IEC 61784-3

Edition 4.1 2024-04
CONSOLIDATED VERSION

INTERNATIONAL STANDARD

colour inside

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

IEC 61784-3:2021-02+AMD1:2024-04 CSV(en)

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

Tel.: +41 22 919 02 11
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 corrigendum or an amendment might have been published.

IEC publications search - webstore.iec.ch/advsearchform
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 It also gives information on projects, replaced and withdrawn publications.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 once a month by email.

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: sales@iec.ch.

IEC Products & Services Portal - products.iec.ch
Discover our powerful search engine and read freely all the publications previews, graphical symbols and the glossary. With a subscription you will always have access to up to date content tailored to your needs.

Electropedia - www.electropedia.org
The world's leading online dictionary on electrotechnology, containing more than 22 500 terminological entries in English and French, with equivalent terms in 25 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC 61784-3

Edition 4.1 2024-04
CONSOLIDATED VERSION

INTERNATIONAL STANDARD

colour inside

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

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 25.040.40, 35.100.05

ISBN 978-2-8322-8373-8

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

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES –

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

FOREWORD

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

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

IEC 61784-3 edition 4.1 contains the fourth edition (2021-02) [documents 65C/1067/FDIS and 65C/1072/RVD] and its amendment 1 (2024-02) [documents 65C/1284/FDIS and 65C/1291/RVD].

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

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

This fourth edition constitutes a technical revision.

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

- Contents of previous Annex F were corrected based on feedback from peer review and subsequent analysis (in particular deletion of RP_U for data integrity, reduction of the Equation for RR_A, and clarifications on the values of RP_I and R_T).
- Additional assumptions for residual error rate calculations, clarification of assumption a).
- After correction, contents of previous Annex F were exchanged with the contents of previous Subclause 5.8.
- Contents of Subclause 5.9 on security replaced by a simple reference to IEC 62443 in accordance with Guide 120.
- Changes in Annex B: Dependency of this Annex B with the BSC model has been highlighted. First two paragraphs and figure in Clause B.2 have been deleted because of little relevance. The approximation Equation (B.4) has been deleted due to obsolescence, based on the observations that the CRC shall be anyway explicitly calculated in order to prove properness, and that it may produce optimistic results. Guidance for calculation of R_{CRC} in B.4.2 has been reviewed.
- Changes in Annex D: Formula D.1 was changed from an approximation to a proper Equation, with some adjustments, and contents of D.4.3 were clarified (default safety action).
- New informative Annex H, providing additional guidance for the calculation of RCRC.

This document 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 document and its amendment will remain unchanged until the stability date indicated on the IEC website under webstore.iec.ch in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn, or
- revised.

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

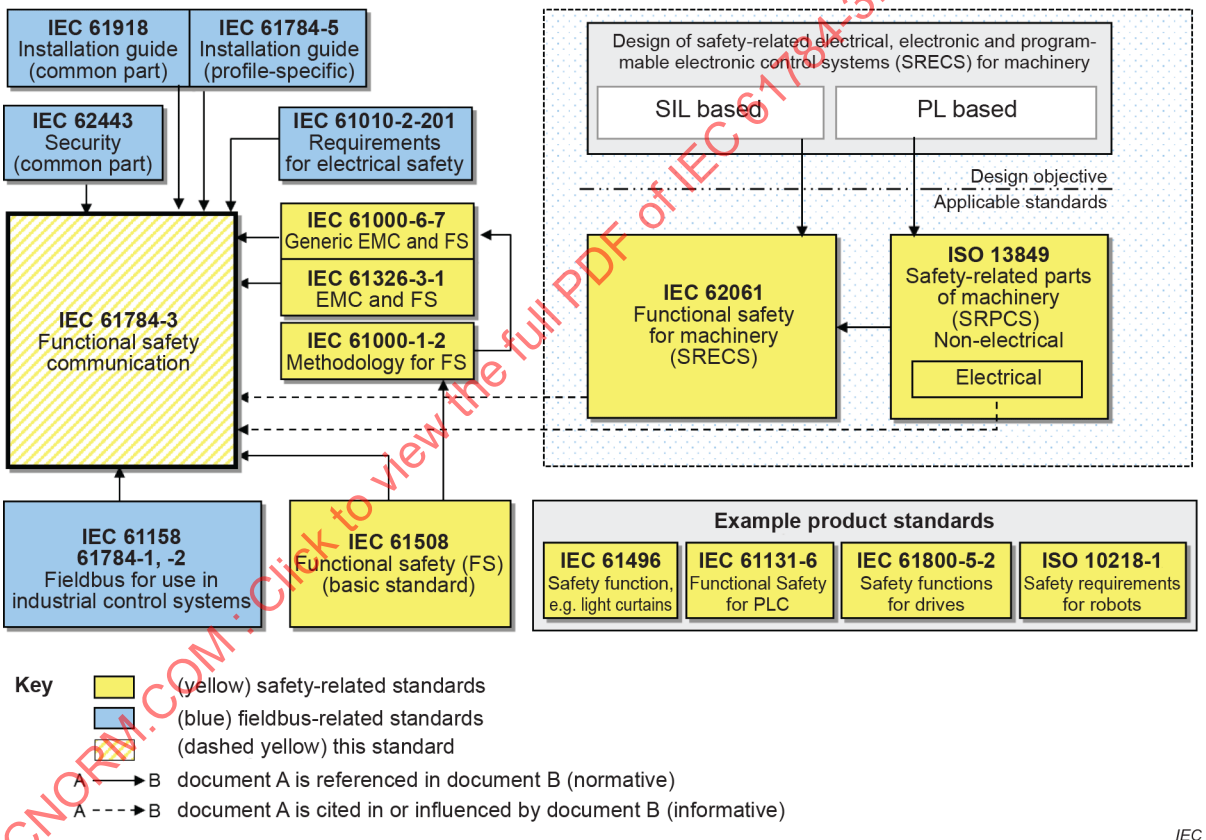
0 Introduction

0.1 General

The IEC 61158 (all parts) 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 and safety-related applications.

IEC 61784-3 (all parts) explains the relevant principles for functional safety communications with reference to IEC 61508 (all parts) 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 IEC 61158 (all parts). It does not cover electrical safety and intrinsic safety aspects. It also does not cover security aspects, nor does it provide any requirements for security.

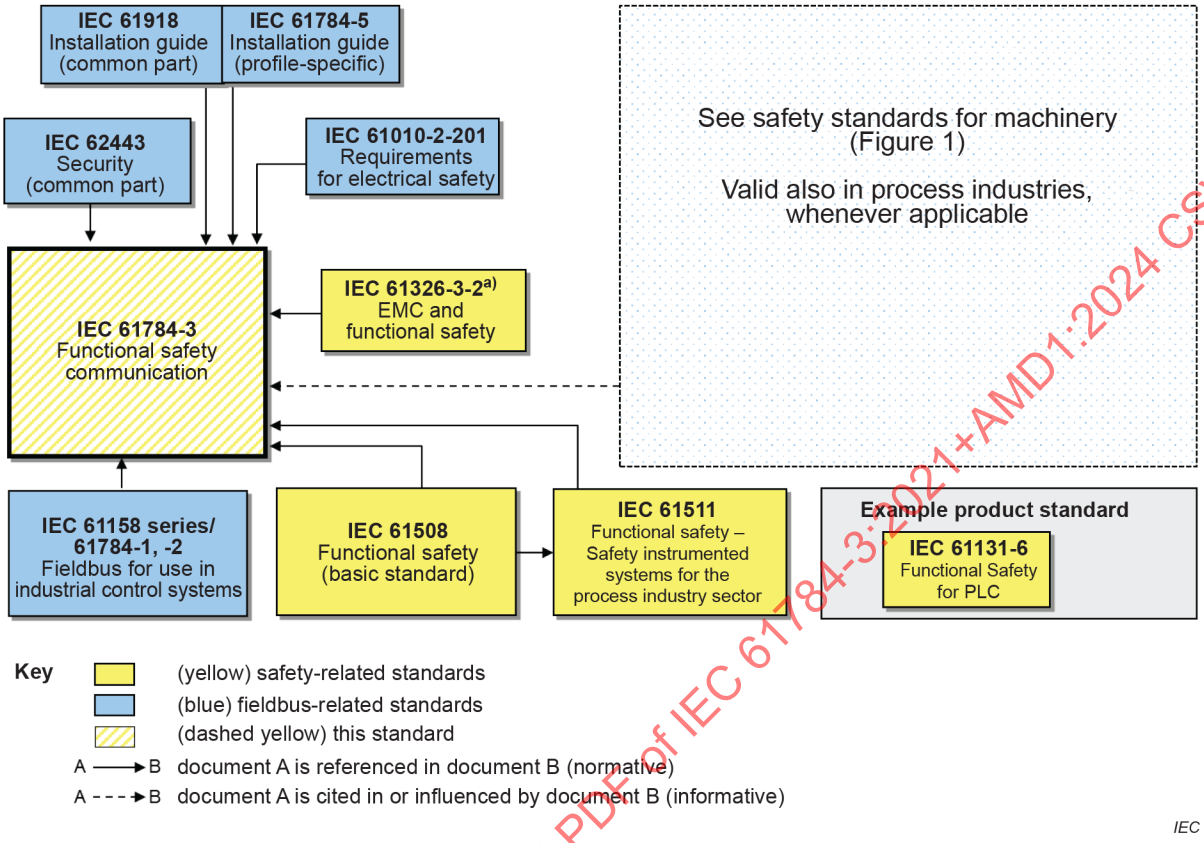
Figure 1 shows the relationships between IEC 61784-3 (all parts) and relevant safety and fieldbus standards in a machinery environment.



NOTE IEC 62061 specifies the relationship between PL (Category) and SIL.

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

Figure 2 shows the relationships between IEC 61784-3 (all parts) and relevant safety and fieldbus standards in a process environment.



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

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

Safety communication layers which are implemented as parts of safety-related systems according to IEC 61508 (all parts) 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 IEC 61784-3 (all parts) 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.

IEC 61784-3 (all parts) describes:

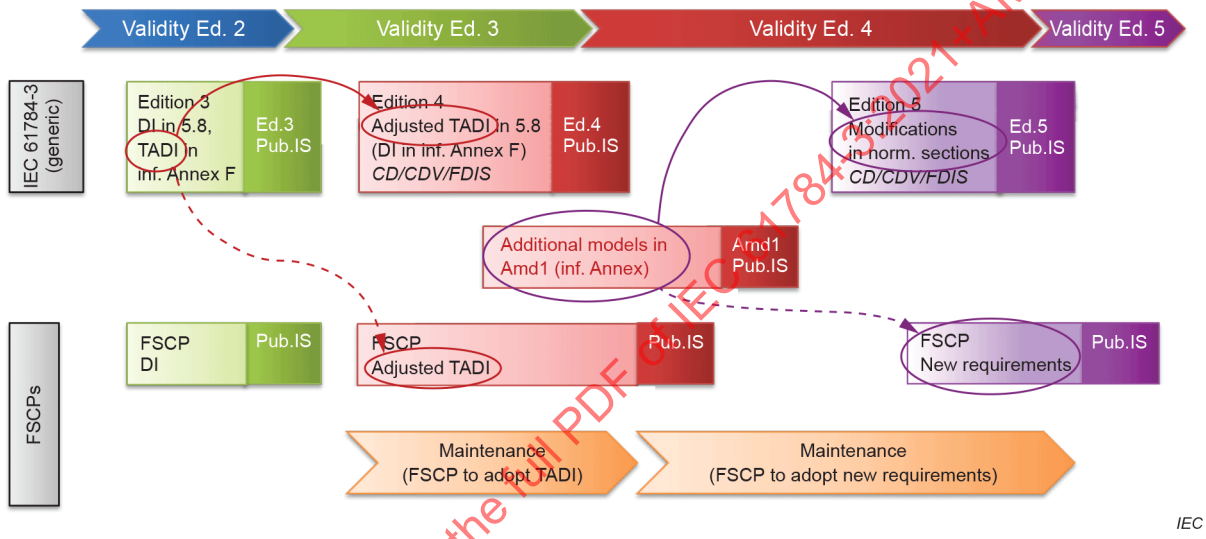
- basic principles for implementing the requirements of IEC 61508 (all parts) for safety-related data communications, including possible transmission faults, remedial measures and considerations affecting data integrity;
- functional safety communication profiles for several communication profile families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

0.2 Use of extended assessment methods in Edition 4

This edition of the generic part of IEC 61784-3 (all parts) includes extended models for 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 5.8.

Upon publication of this new edition of the generic part, FSCPs shall be assessed using the methods from this Edition 4, based on the extended models specified in 5.8 (derived from a modified version of Annex F of Edition 3). The informative Annex F contains the legacy models for reference purpose only.

Figure 3 shows the transitions from original assessment methods of Edition 2 to extended assessment methods in this Edition 4 and the future Edition 5.



Key

DI Data Integrity

TADI Timeliness, Authenticity, Data Integrity

Figure 3 – Transitions from Ed. 2 to Ed. 4 and future Ed. 5 assessment methods

0.3 Patent declaration

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

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

The holders of these patent rights have assured IEC that they are willing to negotiate licences under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statements of the holders of these patent rights are registered with IEC. Information may be obtained from the patent database available at http://patents.iec.ch.

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

INTRODUCTION to Amendment 1

This Amendment 1 discusses the concepts of a comprehensive channel model for data integrity calculations for functional safety communications protocols (FSCPs) as specified in IEC 61784-3:2021. The comprehensive channel model addresses data corruption error types where multiple contiguous bits are affected by a single fault.

It also reviews typical relationships between the possible errors and the various safety measures which can be implemented.

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 (all parts)[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 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 IEC 61158 (all parts). 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 (all parts) can exist that are not included in IEC 61784-3 (all parts).

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

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

NOTE 3 Implementation of a functional safety communication profile according to this document in a device is not sufficient to qualify it as a safety device, as defined in IEC 61508 (all parts).

NOTE 4 The resulting SIL claim of a system depends on the implementation of the selected functional safety communication profile within this system.

NOTE 5 Annex C explains the numbering scheme used for the technology-specific parts (IEC 61784-3-x) as well as their common general structure.

NOTE 6 Annex D provides a guideline for the assessment and test of safety communication profiles as well as safety-related devices using these profiles.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 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 document, “IEC 61508” will be used for “IEC 61508 (all parts)”.

IEC 61010-2-201, *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/IEEE 8802-3*

IEC 61784-3 (all parts), *Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses*

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

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

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

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

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

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

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

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

IEC 61784-3-17, *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 61918:2018, *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.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp

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 of "devices" and "fieldbus" instead of "entities" and "transmission system"]

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 61918:2018, 3.1.2]

3.1.3
bit error probability
Pe
probability for a given bit to be received with the incorrect value

3.1.4
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.

3.1.5
bridge
abstract device that connects multiple network segments along the data link layer

3.1.6
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]

3.1.7
communication channel
logical connection between two end-points within a *communication system*

3.1.8
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

3.1.9
connection
logical binding between two application objects within the same or different devices

3.1.10
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 document to refer to the redundant data.

Note 2 to entry: See also [71], [72][2].

3.1.11
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 (all parts), using for example zones and conduits

3.1.12
device
physical entity connected to the fieldbus composed of communication element and possibly other functional elements

[SOURCE: IEC 61158-2:2014, 3.1.13, modified – Note to entry and some details have been deleted.]

2 Figures in square brackets refer to the bibliography.

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]

3.1.14
DLPDU
DEPRECATED: frame
Data Link Protocol Data Unit

3.1.15
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]

3.1.16
explicit code
code for safety measure that is actually transmitted within the SPDU and is known to the sender and receiver

3.1.17
explicit data
data that is transmitted

Note 1 to entry: Explicit data is defined in contrast to implicit data.

3.1.18
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]

3.1.19
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]

3.1.20
fieldbus
communication system based on serial data transfer and used in industrial automation or process control applications

3.1.21
fieldbus system
system using a *fieldbus* with connected devices

3.1.22
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 [71], [72].

3.1.23
functional safety communication profile
FSCP
technology specification for the implementation of an SCL

3.1.24
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.

3.1.25
hazard
potential source of harm

Note 1 to entry: The term includes danger to persons arising within a short time scale (for example, fire and explosion) and also those that have a long-term effect on a person's health (for example, release of a toxic substance).

[SOURCE: IEC 61508-4:2010, 3.1.2 and ISO/IEC Guide 51:2014, definition 3.2]

3.1.26
implicit code
code for safety measure that is not transmitted within the SPDU but is known to the sender and receiver

3.1.27
implicit data
additional data that is not transmitted but is known to the sender and receiver, and used in the encoding and decoding of the message/SPDU

Note 1 to entry: Implicit data is defined in contrast to explicit data.

[SOURCE: IEC 62280:2014, 3.1.25, modified – addition of ", and used in the encoding and decoding of the message/SPDU" and of Note 1 to entry]

3.1.28
master
communication entity able to initiate and schedule communication activities by other stations which may be masters or slaves

3.1.29
message
<information theory and communication theory> ordered sequence of characters (usually octets) intended to convey information

[SOURCE: ISO/IEC 2382:2015, 2123205, modified – insertion of "(usually octets)", deletion of notes and source]

3.1.30
message sink
information sink
part of a *communication system* in which *messages* are considered to be received

[SOURCE: ISO/IEC 2382:2015, 2123207, modified – deletion of notes and source]

3.1.31
message source
information source
part of a *communication system* from which *messages* are considered to originate

[SOURCE: ISO/IEC 2382:2015, 2123206, modified – deletion of notes and source]

3.1.32
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]

3.1.33
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]

3.1.34
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]

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

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

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

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

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

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

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

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

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

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

3.1.44
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 document.

3.1.45
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.

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

3.1.46
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.

3.1.47
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.

3.1.48
safety-related application
programs designed in accordance with IEC 61508 to meet the SIL requirements of the application

3.1.49
safety-related system
system performing *safety functions* according to IEC 61508

3.1.50
slave
communication entity able to receive messages and send them in response to another communication entity which may be a master or a slave, but not to initiate communication activities

3.1.51
spurious trip
trip caused by the safety system without a process demand

3.1.52
time stamp
time information included in a *message*

3.1.53
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.

