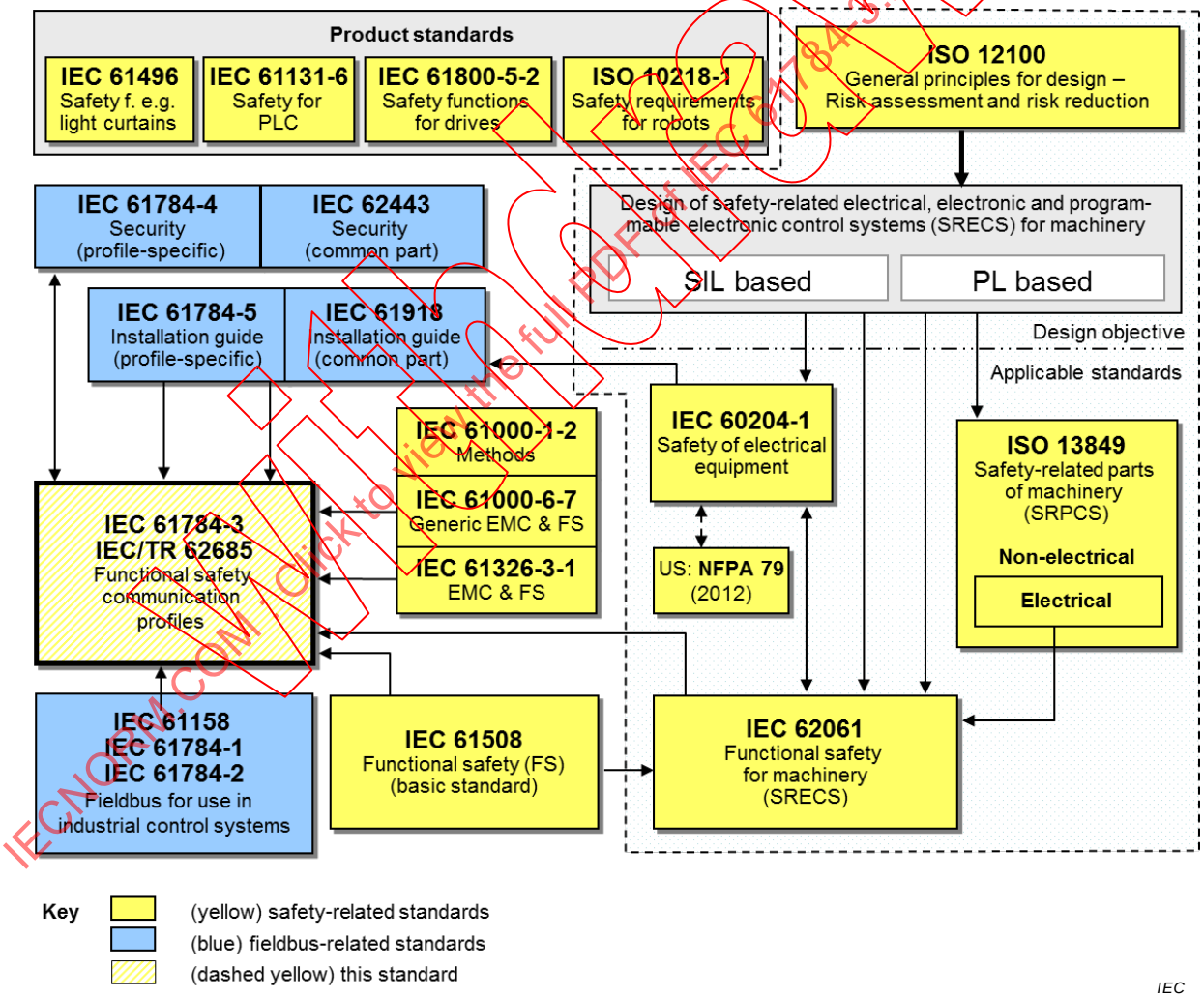
0 Introduction

0.1 General

The IEC 61158 fieldbus standard together with its companion standards IEC 61784-1 and IEC 61784-2 defines a set of communication protocols that enable distributed control of automation applications. Fieldbus technology is now considered well accepted and well proven. Thus fieldbus enhancements continue to emerge, addressing applications for areas such as real time, safety-related and security-related applications.

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

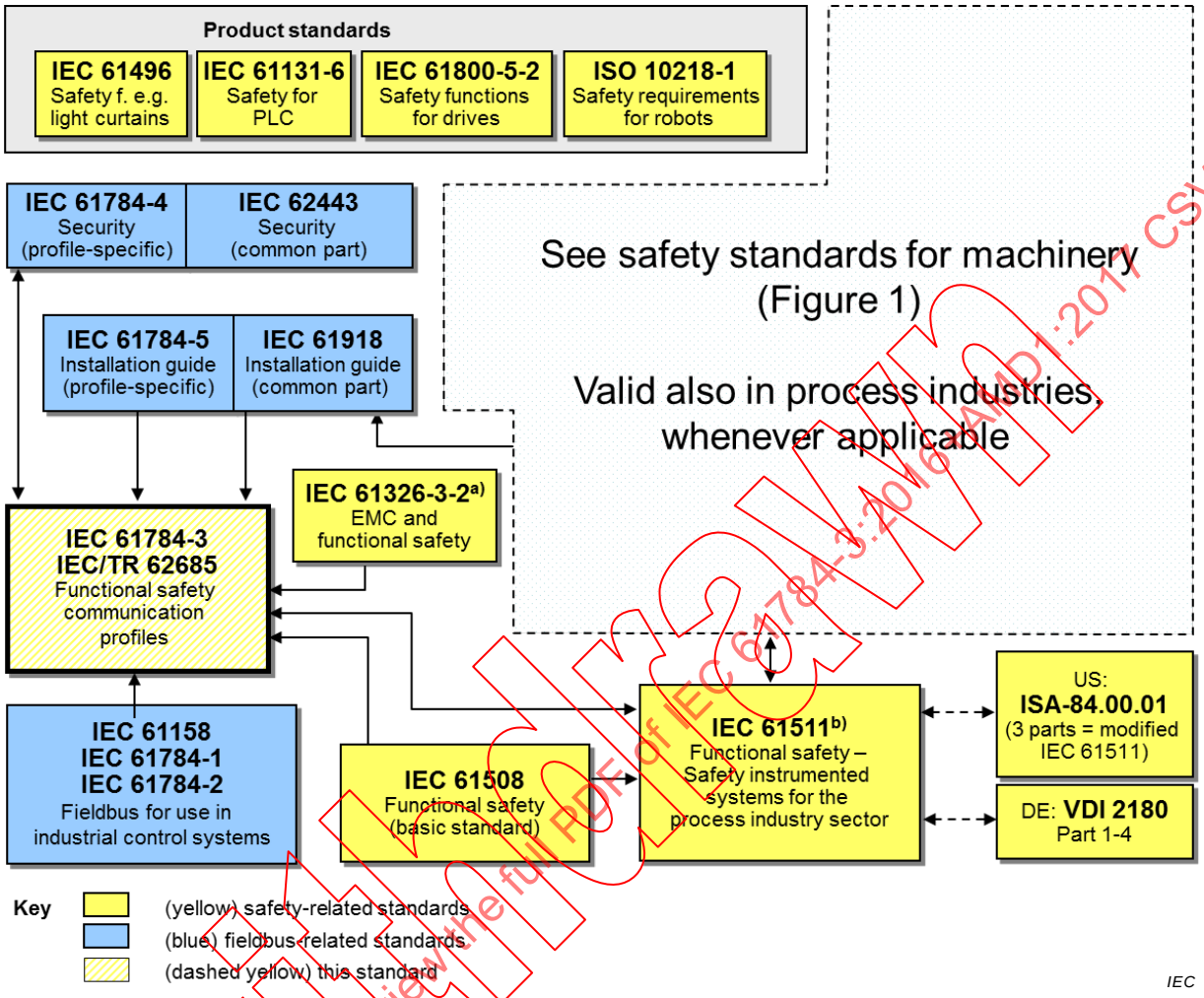
Figure 1 shows the relationships between this standard and relevant safety and fieldbus standards in a machinery environment.



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

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

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



[a] For specified electromagnetic environments; otherwise IEC 61326-3-1 or IEC 61000-6-7.

[b] EN ratified.

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

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

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

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

This standard describes:

- basic principles for implementing the requirements of IEC 61508 series for safety-related data communications, including possible transmission faults, remedial measures and considerations affecting data integrity;
- functional safety communication profiles for several communication profile families in IEC 61784-1 and IEC 61784-2, including safety layer extensions to the communication service and protocols sections of the IEC 61158 series.

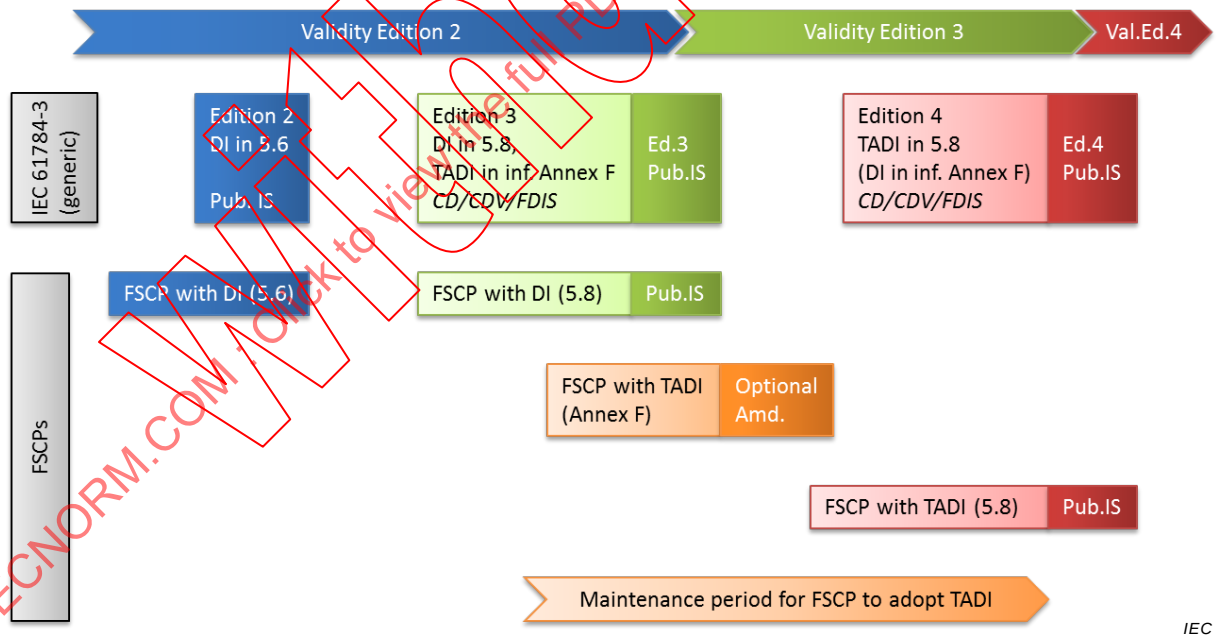
0.2 Transition from Edition 2 to extended assessment methods in Edition 3

This edition of the generic part of the standard includes additional extended models for future use when estimating the total residual error rate for an FSCP. This value can be used to determine if the FSCP meets the requirements of functional safety applications up to a given SIL. These extended models for qualitative and quantitative safety determination methods are detailed in Annex E and Annex F.

However, because of the typical duration of the assessment process, the FSCPs published prior to or concurrently with this new edition of the generic part can only be assessed using the methods from previous editions, based on data integrity considerations specified in 5.8.

The validity schema in Figure 3 shows how to handle the transition from original assessment methods of Edition 2 (specified in 5.8) to extended assessment methods in Edition 3 (currently specified in Annex F). According to this schema, the FSCPs are exempt from a new assessment according to Annex F until Edition 4, where the contents of current Annex F will replace the current 5.8.

NOTE However, a particular FSCP can achieve an earlier assessment and publish an adequate amendment.



Key

DI Data Integrity

TADI Timeliness, Authenticity, Data Integrity

Figure 3 – Transition from Edition 2 to Edition 3 assessment methods

0.3 Patent declaration

The International Electrotechnical Commission (IEC) draws attention to the fact that it is claimed that compliance with this document may involve the use of patents concerning functional safety communication profiles for families 1, 2, 3, 6, 8, 12, 13, 14, 17 and 18 given in IEC 61784-3-1, IEC 61784-3-2, IEC 61784-3-3, IEC 61784-3-6, IEC 61784-3-8, IEC 61784-3-12, IEC 61784-3-13, IEC 61784-3-14, IEC 61784-3-17 and IEC 61784-3-18.

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

NOTE Patent details and corresponding contact information are provided in IEC 61784-3-1, IEC 61784-3-2, IEC 61784-3-3, IEC 61784-3-6, IEC 61784-3-8, IEC 61784-3-12, IEC 61784-3-13, IEC 61784-3-14, IEC 61784-3-17 and IEC 61784-3-18.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights other than those identified above. IEC shall not be held responsible for identifying any or all such patent rights.

ISO (www.iso.org/patents) and IEC (http://patents.iec.ch) maintain on-line data bases of patents relevant to their standards. Users are encouraged to consult the data bases for the most up to date information concerning patents.

INTRODUCTION to the Amendment

This Amendment 1 discusses the concepts of implicit data safety mechanisms for use in functional safety communications protocols (FSCPs) as specified in IEC 61784-3:2016.

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 that can be used in the transmission of safety-relevant messages among participants within a distributed network which use fieldbus technology in accordance with the requirements of IEC 61508 series[1] for functional safety. These principles are based on the black channel approach. They can be used in various industrial applications such as process control, manufacturing automation and machinery.

This part[2] and the IEC 61784-3-x parts specify several functional safety communication profiles based on the communication profiles and protocol layers of the fieldbus technologies in IEC 61784-1, IEC 61784-2 and the IEC 61158 series. These functional safety communication profiles use the black channel approach, as defined in IEC 61508. These functional safety communication profiles are intended for implementation in safety devices exclusively.

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

NOTE 2 It does not cover electrical safety and intrinsic safety aspects. Electrical safety relates to hazards such as electrical shock. Intrinsic safety relates to hazards associated with potentially explosive atmospheres.

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

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

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

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

---

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

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

3 Proposed new work item under consideration.

IEC 61010-2-201:2013, *Safety requirements for electrical equipment for measurement, control and laboratory use – Part 2-201: Particular requirements for control equipment*

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*

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

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

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

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

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

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

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

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

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

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

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

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

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

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

IEC 61784-3-17[4], *Industrial communication networks – Profiles – Part 3-17: Functional safety fieldbuses – Additional specifications for CPF 17*

IEC 61784-3-18, *Industrial communication networks – Profiles – Part 3-18: Functional safety fieldbuses – Additional specifications for CPF 18*

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

IEC 61918:2013, *Industrial communication networks – Installation of communication networks in industrial premises*

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

3 Terms, definitions, symbols, abbreviated terms and conventions

3.1 Terms and definitions

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

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

3.1.1
absolute time stamp
time stamp referenced to a global time which is common for a group of devices using a *fieldbus*

[SOURCE: IEC 62280:2014, 3.1.1, modified – use devices and fieldbus]

3.1.2
active network element
network element containing electrically and/or optically active components that allows extension of the network

Note 1 to entry: Examples of active network elements are repeaters and switches.

[SOURCE: IEC 61918:2013, 3.1.2]

3.1.3
availability
probability for an automated system that for a given period of time there are no unsatisfactory system conditions such as loss of production

3.1.4
bit error probability
Pe
probability for a given bit to be received with the incorrect value

3.1.5
black channel
defined communication system containing one or more elements without evidence of design or validation according to IEC 61508

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

4 To be published

3.1.6
bridge
abstract device that connects multiple network segments along the data link layer

3.1.7
closed communication system
fixed number or fixed maximum number of participants linked by a communication system with well-known and fixed properties, and where the risk of unauthorized access is considered negligible

[SOURCE: IEC 62280:2014, 3.1.6, modified – transmission replaced by communication]

3.1.8
communication channel
logical connection between two end-points within a *communication system*

3.1.9
communication system
arrangement of hardware, software and propagation media to allow the transfer of *messages* (ISO/IEC 7498-1 application layer) from one application to another

3.1.10
connection
logical binding between two application objects within the same or different devices

3.1.11
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 to entry: 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 to entry: See also [28], [29][5].

3.1.12
defined communication system
defined channel
fixed number or fixed maximum number of participants linked by a fieldbus based communication system with well-known and fixed properties, such as installation conditions, electromagnetic immunity, industrial (active) network elements, and where the risk of unauthorized access is reduced to a tolerated level according to the lifecycle model of IEC 62443, using for example zones and conduits

3.1.13
diversity
different means of performing a required function

Note 1 to entry: Diversity may be achieved by different physical methods or different design approaches.

[SOURCE: IEC 61508-4:2010, 3.3.7]

5 Figures in square brackets refer to the bibliography.

3.1.14
error
discrepancy between a computed, observed or measured value or condition and the true, specified or theoretically correct value or condition

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

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

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

3.1.15
explicit code
code for safety measure that is actually transmitted within the SPDU and is known to the sender and receiver

3.1.16
failure
termination of the ability of a functional unit to perform a required function or operation of a functional unit in any way other than as required

Note 1 to entry: Failure may be due to an *error* (for example, problem with hardware/software design or message disruption).

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

3.1.17
fault
abnormal condition that may cause a reduction in, or loss of, the capability of a functional unit to perform a required function

Note 1 to entry: IEC 60050-191:1990, 191-05-01 defines "fault" as a state characterized by the inability to perform a required function, excluding the inability during preventive maintenance or other planned actions, or due to lack of external resources.

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

3.1.18
fieldbus
communication system based on serial data transfer and used in industrial automation or process control applications

3.1.19
fieldbus system
system using a *fieldbus* with connected devices

3.1.20
DLPDU
DEPRECATED: frame
Data Link Protocol Data Unit

3.1.21
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 to entry: An FCS can be derived using for example a CRC or other hash function.

Note 2 to entry: See also [28], [29].

Note 3 to entry: This note applies to the French language only.

3.1.22
hash function
(mathematical) function that maps values from a (possibly very) large set of values into a (usually) smaller range of values

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

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

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

3.1.23
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

3.1.24
implicit code
code for safety measure that is not transmitted within the SPDU but is known to the sender and receiver

3.1.25
master
active communication entity able to initiate and schedule communication activities by other stations which may be masters or slaves

3.1.26
message
ordered series of octets intended to convey information

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

3.1.27
message sink
part of a *communication system* in which *messages* are considered to be received

[SOURCE: ISO/IEC 2382-16:1996, 16.02.03]

3.1.28
message source
part of a *communication system* from which *messages* are considered to originate

[SOURCE: ISO/IEC 2382-16:1996, 16.02.02]

3.1.29
nuisance trip
spurious trip with no harmful effect

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

3.1.30
performance level
PL
discrete level used to specify the ability of safety-related parts of control systems to perform a safety function under foreseeable conditions

[SOURCE: ISO 13849-1:2015, 3.1.23]

3.1.31
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 1 to entry: A PELV circuit incorporates a connection to protective earth. Without the protective earth connection or if there is a fault in the protective earth connection, the circuit voltages are not controlled.

[SOURCE: IEC 61010-2-201:2013, 3.109, modified – deletion of "circuit" from term, and deletion of second note to entry]

3.1.32
redundancy
existence of more than one means for performing a required function or for representing information

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

3.1.33
relative time stamp
time stamp referenced to the local clock of an entity

Note 1 to entry: In general, there is no relationship to clocks of other entities.

[SOURCE: IEC 62280:2014, 3.1.43]

3.1.34
reliability
probability that an automated system can perform a required function under given conditions for a given time interval (t1,t2)

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

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

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

Note 4 to entry: Reliability differs from availability.

[SOURCE: IEC TR 62059-11:2002, 3.17, modified – use of "automated system" instead of "item" and addition of two notes]

3.1.35
residual error probability
RP
probability of an error undetected by the SCL safety measures

Note 1 to entry: This note applies to the French language only.

3.1.36
residual error rate
statistical rate at which the SCL safety measures fail to detect errors

3.1.37
risk
combination of the probability of occurrence of harm and the severity of that harm

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

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

3.1.38
safety communication channel
SC
communication channel starting at the top of the SCL of the source and ending at the top of the SCL of the sink

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

3.1.39
safety communication layer
SCL
communication layer above the FAL that includes all necessary additional measures to ensure safe transmission of data in accordance with the requirements of IEC 61508

Note 1 to entry: This note applies to the French language only.

3.1.40
safety connection
connection that utilizes the safety protocol for communications transactions

3.1.41
safety data
data transmitted across a safety network using a safety protocol

Note 1 to entry: The Safety Communication Layer does not ensure safety of the data itself, only that the data is transmitted safely.

3.1.42
safety device
device designed in accordance with IEC 61508 and which implements the functional safety communication profile

3.1.43
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

[SOURCE: IEC 61010-2-201:2013, 3.110, modified – deletion of "circuit" from term, and deletion of note to entry]

3.1.44
safety function
function to be implemented by an E/E/PE safety-related system or other risk reduction measures, that is intended to achieve or maintain a safe state for the EUC, in respect of a specific hazardous event

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

3.1.45
safety function response time
worst case elapsed time following an actuation of a safety sensor connected to a fieldbus, until the corresponding safe state of its safety actuator(s) is achieved in the presence of errors or failures in the safety function

Note 1 to entry: This concept is introduced in 5.2.4 and addressed by the functional safety communication profiles defined in this part.

3.1.46
safety integrity level
SIL
discrete level (one out of a possible four), corresponding to a range of safety integrity values, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest

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

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

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

Note 4 to entry: This note applies to the French language only.

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

3.1.47
safety measure
measure to control possible communication *errors* that is designed and implemented in compliance with the requirements of IEC 61508

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

Note 2 to entry: Communication *errors* and related safety measures are detailed in 5.3 and 5.4.

3.1.48
safety PDU
SPDU
PDU transferred through the safety communication channel

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

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

Note 3 to entry: This note applies to the French language only.

3.1.49
safety-related application
programs designed in accordance with IEC 61508 to meet the SIL requirements of the application

3.1.50
safety-related system
system performing *safety functions* according to IEC 61508

3.1.51
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

3.1.52
spurious trip
trip caused by the safety system without a process demand

3.1.53
time stamp
time information included in a *message*

3.1.54
uniform distribution
probability distribution where all values from a finite set are equally likely to occur

Note 1 to entry: For a field of bit length i the probability of occurrence of a particular field value is 2^{-i} since the sum of all probabilities of occurrence is equal to 1.

3.1.55
white channel
defined communication system in which all relevant hardware and software elements are designed, implemented and validated according to IEC 61508

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

3.1.56
explicit data
data that is transmitted

3.1.57
implicit data
additional data that is not transmitted but is known to the sender and receiver

[SOURCE: IEC 62280:2014, 3.1.25]

3.2 Symbols and abbreviated terms

3.2.1 Abbreviated terms

A-code	Authenticity code	
BSC	Binary Symmetric Channel	
CP	Communication Profile	[IEC 61784-1]
CPF	Communication Profile Family	[IEC 61784-1]
CRC	Cyclic Redundancy Check	
DLL	Data Link Layer	[ISO/IEC 7498-1]
DLPDU	Data Link Protocol Data Unit	
EMC	Electromagnetic Compatibility	
EMI	Electromagnetic Interference	
EUC	Equipment Under Control	[IEC 61508-4:2010]
E/E/PE	Electrical/Electronic/Programmable Electronic	[IEC 61508-4:2010]
FAL	Fieldbus Application Layer	[IEC 61158-5]
FCS	Frame Check Sequence	

FIT	Failure In Time (equals 10^{-9} failure per hour)	
FS	Functional Safety	
FSCP	Functional Safety Communication Profile	
IACS	Industrial Automation and Control System	
MTBF	Mean Time Between Failures	
MTTF	Mean Time To Failure	
NSR	Non Safety Related	
PDU	Protocol Data Unit	[ISO/IEC 7498-1]
PELV	Protective Extra Low Voltage	
PES	Programmable Electronic System	[IEC 61508-4:2010]
PFD_{avg}	Average probability of dangerous Failure on Demand	[IEC 61508-4:2010]
PFH	Average frequency of dangerous failure [h^{-1}] per hour	[IEC 61508-4:2010]
PhL	Physical Layer	[ISO/IEC 7498-1]
PL	Performance Level	[ISO 13849-1]
PLC	Programmable Logic Controller	
SCL	Safety Communication Layer	
SELV	Safety Extra Low Voltage	
SIS	Safety Instrumented Systems	
SL	Security Level	[IEC 62443]
SMS	Security Management System	[IEC 62443]
SPDU	Safety PDU	
SR	Safety Related	
T-code	Timeliness code	

3.2.2 Symbols

A_k	Weight distribution of the code: number of valid codewords having k bits set to “one”
e	Bit length of explicit data
err_{impl}	Bitwise disjunction of $impl_S$ and $impl_R$
expl	Explicit data
$expl_R$	Explicit data in the receiver
$expl_S$	Explicit data in the sender
FCS_C	Frame check sequence calculated in the receiver
FCS_R	Frame check sequence received
FCS_S	Frame check sequence sent
i	Bit length of implicit data
ID	Incorrect delivery
$impl_R$	Implicit data in the receiver
$impl_S$	Implicit data in the sender
n	Bit length of SPDU
P_e	Bit error probability
P_{ID}	Probability of incorrect delivery
r	Bit length of FCS (degree of generator polynomial)
RP	Residual error probability

4 Conformance

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

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

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

or

conformance to IEC 61784-3 (Ed.3.0) FSCP n/m <Type>

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

Alternatively, a statement of conformance may be stated as either

conformance to IEC 61784-3-N:20xx

or

conformance to IEC 61784-3-N (Ed.3.0)

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

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

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

5 Basics of safety-related fieldbus systems

5.1 Safety function decomposition

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

The communication system itself in this standard performs transmission of safety data. To simplify system calculations, it is recommended that one logical connection of safety communication channels of a safety function does not consume more than 1 % of the maximum PFH or PFD_{avg} of the target SIL for which the functional safety communication profile is designed (see Figure 4 and 5.8.2).

