IEC 61784-3

Edition 3.0 2016-05
REDLINE VERSION

INTERNATIONAL STANDARD

colour
inside

Withdrawn

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

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

IEC 61784-3:2016-05 RLV(en)

THIS PUBLICATION IS COPYRIGHT PROTECTED
Copyright © 2016 IEC, Geneva, Switzerland

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

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 It also gives information on projects, replaced and withdrawn publications.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 15 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

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

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

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

IEC 61784-3

Edition 3.0 2016-05
REDLINE VERSION

INTERNATIONAL STANDARD

colour
inside

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

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 25.040.40; 35.100.05 ISBN 978-2-8322-3372-6

Warning! Make sure that you obtained this publication from an authorized distributor.

® Registered trademark of the International Electrotechnical Commission

CONTENTS

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV
Withdrawn

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV
Withdrawn

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

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 redline version of the official IEC Standard allows the user to identify the changes made to the previous edition. A vertical bar appears in the margin wherever a change has been made. Additions are in green text, deletions are in strikethrough red text.

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

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 cancels and replaces the second edition published in 2010. This 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.

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

FDIS	Report on voting
65C/840/FDIS	65C/848/RVD

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

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

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

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC website 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.

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV
Withdrawn

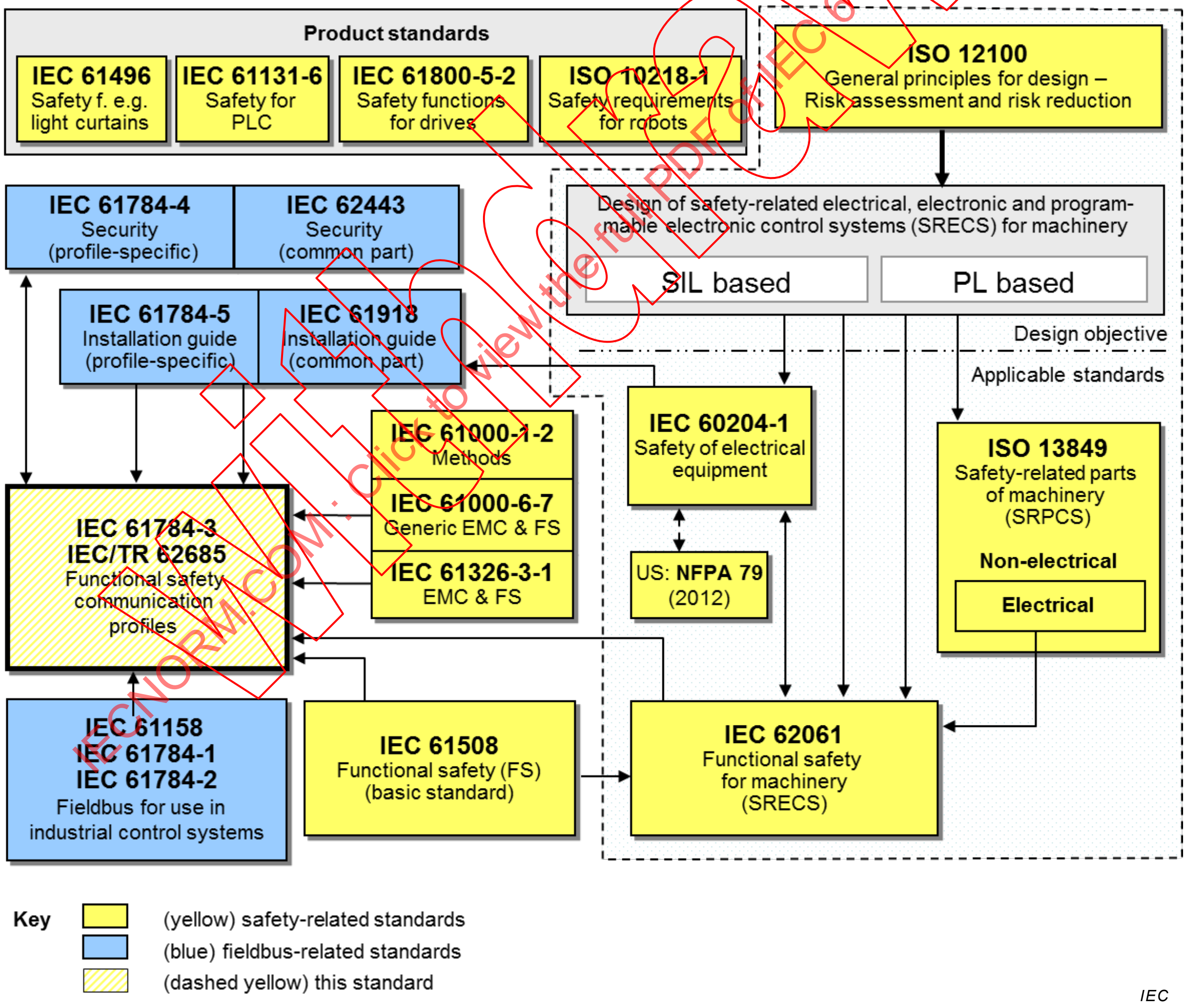
0 Introduction

0.1 General

The IEC 61158 fieldbus standard together with its companion standards IEC 61784-1 and IEC 61784-2 defines a set of communication protocols that enable distributed control of automation applications. Fieldbus technology is now considered well accepted and well proven. Thus ~~many~~ fieldbus enhancements ~~are emerging~~ continue to emerge, addressing ~~not yet standardized~~ 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.

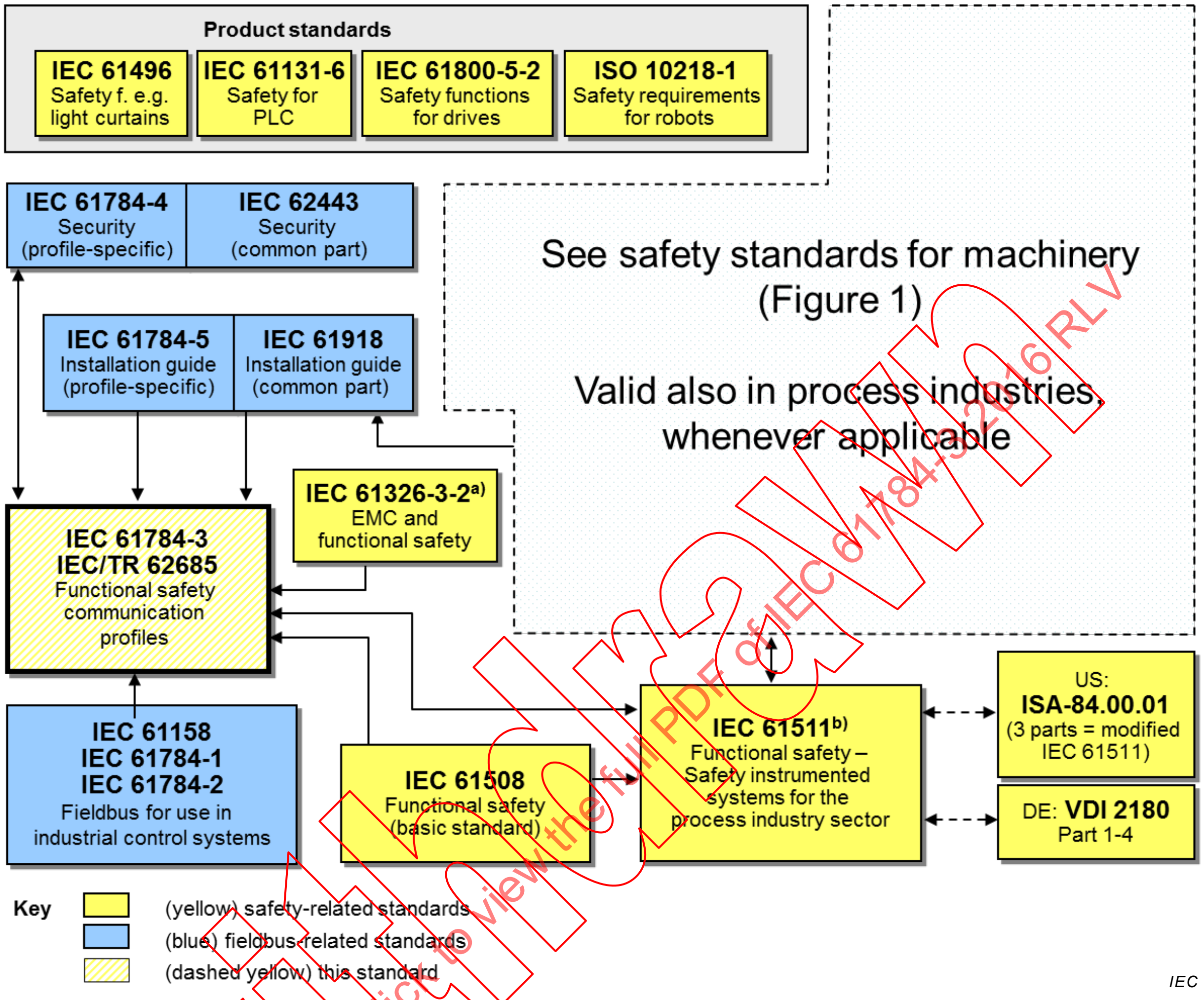

Product standards
IEC 61496 Safety f. e.g. light curtains
IEC 61131-6 Safety for PLC
IEC 61800-5-2 Safety functions for drives
ISO 10218-1 Safety requirements for robots
ISO 12100 General principles for design – Risk assessment and risk reduction
IEC 61784-4 Security (profile-specific)
IEC 62443 Security (common part)
Design of safety-related electrical, electronic and programmable electronic control systems (SRECS) for machinery
SIL based
PL based
Design objective
Applicable standards
IEC 61784-5 Installation guide (profile-specific)
IEC 61918 Installation guide (common part)
IEC 61000-1-2 Methods
IEC 61000-6-7 Generic EMC & FS
IEC 61326-3-1 EMC & FS
IEC 60204-1 Safety of electrical equipment
US: NFPA 79 (2012)
ISO 13849 Safety-related parts of machinery (SRPCS)
Non-electrical
Electrical
IEC 61784-3 IEC/TR 62685 Functional safety communication profiles
IEC 61158 IEC 61784-1 IEC 61784-2 Fieldbus for use in industrial control systems
IEC 61508 Functional safety (FS) (basic standard)
IEC 62061 Functional safety for machinery (SRECS)
Key
(yellow) safety-related standards
(blue) fieldbus-related standards
(dashed yellow) this standard
IEC

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

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.


Product standards
IEC 61496 Safety f. e.g. light curtains
IEC 61131-6 Safety for PLC
IEC 61800-5-2 Safety functions for drives
ISO 10218-1 Safety requirements for robots
IEC 61784-4 Security (profile-specific)
IEC 62443 Security (common part)
See safety standards for machinery (Figure 1)
Valid also in process industries, whenever applicable
IEC 61784-5 Installation guide (profile-specific)
IEC 61918 Installation guide (common part)
IEC 61326-3-2a) EMC and functional safety
IEC 61784-3
IEC/TR 62685
Functional safety communication profiles
IEC 61158
IEC 61784-1
IEC 61784-2
Fieldbus for use in industrial control systems
IEC 61508 Functional safety (basic standard)
IEC 61511b) Functional safety – Safety instrumented systems for the process industry sector
US: ISA-84.00.01 (3 parts = modified IEC 61511)
DE: VDI 2180 Part 1-4
Key
(yellow) safety-related standards
(blue) fieldbus-related standards
(dashed yellow) this standard
IEC

[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)

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

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;
- ~~individual description of~~ 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.

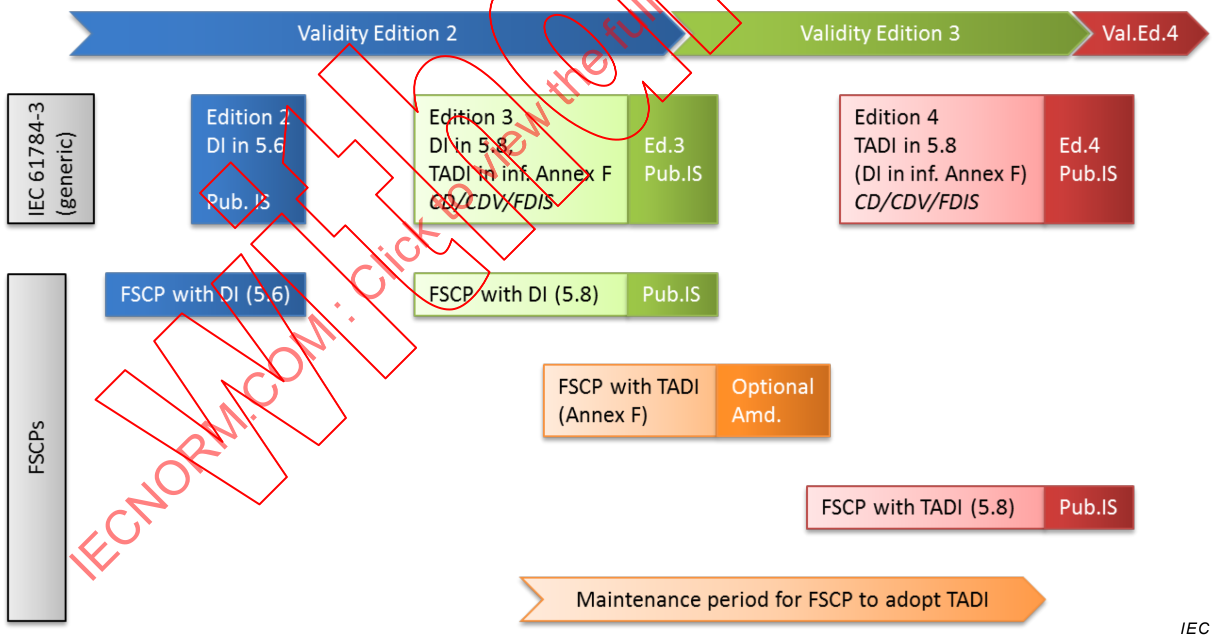
0.2 Transition from Edition 2 to extended assessment methods in Edition 3

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

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV
Withdrawn

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.

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

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 ~~may~~ 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 ~~may~~ can also be specified in IEC 61784-4[3] ~~[10]~~.

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

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

2 Normative references

The following 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.

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

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

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

IEC 61326-3-1, *Electrical equipment for measurement, control and laboratory use – EMC requirements – Part 3-1: Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety) – General industrial applications*

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

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

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

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

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

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

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

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

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

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

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

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

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

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

[4] ~~To be published.~~

~~[5] To be published.~~

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

IEC 61784-3-17[6], *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~~ – Installation profiles for CPF x~~*

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

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

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

3 Terms, definitions, symbols, abbreviated terms and conventions

3.1 Terms and definitions

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

~~**3.1.1 Common terms and definitions**~~

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~~-2~~: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

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

[6] To be published

3.1.5
black channel

defined communication~~ *channel*~~ *system containing one or more elements* without~~ available~~ evidence of design or validation according to IEC 61508

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

3.1.6
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]~~, [30]~~[7].

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

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

Withdrawn

IECNORM.COM: Click to view the full PDF of IEC 61784-3:2016 RLV

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~~[8]~~]

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]~~, [IEC 61158]~~

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

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]~~,~~ ~~[ISO/IEC 2382-14.01.11, modified]~~

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]~~,~~ ~~[ISO/IEC 2382-14.01.10, modified]~~

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

~~[8] To be published.~~

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

3.1.20
DLPDU
DEPRECATED: frame
~~denigrated synonym for DLPDU~~

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]~~, [30]~~.

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

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

[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 ~~is similar to an SELV circuit that is connected~~ 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 ~~61131-2~~ 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 means, in addition to the means which would be sufficient for a functional unit to perform a required function or for data to represent information~~
existence of more than one means for performing a required function or for representing information

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

[SOURCE: IEC 61508-4:2010, 3.4.6, modified – example and notes deleted]~~,~~ ~~[ISO/IEC 2382-14.01.12, modified]~~

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~~-2~~:2014~~, modified~~, 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.

Withdrawn
IECNORM.COM: Click to view the full PDF of IEC 61784-3:2016 RLV

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~~[9]~~.

[SOURCE: IEC 61508-4:2010, 3.1.6, and ISO/IEC Guide 51:~~1999~~ 2014, definition ~~3.2~~ 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 ~~the~~ 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.

Withdrawn

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

~~[9] To be published.~~

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

~~NOTE An SELV circuit is not connected to protective earth.~~

[SOURCE: IEC ~~61131-2~~ 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

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

[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, ~~before~~ until the corresponding safe state of its safety actuator(s) is achieved in the presence of errors or failures in the safety function ~~channel~~

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~~[10]~~.

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]

withdrawn

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

~~[10] To be published.~~

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

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

Note 2 to entry: Communication *errors* and related safety measures are detailed in 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 ~~*channel*~~ *system* in which all relevant hardware and software ~~components~~ 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.

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

~~3.1.2 CPF 1: Additional terms and definitions~~

~~None required for this part.~~

~~3.1.3 CPF 2: Additional terms and definitions~~

~~None required for this part.~~

~~3.1.4 CPF 3: Additional terms and definitions~~

~~None required for this part.~~

~~3.1.5 CPF 6: Additional terms and definitions~~

~~None required for this part.~~

~~3.1.6 CPF 8: Additional terms and definitions~~

~~None required for this part.~~

~~3.1.7 CPF 12: Additional terms and definitions~~

~~None required for this part.~~

~~3.1.8 CPF 13: Additional terms and definitions~~

~~None required for this part.~~

~~3.1.9 CPF 14: Additional terms and definitions~~

~~None required for this part.~~

3.2 Symbols and abbreviated terms

~~3.2.1 Common symbols and abbreviated terms~~

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	

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

MTTF	Mean Time To Failure	
NSR	Non Safety ~~Relevant~~ 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 ~~61508-6~~ 61508-4:2010~~[11]~~]
PFH	Average frequency of dangerous failure [h^{-1}] per hour	[IEC ~~61508-6~~ 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	
~~SIL~~	~~Safety Integrity Level~~	~~[IEC 61508-4:2010]~~
SL	Security Level	[IEC 62443]
SMS	Security Management System	[IEC 62443]
SPDU	Safety PDU	
SR	Safety ~~Relevant~~ Related	

~~3.2.2 CPF 1: Additional symbols and abbreviated terms~~

~~SIS~~	~~Safety Instrumented Systems~~

~~3.2.3 CPF 2: Additional symbols and abbreviated terms~~

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

~~3.2.4 CPF 3: Additional symbols and abbreviated terms~~

~~DP~~	~~Decentralized Peripherals~~

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

~~None required for this part.~~

~~3.2.6 CPF 8: Additional symbols and abbreviated terms~~

~~ASE~~	~~Application Service Element~~
~~SASE~~	~~Safety Application Service Element~~

~~3.2.7 CPF 12: Additional symbols and abbreviated terms~~

~~FSoE~~	~~Failsafe over CPF 12~~

~~3.2.8 CPF 13: Additional symbols and abbreviated terms~~

~~None required for this part.~~

~~[11] To be published.~~

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV
Withdrawn

~~3.2.9 CPF 14: Additional symbols and abbreviated terms~~

~~IP~~	~~Internet Protocol~~
~~UDP~~	~~User Datagram Protocol~~

4 Conformance

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

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

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

or

conformance to IEC 61784-3 (Ed.~~2.0~~ 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.~~2.0~~ 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 ~~highly~~ recommended that ~~the~~ one logical connection of safety communication channels of a safety function does not consume more than 1 % of the maximum ~~PFD or PFH~~ PFH or PFD_{avg} of the target SIL for which the functional safety communication profile is designed (see Figure 4 and 5.8.2).

~~EXAMPLE~~

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

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}.

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

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.

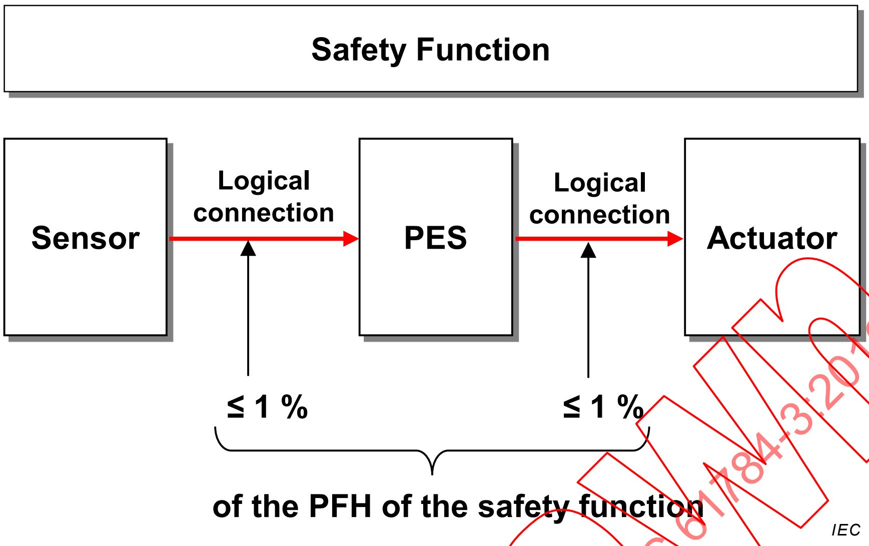


Figure 4 – Safety communication as a part of a safety function

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.

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

5.2.2 IEC 61158 fieldbuses

While IEC 61508 is not restricting the use of communication technologies, this standard focuses on the use of fieldbus based functional safety communication systems. Figure 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.

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV
Withdrawn

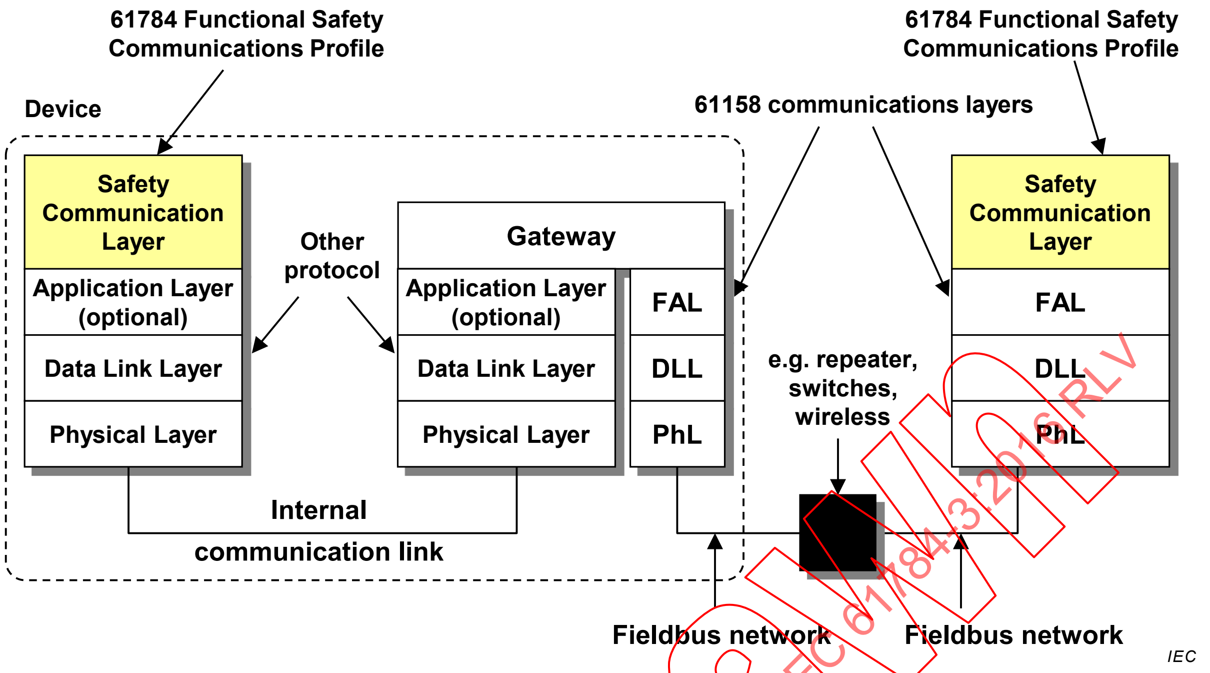

61784 Functional Safety Communications Profile
Device
Safety Communication Layer
Application Layer (optional)
Data Link Layer
Physical Layer
Other protocol
Gateway
Application Layer (optional)
Data Link Layer
Physical Layer
FAL
DLL
PhL
Internal communication link
61158 communications layers
61784 Functional Safety Communications Profile
e.g. repeater, switches, wireless
Safety Communication Layer
FAL
DLL
PhL
Fieldbus network
Fieldbus network
IEC

Figure 5 – Example model of a functional safety communication system

~~NOTE 1~~ While implementation of the Fieldbus Application Layer (FAL) is required~~, while the AL~~ 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).

~~NOTE 2~~ Functions~~ of the user layer~~ 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.~~ Whether a communication channel is white or black is determined by where the safety measures are accomplished with respect to the base fieldbus.~~ This standard specifies functional safety communication profiles that use the black channel approach.

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

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.

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

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

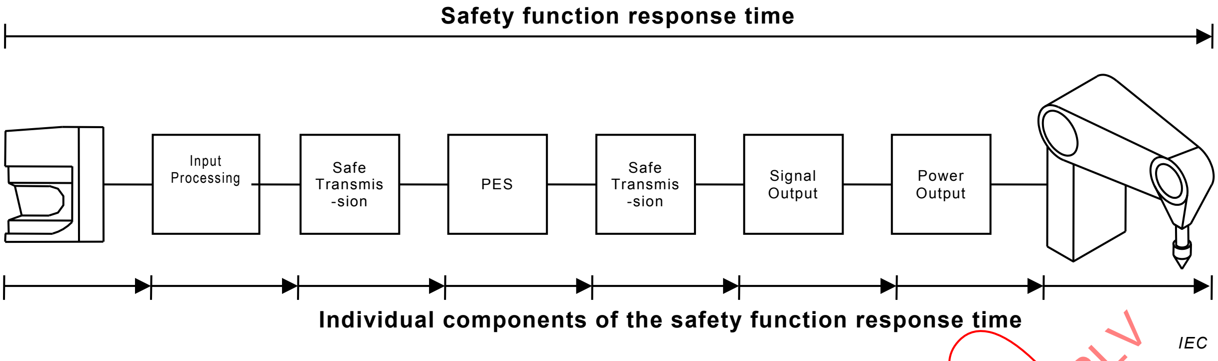

Safety function response time
Input Processing
Safe Transmis-sion
PES
Safe Transmis-sion
Signal Output
Power Output
Individual components of the safety function response time
IEC

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 ~~should~~ 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 ~~may~~ 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, ~~old not updated~~ messages are repeated ~~at an incorrect point in time~~.