3.1.54
white channel
defined communication system in which all relevant hardware and software elements are designed, implemented and validated according to IEC 61508

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

3.1.55
uniformly distributed segment
UDS
segment of a message consisting of contiguous bits within which error patterns are uniformly distributed

3.2 Symbols and abbreviated terms

3.2.1 Abbreviated terms

A-code	Authenticity code	
BSC	Binary Symmetric Channel	(see Clause B.2)
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 (all parts)]
FCS	Frame Check Sequence	
FIT	Failure In Time (equals 10^{-9} failure per hour)	
FS	Functional Safety	
FSCP	Functional Safety Communication Profile	
IACS	Industrial Automation and Control System	
MTBF	Mean Time Between Failures	
MTTF	Mean Time To Failure	
NSR	Non Safety Related	
PDU	Protocol Data Unit	[ISO/IEC 7498-1]
PELV	Protective Extra Low Voltage	[IEC 61010-2-201]
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	
SC	Safety Communication Channel	
SCL	Safety Communication Layer	
SELV	Safety Extra Low Voltage	[IEC 61010-2-201]
SIS	Safety Instrumented Systems	

SIL	Safety Integrity Level	[IEC 61508-4:2010]
SMS	Security Management System	[IEC 62443 (all parts)]
SPDU	Safety PDU	
SR	Safety Related	
T-code	Timeliness code	
UDS	uniformly distributed segment	

3.2.2 Symbols

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

4 Conformance

Each functional safety communication profile within IEC 61784-3 (all parts) is based on communication profiles of IEC 61784-1 or IEC 61784-2 and protocol layers of IEC 61158 (all parts).

A statement of conformance to a Functional Safety Communication Profile (FSCP) of IEC 61784-3 (all parts) shall be stated as either

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

or

conformance to IEC 61784-3 (Ed.y.z) 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.y.z)

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 document performs transmission of safety data. To simplify system calculations, it is recommended that any logical connection of the 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 5.8.11).

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.

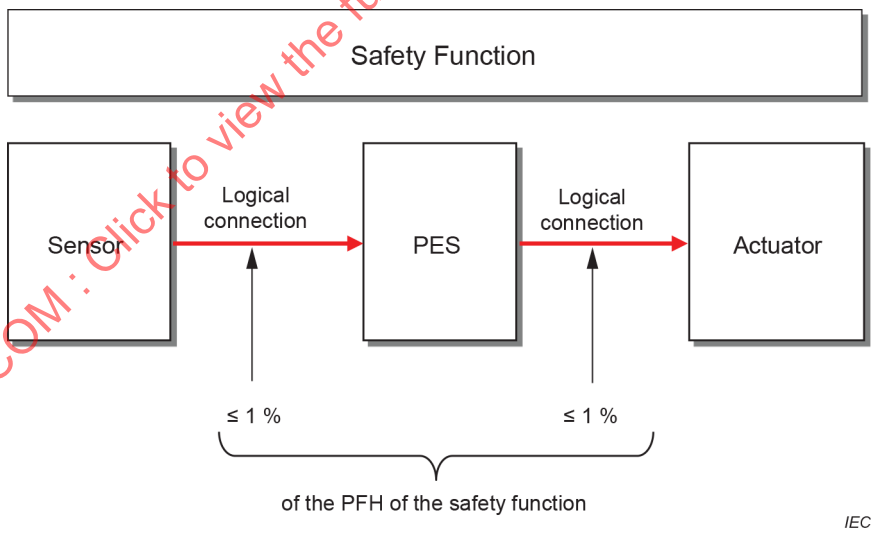


Figure 4 – Safety communication as a part of a safety function

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.

In any case, the safety manual for this FSCP shall provide guidance on the calculations of the PFH or PFD_{avg} for a safety function (see 5.8.10).

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 document focuses on the use of fieldbus based functional safety communication systems. Figure 5 shows an example model of the use of functional safety communications with a fieldbus based on the black channel approach.

When using IEC 61158 based fieldbus structures without modifications in the definition of each communication layer, all the measures necessary to implement transmission of safety data in accordance with the requirements of IEC 61508 shall be performed by an additional "safety communication layer", positioned as shown in Figure 5.

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

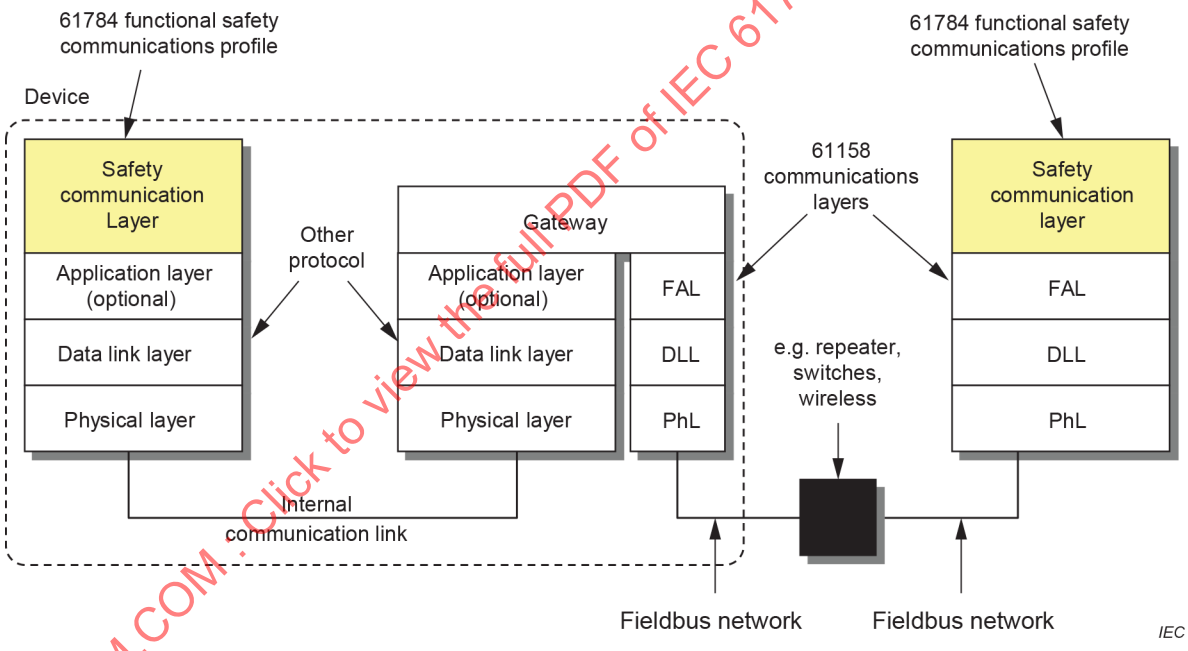


Figure 5 – Example model of a functional safety communication system

While implementation of the Fieldbus Application Layer (FAL) is required for functional safety communication systems according to this document, 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 "black channel" or "white channel" to define the requirements of the base fieldbus for transmission of safety data. This document 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 (all parts).

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

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

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

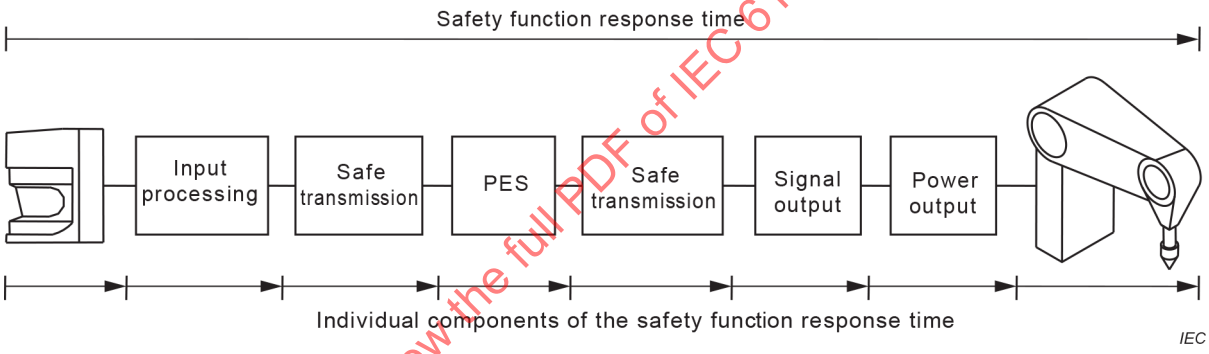


Figure 6 – Example of safety function response time components

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

5.3 Communication errors

5.3.1 General

Subclauses 5.3.2 to 5.3.9 specify possible communication errors. Additional notes are provided to indicate the typical behaviour of a black channel.

5.3.2 Corruption

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

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

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

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

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

5.3.3 Unintended repetition

Due to an error, fault or interference, messages are repeated.

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

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

5.3.4 Incorrect sequence

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

NOTE 1 This "incorrect sequence" error is also referred to as "out-of-sequence" error.

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

NOTE 3 When multiple sequences are active, such as messages from different source entities or reports relating to different object types, these sequences are monitored separately, and errors can be reported for each sequence.

5.3.5 Loss

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

5.3.6 Unacceptable delay

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

5.3.7 Insertion

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

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

5.3.8 Masquerade

Due to a fault or interference, a message from a non-safety related source is interpreted in such a way that it appears to originate from a valid safety related source entity. Non-safety related data would therefore 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 passphrases 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~~ 5.4.8 list measures commonly used to detect deterministic errors and failures of a communication system, as contrasted to stochastic errors like message corruption due to electromagnetic interference.

5.4.2 Sequence number

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

5.4.3 Time stamp

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

NOTE Relative time stamps and absolute time stamps can be used.

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

5.4.4 Time expectation

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

EXAMPLE

Time-slot-oriented access method:

– the exchange of messages takes place within fixed cycles and predetermined time slots for every participant;

– optionally, every participant sends his data within its time slot even if there is no value change (this is an example of cyclic communication);

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

5.4.5 Connection authentication

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

5.4.6 Feedback message

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

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

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

5.4.7 Data integrity assurance

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

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

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

5.4.8 Redundancy with cross checking

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

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

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

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

~~**5.4.9 Different data integrity assurance systems**~~

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

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

5.5 Typical relationships between errors and safety measures

The safety measures outlined in 5.4 can be related to the set of possible errors, defined in 5.3. Typical relationships are shown in Table 1, actual relationships shall be specified by each FSCP. Each safety measure can provide protection against one or more errors in the transmission. It shall be demonstrated that there is at least one corresponding safety measure or combination of safety measures for the defined possible errors in accordance with Table 1.

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

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

Table 1 – ~~Overview of the effectiveness of the various measures on the possible errors~~ Typical relationships between errors and safety measures

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] X	
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		X	X [d]	X	X	~~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 A reaches the values required in 5.4.9 when two messages are sent through independent transceivers.~~ Void

[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~~ acknowledging of the feedback message.

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

5.6 Communication phases

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

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

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

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

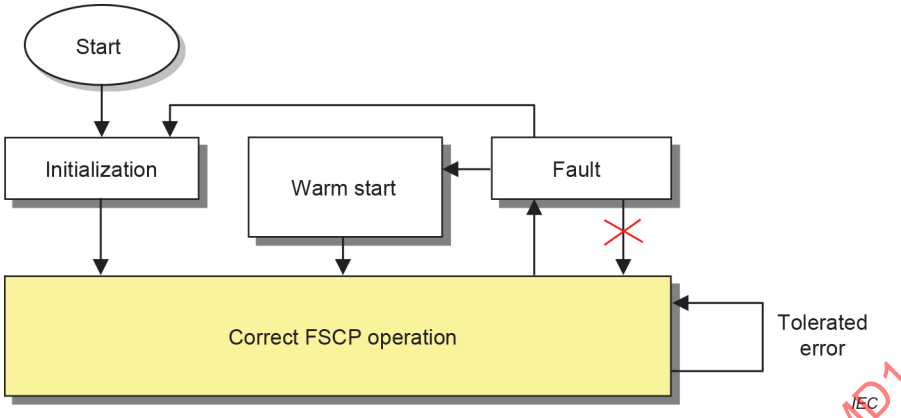


Figure 7 – Conceptual FSCP protocol model

5.7 FSCP implementation aspects

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

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

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

This document 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 endpoints (using only basic assumptions on the black channel performance as stated in the safety manuals of the individual FSCPs).

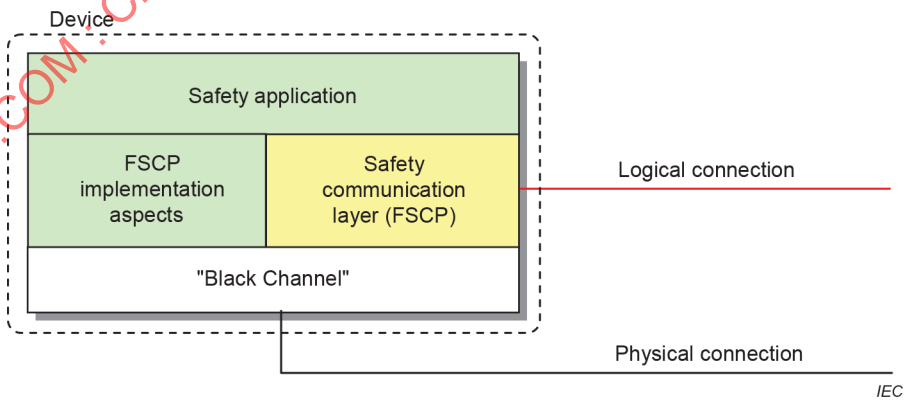


Figure 8 – FSCP implementation aspects

5.8 Models for estimation of the total residual error rate

5.8.1 Applicability

Subclause 5.8 specifies models for estimating the total residual error rate for an FSCP, for the purpose of assessing this FSCP.

5.8.2 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 9 shows a black channel that contains different types of communication: Fieldbus messages with safety and non-safety PDUs.

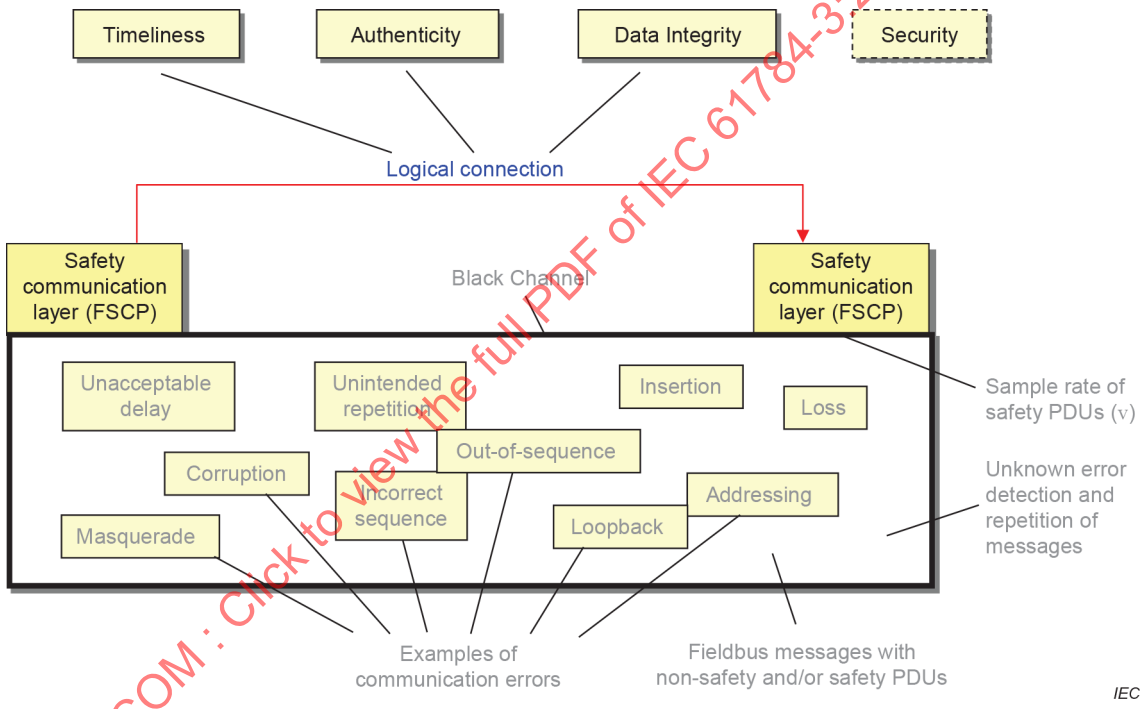


Figure 9 – Black channel from an FSCP perspective

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.

5.8.3 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 9):

- data integrity;
- authentication;
- 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 correct 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 document. Security issues are addressed in IEC 62443 (all parts).

Another generic safety aspect that shall be considered is the configuration and/or parameterization of the FSCP (see 5.8.12).

A fault in any of these generic safety measures may result in a hazard.

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 5.8.10.

5.8.4 Assumptions for residual error rate calculations

Subclause 5.8 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 5.8:

a) assuming a failure rate of an average black channel device to be 10^{-7}/h (100 FIT), the black channel device failure rate is taken to be 10 000 times this value for SCL calculations. Therefore, the 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 The error rate of 10^{-3} for a non-safety device is derived from ISO 13849-1:2015, Table 7, using a conservative margin compared to the weakest performance level.

   NOTE 3 A failure rate less conservative than 10^{-3}/h 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}/h would therefore render the safety communication channel inoperable.

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

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

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

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

f) each logical connection is assigned a unique authentication code, which is known to both sender and receiver prior to transmission of SPDUs;

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;

i) the CRC calculation is performed on the entire SPDU, including A-code and T-code.

5.8.5 Residual error rates

5.8.5.1 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 1 Implicit mechanism is typically used to accommodate limited systems with fixed black channel message sizes, slow transmission rates, or low-cost implementations.

The FSCPs specified in IEC 61784-3 (all parts) 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. Proof of sufficiently low residual error probability shall be demonstrated specifically for each FSCP. Therefore, Subclause 5.8 only deals with the explicit category.

NOTE 2 Annex G presents formulae examples for special cases, in order to provide guidance for the development of additional formulae for the residual error probabilities of FSCPs using implicit data safety mechanisms.

5.8.5.2 Residual error rate calculations

5.8.5.2.1 General

Subclauses 5.8.5.2.2 to 5.8.5.2.5 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.

5.8.5.2.2 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 (1).

$$RR_I = RP_I \times v \times RP_{FSCP\_I} \quad (1)$$

where

RR_I is the residual error rate for Data Integrity;

RP_I is the residual error probability for Data Integrity (see 5.8.6.3);

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

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

The measures used for RP_{FSCP_I} shall be independent of the data integrity measure.

5.8.5.2.3 Contribution of authenticity errors (RR_A)

There are three conditions necessary for this residual rate:

a) a misdirected PDU;

b) bit errors in the received authentication code resulting in a match with the expected authentication code, and

c) these bit errors are not detected by CRC.

Since the A-code is transmitted explicitly, bit errors in the received authentication code are already considered in the calculation of RP_I.

Since v is the maximum message sample rate, R_A (rate of occurrence for misdirected safety PDUs, see 5.8.7.2) is included in v.

As a result, a value of 0 (zero) will be used for RR_A in all equations where this term appears.

5.8.5.2.4 Contribution of timeliness errors (RR_T)

An example for the calculation of the residual error rate for Timeliness RR_T is shown in Equation (2).

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

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 (see 5.8.8.2) (value cannot exceed v, as specified in 5.8.5.2.2);

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

The measures used for RP_{FSCP_T} shall be independent of the timeliness measure.

Unlike the A-code, the T-code value changes over time, and therefore data integrity measures are necessary but not sufficient to detect timeliness errors.