If this value of 1 % for one logical connection cannot be guaranteed by a given FSCP, the safety manual for this FSCP shall provide additional guidance on the calculations of the PFH or PFD_{avg}.

The overall PFH and PFD_{avg} of each safety device shall incorporate the PFH and PFD_{avg} of the logical connection. The PFD_{avg} shall be provided if the FSCP is also used for low demand mode applications according to IEC 61508.

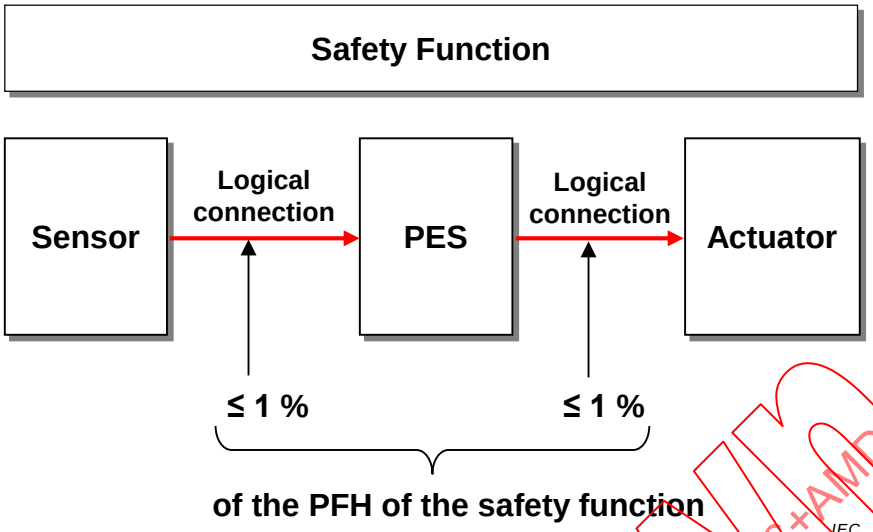


Figure 4 – Safety communication as a part of a safety function

Alternatively, the PFH / PFD_{avg} of the communication can be calculated for the whole safety function. In this case, the PFH / PFD_{avg} of the safety communication needs to be considered only once.

5.2 Communication system

5.2.1 General

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

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 5 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 5.

The safety communication layer includes suitable services and protocol to encode safety data into safety PDUs and pass them to the black channel and to receive safety PDUs from the black channel and decode them to extract safety data.

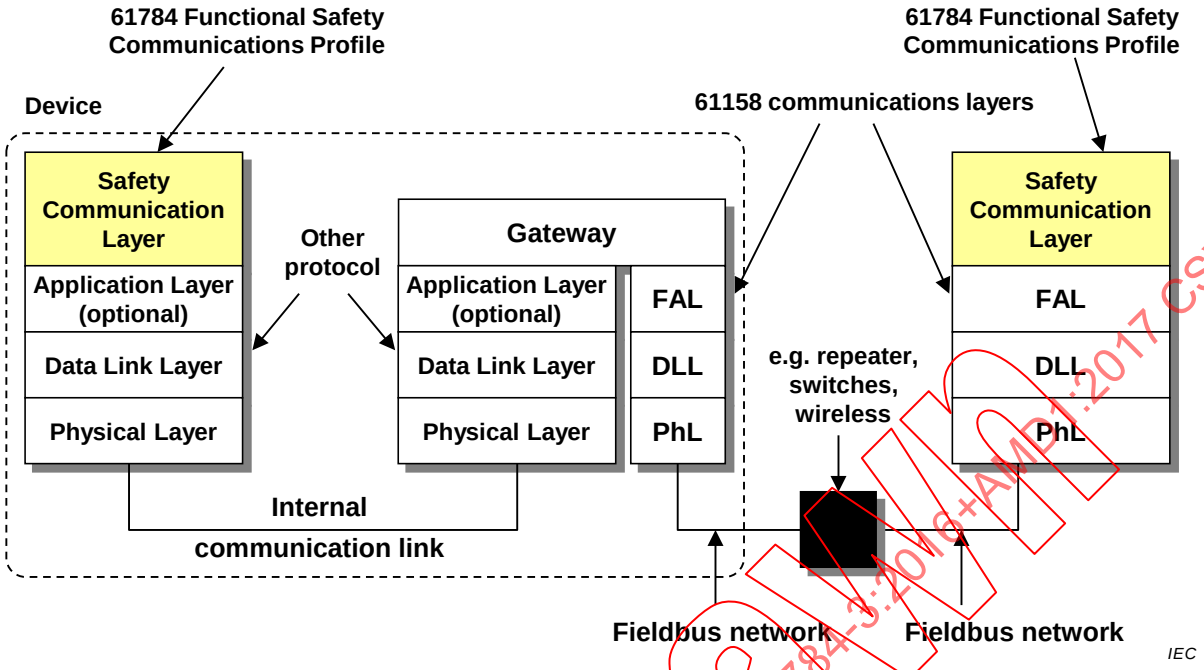


Figure 5 – Example model of a functional safety communication system

While implementation of the Fieldbus Application Layer (FAL) is required for functional safety communication systems according to this standard, the Application Layer may be omitted for communication links internal to a device (for example with a gateway).

Functions that are not safety-related may bypass the SCL and access the FAL directly.

5.2.3 Communication channel types

IEC 61508 uses the concepts of the so called “black channel” or “white channel” to define the requirements of the base fieldbus for transmission of safety data. This standard specifies functional safety communication profiles that use the black channel approach.

In this context, a safety communication channel is defined to start at the top of the safety communication layer of the source and stop at the top of the safety communication layer of the sink (see Figure 5). The black channel includes everything between the safety communication layers.

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, until 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.

Calculation of the safety function response time is specified in the profile specific parts of IEC 61784-3.

Empirical measurements may only serve as a plausibility check of the worst case calculation.

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

Figure 6 shows an example of typical components making up a safety function response time.

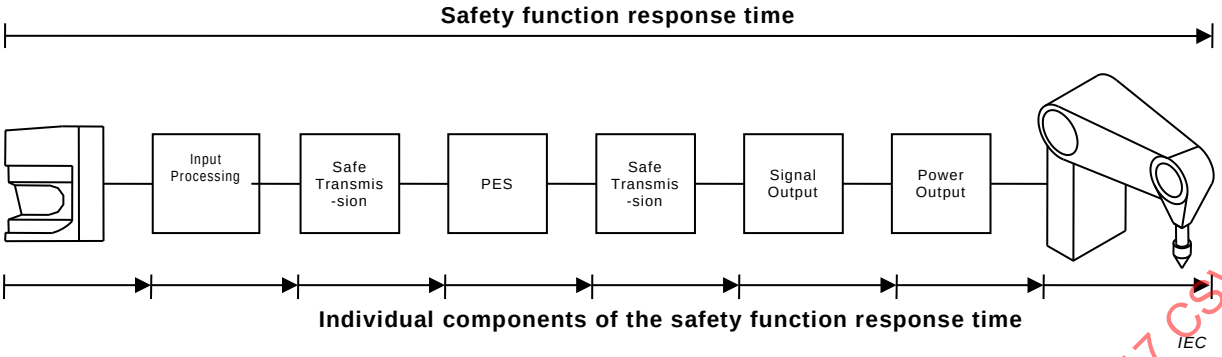


Figure 6 – Example of safety function response time components

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

Subclauses 5.3.2 to 5.3.9 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 will 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 can 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, messages are repeated.

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.

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 This “incorrect sequence” error is also referred to as “out-of-sequence” error.

NOTE 2 Fieldbus systems can contain elements that store messages (for example FIFOs in switches, bridges, routers) or use protocols that can alter the sequence (for example by allowing messages with high priority to overtake those with lower priority).

NOTE 3 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 can be reported for each sequence.

5.3.5 Loss

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

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)..

5.3.7 Insertion

Due to a fault or interference, a message is received 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 related message may be received by a safety related participant, which then treats it as safety related.

NOTE Communication systems used for safety-related applications can 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 related message is delivered to the incorrect safety related participant, which then treats reception as correct. This includes the so-called loopback error case, where the sender receives back its own sent message.

5.4 Deterministic remedial measures

5.4.1 General

Subclauses 5.4.2 to 5.4.9 list 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 Relative time stamps and absolute time stamps can be used.

Time stamping requires the time base to be synchronized. For safety applications, synchronization shall be regularly monitored, and the probability of this mechanism failing shall be included in the assessment of the overall safety function.

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 sends 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 related participant.

5.4.6 Feedback message

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

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

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

5.4.7 Data integrity assurance

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

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

If a hash function is used, it shall not include error correction mechanisms.

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 related (SR) and non-safety related (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.

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

5.5 Typical 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. Typical relationships are shown in Table 1, actual relationships shall be specified by each FSCP. Each safety measure can provide protection against one or more errors in the transmission. It shall be demonstrated that there is at least one corresponding safety measure or combination of safety measures for the defined possible errors in accordance with Table 1.

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

A safety measure shall only be listed in the corresponding table for a given FSCP if this measure takes effect before the guaranteed fieldbus safety response time.

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

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

NOTE Table adapted from IEC 62280:2014, Table 1.

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

[b] Required in all cases.

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

[d] Effective only if feedback message includes original data or information about the original data, and if the receiver only acts on the data after acknowledge of the feedback message.

[e] Effective only if the sequence numbers or time stamps of the source entities are different.

5.6 Communication phases

An FSCP shall be designed so that either a safe state or a sufficient residual error rate at the receiver side can be achieved according to IEC 61508 within each and every communication phase of the safety network, including:

- setup or change of the safety network (configuration and parameterization);
- start-up with initialization (e.g. connection establishment);
- operation (safety data exchange);
- warm-start after transition from a fault;
- shutdown.

Figure 7 shows a conceptual FSCP protocol model. An FSCP shall not return directly to correct FSCP communication after a fault, but first go through warm start or new initialization phases, depending on the FSCP.

NOTE In case of faults, the FSCP can take care of application requirements such as an operator acknowledge prior to a machine start.

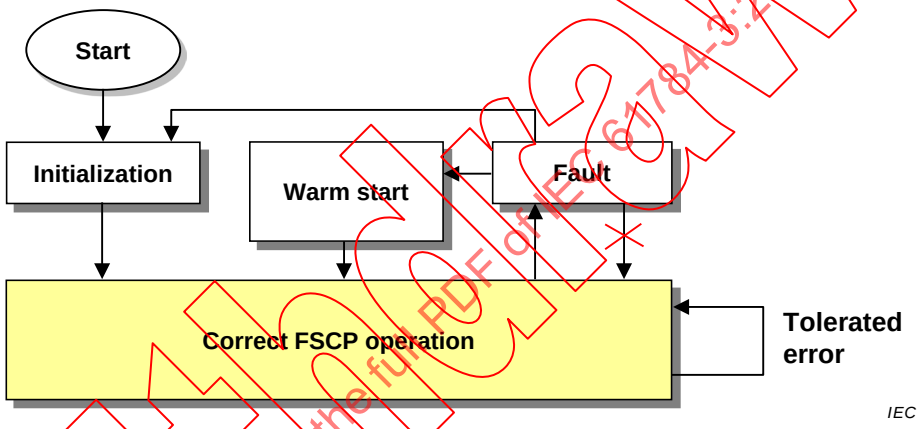


Figure 7 – Conceptual FSCP protocol model

5.7 FSCP implementation aspects

All FSCP technical measures shall be implemented within the SCL in devices designed in accordance with IEC 61508 and shall meet the target SIL.

Some protocol measures depend on the manner they are implemented in a particular safety device. Figure 8 shows the separation between FSCP implementation aspects and its deterministic and probabilistic aspects.

An example of an implementation aspect is a dependency on the failure rate of real-time clocks, watchdogs or microcontrollers. These aspects require quantitative safety assessments according to IEC 61508 to determine their relevance to the individual considerations of generic safety properties.

This standard does not consider implementation aspects, except when an implementation aspect is required by an FSCP and that aspect can affect the FSCPs residual error rate. Generic safety properties are considered based on logical connections between SCL end-points (using only basic assumptions on the black channel performance as stated in the safety manuals of the individual FSCPs).

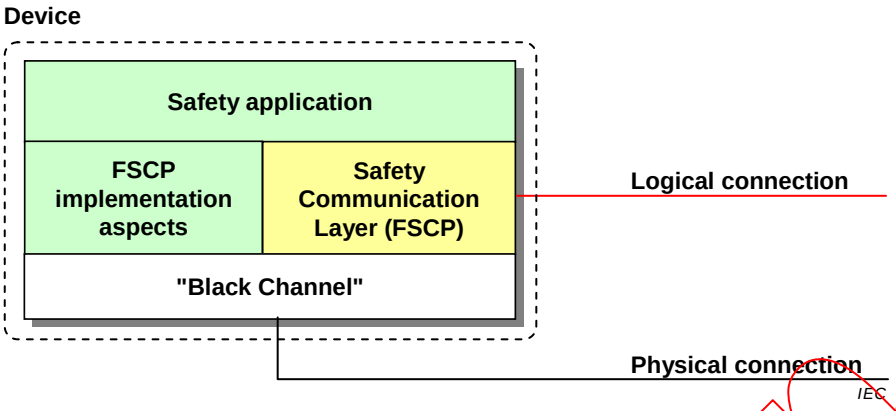


Figure 8 – FSCP implementation aspects

5.8 Data integrity considerations

5.8.1 Calculation of the residual error rate

Even when the messages are arriving in a correct (deterministic) manner the SPDU 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 fieldbus DLL shall not use the same hash function as the superimposed safety communication layer unless special care is taken for those cases. The safety code shall be functionally independent from the transmission code.

EXAMPLE When CRC is used as the hash function, the fieldbus DLL 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 sample rate of SPDUs. In case of calculation of PFH / PFD_{avg} per safety function, one shall take into account for the assessment the maximum number of information sinks (m) that is permitted in a single safety function.

Equations (1) and (2) shown below shall be used to calculate the residual error rates resulting from R_{SC} (Pe), unless the underlying model does not apply, or if another method may be more relevant. Items of the equations are specified in Table 2.

$$\lambda_{SC}(Pe) = R_{SC}(Pe) \times v \quad (1)$$

$$\lambda_{SCL}(Pe) = \lambda_{SC}(Pe) \times m \quad (2)$$

NOTE These equations assume cyclic sampling of SPDUs by the SCL.

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

Equation items	Definition
λ_{SC} (Pe)	Residual error rate per hour of the safety communication channel with respect to the bit error probability (see 3.1.36)
λ_{SCL} (Pe)	Residual error rate per hour of the safety communication layer with respect to the bit error probability (see 3.1.36)
Pe	Bit error probability (see Clause B.3)
R_{SC} (Pe)	Residual error probability of the safety communication channel with respect to the bit error probability (see 3.1.35)
v	Maximum sample rate of SPDUs per hour
m	Maximum number of logical connections that is permitted in a single safety function (see Figure 9 and Figure 10)

The number m of logical connections depends on the individual safety function application. Figure 9 and Figure 10 illustrate how this number can be determined.

The figures show the physical connections with possible network elements such as repeaters, switches, or wireless links and the logical connections between the subsystems involved in the safety function.

The logical connections can be based on single cast or multicast communications.

Figure 9 shows an example 1 of an application where m = 4. In this application, all three drives are considered to be hazardous at a single point in time according to the risk analysis.

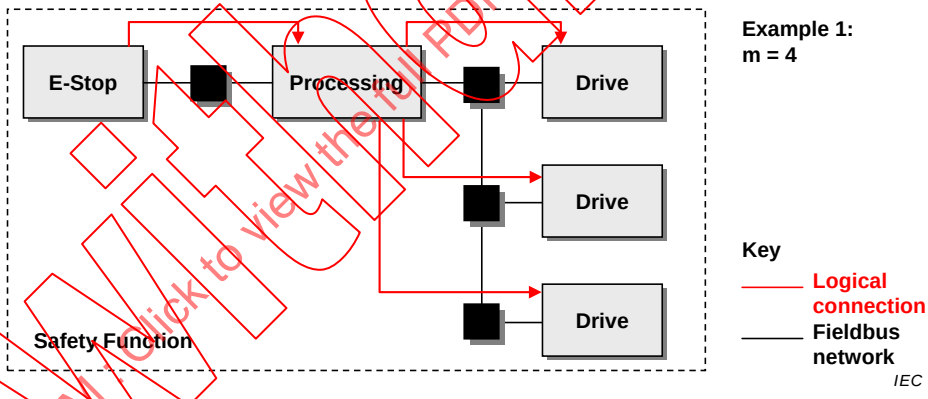


Figure 9 – Example application 1 (m=4)

Figure 10 shows an example 2 of an application where m = 2. In this application, only one of the drives is considered to be hazardous at a single point in time according to the risk analysis.

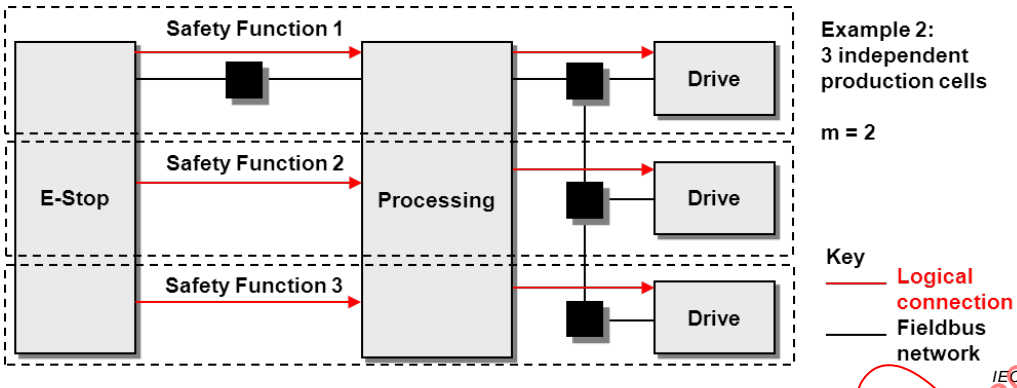


Figure 10 – Example application 2 (m = 2)

5.8.2 Total residual error rate and SIL

A functional safety communication system shall provide a residual error rate in accordance with this standard. Table 3 and Table 4 show the typical relationships between residual error rate and SIL, based on the assumption that the functional safety communication system contributes no more than 1 % per logical connection of the safety function.

Both low demand and high demand mode systems shall have a defined safety function response time, so a necessary rate of SPDUs shall be guaranteed. The PFH for a certain SIL shall be provided in all cases, while the PFD_{avg} is optional.

Table 3 – Typical relationship of residual error rate to SIL

Applicable for safety functions up to SIL	Average frequency of a dangerous failure for the safety function (PFH)	Maximum permissible residual error rate for one logical connection of the safety function (λ_{sc} (Pe))
4	$< 10^{-8}$/h	$< 10^{-10}$/h
3	$< 10^{-7}$/h	$< 10^{-9}$/h
2	$< 10^{-6}$/h	$< 10^{-8}$/h
1	$< 10^{-5}$/h	$< 10^{-7}$/h

Table 4 – Typical relationship of residual error on demand to SIL

Applicable for safety functions up to SIL	Average probability of a dangerous failure on demand for the safety function (PFDavg)	Maximum permissible residual error probability for one logical connection of the safety function
4	$< 10^{-4}$	$< 10^{-6}$
3	$< 10^{-3}$	$< 10^{-5}$
2	$< 10^{-2}$	$< 10^{-4}$
1	$< 10^{-1}$	$< 10^{-3}$

5.9 Relationship between functional safety and security

Security threat and risk assessment is necessary for safety-related applications. Requirements for security are detailed in the IEC 62443 series.

Security means protection against unacceptable intentional (cyber) attacks or unintentional changes of an industrial automation and control system (IACS).

Security concepts in IEC 62443 follow a similar life cycle concept as IEC 61508, starting with a security threat and risk assessment and the assignment of target Security Levels. However, due to the nature of the threats caused by individuals, IEC 62443 emphasizes primarily on issues such as policies and procedures for a Security Management System (SMS) established by plant owners and suppliers within their organization. One major issue of the SMS is maintenance of the security system to counter degradation, for example via monitoring, periodic assessments, or software patches.

IEC 62443 then specifies technologies and methods to achieve a secure system by partitioning the architecture of an IACS into zones and conduits. The plant owner or integrator is provided with appropriate countermeasures and technologies to achieve the target Security Level and its seven foundational requirements (vector) for the zones and conduits.

IEC 62443 also addresses the requirements to secure system components.

IEC 62443 allows designers to choose where to implement the security countermeasures with respect to safety devices.

NOTE Additional profile specific requirements can also be specified in IEC 61784-4.

Figure 11 shows an example of the zones and conduits partitioning of an IACS with functional safety islands.

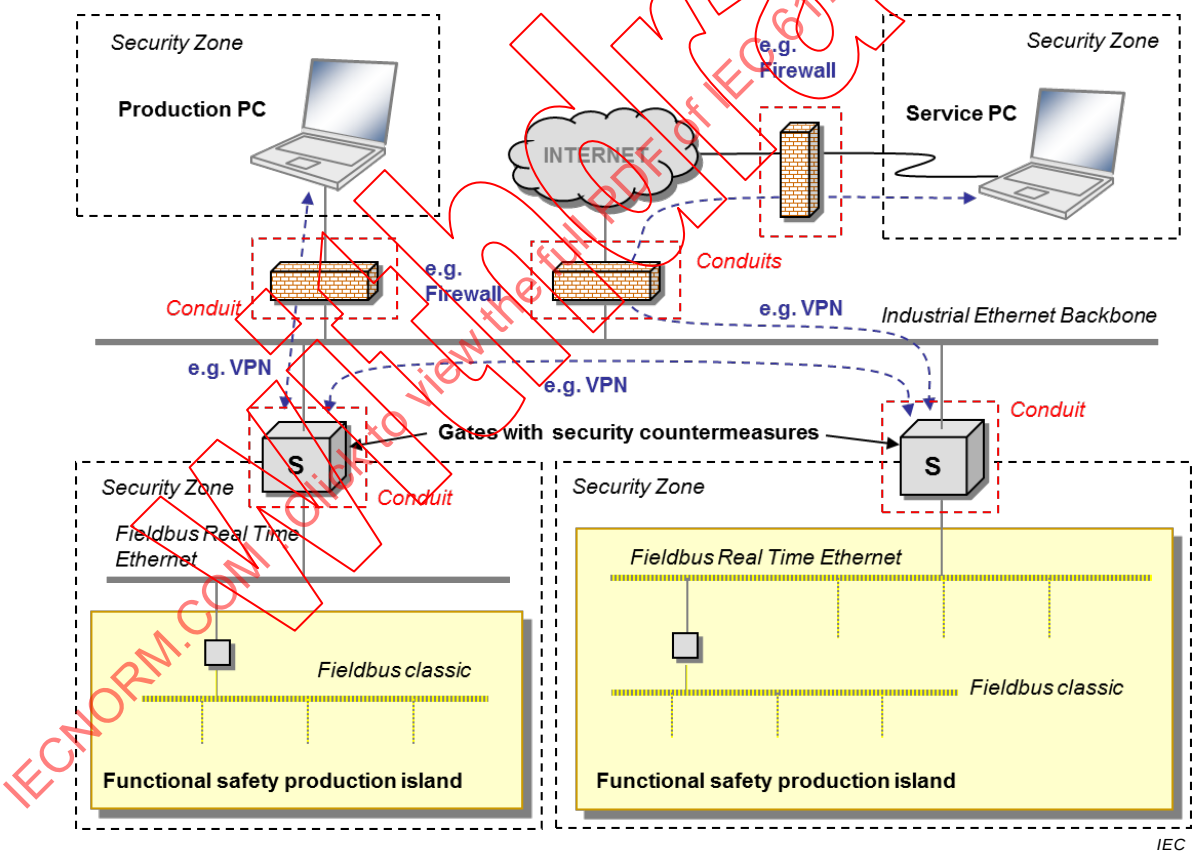


Figure 11 – Zones and conduits concept for security according to IEC 62443

5.10 Boundary conditions and constraints

5.10.1 Electrical safety

Electrical safety is a precondition for a functional safety communication system. Therefore, all safety devices connected to it shall conform to the relevant IEC electrical safety standards (for example SELV/PELV as specified in IEC 61010-2-201). The Safety Manual shall specify

the constraints required of the devices connected in a functional safety communication system, whether safety devices or non-safety devices, including active network elements.

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

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

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

5.10.2 Electromagnetic compatibility (EMC)

Safety devices shall comply with the increased test levels and durations, as well as corresponding performance criteria specified in IEC 61326-3-1 or the generic standard IEC 61000-6-7. 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 can require higher levels than those specified in IEC 61326-3-1, according to Safety Requirements Specification (SRS).

5.11 Installation guidelines

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

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

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

NOTE Additional details can be provided in the technology-specific parts of the IEC 61784-3 sub-series if relevant.

5.12 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.

5.13 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 communication technologies specified in this standard shall only be implemented in devices designed in accordance with the requirements of IEC 61508.

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

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

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

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

It is strongly recommended that implementers of a specific profile comply with the appropriate conformance tests and validations provided by the related technology-specific organization.

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

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

Communication Profile Family 1 (commonly known as FOUNDATION™ Fieldbus[6]) 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™[6]) 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.

7 Communication Profile Family 2 (CIP™) and Family 16 (SERCOS®) – Profiles for functional safety

Communication Profile Family 2 (commonly known as CIP™[7]) 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.

Communication Profile Family 16 (commonly known as SERCOS®[8]) defines a communication profile CP 16/3 based on IEC 61158-3-19, IEC 61158-4-19, IEC 61158-5-19, and IEC 61158-6-19.

---

6 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 and compliance with conditions for their use (such as testing and validation).

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

8 SERCOS® is a trade name of SERCOS International e.V. This information is given for the convenience of users of this International Standard and does not constitute an endorsement by IEC of the trademark holder or any of its products. Compliance to this standard does not require use of the trade name SERCOS®. Use of the trade

The basic profiles CP 2/1, CP 2/2, CP 2/3 and CP 16/3 are defined in IEC 61784-1 and IEC 61784-2. The CPF 2 functional safety communication profile FSCP 2/1 (CIP Safety™[7]) is based on the CPF 2 basic profiles in IEC 61784-1 and IEC 61784-2, the CP 16/3 basic profile in IEC 61784-2, and the safety communication layer specifications defined in IEC 61784-3-2.