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

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

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

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV
Withdrawn

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 ~~may~~ can contain elements that store messages (for example FIFOs in switches, bridges, routers) or ~~may~~ use protocols that ~~may~~ 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 ~~may~~ can be reported for each sequence.

5.3.5 Loss

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

5.3.6 Unacceptable delay

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

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

~~a) immediate repetition;~~

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

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

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

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

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

5.3.7 Insertion

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

NOTE Communication systems used for safety-related applications ~~may~~ 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 ~~relevant~~ related message is ~~sent~~ delivered to the ~~wrong~~ incorrect safety ~~relevant~~ related participant, which then treats reception as correct. This

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

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 ~~1~~ Relative time stamps and absolute time stamps ~~may~~ can be used.

~~NOTE 2~~ Time stamping ~~implicitly~~ requires the time base to be synchronized. For safety applications, synchronization ~~needs to~~ 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 ~~shall~~ 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 ~~relevant~~ 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 ~~may~~ can contain for example only a short acknowledge, or ~~may~~ can also contain the original data, or other information enabling the source to check the correct reception.

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV
Withdrawn

5.4.7 Data integrity assurance

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

NOTE Communication systems used for safety-related applications ~~may~~ 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 ~~relevant~~ related (SR) and non-safety ~~relevant~~ 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.

~~NOTE~~ 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. ~~This relationship is~~ 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.

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

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

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~~-2~~:2014 ~~[15] and [28]~~, 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.

IECNORM.COM: Click to view the full PDF of IEC 61784-3:2016 RLV

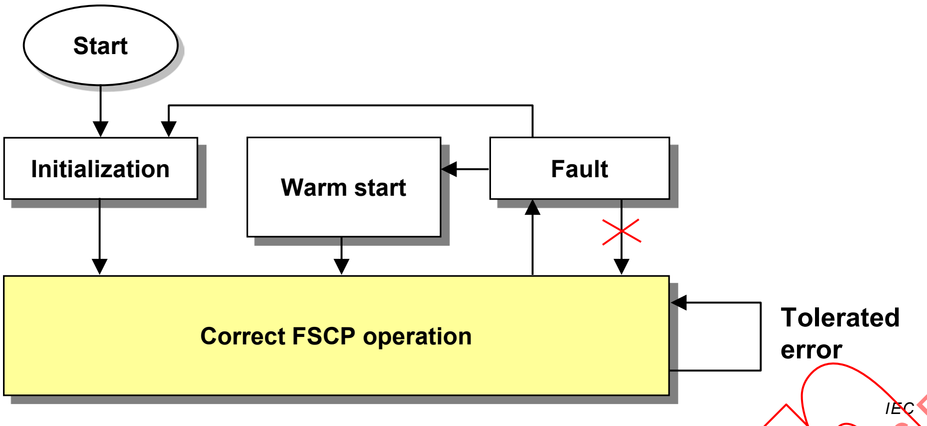


Figure 7 – Conceptual FSCP protocol model

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).

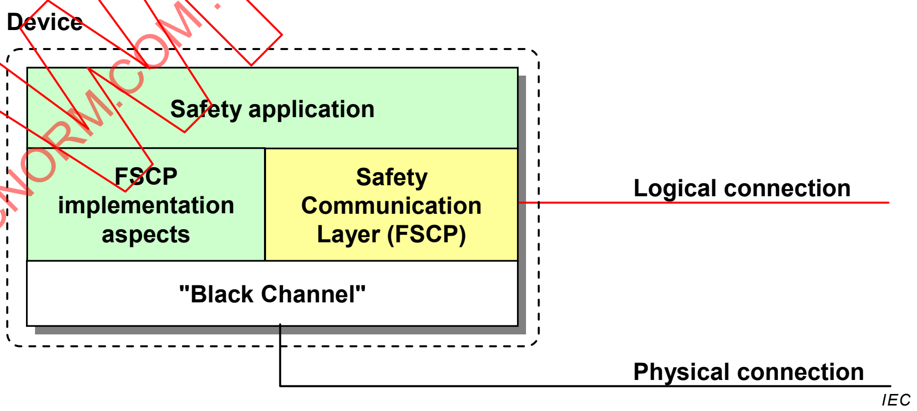


Figure 8 – FSCP implementation aspects

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV
Withdrawn

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

~~NOTE 1~~ EXAMPLE When CRC is used as the hash function, the ~~communication channel~~ 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 ~~transmission rate of safety messages~~ sample rate of SPDUs. In ~~addition~~ 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_{SL}~~ 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.

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

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

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

NOTE ~~2~~ These equations assume cyclic ~~transmission of safety messages~~ sampling of SPDUs by the SCL.

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

Withdrawn

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

Equation items	Definition
~~A_{SL}~~ λ_{SC} (Pe)	Residual error rate per hour of the safety communication ~~layer~~ 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). ~~Unless a better error probability can be proven, a value of 10^{-2} shall be used~~ ~~[a]~~
~~R_{SL}~~ R_{SC} (Pe)	Residual error probability of the safety ~~message~~ communication channel with respect to the bit error probability (see 3.1.35)
v	Maximum ~~number of safety messages~~ sample rate of SPDUs per hour
m	Maximum number of ~~information sinks that is permitted in a single safety function (see Figure 6)~~ logical connections that is permitted in a single safety function (see Figure 9 and Figure 10)

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

~~The design of a safety layer cannot be based on such an assumption, as single burst interferences with many perturbed bits are common in industrial environments.~~

~~In order to detect these kind of disturbances, the error detection mechanisms shall be powerful enough to achieve the required Residual Error Probability RSL (Pe) at a 100 times higher Pe, that is 10^{-2}.~~

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.

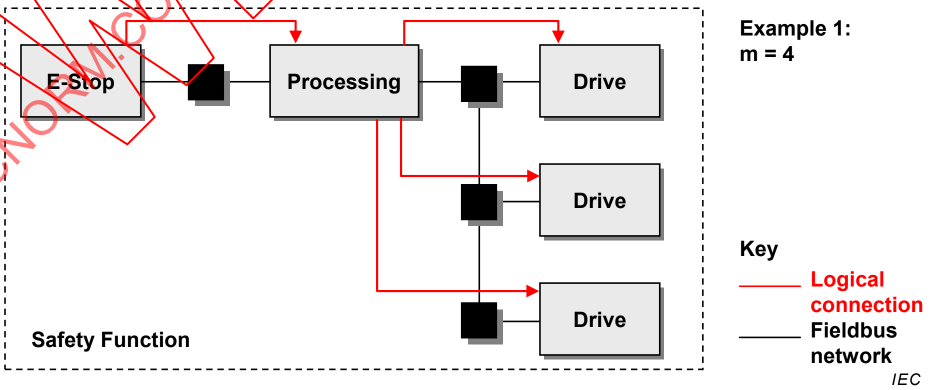


Figure 9 – Example application 1 (m=4)

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.

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

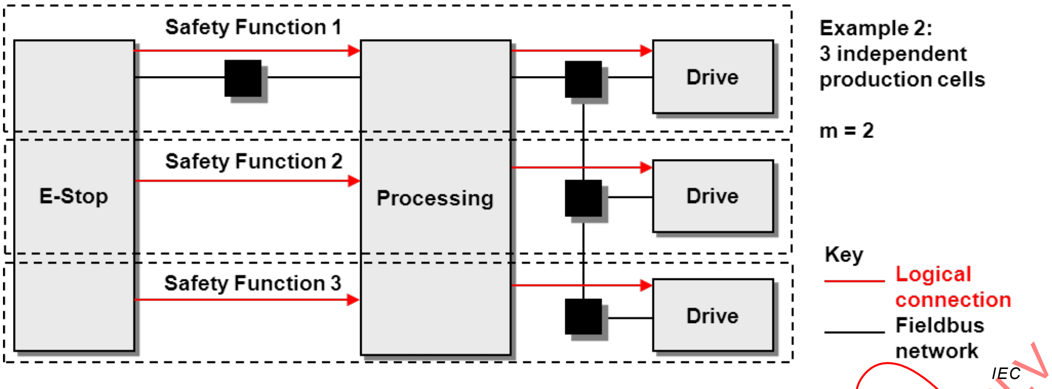


Figure 10 – Example application 2 (m = 2)

5.8.2 Total residual error rate and SIL

A functional safety communication system shall provide a residual error rate ~~as specified in Table 3~~ 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 ~~number of safety messages per second~~ rate of SPDUs shall be guaranteed. ~~The calculation of the error rate is based on high demand mode, and is therefore also applicable to the low demand mode.~~ 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 ~~level~~

Applicable for safety functions up to SIL	~~Probability of a dangerous failure per hour for the functional safety communication system~~ Average frequency of a dangerous failure for the safety function (PFH)	Maximum permissible residual error rate for ~~the functional safety communication system~~ one logical connection of the safety function (λ_{SC} (Pe))
4	< 10~~$^{-10}$~~$^{-8}$/h	~~Λ~~ < 10^{-10}/h
3	< 10~~$^{-9}$~~$^{-7}$/h	~~Λ~~ < 10^{-9}/h
2	< 10~~$^{-8}$~~$^{-6}$/h	~~Λ~~ < 10^{-8}/h
1	< 10~~$^{-7}$~~$^{-5}$/h	~~Λ~~ < 10^{-7}/h
~~NOTE Values in this table are based on the assumption that the functional safety communication system contributes no more than 1 % of the total failures of the safety function.~~		

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}

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV
Withdrawn

5.9 Relationship between functional safety and security

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

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

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

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

Withdrawn IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

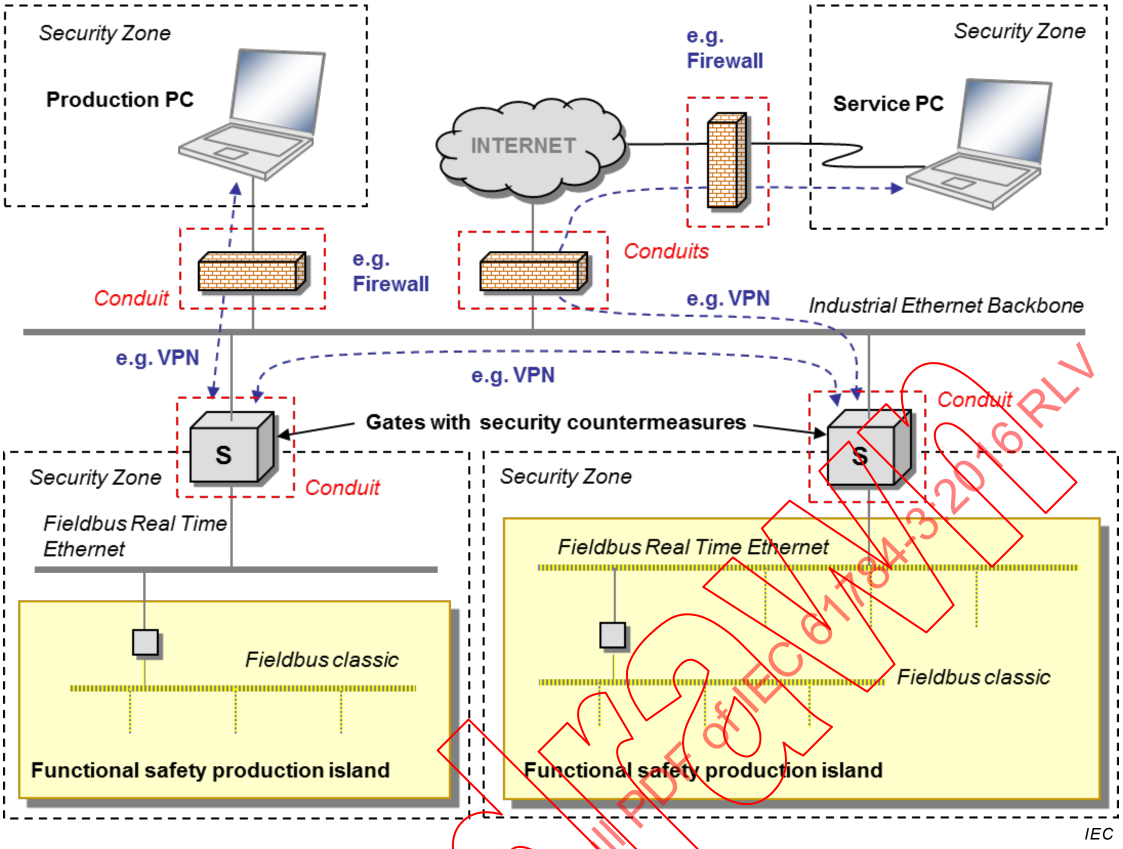


Figure 11 – Zones and conduits concept for security according to IEC 62443

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 ~~SELV/PELV IEC specifications (for example IEC 61131-2)~~ 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)

~~IEC 61508 requires "Increase of interference immunity", but does not specify how to achieve this. Functional safety communication profiles in this standard will use for that purpose the increased test levels and corresponding performance criteria specified in IEC 61326-3-1.~~ 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 ~~may~~ can require higher levels than those specified in IEC 61326-3-1, according to Safety Requirements Specification (SRS).

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

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 ~~may~~ can be provided in the technology-specific parts of ~~this standard~~ 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. ~~Information about test laboratories which can provide conformance tests and validations in accordance with the requirements in this clause can be found in Annex B of each individual profile part.~~

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

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

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

~~6.1 Functional Safety Communication Profile 1/1~~

Communication Profile Family 1 (commonly known as FOUNDATION™ Fieldbus[12]) 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.

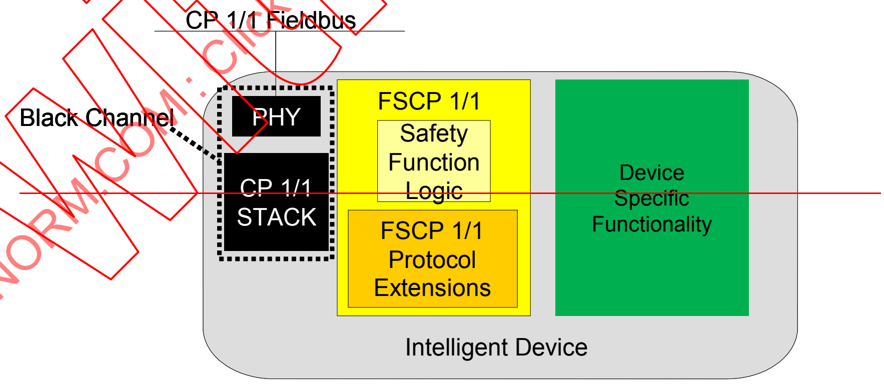
~~6.2 Technical overview~~

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

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

~~The FSCP 1/1 safety communication layer specified in IEC 61784-3-1 makes it possible to use intelligent devices in a safety-related system adding more capability to the system, yet the system can meet its safety integrity level requirements. The safety communication layer specified in IEC 61784-3-1 is only applicable to CP 1/1 as described in IEC 61784-1.~~

~~IEC 61784-3-1 does not define requirements for engineering tools or internal measurement functionality of devices. The safety communication layer ensures that a configuration created using an engineering tool is downloaded into the safety devices without the protocol impacting the safety integrity level. The scope of IEC 61784-3-1 is defined in Figure 7.~~



~~Figure 7 – Scope of FSCP 1/1~~

~~FSCP 1/1 alone does not ensure functional safety. In addition to FSCP 1/1 protocol interoperability registration, the vendor will also obtain functional safety assessment for the~~

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV
Withdrawn

[12] 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).

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

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

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

~~7.1 Functional Safety Communication Profile 2/1~~

Communication Profile Family 2 (commonly known as CIP™[13]) 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®[14]) 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.

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.

~~7.2 Technical overview~~

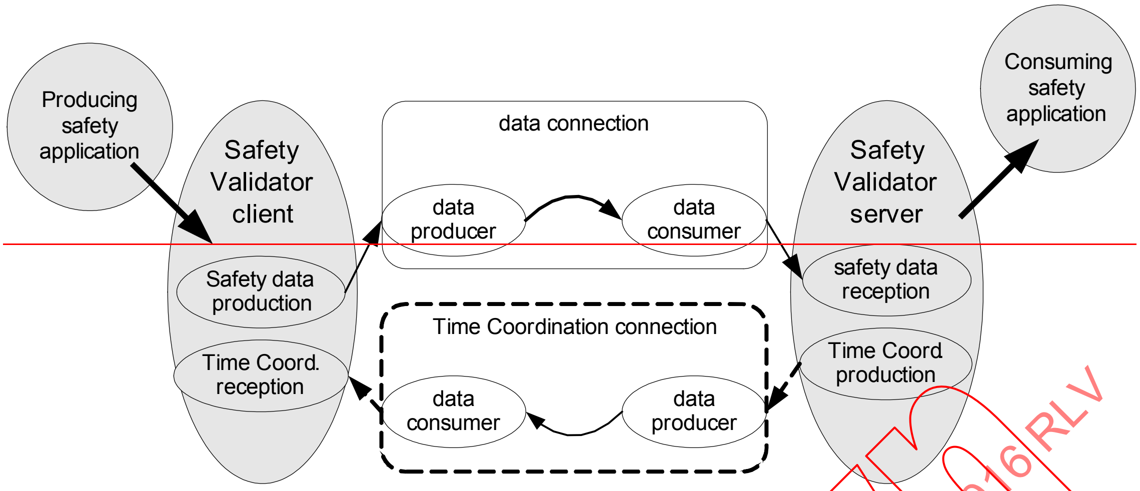
~~FSCP 2/1 is based on the producer/consumer model of CPF 2. The pairing of producers and consumers is an important part of the relationship that provides the high integrity needed for safety-related applications.~~

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

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV
Withdrawn

[13] 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).

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



~~**Figure 8 – Relationship of Safety Validators**~~

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

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

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

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

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

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

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

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

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

~~8.1 Functional Safety Communication Profile 3/1~~

Communication Profile Family 3 (commonly known as PROFIBUS™, PROFINET™[15]) 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.

~~8.2 Technical overview~~

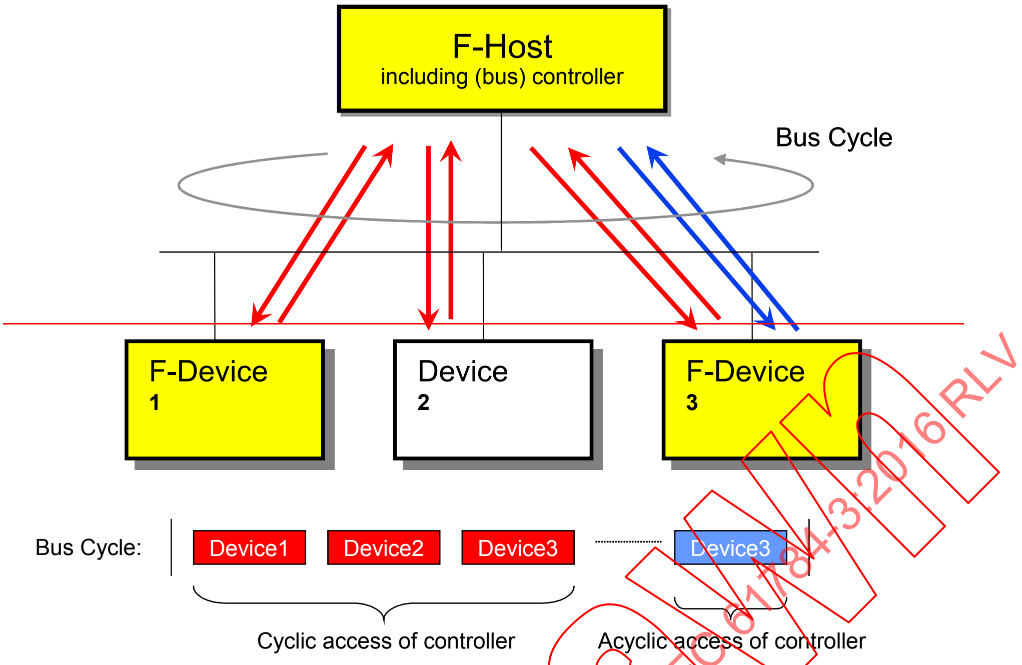
~~FSCP 3/1 is based on the cyclic data exchange of a (bus) controller with its associated (field) devices using a one-to-one communication relationship (Figure 9). One controller can operate any mix of standard and safety devices connected to the network. Assigning safety tasks and standard tasks to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

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

- ~~(virtual) consecutive numbering;~~
- ~~watchdog time monitoring with acknowledgement;~~
- ~~codename per communication relationship;~~
- ~~cyclic redundancy checking for data integrity.~~

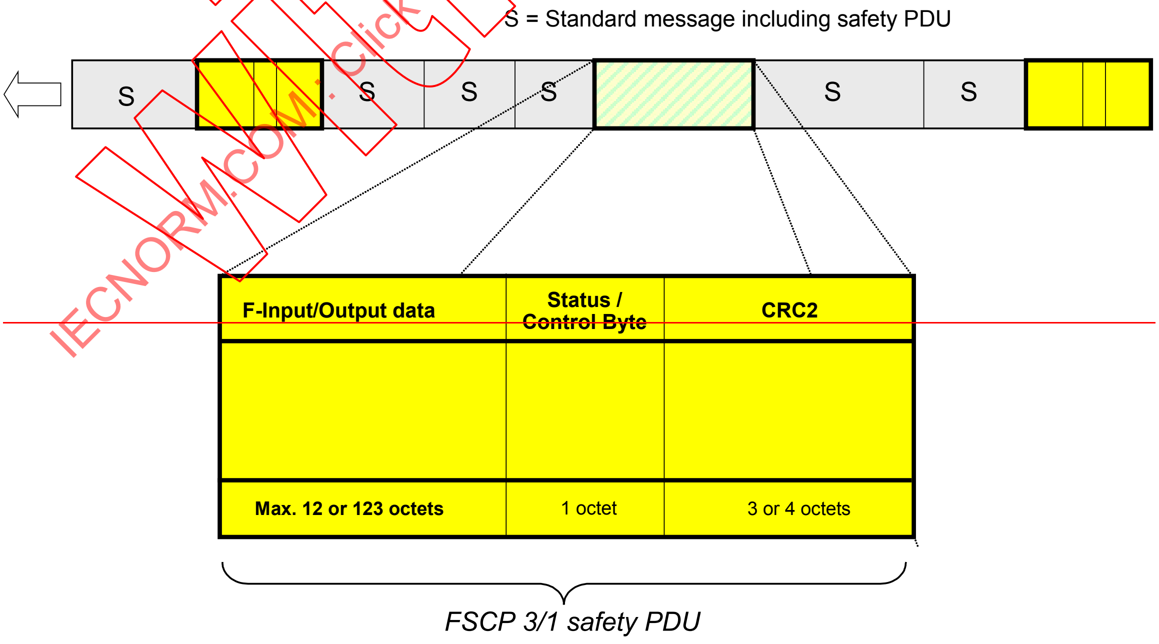
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV
Withdrawn

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


F-Host
including (bus) controller
Bus Cycle
F-Device
1
Device
2
F-Device
3
Bus Cycle:
Device1
Device2
Device3
Device3
Cyclic access of controller
Acyclic access of controller

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

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

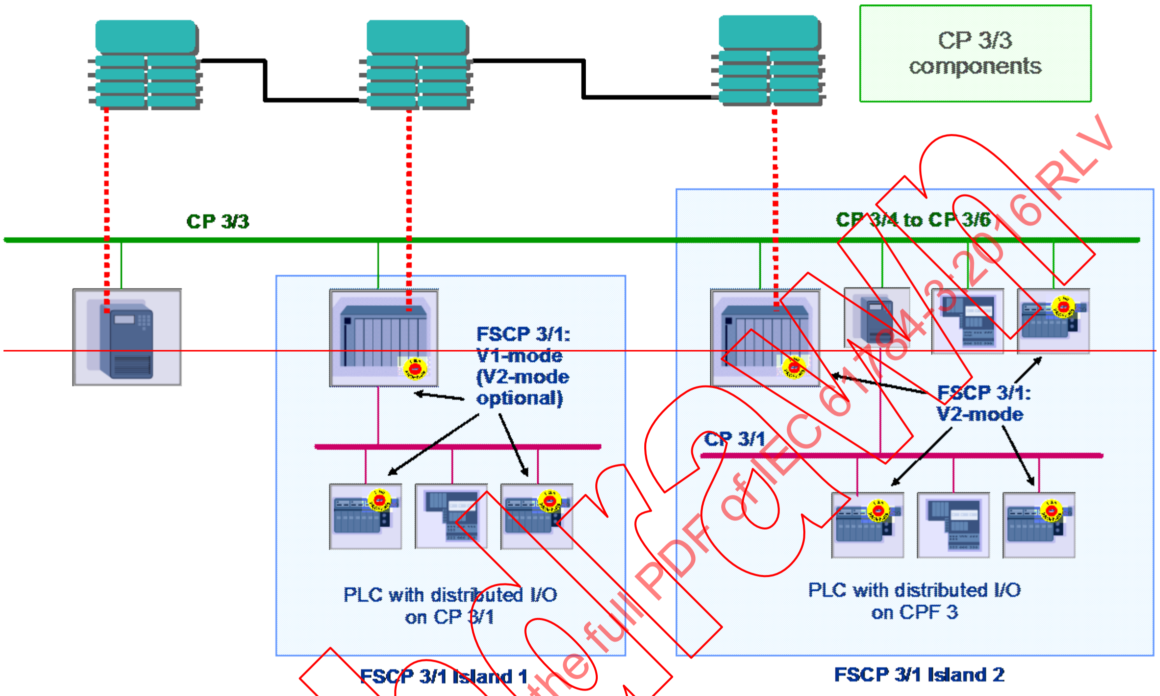


~~**Figure 10 – Structure of a FSCP 3/1 safety PDU**~~

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

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV
Withdrawn

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



~~Figure 11 – Safe communication modes~~

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

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

~~9.1 Functional Safety Communication Profile 6/7~~

Communication Profile Family 6 (commonly known as INTERBUS®[16]) 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.