5.8.5.2.5 Contribution of masquerade errors (RR_M)

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 (3). This Equation (3) assumes the SPDU structure differs from the structure of non-safety PDUs in terms of location of the fields of uniqueness.

$$RP_U = \frac{V_{A1}}{V_{R1}} \times \frac{V_{A2}}{V_{R2}} \times \ldots \times \frac{V_{AN}}{V_{RN}} \quad (3)$$

where

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

V_{Ai} is the number of values accepted by a sink in data field i (i = 1…N);

V_{Ri} is the number of values representing the total range for data field i (i = 1…N).

An example for the calculation of the residual error rate for Masquerade RR_M is shown in Equation (4).

$$RR_M = 2^{-LA} \times 2^{-LT} \times w \times 2^{-r} \times RP_U \times 2^{-LR} \times R_M \quad (4)$$

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 (see 5.8.9.2).

5.8.6 Data integrity

5.8.6.1 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;

– measures to assure that each SPDU checked by the black channel CRC is also checked by the SCL CRC since additional trials in the black channel with identical check would increase the Residual Error Rate.

5.8.6.2 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.

5.8.6.3 Residual error probability for data integrity RP_I

RP_I is the residual error probability for Data Integrity.

EXAMPLE See R_{CRC} in Annex B.

Annex B provides information on CRC-based error checking to address data integrity. Example literature is listed in B.4.2.

NOTE Annex I complements Annex B by providing a comprehensive data integrity model using CRC-based error checking.

5.8.7 Authenticity

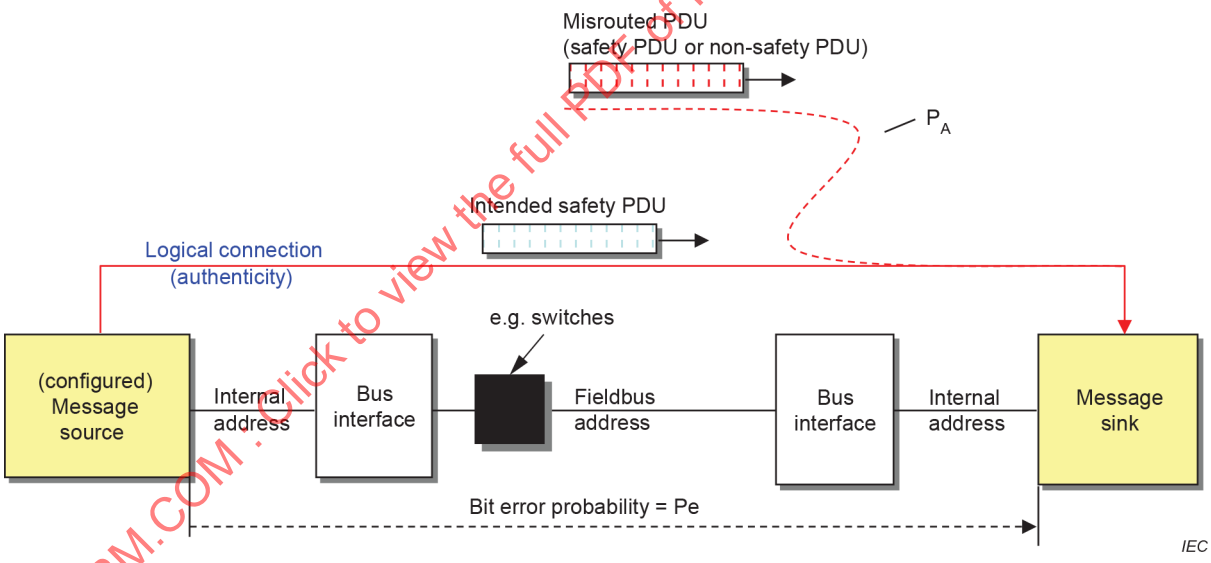
5.8.7.1 General

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 10):

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



Key

PA Probability of an authenticity error for logical connections

Figure 10 – Model for authentication considerations

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

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

NOTE

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

– falsification of an address within the message or an error within an internal communication link (see Figure 11) 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 11 shows typical locations of addressing errors due to corrupted addresses within the fieldbus communication system or possible internal addressing errors (for example due to corrupted pointers within modular remote I/O devices).

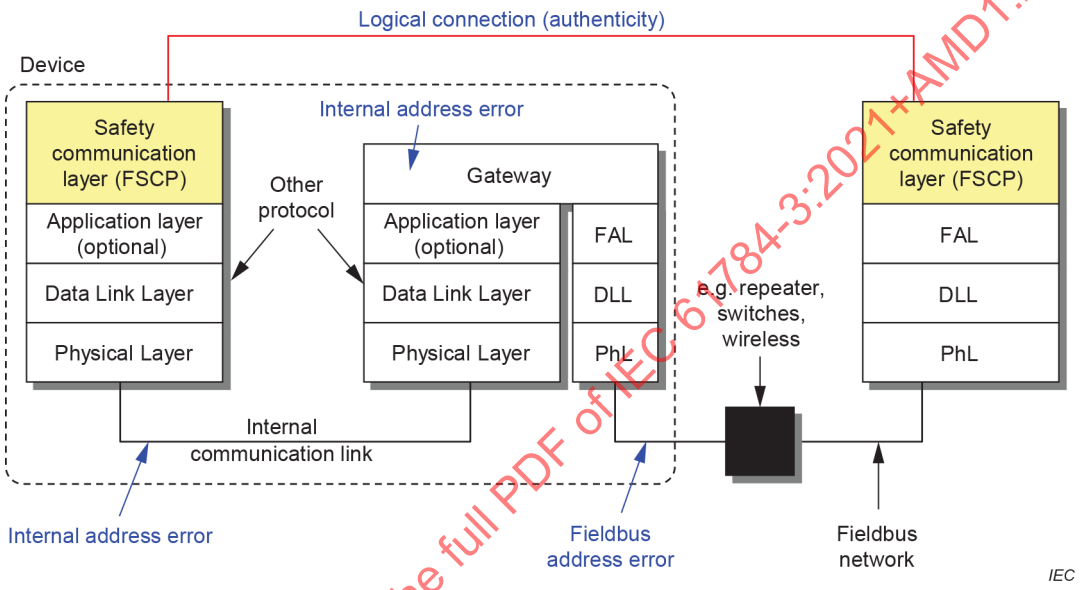


Figure 11 – Fieldbus and internal address errors

Additional systematic causes for incorrect authenticity may be identified within configuration and parameterization procedures as shown in 5.8.12. 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.

5.8.7.2 Rate of occurrence of misdirected SPDUs (R_A)

In accordance with 5.8.4 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 technical measures for the authentication can be supplemented by organizational measures, which shall be practical for the user to perform (see 5.8.12).

5.8.8 Timeliness

5.8.8.1 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 act as a message source and a message sink at the same time.

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

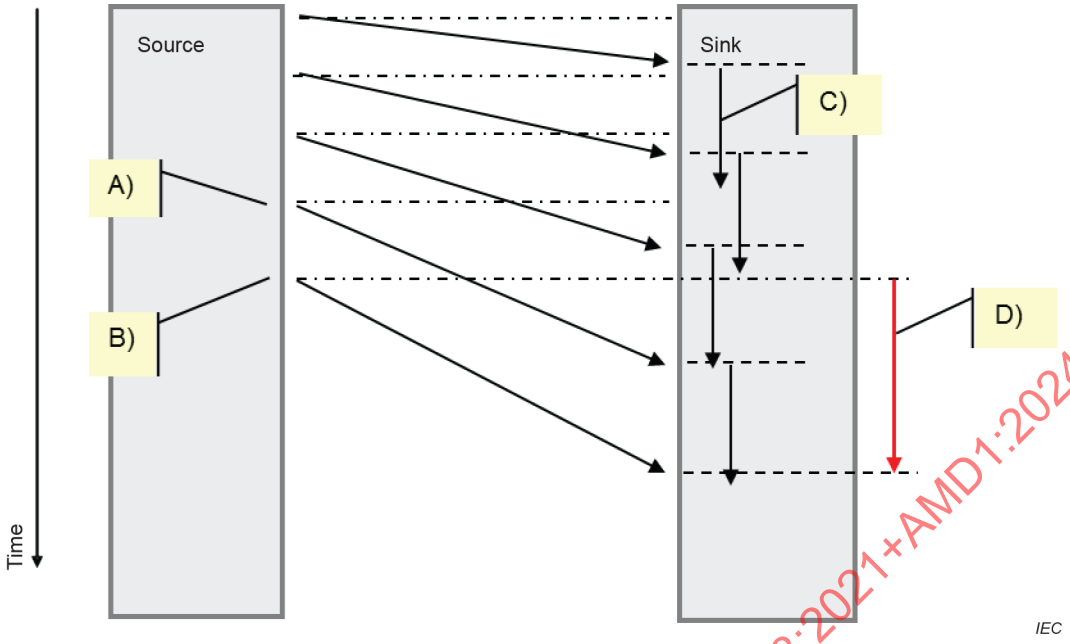
Typical causes for non-timely communication which shall be considered during the design of the FSCP are variable performances of the black channel.

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 12);
– 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 12 shows an example of a slowly increasing message latency of the black channel.



Key

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

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

C) Timeout check in sink

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

Figure 12 – 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 13).

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

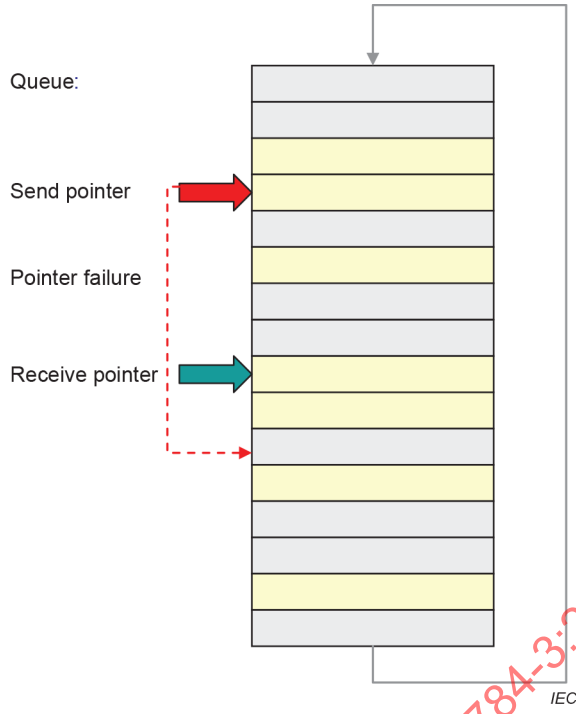


Figure 13 – Example of an active network element failure

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:

- 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.

5.8.8.2 Rate of occurrence of incorrect sequence SPDUs (R_T)

In a safety-related network with message storing elements (see Figure 13), in accordance with 5.8.4 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.

R_T shall be multiplied by 1 in case the SCL enters the safe state after detecting the first communication error. Otherwise R_T shall be multiplied with the maximum number of SPDUs sampled (checked by the receiving SCL) until the safe state has been entered by the SCL.

NOTE The multiplication is necessary because when an active network element fails as described in Figure 13, multiple erroneous SPDUs will be received, all potentially having a different timeliness code.

5.8.9 Masquerade

5.8.9.1 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).

5.8.9.2 Rate of occurrence for masqueraded SPDUs (R_M)

In accordance with 5.8.4 bullet a), a value of 10^{-3}/h per device (both safety related and non-safety related) shall be assumed for the rate of occurrence for masqueraded safety PDUs (R_M), unless otherwise specified.

5.8.10 Calculation of the total residual error rates

5.8.10.1 General

The total residual error rate λ_{SC} for the safety communication channel is needed to calculate the PFH or PFD_{avg} contributions, as explained in 5.1.

5.8.10.2 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 (5).

$$\lambda_{SC} = RR_T + RR_A + RR_I + RR_M \quad (5)$$

where

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

RR_T is the residual error rate per hour for Timeliness (see 5.8.5.2.4);

RR_A is the residual error rate per hour for Authenticity (see 5.8.5.2.3);

RR_I is the residual error rate per hour for Data Integrity (see 5.8.5.2.2);

RR_M is the residual error rate per hour for Masquerade (see 5.8.5.2.5).

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 (6) and in Figure 14 and Figure 15.

$$\lambda_{SCL} = \lambda_{SC} \times m \quad (6)$$

where

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

λ_{SC} is the total residual error rate per hour for the safety communication channel of one logical connection (see Equation (5));

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 14 and Figure 15 illustrate how this number can be determined.

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

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

Figure 14 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.

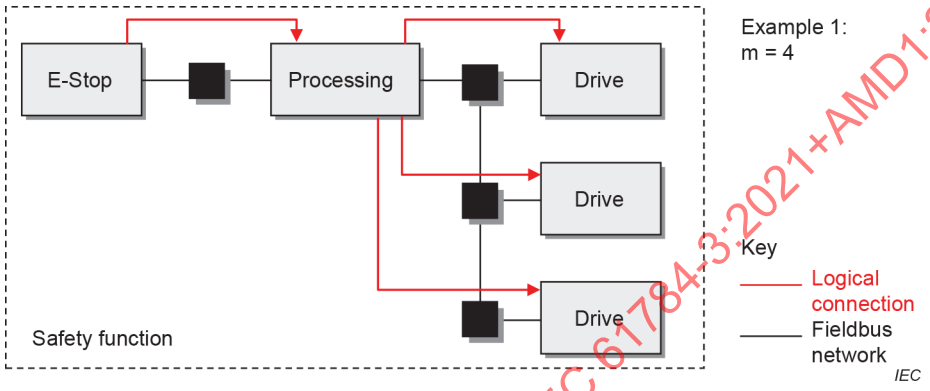


Figure 14 – Example application 1 (m = 4)

Figure 15 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.

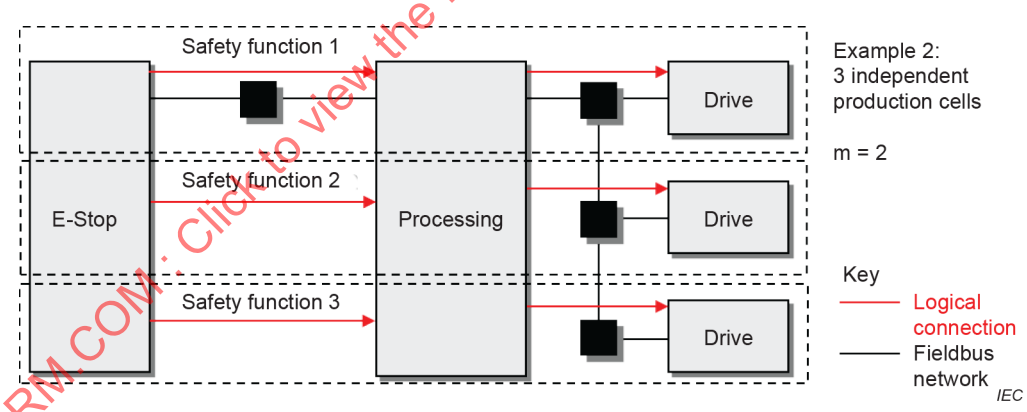


Figure 15 – Example application 2 (m = 2)

5.8.10.3 Based on other quantitative proofs

The summation of the residual error rates of the generic safety properties as shown in 5.8.10.1 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 directly use the methods of the IEC 61508 and to determine the Safe Failure Fraction and the Diagnostic Coverage of the FSCP.

5.8.11 Total residual error rate and SIL

A functional safety communication system shall provide a residual error rate in accordance with this document. Table 2 and Table 3 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 2 – 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 3 – 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 (PFD_{avg})	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	$< 10^{-1}$	$< 10^{-3}$

5.8.12 Configuration and parameterization for an FSCP

5.8.12.1 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 16.

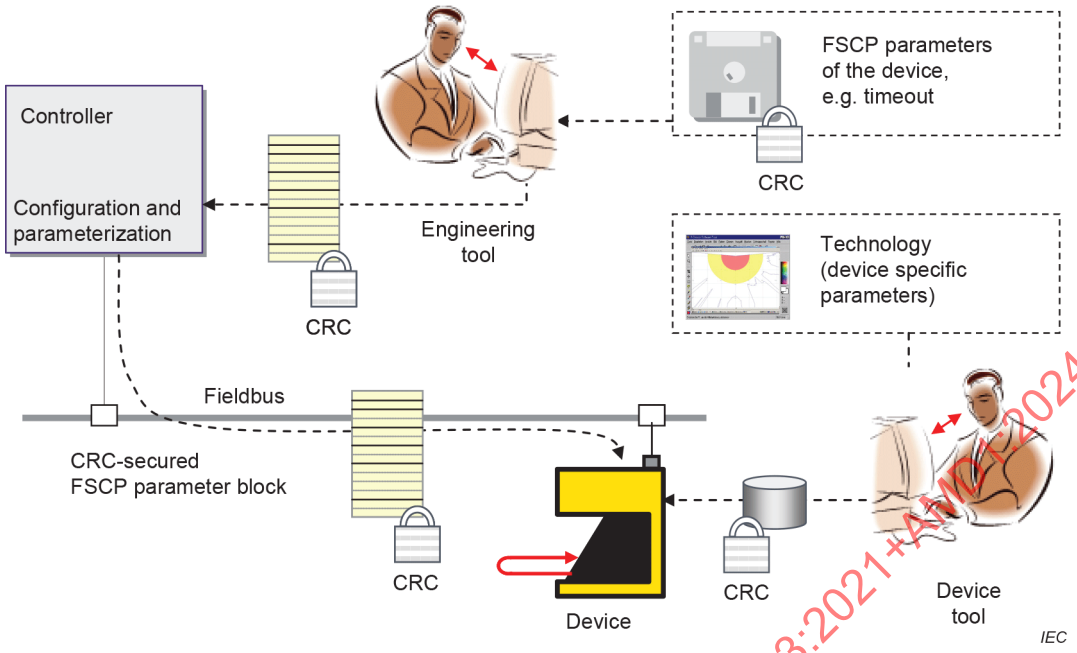


Figure 16 – Example of configuration and parameterization procedures for FSCP

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~~ IEC 62061:2021, 6.7.3 and IEC 62061:2021, 6.7.4 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.
– Detection of conflict between safety technology limits and FSCP parameters (such as safety technology cycle time longer than FSCP watchdog time).

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~~ IEC 62061:2021, 6.7.3 and IEC 62061:2021, 6.7.4 and ISO 13849-1:2015, 4.6.4.

5.8.12.2 Configuration and parameterization change rate

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

5.8.12.3 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 5.8.12.2.

5.9 Relationship between functional safety and security

Security shall be considered for safety-related applications that include functional safety communication systems. However, this document does not cover security aspects, nor does it provide any requirements for security. Security of industrial automation and control systems (IACS) is addressed in IEC 62443 (all parts).

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 (all parts).

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 (all parts).

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 IEC 61784-3 (all parts) are specified in IEC 61918 and the profile specific parts of IEC 61784-5 (all parts), 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), 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 IEC 61784-3 (all parts) 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.

Table 5 lists the summary of topics to be added in the safety manual of products implementing IEC 61784-3-x, if relevant.