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

Communication Profile Family 3 (commonly known as PROFIBUS™, PROFINET™[9]) 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™[9]) 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.

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

Communication Profile Family 6 (commonly known as INTERBUS®[10]) 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™[10]) 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 5.

Table 5 – 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.

name SERCOS® requires permission of the trade name holder and compliance with conditions for its use (such as testing and validation).

9 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 trade names for PROFIBUS™, PROFINET™ or PROFIsafe™. Use of the registered trade names for PROFIBUS™, PROFINET™ or PROFIsafe™ requires permission of PNO and compliance with conditions for their use (such as testing and validation).

10 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 and compliance with conditions for their use (such as testing and validation).

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

10.1 Functional Safety Communication Profile 8/1

Communication Profile Family 8 (commonly known as CC-Link™[11]) defines communication profiles based on IEC 61158-2 Type 18, IEC 61158-3-18, IEC 61158-4-18, IEC 61158-5-18, and IEC 61158-6-18.

The basic profiles CP 8/1, CP 8/2, and CP 8/3 are defined in IEC 61784-1. The CPF 8 functional safety communication profile FSCP 8/1 (CC-Link Safety™[11]) is based on the CPF 8 basic profiles in IEC 61784-1 and the safety communication layer specifications defined in IEC 61784-3-8.

10.2 Functional Safety Communication Profile 8/2

Communication Profile Family 8 also defines communication profiles based on IEC 61158-5-23 and IEC 61158-6-23.

The basic profiles CP 8/4 and CP 8/5 (commonly known as CC-Link IE™[12]) are defined in IEC 61784-2. The CPF 8 functional safety communication profile FSCP 8/2 (CC-Link IE™ Safety communication function) is based on the CPF 8 basic profiles in IEC 61784-2 and the safety communication layer specifications defined in IEC 61784-3-8.

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

Communication Profile Family 12 (commonly known as EtherCAT™[13]) defines communication profiles based on IEC 61158-2 Type 12, IEC 61158-3-12, IEC 61158-4-12, IEC 61158-5-12 and IEC 61158-6-12.

The basic profiles CP 12/1 and CP 12/2 are defined in IEC 61784-2. The CPF 12 functional safety communication profile FSCP 12/1 (Safety-over-EtherCAT™[13]) is based on the CPF 12 basic profiles in IEC 61784-2 and the safety communication layer specifications defined in IEC 61784-3-12.

---

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

12 CC-Link IE™ is a trade name of the non-profit organization CC-Link Partner Association. This information is given for the convenience of users of this International Standard and does not constitute an endorsement by IEC of the trade name holder or any of its products. Compliance to this standard does not require use of the trade name CC-Link IE™. Use of the trade name CC-Link IE™ requires permission of CC-Link Partner Association and compliance with conditions for its use (such as testing and validation).

13 EtherCAT™ and Safety-over-EtherCAT™ are trade names of Beckhoff, Verl. This information is given for the convenience of users of this International Standard and does not constitute an endorsement by IEC of the trade name holder or any of its products. Compliance to this standard does not require use of the trade names EtherCAT™ or Safety-over-EtherCAT™ Use of the trade names EtherCAT™ or Safety-over-EtherCAT™ requires permission of Beckhoff, Verl and compliance with conditions for their use (such as testing and validation).

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

Communication Profile Family 13 (commonly known as Ethernet POWERLINK™[14]) defines communication profiles based on IEC 61158-3-13, IEC 61158-4-13, IEC 61158-5-13, and IEC 61158-6-13.

The basic profile CP 13/1 is defined in IEC 61784-2. The CPF 13 functional safety communication profile FSCP 13/1 (openSAFETY™[14]) is based on the CPF 13 basic profiles in IEC 61784-2 and the safety communication layer specifications defined in IEC 61784-3-13.

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

Communication Profile Family 14 (commonly known as EPA®[15]) defines communication profiles based on IEC 61158-3-14, IEC 61158-4-14, IEC 61158-5-14, and IEC 61158-6-14.

The basic profiles CP 14/1 and CP 14/2 are defined in IEC 61784-2. The CPF 14 functional safety communication profile FSCP 14/1 (EPASafety®[15]) is based on the CPF 14 basic profiles in IEC 61784-2 and the safety communication layer specifications defined in IEC 61784-3-14.

14 Communication Profile Family 17 (RAPIEnet™) – Profiles for functional safety

Communication Profile Family 17 (commonly known as RAPIEnet™[16]) defines a communication profile based on IEC 61158-3-21, IEC 61158-4-21, IEC 61158-5-21, and IEC 61158-6-21.

The basic profile CP 17/1 is defined in IEC 61784-2. The CPF 17 functional safety communication profile FSCP 17/1 (RAPIEnet Safety™[16]) is based on the CPF 17 basic profile in IEC 61784-2 and the safety communication layer specifications defined in IEC 61784-3-17.

---

14 Ethernet POWERLINK™ and openSAFETY™ are trade names of the non-profit organization Ethernet POWERLINK™ Standardization Group (EPSG). This information is given for the convenience of users of this International Standard and does not constitute an endorsement by IEC of the trade name holder or any of its products. Compliance to this standard does not require use of the trade names Ethernet POWERLINK™ or openSAFETY™. Use of the trade names Ethernet POWERLINK™ or openSAFETY™ requires permission of Ethernet POWERLINK™ Standardization Group (EPSG) and compliance with conditions for their use (such as testing and validation).

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

16 RAPIEnet™ and RAPIEnet Safety™ are trade names of the non-profit organization RAPIEnet Association. This information is given for the convenience of users of this International Standard and does not constitute an endorsement by IEC of the trade name holder or any of its products. Compliance with this standard does not require use of the registered trade names for RAPIEnet™ or RAPIEnet Safety™. Use of the registered trade names for RAPIEnet™™ or RAPIEnet Safety™ requires permission of RAPIEnet Association and compliance with conditions for their use (such as testing and validation).

15 Communication Profile Family 18 (SafetyNET p™ Fieldbus) – Profiles for functional safety

Communication Profile Family 18 (commonly known as SafetyNET p™[17]) defines communication profiles based on IEC 61158-3-22, IEC 61158-4-22, IEC 61158-5-22 and IEC 61158-6-22.

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

17 SafetyNET p is a trade name of the Pilz GmbH & Co. KG. 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 profile does not require use of the trade name SafetyNET p. Use of the trade name SafetyNET p requires permission of the trade name holder and compliance with conditions for its use (such as testing and validation).

Annex A
(informative)

Example functional safety communication models

A.1 General

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

Some examples are listed in Clauses A.2 to A.5 – other models may be used.

NOTE Implementation structures in these examples are based on redundant safety communication layers, in accordance with IEC 61508 examples.

A.2 Model A (single message, channel and FAL, redundant SCLs)

Model A shown in Figure A.1 serves as the base reference model for the other models. Only one fieldbus is used as the communication channel.

Two SCLs operate independently to generate two SPDUs from the same safety data. The SPDUs are cross-checked before one of them is transferred using a single fieldbus message. The received SPDU is independently decoded and safety checked by the two receiving SCLs and cross-checked. Both safety communication layers are involved in the production of the message.

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

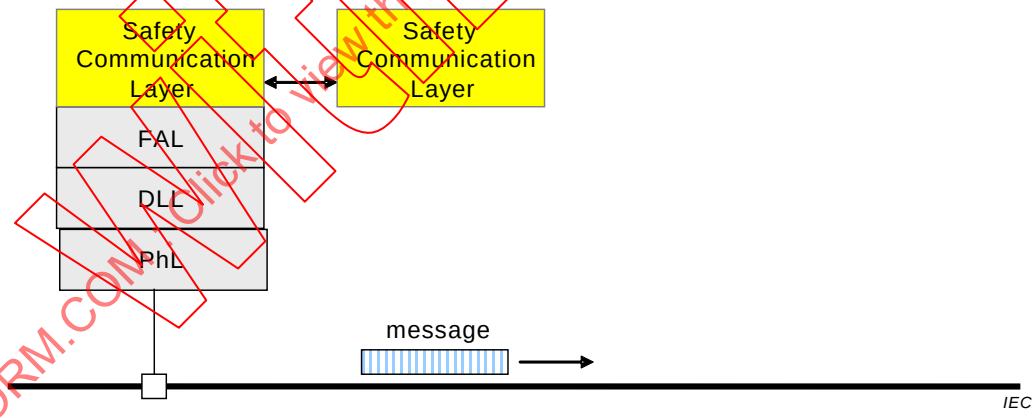


Figure A.1 – Model A

A.3 Model B (full redundancy)

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

Each SCL generates an SPDU from the same safety data and sends it on the attached fieldbus. The messages from both safety communication channels are safety-checked and cross-checked.

Transmission layers and transmission media may be of different types.

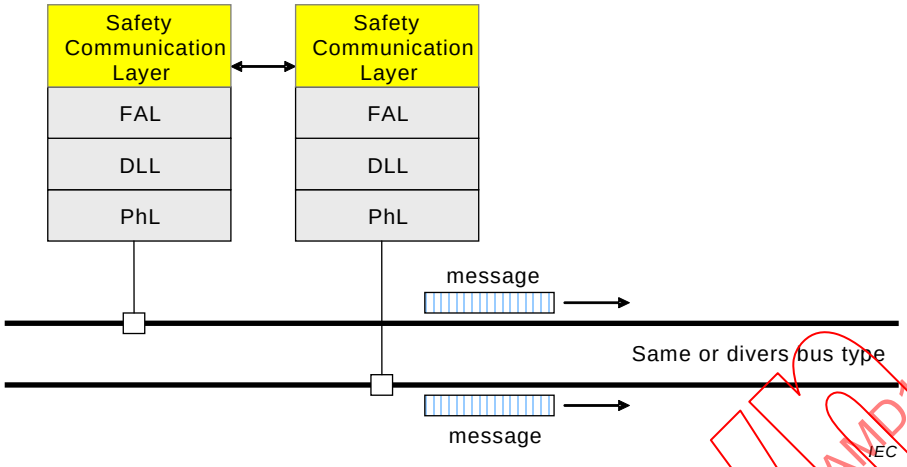


Figure A.2 – Model B

A.4 Model C (redundant messages, FALs and SCLs, single channel)

Model C in Figure A.3 shows a system with full redundancy of the fieldbus device components and only one transmission medium.

Two SCLs generate SPDUs from the same safety data. The SPDUs are sent at different times on the same fieldbus using different messages. The messages from both safety communication channels are safety-checked by both and cross-checked.

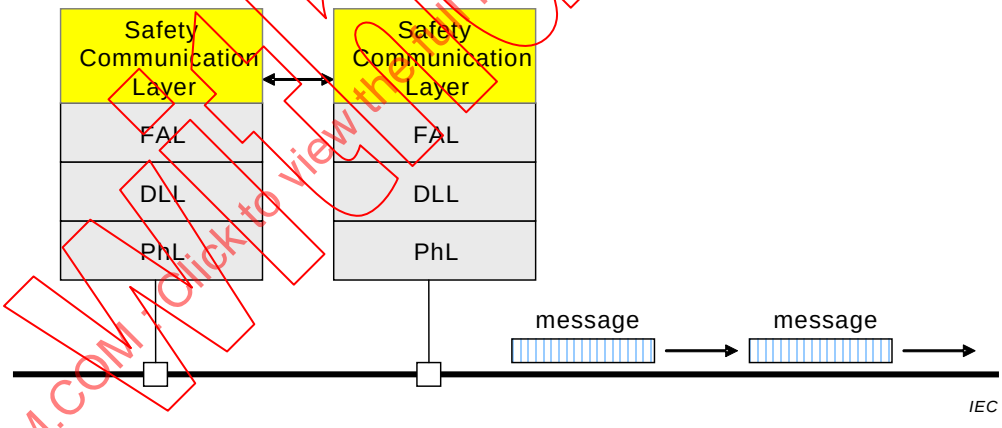


Figure A.3 – Model C

A.5 Model D (redundant messages and SCLs, single channel and FAL)

Model D in Figure A.4 shows a system with dual safety communication layers while the transmission layers exist only once.

Two SCLs generate SPDUs from the same safety data. The SPDUs are sent at different times on the same fieldbus using different messages. Alternatively the two SPDUs can be sent as separate fields in the same message.

The messages from both safety communication layers are safety-checked independently and cross-checked.

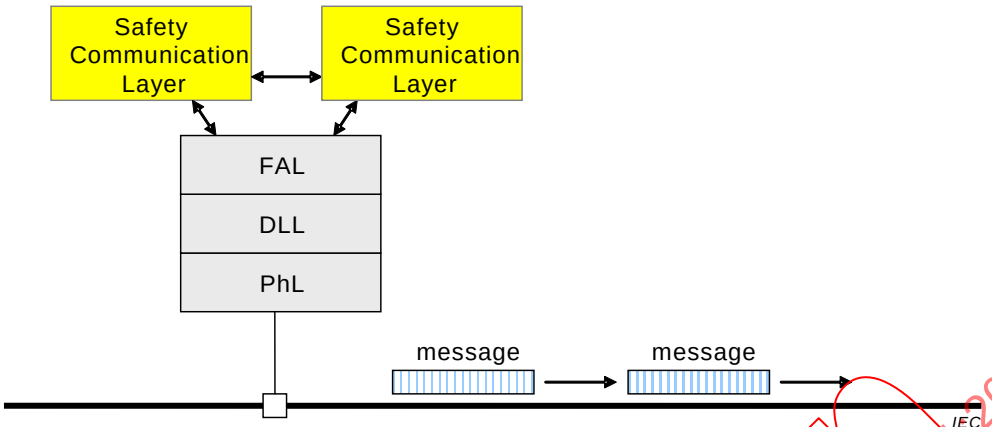


Figure A.4 – Model D

Annex B
(normative)

Safety communication channel model using CRC-based error checking

B.1 Overview

This annex contains a black channel model for data integrity calculations. Use of this model is recommended, unless a different model can be proven more applicable for a particular FSCP.

B.2 Channel model for calculations

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

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

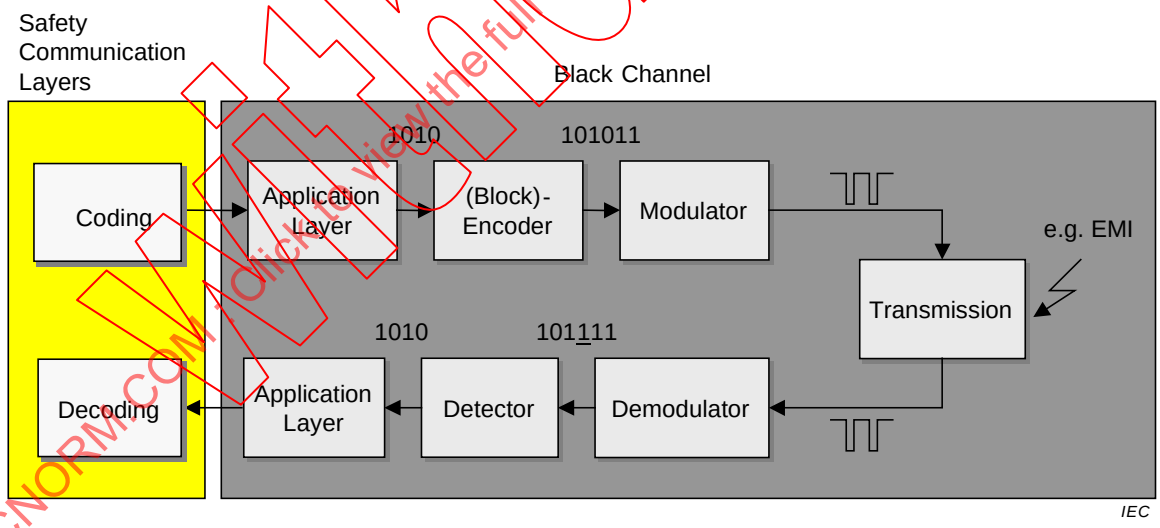


Figure B.1 – Communication channel with perturbation

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

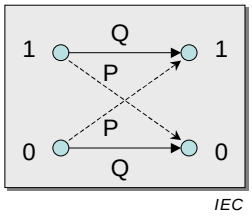


Figure B.2 – Binary symmetric channel (BSC)

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

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

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

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

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

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

B.3 Bit error probability Pe

A Bit Error Probability (Pe) of 10^{-4} in the presence of continuous electromagnetic interference would lead to a stop of communication (nuisance trip) in case of cyclic data exchange (e.g. watchdog time expires after too many retries). Through correct installation (e.g. shielding, equipotential bonding), these nuisance trips normally can be mitigated.

The design of a safety layer assuming a Pe of 10^{-4} is not recommended, as single burst interferences with many corrupted bits are common in industrial environments.

In order to detect these kinds of disturbances, the error detection mechanisms should be powerful enough to achieve the required total Residual Error Probability at a 100 times higher Pe than 10^{-4}, that is 10^{-2}.

Therefore, unless a better (lower) error probability can be proven, a maximum value of 10^{-2} shall be used for the bit error probability.

B.4 Cyclic redundancy checking

B.4.1 General

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

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

where

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

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

P_e is the bit error probability.

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

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

The function (curve) of this approximation Equation (B.4) may deliver smaller (better) residual error probability values than exact calculations (see for example [31]). 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.

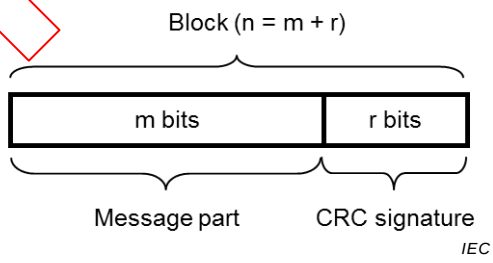


Figure B.3 – Example of a block with a message part and a CRC signature

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

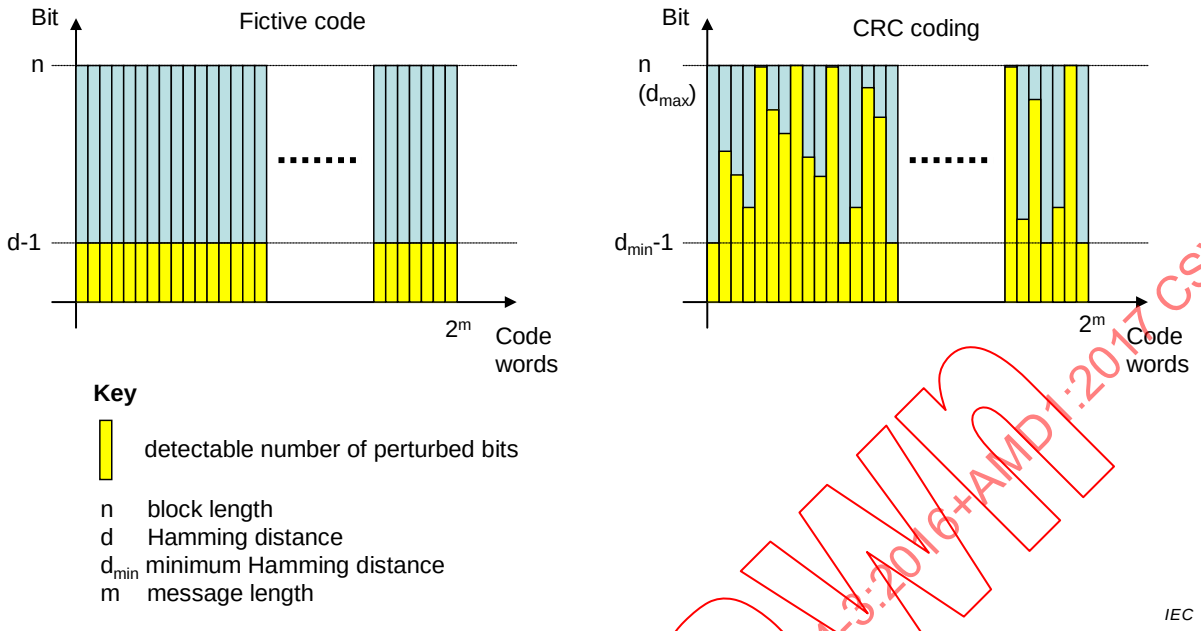


Figure B.4 – Block codes for error detection

Usually the CRC mechanism provides better residual error probability with smaller block bit length n. Thus a dependency exists between block bit 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 bit length n

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

B.4.2 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 [29], [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.

NOTE More information can be found in [32].

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

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

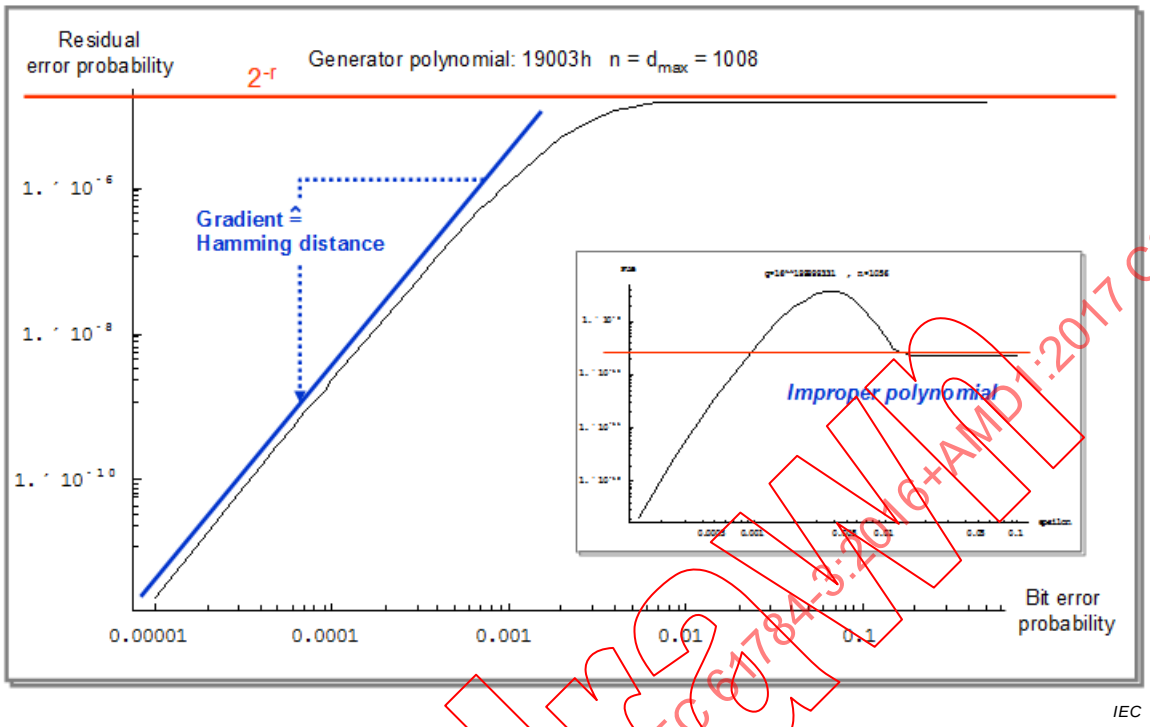


Figure B.5 – Proper and improper CRC polynomials

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

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

Annex C
(informative)

Structure of technology-specific parts

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

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

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

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

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

5.5	Relationships with FAL (and DLL, PhL)	May include existing diagnostics, expected services, constraints (for example, “to be used in conjunction with FSCP x/y”)
5.5.1	Data Types	List of the IEC 61158 data types used by the profile
6	Safety communication layer services	May include application objects used, diagnostic services
7	Safety communication layer protocol	First subclause is listed below, others may be added as needed. May include specific time mechanisms , state machines, sequence charts, reaction on power off/power down, diagnostic protocol and corresponding diagnosis
7.1	Safety PDU format	Includes detailed definition of safety PDU (message) formats. Will include several subclauses to specify the various format elements (for example safety CRC specification)
8	Safety communication layer management	Includes specifications for the following aspects of parameterization: – safe parameter data supplied by another safety device (for example a parameter server) – safe parameter data supplied by a tool (for example device description) (including any required measure to secure the storage, handling and transfer)
9	System requirements	First subclauses are listed below, others may be added as needed
9.1	Indicators and switches	Specifications for device indicators and switch function and behaviour
9.2	Installation guidelines	Detailed clause references within IEC 61918 or other relevant documents
9.3	Safety function response time	Calculations and related examples of reaction times relevant for the technology (for example worst case reaction time of safety loop)
9.4	Duration of demands	Specifications for the duration of demands within devices
9.5	Constraints for calculation of system characteristics	Includes black channel retries, number of telegram per second, number of message sinks
9.6	Maintenance	Specifications for system behaviour in case of device repair and replacement
9.7	Safety manual	If relevant, includes the minimum information required by the profile to be included in the safety manual
9.8	Wireless transmission channels	This subclause is optional. If relevant,it includes specific requirements when using wireless transmission
9.9	Conformance classes	This subclause is optional. If relevant, it includes additional conformance requirements for the base fieldbus protocol
10	Assessment	Include information on assessment requirements
Annex A (informative)	Additional information for functional safety communication profiles of CPF X	Mandatory informative annex used to provide additional non-normative information on the protocol. If there is none, then this will contain the following sentence: “There is no additional information for this FSCP”.

A.1	Hash function calculation	For example algorithms for CRC calculation
	Bibliography	Bibliographic references relevant for this part

Annex D
(informative)

Assessment guideline

D.1 Overview

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

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

The documentation that is provided for the test or assessment shall specify the exact operating conditions according to 5.10.2. No deviation from these conditions is permitted under any circumstances.

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

NOTE IEC TR 62685 is a companion guideline which provides information about additional assessment aspects of safety devices for functional safety communication, such as test beds, proof of increased interference immunity (EMC for functional safety), electrical safety, and other environmental requirements.

D.2 Channel types

D.2.1 General

Clause D.2 defines two general types of safety communication concepts, the black channel and the white channel approach. This guideline covers both safety communication concepts.