[16] 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).

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

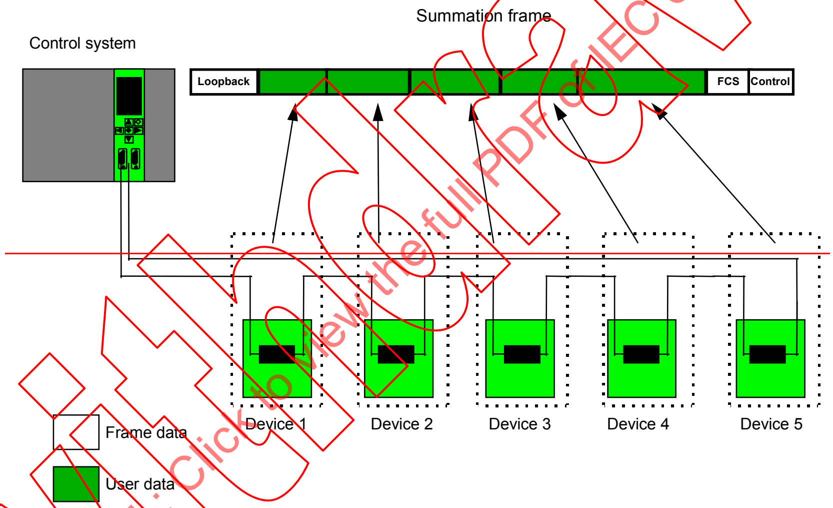
Table 5 – Overview of profile identifier usable for FSCP 6/7

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.

~~9.2 Technical overview~~

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



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

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

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

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

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

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV
Withdrawn

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

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

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

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

10.1 Functional Safety Communication Profile 8/1

Communication Profile Family 8 (commonly known as CC-Link™[17]) 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 ~~Technical overview~~ Functional Safety Communication Profile 8/2

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

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

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

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

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

[17] 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).

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™[18]) 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

~~11.1 Functional Safety Communication Profile 12/1~~

Communication Profile Family 12 (commonly known as EtherCAT™[19]) 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.

~~11.2 Technical overview~~

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

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

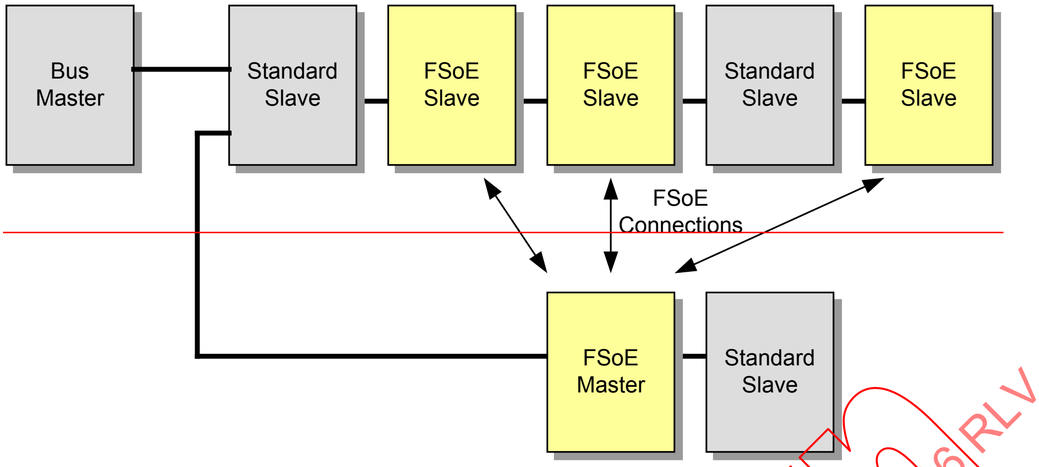
~~The FSoE Master can handle more than one FSoE Connection to support several FSoE Slaves.~~

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

Withdrawn

[18] 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).

[19] 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).



~~**Figure 13 – Basic FSCP 12/1 system**~~

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

- ~~session-number for detecting buffering of a complete startup sequence;~~
- ~~sequence number for detecting interchange, repetition, insertion or loss of whole messages;~~
- ~~unique connection identification for safely detecting misrouted messages via a unique address relationship;~~
- ~~watchdog monitoring for safely detecting of not allowed delays on the communication path;~~
- ~~cyclic redundancy checking for data integrity for detecting message corruption from source to sink.~~

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

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

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

~~12.1 Functional Safety Communication Profile 13/1~~

Communication Profile Family 13 (commonly known as Ethernet POWERLINK™[20]) 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™[20] ~~Ethernet POWERLINK safety[17]~~) is based on the CPF 13 basic profiles in IEC 61784-2 and the safety communication layer specifications defined in IEC 61784-3-13.

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV
Withdrawn

[20] 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).

~~12.2 Technical overview~~

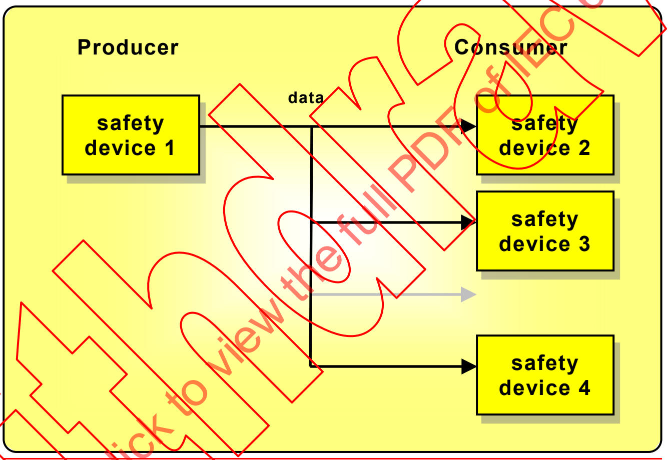
~~Functional Safety Communication Profile FSCP 13/1 is designed to provide fieldbus communication for functional safety applications in the microsecond range.~~

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

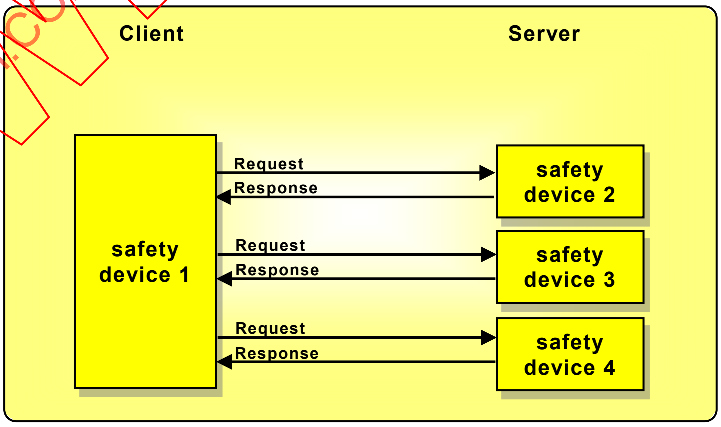
~~The following services are defined:~~

- ~~network configuration;~~
- ~~network management (booting, runtime diagnosis);~~
- ~~exchange of spontaneous data; and~~
- ~~exchange of synchronous data.~~

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



~~Figure 14 – Producer consumer example~~



~~Figure 15 – Client server example~~

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

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

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

~~13.1 Functional Safety Communication Profile 14/1~~

Communication Profile Family 14 (commonly known as EPA®[21]) 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.

~~13.2 Technical overview~~

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

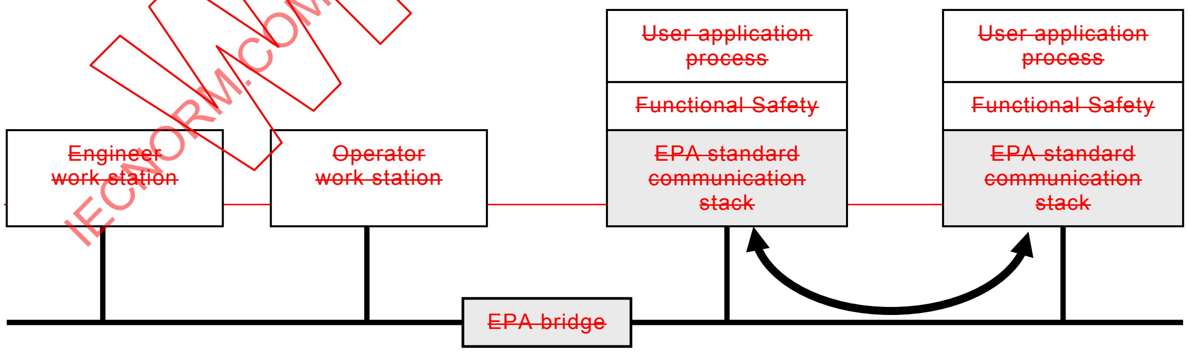
~~EPA communication is based on black channel principle as shown in Figure 16. Black channel includes non safety-relevant devices such as wires, fibre optics, repeater, barrier, power supplies, ASIC, communication stack, EPA bridge, interface. Communication stack includes the following layers: physical,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

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

- ~~random fault;~~
- ~~standard hardware failure/fault;~~
- ~~system failure caused by standard hardware or software components.~~

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

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV


~~User application process~~
~~Functional Safety~~
~~EPA standard communication stack~~
~~User application process~~
~~Functional Safety~~
~~EPA standard communication stack~~
~~Engineer work station~~
~~Operator work station~~
~~EPA bridge~~

~~Figure 16 – FSCP 14/1 safety communication architecture~~

[21] 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).

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

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

Communication Profile Family 17 (commonly known as RAPIEnet™[22]) 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.

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

Communication Profile Family 18 (commonly known as SafetyNET p™[23]) 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.

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

[22] 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).

[23] 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 ~~channel~~ fieldbus is ~~connected to~~ used as the ~~bus~~ communication channel.

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

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.

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

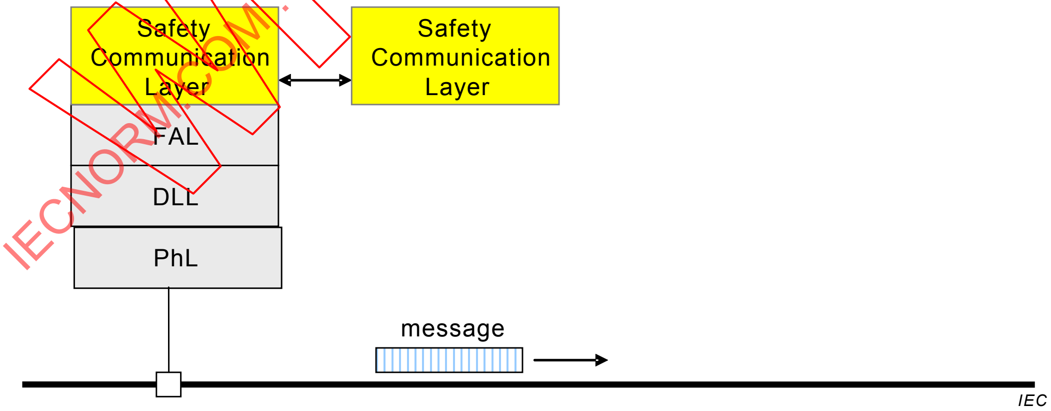


Figure A.1 – Model A

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.~~ If cross-checking shows discrepancy, an appropriate action is initiated to maintain safety.~~

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

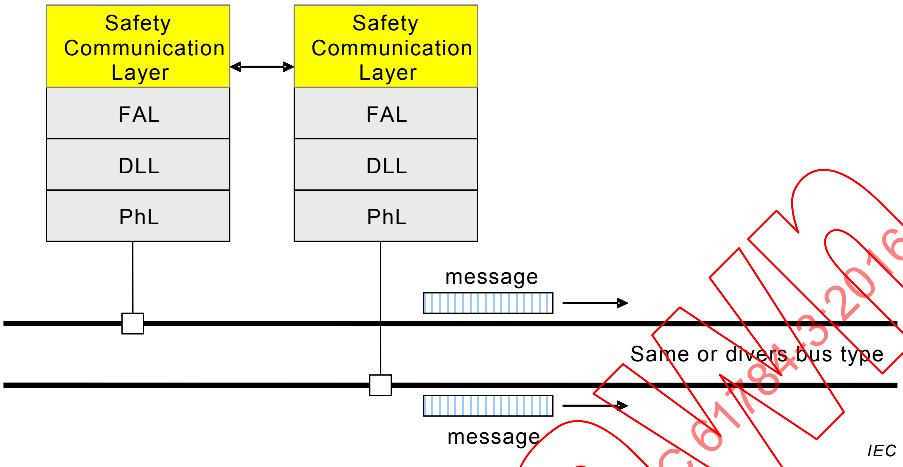


Figure A.2 – Model B

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

Model C in Figure A.3 shows a system with full redundancy ~~approach similar to Model B~~ 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.~~ If cross-checking shows discrepancy, an appropriate action is initiated to maintain safety.~~

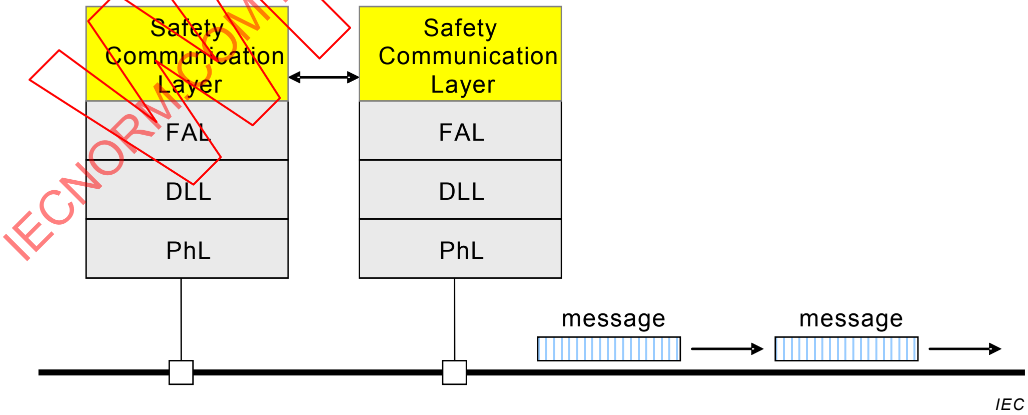


Figure A.3 – Model C

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.~~ Both safety communication layers access the transmission layers independently. The safety data may be transmitted by one or two messages.~~

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV
Withdrawn

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. ~~If cross-checking shows discrepancy, an appropriate action is initiated to maintain safety.~~

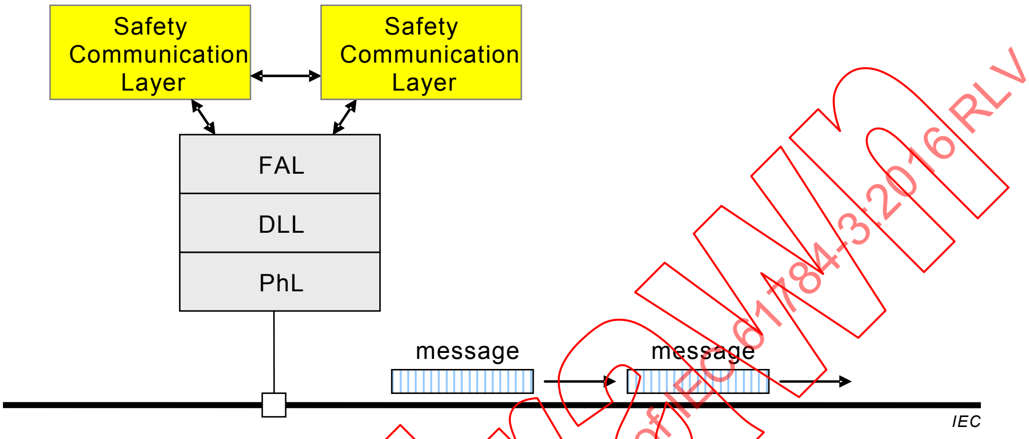


Figure A.4 – Model D

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

Annex B
(~~informative~~ normative)

Safety communication channel model using CRC-based error checking

B.1 Overview

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

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

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.

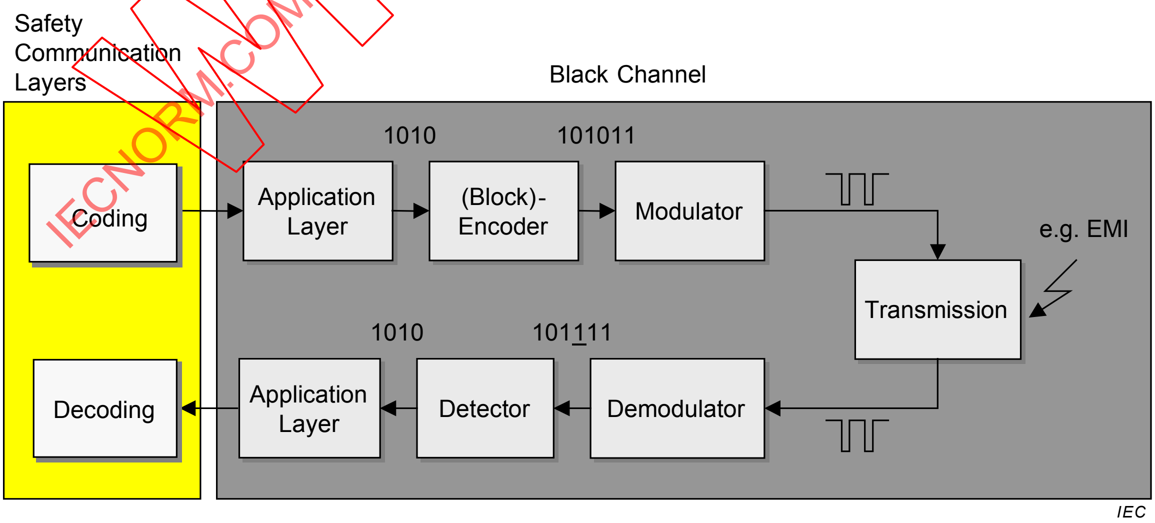


Figure B.1 – Communication channel with perturbation

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

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 $P_e = P$.

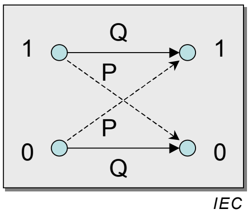


Figure B.2 – Binary symmetric channel (BSC)

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.

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

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

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

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.

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV
Withdrawn

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).

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

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

Withdrawn

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.

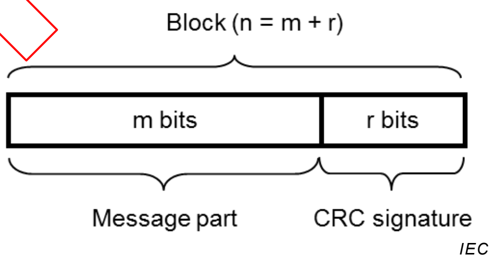


Figure B.3 – Example of a block with a message part and a CRC ~~bits (redundancy code)~~ signature

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

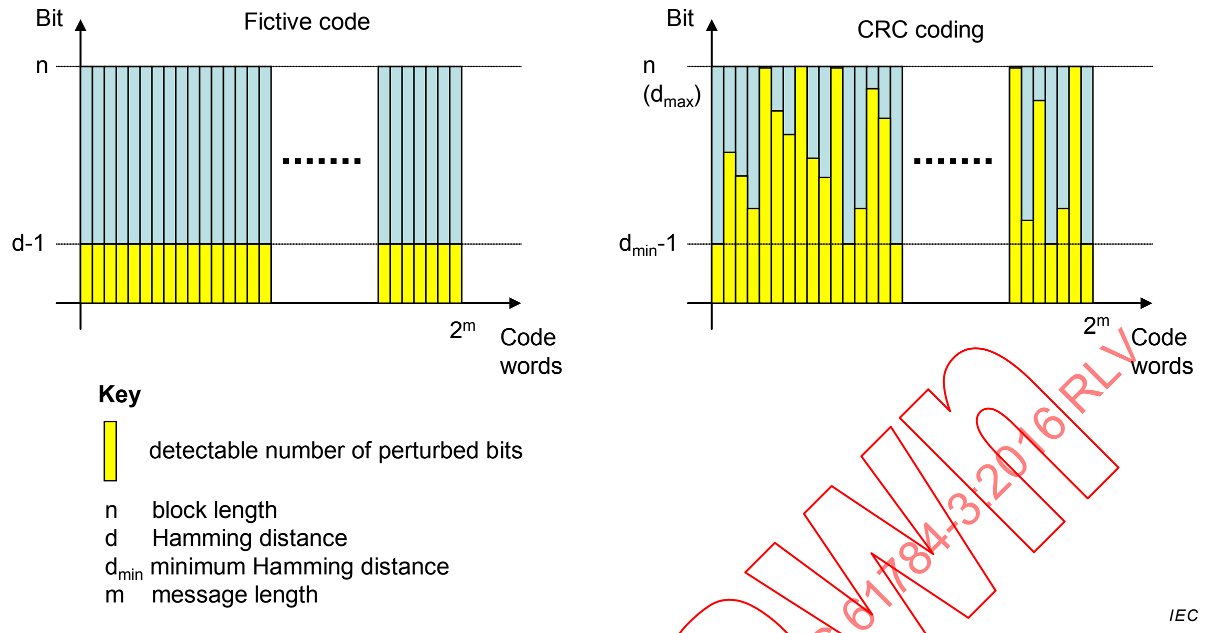


Figure B.4 – Block codes for error detection

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

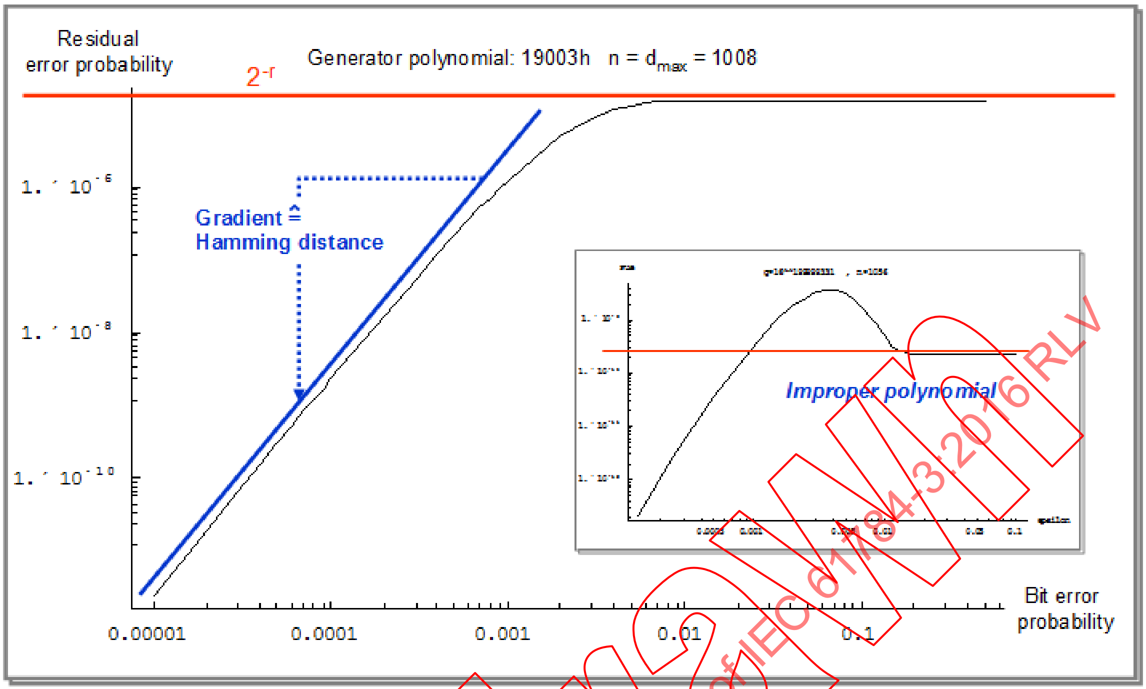
Proper CRC polynomials are characterized by a monotonic ascending slope of the residual error probability function over the bit error probability. Figure B.5 illustrates the difference between a proper and an improper CRC polynomial. It is highly recommended to deploy only those proper CRC polynomials 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]~~,~~ ~~[30]~~,[33] and [34]~~, [36] and [37]~~. Whether or not the polynomial is proper has to be checked for all the intended safety block sizes (see Table B.1). Improper polynomials may show a better residual error probability at high bit error probabilities (2^{-r}) than with smaller bit error probabilities ($>2^{-r}$). When using improper CRC polynomials, the worst case value ($>2^{-r}$) shall be used, whereas with proper polynomials it is sufficient to use 2^{-r} for an estimate of the residual error probability.

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.

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV
Withdrawn

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



IEC

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.