Table 5 – Topics for the safety manual of products implementing IEC 61784-3-x

#	Item	Reference	Notes
1	Safety function decomposition PFH, PFDavg	5.1 and 5.8.10	Guidance on the calculations of the PFH or PFDavg for a safety function shall be provided.
2	FSCP installation aspects	5.7 5.8.4	If the safe behaviour of an FSCP or its provided PFH and PFDavg values depend on prerequisites made for the underlying communication channel, these prerequisites should be mentioned in the manual. Potential prerequisites include, but are not limited to: • maximum number of safe network endpoints; • maximum number of non-safe network endpoints; • maximum number of network devices (routers, switches); • maximum or minimum safety PDU and non-safety PDU rates; • watchdog time. Where appropriate, it should be explained in the manual how the end user can verify whether the prerequisites are fulfilled or not.
3	Installation guideline	5.11	The requirements for installation of equipment using the communication technologies specified in IEC 61784-3 are specified in IEC 61918 and IEC 61784-5-x.

#	Item	Reference	Notes
4	Authenticity	5.8.7.1	According to 5.8.7.1, authenticity requirements shall be met during all communication phases in 5.6 for which connection authentication is relevant. If automatic authenticity checks are not possible for certain phases (e.g. at first-time connection establishment), this shall be documented.
5	Configuration and parameterization	5.8.12.1	Systematic configuration and parameterization errors can only be safely prevented by verification and validation. The safety manuals shall provide the necessary instructions. (Relevant information see IEC 62061:2021, 6.7.3, 6.7.4 and ISO 13849-1:2015, 4.6.4)
6	Electrical safety	5.10.1	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.
7	Security	5.9	Security shall be considered for safety-related applications that include functional safety communication systems. Security of industrial automation and control systems (IACS) is addressed in IEC 62443 (all parts).
8	Safety function response time (SFRT)	D.4.6	Maximum safety function response time specified by the manufacturer and time required to complete a safety-related reaction shall not be exceeded, even in the presence of errors and failures.

5.13 Safety policy

Users of this document 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 IEC 61784-3 (all parts) shall only be implemented in devices designed in accordance with the requirements of IEC 61508.

The use of communication technologies specified in IEC 61784-3 (all parts) 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 IEC 61784-3 (all parts) 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 IEC 61784-3 (all parts) is responsible for the correct implementation of the standard, the correctness and completeness of the device documentation and information.

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

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

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

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

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

---

3 FOUNDATION™ Fieldbus and FF-SIS™ are trade names of the non-profit organization FieldComm Group. This information is given for the convenience of users of this document and does not constitute an endorsement by IEC of the trade name holder or any of its products. Compliance to this document 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 FieldComm Group and compliance with conditions for their use (such as testing and validation).

4 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 document and does not constitute an endorsement by IEC of the trade name holder or any of its products. Compliance to this document 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).

5 SERCOS® is a trade name of SERCOS International e.V. This information is given for the convenience of users of this document and does not constitute an endorsement by IEC of the trademark holder or any of its products. Compliance to this document 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).

6 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 document and does not constitute an endorsement by IEC of the trade name holder or any of its products. Compliance to this document 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™[6]) 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®[7]) 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™[7]) is based on the CPF 6 basic profiles in IEC 61784-1 and the safety communication layer specifications defined in IEC 61784-3-6.

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

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

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

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

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™[8]) 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™[8]) is based on the CPF 8 basic profiles in IEC 61784-1 and the safety communication layer specifications defined in IEC 61784-3-8.

---

7 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 document and does not constitute an endorsement by IEC of the trade name holder or any of its products. Compliance to this document 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).

8 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 document and does not constitute an endorsement by IEC of the trade name holder or any of its products. Compliance to this document 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™[9]) 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™[10]) 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™[10]) 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 Communication Profile Family 13 (Ethernet POWERLINK™) – Profiles for functional safety

Communication Profile Family 13 (commonly known as Ethernet POWERLINK™[11]) 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™[11]) 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®[12]) defines communication profiles based on IEC 61158-3-14, IEC 61158-4-14, IEC 61158-5-14, and IEC 61158-6-14.

---

9 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 document and does not constitute an endorsement by IEC of the trade name holder or any of its products. Compliance to this document 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).

10 EtherCAT™ and Safety-over-EtherCAT™ are trade names of Beckhoff, Verl. This information is given for the convenience of users of this document and does not constitute an endorsement by IEC of the trade name holder or any of its products. Compliance to this document 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).

11 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 document and does not constitute an endorsement by IEC of the trade name holder or any of its products. Compliance to this document 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 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 document and does not constitute an endorsement by

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®[12]) 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™ [13]) 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™[13]) 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™ [14]) 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.~~

IEC of the trade name holder or any of its products. Compliance to this document 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).

13 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 document and does not constitute an endorsement by IEC of the trade name holder or any of its products. Compliance with this document 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).

~~14 SafetyNET p is a trade name of the Pilz GmbH & Co. KG. This information is given for the convenience of users of this document and does not constitute an endorsement by IEC of the trade name holder or any of its products. Compliance to this profile does not require use of the trade name SafetyNET p. Use of the trade name SafetyNET p requires permission of the trade name holder and compliance with conditions for its use (such as testing and validation).~~

Annex A
(informative)

Example functional safety communication models

A.1 General

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

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

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

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

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

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

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

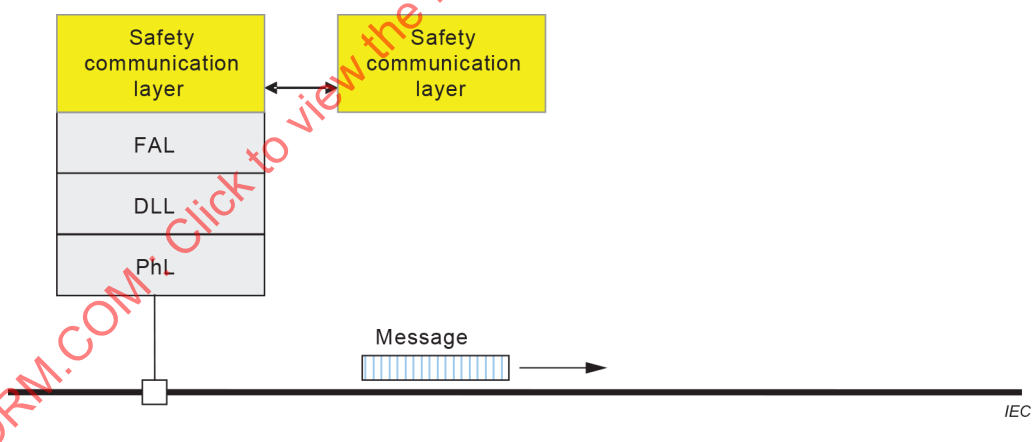


Figure A.1 – Model A

A.3 Model B (full redundancy)

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

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

Transmission layers and transmission media may be of different types.

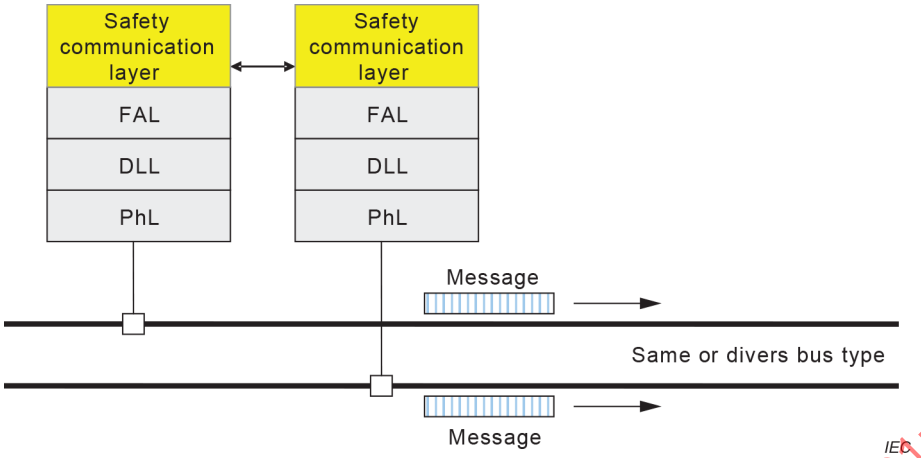


Figure A.2 – Model B

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

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

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

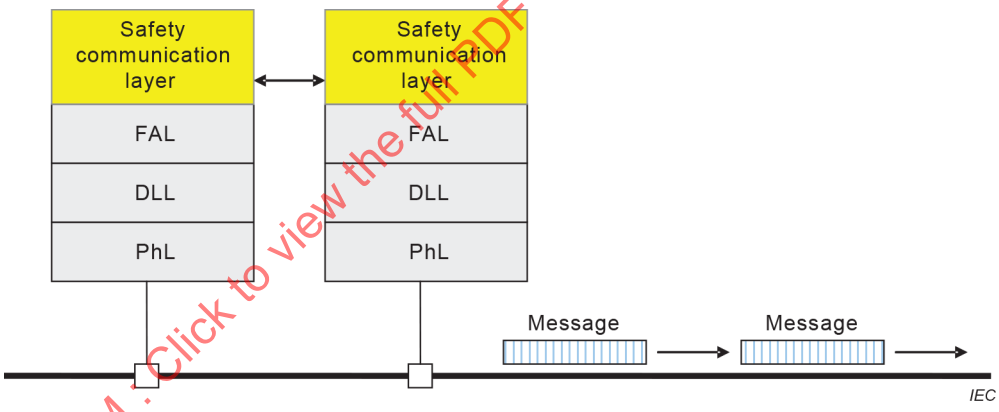


Figure A.3 – Model C

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

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

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

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

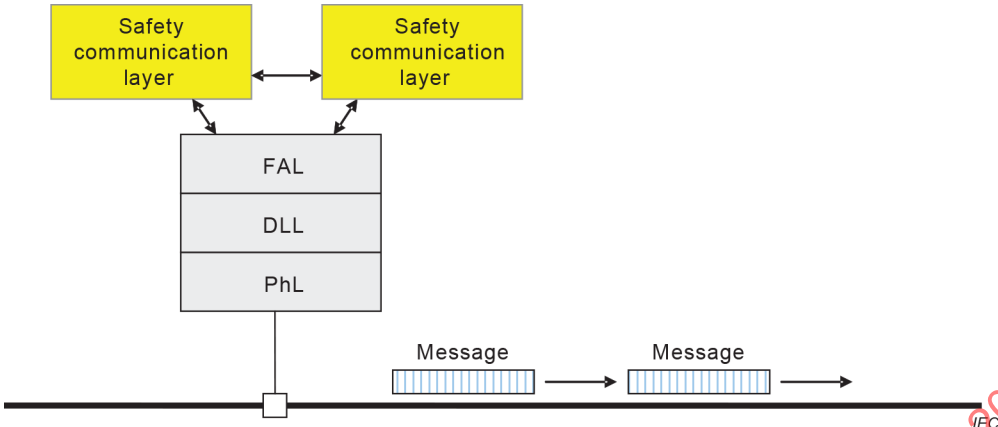


Figure A.4 – Model D

Annex B
(normative)

Safety communication channel model using CRC-based error checking

B.1 Overview

Annex B contains a black channel model for data integrity calculations based on binary symmetric channel. Use of the binary symmetric channel model is recommended unless a different model can be proven more applicable for a particular FSCP.

B.2 Channel model for calculations

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.1). Furthermore, it is assumed all bit cells have the same bit error probability $P_e = P$.

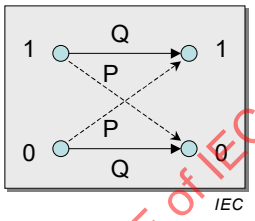


Figure B.1 – Binary symmetric channel (BSC)

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.

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

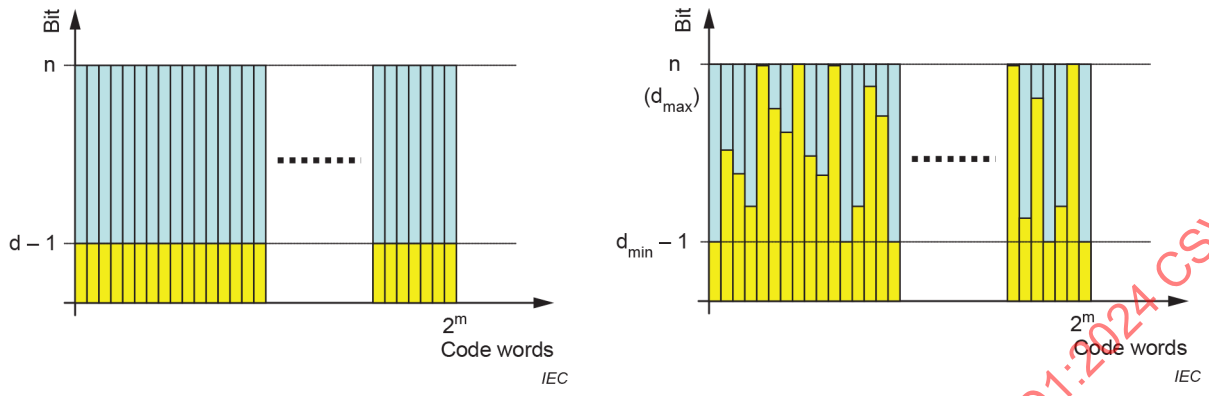
In case the block contains a fictive coding to detect error patterns up to d-1 such as shown in Figure B.2 with a minimum Hamming distance d_{min}, an upper limit residual error probability $R_{UL}(P_e)$ can be calculated with the Equation (B.2) shown below.

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

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

However, this simplified equation does not take into account that even a simple parity bit (minimum Hamming distance $d_{min} = 2$) 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.

Figure B.2 illustrates the background for the Equation (B.2).



a) Fictive code

b) CRC coding

Key

	detectable number of perturbed bits
n	block length
d	Hamming distance
d_{min}	minimum Hamming distance
m	message length

Figure B.2 – 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.

EXAMPLE

Table B.1 shows the block bit length n for different d_{min} values for a specific polynomial (0x1F29F in this case). Different polynomials will result in different values.

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

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

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 (spurious 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 spurious trips normally can be mitigated.

The design of a safety layer assuming a Pe of 10^{-4} is not recommended, as 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 all values up to 100 times higher Pe than 10^{-4}, that is 10^{-2}.

Therefore, unless a better lower bit error probability can be undeniably justified (beyond physical measurements on systems in actual installations and theoretical considerations based on arguments regarding the availability or long term stability of network connections), a maximum value of 10^{-2} shall be used for the bit error probability.

B.4 Cyclic redundancy checking

B.4.1 General

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

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

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.

NOTE For all i from 1 to (d_{min}-1), the value of A_i is equal to 0.

For a high bit error probability (close to 0,5), the worst case value for R_{CRC} is 2^{-r} for proper CRC polynomials (see for example [73]).

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.

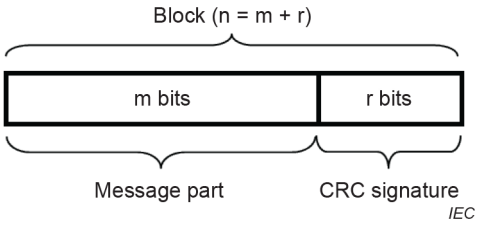


Figure B.3 – Example of a block with a message part and a CRC signature

B.4.2 Requirements for methods to calculate R_{CRC}

Various methods for calculating R_{CRC} have been provided in existing literature (for example [74], [76], [77], [78], [79], [80]). However, polynomial evaluations from published literature should be used with caution as some results have been questioned by subsequent analysis.

In addition, there are no known conservative approximation formulas, which would allow for a general calculation of R_{CRC}. Not even the "conservative" bound 2^{-r} is valid for all polynomials and all values of R_{CRC}.

NOTE 1 As a guidance for the calculation of R_{CRC}, Annex H provides numerical results which can be compared to the output values of algorithms in order to verify them.

Therefore, the R_{CRC} for the selected generator polynomial shall be explicitly calculated, as specified below.

- R_{CRC} shall be calculated for all values of n in use.

  NOTE 2 Calculating R_{CRC} e.g. for the longest telegram length is not sufficient. For example, the polynomial CCITT16 ($x^{16}+x^{12}+x^5+1$ or 0x11021) has a very high R_{CRC} for some small values of n.

  NOTE 3 If a polynomial is proper for a given data length n, it can still be improper for other data lengths (be it smaller or larger).

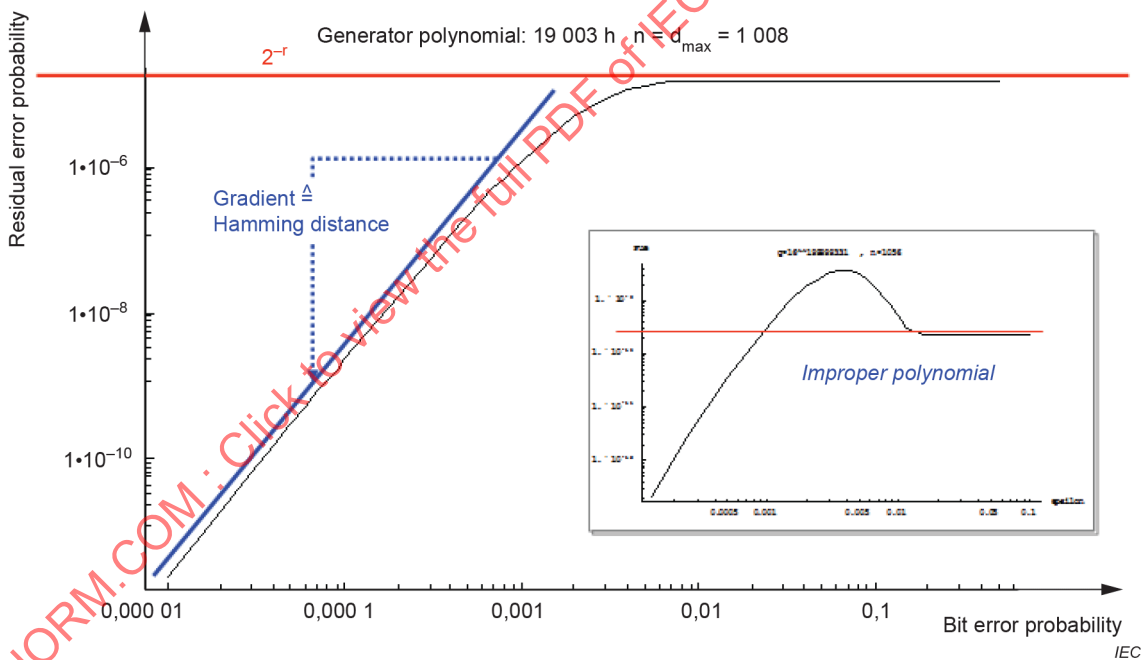
- R_{CRC} shall be calculated for all relevant values of P_e in the interval [2/n to 0,01].