D.2.2 Black channel

According to definition 3.1.5, black channel type safety communication requires only evidence of design or validation of the safety communication layer (SCL) according to IEC 61508. It is possible for a safety device designer to use a pre-assessed and approved hardware/software component, which provides the functions of the particular SCL. If the designer implements this component in its specified manner, a safety assessment of the component itself according to IEC 61508 can be omitted. Thus, efforts can be reduced to the assessment of the safety-related technology of the device and the correct implementation of the SCL component.

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

D.2.3 White channel

According to definition 3.1.55, white channel type safety communication requires all relevant hardware and software components to be designed, implemented and validated according to IEC 61508. Due to the large variety of possible solutions this guideline only provides help on how to proceed with the aspects of data integrity assurance.

NOTE Further information can be found in IEC 62280.

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

D.3 Data integrity considerations for white channel approaches

D.3.1 General

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

D.3.2 Models B and C

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

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

NOTE 2 Equations in this Subclause D.3.2 can also be applied to black channel systems.

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

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

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

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

NOTE 3 This equation can only be applied for proper polynomials (see B.4.2), see [31].

An analysis according to D.3.3 together with a calculation using Equation (D.2) is required for a complete evaluation of the residual error probability in case of a white channel solution.

NOTE 4 See IEC 62280 for more information.

The calculation of $\Lambda_{SCL}(P_e)$ is carried out along the lines of 5.8.1 (Equation (1)).

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

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

D.3.3 Models A and D

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

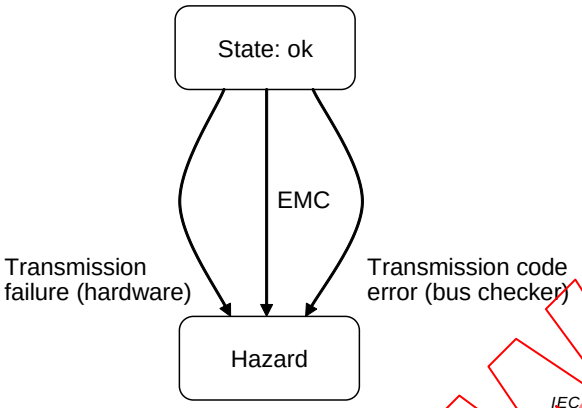


Figure D.1 – Basic Markov model

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

In this case a Markov analysis can be expressed by three fundamental transition possibilities (Figure D.1):

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

NOTE 1 This Markov analysis is derived from IEC 62280.

The residual error probability R_{AD} of the system is the summation of the individual probabilities (Equation (D.2)). The calculation of $\Lambda_{SCL}(p_e)$ is carried out along the lines of 5.8.1 with the residual error probability:

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

where

R_{AD} is the residual error probability of the system for models A and D;

R_{HW} is the residual error probability for faults resulting from hardware failures;

R_{EMC} is the residual error probability for faults resulting from electromagnetic interferences;

R_{TC} is the residual error probability for faults resulting from failures of bus checking mechanisms.

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

NOTE 2 See IEC 62280 for more information.

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

D.4 Verification of safety measures

D.4.1 General

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

D.4.2 Implementation

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

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

D.4.3 "De-energize to trip" principle

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

Assessment: See 5.4.4.

D.4.4 Safe state

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

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

D.4.5 Transmission errors

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

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

D.4.6 Safety reaction and response times

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

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

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

D.4.7 Combination of measures

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

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

D.4.8 Absence of interference

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

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

D.4.9 Additional fault causes (white channel)

In addition to the already described methods for the estimation of residual errors using the BSC model, further fault causes need to be considered and controlled, such as "synchronisation slip errors" within the physical and data link layers.

NOTE Details can be found in IEC 62280 or [28].

Assessment: This assessment is outside the scope of this standard.

D.4.10 Reference test beds and operational conditions

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

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

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

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

D.4.11 Conformance tester

Conformance to a particular FSCP should be tested by a profile conformance tester defined by the technology-specific organization related to the individual FSCP.

NOTE Conformance testing includes both positive and negative tests.

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

Annex E
(informative)

Examples of implicit vs. explicit FSCP safety measures

E.1 General

The examples provided in E.2 to E.7 illustrate the concepts of explicit and implicit safety measures.

E.2 Example fieldbus message with safety PDUs

Figure E.1 shows safety PDUs embedded in a fieldbus message during transmission.

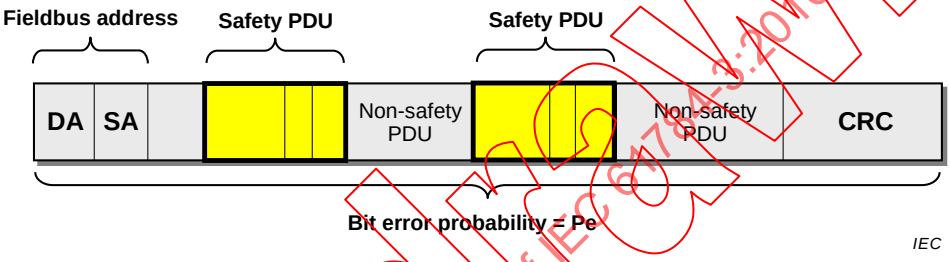


Figure E.1 – Example safety PDUs embedded in a fieldbus message

E.3 Model with completely explicit safety measures

Figure E.2 shows the model and the safety checking of a safety PDU with completely explicit safety measures for timeliness and authenticity.

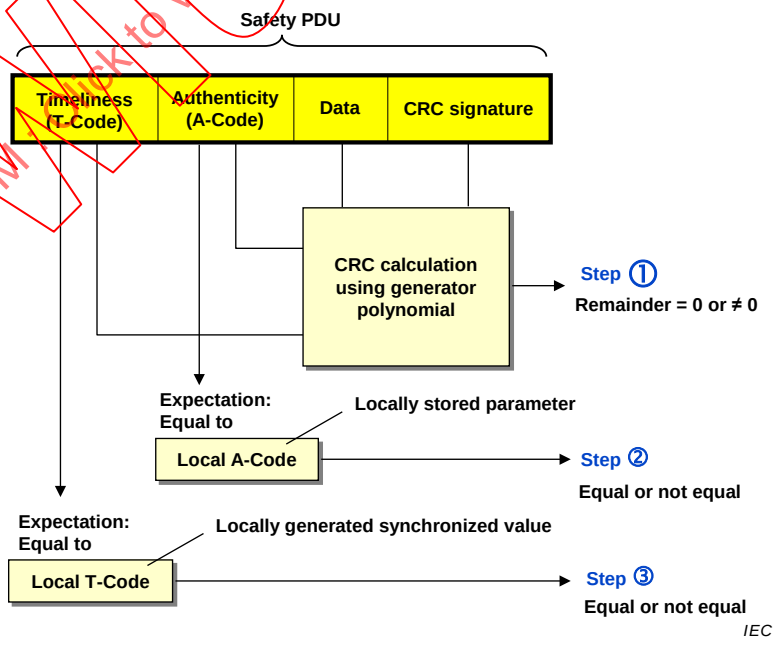


Figure E.2 – Model with completely explicit safety measures

Checking is done according to the following steps:

Step ①	Remainder ≠ 0	→	Any error detected
	Remainder = 0	→	Data correct or incorrect with RR_I according to F.5.2.2
Step ②	Not equal	→	Any error detected
	Equal	→	Authenticity correct or incorrect with RR_A according to F.5.2.3
Step ③	Not equal	→	Any error detected
	Equal	→	Timeliness correct or incorrect with RR_T according to F.5.2.4

E.4 Model with explicit A-code and implicit T-code safety measures

Figure E.3 shows the model and the safety checking of a safety PDU with explicit safety measure for Authenticity and implicit safety measure for Timeliness.

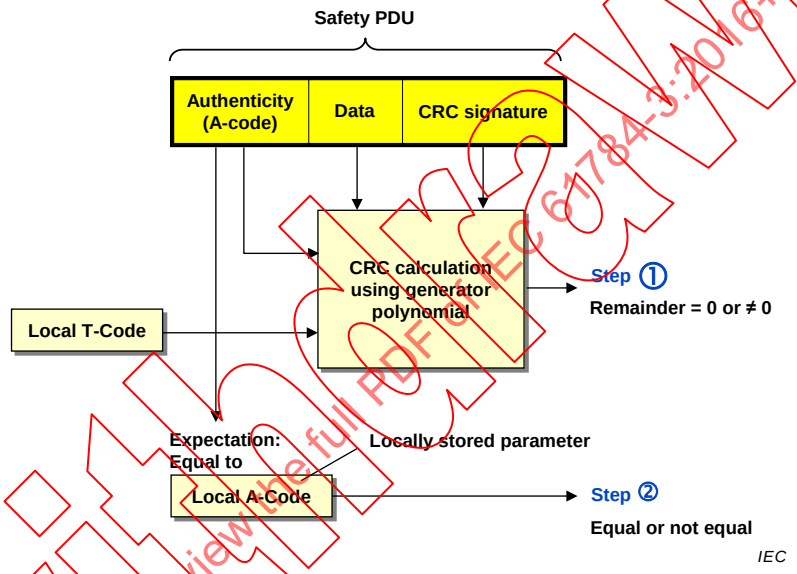


Figure E.3 – Model with explicit A-code and implicit T-code safety measures

Checking is done according to the following steps:

Step ①	Remainder ≠ 0	→	Any error detected
	Remainder = 0	→	Data and Timeliness correct or incorrect with certain RR
Step ②	Not equal	→	Any error detected
	Equal	→	Authenticity correct or incorrect with RR_A according to F.5.2.3

E.5 Model with explicit T-code and implicit A-code safety measures

Figure E.4 shows the model and the safety checking of a safety PDU with explicit safety measure for Timeliness and implicit safety measure for Authenticity.

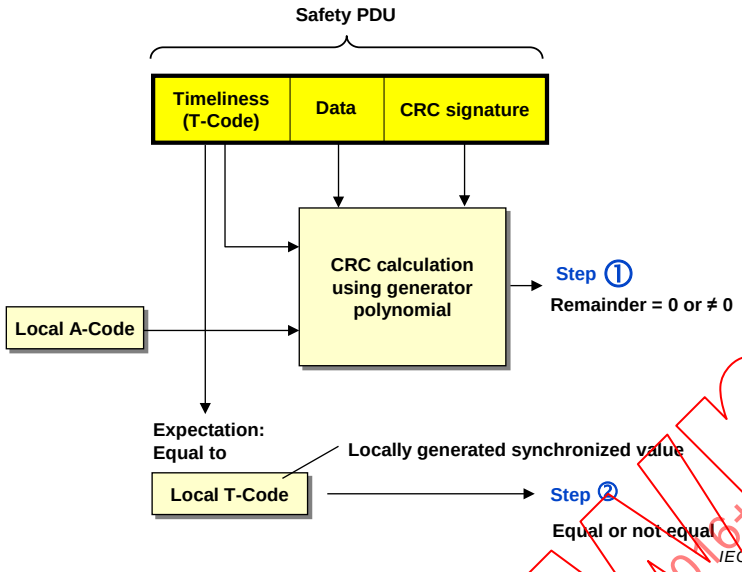


Figure E.4 – Model with explicit T-code and implicit A-code safety measures

Checking is done according to the following steps:

Step ①	Remainder ≠ 0	→	Any error detected
	Remainder = 0	→	Data and Authenticity correct or incorrect with certain RR
Step ②	Not equal	→	Any error detected
	Equal	→	Timeliness correct or incorrect with RR_T according to F.5.2.4

E.6 Model with split explicit and implicit safety measures

Figure E.5 shows the model and the safety checking of a safety PDU with split explicit and implicit safety measures for timeliness and implicit measures for authenticity.

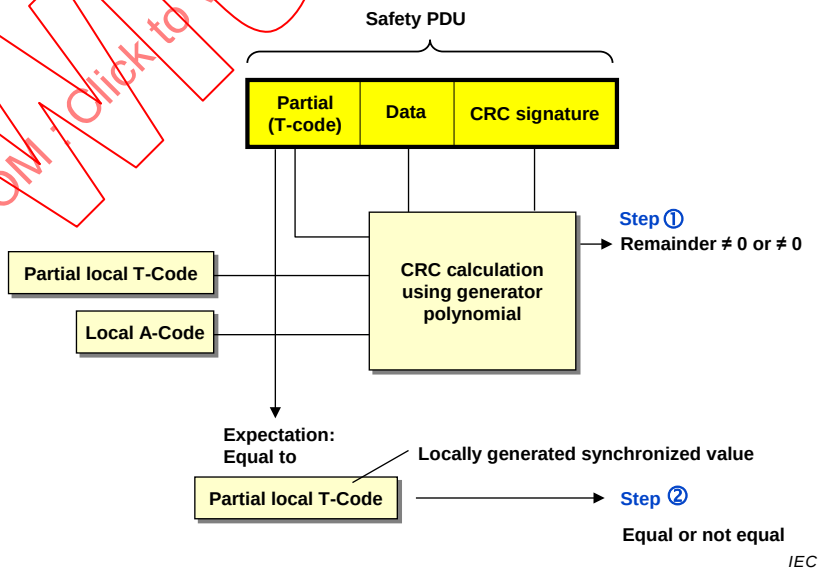


Figure E.5 – Model with split explicit and implicit safety measures

Checking is done according to the following steps:

Step ① Remainder ≠ 0 → Any error detected
Remainder = 0 → Data, Authenticity and Timeliness correct or incorrect with certain RR

Step ② Not equal → Any error detected
Equal → Timeliness correct or incorrect with certain RR

E.7 Model with completely implicit safety measures

Figure E.6 shows the model and the safety checking of a safety PDU with implicit safety measure for both Authenticity and Timeliness.

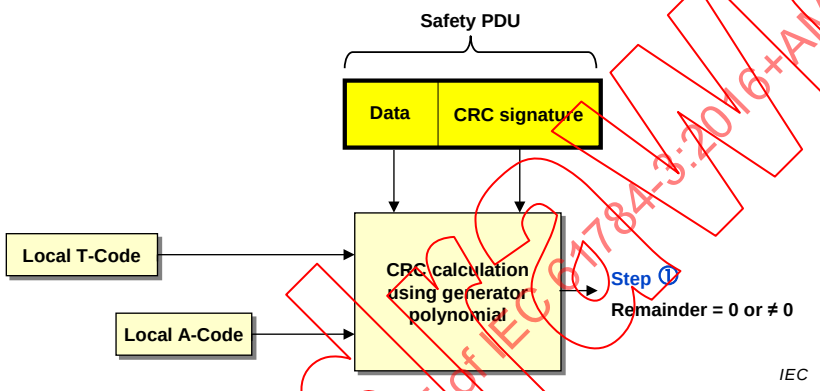


Figure E.6 – Model with completely implicit safety measures

Checking is done according to the following step:

Step ① Remainder ≠ 0 → Any error detected
Remainder = 0 → Data, Authenticity and Timeliness correct or incorrect with certain RR

E.8 Addition to Annex B – impact of implicit codes on properness

The presence of bit errors combined with an erroneous implicit code can influence the properness of the CRC polynomial. As a consequence, the application of implicit codes for safety measures leads to additional effort.

Due to the various possible approaches generic formulae cannot be provided. It is up to the individual FSCP to prove sufficient residual error probabilities.

Annex F
(informative)

Extended models for estimation of the total residual error rate

F.1 Applicability

This Annex F specifies additional extended models for estimating the total residual error rate for an FSCP, for the purpose of assessing this FSCP. These models are intended to replace the models currently specified in 5.8 in the subsequent editions of this standard.

Accordingly, the FSCPs are exempt from a new assessment according to this Annex F until Edition 4, where the contents of current Annex F will replace the current 5.8.

F.2 General models for black channel communications

All FSCPs make a fundamental assumption that all functional safety communications take place through a black channel (see 5.2.3).

To properly quantify the residual error of the safety measures, it is important to first constrain the model for the black channel with respect to the FSCP SCL. This allows the proper definition of the type of messages and the types and rates of errors that the designer of FSCP SCL shall consider with the safety measures.

Figure F.1 shows a black channel that contains different types of communication: Fieldbus messages with safety and non-safety PDUs.

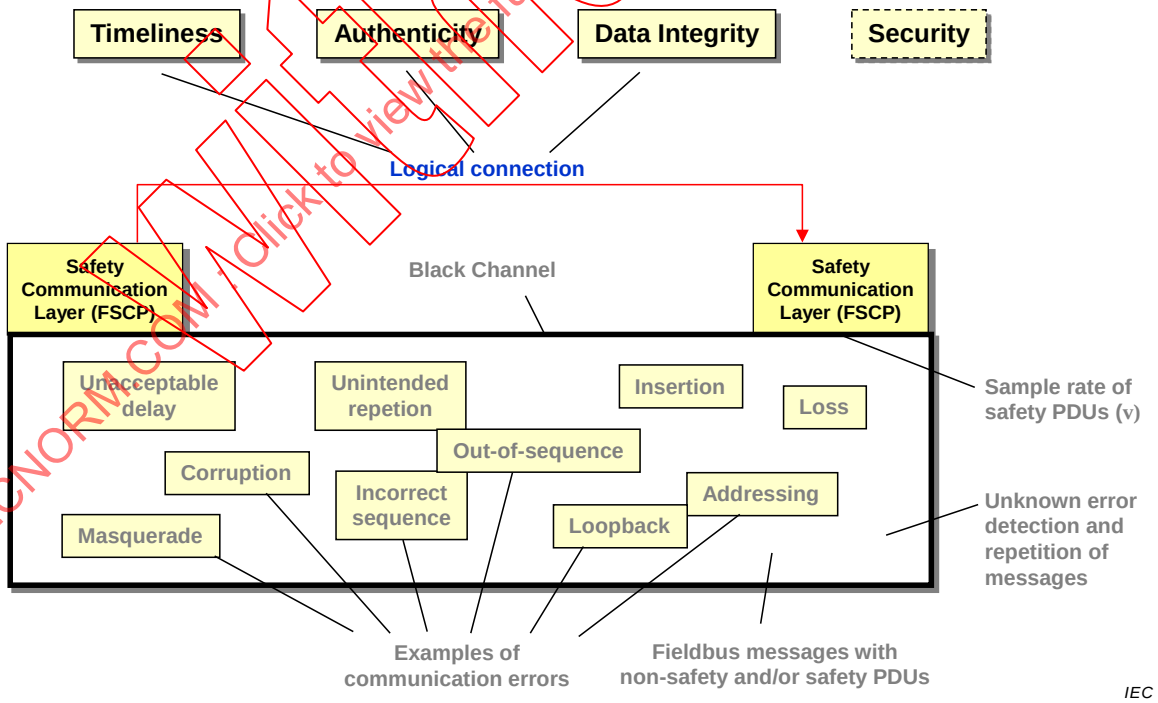


Figure F.1 – Black channel from an FSCP perspective

The black channel includes the underlying fieldbus communication layers below the SCL, as well as any additional communication between the FAL and the SCL within a device.

Errors in the black channel can be generated from several sources:

- bit corruption of messages in the transmission medium; or
- random hardware faults and systematic faults of electronic equipment and software in the black channel.

The frequency of the exchange of messages within the black channel can be different from the frequency at which the SCL is sampling and processing safety PDUs.

F.3 Identification of generic safety properties

Table 1 lists possible discrete safety measures, which alone or in combinations contribute to the following generic safety properties for messages (see Figure F.1):

- data integrity;
- authentication (including masquerade rejection);
- timeliness.

The correct delivery of the content of messages from a message source to the configured message sink(s) is the property of data integrity. The delivery of messages from a correct message source to the configured associated message sink(s) is the property of authentication. The rejection of random bits at a message sink that happen to appear proper is the property of masquerade rejection. Up-to-date delivery of messages between a message source and a message sink within a configured time frame is the property of timeliness.

NOTE Security is an additional known property which is beyond the scope of this standard. Security issues are addressed in IEC 62443.

Another generic safety aspect that shall be considered is the configuration and/or parameterization of the FSCP (see Clause F.12).

A fault in any of these generic safety measures may result in a hazardous state or unintended start-up.

A supplier of an FSCP shall provide proof of a sufficient overall residual error rate taking into account all three generic safety properties as specified in Clause F.10.

F.4 Assumptions for residual error rate calculations

Annex F specifies examples of the types of formulae employed in the calculation of residual error rate, based on assumptions that are taken regarding both black channel and SCL. Alternative formulae shall be employed for cases where these assumptions can be shown not suitable for a given SCL type.

The following general assumptions are valid for all formulae defined in Annex F:

a) assuming a failure rate of an average black channel device to be 100 FIT, it is expected that the SCL shall assume a black channel failure rate 10 000 times this value. Therefore failure rate for electronic equipment is better than 10^{-3}/h (10^{6} FIT) for each active network element or fieldbus part of a safety device;

NOTE 1 Once any device fails, failure could become continuous until it is detected and corrected. This includes permanent, intermittent and transient errors.

NOTE 2 A failure rate less conservative than 10^{-3} can be assumed for an FSCP, if this FSCP drives its safety function to safe state when it detects one or more dangerous black channel failures (see Fault state in Figure 7), if it only returns to operation when it is repaired, and if it can be proven that a failure rate of 10^{-3} would therefore render the safety communication channel inoperable.

b) the presence of store and forward devices is considered, when relevant for the FSCP;

c) safety PDU hash function is different from the one used by the underlying fieldbus DLL (this can be ensured by design or administrative procedures);

d) safety PDU hash function is a CRC which does not include error correction mechanisms;

e) black channel PDU hash function may include error correction mechanisms;

f) each logical connection is assigned a unique authentication code;

g) whenever fixed worst case values are used in the formulae for error or event occurrence probabilities or rates (state of the art), FSCPs may specify instead their own values if sufficient proof is provided;

h) whenever a single mechanism is used to detect multiple types of errors, then these error types shall be considered both individually and in combination when calculating the residual error probability.

F.5 Residual error rates

F.5.1 Explicit and implicit mechanisms

The explicit mechanism includes data corresponding to FSCP safety measures such as sequence number, time stamp and connection authentication in the safety PDU.

The implicit mechanism does not actually transmit all data corresponding to safety measures, but uses them to calculate the overall CRC signature, based on the assumption that the receiver has equivalent knowledge.

NOTE Implicit mechanism is typically used to accommodate limited systems with fixed black channel message sizes or slow transmission rates.

The FSCPs specified in the IEC 61784-3 series can be classified into explicit, implicit and partly explicit/implicit categories (see examples in Annex E). Due to the various possible approaches generic formulae cannot be provided for the implicit category. It is up to the individual FSCP to prove sufficient residual error probabilities. Therefore, this Annex F only deals with the explicit category.

F.5.2 Residual error rate calculations

F.5.2.1 General

Subclauses F.5.2.4 to F.5.2.5 show example equations for the calculation of residual error rates for the explicit FSCP category depending on the lengths of sequence numbers, time stamps and connection authentication data. Specific FSCPs may provide their own equations as applicable.

An SCL may restrict certain fields to only certain values. This is represented by the uniqueness coefficient of limited fields (RP_U) which is included in the residual error rate calculations where appropriate. It is given by Equation (F.1).

$$RP_U = \frac{V_{A1}}{V_{R1}} \times \frac{V_{A2}}{V_{R2}} \times \ldots \times \frac{V_{AN}}{V_{RN}} \qquad \text{(F.1)}$$

where

RP_U is the residual error probability for other fields of uniqueness that distinguish a properly formatted safety PDU;

V_{AN} is the number of values accepted by a sink in data field N;

V_{RN} is the number of values representing the total range for data field N.

F.5.2.2 Contribution of data integrity errors (RR_I)

An example for the calculation of the residual error rate for Data Integrity RR_I is shown in Equation (F.2).

$$RR_I = RP_I \times v \times RP_U \times RP_{FSCP} \quad (F.2)$$

where

RR_I is the residual error rate for Data Integrity;

RP_I is the residual error probability for Data Integrity;

v is the maximum number of SPDU samples by the SCL ("sample rate") per hour;

RP_U is the residual error probability for other fields of uniqueness that distinguish a properly formatted safety PDU;

RP_{FSCP} is the residual error probability for other measures unique to the FSCP.

F.5.2.3 Contribution of authenticity errors (RR_A)

There are three factors for this residual rate:

a) a misdirected PDU;

b) an undetected data corruption error, and;

c) the error must result in a match of the authentication code.

An example for the calculation of the residual error rate for Authenticity RR_A is shown in Equation (F.3).

$$RR_A = RP_I \times 2^{-LA} \times R_A \times RP_{FSCP} \quad (F.3)$$

where

RR_A is the residual error rate for Authenticity regarding misdirected safety PDUs;

RP_I is the residual error probability for Data Integrity;

LA is the bit length of the connection authentication;

R_A is the rate of occurrence for misdirected safety PDUs;

RP_{FSCP} is the residual error probability for other measures unique to the FSCP.

NOTE The use of 2^{-LA} assumes uniform distribution of error patterns in the A-code.

F.5.2.4 Contribution of timeliness errors (RR_T)

An example for the calculation of the residual error rate for Timeliness RR_T is shown in Equation (F.4).

$$RR_T = 2^{-LT} \times w \times R_T \times RP_{FSCP} \quad (F.4)$$

where

RR_T is the residual error rate for Timeliness;

LT is the bit length of the sequence number;

w is the range of values (window) of accepted time stamps or sequence numbers for receiving safety PDUs;

R_T is the rate of occurrence for incorrect sequence safety PDUs (value cannot exceed v, as specified in F.5.2.2);

RP_{FSCP} is the residual error probability for other measures unique to the FSCP.

F.5.2.5 Contribution of masquerade errors (RR_M)

An example for the calculation of the residual error rate for Masquerade RR_M is shown in Equation (F.5).

$$RR_M = 2^{-LA} \times 2^{-LT} \times w \times 2^{-r} \times RP_U \times 2^{-LR} \times R_m \quad (F.5)$$

where

RR_M is the residual error rate for Masquerade;

LA is the bit length of the connection authentication;

LT is the bit length of the sequence number;

w is the range of values (window) of accepted time stamps or sequence numbers for receiving safety PDUs;

r is the bit length of the CRC signature (in case two CRCs with independent polynomials are used, r is the sum of the two corresponding bit lengths);

RP_U is the residual error probability for other fields of uniqueness that distinguish a properly formatted safety PDU;

LR is the bit length of the repeated portion of the safety PDU (for redundancy with cross-checking, otherwise LR = 0);

R_m is the rate of occurrence for masqueraded safety PDUs.