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV
Withdrawn

Annex C
(informative)

Structure of technology-specific parts

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

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

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

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

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

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

Clause and subclause No.	Title	Contents
	services	
7	Safety communication layer protocol	First subclause is listed below, others may be added as needed. May include specific time mechanisms , state machines, sequence charts, reaction on power off/power down, diagnostic protocol and corresponding diagnosis
7.1	Safety PDU format	Includes detailed definition of safety PDU (message) formats. Will include several subclauses to specify the various format elements (for example safety CRC specification)
8	Safety communication layer management	Includes specifications for the following aspects of parameterization: - safe parameter data supplied by another safety device (for example a parameter server) - safe parameter data supplied by a tool (for example device description) (including any required measure to secure the storage, handling and transfer)
9	System requirements	First subclauses are listed below, others may be added as needed
9.1	Indicators and switches	Specifications for device indicators and switch function and behaviour
9.2	Installation guidelines	Detailed clause references within IEC 61918 or other relevant documents
9.3	Safety function response time	Calculations and related examples of reaction times relevant for the technology (for example worst case reaction time of safety loop)
9.4	Duration of demands	Specifications for the duration of demands within devices
9.5	Constraints for calculation of system characteristics	Includes black channel retries, number of telegram per second, number of message sinks
9.6	Maintenance	Specifications for system behaviour in case of device repair and replacement
9.7	Safety manual	If relevant, includes the minimum information required by the profile to be included in the safety manual
9.8	Wireless transmission channels	This subclause is optional. If relevant, 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
~~Annex B (informative)~~	~~Information for assessment of the functional safety communication profiles of CPF X~~	~~Mandatory informative annex used to provide information about test laboratories which test and validate the conformance of FSCP X/1 products with IEC 61784-3-X~~
	Bibliography	Bibliographic references relevant for this part

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV
Withdrawn

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 ~~[5]~~), then this product and the related safety communication components shall meet the requirements to the extent that is mentioned in the scope of the relevant standard, or as defined in a specific safety communication profile within the IEC 61784-3 series.

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.

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

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 Subclause D.3.2 ~~may~~ 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 ~~safety message~~ SPDU and bit by bit comparison within the receiver it is a precondition for an undetected error that both messages are corrupted equally. ~~With the help of the BSC model,~~ The residual error probability can be calculated along the lines of Annex B. The probability for a particular bit error combination within each message is the same in this case and thus the expression is squared. The possibilities for bit error combinations are in accordance with those of a single message (binomial coefficients).

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

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

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

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. ~~IEC 62280-1 should be considered to the extent to which it is applicable.~~

NOTE 4 See IEC 62280 for more information.

The calculation of ~~Λ_{SL}~~ Λ_{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).

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV
Withdrawn

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.

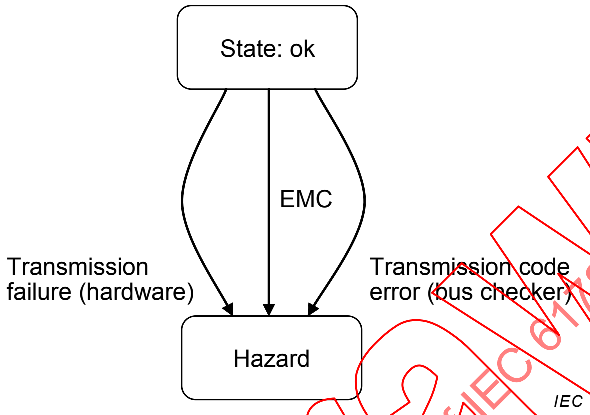

State: ok
EMC
Transmission failure (hardware)
Transmission code error (bus checker)
Hazard
IEC

Figure D.1 – Basic Markov model

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

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

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

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 ~~Λ_{SL}~~ $\Lambda_{SCL}(p_e)$ is carried out along the lines of 5.8.1 with the residual error probability:

$$R_{AD} = R_{HW} + R_{EMC} + R_{TC} \tag{D.2}$$

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.

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

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

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.

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

NOTE In some bus systems, the transmission rate and the reaction or response times depend on the number of participants. If transmission rate and reaction or response times are safety-related, it ~~may~~ 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*: Checking of the documentation and implementation shall include specific functional tests and those with impact of for example personal computer (PC) simulation such as traffic burden or stimulated address changes.~~

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.

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

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

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

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

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

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

D.4.11 Conformance tester

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

Withdrawn

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

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.

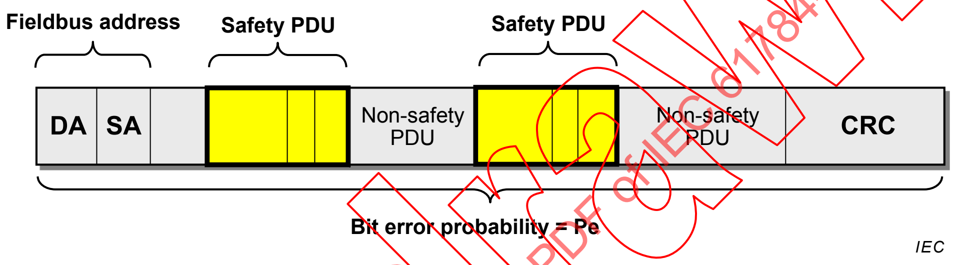


Figure E.1 – Example safety PDUs embedded in a fieldbus message

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.

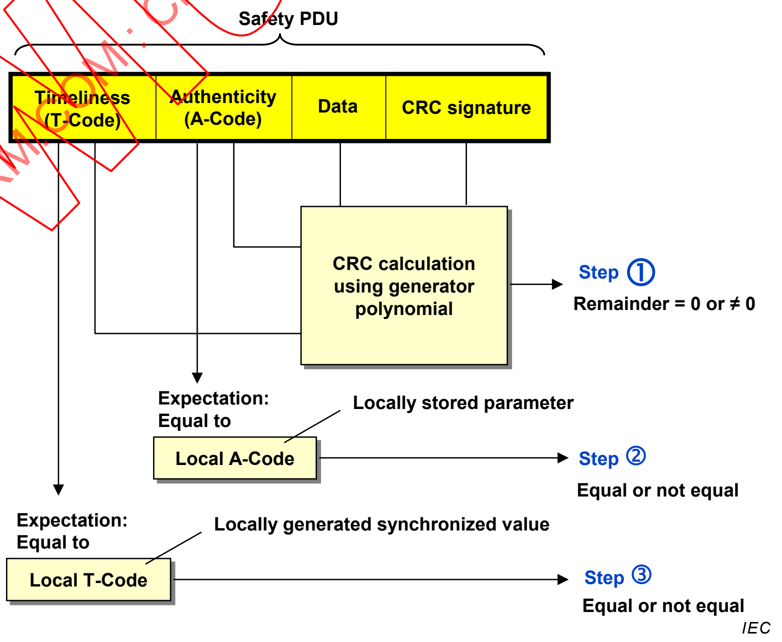


Figure E.2 – Model with completely explicit safety measures

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV
WITHDRAWN

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.

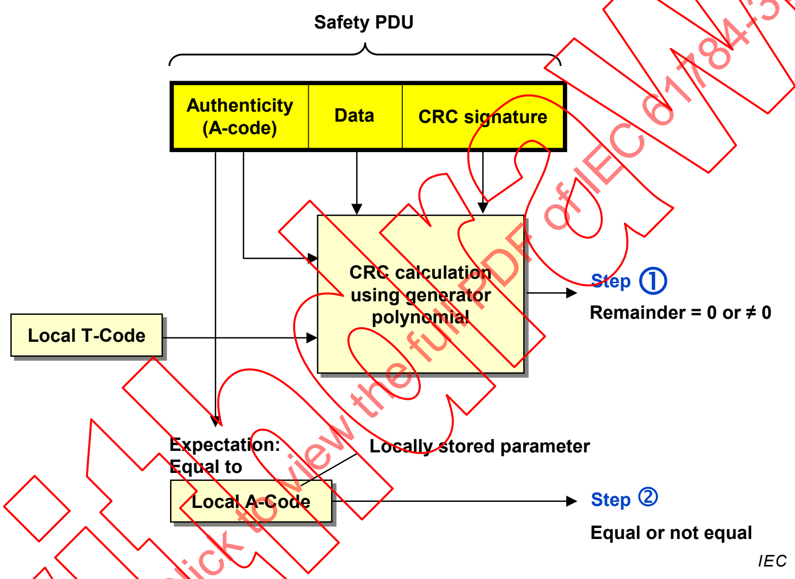


Figure E.3 – Model with explicit A-code and implicit T-code safety measures

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.

IECNORM.COM: Click to view the full PDF of IEC 61784-3:2016 RLV
Withdrawn

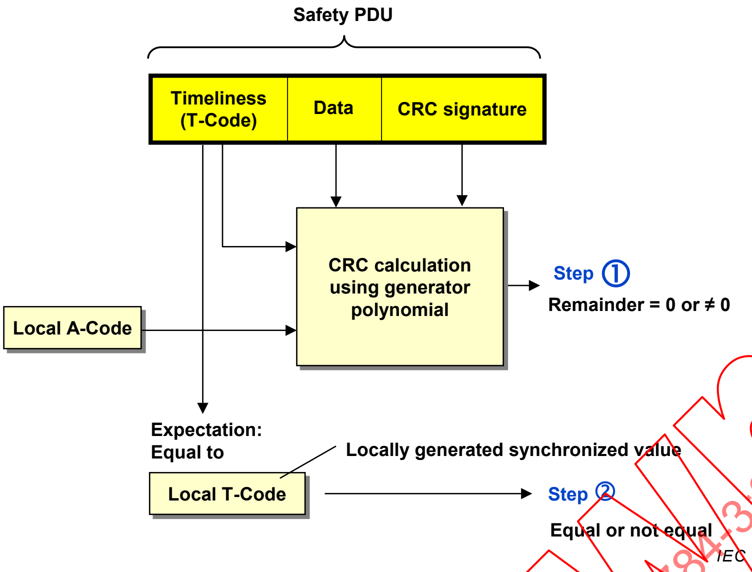


Figure E.4 – Model with explicit T-code and implicit A-code safety measures

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.

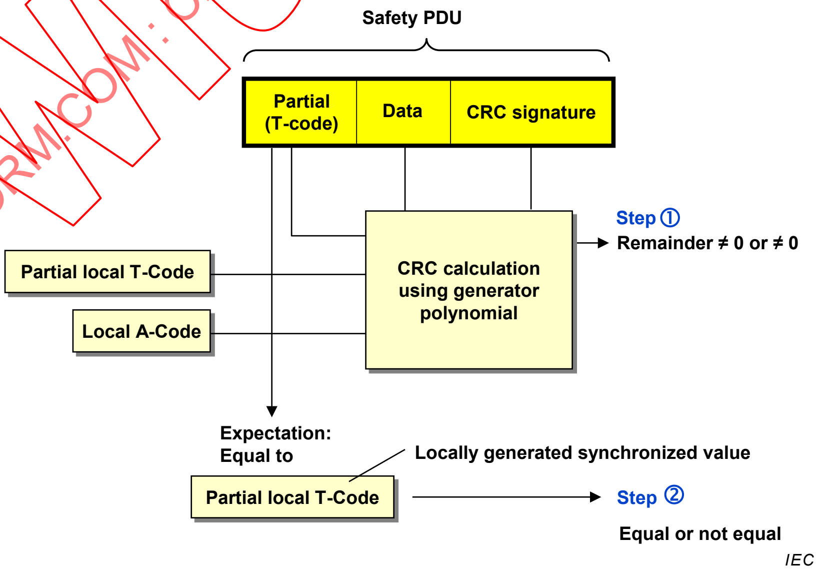


Figure E.5 – Model with split explicit and implicit safety measures

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV
Withdrawn

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.

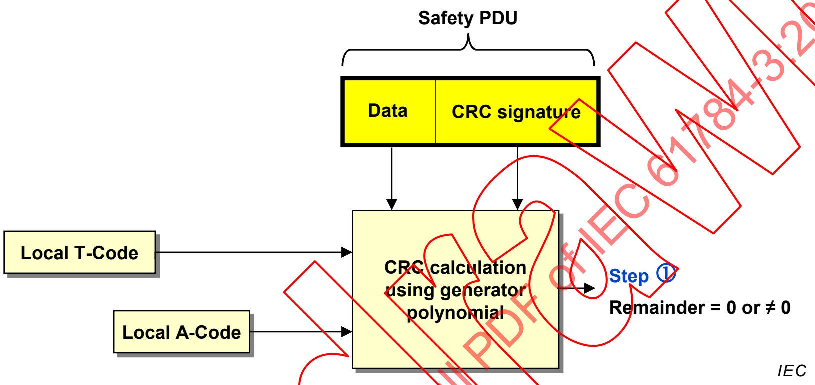


Figure E.6 – Model with completely implicit safety measures

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.

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV
Withdrawn

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.

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

Withdrawn

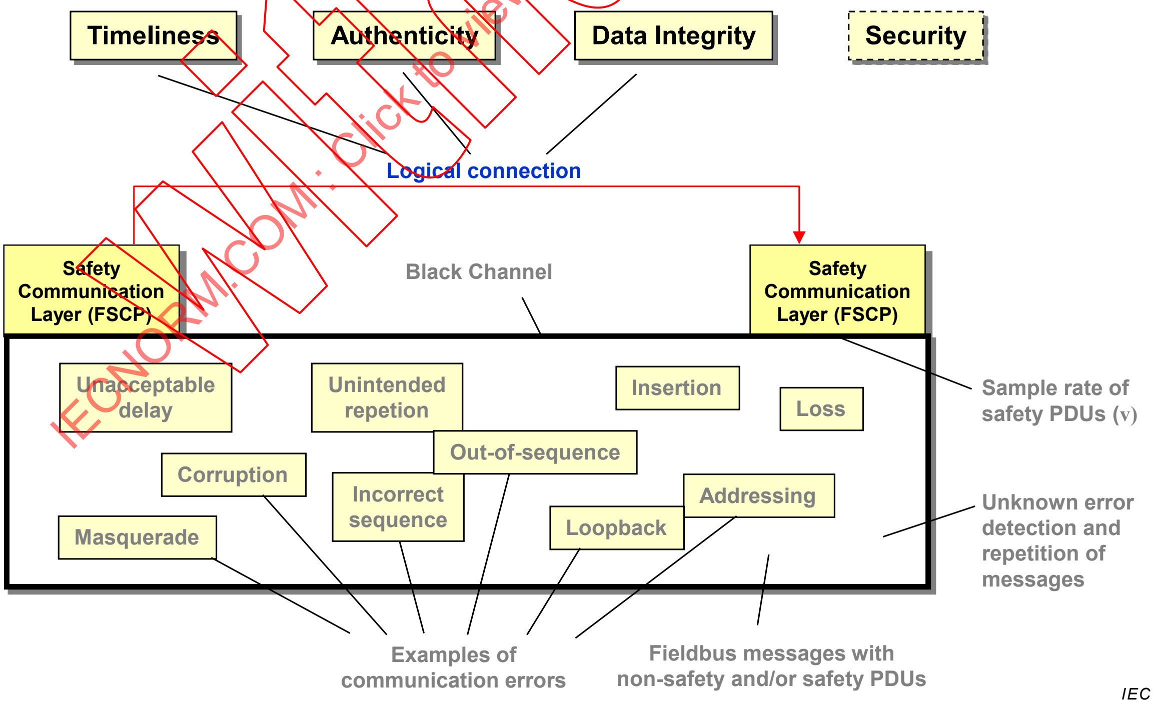

Timeliness
Authenticity
Data Integrity
Security
Logical connection
Safety Communication Layer (FSCP)
Black Channel
Safety Communication Layer (FSCP)
Unacceptable delay
Unintended repetion
Insertion
Loss
Sample rate of safety PDUs (ν)
Out-of-sequence
Corruption
Incorrect sequence
Addressing
Masquerade
Loopback
Unknown error detection and repetition of messages
Examples of communication errors
Fieldbus messages with non-safety and/or safety PDUs
IEC

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;

Withdrawn
IECNORM.COM: Click to view the full PDF of IEC 61784-3:2016 RLV

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).

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

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.

Withdrawn IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

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).

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

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).

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

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).

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

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.

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

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).

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

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.

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV
Withdrawn

F.7 Authenticity

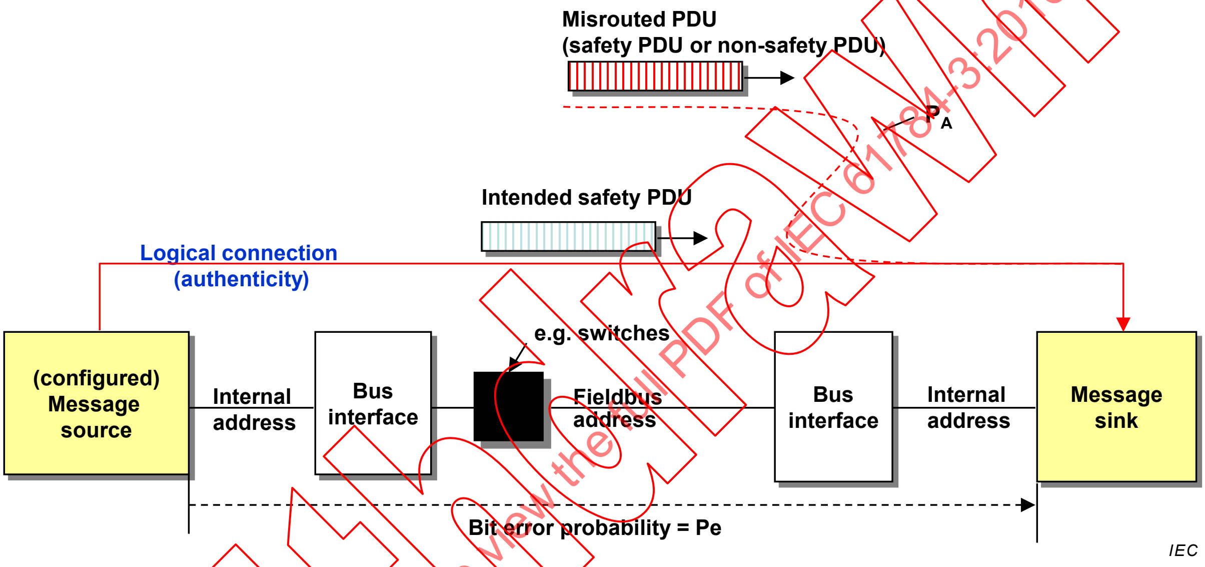
F.7.1 General

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

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV
Withdrawn

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).

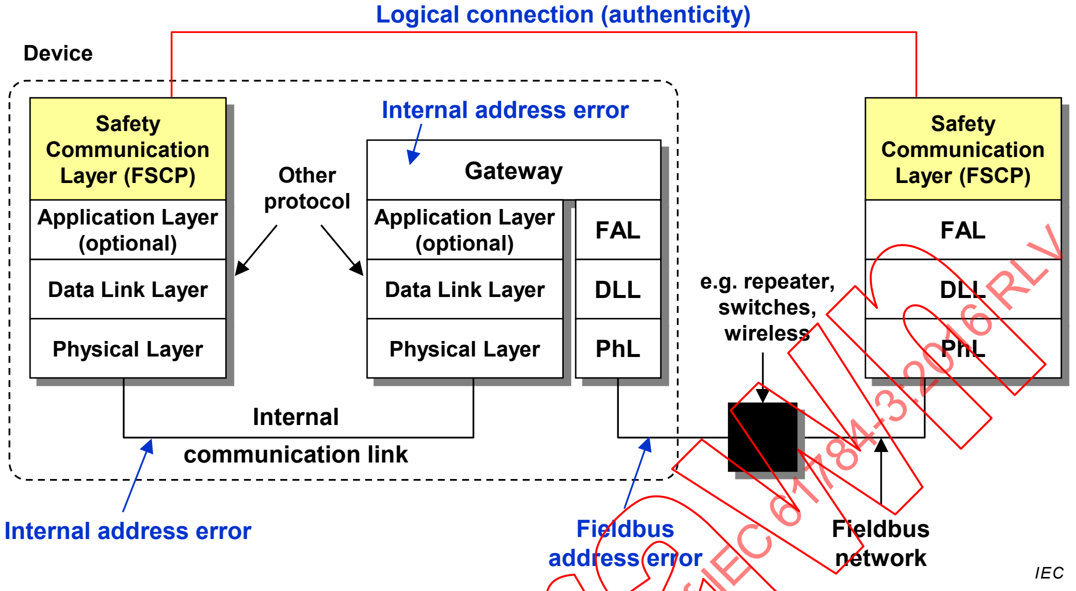

Logical connection (authenticity)
Device
Safety Communication Layer (FSCP)
Application Layer (optional)
Data Link Layer
Physical Layer
Other protocol
Internal address error
Gateway
Application Layer (optional)
Data Link Layer
Physical Layer
FAL
DLL
PhL
e.g. repeater, switches, wireless
Safety Communication Layer (FSCP)
FAL
DLL
PhL
Internal communication link
Internal address error
Fieldbus address error
Fieldbus network
IEC

Figure F.3 – Fieldbus and internal address errors

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV
Withdrawn

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.

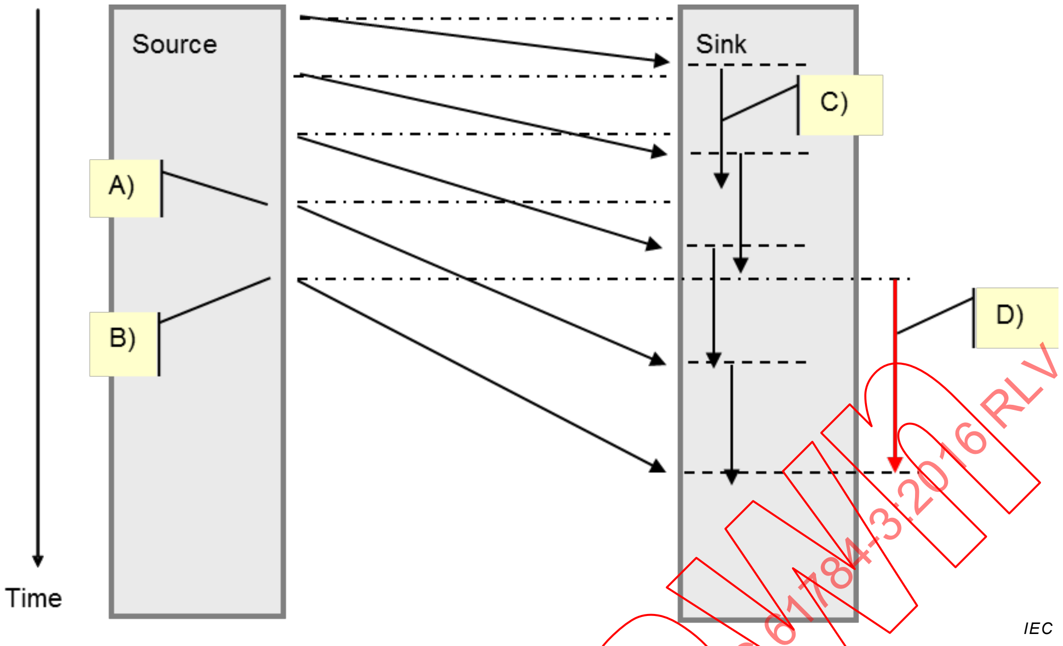
EXAMPLES

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.

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV



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.

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV
Withdrawn

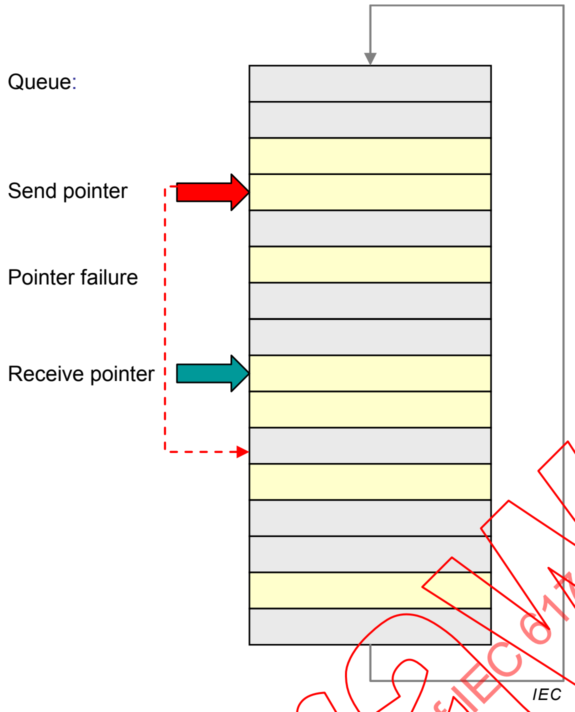


Figure F.5 – Example of an active network element failure

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.

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

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).

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

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.

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

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.

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

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.

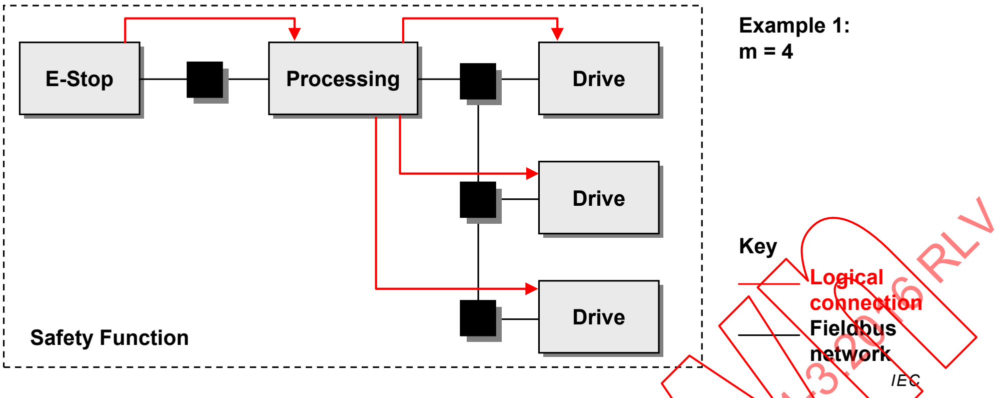
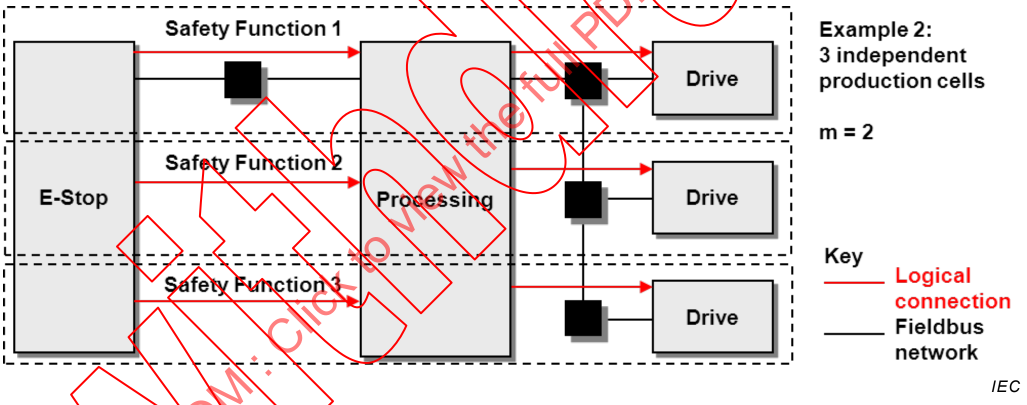


Figure F.6 – Example application 1 (m = 4)

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.



IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

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.

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

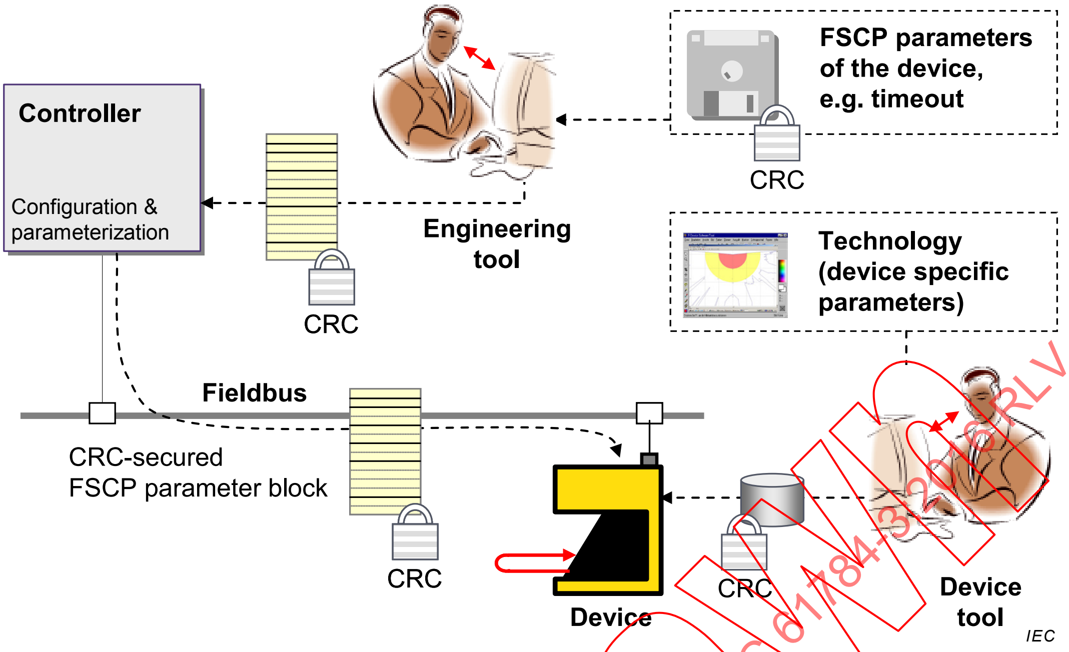

Controller
Configuration & parameterization
CRC
Engineering tool
FSCP parameters of the device, e.g. timeout
CRC
Technology (device specific parameters)
Fieldbus
CRC-secured FSCP parameter block
CRC
Device
CRC
Device tool
IEC

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.

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

- 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.

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

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~~[24]~~, *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~~[25]~~, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations*

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

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

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

[12] IEC 61784-4[26], *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*

Withdrawn

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

~~[24] In preparation.~~

~~[25] To be published.~~

[26] Proposed new work item under consideration.

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

[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*

~~[15] IEC 62280-2, *Railway applications – Communication, signalling and processing systems – Part 2: Safety-related communication in open 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:~~1999~~ 2014, *Safety aspects — Guidelines for their inclusion in standards*

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

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

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

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

~~[23] ISO 12100-1, *Safety of machinery – Basic concepts, general principles for design – Part 1: Basic terminology, methodology*~~

[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*

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

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

~~[25] EN 954-1:1996[27], *Safety of machinery – Safety related parts of control systems – General principles for design*~~

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

~~[27] To be replaced by ISO 13849-1 and/or IEC 62061.~~

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV
Withdrawn

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

~~[28] GS-ET-26[28], *Grundsatz für die Prüfung und Zertifizierung von Bussystemen für die Übertragung sicherheitsrelevanter Nachrichten*, May 2002. HVBG, Gustav-Heinemann-Ufer 130, D-50968 Köln ("*Principles for Test and Certification of Bus Systems for Safety relevant Communication*")~~

[28] ANDREW S. TANENBAUM, DAVID J. WETHERALL, *Computer Networks*,~~ 4th~~ 5th Edition, Prentice Hall, N.J., ISBN-10:~~0130661023~~ 0132126958, ISBN-13:~~ 978-0130661029~~ 978-0132126953

[29] W. WESLEY PETERSON, EDWARD J. WELDON, *Error-Correcting Codes*, 2nd Edition ~~1981~~ 1972, MIT-Press, ISBN 0-262-16-039-0

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

~~[32] *New concepts for safety-related bus systems*, 3rd International Symposium "Programmable Electronic Systems in Safety Related Applications ", May 1998, from Dr. Michael Schäfer, BG-Institute for Occupational Safety and Health.~~

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

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

[30] NFPA79 (~~2002~~ 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

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

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

~~[28] This document has been one of the starting points for this part. It is currently undergoing a major revision.~~

Withdrawn

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

Withdrawn

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

IEC 61784-3

Edition 3.0 2016-05

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

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

IEC 61784-3:2016-05(en-fr)

CONTENTS

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

INTERNATIONAL ELECTROTECHNICAL COMMISSION

____

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES –

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

FOREWORD

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.

2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.

3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.

4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.

5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.

6) All users should ensure that they have the latest edition of this publication.

7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.

8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.

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

This third edition cancels and replaces the second edition published in 2010. This 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.

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

FDIS	Report on voting
65C/840/FDIS	65C/848/RVD

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

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

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

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC website 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.

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

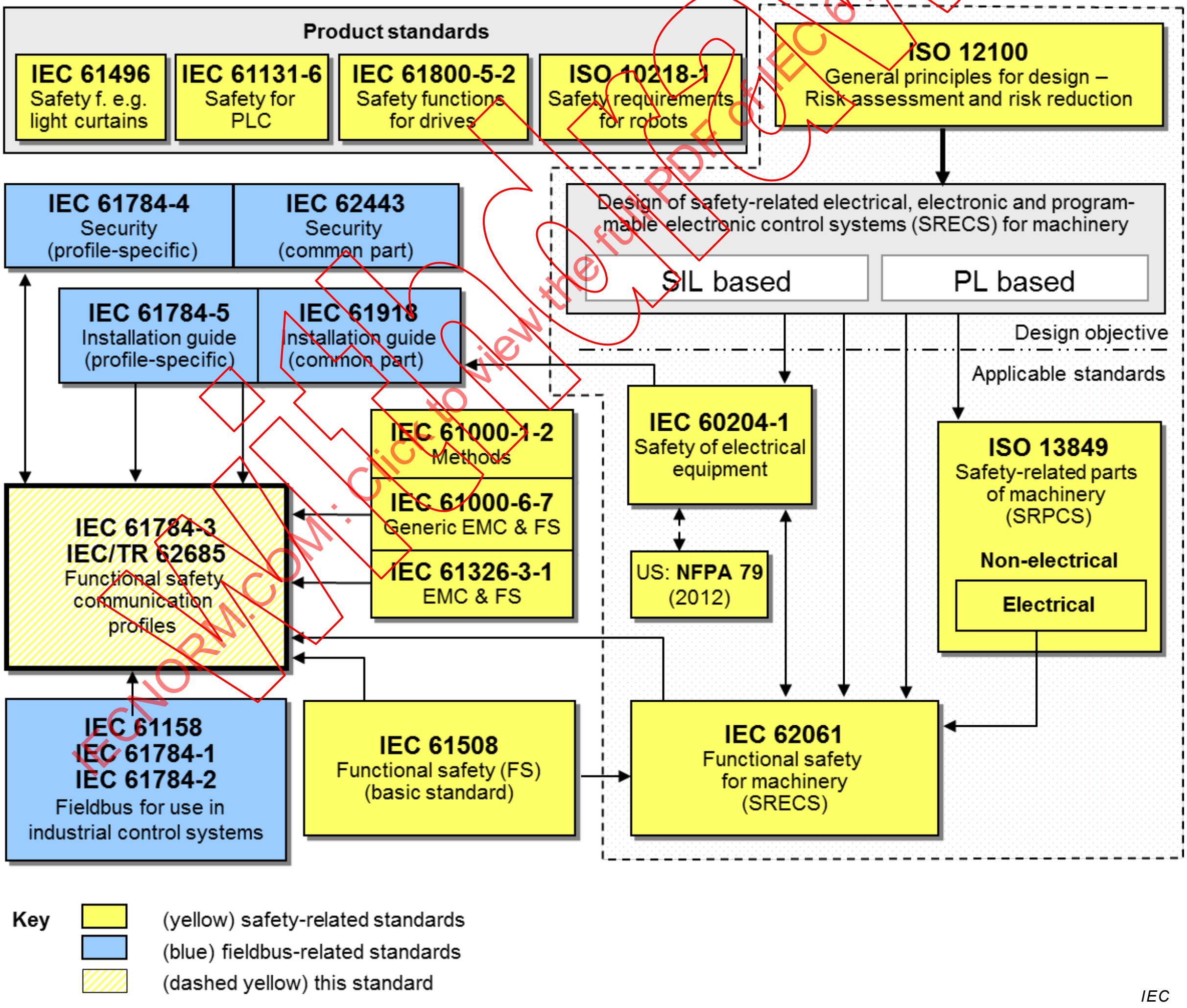
0 Introduction

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.

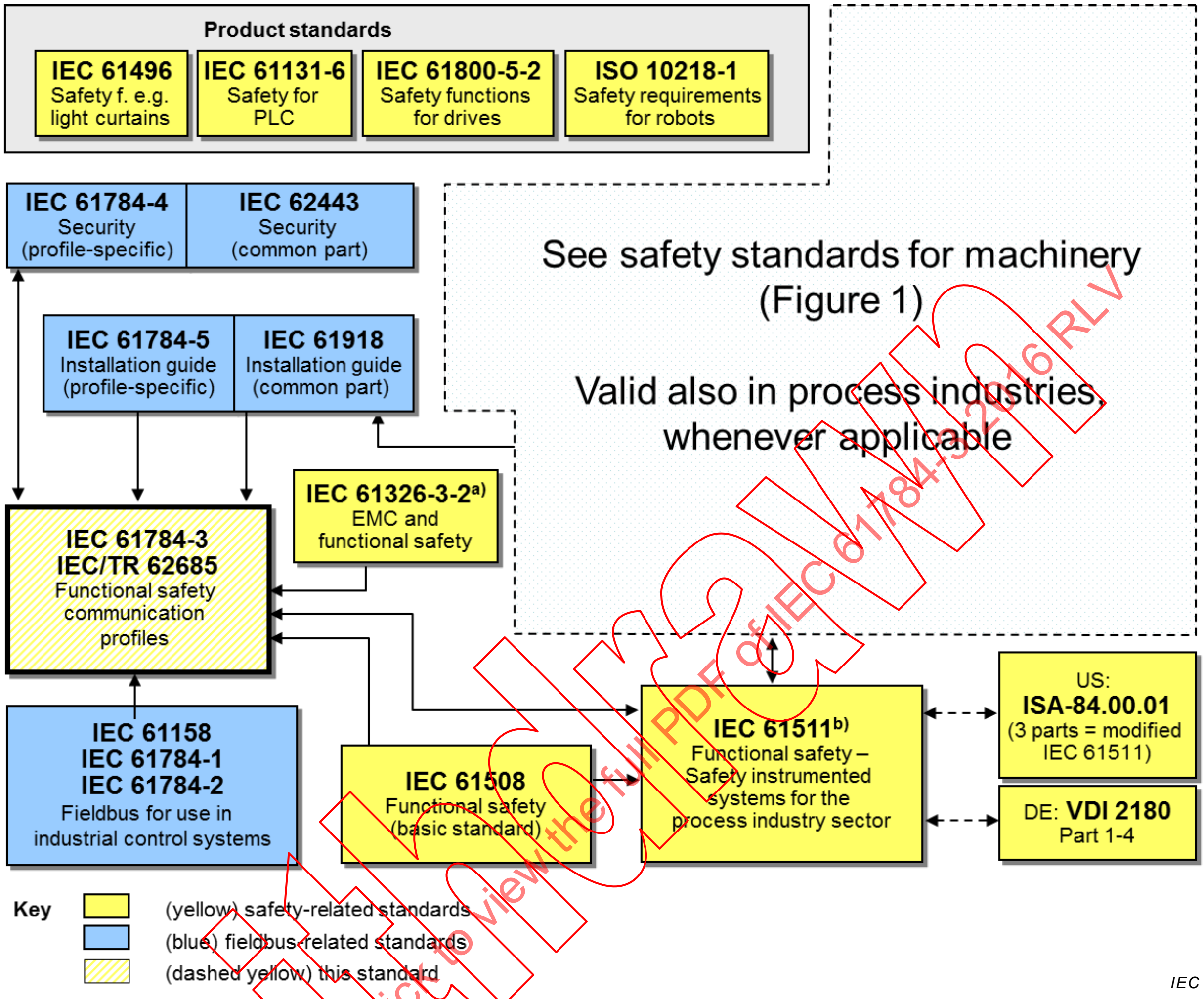

Product standards
IEC 61496 Safety f. e.g. light curtains
IEC 61131-6 Safety for PLC
IEC 61800-5-2 Safety functions for drives
ISO 10218-1 Safety requirements for robots
ISO 12100 General principles for design – Risk assessment and risk reduction
IEC 61784-4 Security (profile-specific)
IEC 62443 Security (common part)
Design of safety-related electrical, electronic and programmable electronic control systems (SRECS) for machinery
SIL based
PL based
Design objective
Applicable standards
IEC 61784-5 Installation guide (profile-specific)
IEC 61918 Installation guide (common part)
IEC 61000-1-2 Methods
IEC 61000-6-7 Generic EMC & FS
IEC 61326-3-1 EMC & FS
IEC 60204-1 Safety of electrical equipment
US: NFPA 79 (2012)
ISO 13849 Safety-related parts of machinery (SRPCS)
Non-electrical
Electrical
IEC 61784-3 IEC/TR 62685 Functional safety communication profiles
IEC 61158 IEC 61784-1 IEC 61784-2 Fieldbus for use in industrial control systems
IEC 61508 Functional safety (FS) (basic standard)
IEC 62061 Functional safety for machinery (SRECS)
Key
(yellow) safety-related standards
(blue) fieldbus-related standards
(dashed yellow) this standard
IEC

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)

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

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


Product standards
IEC 61496 Safety f. e.g. light curtains
IEC 61131-6 Safety for PLC
IEC 61800-5-2 Safety functions for drives
ISO 10218-1 Safety requirements for robots
IEC 61784-4 Security (profile-specific)
IEC 62443 Security (common part)
See safety standards for machinery (Figure 1)
Valid also in process industries, whenever applicable
IEC 61784-5 Installation guide (profile-specific)
IEC 61918 Installation guide (common part)
IEC 61326-3-2a) EMC and functional safety
IEC 61784-3 IEC/TR 62685 Functional safety communication profiles
IEC 61158 IEC 61784-1 IEC 61784-2 Fieldbus for use in industrial control systems
IEC 61508 Functional safety (basic standard)
IEC 61511b) Functional safety – Safety instrumented systems for the process industry sector
US: ISA-84.00.01 (3 parts = modified IEC 61511)
DE: VDI 2180 Part 1-4
Key
(yellow) safety-related standards
(blue) fieldbus-related standards
(dashed yellow) this standard
IEC

[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)

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

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.

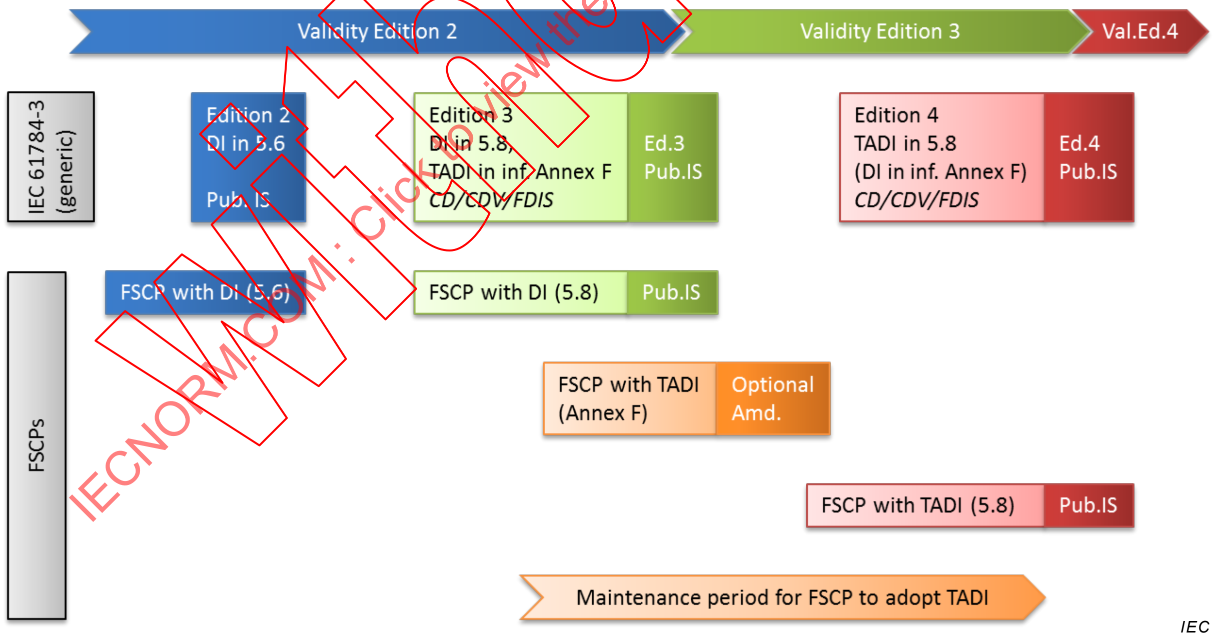
0.2 Transition from Edition 2 to extended assessment methods in Edition 3

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

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

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.

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

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*

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

[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*

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

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

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

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]

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

[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].

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

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

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

[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

Withdrawn
IECNORM.COM: Click to view the full PDF of IEC 61784-3:2016 RLV

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]

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

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

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

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.

3.2 Symbols and abbreviated terms

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	

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

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	

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)).

Withdrawn
IECNORM.COM: Click to view the full PDF of IEC 61784-3:2016 RLV

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.

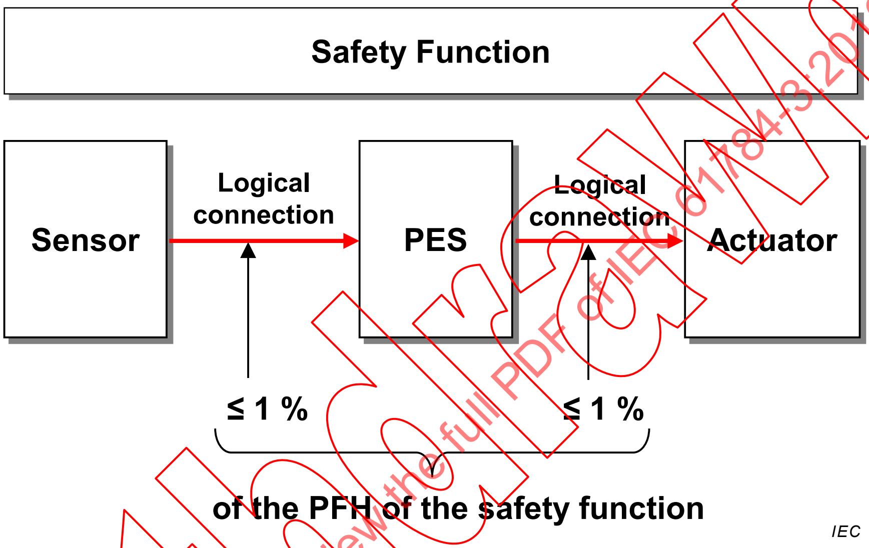


Figure 4 – Safety communication as a part of a safety function

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.

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV Withdrawn

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.

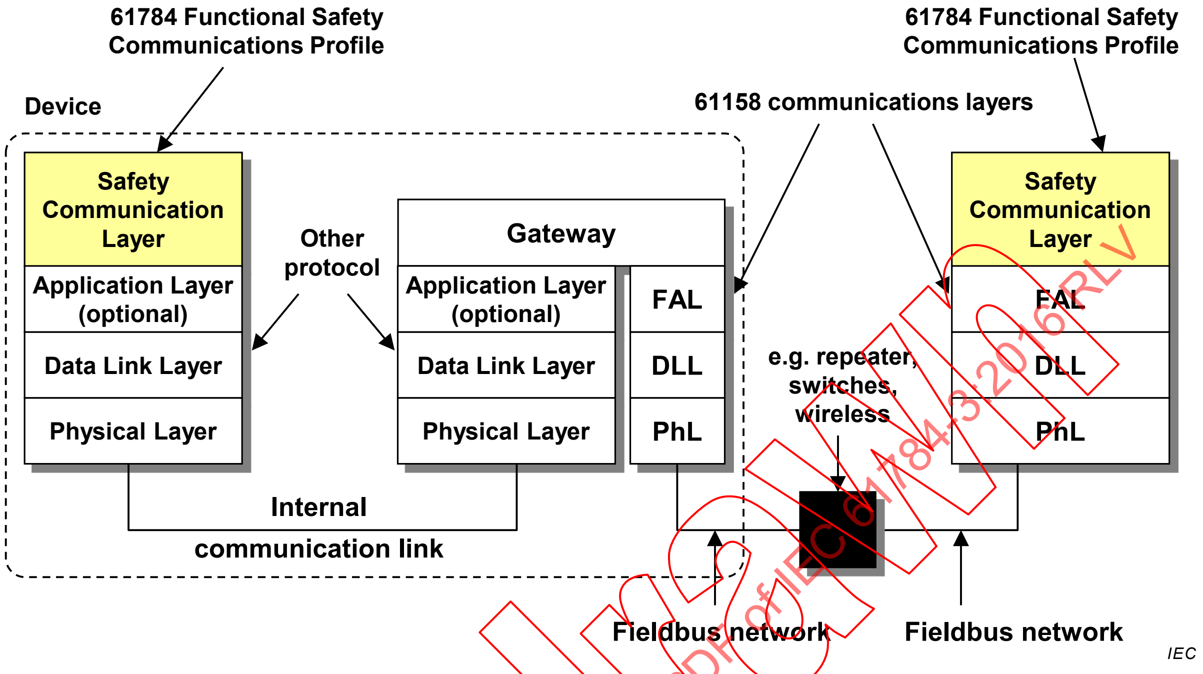

61784 Functional Safety Communications Profile
Device
61158 communications layers
61784 Functional Safety Communications Profile
Safety Communication Layer
Application Layer (optional)
Data Link Layer
Physical Layer
Other protocol
Gateway
Application Layer (optional)
Data Link Layer
Physical Layer
FAL
DLL
PhL
e.g. repeater, switches, wireless
Safety Communication Layer
FAL
DLL
PhL
Internal communication link
Fieldbus network
Fieldbus network
IEC

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.

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016RLV
Withdrawn

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.

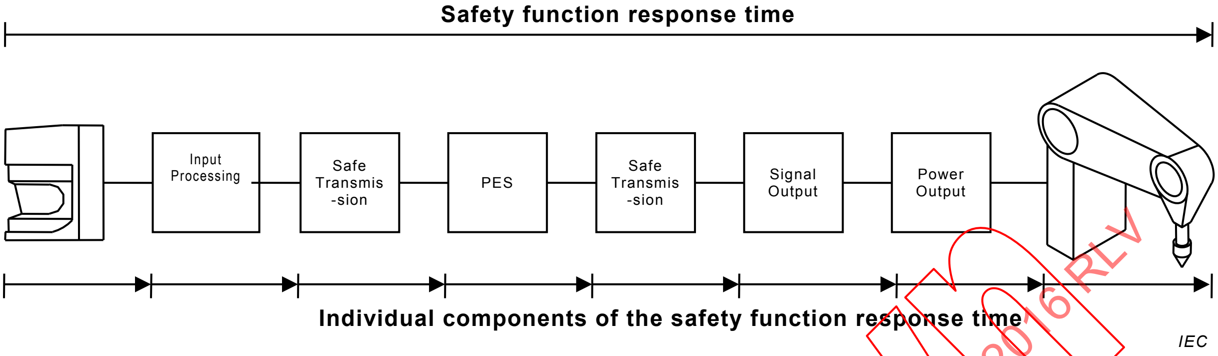

Safety function response time
Input Processing
Safe Transmis -sion
PES
Safe Transmis -sion
Signal Output
Power Output
Individual components of the safety function response time
IEC

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.

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV
Withdrawn

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.

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 PLV
Withdrawn

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).

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

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.

Withdrawn

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

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.

IECNORM.COM: Click to view the full PDF of IEC 61784-3:2016 RLV

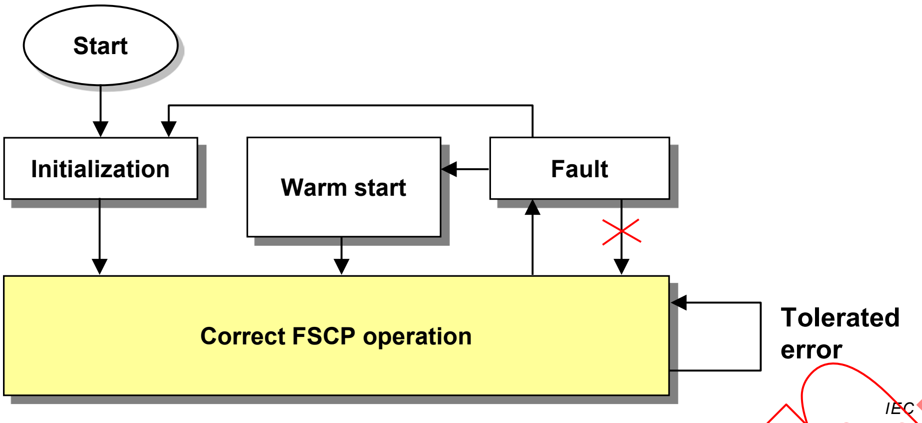


Figure 7 – Conceptual FSCP protocol model

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV
Withdrawn

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).