  NOTE 4 In some cases, R_{CRC} does not grow monotonously with the P_e (so-called improper polynomials, see Figure B.4).

  NOTE 5 See [33] for a justification on using 2/n as the lowest P_e.

- Subsequently, it follows that:
  - if n<=200, it is sufficient to evaluate the single value P_e = 0,01;
  - if n>200, multiple values within this interval shall be evaluated (at least 2/n, 4/n, 8/n, 16/n, and so on until 0,01).

When choosing and implementing an algorithm for calculating R_{CRC}, numerical stability (for example ranges, precision, resolution, error propagation) shall be considered in order to avoid incorrect results. For instance, the subtraction of values of the same magnitude and the summation of many small values are problematic, when using floating point numbers.



Key

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

Figure B.4 – Proper and improper CRC polynomials

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

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

Annex C
(informative)

Structure of technology-specific parts

All technology-specific parts of IEC 61784-3 (all parts) 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

Clause and subclause No.	Title	Contents
5.5	Relationships with FAL (and DLL, PhL)	May include existing diagnostics, expected services, constraints (for example, "to be used in conjunction with FSCP x/y")
5.5.1	Data Types	List of the IEC 61158 data types used by the profile
6	Safety communication layer services	May include application objects used, diagnostic services
7	Safety communication layer protocol	First subclause is listed below, others may be added as needed. May include specific time mechanisms, state machines, sequence charts, reaction on power off/power down, diagnostic protocol and corresponding diagnosis
7.1	Safety PDU format	Includes detailed definition of safety PDU (message) formats. Will include several subclauses to specify the various format elements (for example safety CRC specification)
8	Safety communication layer management	Includes specifications for the following aspects of parameterization: – safe parameter data supplied by another safety device (for example a parameter server) – safe parameter data supplied by a tool (for example device description) (including any required measure to secure the storage, handling and transfer)
9	System requirements	First subclauses are listed below, others may be added as needed
9.1	Indicators and switches	Specifications for device indicators and switch function and behaviour
9.2	Installation guidelines	Detailed clause references within IEC 61918 or other relevant documents
9.3	Safety function response time	Calculations and related examples of reaction times relevant for the technology (for example worst case reaction time of safety loop)
9.4	Duration of demands	Specifications for the duration of demands within devices
9.5	Constraints for calculation of system characteristics	Includes black channel retries, number of telegrams 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

Clause and subclause No.	Title	Contents
Annex A (informative)	Additional information for functional safety communication profiles of CPF X	Mandatory informative annex used to provide additional non-normative information on the protocol. If there is none, then this will contain the following sentence: "There is no additional information for this FSCP".
A.1	Hash function calculation	For example, algorithms for CRC calculation
	Bibliography	Bibliographic references relevant for this part

Annex D
(informative)

Assessment guideline

D.1 Overview

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

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

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

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

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 3.1.4, 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 3.1.54, 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, Equation (D.1) can be used to calculate the residual error probability based on binary symmetric channel (BSC) (see Annex B).

$$R_{CRC}(P_e) = \sum_{i=1}^{n} A_i \times (P_e^i \times (1-P_e)^{n-i})^2 \quad \text{(D.1)}$$

An analysis according to D.3.3 together with a calculation using Equation (D.1) is required for a complete evaluation of the residual error probability in case of a white channel solution.

NOTE 3 See IEC 62280 for more information.

The calculation of $\lambda_{SCL}(P_e)$ is carried out along the lines of 5.8.10.1.

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

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

D.3.3 Models A and D

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

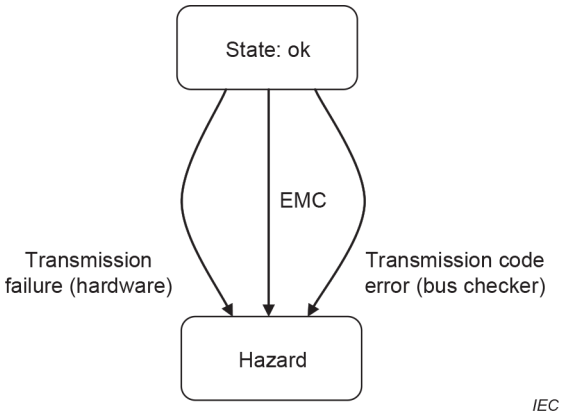


Figure D.1 – Basic Markov model

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

In this case a Markov analysis can be expressed by three fundamental transition possibilities (see 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.

NOTE 2 Calculations of the residual error probability RP_{sc} of the channel and resulting $\lambda_{SCL}(p_e)$ are detailed in IEC 62280.

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

NOTE 2 See IEC 62280 for more information.

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

D.4 Verification of safety measures

D.4.1 General

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

D.4.2 Implementation

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

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

D.4.3 Default safety action

At loss of power, or absence of expected safety messages, an SCL and its related devices shall transition to a specified safe state within a specified maximum time delay.

EXAMPLE 1 Upon loss of messages, a Watchdog timer drives its related device to a safe state.

EXAMPLE 2 Upon loss of power, a spring is released to apply a brake or movement lock.

Assessment: See 5.4.4.

D.4.4 Safe state

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

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

D.4.5 Transmission errors

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

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

D.4.6 Safety reaction and response times

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

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

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

D.4.7 Combination of measures

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

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

D.4.8 Absence of interference

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

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

D.4.9 Additional fault causes (white channel)

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

NOTE Details can be found in IEC 62280 or [71].

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

D.4.10 Reference test beds and operational conditions

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

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

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

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

D.4.11 Conformance tester

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

NOTE Conformance testing includes both positive and negative tests.

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

Annex E
(informative)

Examples of implicit vs. explicit FSCP safety measures

E.1 General

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

E.2 Example fieldbus message with safety PDUs

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

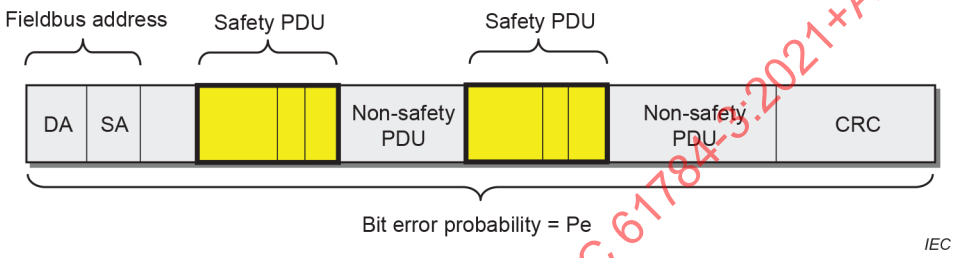


Figure E.1 – Example safety PDUs embedded in a fieldbus message

E.3 Model with completely explicit safety measures

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

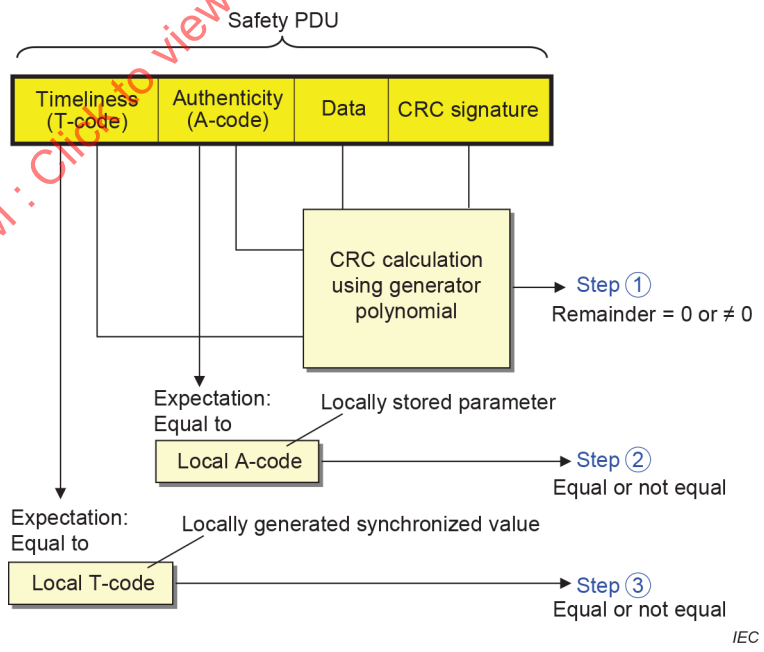


Figure E.2 – Model with completely explicit safety measures

Checking is done according to the following steps:

Step ①	Remainder ≠ 0	→	Any error detected
	Remainder = 0	→	Data correct or incorrect with RR_I according to 5.8.5.2.2
Step ②	Not equal	→	Any error detected
	Equal	→	Authenticity correct or incorrect with RR_A according to 5.8.5.2.3
Step ③	Not equal	→	Any error detected
	Equal	→	Timeliness correct or incorrect with RR_T according to 5.8.5.2.4

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.

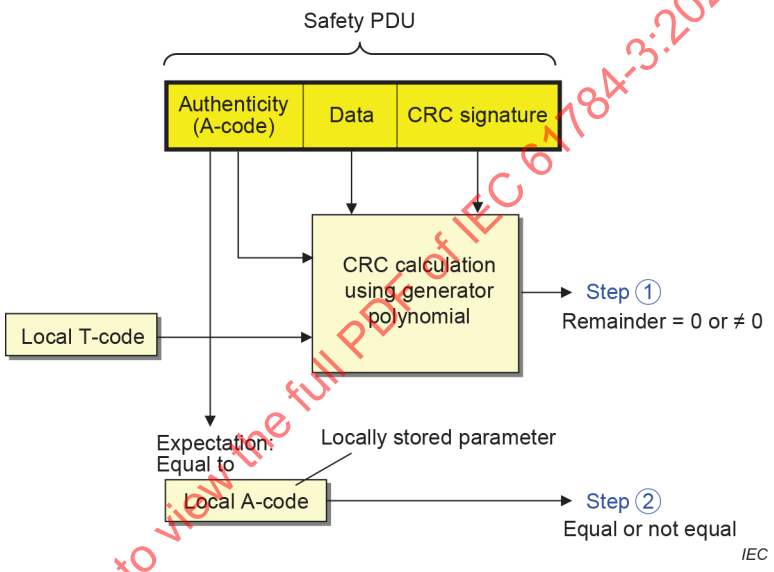


Figure E.3 – Model with explicit A-code and implicit T-code safety measures

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 5.8.5.2.3

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

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

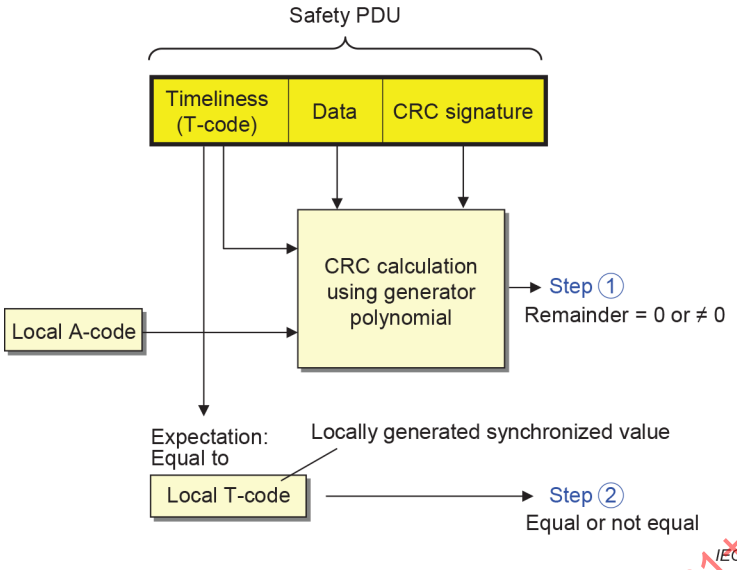


Figure E.4 – Model with explicit T-code and implicit A-code safety measures

Checking is done according to the following steps:

Step ①	Remainder ≠ 0	→	Any error detected
	Remainder = 0	→	Data and Authenticity correct or incorrect with certain RR
Step ②	Not equal	→	Any error detected
	Equal	→	Timeliness correct or incorrect with RR_T according to 5.8.5.2.4

E.6 Model with split explicit and implicit safety measures

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

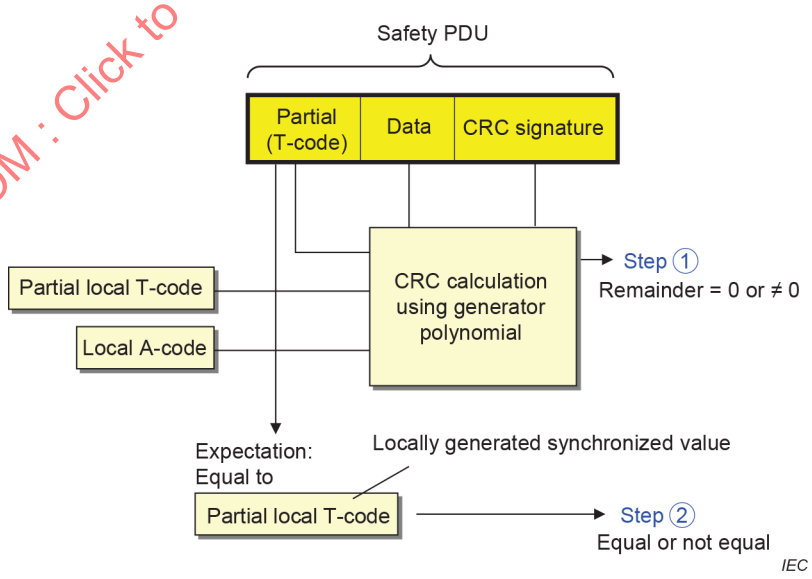


Figure E.5 – Model with split explicit and implicit safety measures

Checking is done according to the following steps:

Step ①	Remainder ≠ 0	→	Any error detected
	Remainder = 0	→	Data, Authenticity and Timeliness correct or incorrect with certain RR
Step ②	Not equal	→	Any error detected
	Equal	→	Timeliness correct or incorrect with certain RR

E.7 Model with completely implicit safety measures

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

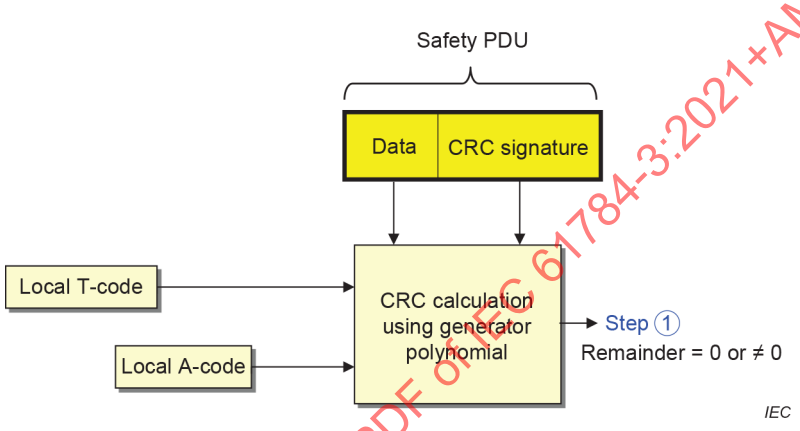


Figure E.6 – Model with completely implicit safety measures

Checking is done according to the following step:

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

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

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

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

Annex F
(informative)

Legacy models for estimation of the total residual error rate

F.1 General

Annex F describes the legacy models which were used in previous editions of this document for estimating the total residual error rate for an FSCP, for the purpose of assessing this FSCP.

NOTE These legacy models are kept in Annex F for reference purpose, which will be removed in future editions of this document.

F.2 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 (F.1) and (F.2) shown below shall be used to calculate the residual error rates resulting from RP_{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 F.1.

$$\lambda_{SC}\,(Pe) = RP_{SC}\,(Pe) \times v \qquad (F.1)$$

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

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

Table F.1 – 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)
RP_{SC} (Pe)	Residual error probability of the safety communication channel with respect to the bit error probability (see 3.1.35). This is equal to R_{CRC} (Pe)
v	Maximum sample rate of SPDUs per hour
m	Maximum number of logical connections that is permitted in a single safety function (see Figure F.1 and Figure F.2)

The number m of logical connections depends on the individual safety function application. Figure F.1 and Figure F.2 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 F.1 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.

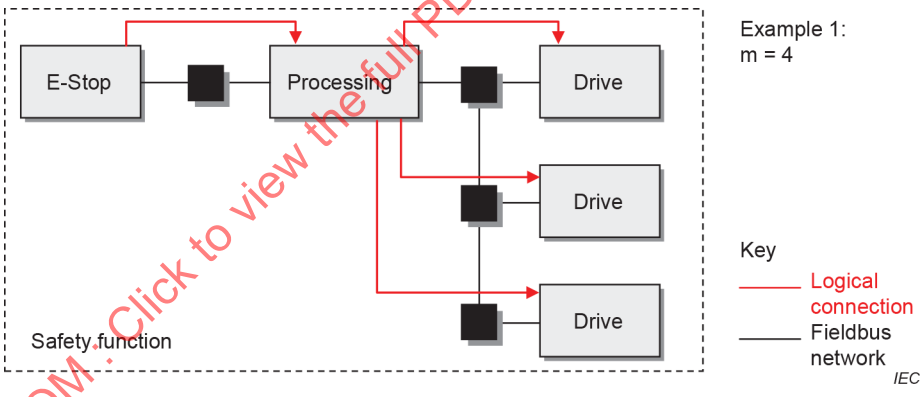


Figure F.1 – Example application 1 (m = 4)

Figure F.2 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.