F.6 Data integrity

F.6.1 Probabilistic considerations

The generic safety property data integrity requires the detection of the following communication error according to Table 1:

- corruption (see 5.3.2).

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 and/or data repetition, and similar forms of redundancy shall be applied.

If the residual error probability of the data integrity measures is dependent on the safety data values, then the worst case values shall be considered.

When using cyclic redundancy check (CRC) as hash function, the designer of an FSCP shall prevent or consider the possibility of the "black channel" using the same polynomial. This can be achieved using various methodologies.

EXAMPLES

Possible methodologies include:

– measures allowing only specific combinations of FSCP and CPs;

– appropriate measures in the design of the SCL;

– calculations of the residual error rate using 0,5 as value for Pe.

F.6.2 Deterministic considerations

In addition to random bit patterns, the following specific error patterns shall be evaluated: completely inverted data, completely "0" or "1" data sets, synchronisation slip errors and burst errors.

F.7 Authenticity

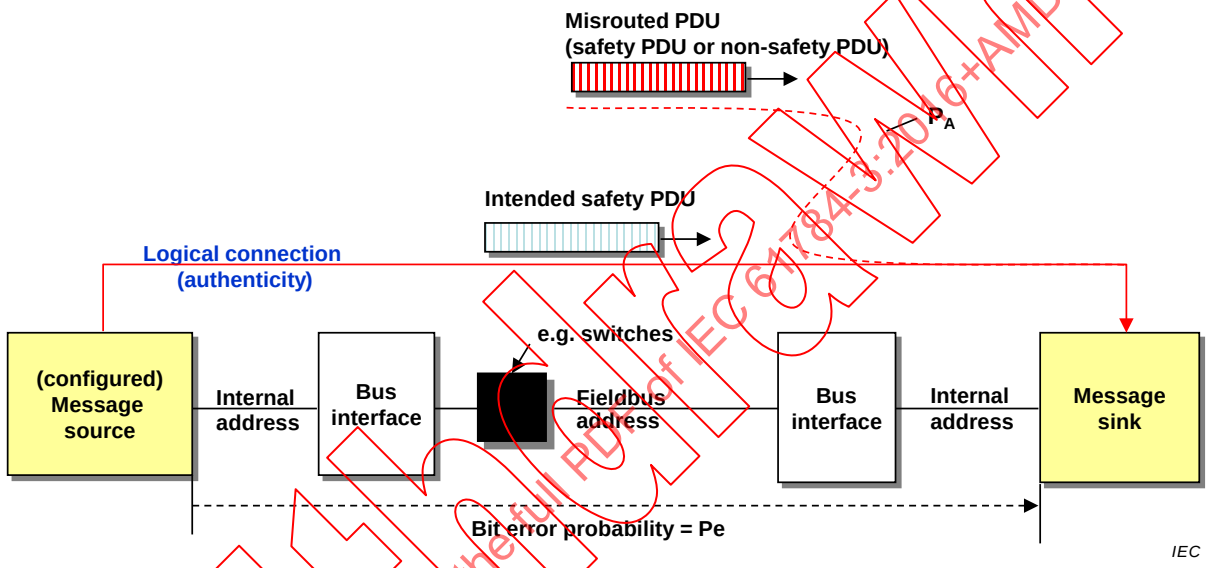
F.7.1 General

The generic safety property authenticity requires the detection of the following communication errors according to Table 1:

- addressing (see 5.3.9);
- insertion (see 5.3.7).

The FSCP shall meet the following requirement (see Figure F.2):

- the message sink shall only process safety data in correctly addressed messages received from an authenticated message source.



Key

PA Probability of an authenticity error for logical connections

Figure F.2 – Model for authentication considerations

These requirements shall be met during all communication phases in 5.6 for which connection authentication is relevant (FSCP dependant). Exclusions shall be documented in the safety manual.

Authentication prevents the processing of safety data in a received message that passes all other checks but is not a valid message for this receiver.

NOTE

Possible stochastic causes for incorrect authenticity include but are not limited to:

– Falsification of an address within the message or an error within an internal communication link (see Figure F.3) regardless whether it is related to a non-safety or safety address mechanism.

– Disturbed or erroneously operating protocol stacks/layers within the black channel.

– Disturbed or erroneously operating routing devices, for example switches or routers.

– Disturbed or erroneously operating gateways, for example bus couplers.

– Disturbed or erroneously operating black channel devices mirroring messages (“loopback error”) or redirect messages by other means.

– The authentication mechanism within the message sink is not sufficient to differentiate between messages from different message sources.

Figure F.3 shows possible addressing errors due to corrupted addresses within the fieldbus communication system or possible internal addressing errors (for example due to corrupted pointers within modular remote I/O devices).

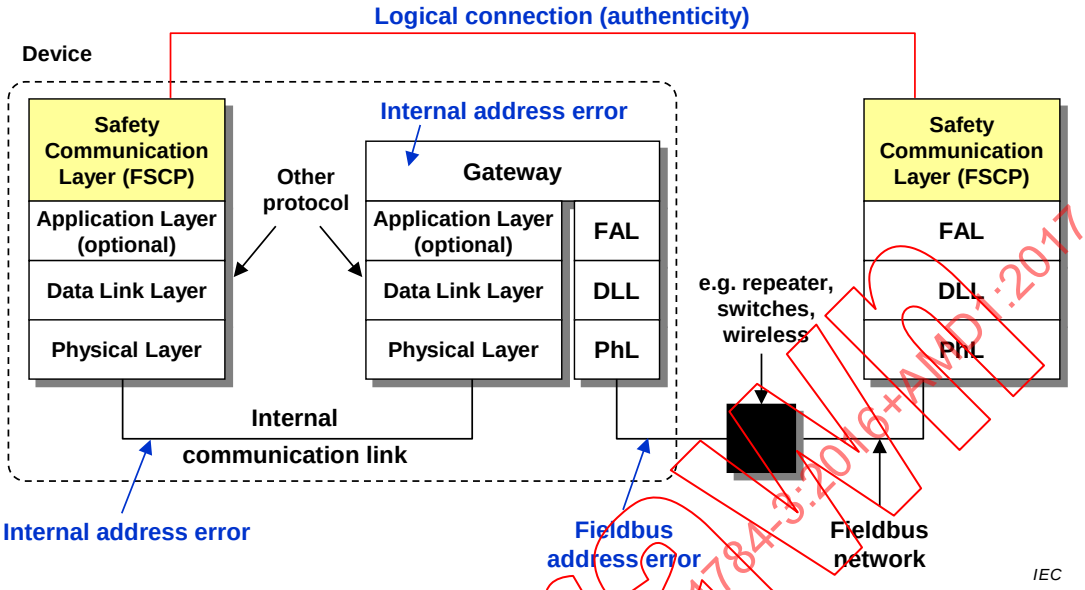


Figure F.3 – Fieldbus and internal address errors

Additional systematic causes for incorrect authenticity may be identified within configuration and parameterization procedures as shown in F.12. Additional organizational measures may be required to control these systematic error causes.

A connection authentication can be used to uniquely and unambiguously identify one of the following:

- a single message source or message sink;
- a single connection between a message source and a message sink;
- a multiple connection between a message source and multiple message sinks in case of multicast;
- a group connection between multiple message sources and sinks.

Several methods are available to avoid authentication errors.

EXAMPLES

– A unique connection authentication (e.g. “connection ID") that is transmitted with each and every FSCP message.

– A locally stored unique connection authentication (e.g. "connection ID") that is encrypted via hash functions such as CRC signatures and transmitted to the message sink. This encryption is usually part of the overall data integrity measures of FSCPs according to 5.9.

F.7.2 Residual error rate for authenticity (RR_A)

The residual error rate RR_A for the generic safety property authenticity shall be calculated from a message sink perspective as shown in Figure F.2.

In accordance with Clause F.4 bullet a), a value of 10^{-3}/h per device shall be assumed for the rate of occurrence for misdirected safety PDUs (R_A), unless otherwise specified.

It is further assumed that R_A shall have the value of v (SPDU sample rate) after the first occurrence of a misdirected safety PDU, until the system is repaired.

The residual error rate RR_A shall be sufficient for all communication phases in 5.6 for which connection authentication is relevant (FSCP dependant).

The technical measures for the authentication can be supplemented by organizational measures, which shall be practical for the user to perform (see Clause F.12).

F.8 Timeliness

F.8.1 General

The generic safety property timeliness requires the detection of the following communication errors according to Table 1:

- unacceptable delay (see 5.3.6);
- unintended repetition (see 5.3.3);
- incorrect sequence (see 5.3.4);
- loss (see 5.3.5).

The FSCP shall meet the following requirements:

- the message sink processes up-to-date messages;
- the message sink monitors the operational status of the safety layer of the message source.

NOTE 1 Depending on unidirectional or bidirectional communication, a device can provide a message source and a message sink at the same time.

The technical measures for timeliness can be supplemented by organizational measures.

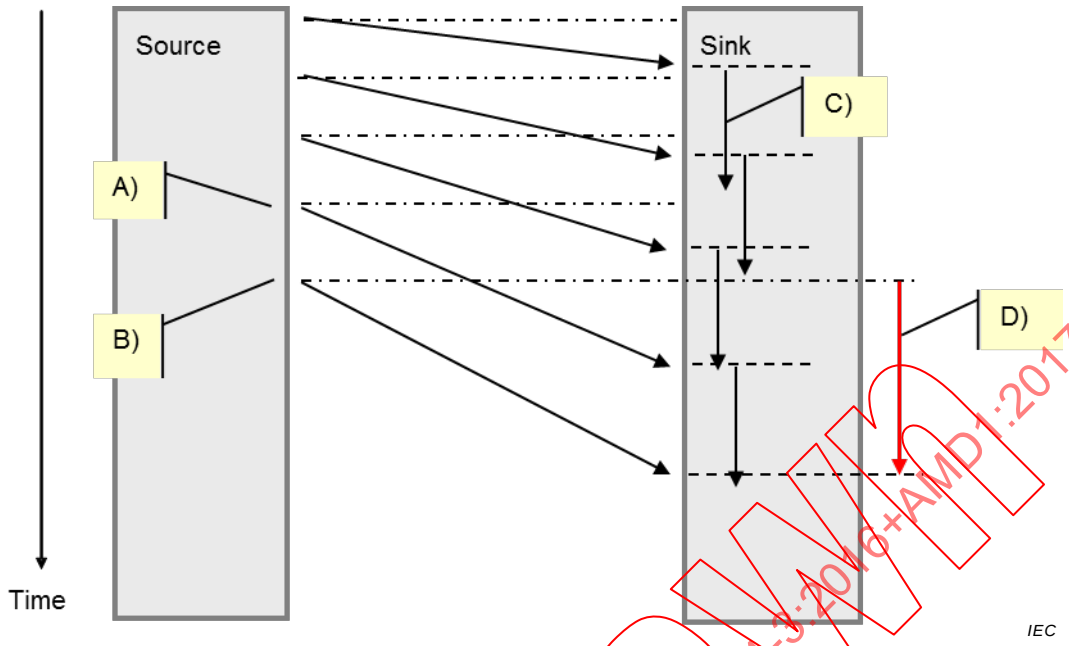
Typical causes for non-timely communication which shall be considered during the design of the FSCP are variable performances of the black channel.

EXAMPLES

Variations in black channel performance can result from:

– insufficient throughput (e.g. bandwidth, traffic);
– loss of communication (temporary or total);
– varying latency;
– slowly increasing latency (see Figure F.4);
– different latency for each message source / sink pair;
– variations in synchronization clock times at message source or message sink; or
– any combination of these.

Figure F.4 shows an example of a slowly increasing message latency of the black channel.



Key

A) Message departure times do not correlate with the message reception times

B) Message departure time is earlier than message reception time of the previous message

C) Timeout check in sink

D) A message sink cannot determine the message departure times out of the message reception times and the intervals. The message delay can be larger than the timeout without being detected!

Figure F.4 – Example of slowly increasing message latency

Another issue that shall be considered is the unintended transmission from memory of messages or parts of messages.

EXAMPLES

– Active network elements such as switches, routers (see Figure 5).

– Communication devices outside the defined communication system (e.g. the Internet or introduced via wireless communication links).

– Multi-path communication (e.g. the Internet).

Figure F.5 shows an example of unintended transmission from memory due to an active network element failing as follows: "queue-jumping" in a revolving memory where the send pointer passes the receive pointer, which will cause emptying/sending of the whole queue of a switch.

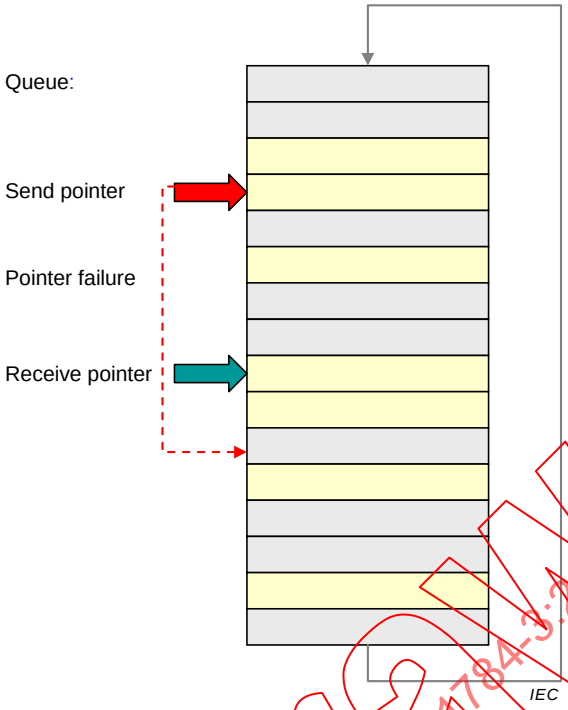


Figure F.5 – Example of an active network element failure

NOTE 2 Black channel can include other types of storage elements than switches.

Several methods are available to detect errors from unintended transmission from memory.

EXAMPLES

– Cyclic communication with monitoring of latencies.
– Synchronized clocks in all devices and time stamping of SPDUs.
– Sufficiently ranged sequence numbering of SPDUs.

In each case, time precision and ranges shall meet the requirements arising from:

- the intended safety application timing issues;
- potential storage of messages inside or outside the system.

The error rate for time bases exceeding specified safety limits shall be determined during the design and implementation assessments according to IEC 61508.

NOTE 3 Use of a synchronized time base throughout the safety network is part of implementation aspects.

F.8.2 Residual error rate for timeliness (RR_T)

In a safety-related network with message storing elements (see Figure F.5), in accordance with Clause F.4 bullet a), a value of 10^{-3}/h per storing element shall be assumed for the rate of timeliness errors (R_T), unless otherwise specified.

The series of unintended transmission from memory of SPDUs shall be assumed to be not more than 65 000.

F.9 Masquerade

F.9.1 General

The safety property masquerade rejection requires the detection of the following communication error according to Table 1:

- masquerade (see 5.3.8).

In general, non-safety PDUs (masquerade) are more likely to be detected by the SCL since they have to fulfill all the preconditions (Timeliness, Authenticity, and Data Integrity).

F.9.2 Other terms used to calculate residual error rate for masquerade rejection (RR_M)

In accordance with Clause F.4 bullet a), a value of 10^{-3}/h per device shall be assumed for the rate of occurrence for masqueraded safety PDUs (R_m), unless otherwise specified.

F.10 Calculation of the total residual error rates

F.10.1 Based on the summation of the residual error rates

The total residual error rate λ_{SC} for the safety communication channel is the sum of the individual residual error rates RR_T, RR_A, RR_I and RR_M as shown in Equation (F.6).

$$\lambda_{SC} = RR_T + RR_A + RR_I + RR_M \qquad \text{(F.6)}$$

where

λ_{SC} is the total residual error rate per hour for the safety communication channel;

RR_T is the residual error rate per hour for Timeliness (see F.5.2.4);

RR_A is the residual error rate per hour for Authenticity (see F.5.2.3);

RR_I is the residual error rate per hour for Data Integrity (see F.5.2.2);

RR_M is the residual error rate per hour for Masquerade (see F.5.2.5).

The residual error rate of the SCL is calculated from the total residual error rate λ_{SC} of the safety communication channels and the maximum number of logical connections (m) that is permitted in a single safety function as shown in Equation (F.7) and in Figure F.6 and Figure F.7.

$$\lambda_{SCL} = \lambda_{SC} \times m \qquad \text{(F.7)}$$

where

λ_{SCL} is the residual error rate per hour of the SCL;

λ_{SC} is the residual error rate per hour per logical connection (see Equation (F.6));

m is the maximum number of logical connections (m) that is permitted in a single safety function.

NOTE This equation assumes cyclic sampling of SPDUs and assumes the worst case that each safety PDU passed over from the black channel can be erroneous.

The number m of logical connections depends on the individual safety function application. Figure F.6 and Figure F.7 illustrate how this number can be determined.

The figures show the physical connections with possible network components such as repeaters, switches, or wireless links and the logical connections between the subsystems involved in the safety function.

The logical connections can be based on single cast or multicast communications.

Figure F.6 shows an example 1 of an application where m = 4. In this application, all three drives are considered to be hazardous at a single point in time according to the risk analysis.

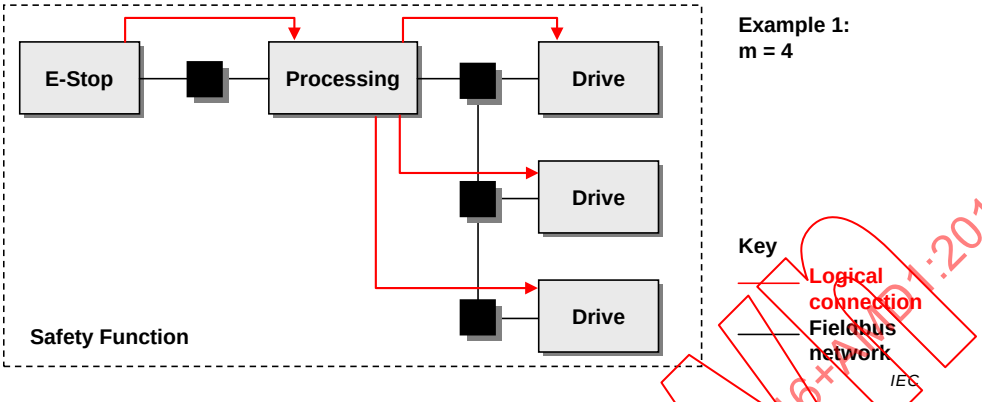


Figure F.6 – Example application 1 (m = 4)

Figure F.7 shows an example 2 of an application where m = 2. In this application, only one of the drives is considered to be hazardous at a single point in time according to the risk analysis.

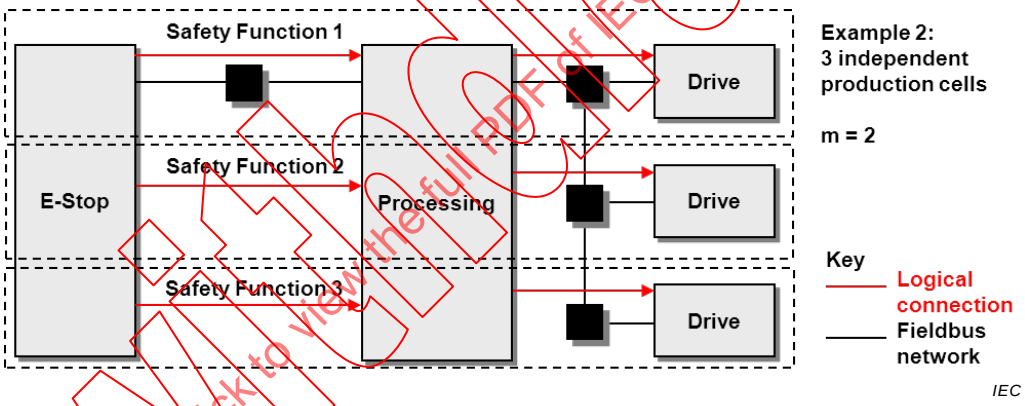


Figure F.7 – Example application 2 (m = 2)

F.10.2 Based on other quantitative proofs

The summation of the residual error rates of the generic safety properties as shown in F.10.1 is an acceptable method to calculate the total residual error rate for a given FSCP.

It is possible to use combined mathematical methods for the calculations taking into account cross effects of the individual safety measures and thus achieve better residual error rates.

It is also possible to use directly the methods of the IEC 61508 and to determine the Safe Failure Fraction and the Diagnostic Coverage of the FSCP.

F.11 Total residual error rate and SIL

A functional safety communication system shall provide a residual error rate in accordance with this standard. Table F.1 and Table F.2 show the typical relationships between residual error rate and SIL, based on the assumption that the functional safety communication system contributes no more than 1 % per logical connection of the safety function.

Both low demand and high demand mode systems shall have a defined safety function response time, so a necessary rate of SPDUs shall be guaranteed. The PFH for a certain SIL shall be provided in all cases, while the PFD_{avg} is optional.

Table F.1 – Typical relationship of residual error rate to SIL

Applicable for safety functions up to SIL	Average frequency of a dangerous failure for the safety function (PFH)	Maximum permissible residual error rate for one logical connection of the safety function (λ_{SC} (Pe))
4	$< 10^{-8}$/ h	$< 10^{-10}$ / h
3	$< 10^{-7}$ / h	$< 10^{-9}$ / h
2	$< 10^{-6}$ / h	$< 10^{-8}$ / h
1	$< 10^{-5}$ / h	$< 10^{-7}$ / h

Table F.2 – Typical relationship of residual error on demand to SIL

Applicable for safety functions up to SIL	Average probability of a dangerous failure on demand for the safety function (PFDavg)	Maximum permissible residual error probability for one logical connection of the safety function
4	$< 10^{-4}$	$< 10^{-6}$
3	$< 10^{-3}$	$< 10^{-5}$
2	$< 10^{-2}$	$< 10^{-4}$
1	$< 10^{-1}$	$< 10^{-3}$

F.12 Configuration and parameterization for an FSCP

F.12.1 General

Correct configuration and parameterization of the safety devices and their SCL during the different phases is essential for functional safety. The engineering of safety functions using an FSCP usually comprises configuration, parameterization, and programming activities as shown in the example of Figure F.8.

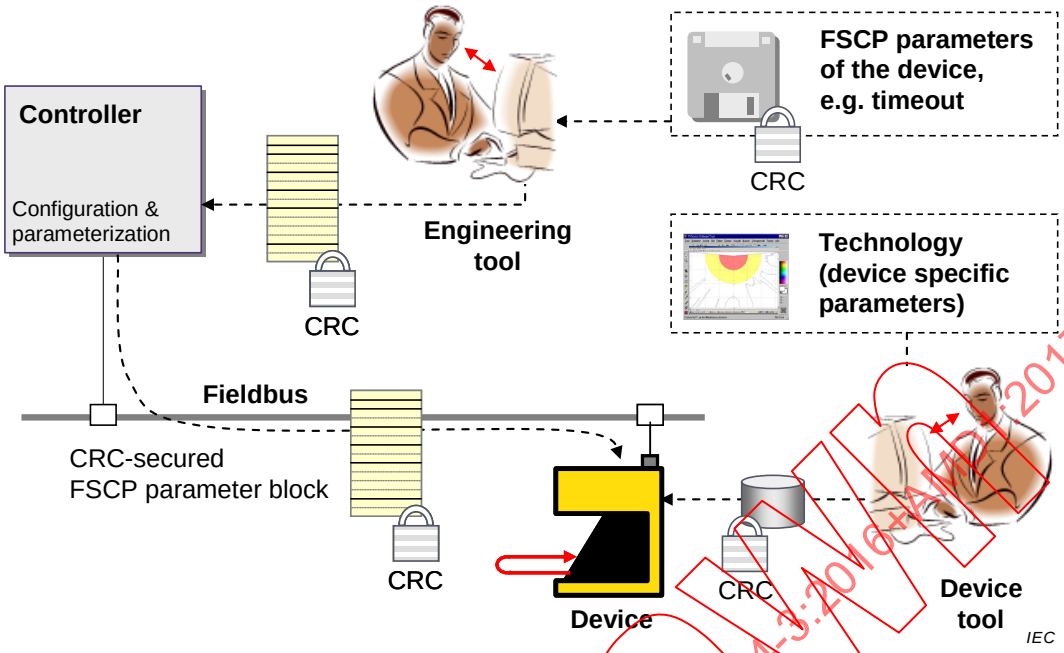


Figure F.8 – Example of configuration and parameterization procedures for FSCP

Configuration requires an engineering tool to set-up the fieldbus network structure, to connect the field devices and to assign values to the black channel layer parameters as well as to the FSCP parameters such as connection authentication, timeout, SIL claim, etc. Usually, the field devices provide a data sheet in electronic form stored within a file that can be imported into the engineering tool.

After a configuration session, the configuration data including parameter values are downloaded to the fieldbus controller to set-up communication. The field device related part of the configuration and parameter data is downloaded to the particular field device prior to cyclic process data exchange.

More complex safety devices may require a dedicated tool for the configuration or parameterization of the technology specific safety device application.

NOTE 1 Relevant information can be found in IEC 62061:2005, 6.11.2.3 and ISO 13849-1:2015, 4.6.4.

NOTE 2 Aspects of incorrect configuration and parameterization include but are not limited to:

– human errors resulting in the entry of incorrect initialization and parameter values;
– data corruption during storage;
– incorrect addressing during download;
– data corruption during download;
– inconsistent update of safety devices;
– connection of identical "safety islands" (serial machines);
– systematic errors while working with engineering tools due to specific computer settings (for example differences between displayed and stored values);
– unrecognized changes within the technology specific safety parameters of the safety device be it stochastic or intentional;
– use of safety devices previously installed in other safety functions.