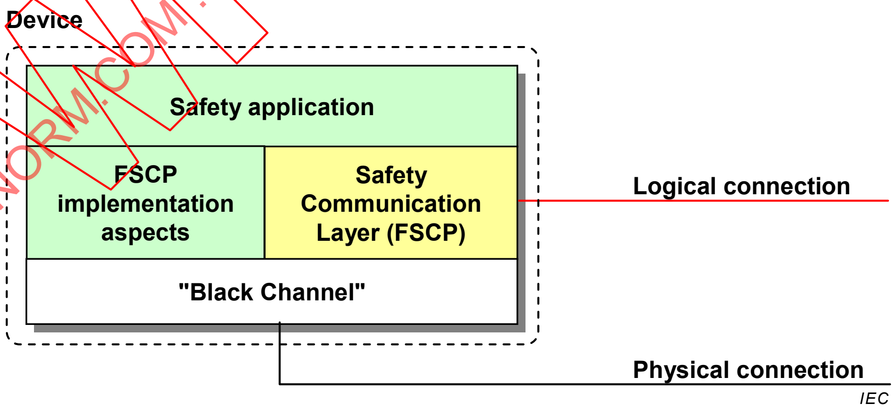


Figure 8 – FSCP implementation aspects

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.

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

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

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.

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV
Withdrawn

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.

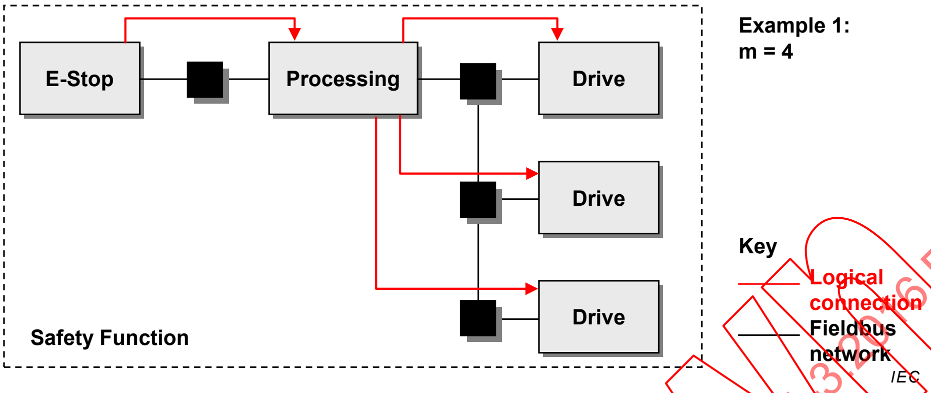


Figure 9 – Example application 1 (m=4)

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.

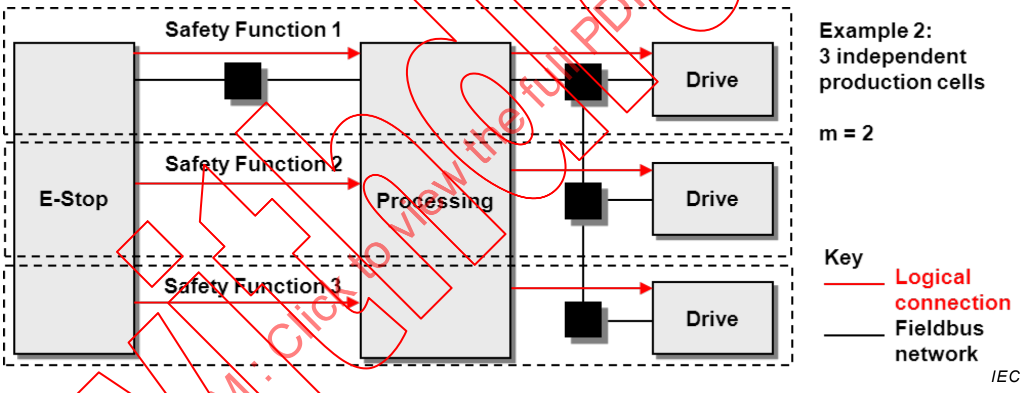


Figure 10 – Example application 2 (m = 2)

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.

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

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.

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV
Withdrawn

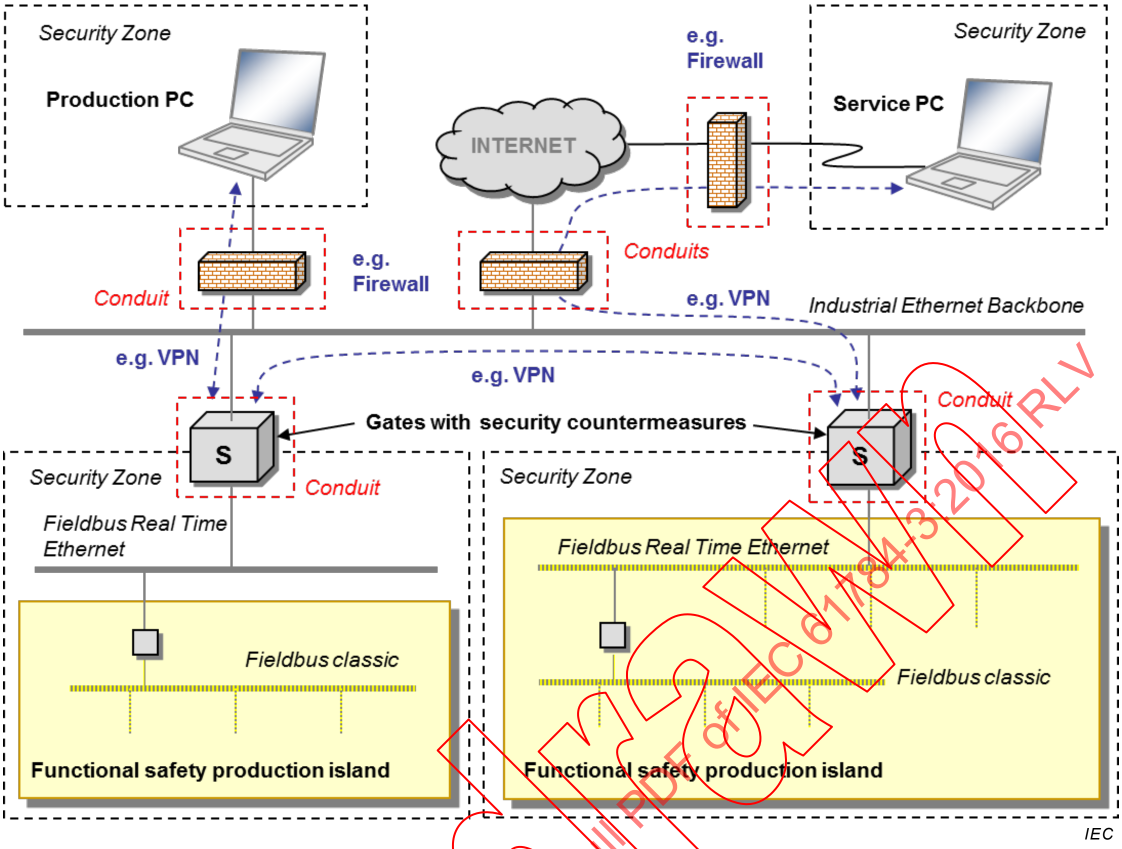


Figure 11 – Zones and conduits concept for security according to IEC 62443

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV
Withdrawn

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.

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

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.

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.

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

[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 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).

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.

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.

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV
Withdrawn

[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).

[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).

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.

[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).

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

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.

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

[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 to 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.

Withdrawn

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

[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.

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

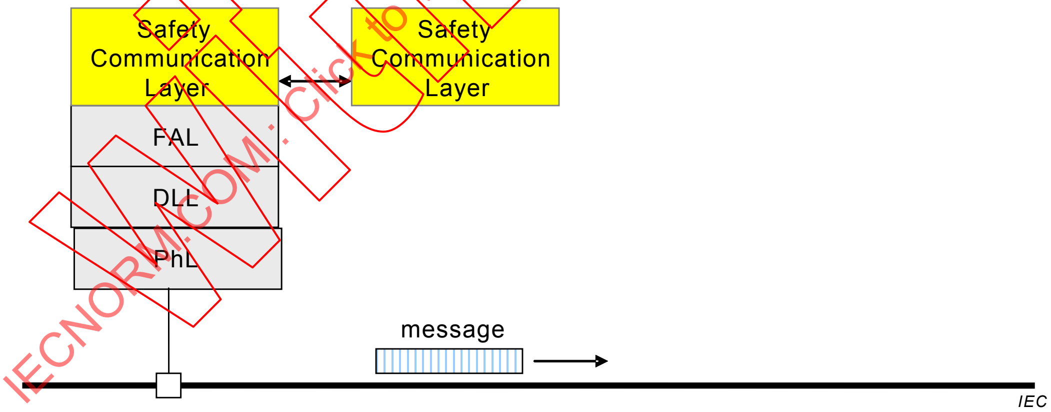


Figure A.1 – Model A

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.

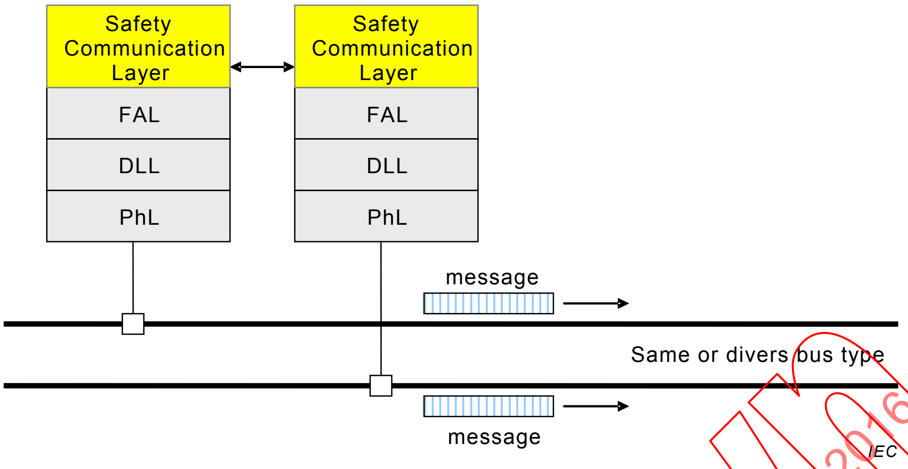


Figure A.2 – Model B

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

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.

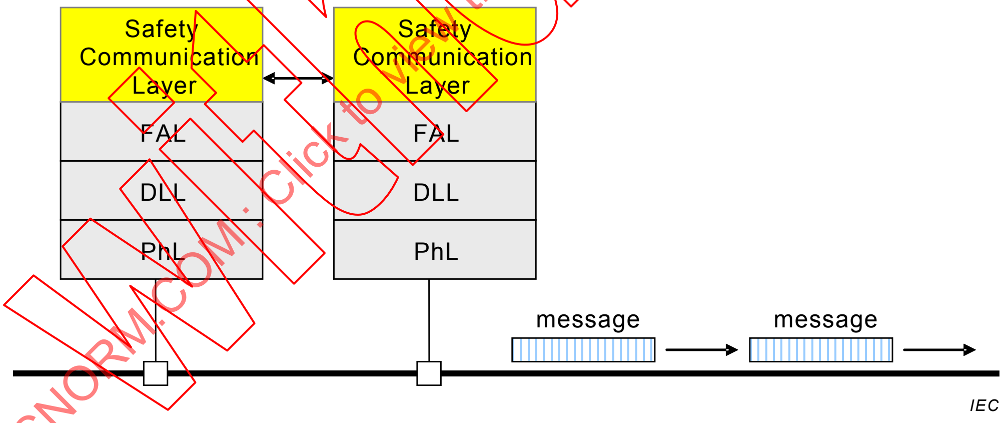


Figure A.3 – Model C

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.

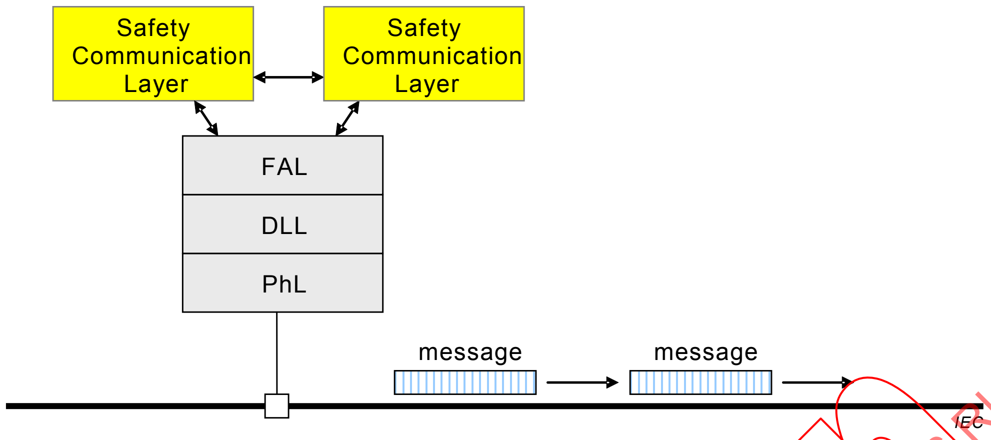


Figure A.4 – Model D

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

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.

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

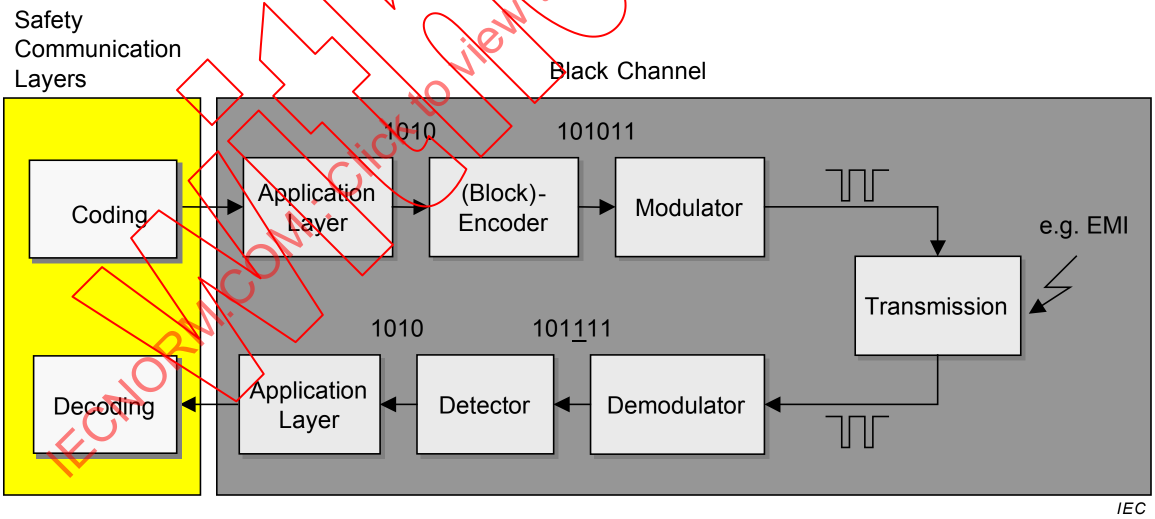


Figure B.1 – Communication channel with perturbation

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 $P_e = P$.

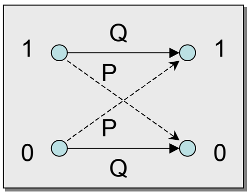


Figure B.2 – Binary symmetric channel (BSC)

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.

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

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.

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

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.

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

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.

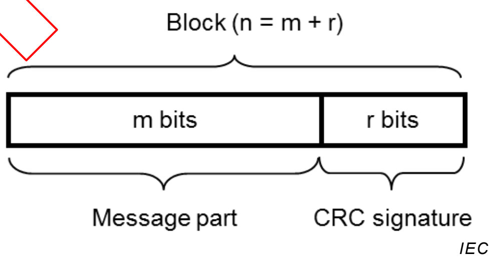


Figure B.3 – Example of a block with a message part and a CRC signature

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

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

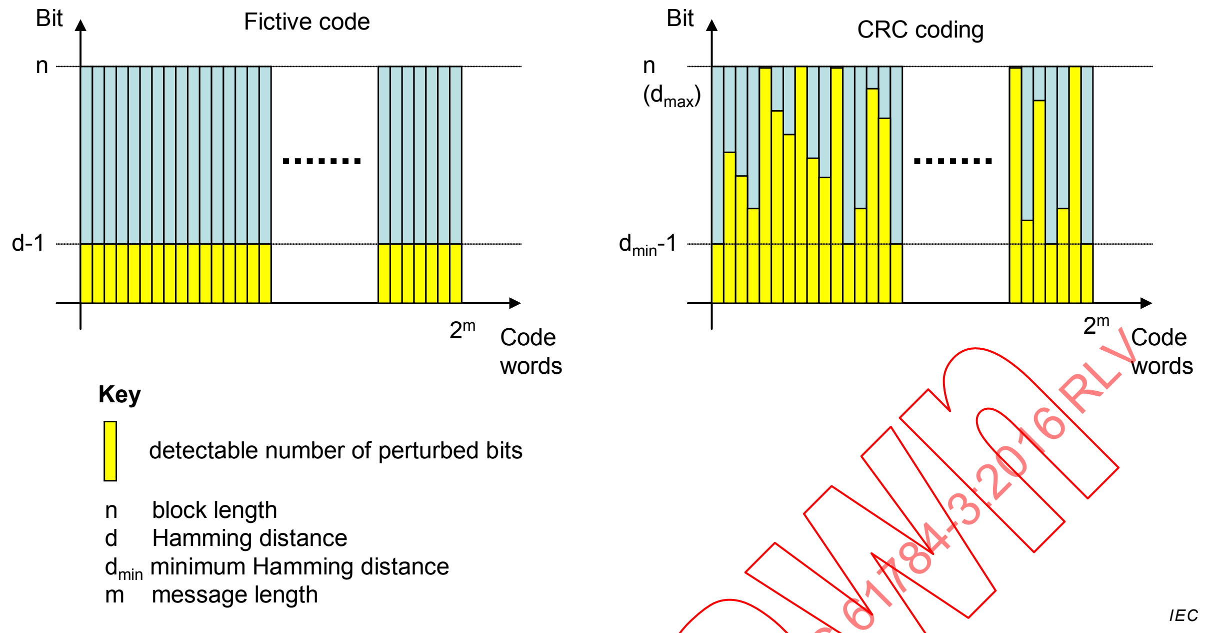


Figure B.4 – Block codes for error detection

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

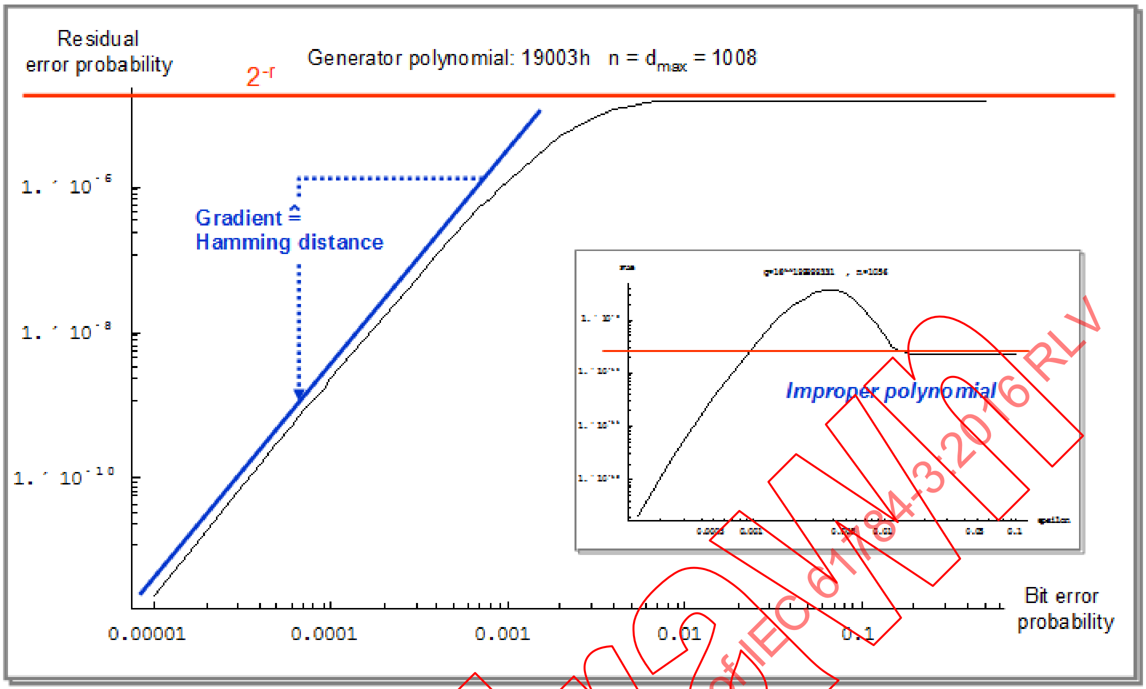
Proper CRC polynomials are characterized by a monotonic ascending slope of the residual error probability function over the bit error probability. Figure B.5 illustrates the difference between a proper and an improper CRC polynomial. It is highly recommended to deploy only those proper CRC polynomials 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.

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV
Withdrawn

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



IEC

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.

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV
Withdrawn

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")

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV
Withdrawn

Clause and subclause No.	Title	Contents
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

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

Withdrawn

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

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.

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV
Withdrawn

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.

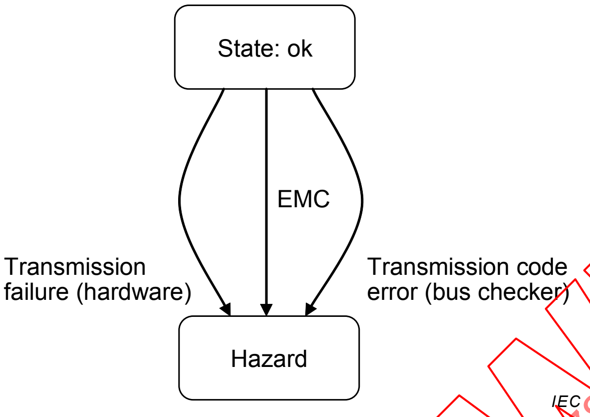

State: ok
EMC
Transmission failure (hardware)
Transmission code error (bus checker)
Hazard
IEC

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:

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

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.

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV
Withdrawn

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

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

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.

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

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.

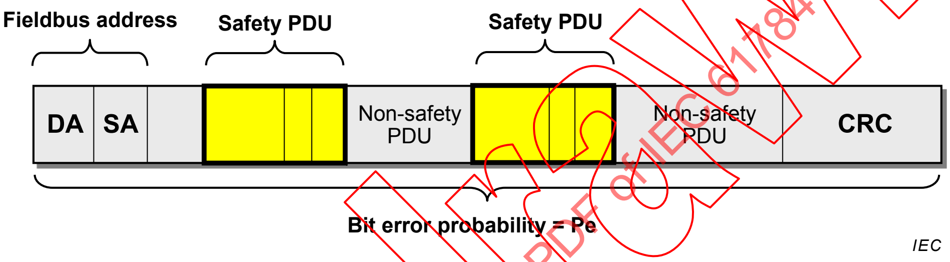


Figure E.1 – Example safety PDUs embedded in a fieldbus message

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.

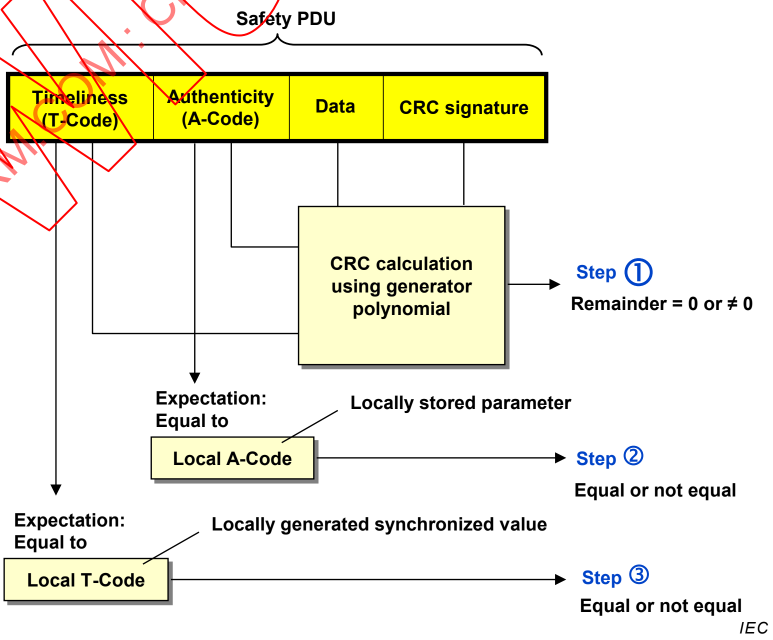


Figure E.2 – Model with completely explicit safety measures

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

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.