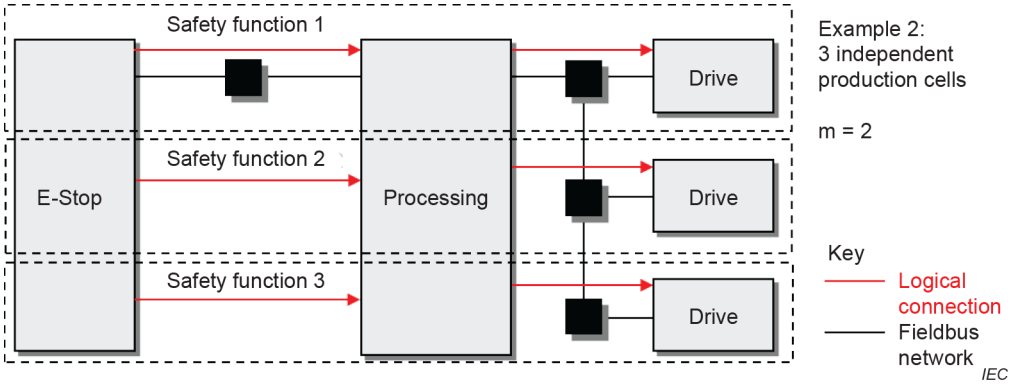


Figure F.2 – Example application 2 (m = 2)

F.3 Total residual error rate and SIL

A functional safety communication system shall provide a residual error rate in accordance with this document. Table F.2 and Table F.3 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.2 – 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.3 – 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 (PFD_{avg})	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	$< 10^{-1}$	$< 10^{-3}$

Annex G
(informative)

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

G.1 Overview

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

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

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

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

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

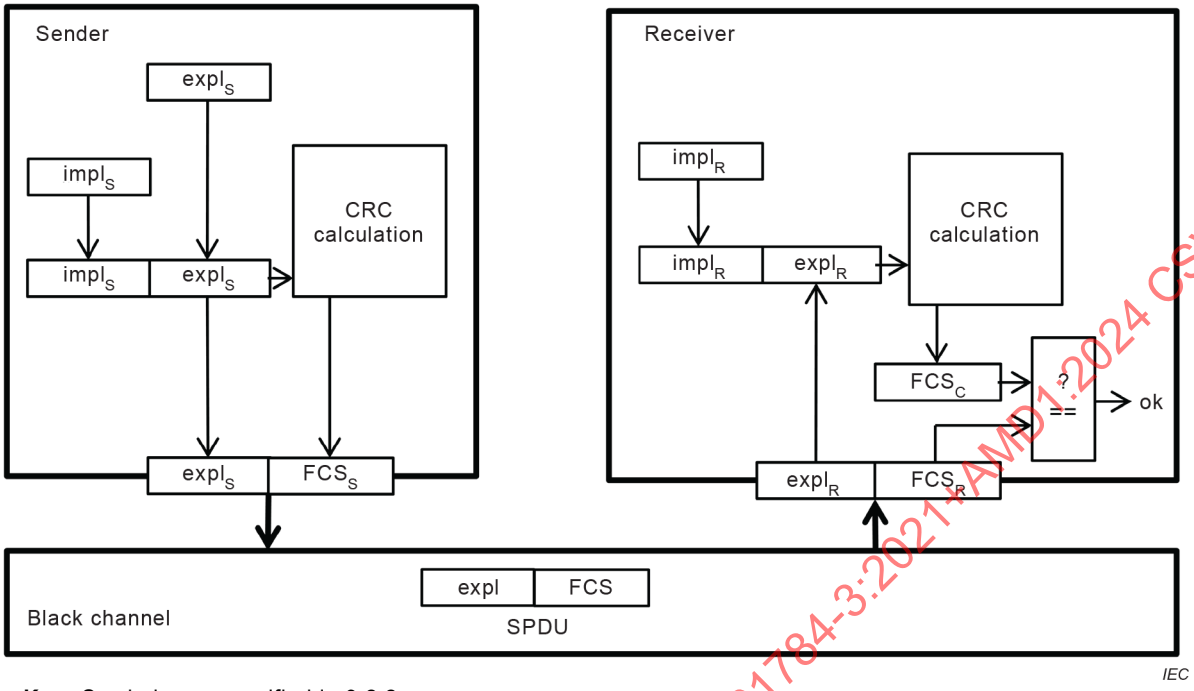
G.2 Basic principles

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

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

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

NOTE 2 Initialization details are addressed in 5.8.12.1.



Key Symbols are specified in 3.2.2.

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

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

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

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

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

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

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

e length of explicit data;

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

G.3 Problem statement: constant values for implicit data

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

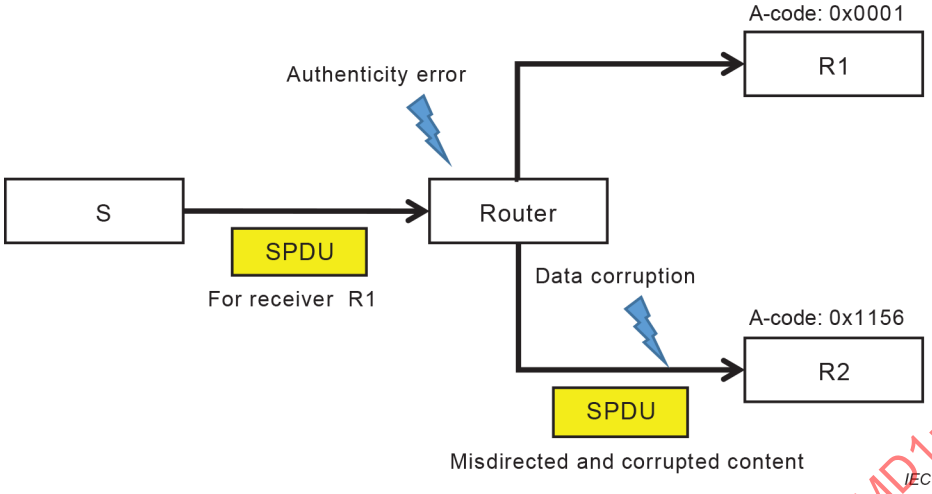


Figure G.2 – Example of an incorrect transmission with multiple error causes

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

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

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

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

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

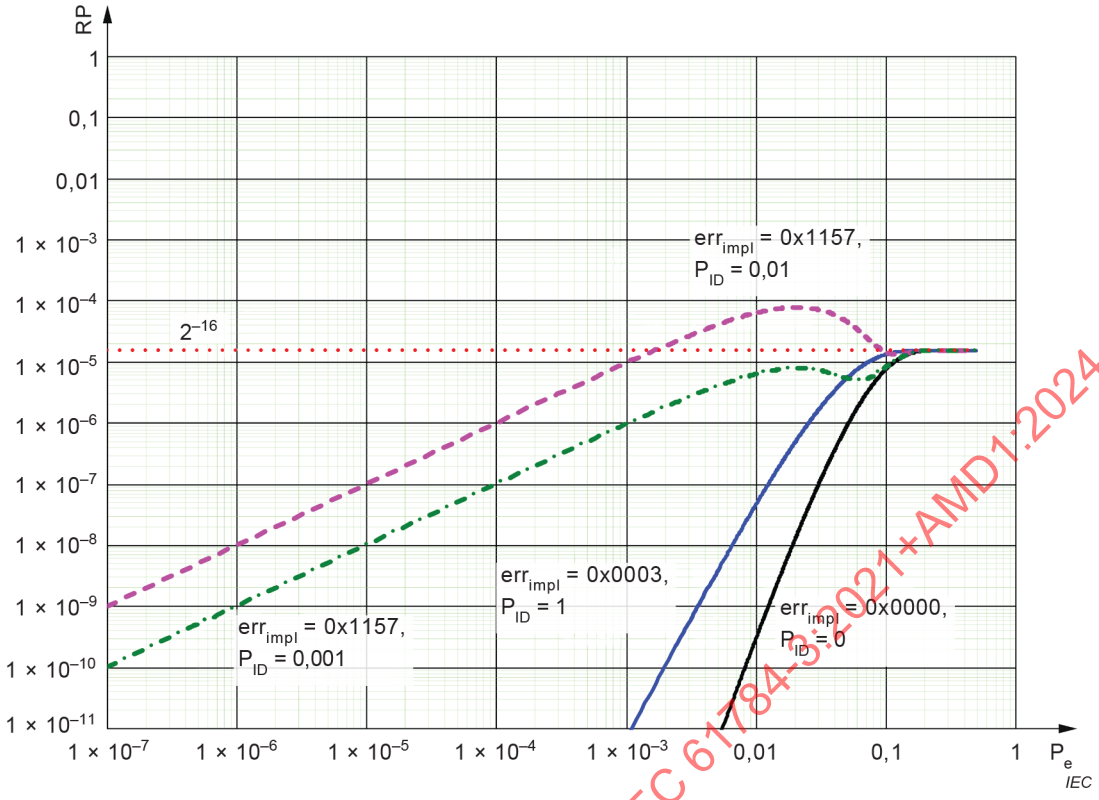


Figure G.3 – Impact of errors in implicit data on the residual error probability

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

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

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

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

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

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

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

Conclusion: When using implicit transmission mechanisms, the residual error probability is not necessarily bounded by 2^{-r}. This bound is only valid if the FSCP provides additional mechanisms such as the ones shown in Clause G.4.

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

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

G.4.1 General

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

As already defined earlier, err_{impl} is the bitwise exclusive disjunction (XOR) between the implicit data $impl_S$ used in the sender of the erroneous packet, and the expected value for the implicit data $impl_R$ in the receiver. Clearly, if $impl_S$ and $impl_R$ are uniformly distributed, independent random variables, also err_{impl} is uniformly distributed, i.e. takes each possible value with equal possibility. However, because errors can be assumed to happen at 'random' points of time, it is also possible to achieve a uniformly distributed err_{impl} if $impl_S$ and $impl_R$ are non-random variables. In order to validate whether err_{impl} follows a uniform distribution, statistical checks such as the Chi-Square-Test or the Kolmogoroff-Smirnoff-Test can be used, (see for example [77]).

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

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

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

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

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

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

In the following, the two variants are shown separately.

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

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

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

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

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

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

This case applies in particular to FSCPs that use random number generators to derive implicit data values in order to produce uniformly distributed error patterns in the implicit data.

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

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

In combination, the following disjoint cases can be discriminated:

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

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

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

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

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

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

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

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

RP_I is the residual error probability for data corruption as defined in 5.8.

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

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

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

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

n is the number of bits of the SPDU.

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

In general, RP_x is calculated by:

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

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

Case 2 (IC)

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

Explanations on P_{IC}:

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

Case 3 (CI)

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

Case 4 (II)

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

Explanations:

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

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

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

Explanation:

- Cases 2 to 4 are disjoint events.

In case of a proper polynomial, the following applies:

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

Explanations:

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

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

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

The following cases of error combinations can be discriminated:

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

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

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

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

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

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

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

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

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

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

n is the number of bits in the SPDU.

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

In general, RP_x is calculated by:

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

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

Case 2 (IC)

$$RP_2 = P_{ID} \times (1 - P_{IED}) \times P_{IC}$$
$$= 0$$

Explanation:

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

Case 3 (CI)

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

Case 4 (II)

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

Explanations:

- $$P_{II} = \sum_{i=1}^{2^r-1} P\{err_{impl} = i\} \times P_{EIC}(i)$$
$$= \sum_{i=1}^{2^r-1} \frac{1}{2^r-1} \times P_{EIC}(i)$$
$$= \frac{1}{2^r-1} \times \sum_{i=1}^{2^r-1} P_{EIC}(i)$$
$$= \frac{1}{2^r-1}$$ (because for all possible err_{expl} there is exactly one matching err_{impl})
$$\approx 2^{-r}$$

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

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

Explanation:

- Cases 2 to 4 are disjoint events.

G.5 General case

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

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

where

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

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

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

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

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

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

where

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

Explanations:

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

G.6 Calculation of P_{ID}

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

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

where

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

R_T is the rate of occurrence for incorrect sequence safety PDUs (see 5.8.5.2.4);

R_A is the rate of occurrence for misdirected safety PDUs (see 5.8.5.2.3);

v is the maximum number of SPDUs checked by the receiving SCL ("SPDU sample rate") per hour (see 5.8.5.2.2).

Explanation:

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

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

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

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

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

Calculation of the total residual error rate

According to 5.8.10.1, the total residual error rate is calculated by (see Equation (5)):

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

Alternatively, the following formula can be used:

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

Annex H
(informative)

Residual error probability for example CRC codes (tables for verification of calculation methods)

H.1 Overview

This Annex H provides guidance for the calculation of residual error probability for CRC-based data integrity measures. Numerical results are provided to enable verification of algorithms by comparing output values to those provided in Clauses H.2 and H.3.

The sources for the calculation methods used in Clauses H.2 and H.3 are found in [76], [78] and [80].

H.2 Example of a 32-bit CRC

Generator Polynomial:	0x1f1922815 (hexadecimal notation)

NOTE This polynomial is named CRC-32/8 in [76], and is referenced as CRC1 in Table H.1.

Length (r) of the polynomial:	32
Bit error probability (Pe):	at "maximum of R_{CRC1}"; 2/n; 4/n; 0,01; 0,001; 0,0001; (n is number of Bit)
SPDU length (octets):	8, 16, 64, 132, 192, 256

Table H.1 shows the results of the calculation of residual error probability of CRC according to method 1 (see [76]) and is verified with method 2 (see [80]) which complies with [78]. The results between method 1 and method 2 match to within 7 significant digits but may differ beyond that due to numerical deviations.

The polynomial used in Table H.1 is:

$x^{32} + x^{31} + x^{30} + x^{29} + x^{28} + x^{24} + x^{23} + x^{20} + x^{17} + x^{13} + x^{11} + x^4 + x^2 + 1$ (0x1f1922815)

WARNING This polynomial is not applicable to all data lengths. Improper behaviour may occur at certain data lengths.

Table H.1 – Residual error probabilities (R_{CRC1}) for example CRC32 polynomial

SPDU (incl. CRC) (octets)	SPDU (incl. CRC) (n Bit)	HD	Maximum or R_{CRC1}		R_{CRC1} at Pe 2/n	R_{CRC1} at Pe 4/n	R_{CRC1} at Pe 0,01	R_{CRC1} at Pe 0,001	R_{CRC1} at Pe 0,000 1
			Pe	Value of R_{CRC1}					
8	64	10	0,3 … 0,5 (proper behaviour)	2,3283064E-10 = 2^{-32}	7,1473931E-15	1,4099777E-12	2,5085225E-19	4,0740000E-29	4,2768430E-39
16	128	8	0,2 … 0,5 (proper behaviour)	2,3283064E-10 = 2^{-32}	2,4717834E-13	1,1208444E-11	1,3290758E-14	3,8410779E-22	4,2783584E-30
64	512	8	0,03 … 0,5 (proper behaviour)	2,3283064E-10 = 2^{-32}	4,1818700E-13	1,6873006E-11	4,5015881E-11	3,2193220E-17	5,0546386E-25
132	1056	4	0,0038323 (improper behaviour)	2,0233E-9 > 2^{-32}	9,2507671E-10	2,0229532E-9	3,3933638E-10	1,8430726E-10	4,7527378E-14
192	1536	4	0,002605 (improper behaviour)	1,1122E-7 > 2^{-32}	5,12890345E-8	1,1122042E-7	5,0108849E-10	2,83587131E-8	1,1267305E-11
256	2048	2	0,001266 (improper behaviour)	3,41231E-7 > 2^{-32}	3,23169798E-7	2,80176357E-7	2,3930242E-10	3,26134943E-7	1,63420759E-8

Figure H.1, Figure H.2 and Figure H.3 depict R_{CRC1} (polynomial 0x1f1922815) for SPDU lengths listed in Table H.1. The figures show Pe as "**e**". The red dot shows the relevant R_{CRC} for a maximum Pe = 0,01.

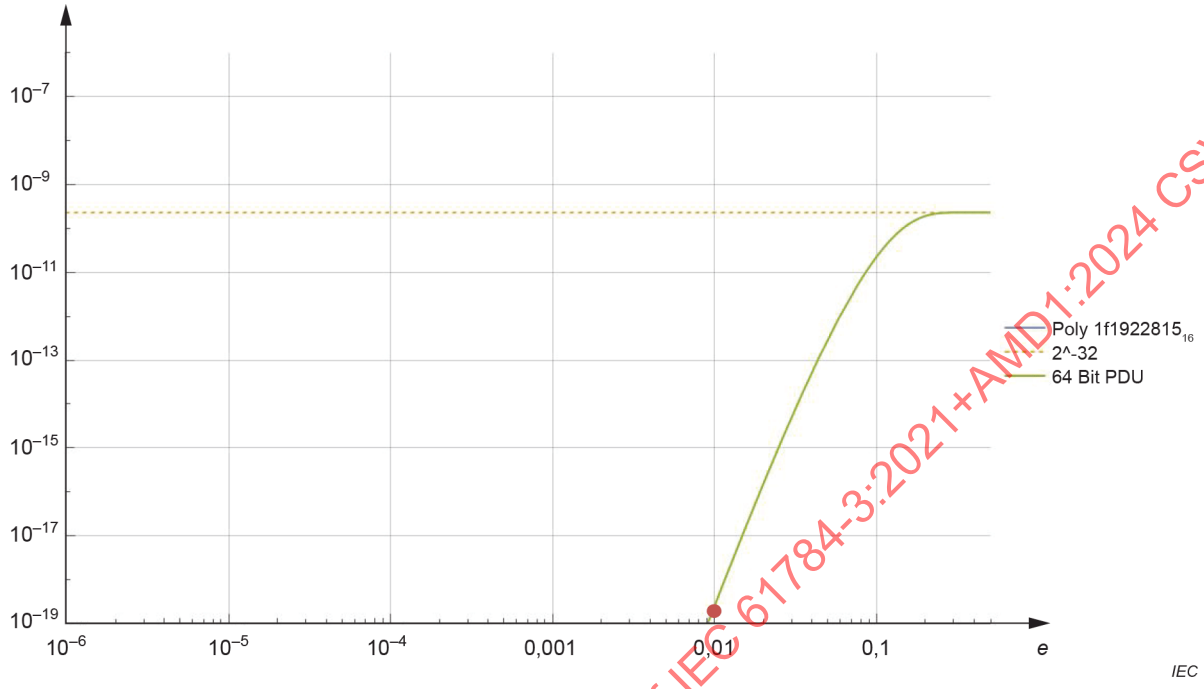


Figure H.1 – Residual error probabilities (example of a 32-bit CRC – result 1)

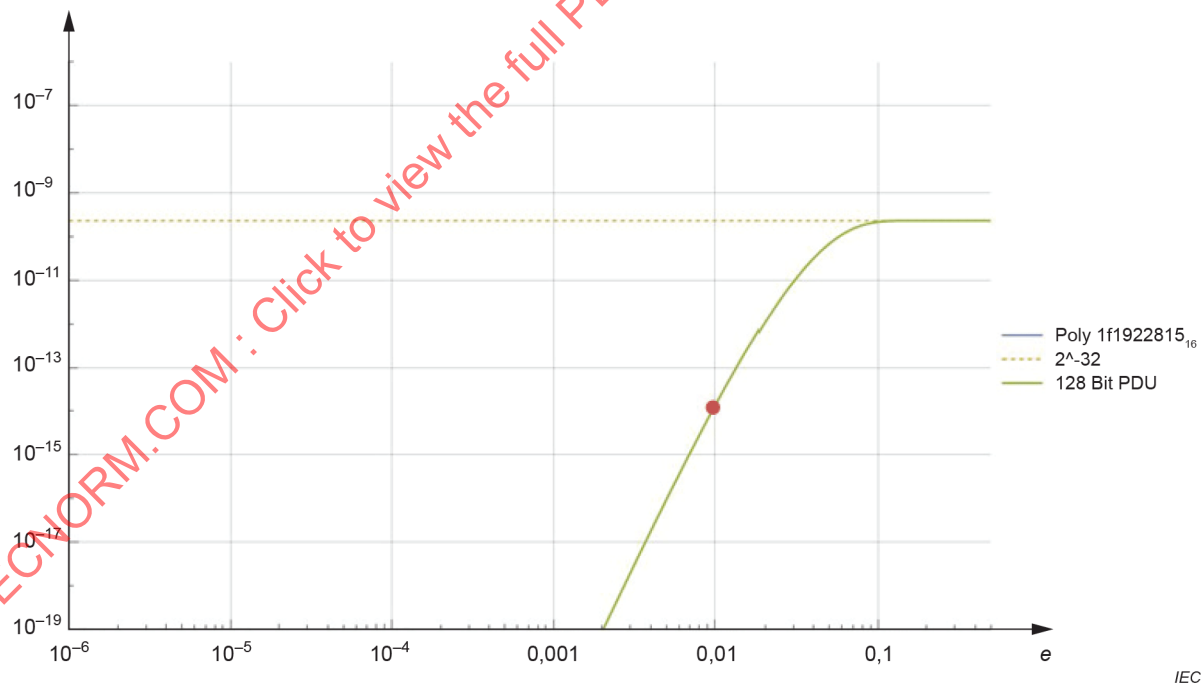


Figure H.2 – Residual error probabilities (example of a 32-bit CRC – result 2)