An FSCP shall specify methods to protect against stochastic errors in the safety configuration and parameters.

EXAMPLES

– Incorrect addressing.

– Data corruption.

– Unrecognized changes.

The above requirements shall be considered by the designer of the FSCP for all relevant communication phases (see 5.6).

Several methods are available to avoid incorrect configuration and parameterization.

EXAMPLES

– CRC signatures across configuration and parameter data.

– Correlation between safety technology parameters and FSCP parameters.

Stochastic configuration and parameterization errors during operation can be prevented by the generic safety measures.

Systematic configuration and parameterization errors can only be safely prevented by verification and validation. The safety manuals shall provide the necessary instructions.

NOTE 3 Relevant information can be found in IEC 62061:2005, 6.11.2.3 and ISO 13849-1:2015, 4.6.4.

F.12.2 Configuration and parameterization change rate

Unless otherwise specified, the configuration and parameterization change rate for calculations shall be assumed as 1 per day.

F.12.3 Residual error rate for configuration and parameterization

The residual error rate RR_{CP} for the stochastic configuration and parameterization errors during onetime operations such as download can be calculated using the residual error probability of the chosen CRC signature (see B.4.2) multiplied by the change rate from F.12.2.

Annex G
(informative)

Implicit data safety mechanisms for IEC 61784-3 functional safety communication profiles (FSCPs)

G.1 Overview

Annex G discusses the concepts of implicit data safety mechanisms for use in functional safety communications protocols (FSCPs) as specified in this standard. Implicit data is that which is not explicitly transmitted in a PDU. Instead, the implicit data values are known by both the sender (source) and the receiver (sink). Implicit data values are validated by the value of one or more transmitted frame check sequence(s) (FCS) which are calculated using an overall data string comprised of the implicit data string appended with the explicit data string. Because the implicit data is not transmitted, the load on the transmission media is reduced.

Today, the FSCPs that use implicit data mechanisms do so in order to communicate complete or partial timeliness codes (T-codes) and/or authenticity codes (A-codes), see Annex E. These FSCPs also use cyclic redundancy check (CRC) algorithms for the frame check sequence (FCS) exclusively. Therefore, Annex G is limited to the analysis of implicitly transmitted T-codes and A-codes using CRC-algorithms.

According to Clause E.8, with regard to implicit data, "Due to the various possible approaches generic formulae cannot be provided. It is up to the individual FSCP to prove sufficient residual error probabilities." In the hope of advancing IEC 61784-3 for the next edition and beyond, the subject of this new Annex G is to improve the understanding of formulating models for the residual error probabilities of FSCPs using CRC-algorithms to implicitly transmit T-codes and A-codes when a single FCS code is used by the protocol.

Presented in Annex G are two formulae examples, applicable for two special cases, and from which a better understanding is promoted for the development of additional (specific and general) formulae.

Also presented is a summation method generally applicable when conditional weight distributions for implicit data error patterns are known and can be quantified in a way either leading to a closed-form solution, or suitable for iterative summation with a reasonably bounded execution time.

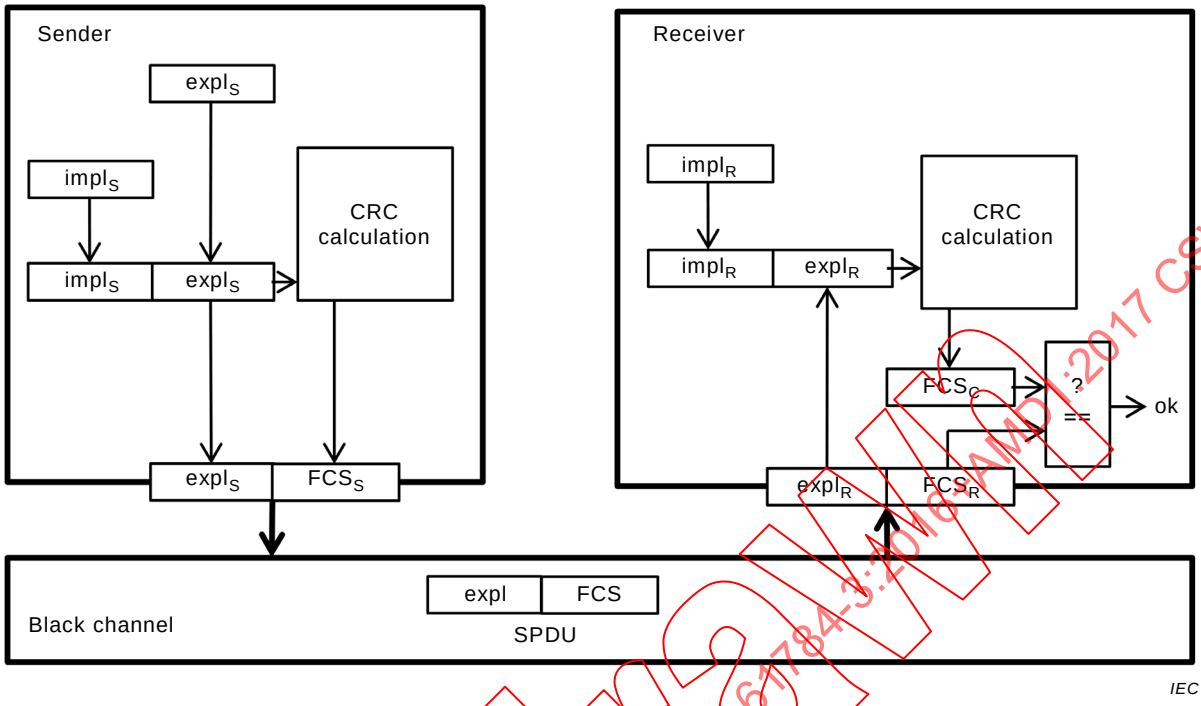
G.2 Basic principles

Calculations in Annex G also use the binary symmetric channel (BSC) model as specified in Annex B.

NOTE 1 Although it does not take into account burst errors, the BSC model with a sufficiently conservative bit error probability is so far the most practical known for use in probability calculations needed for the determination of the FSCP residual error rate.

Figure G.1 shows the basic principle of an FSCP using single FCS protection mechanisms involving implicit data. In the sender, a CRC-checksum over the implicit data $impl_S$ concatenated with the explicit data $expl_S$ is generated, resulting in a frame check sequence FCS_S. When multiple FCS codes are used in an FCSP format, the calculation shall be done for each FCS code. While $expl_S$ and FCS_S are explicitly transmitted over the black channel, $impl_S$ is not transmitted, but impacts the value of the FCS_S. Therefore, it can only contain data whose value is already known to the receiver. Implicit data is used to detect e.g. SPDUs which were misdirected in either space (“authentication error”) or time (“timeliness error”). This is accomplished by deriving the implicit data from the A-code (e.g. connection identifier) and/or the T-code (e.g. sequence number) of an SPDU.

NOTE 2 Initialization details are addressed in F.12.1.



Key Symbols are specified in 3.2.2

Figure G.1 – FSCP with implicit transmission of authenticity and/or timeliness codes

When the SPDU comprising expl and FCS is delivered to the FSCP-layer in the receiver, it may contain transmission errors, i.e. the value delivered may differ from the value sent. For discrimination, the symbols expl$_R$ and FCS$_R$ are used in the receiver.

The expected value of the implicit data is called impl$_R$. In the error free case, this expectation is identical to impl$_S$. In case of, for example, a misdirected SPDU, impl$_R$ and impl$_S$ may differ.

The receiver generates one or more frame check sequence(s) FCS$_C$ by building a CRC-checksum over the concatenation of impl$_R$ and expl$_R$. When each FCS$_C$ is identical to its corresponding FCS$_R$, it is assumed that no error occurred. Otherwise an error has been detected.

The lengths of the bitstrings for a single FCS are defined as follows:

r length of FCS (degree of generator-polynomial);

i length of implicit data (it is assumed that i ≥ r);

e length of explicit data;

n length of SPDU, with n = e + r.

G.3 Problem statement: constant values for implicit data

In FSCPs using implicit data, the CRC-check in the receiver is used for both the detection of data integrity errors as well as the detection of mis-directed or mis-timed SPDUs. Therefore, it may happen that the CRC-mechanism becomes “overburdened” by multiple simultaneous errors, resulting in an increase of the overall residual error probability. This is exemplified in the following scenario in Figure G.2.

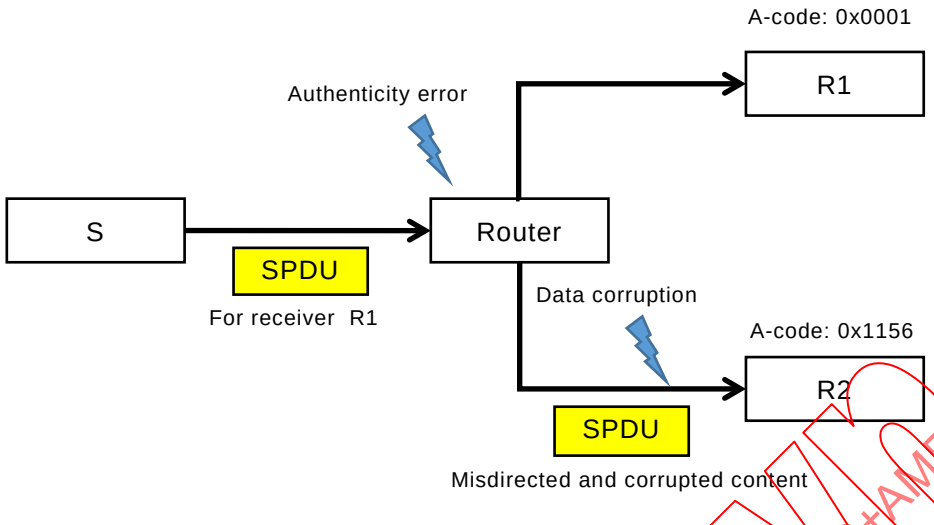


Figure G.2 – Example of an incorrect transmission with multiple error causes

The scenario assumes a sender S sending SPDUs to receiver R1 and receiver R2, using a black channel containing a router. The implicit data used comprises a single field containing an authenticity-code (A-code) of length 16 bits, identifying the receiver (see Figure E.4). For each SPDU sent from S to R1, the A-code of R1 is used as implicit data, and similarly the A-code of R2 for SPDUs sent from S to R2. It is further assumed that the following errors can occur during the transmission of an SPDU.

a) Authenticity error: Due to a fault within the router, the SPDU is delivered to the incorrect receiver (receiver R2 instead of receiver R1 or vice versa). Thus, the implicit authenticity code $impl_S$ used to calculate the FCS_S in the sender is unequal to the expected authenticity code $impl_R$ in the receiver.

b) Data corruption: Due to for example interference or noise on the transmission media, the content of the SPDU is corrupted (expl and/or FCS).

It is further assumed that the black channel itself does not detect any of these errors. Therefore, the errors, and possibly a combination of errors shall be detected by the check within the safety layer of the receiver. The error pattern err_{impl} caused by the authenticity error is defined by the bit-wise exclusive disjunction (XOR) of the A-codes in use. In this case with only two receivers, this error pattern is constant. The error pattern err_{expl} is defined as the bit-wise exclusive disjunction (XOR) of $expl_S$ and $expl_R$. It is modelled by a BSC (see Annex B).

Figure G.3 shows the residual error probabilities for different parameters when using the proper generator polynomial $x^{16}+x^{14}+x^{11}+x^{10}+x^9+x^7+x^5+x^3+x+1$ (0x14EAB) of degree 16.

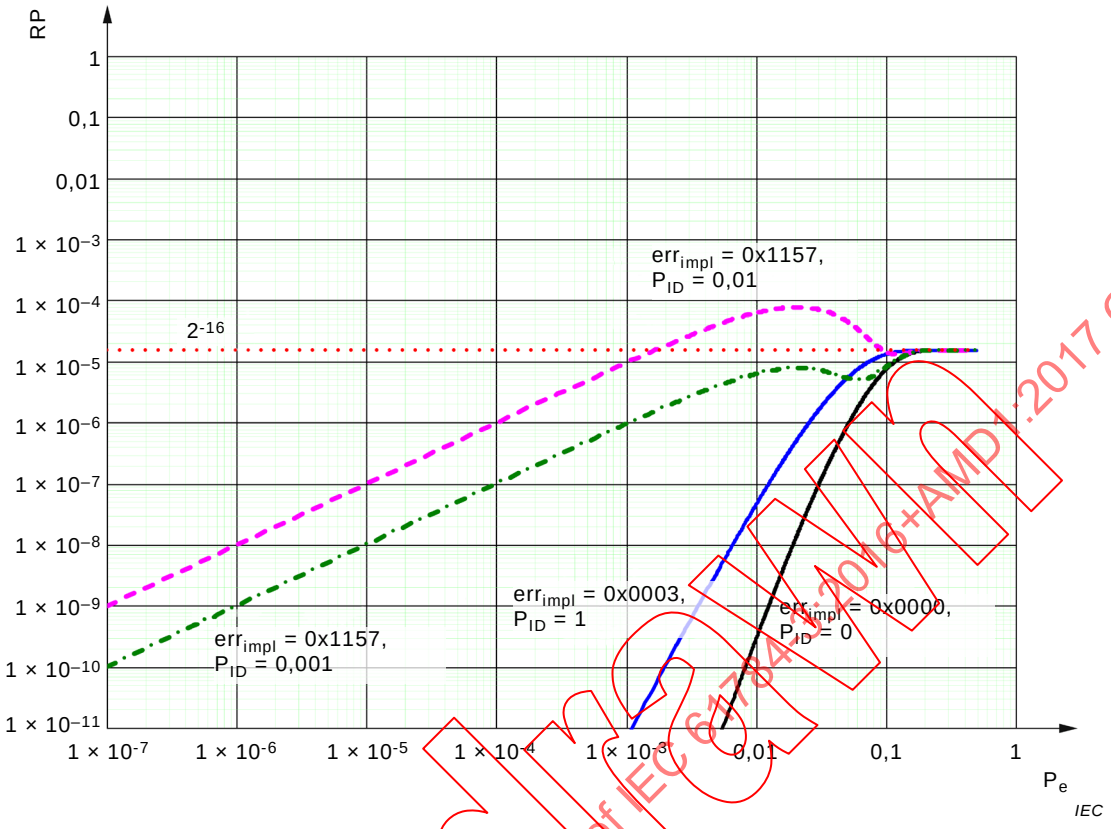


Figure G.3 – Impact of errors in implicit data on the residual error probability

Figure G.3 is based on data which was generated by a brute force algorithm checking all possible error patterns. In addition to the generator polynomial, the following input data was used in the algorithm:

P_{ID} probability of incorrect delivery (here: addressing error);

err_{impl} constant error pattern caused by an addressing error (bitwise disjunction of the A-codes).

It is important to note that the residual error probability does not only depend on p and P_{ID}, but also on the constant err_{impl} and hence on the values of the A-codes chosen during commissioning.

The curve for $P_{ID} = 0$ (solid black) proves the properness of the generator polynomial. In this case of no errors in implicit data, the residual error probability is always below the limit 2^{-16} and the curve is monotonically increasing.

The dashed purple curve and the dotted-dashed green curve show the characteristics when using A-codes resulting in an err_{impl} of 0x1157 (for example the A-codes 0x0001 and 0x1156). The residual error probability is no longer monotonically increasing but has a maximum greater than 2^{-16}. For $P_{ID} = 10^{-3}$, the corresponding curve (dotted-dashed green) does not pass the limit of 2^{-16}. However, if P_{ID} is set to 10^{-2} (dashed purple), the maximum is greater (worse) than the limit 2^{-16}. As a consequence the limit 2^{-r} cannot be used as an approximation even if the generator polynomial has proven properness for the case $P_{ID} = 0$.

The green and purple curve is only observed for certain rare values of err_{impl}. For most other values of err_{impl}, the curves are below the limit even for a probability of occurrence $P_{ID} = 1$. As an example, the curve for $err_{impl} = 0x0003$ (e.g. A-codes equal to 0x0001 and 0x0002) shows this characteristics (solid blue).

Conclusion: When using implicit transmission mechanisms, the residual error probability is not necessarily bounded by 2^{-r}. This bound is only valid if the FSCP provides additional mechanisms such as the ones shown in the following clauses.

NOTE Improper bounding of an FCS would not necessarily lead to insufficient residual error when other FSCP specific protocol measures are combined in the error detection scheme.

G.4 RP for FSCPs with random, uniformly distributed err_{impl}

G.4.1 General

Clause G.4 investigates the case of a random err_{impl} taking each possible value with equal probability ("uniform distribution"). As seen in Clause G.3 where err_{impl} is constant, this assumption is not always justified and shall be provably guaranteed by the design of the respective FSCP.

As already defined earlier, err_{impl} is the bitwise exclusive disjunction (XOR) between the implicit data $impl_S$ used in the sender of the erroneous packet, and the expected value for the implicit data $impl_R$ in the receiver. Clearly, if $impl_S$ and $impl_R$ are uniformly distributed, independent random variables, also err_{impl} is uniformly distributed, i.e. takes each possible value with equal possibility. However, because errors can be assumed to happen at 'random' points of time, it is also possible to achieve a uniformly distributed err_{impl} if $impl_S$ and $impl_R$ are non-random variables. In order to validate whether err_{impl} follows a uniform distribution, statistical checks such as the Chi-Square-Test or the Kolmogoroff-Smirnoff-Test can be used, (see for example [35]).

NOTE 1 err_{impl} being a uniformly distributed random variable, it does not require that all possible values are observed with equal frequency during a finite interval of time. It is therefore not always possible to evaluate a random number generator by simply counting the number of occurrences within a limited time interval.

Depending on the design of the FSCP, there are two reasonable variants of the assumption "err_{impl} is uniformly distributed":

a) err_{impl} takes each value out of $[0;2^i-1]$ with probability 2^{-i};

b) err_{impl} takes each value out of $[1;2^i-1]$ with probability $1/(2^i-1)$.

NOTE 2 There is a slight difference in the two variants: in the second variant, a value of $err_{impl} = 0$ means that the SPDU was delivered correctly, as an incorrectly delivered SPDU will always result in a value $err_{impl} \neq 0$. In the first variant, a value of $err_{impl} = 0$ does not necessarily imply a correct delivery.

In the second case, measures shall be implemented to ensure that each SPDU is assigned a unique value for implicit data. Hence, the error pattern in case of a misdirected SPDU can never become zero. In the first case, no such measures are implemented and hence the error pattern 'zero' may occur. Clearly, such an error cannot be detected in the receiver unless there are additional detectable data integrity errors or other FSCP specific checks.

In the following, the two variants are shown separately.

Other and perhaps more detailed models are beyond the scope of this document. For example, it is possible to eliminate data error patterns with demonstrated certainty of detection by the CRC polynomial.

EXAMPLE Examples of these data error patterns include: Hamming distances less than the minimum Hamming distance for the CRC polynomial over the data block length; burst errors of length r; odd number of bit errors; and others.

Subclause G.4.2 shows an example where the implicit data field is at least as long as the FCS and the implicit data values are randomly generated in such a way that A-codes are not guaranteed unique for each endpoint, T-codes are not guaranteed unique for each SPDU time, and the combinations of A-code and T-code are not guaranteed unique.

Subclause G.4.3 shows an example where the implicit data field is exactly as long as the FCS and A-codes and T-codes are guaranteed unique for each endpoint and SPDU time. In actual application, additional terms may be necessary to account for exceptions such as T-code wrap around.

Clause G.5 shows a summation method for general applicability when conditional weight distributions for implicit data error patterns are known and can be quantified.

G.4.2 Uniform distribution within the interval [0;2^i-1], i ≥ r

This case applies in particular to FSCPs that use random number generators to derive implicit data values.

At a coarse-grained level, two main types of errors can be discriminated:

- Incorrect content of an SPDU, i. e. data integrity errors;
- Incorrect delivery of an SPDU, i.e. the SPDU is delivered to the wrong receiver or at the wrong instance of time.

In combination, the following disjoint cases can be discriminated:

- Case 1. CC: No error (correct delivery, and correct explicit data);
- Case 2. IC: Incorrect delivery, and correct explicit data;
- Case 3. CI: Correct delivery, and incorrect explicit data;
- Case 4. II: Incorrect delivery, and incorrect data.

The residual error probabilities RP_2, RP_3, and RP_4 for each of the cases 2, 3, and 4 are calculated from the following parameters:

P_{ID} is the "probability of incorrect delivery", i.e. the probability that due to for example an authenticity or timeliness error an SPDU is erroneously delivered to the FSCP;

NOTE 1 The event "incorrect delivery" can result in an $err_{impl} \neq 0$. However, due to the uniform distribution within [0;2^r-1] the case $err_{impl} = 0$ can also occur.

P_{IED} is the probability of incorrect explicit data, i.e. the probability that data corruption occurs;

P_{IC} is the probability that an error is not detected in the receiver under the condition that case 2 occurs;

P_{CI} is the probability that an error is not detected in the receiver under the condition that case 3 occurs;

P_{II} is the probability that an error is not detected in the receiver under the condition that case 4 occurs;

RP_I is the residual error probability for data corruption as defined in Annex F.

R_{CRC} is the residual error probability for CRC polynomials as defined in Equation B.3.

NOTE 2 $RP_I \leq R_{CRC}$ because other safety measures than CRC can further reduce the value of RP_I.

r is the length of the FCS, identical to the degree of the CRC polynomial;

i is the length of the implicit data, with i ≥ r;

n is the number of bits of the SPDU.

Because the events IC, CI, and II are disjoint, the overall residual error probability can be obtained by building the sum of the respective RP_x values.

In general, RP_x is calculated by:

RP_x = P("error case x takes place") × P("error case x is not detectable").

This leads to the formulae for cases 2, 3 and 4 detailed in the following paragraphs.

Case 2 (IC)

$RP_2 = P_{ID} \times (1 - P_{IED}) \times P_{IC}$
$= P_{ID} \times (1 - P_{IED}) \times 2^{-r}$

Explanations on P_{IC}:

- If i > r, this probability is 2^{-r}, because
  - by assumption, the bitwise disjunction of $impl_S$ and $impl_R$ is uniformly distributed in the interval $[0;2^i-1]$;
  - therefore, the bitwise disjunction of $FCS_S = FCS_R$ and FCS_C is uniformly distributed in the interval $[0;2^r-1]$;
  - therefore, the probability that the bitwise disjunction of FCS_R and FCS_C equals zero is 2^{-r};
  - therefore, the probability that FCS_R is equal to FCS_C is 2^{-r}.
- If i = r, this probability is 2^{-r}, because
  - FCS_R is equal to FCS_C, if and only if $err_{impl} = 0$, because the length of err_{impl} does not exceed the degree of the CRC polynomial. CRC-codes detect all burst errors of length less than or equal to r;
  - the probability that $err_{impl} = 0$ is 2^{-r} because of the uniform distribution in the interval $[0;2^r-1]$.

Case 3 (CI)

$RP_3 = (1-P_{ID}) \times P_{IED} \times P_{CI}$
$= (1-P_{ID}) \times RP_I$
$\leq (1-P_{ID}) \times 2^{-r}$ for proper polynomials.

Case 4 (II)

$RP_4 = P_{ID} \times P_{IED} \times P_{II}$
$= P_{ID} \times P_{IED} \times 2^{-r}$

Explanations:

- Due to the assumptions, err_{impl} takes all values from $[0;2^i-1]$ with equal probability.
- Hence, each bit of err_{impl} takes the value 0 or 1 with equal probability 0,5.
- Because CRC-codes are linear codes, and because $|err_{impl}| \geq r$, each bit of err_{impl} determines the result of one bit in the bitwise exclusive disjunction of FCS_R and FCS_C.
- Hence, the bits in the bitwise exclusive disjunction of FCS_R and FCS_C can be treated as independent random variables, each taking the values 0 and 1 with equal probability 0,5.
- The bitwise exclusive disjunction of FCS_R and FCS_c is a uniformly distributed random variable, taking all values from $[0;2^r-1]$ with equal probability.
- The probability that the bitwise exclusive disjunction of FCS_R and FCS_C equals zero is 2^{-r}.
- The probability that FCS_C is identical to FCS_R is 2^{-r}.

In summary, the residual error probability of an FSCP using implicit mechanisms for the detection of timeliness and authenticity error (guaranteeing that the error in the implicit data is uniformly distributed in the interval $[0;2^i-1]$ can be calculated using the following formula:

RP_{TOTAL} = RP2 + RP3 + RP4

$= (P_{ID} \times (1 - P_{IED}) \times 2^{-r}) + ((1-P_{ID}) \times P_{IED} \times P_{CI}) + (P_{ID} \times P_{IED} \times 2^{-r})$

$= (P_{ID} \times 2^{-r}) + ((1-P_{ID}) \times P_{IED} \times P_{CI})$

$= (P_{ID} \times 2^{-r}) + ((1-P_{ID}) \times RP_I)$

Explanation:

- Cases 2 to 4 are disjoint events.

In case of a proper polynomial, the following applies:

RP_{TOTAL} = RP2 + RP3 + RP4

$= (P_{ID} \times (1 - P_{IED}) \times 2^{-r}) + ((1-P_{ID}) \times P_{IED} \times P_{CI}) + (P_{ID} \times P_{IED} \times 2^{-r})$

$\leq (P_{ID} \times (1 - P_{IED}) \times 2^{-r}) + ((1-P_{ID}) \times 2^{-r}) + (P_{ID} \times P_{IED} \times 2^{-r})$

$\leq 2^{-r}$

Explanations:

- Cases 2 to 4 are disjoint events.
- This upper bound of RP_{TOTAL} is independent of the values of P_{IED} and P_{ID}.

G.4.3 Uniform distribution in the interval [1;2^r-1], i = r

For this variant, it is assumed i = r, i.e. the length of the implicit data is exactly the degree of the CRC polynomial, and that err_{impl} is uniformly distributed within the interval [1;2^r-1]. In contrast to the variant shown in G.4.2, err_{impl} is always unequal to 0 in case of an incorrect delivery.

The following cases of error combinations can be discriminated:

- Case 1. CC: No error (correct delivery, and correct explicit data);
- Case 2. IC: Incorrect delivery, and correct explicit data;
- Case 3. CI: Correct delivery, and incorrect explicit data;
- Case 4. II: Incorrect delivery, and incorrect data.