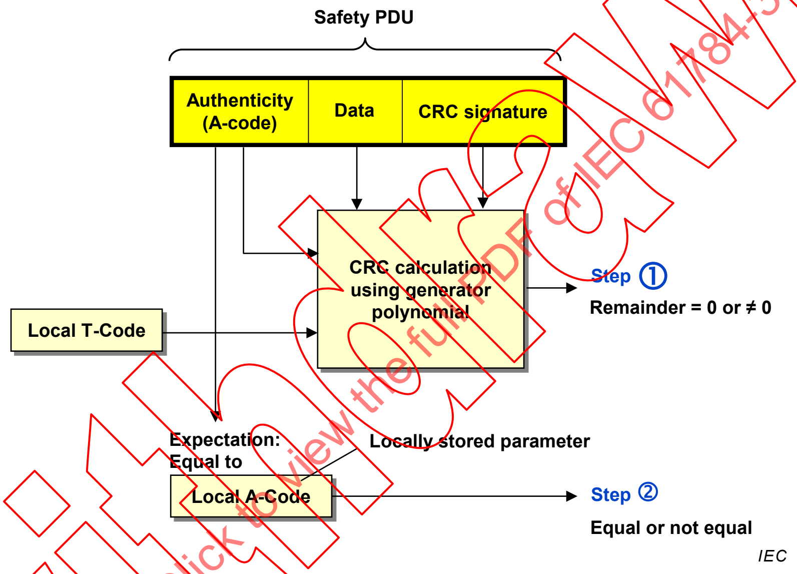


Figure E.3 – Model with explicit A-code and implicit T-code safety measures

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.

IECNORM.COM: Click to view the full PDF of IEC 61784-3:2016 RLV
Withdrawn

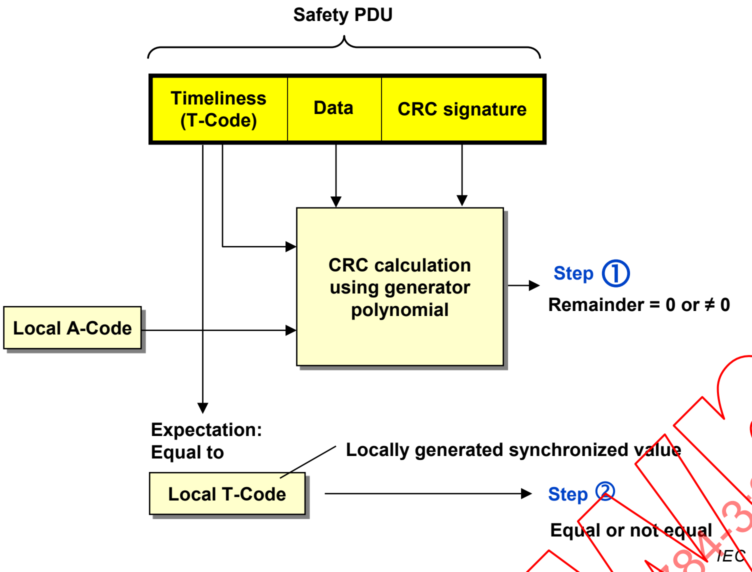


Figure E.4 – Model with explicit T-code and implicit A-code safety measures

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.

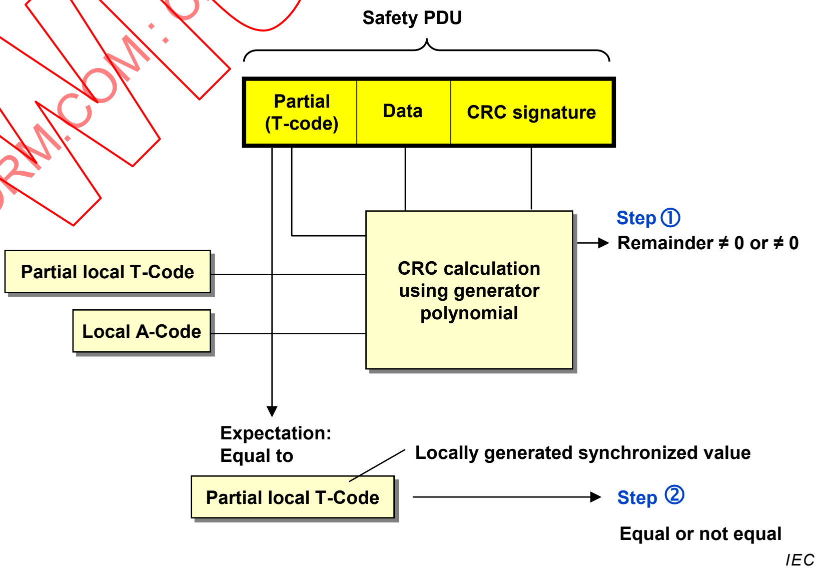


Figure E.5 – Model with split explicit and implicit safety measures

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV
Withdrawn

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.

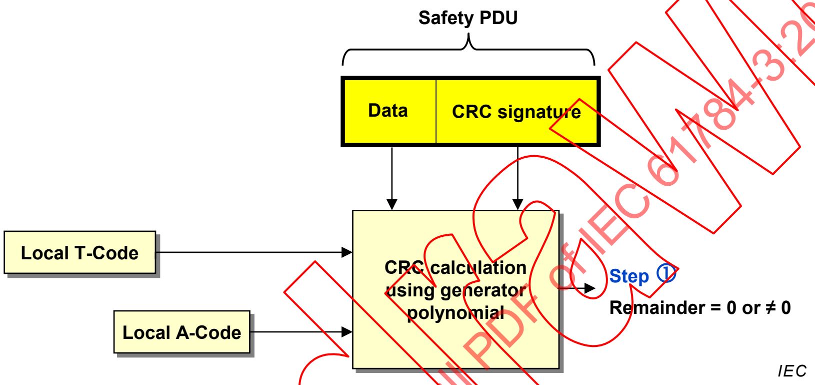


Figure E.6 – Model with completely implicit safety measures

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.

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV
Withdrawn

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.

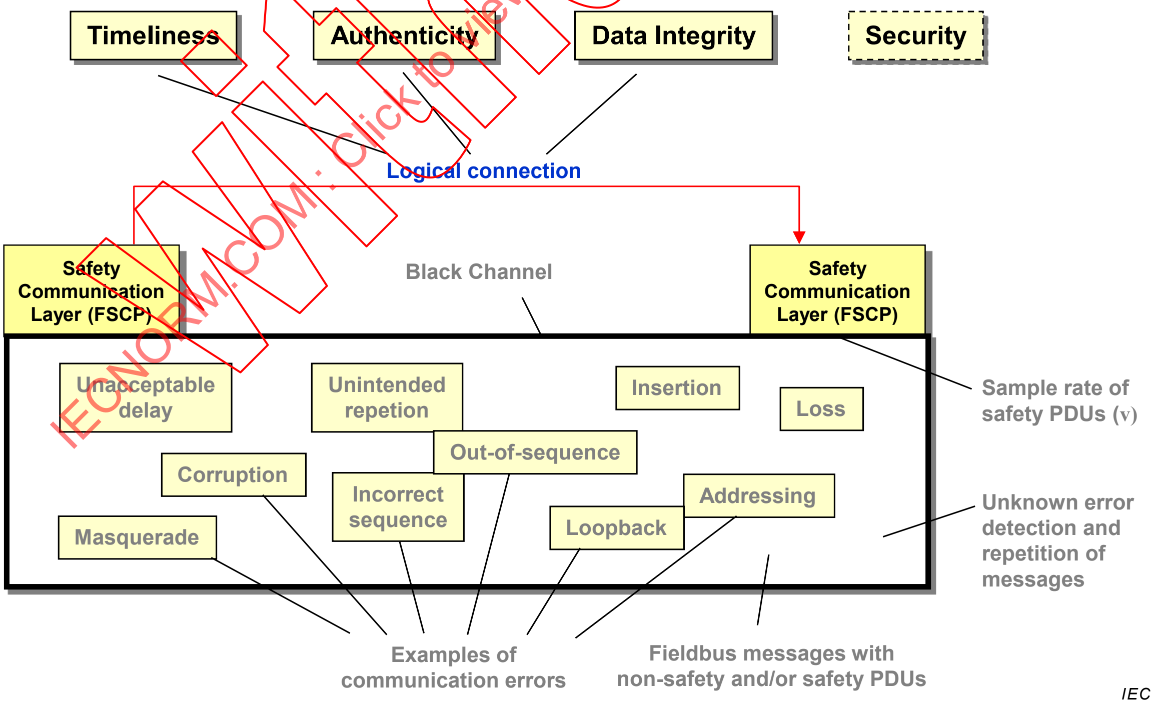

Timeliness
Authenticity
Data Integrity
Security
Logical connection
Safety Communication Layer (FSCP)
Black Channel
Safety Communication Layer (FSCP)
Unacceptable delay
Unintended repetion
Insertion
Loss
Sample rate of safety PDUs (v)
Out-of-sequence
Corruption
Incorrect sequence
Addressing
Loopback
Masquerade
Unknown error detection and repetition of messages
Examples of communication errors
Fieldbus messages with non-safety and/or safety PDUs
IEC

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.

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV
Withdrawn

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;

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV
Withdrawn

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 ($\mathrm{RP_U}$) which is included in the residual error rate calculations where appropriate. It is given by Equation (F.1).

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

where

$\mathrm{RP_U}$ is the residual error probability for other fields of uniqueness that distinguish a properly formatted safety PDU;

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

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

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

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).

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

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).

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

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).

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

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.

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

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).

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

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.

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

F.7 Authenticity

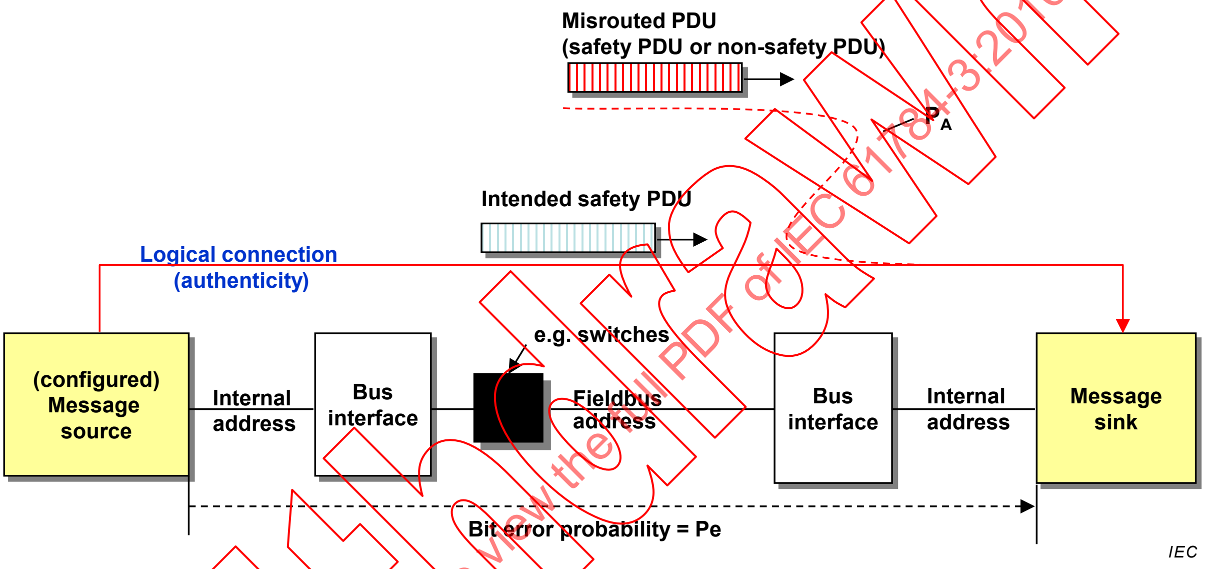
F.7.1 General

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

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV
Withdrawn

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).

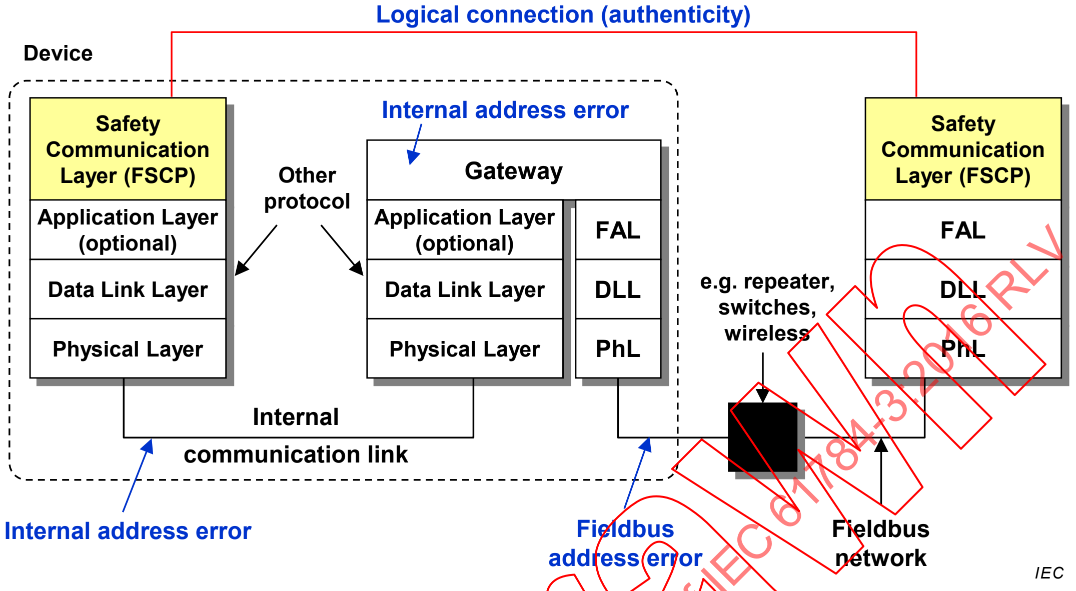

Logical connection (authenticity)
Device
Safety Communication Layer (FSCP)
Application Layer (optional)
Data Link Layer
Physical Layer
Other protocol
Internal address error
Gateway
Application Layer (optional)
Data Link Layer
Physical Layer
FAL
DLL
PhL
Internal communication link
e.g. repeater, switches, wireless
Safety Communication Layer (FSCP)
FAL
DLL
PhL
Internal address error
Fieldbus address error
Fieldbus network
IEC

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.

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV
Withdrawn

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.

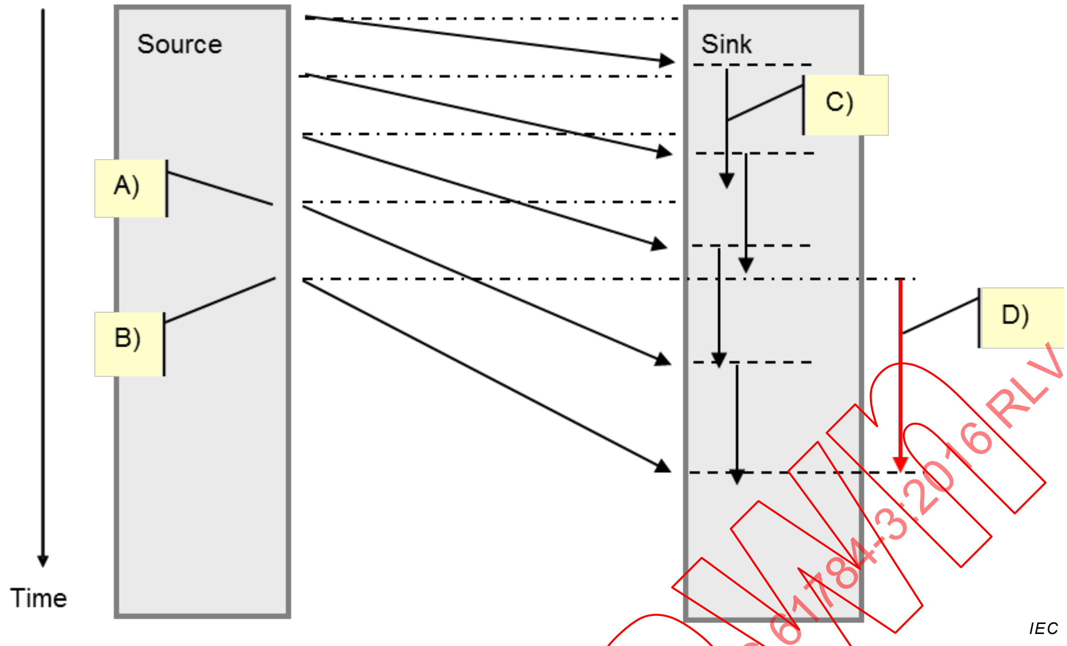
EXAMPLES

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.

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV



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.

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV
Withdrawn

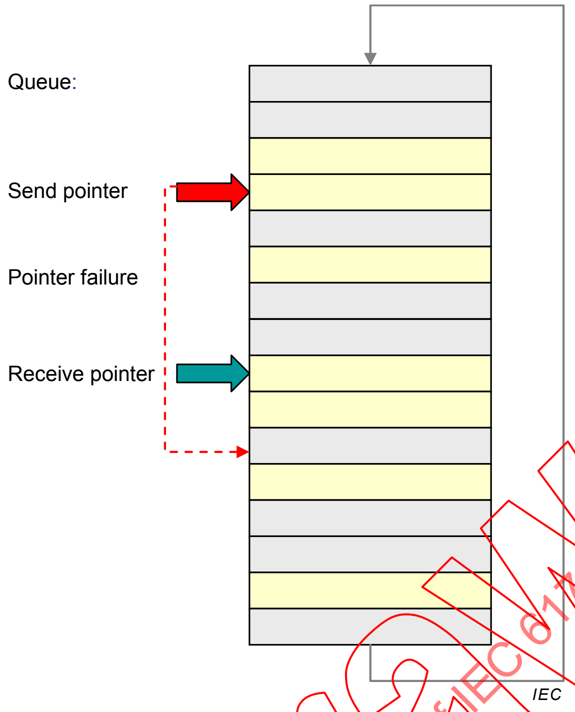


Figure F.5 – Example of an active network element failure

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.

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV
Withdrawn

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.

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

Withdrawn

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.

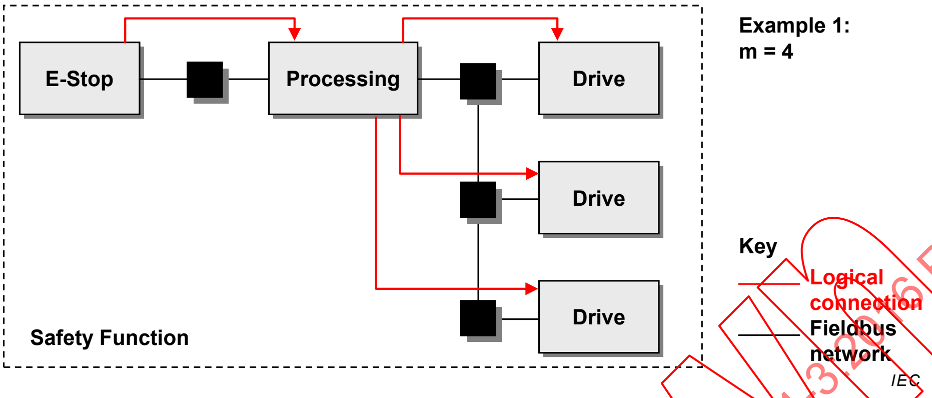


Figure F.6 – Example application 1 (m = 4)

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.

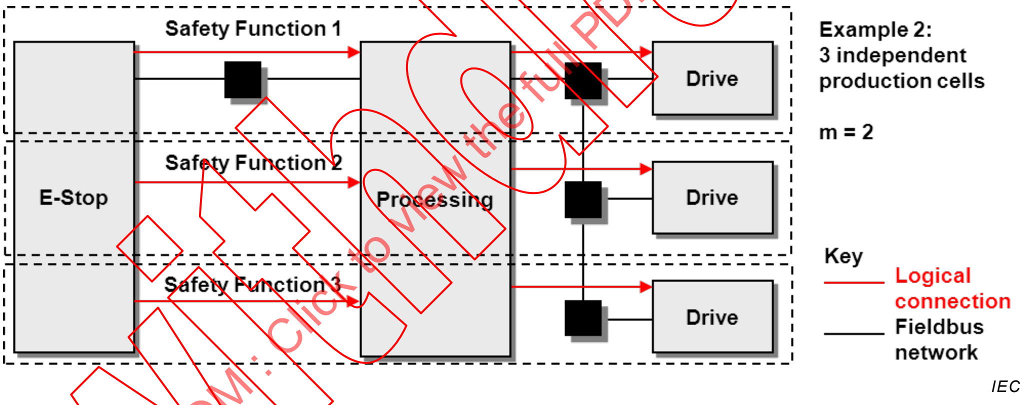


Figure F.7 – Example application 2 (m = 2)

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

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.

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

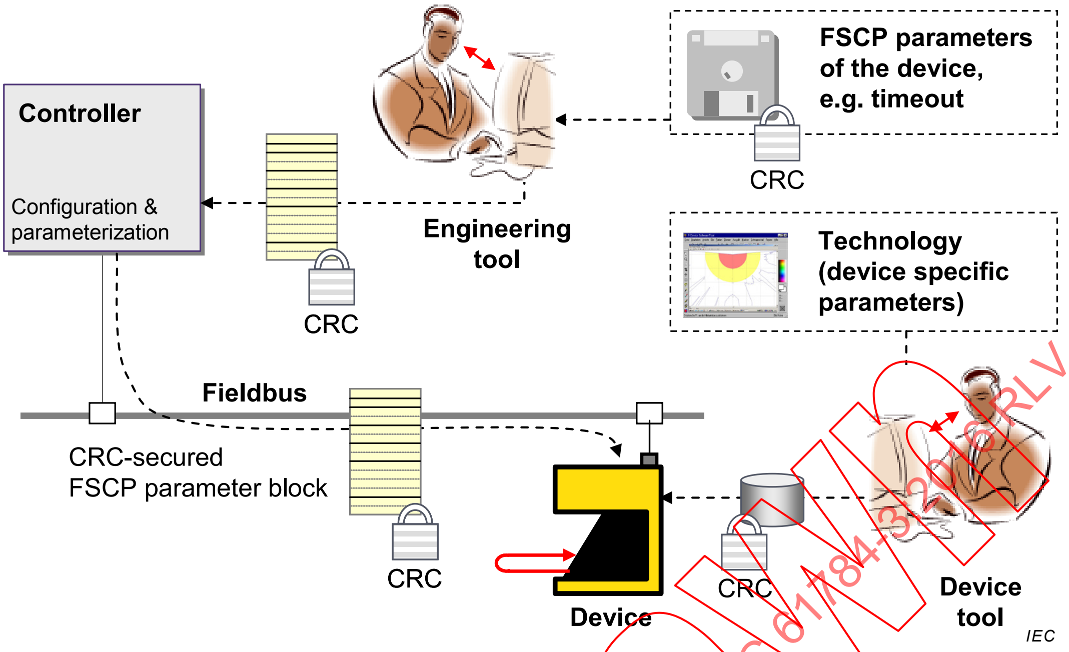

Controller
Configuration & parameterization
CRC
Engineering tool
FSCP parameters of the device, e.g. timeout
CRC
Technology (device specific parameters)
Fieldbus
CRC-secured FSCP parameter block
CRC
Device
CRC
Device tool
IEC

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

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

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.

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

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*

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

[18] Proposed new work item under consideration.

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV
Withdrawn

[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

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

SOMMAIRE

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV
Withdrawn

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

Withdrawn

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

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.

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 annule et remplace la deuxième édition parue en 2010. Cette 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;

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

- 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.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
65C/840/FDIS	65C/848/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à l'approbation de cette norme.

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 cette publication 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.

IECNORM.COM: Click to view the full PDF of IEC 61784-3:2016 RLV
Withdrawn

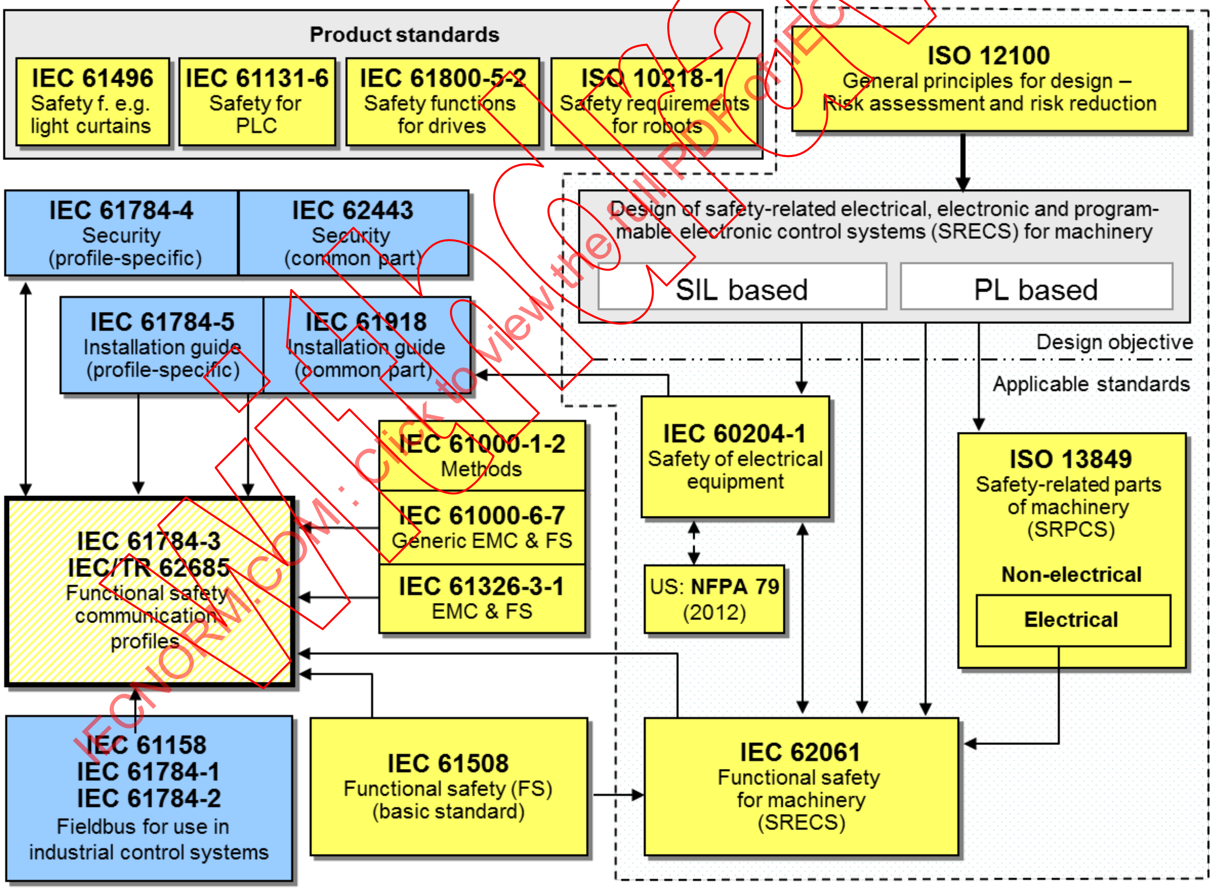
0 Introduction

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.