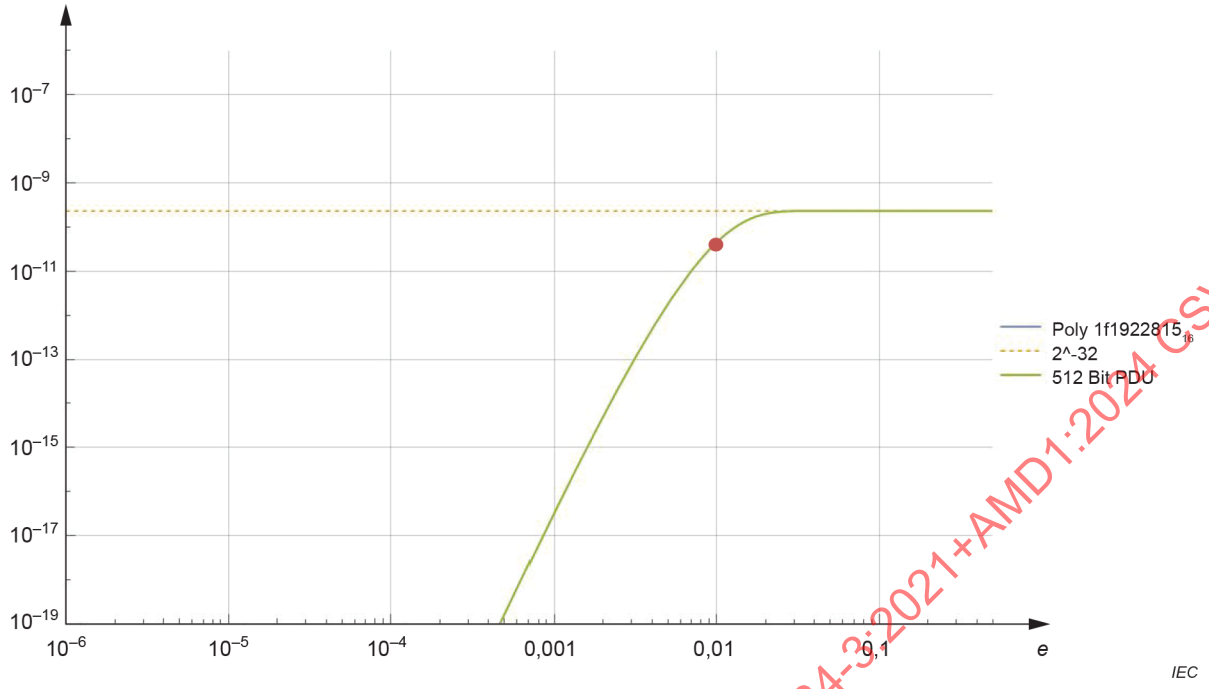


Figure H.3 – Residual error probabilities (example of a 32-bit CRC – result 3)

Figure H.4, Figure H.5 and Figure H.6 show that it obvious that a calculation at Pe = 0,01 is not sufficient.

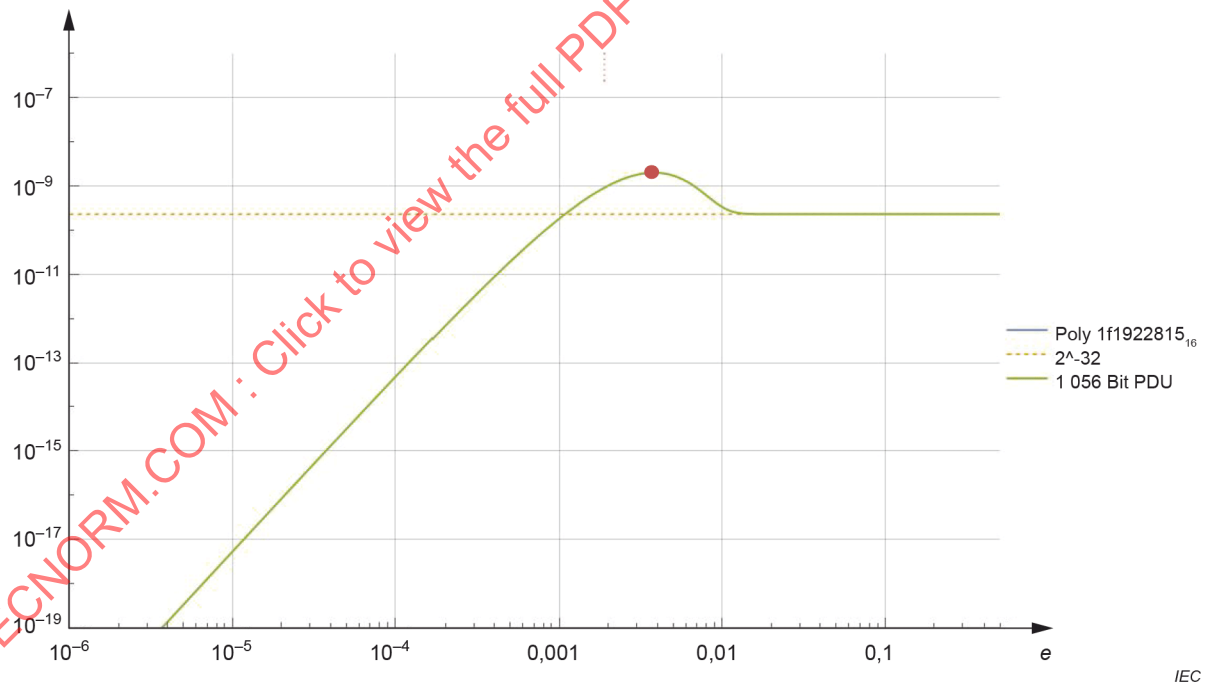


Figure H.4 – Residual error probabilities (example of a 32-bit CRC – result 4)

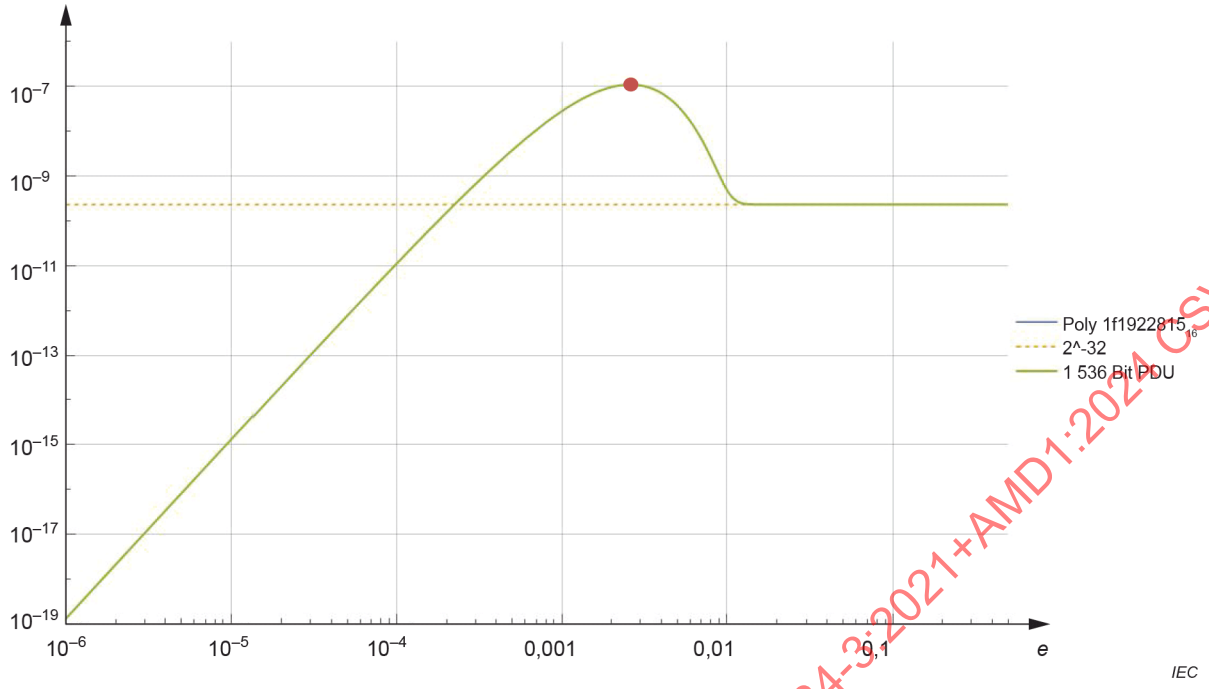


Figure H.5 – Residual error probabilities (example of a 32-bit CRC – result 5)

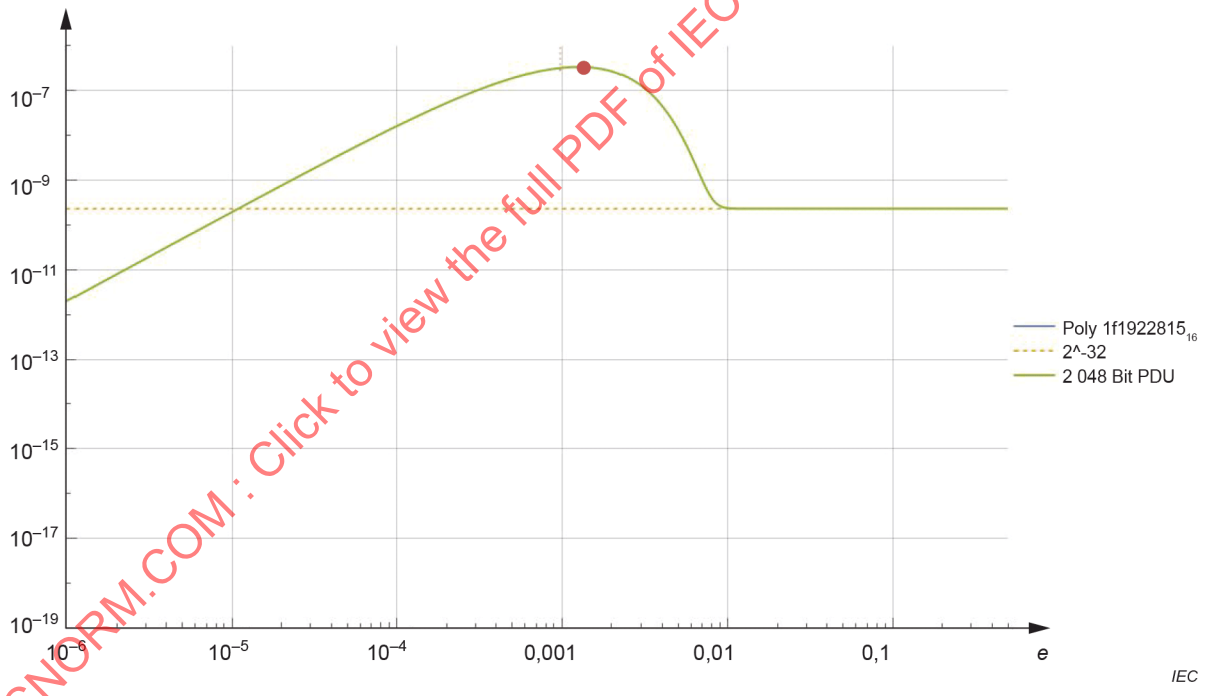


Figure H.6 – Residual error probabilities (example of a 32-bit CRC – result 6)

H.3 Example of a 16-bit CRC

Generator Polynomial:	0x14eab (hexadecimal notation)

NOTE This polynomial is referenced as CRC2 in Table H.2.

Length (r) of the polynomial:	16
Bit error probability (Pe):	at "maximum of R_{CRC2}"; 2/n; 4/n; 0,01; 0,001; 0,0001; (n is number of Bit)
SPDU length (octets):	8, 16, 32, 40, 48

Table H.2 shows the results of the calculation of residual error probability of CRC according to method 1, see [76], and is verified with method 2 (see [80]) which complies with [78]. The results between method 1 and method 2 match to within 7 significant digits but may differ beyond that due to numerical deviations.

The polynomial used in Table H.2 is:

$x^{16} + x^{14} + x^{11} + x^{10} + x^9 + x^7 + x^5 + x^3 + x + 1$ (0x14eab)

WARNING: This polynomial is not applicable to all data lengths. Improper behaviour may occur at certain data lengths.

Table H.2 – Residual error probabilities (R_{CRC2}) for example CRC16 polynomial

SPDU (incl.CRC) (octets)	SPDU (incl. CRC) (n Bit)	HD	Maximum of R_{CRC2}		R_{CRC2} at Pe 2/n	R_{CRC2} at Pe 4/n	R_{CRC2} at Pe 0,01	R_{CRC2} at Pe 0,001	R_{CRC2} at Pe 0,000 1
			Pe	R_{CRC2}					
8	64	6	0,2 … 0,5 (proper behaviour)	1,52588E-5 = 2^{-16}	4,0855074E-7	4,6802171E-6	1,4714077E-9	2,4743046E-15	2,6068369E-21
16	128	6	0,1 … 0,5 (proper behaviour)	1,52588E-5 = 2^{-16}	3,8938438E-7	4,3578577E-6	5,1594242E-8	1,5166598E-13	1,6923502E-19
32	256	2	0,01174 (improper behaviour)	2,34865E-5 > 2^{-16}	2,1286768E-5	2,2410331E-5	2,3127700E-5	1,55761032E-6	1,94991775E-8
40	320	2	0,006343 (improper behaviour)	3,55898E-4 > 2^{-16}	3,5582103E-4	2,0252625E-4	2,8090051E-4	4,8029197E-5	6,3934318E-7
48	384	2	0,005264 (improper behaviour)	4,8443E-4 > 2^{-16}	4,8437693E-4	2,7179904E-4	2,9261350E-4	8,8736147E-5	1,2512782E-6

Figure H.7, Figure H.8 and Figure H.9 depict R_{CRC2} (polynomial 0x14eab) for SPDU lengths listed in Table H.2. The figures show Pe as "***e***". The red dot shows the relevant R_{CRC} for a maximum Pe = 0,01.

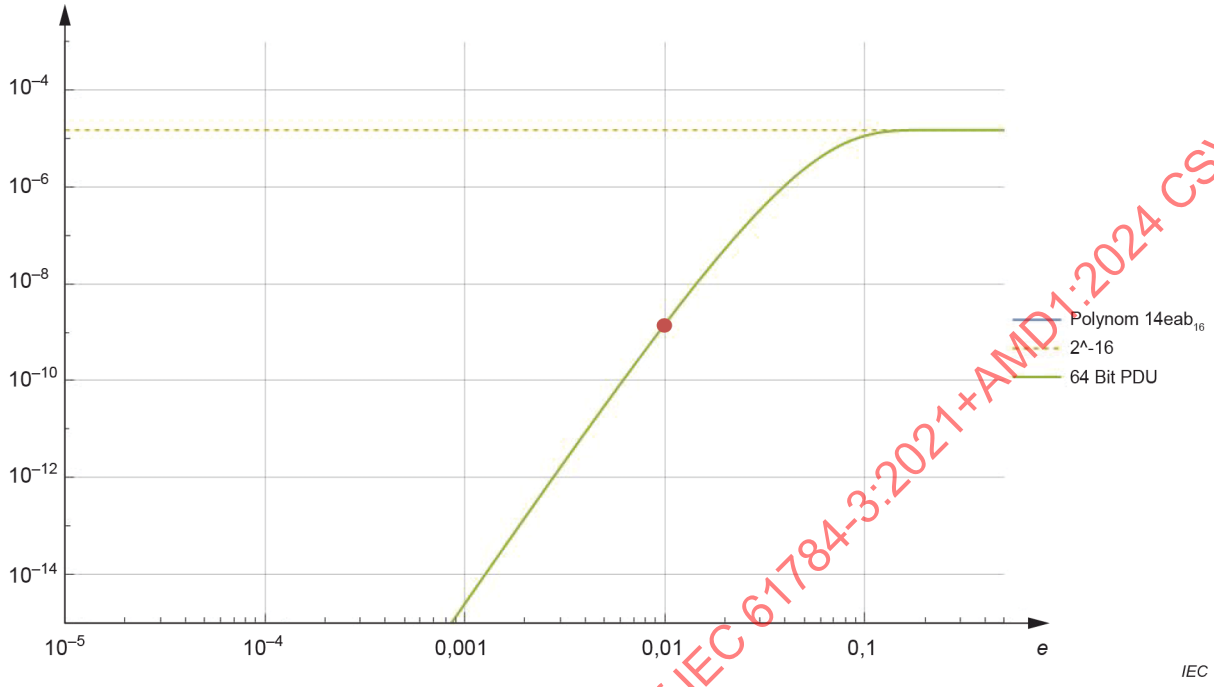


Figure H.7 – Residual error probabilities (example of a 16-bit CRC – result 1)