The residual error probabilities RP_2, RP_3, and RP_4 for each of the cases 2, 3, and 4 are calculated from the following parameters:

P_{ID} is the "probability of incorrect delivery", i.e. the probability that due to for example an authenticity or timeliness error an SPDU is erroneously delivered to the FSCP;

NOTE Due to the uniform distribution within [1;2^r-1], $err_{impl} \neq 0$ is guaranteed. Hence, the event "incorrect delivery" is equivalent to the event "incorrect implicit data" in this case.

P_{IED} is the probability of incorrect explicit data, i.e. the probability that data corruption occurs;

P_{IC} is the probability that an error is not detected in the receiver under the condition that case 2 occurs;

P_{CI} is the probability that an error is not detected in the receiver under the condition that case 3 occurs;

P_{II} is the probability that an error is not detected in the receiver under the condition that case 4 occurs;

$P_{EIC}(i)$ is the probability that the error pattern in the explicit data err_{expl} complements the error pattern in the implicit data err_{impl} making the error undetectable, under the condition that "err_{impl} = i";

r is the length of the implicit data and the length of the FCS (degree of the CRC polynomial);

n is the number of bits in the SPDU.

Because the events IC, CI, and II are disjoint, the overall residual error probability can be obtained by building the sum of the respective RP_x values.

In general, RP_x is calculated by:

RP_x = P("error case x takes place") × P("error case x is not detectable").

This leads to the formulae for cases 2, 3 and 4 detailed in the following paragraphs.

Case 2 (IC)

$$RP_2 = P_{ID} \times (1 - P_{IED}) \times P_{IC}$$
$$= 0$$

Explanation:

- Errors of type 2 are always detected, because the length of err_{impl} does not exceed r. CRC-codes detect all burst errors of length less than or equal to r. Hence P_{IC} is equal to 0 in this case.

Case 3 (CI)

$$RP_3 = (1-P_{ID}) \times P_{IED} \times P_{CI}$$
$$= (1-P_{ID}) \times RP_I$$
$$\leq (1-P_{ID}) \times 2^{-r} \text{ for proper polynomials.}$$

Case 4 (II)

$$RP_4 = P_{ID} \times P_{IED} \times P_{II}$$
$$\approx P_{ID} \times P_{IED} \times 2^{-r}$$

Explanations:

- $$P_{II} = \sum_{i=1}^{2^r-1} P\{err_{impl} = i\} \times P_{EIC}(i)$$
$$= \sum_{i=1}^{2^r-1} \frac{1}{2^r-1} \times P_{EIC}(i)$$
$$= \frac{1}{2^r-1} \times \sum_{i=1}^{2^r-1} P_{EIC}(i)$$
$$= \frac{1}{2^r-1} \text{ (because for all possible } err_{expl} \text{ there is exactly one matching } err_{impl})$$
$$\approx 2^{-r}$$

In summary, the residual error probability of an FSCP using implicit mechanisms for the detection of timeliness and authenticity error guaranteeing that the error in the implicit data is uniformly distributed in the interval $[1;2^r-1]$, can be calculated using the following formula:

$$RP_{TOTAL} = RP2 + RP3 + RP4$$
$$= (P_{ID} \times (1 - P_{IED}) \times 2^{-r}) + ((1-P_{ID}) \times P_{IED} \times P_{CI}) + (P_{ID} \times P_{IED} \times 2^{-r})$$
$$= (P_{ID} \times 2^{-r}) + ((1-P_{ID}) \times P_{IED} \times P_{CI})$$

$$= (P_{ID} \times 2^{-r}) + ((1\text{-}P_{ID}) \times RP_I)$$

Explanation:

- Cases 2 to 4 are disjoint events.

G.5 General case

The calculations presented in G.4.2 and G.4.3 are only valid under the assumption of a uniform distribution of err_{impl} and with certain restrictions on the length of the implicit data field. In the general case, RP_{TOTAL} can be calculated as follows, if the conditional weight distribution of the code is known for each possible value of err_{impl}.

$$RP_{TOTAL} = P_{ID} \times \sum_{j=0}^{2^i-1} R\{ err_{impl} = j\} \times R\{ FCS_C = FCS_R \mid err_{impl} = j\} + (1 - P_{ID}) \times P_{re}^{CRC, BSC}$$

where

$R\{ err_{impl} = j\}$ is the probability that the error pattern in implicit data has the value j (under the condition that there is a misdirected SPDU);

$R\{ FCS_C = FCS_R \mid err_{impl} = j\}$ is the probability that no error is indicated for the given CRC-polynomial and code length, under the condition that the error pattern in implicit data has the value j;

$P_{re}^{CRC, BSC}$ is the residual error probability for the given CRC-polynomial and code length without implicit data.

$P_{re}^{CRC, BSC}$ and $R\{ FCS_C = FCS_R \mid err_{impl} = j\}$ are given by:

$$P_{re}^{CRC,BSC} = \sum_{k=1}^{n} A_k(err_{impl} = 0) \times P_e^k \times (1 - P_e)^{n-k}$$

$$R\{ FCS_C = FCS_R \mid err_{impl} = j\} = \sum_{k=0}^{n} A_k(err_{impl} = j) \times P_e^k \times (1 - P_e)^{n-k}$$

where

$A_k(err_{impl} = j)$ is the weight distribution of the code under the condition that the error pattern in the implicit data takes the value j.

Explanations:

- $R\{ FCS_C = FCS_R \mid err_{impl} = 0\} = P_{re}^{CRC, BSC} + (1\text{-}P_e)^n$.

G.6 Calculation of P_{ID}

If both the T-code and the A- code are implicit, P_{ID} can be calculated as follows:

$$P_{ID} = \min\left(\frac{R_T + R_A}{\nu}, 1\right)$$

where

P_{ID} is the probability that due to for example an authenticity or timeliness error an SPDU is erroneously delivered to the FSCP;

R_T is the rate of occurrence for incorrect sequence safety PDUs (see F.5.2.4);

R_A is the rate of occurrence for misdirected safety PDUs (see F.5.2.3);

v is the maximum number of SPDU samples by the SCL ("sample rate") per hour (see F.5.2.2).

Explanation:

- Due to approximation, $R_T + R_A$ may become greater than one. In this case, the value 1 shall be used for P_{ID}.

If only the T-code is implicit, P_{ID} can be calculated as follows:

$$P_{ID} = \frac{R_T}{v}$$

If only the A-code is implicit, P_{ID} can be calculated as follows:

$$P_{ID} = \frac{R_A}{v}$$

Calculation of the total residual error rate

According to F.10.1, the total residual error rate is calculated by (see Equation (F.6)):

$$\lambda_{SC} = RR_T + RR_A + RR_I + RR_M$$

Alternatively, the following formula can be used:

$$\lambda_{SC} = v \times RP_{TOTAL}$$

Bibliography

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

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

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

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

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

[5] IEC 61131-2:2007, *Programmable controllers – Part 2: Equipment requirements and tests*

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

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

[8] IEC 61496-1, *Safety of machinery – Electro-sensitive protective equipment – Part 1: General requirements and tests*

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

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

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

[12] IEC 61784-4[18], *Industrial communication networks – Profiles – Part 4: Secure communications for fieldbuses*

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

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

[15] IEC 62061:2005, *Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems*

[18] Proposed new work item under consideration.

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

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

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

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

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

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

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

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

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

[25] ISO 13849-1:2015, *Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design*

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

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

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

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

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

[31] J. WOLF, A. MICHELSON, A. LEVESQUE, *On the probability of undetected error for linear block codes*, February 1982, IEEE Transactions on Communications, Volume 30, Issue 2

[32] S. LEUNG-YAN-CHEONG AND M. HELLMAN, *Concerning a bound on undetected error probability*, March 1976, IEEE Transactions on Information Theory, Volume 22, Issue 2

[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, Issue 6

[35] D. KNUTH, *The Art of Computer Programming, Volume 2: Seminumerical Algorithms*, 3rd Edition, Addison-Wesley, 1997

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

RÉSEAUX DE COMMUNICATION INDUSTRIELS – PROFILS –

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

AVANT-PROPOS

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

Cette version consolidée de la Norme IEC officielle et de son amendement a été préparée pour la commodité de l'utilisateur.

L'IEC 61784-3 édition 3.1 contient la troisième édition (2016-05) [documents 65C/840/FDIS et 65C/848/RVD] et son amendement 1 (2017-08) [documents 65C/879/FDIS et 65C/886/RVD].

Cette version Finale ne montre pas les modifications apportées au contenu technique par l'amendement 1. Une version Redline montrant toutes les modifications est disponible dans cette publication.

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

Cette troisième édition constitue une révision technique.

Cette édition inclut les modifications techniques majeures suivantes par rapport à l'édition précédente:

- clarifications et explications complémentaires des exigences, références actualisées;
- suppression des présentations techniques de profils (Articles 6 à 13) et paragraphes dédiés associés à des termes, définitions, symboles et abréviations;
- ajout de profils pour les familles de profils de communication 8, 17 et 18 (Articles 10, 14, 15);
- clarifications des modèles de l'Annexe A;
- modification de l'Annexe B informative qui devient normative;
- ajout d'une nouvelle Annexe E informative pour décrire les modèles des mécanismes FSCP explicites et implicites;
- ajout d'une nouvelle Annexe F informative qui introduit un modèle étendu pour l'estimation du taux total d'erreurs résiduelles;
- actualisations des parties pour les CPF 1, CPF 2, CPF 3, CPF 8, CPF 13 (détails fournis dans les parties);
- ajout d'une nouvelle partie pour CPF 17.

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

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

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

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

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

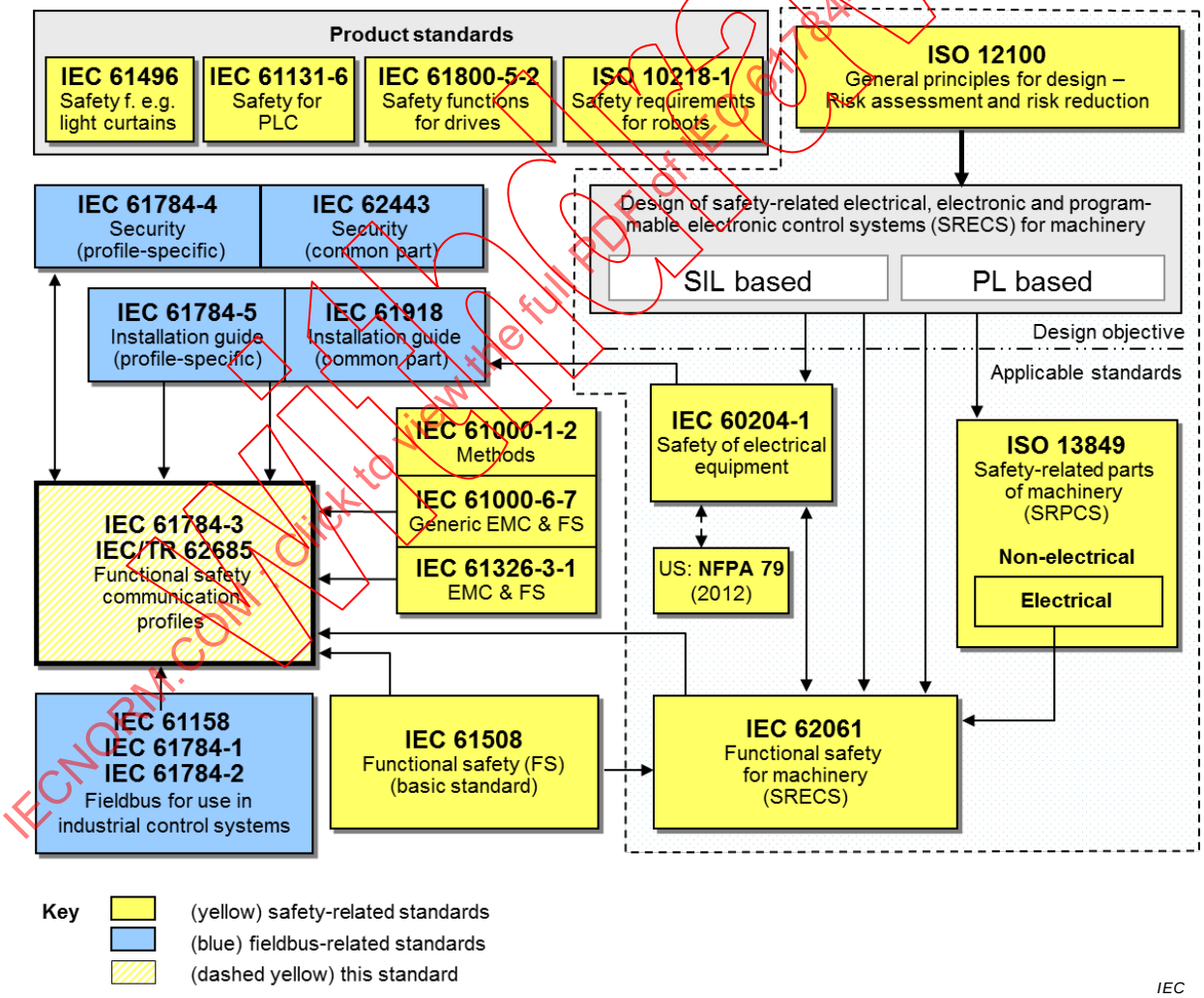
0 Introduction

0.1 Généralités

L'IEC 61158, relative aux bus de terrain, ainsi que ses normes associées IEC 61784-1 et IEC 61784-2, définit un ensemble de protocoles de communication qui assurent la commande répartie d'applications automatisées. La technologie de bus de terrain est désormais reconnue et bien éprouvée. Les améliorations des bus de terrain se poursuivent; elles couvrent des applications pour des domaines comme les applications en temps réel relatives à la sécurité et à la sûreté.

Cette norme définit les principes applicables aux communications de sécurité fonctionnelle en référence à la série IEC 61508; elle spécifie plusieurs couches de communication de sécurité (profils et protocoles correspondants) en fonction des profils de communication et des couches de protocole de l'IEC 61784-1, l'IEC 61784-2 et de la série IEC 61158. Elle ne couvre pas les aspects relatifs à la sécurité électrique et à la sécurité intrinsèque.

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

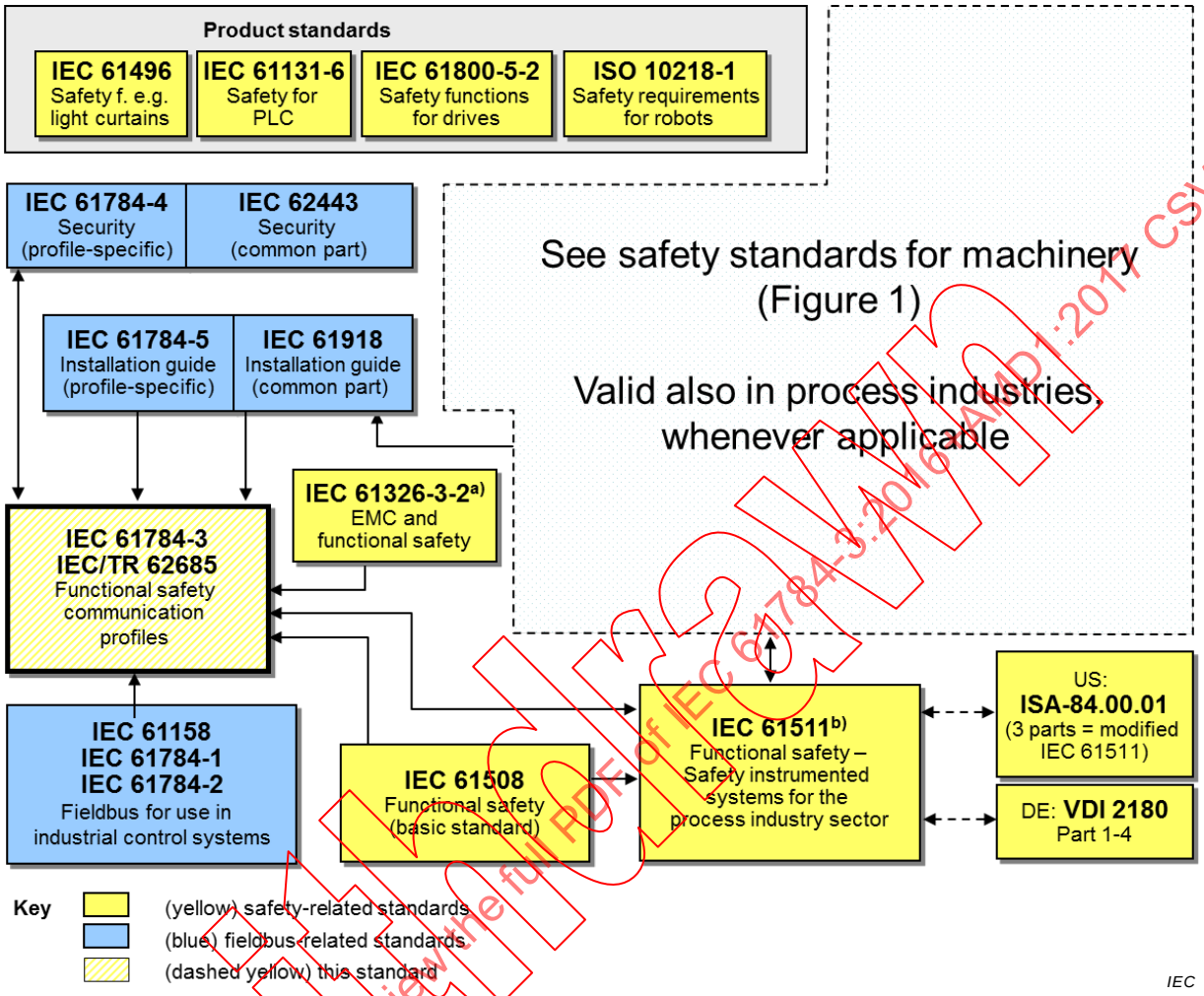


Anglais	Français
Product standards	Normes de produits
Safety function, e.g. light curtains	Fonction de sécurité, par exemple rideaux de lumière
Safety for PLC	Sécurité relative aux automates programmables
Safety functions for drives	Fonctions de sécurité applicables aux entraînements
Safety requirements for robots	Exigences de sécurité applicables aux robots
General principles for design – Risk assessment and risk reduction	Principes généraux de conception – Appréciation du risque et réduction du risque
Security (profile-specific)	Sécurité (spécifique au profil)
Security (common part)	Sécurité (partie commune)
Design of safety-related electrical, electronic and programmable electronic control systems (SRECS) for machinery	Conception des systèmes de commande électriques, électroniques et électroniques programmables relatifs à la sécurité pour les machines
SIL based	Basé sur SIL
PL based	Basé sur PL
Installation guide (profile-specific)	Guide d'installation (spécifique au profil)
Installation guide (common part)	Guide d'installation (partie commune)
Design objective	Objectif de conception
Applicable standards	Normes applicables
Methods	Méthodes
Generic EMC & FS	CEM & FS génériques
EMC & FS	CEM & FS
Safety of electrical equipment	Sécurité des équipements électriques
Safety-related parts of machinery	Sécurité des machines – Parties des systèmes de commande relatives à la sécurité
Non-electrical	Non électrique
Electrical	Electrique
Functional safety communication profiles	Profils de communication de sécurité fonctionnelle
Fieldbus for use in industrial control systems	Bus de terrain pour utilisation dans des systèmes de commande industriels
Functional safety (FS) (basic standard)	Sécurité fonctionnelle (FS) (norme de base)
Functional safety for machinery	Sécurité fonctionnelle des machines
Key	Légende
(yellow) safety-related standards	(jaune) normes relatives à la sécurité
(blue) fieldbus-related standards	(bleu) normes relatives au bus de terrain
(dashed yellow) this standard	(jaune pointillé) la présente norme

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

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

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



Anglais	Français
Product standards	Normes de produits
Safety function, e.g. light curtains	Fonction de sécurité, par exemple rideaux de lumière
Safety for PLC	Sécurité relative aux automates programmables
Safety functions for drives	Fonctions de sécurité applicables aux entraînements
Safety requirements for robots	Exigences de sécurité applicables aux robots
Security (profile-specific)	Sûreté (spécifique au profil)
Security (common part)	Sûreté (partie commune)
Installation guide (profile-specific)	Guide d'installation (spécifique au profil)
Installation guide (common part)	Guide d'installation (partie commune)
See safety standards for machinery (Figure 1)	Voir normes de sécurité pour les machines (Figure 1)
Valid also in process industries, whenever applicable	Valable également dans les industries de transformation, le cas échéant
Functional safety communication profiles	Profils de communication de sécurité fonctionnelle
EMC and functional safety	CEM et sécurité fonctionnelle
Fieldbus for use in industrial control systems	Bus de terrain pour utilisation dans des systèmes de commande industriels
Functional safety (basic standard)	Sécurité fonctionnelle (norme de base)

Anglais	Français
Functional safety–safety instrumented systems for the process industry sector	Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur des industries de transformation
3 parts = modified IEC 61511	3 parties = IEC 61511 modifiée
Part 1 – 4	Parties 1 à 4
Key	Légende
(yellow) safety-related standards	(jaune) normes relatives à la sécurité
(blue) fieldbus-related standards	(bleu) normes relatives au bus de terrain
(dashed yellow) this standard	(jaune pointillé) la présente norme

[a] Pour des environnements électromagnétiques spécifiés; sinon, l'IEC 61326-3-1 ou l'IEC 61000-6-7.

[b] EN ratifiée.

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

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

Les couches de communication de sécurité spécifiées dans la présente norme permettent de garantir cette assurance de sorte qu'un bus de terrain puisse être utilisé dans des applications qui nécessitent une sécurité fonctionnelle jusqu'au niveau d'intégrité de sécurité (SIL) spécifié par son profil de communication de sécurité fonctionnelle correspondant.

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

La présente norme décrit:

- les principes de base de la mise en œuvre des exigences de la série IEC 61508 pour les communications de données relatives à la sécurité, y compris les anomalies de transmission potentielles, les mesures correctives et des considérations relatives à l'intégrité des données;
- les profils de communication de sécurité fonctionnelle pour plusieurs familles de profils de communication dans les IEC 61784-1 et IEC 61784-2, y compris les extensions de la couche de sécurité aux sections relatives au service et aux protocoles de communication de la série IEC 61158.

0.2 Transition de l'édition 2 aux méthodes d'évaluation étendue de l'édition 3

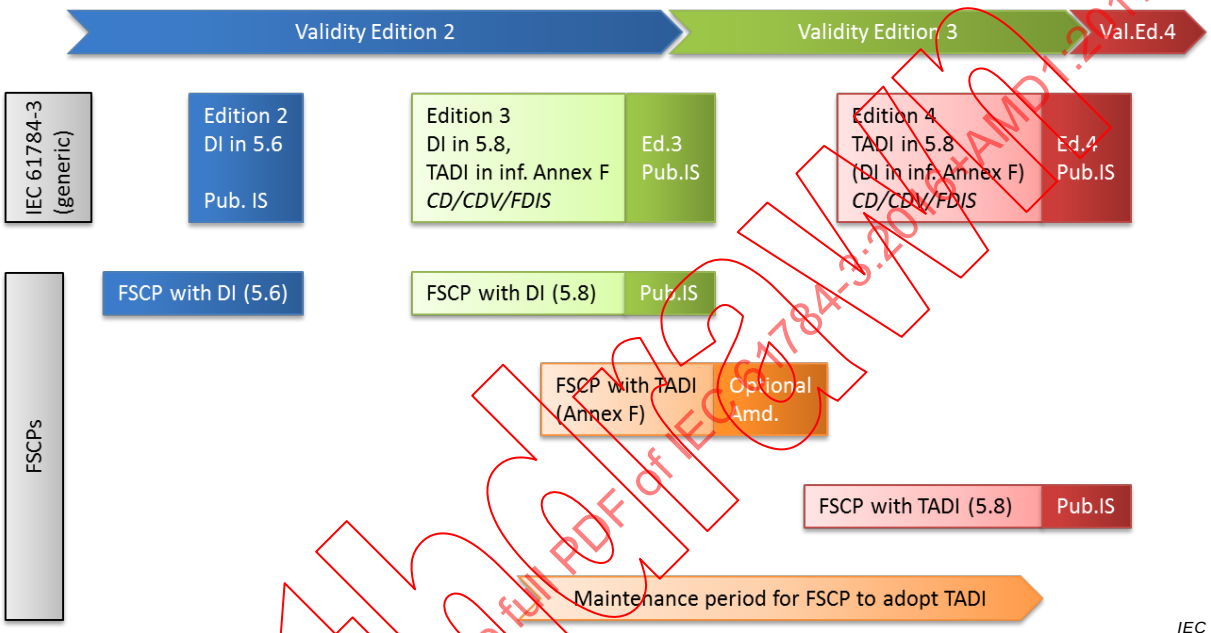
Cette édition de la partie générique de la norme comprend des modèles étendus supplémentaires pour une utilisation ultérieure lors de l'estimation du taux total d'erreurs résiduelles pour un FSCP. Cette valeur peut être utilisée pour déterminer si le FSCP satisfait aux exigences des applications de sécurité fonctionnelle jusqu'à un SIL donné. Ces modèles étendus pour les méthodes qualitatives et quantitatives de détermination de sécurité sont détaillés à l'Annexe E et à l'Annexe F.

Toutefois, en raison de la durée typique du processus d'évaluation, les Profils de Communication de Sécurité Fonctionnelle publiés avant ou en même temps que cette nouvelle édition de la partie générique ne peuvent être évalués qu'en fonction des méthodes

des éditions précédentes, sur la base des considérations relatives à l'intégrité des données détaillées en 5.8.

Le schéma de validité de la Figure 3 présente le procédé de gestion de la transition des méthodes d'évaluation d'origine de l'édition 2 (détaillé en 5.8) aux méthodes d'évaluation étendue de l'édition 3 (actuellement spécifiées à l'Annexe F). Conformément à ce schéma, les Profils de Communication de Sécurité Fonctionnelle sont exemptés d'une nouvelle évaluation conformément à l'Annexe F jusqu'à l'édition 4, lorsque le contenu de l'Annexe F actuelle remplacera le 5.8 actuel.