Product standards
IEC 61496
Safety f. e.g. light curtains
IEC 61131-6
Safety for PLC
IEC 61800-5-2
Safety functions for drives
ISO 10218-1
Safety requirements for robots
ISO 12100
General principles for design – Risk assessment and risk reduction
IEC 61784-4
Security (profile-specific)
IEC 62443
Security (common part)
Design of safety-related electrical, electronic and programmable electronic control systems (SRECS) for machinery
SIL based
PL based
Design objective
Applicable standards
IEC 61784-5
Installation guide (profile-specific)
IEC 61918
Installation guide (common part)
IEC 61000-1-2
Methods
IEC 61000-6-7
Generic EMC & FS
IEC 61326-3-1
EMC & FS
IEC 60204-1
Safety of electrical equipment
US: NFPA 79 (2012)
ISO 13849
Safety-related parts of machinery (SRPCS)
Non-electrical
Electrical
IEC 61784-3
IEC/TR 62685
Functional safety communication profiles
IEC 61158
IEC 61784-1
IEC 61784-2
Fieldbus for use in industrial control systems
IEC 61508
Functional safety (FS) (basic standard)
IEC 62061
Functional safety for machinery (SRECS)

Key 🟨 (yellow) safety-related standards
🟦 (blue) fieldbus-related standards
▨ (dashed yellow) this standard

IEC

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

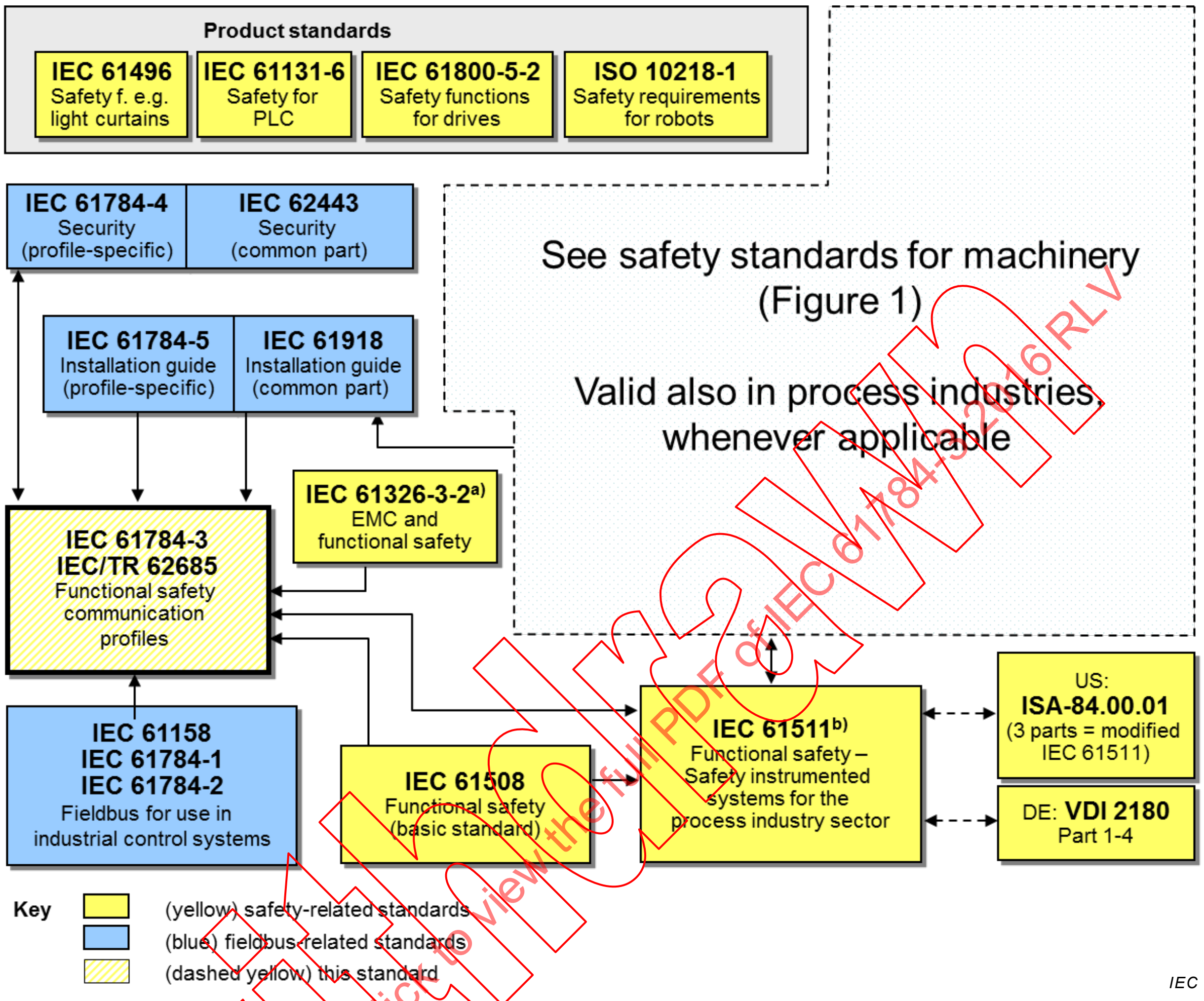
Anglais	Français
Product standards	Normes de produits
Safety function, e.g. light curtains	Fonction de sécurité, par exemple rideaux de lumière
Safety for PLC	Sécurité relative aux automates programmables
Safety functions for drives	Fonctions de sécurité applicables aux entraînements
Safety requirements 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)

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV
Withdrawn

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.


Product standards
IEC 61496 Safety f. e.g. light curtains
IEC 61131-6 Safety for PLC
IEC 61800-5-2 Safety functions for drives
ISO 10218-1 Safety requirements for robots
IEC 61784-4 Security (profile-specific)
IEC 62443 Security (common part)
See safety standards for machinery (Figure 1)
Valid also in process industries, whenever applicable
IEC 61784-5 Installation guide (profile-specific)
IEC 61918 Installation guide (common part)
IEC 61326-3-2a) EMC and functional safety
IEC 61784-3 IEC/TR 62685 Functional safety communication profiles
IEC 61158 IEC 61784-1 IEC 61784-2 Fieldbus for use in industrial control systems
IEC 61508 Functional safety (basic standard)
IEC 61511b) Functional safety – Safety instrumented systems for the process industry sector
US: ISA-84.00.01 (3 parts = modified IEC 61511)
DE: VDI 2180 Part 1-4
Key
(yellow) safety-related standards
(blue) fieldbus-related standards
(dashed yellow) this standard
IEC

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

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.

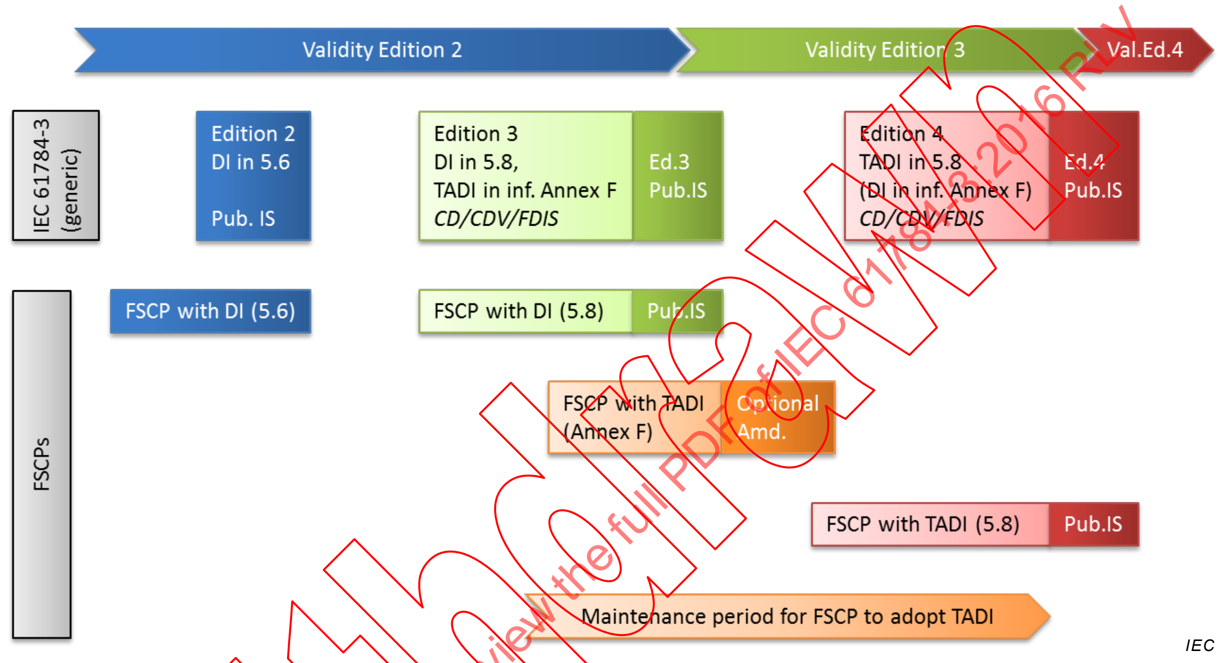
Toutefois, en raison de la durée typique du processus d'évaluation, les Profils de Communication de Sécurité Fonctionnelle publiés avant ou en même temps que cette nouvelle édition de la partie générique ne peuvent être évalués qu'en fonction des méthodes

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

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.



IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

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.

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

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).

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

[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*

IECNORM.COM: Click to view the full PDF of IEC 61784-3:2016 RLV

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*

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV
Withdrawn

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

withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

[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)

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

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]

Withdrawn
IECNORM.COM: Click to view the full PDF of IEC 61784-3:2016 RLV

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.

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

[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

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

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.

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

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.

3.2 Symboles et abréviations

BSC	Binary Symmetric Channel (Canal symétrique binaire)	
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	

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

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)	

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV
Withdrawn

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

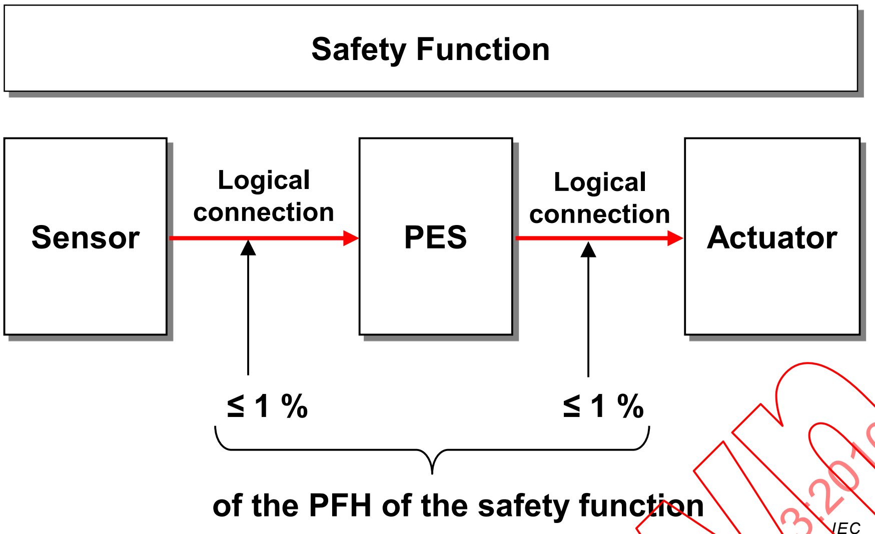
Conformément à l'IEC 61508, une analyse des risques permet de définir les fonctions de sécurité. Ces fonctions de sécurité peuvent être décomposées en parties contribuant à la fonction de sécurité globale (par exemple, capteur(s) – Canal de communication de sécurité – PES(s) – Canal de communication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

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV



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

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

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

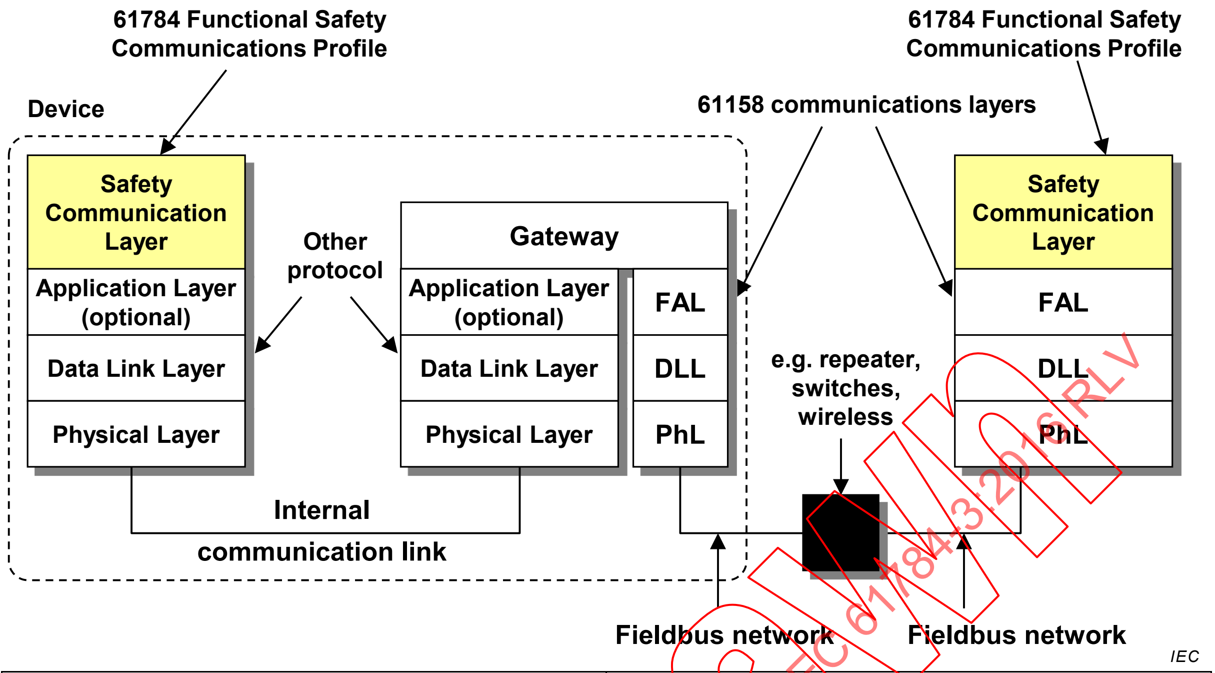
Les informations suivantes permettent une compréhension commune de la technologie et des termes employés.

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.


61784 Functional Safety Communications Profile
Device
Safety Communication Layer
Application Layer (optional)
Data Link Layer
Physical Layer
Other protocol
Gateway
Application Layer (optional)
Data Link Layer
Physical Layer
FAL
DLL
PhL
Internal communication link
61158 communications layers
61784 Functional Safety Communications Profile
e.g. repeater, switches, wireless
Safety Communication Layer
FAL
DLL
PhL
Fieldbus network
Fieldbus network
IEC

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

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV
Withdrawn

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.

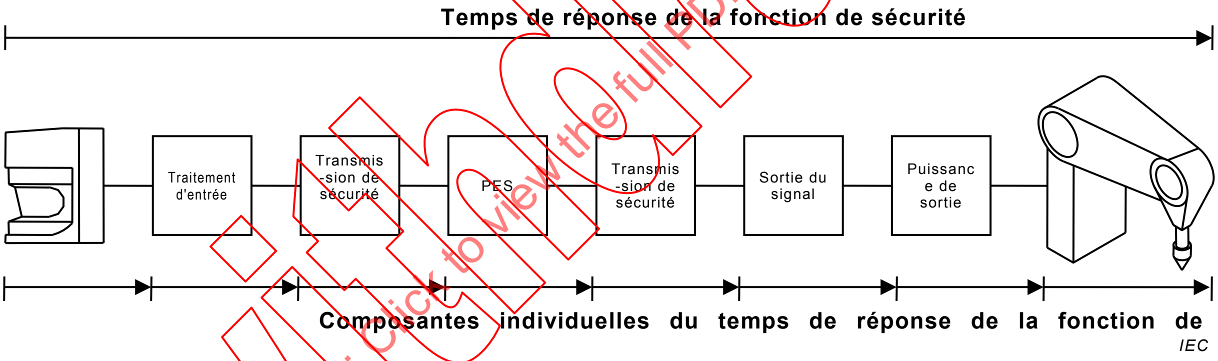

Temps de réponse de la fonction de sécurité
Traitement d'entrée
Transmis-sion de sécurité
PES
Transmis-sion de sécurité
Sortie du signal
Puissance de sortie
Composantes individuelles du temps de réponse de la fonction de
IEC

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.

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 PLV

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.

withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

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.

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

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

IECNORM.COM: Click to view the full PDF of IEC 61784-3:2016 RLV
Withdrawn

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.

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

5.6 Phases de communication

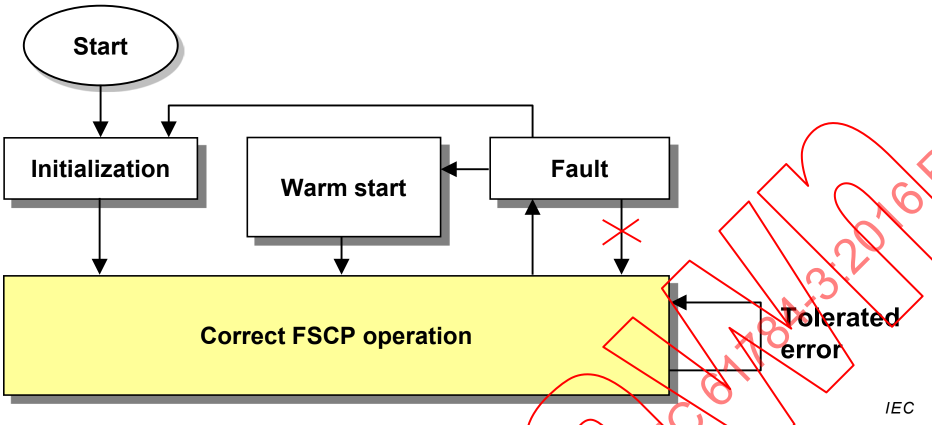
Un FSCP doit être conçu de sorte qu'un état de sécurité ou qu'un taux d'erreurs résiduelles suffisant du côté du récepteur puisse être atteint, conformément à l'IEC 61508, dans chacune des phases de communication du réseau de sécurité, y compris:

- 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

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV
Withdrawn

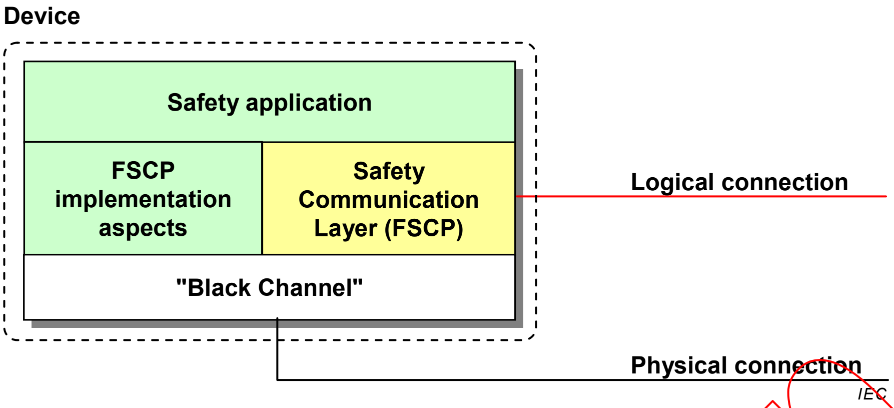
5.7 Aspects relatifs à la mise en œuvre du FSCP

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

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

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)

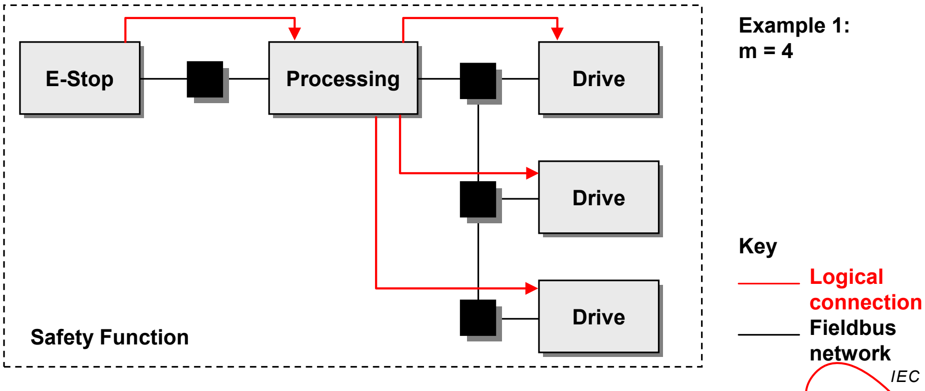
Le nombre m de connexions logiques dépend de l'application de la fonction de sécurité individuelle. La Figure 9 et la Figure 10 présentent la manière dont ce nombre peut être déterminé.

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.

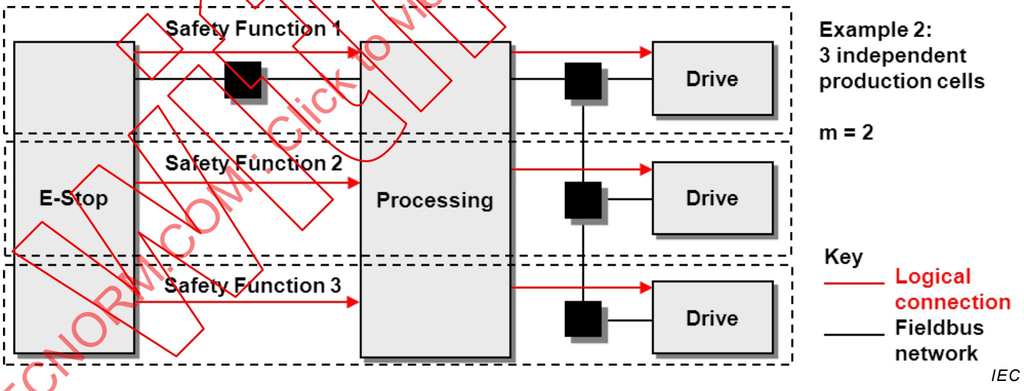
IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV
WITHDRAWN



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)

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

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

IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV
Withdrawn

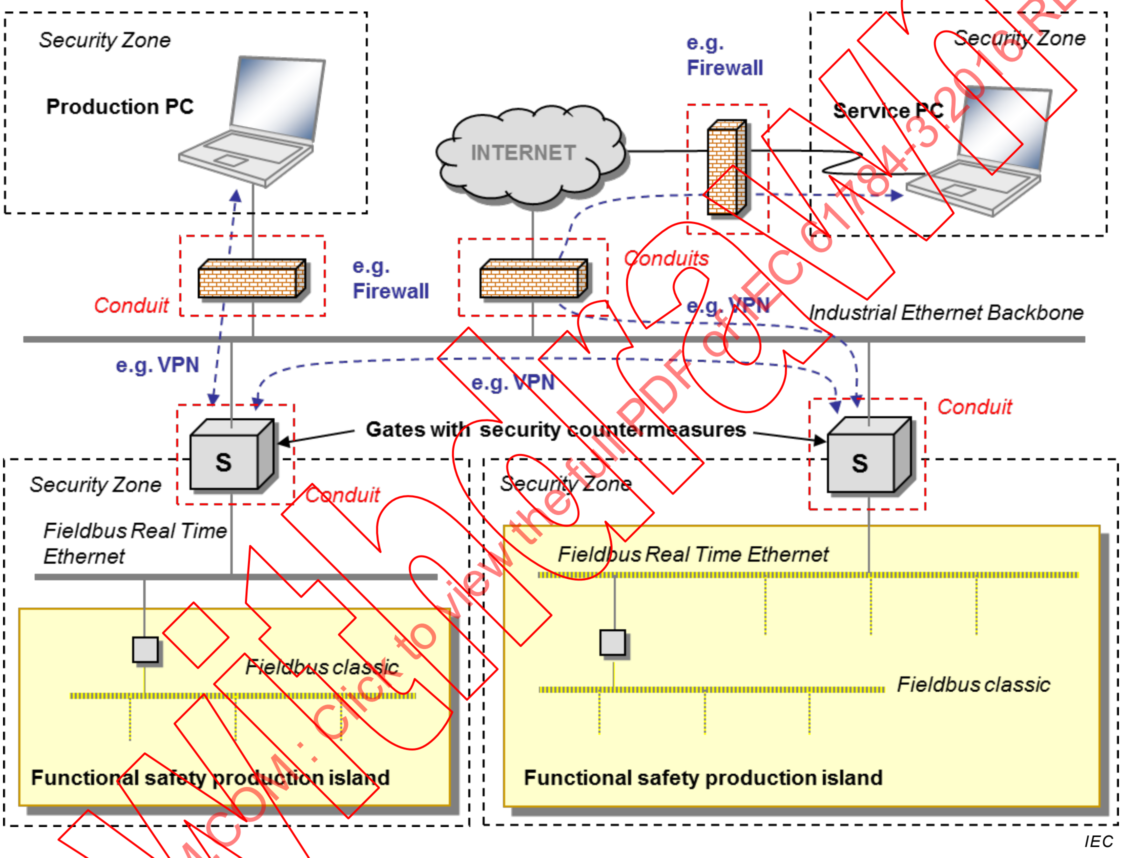
appropriées pour atteindre le niveau de sûreté cible et satisfaire à ses sept exigences fondamentales (vecteur) pour les zones et les conduits.

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.



IECNORM.COM : Click to view the full PDF of IEC 61784-3:2016 RLV

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