NOTE Un FSCP peut cependant réaliser une évaluation antérieure et publier un amendement approprié.



Anglais	Français
Validity edition	Edition de validité
(generic)	(générique)
DI in ...	DI en ...
... in inf. Annex F	... à l'Annexe F inf.
... with DI	... avec DI
... with TADI	... avec TADI
Optional amd.	Amd. facultatif
Maintenance period for FSCP to adopt TADI	Période de maintenance permettant au FSCP d'adopter TADI

Légende

DI Data Integrity (Intégrité des données)

TADI Timeliness, Authenticity, Data Integrity (Opportunité, Authenticité, Intégrité des données)

Figure 3 – Transition de l'édition 2 aux méthodes d'évaluation de l'édition 3

0.3 Déclaration de brevet

La commission électrotechnique internationale (IEC) attire l'attention sur le fait qu'il est déclaré que la conformité aux dispositions du présent document peut impliquer l'utilisation de brevets qui intéressent les profils de communication de sécurité fonctionnelle pour les familles 1, 2, 3, 6, 8, 12, 13, 14, 17 et 18 de l'IEC 61784-3-1, l'IEC 61784-3-2,

l'IEC 61784-3-3, l'IEC 61784-3-6, l'IEC 61784-3-8, l'IEC 61784-3-12, l'IEC 61784-3-13, l'IEC 61784-3-14, l'IEC 61784-3-17 et l'IEC 61784-3-18.

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

Les détenteurs de ces droits de propriété ont donné l'assurance à l'IEC qu'ils consentent à négocier des licences avec des demandeurs du monde entier, sans frais ou à des termes et conditions raisonnables et non discriminatoires. A ce propos, les énoncés des détenteurs de ces droits de propriété sont enregistrés à l'IEC.

NOTE Les détails relatifs aux brevets et les informations relatives aux coordonnées correspondantes sont fournis dans l'IEC 61784-3-1, l'IEC 61784-3-2, l'IEC 61784-3-3, l'IEC 61784-3-6, l'IEC 61784-3-8, l'IEC 61784-3-12, l'IEC 61784-3-13, l'IEC 61784-3-14, l'IEC 61784-3-17 et l'IEC 61784-3-18.

L'attention est attirée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété intellectuelle autres que ceux identifiés ci-dessus. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et de ne pas avoir signalé leur existence.

L'ISO (www.iso.org/patents) et l'IEC (http://patents.iec.ch) maintiennent à disposition des bases de données en ligne des droits de propriété relatifs à leurs normes. Les utilisateurs sont encouragés à consulter ces bases de données pour obtenir les informations les plus récentes concernant les droits de propriété.

INTRODUCTION à l'Amendement

Le présent Amendement 1 traite des concepts de mécanismes de sécurité reposant sur des données implicites destinés à être utilisés dans les protocoles de communication de sécurité fonctionnelle (FSCP, *functional safety communications protocols*) spécifiés dans l'IEC 61784-3:2016.

RÉSEAUX DE COMMUNICATION INDUSTRIELS – PROFILS –

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

1 Domaine d'application

La présente partie de la série IEC 61784-3 définit des principes communs qui peuvent être appliqués pour la transmission des messages relatifs à la sécurité entre les participants d'un réseau réparti, à l'aide de la technologie de bus de terrain conformément aux exigences de la série IEC 61508[1] sur la sécurité fonctionnelle. Ces principes peuvent s'appuyer sur le principe de canal noir. Ils peuvent être utilisés dans différentes applications industrielles, par exemple la commande de processus, l'usinage automatique et les machines.

La présente partie[2] et les parties IEC 61784-3-x spécifient plusieurs profils de communication de sécurité fonctionnelle basés sur les profils de communication et les couches de protocole des technologies des bus de terrain de l'IEC 61784-1, de l'IEC 61784-2 et de la série IEC 61158. Ces profils de communication de sécurité fonctionnelle utilisent le principe de canal noir, comme défini dans l'IEC 61508. Ces profils de communication de sécurité fonctionnelle sont destinés à être exclusivement mis en œuvre dans des appareils de sécurité.

NOTE 1 Il peut exister d'autres systèmes de communication relatifs à la sécurité qui satisfont aux exigences de la série IEC 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 comme les chocs électriques. La sécurité intrinsèque concerne les dangers associés aux atmosphères explosibles.

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

NOTE 3 Des exigences spécifiques au profil peuvent également être spécifiées dans l'IEC 61784-4[3].

NOTE 4 La mise en œuvre du profil de communication de sécurité fonctionnelle, conforme à la présente partie, dans un appareil normal ne suffit pas à le qualifier d'appareil de sécurité, comme défini dans la série IEC 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 suivants sont cités en référence de manière normative, en intégralité ou en partie, dans le présent document et sont indispensables pour son application. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

---

1 Dans les pages suivantes de la présente norme, "IEC 61508" remplace "série IEC 61508".

2 Dans les pages suivantes de la présente norme, "la présente partie" remplace "cette partie de la série IEC 61784-3".

3 Proposition d'un nouveau sujet de travail à l'étude.

IEC 61000-6-7, *Compatibilité électromagnétique (CEM) – Partie 6-7: Normes génériques – Exigences d'immunité pour les équipements visant à exercer des fonctions dans un système lié à la sécurité (sécurité fonctionnelle) dans des sites industriels*

IEC 61010-2-201:2013, *Règles de sécurité pour appareils électriques de mesurage, de régulation et de laboratoire – Partie 2-201: Exigences particulières pour les équipements de commande*

IEC 61158 (toutes les parties), *Réseaux de communication industriels – Spécifications des bus de terrain*

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

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

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

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

IEC 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, *Réseaux de communication industriels – Profils – Part 1: Profils de bus de terrain*

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

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

IEC 61784-3-2, *Réseaux de communication industriels – Profils – Partie 3-2: Bus de terrain de sécurité fonctionnelle – Spécifications supplémentaires pour CPF 2*

IEC 61784-3-3, *Réseaux de communication industriels – Profils – Partie 3-3: Bus de terrain de sécurité fonctionnelle – Spécifications supplémentaires pour CPF 3*

IEC 61784-3-6, *Réseaux de communication industriels – Profils – Partie 3-6: Bus de terrain de sécurité fonctionnelle – Spécifications supplémentaires pour CPF 6*

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

IEC 61784-3-12, *Réseaux de communication industriels – Profils – Partie 3-12: Bus de terrain de sécurité fonctionnelle – Spécifications supplémentaires pour CPF 12*

IEC 61784-3-13, *Réseaux de communication industriels – Profils – Partie 3-13: Bus de terrain de sécurité fonctionnelle – Spécifications supplémentaires pour CPF 13*

IEC 61784-3-14, *Réseaux de communication industriels – Profils – Partie 3-14: Bus de terrain de sécurité fonctionnelle – Spécifications supplémentaires pour CPF 14*

IEC 61784-3-17[4], *Réseaux de communication industriels – Profils – Partie 3-17: Bus de terrain de sécurité fonctionnelle – Spécifications supplémentaires pour CPF 17*

IEC 61784-3-18, *Réseaux de communication industriels – Profils – Partie 3-18: Bus de terrain de sécurité fonctionnelle – Spécifications supplémentaires pour CPF 18*

IEC 61784-5 (toutes les parties), *Réseaux de communication industriels – Profils – Partie 5: Installation des bus de terrain*

IEC 61918:2013, *Réseaux de communication industriels – Installation de réseaux de communication dans des locaux industriels*

IEC 62443 (toutes les parties), *Réseaux industriels de communication – Sécurité dans les réseaux et les systèmes*

3 Termes, définitions, symboles, abréviations et conventions

3.1 Termes et définitions

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

NOTE Les italiques sont utilisés dans les définitions pour mettre en évidence les termes définis en 3.1.

3.1.1
date absolue
date référencée par rapport à un temps global, commun à un groupe d'appareils utilisant un *bus de terrain*

[SOURCE: IEC 62280:2014, 3.1.1, modifié – utilisation d'appareils et de bus de terrain]

3.1.2
élément de réseau actif
élément de réseau contenant des composants actifs du point de vue électrique et/ou optique et permettant d'étendre le réseau

Note 1 à l'article: Les répéteurs et les commutateurs sont des exemples d'éléments de réseau actif.

[SOURCE: IEC 61918:2013, 3.1.2]

3.1.3
disponibilité
probabilité, pour un système automatisé, qu'il ne se produise pas de condition opérationnelle non satisfaisante, par exemple la perte de production, pendant une période donnée

3.1.4
probabilité d'erreurs sur les éléments binaires
Pe
probabilité de réception d'un bit donné avec la valeur incorrecte

4 A publier

3.1.5
canal noir
système de communication défini qui contient un ou plusieurs éléments sans preuve de conception ou de validation conformément à l'IEC 61508

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

3.1.6
pont
appareil abstrait qui relie plusieurs segments de réseau le long de la couche de liaison de données

3.1.7
système de communication fermé
nombre fixe ou nombre maximal fixe d'éléments reliés par un système de communication dont les propriétés sont connues et fixées et où le risque d'accès non autorisé est considéré comme négligeable

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

3.1.8
canal de communication
connexion logique entre deux points limites d'un *système de communication*

3.1.9
système de communication
ensemble de matériels, de logiciels et de supports de propagation qui permet la transmission de *messages* (ISO/IEC 7498-1, couche d'application) d'une application à une autre

3.1.10
connexion
liaison logique entre objets applicatifs au sein du même appareil ou d'appareils différents

3.1.11
contrôle de redondance cyclique
CRC
<valeur> donnée redondante déduite et enregistrée ou transmise simultanément d'un bloc de données afin de détecter toute corruption des données

<méthode> procédure utilisée pour calculer les données redondantes

Note 1 à l'article: Les termes "code CRC" et "signature CRC", ainsi que les étiquettes comme CRC1, CRC2, peuvent également être utilisés dans la présente norme pour se référer aux données redondantes.

Note 2 à l'article: Voir également [28], [29][5].

3.1.12
système de communication défini
canal défini
nombre fixe ou nombre maximal fixe d'éléments reliés par un système de communication à bus de terrain, dont les propriétés sont connues et fixées, par exemple les conditions d'installation, l'immunité électromagnétique, les éléments (actifs) de réseau industriel, et où le risque d'accès non autorisé est réduit à un niveau tolérable conformément au modèle de cycle de vie de l'IEC 62443, en utilisant par exemple des zones et des conduits

5 Les chiffres entre crochets se réfèrent à la bibliographie.

3.1.13
diversité
moyens différents pour réaliser une fonction requise

Note 1 à l'article: La diversité peut être réalisée en utilisant des méthodes physiques ou des approches conceptuelles différentes.

[SOURCE: IEC 61508-4:2010, 3.3.7]

3.1.14
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 à l'article: Les erreurs peuvent être causées par des erreurs de conception du matériel/logiciel et/ou des informations altérées du fait d'un brouillage électromagnétique et/ou autres effets.

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

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

3.1.15
code explicite
code de mesure de sécurité réellement transmis dans le SPDU et connu de l'émetteur et du destinataire

3.1.16
défaillance
cessation de l'aptitude d'une unité fonctionnelle à accomplir une fonction requise ou à fonctionner comme prévu

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

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

3.1.17
anomalie
condition anormale qui peut entraîner une réduction de capacité ou la perte de capacité d'une unité fonctionnelle à accomplir une fonction requise

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

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

3.1.18
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

3.1.19
système de bus de terrain
système qui utilise un *bus de terrain* avec des appareils reliés

3.1.20
DLPDU
DÉCONSEILLÉ: trame
Data Link Protocol Data Unit (Unité de données de protocole de liaison de données)

3.1.21
Séquence de contrôle de trame
FCS
données redondantes issues d'un bloc de données d'une DLPDU (trame), qui utilisent une fonction de hachage et enregistrées ou transmises avec le bloc de données, afin de déterminer l'altération des données

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

Note 2 à l'article: Voir également [28], [29].

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

3.1.22
fonction de hachage
fonction (mathématique) de mise en correspondance des valeurs d'un ensemble (éventuellement) très grand de valeurs en une plage de valeurs (habituellement) plus petite

Note 1 à l'article: Les fonctions de hachage peuvent être utilisées pour déterminer l'altération des données.

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

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

3.1.23
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

3.1.24
code implicite
code de mesure de sécurité qui n'est pas transmis dans le SPDU, mais qui est connu de l'émetteur et du destinataire

3.1.25
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

3.1.26
message
série ordonnée d'octets, destinée à véhiculer des informations

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

3.1.27
collecteur de messages
partie d'un *système de communication* destiné à recevoir des *messages*

[SOURCE: ISO/IEC 2382-16:1996, 16.02.03]

3.1.28
source de messages
partie d'un *système de communication* destiné à envoyer des *messages*

[SOURCE: ISO/IEC 2382-16:1996, 16.02.02]

3.1.29
déclenchement de nuisance
déclenchement parasite sans effet préjudiciable

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

3.1.30
niveau de performances
PL
niveau discret utilisé pour spécifier la capacité des parties relatives à la sécurité des systèmes de commande à accomplir une fonction de sécurité dans des conditions prévisibles

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

[SOURCE: ISO 13849-1:2015, 3.1.23, traduction française modifiée – amélioration]

3.1.31
très basse tension de protection
TBTP
circuit électrique dans lequel la tension ne peut pas dépasser 30 V eff. c.a., 42,4 V crête ou 60 V c.c. en conditions normales et en conditions de défaut isolé, sauf en conditions de défauts de terre dans d'autres circuits

Note 1 à l'article: Un circuit TBTP comprend un raccordement à un conducteur de protection. En l'absence de raccordement à un conducteur de protection, ou si une défaillance existe au niveau du raccordement, les tensions ne sont pas corrigées.

[SOURCE: IEC 61010-2-201:2013, 3.109, modifié – suppression de "circuit" dans le terme, et suppression de la seconde note à l'article]

3.1.32
redondance
existence de plusieurs moyens pour accomplir une fonction requise ou pour représenter des informations

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

3.1.33
date relative
date référencée par rapport à l'horloge locale d'une entité

Note 1 à l'article: En général, il n'y a pas de relation avec les horloges des autres entités.

[SOURCE: IEC 62280:2014, 3.1.43]

3.1.34
fiabilité
probabilité pour qu'un système automatisé puisse accomplir une fonction requise, dans des conditions données, pendant un intervalle de temps donné (t1, t2)

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

Note 2 à l'article: Le terme "fiabilité" est aussi employé pour désigner l'aptitude caractérisée par cette probabilité.

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

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

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

3.1.35
probabilité d'erreurs résiduelles
RP
probabilité de non-détection d'une erreur par les mesures de sécurité SCL

Note 1 à l'article: L'abréviation «RP» est dérivée du terme anglais développé correspondant «residual error probability».

3.1.36
taux d'erreurs résiduelles
taux statistique de défaut de détection d'erreurs par les mesures de sécurité SCL

3.1.37
risque
combinaison de la probabilité d'un dommage et de sa gravité

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

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

3.1.38
canal de communication de sécurité
SC
canal de communication qui débute au sommet de la SCL de la source et qui se termine au sommet de la SCL du collecteur

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

3.1.39
couche de communication de sécurité
SCL
couche de communication située au-dessus de la FAL qui comprend toutes les mesures supplémentaires nécessaires qui permettent d'assurer la transmission de données en toute sécurité conformément aux exigences de l'IEC 61508

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

3.1.40
connexion de sécurité
connexion qui utilise le protocole de sécurité pour des transactions de communications

3.1.41
données de sécurité
données transmises par un réseau de sécurité qui utilise un protocole de sécurité

Note 1 à l'article: La couche de communication de sécurité ne garantit pas la sécurité des données proprement dites, mais uniquement la transmission en toute sécurité de ces dernières.

3.1.42
appareil de sécurité
appareil conçu conformément à l'IEC 61508 et qui met en œuvre le profil de communication de sécurité fonctionnelle

3.1.43
très basse tension de sécurité
TBTS
circuit électrique dans lequel la tension ne peut pas dépasser 30 V eff. c.a., 42,4 V crête ou 60 V c.c. en conditions normales et en conditions de défaut isolé, y compris en conditions de défauts de terre dans d'autres circuits

[SOURCE: IEC 61010-2-201:2013, 3.110, modifié — suppression de "circuit" dans le terme, et suppression de la note à l'article]

3.1.44
fonction de sécurité
fonction à réaliser par un système E/E/PE relatif à la sécurité ou par un dispositif externe de réduction de risque, prévue pour assurer ou maintenir un état de sécurité de l'EUC par rapport à un événement dangereux spécifique

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

3.1.45
temps de réponse de la fonction de sécurité
temps écoulé dans le cas le plus défavorable à la suite de l'activation d'un capteur de sécurité relié à un bus de terrain, avant que ne soit atteint l'état de sécurité correspondant de ses actionneurs de sécurité, du fait d'erreurs ou de défaillances dans la fonction de sécurité

Note 1 à l'article: Ce concept, introduit en 5.2.4, est traité dans le cadre des profils de communication de sécurité fonctionnelle définis dans la présente partie.

3.1.46
niveau d'intégrité de sécurité
SIL
niveau discret (parmi quatre possibles) correspondant à une gamme de valeurs d'intégrité de sécurité, où le niveau 4 d'intégrité de sécurité possède le plus haut degré d'intégrité et le niveau 1 possède le plus bas

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

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

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

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

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

3.1.47
mesure de sécurité
mesure permettant de contrôler les *erreurs* de communication éventuelles, qui est conçue et mise en œuvre conformément aux exigences de l'IEC 61508

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

Note 2 à l'article: Les *erreurs* de communication et les mesures de sécurité associées sont détaillées en 5.3 et 5.4.

3.1.48
PDU de sécurité
SPDU
PDU transféré via le canal de communication de sécurité

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

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

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

3.1.49
application relative à la sécurité
programmes conçus conformément à l'IEC 61508 pour satisfaire aux exigences SIL de l'application

3.1.50
système relatif à la sécurité
système qui exécute les *fonctions de sécurité* conformément à l'IEC 61508

3.1.51
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

3.1.52
déclenchement parasite
déclenchement provoqué par le système de sécurité sans injonction du processus

3.1.53
horodatage
information temporelle incluse dans un *message*

3.1.54
répartition uniforme
loi de probabilité où toutes les valeurs d'un ensemble fini sont également susceptibles de se produire

Note 1 à l'article: Pour un champ de longueur de bit i, la probabilité d'occurrence d'une valeur de champ particulier est égale à 2^{-i} étant donné que la somme de toutes les probabilités d'occurrence est égale à 1.

3.1.55
canal blanc
système de communication défini dans lequel tous les éléments pertinents du matériel et des logiciels sont conçus, mis en œuvre et validés conformément à l'IEC 61508

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

3.1.56
données explicites
données qui sont transmises

3.1.57
données implicites
données additionnelles qui ne sont pas transmises, mais sont connues de l'émetteur et du récepteur

[SOURCE: IEC 62280:2014, 3.1.25]

3.2 Symboles et abréviations

3.2.1 Abréviations

BSC	Binary Symmetric Channel (Canal symétrique binaire)	
Code A	Code d'authenticité	
Code T	Code d'opportunité	
CP	Communication Profile (Profil de communication)	[IEC 61784-1]
CPF	Communication Profile Family (Famille de profils de communication)	[IEC 61784-1]
CRC	Contrôle de redondance cyclique	
DLL	Data Link Layer (Couche de liaison de données)	[ISO/IEC 7498-1]
DLPDU	Data Link Protocol Data Unit (Unité de données de protocole de liaison de données)	
CEM	Compatibilité électromagnétique	
EMI	Electromagnetic Interference (Brouillage électromagnétique)	
EUC	Equipment Under Control (Equipement commandé)	[IEC 61508-4:2010]
E/E/PE	Electrique/électronique/électronique programmable	[IEC 61508-4:2010]
FAL	Fieldbus Application Layer (Couche d'application de bus de terrain)	[IEC 61158-5]
FCS	Frame Check Sequence (Séquence de contrôle de trame)	
FIT	Failure In Time (Intensité de défaillance) (équivaut à 10^{-9} de défaillance par heure)	
FS	Functional Safety (Sécurité fonctionnelle)	
FSCP	Functional Safety Communication Profile (Profil de communication de sécurité fonctionnelle)	
IACS	Industrial Automation and Control System (Automatisation Industrielle et système de commande)	
MTBF	Mean Time Between Failures (Temps moyen de bon fonctionnement)	
MTTF	Mean Time To Failure (Durée moyenne de fonctionnement avant défaillance)	
NSR	Non Safety Related (Non relatif à la sécurité)	
PDU	Protocol Data Unit (Unité de données de protocole)	[ISO/IEC 7498-1]
TBTP	Très basse tension de protection	
PES	Programmable Electronic System (Système électronique programmable)	[IEC 61508-4:2010]
PFD_{avg}	Probabilité moyenne de défaillance dangereuse en cas de sollicitation	[IEC 61508-4:2010]
PFH	Fréquence moyenne de défaillance dangereuse [h^{-1}] par heure	[IEC 61508-4:2010]
PhL	Couche physique	[ISO/IEC 7498-1]
PL	Niveau de performances	[ISO 13849-1]
PLC	Programmable Logic Controller (Automate programmable)	
SCL	Safety Communication Layer (Couche de communication de sécurité)	
TBTS	Très basse tension de sécurité	

SIS	Safety Instrumented Systems (Systèmes de sécurité instrumentés)	
SL	Security Level (Niveau de sécurité)	[IEC 62443]
SMS	Security Management System (Système de gestion de sécurité)	[IEC 62443]
SPDU	Safety PDU (PDU de sécurité)	
SR	Safety Related (Relatif à la sécurité)	

3.2.2 Symboles

A_k	Répartition du poids du code: nombre de mots de code valides à k bits définis sur "un"
e	Longueur binaire des données explicites
err_{impl}	Disjonction bit à bit de $impl_S$ et $impl_R$
expl	Données explicites
$expl_R$	Données explicites côté récepteur
$expl_S$	Données explicites côté émetteur
FCS_C	Séquence de contrôle de trame calculée au niveau du récepteur
FCS_R	Séquence de contrôle de trame reçue
FCS_S	Séquence de contrôle de trame émise
i	Longueur binaire des données implicites
ID	Remise incorrecte (*Incorrect Delivery*)
$impl_R$	Données implicites côté récepteur
$impl_S$	Données implicites côté émetteur
n	Longueur binaire du SPDU
P_e	Probabilité d'erreurs sur les éléments binaires
P_{ID}	Probabilité de remise incorrecte
r	Longueur binaire de la FCS (degré de polynôme générateur)
RP	Probabilité d'erreurs résiduelles

4 Conformité

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

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

une conformité à l'IEC 61784-3:20xx FSCP n/m <Type>

ou

une conformité à l'IEC 61784-3 (Ed.3.0) FSCP n/m <Type>

où le Type entre les crochets obliques < > est facultatif et les crochets obliques ne doivent pas être inclus.

En variante, une déclaration de conformité peut être présentée comme

une conformité à l'IEC 61784-3-N:20xx

ou

une conformité à l'IEC 61784-3-N (Ed.3.0)

où N est le numéro de famille attribué à la CPF correspondante.

La conformité à une partie IEC 61784-3-N implique que toutes les exigences obligatoires des FSCP correspondants applicables à l'appareil, au système ou à l'application spécifiques 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

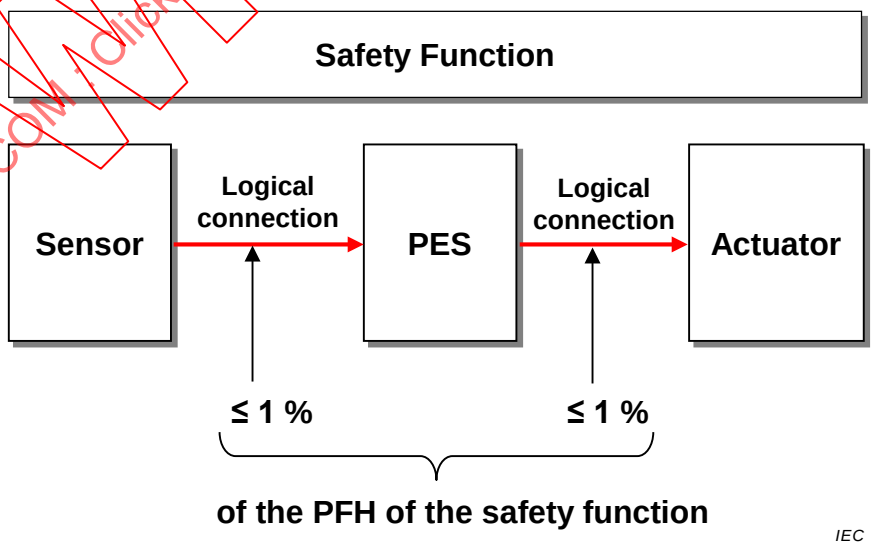
5.1 Décomposition d'une fonction de sécurité

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

Le système de communication proprement dit, défini dans la présente norme, transmet les données de sécurité. Pour simplifier les calculs de système, il est recommandé qu'une connexion logique aux canaux de communication de sécurité d'une fonction de sécurité ne consomme pas plus de 1 % de la PFH ou de la PFD_{avg} maximale du SIL cible pour lequel le profil de communication de sécurité fonctionnelle est conçu (voir la Figure 4 et 5.8.2).

Si cette valeur de 1 % pour une connexion logique ne peut pas être garantie par un FSCP donné, le manuel de sécurité de ce FSCP doit fournir des lignes directrices supplémentaires sur les calculs de la PFH ou de la PFD_{avg}.

La PFH et la PFD_{avg} globales de chaque appareil de sécurité doivent comprendre la PFH et la PFD_{avg} de la connexion logique. La PFD_{avg} doit être fournie si le FSCP est également utilisé pour les applications en mode à faible sollicitation conformes à l'IEC 61508.



Anglais	Français
Safety function	Fonction de sécurité
Sensor	Capteur