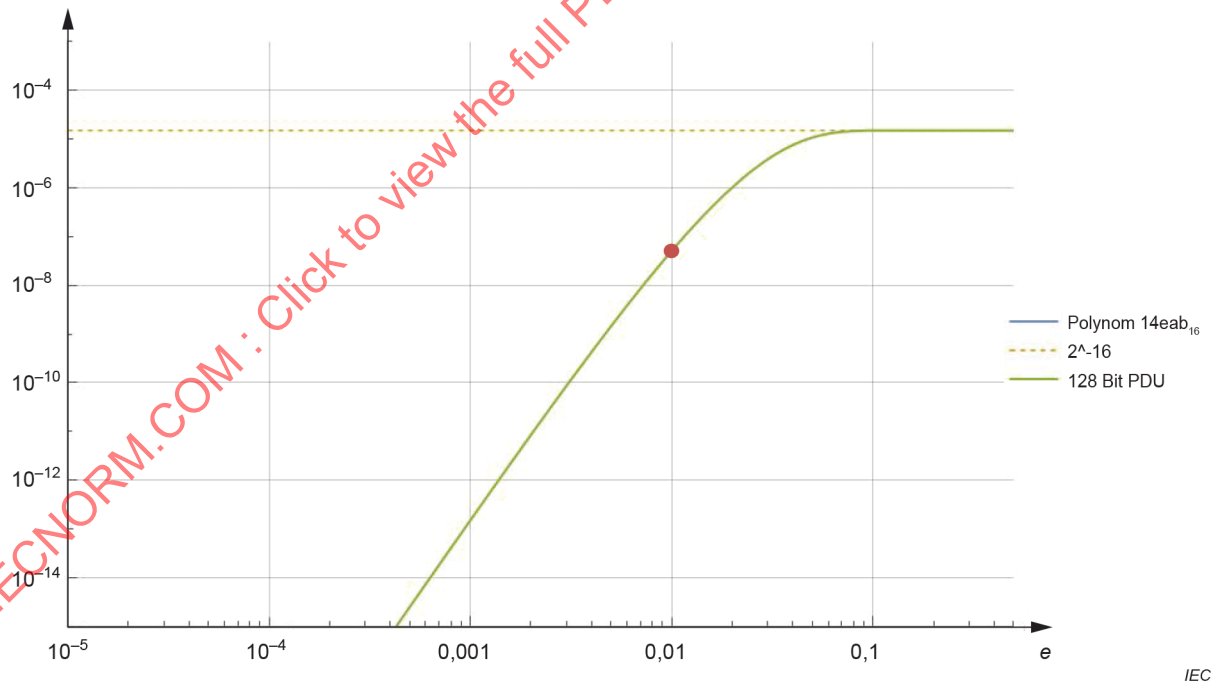


Figure H.8 – Residual error probabilities (example of a 16-bit CRC – result 2)

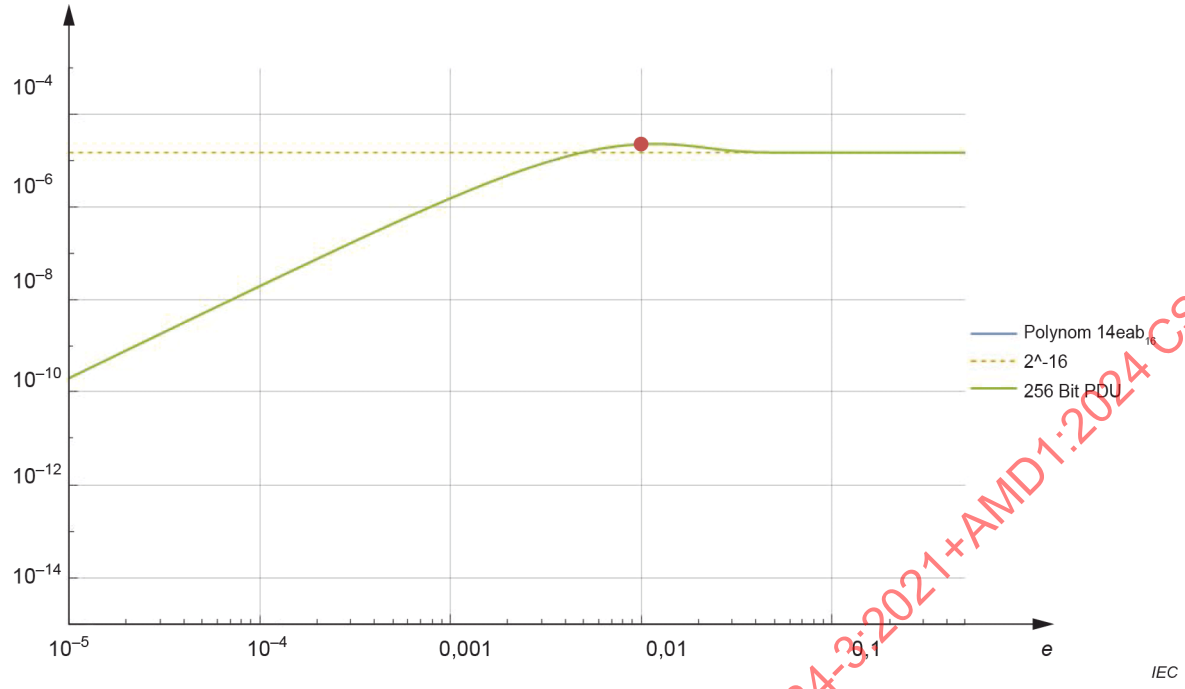


Figure H.9 – Residual error probabilities (example of a 16-bit CRC – result 3)

Figure H.10 and Figure H.11 show that it obvious that a calculation at Pe = 0,01 is not sufficient.

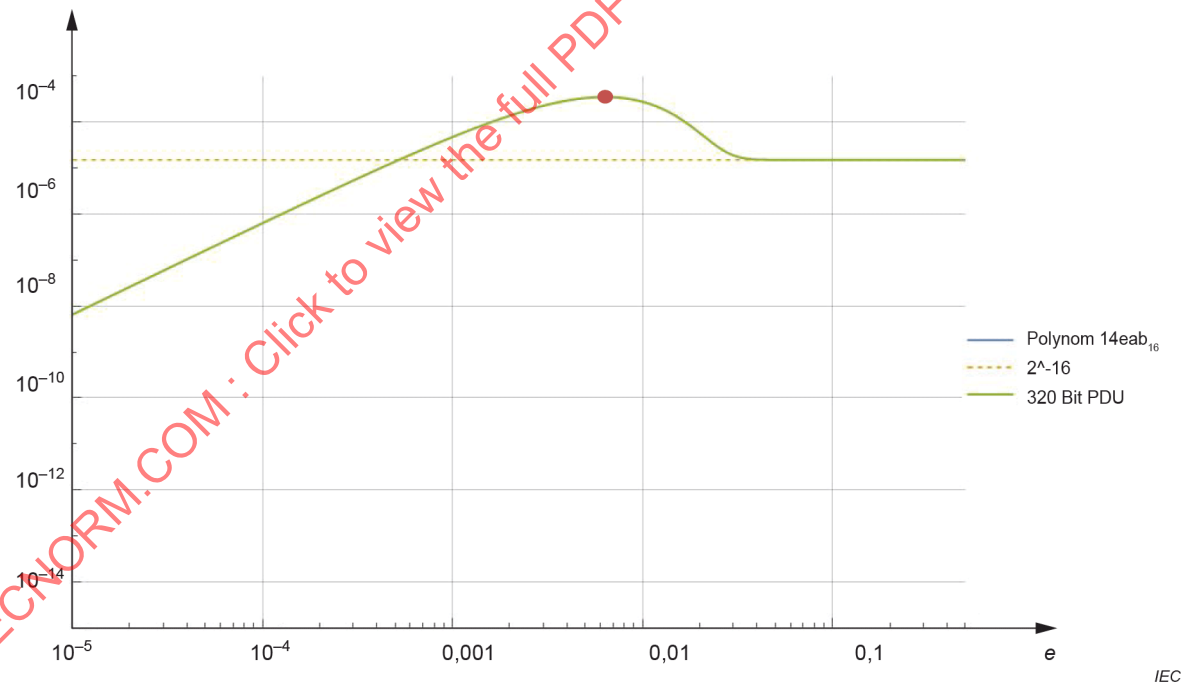


Figure H.10 – Residual error probabilities (example of a 16-bit CRC – result 4)

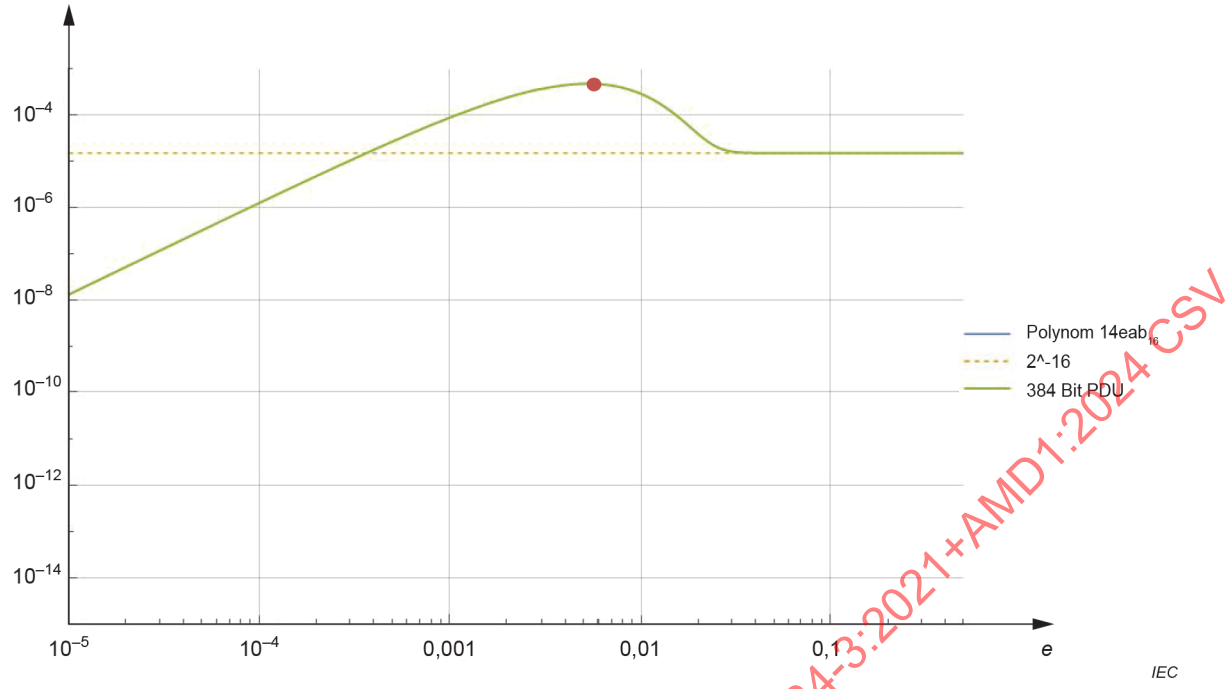


Figure H.11 – Residual error probabilities (example of a 16-bit CRC – result 5)

H.4 Conclusion

If the maximum residual error probability at any Pe < 0,01 is larger than the maximum value at Pe = 0,01 then this maximum residual error probability shall be applied in the calculation.

Figure H.12 and Figure H.13 show examples of improper polynomials.

Case 1: Maximum of R_{CRC} is where Pe > 0,01, therefore the residual error probability at a Pe = 0,01 applies.

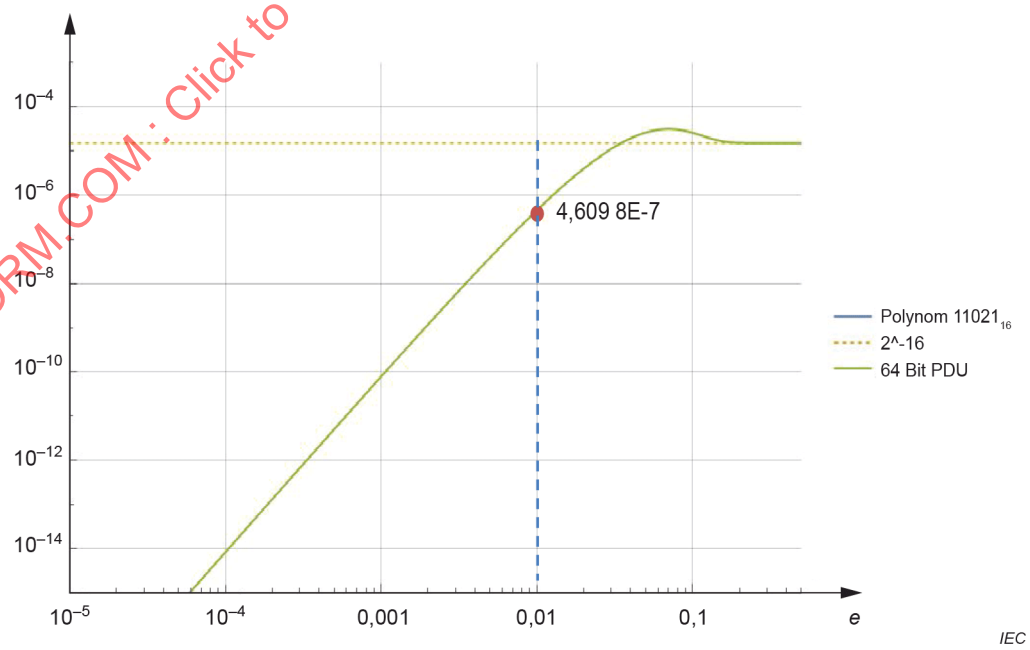


Figure H.12 – Example 1 of improper polynomial

Case 2: Maximum of R_{CRC} is where Pe < 0,01, therefore this maximum residual error probability applies.

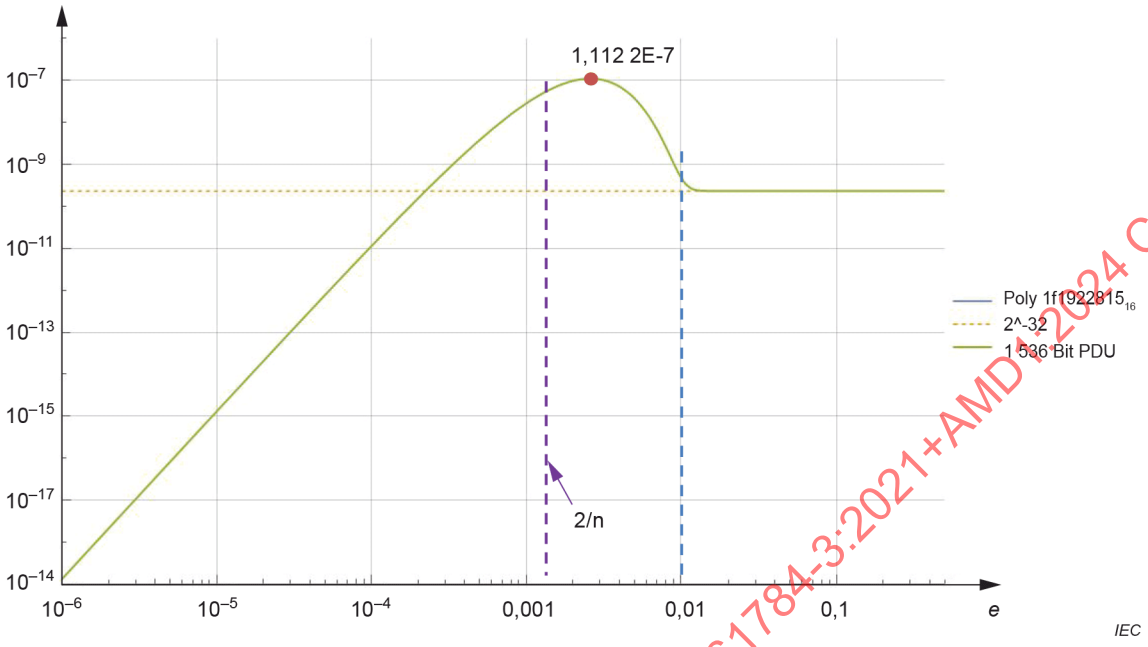


Figure H.13 – Example 2 of improper polynomial

Annex I
(informative)

Comprehensive safety communication channel data integrity model using CRC-based error checking

I.1 Overview

Annex I contains a black channel model for data integrity calculations based on binary symmetric channel in addition to data corruption faults affecting multiple contiguous bits.

For data integrity calculations of safety communication channels, application of the binary symmetric channel (BSC) model alone is useful for evaluating comparisons of CRC-based error checking efficacy. However, it is not sufficient for modeling several data corruption error types.

Annex B recommends use of the BSC model unless a different model can be proven more applicable for a particular functional safety communications protocol (FSCP). This recommendation has a history based on a recognition that alternative models were generally complex and difficult to calculate, and further, using a sufficiently conservative upper limit for bit error probability P_e results in sufficiently conservative values for residual error probability RP_I that can be used to evaluate the relative effectiveness of CRC-based error checking implementations.

This Annex I describes a comprehensive data corruption model which is more applicable than BSC alone for evaluating the data integrity of FSCPs. In addition to single bit error probability (BSC), this comprehensive model accounts for faults that affect multiple data bits with a single fault occurrence. These multiple-bit data faults are a prevalent type of data corruption fault affecting black channels.

This comprehensive data corruption model adds to the BSC model yet is no more complicated to calculate because, like BSC, it uses binary distribution. Further, it demonstrates that using BSC alone, with an upper limit of 10^{-2} for P_e is not sufficiently conservative for evaluating the residual error probability of data corruption errors for FSCPs unless the associated black channel is shown to exhibit only BSC type errors.

I.2 Basic principles

Although the BSC model accounts for some data corruption errors, a number of data error types, where multiple contiguous bits are affected by a single fault, are not addressed with BSC alone.

For example, there are data corruption errors that do not follow the BSC model (see [81]):

- burst errors;
- overwrite errors;
- shift errors;
- message length errors;
- bit slipping errors;
- masquerade errors;
- data errors before bit de-stuffing;
- data errors before symbol decoding;
- data errors before decompression;

- data errors before error correction;
- data errors before decryption.

To account for these multiple-bit error types, a comprehensive channel model for data integrity calculations is needed.

I.3 General case

A comprehensive model has been developed (see [81]) that considers the aforementioned multiple-bit data corruption error cases by applying approximation modeling using uniformly distributed segments (UDS) and superimposes this with the BSC model.

The UDS model treats data corruption errors as affected segments of bits within which the error patterns are uniformly distributed. All possible combinations of affected segment lengths, positions, and bit values occur with equal probability.

In accordance with mathematical analysis, the UDS model is described by means of a binomial distribution with probability parameter p up to 0,5. This UDS model is superimposed with the BSC model (also using binomial distribution) with probability parameter p as described in Annex B (using bit error probability P_e) up to the limit p_{max}^{BSC}.

NOTE 1 p represents a parameter of the binomial distribution for the UDS model, in contrast to its meaning in the BSC model, where, for example, a P_e of 0,5 implies a case where on average one out of two bits is erroneous.

The comprehensive data corruption residual error probability RP_I is given by Equation (I.1).

$$RP_I \leq \max_{0 \leq p \leq p_{max}^{BSC}} RP_I^{Binom}(p) \times (1 - P(f^{UDS})) + \max_{0 \leq p \leq 0,5} RP_I^{Binom}(p) \times P(f^{UDS}) \quad (I.1)$$

where

RP_I is the comprehensive data corruption residual error probability;

p_{max}^{BSC} is the upper limit of the BSC bit error probability;

RP_I^{Binom} is the residual error probability with binomial distribution;

$P(f^{UDS})$ is the probability of occurrence of a fault causing UDS errors.

In the first summand, a maximum bit error probability (usually 10^{-2}) of the BSC applies. Both summands contain the probability of occurrence of a fault causing UDS errors $P(f^{UDS})$. The worst-case value of 1 shall be used for $P(f^{UDS})$ as shown in Clause I.4. However, FSCPs may specify instead their own values if sufficient proof is provided.

NOTE 2 Actual methods of proof for $P(f^{UDS})$ of less than 1 are beyond the scope of IEC 61784-3.

I.4 Upper estimation

For cases where the probability of occurrence for UDS errors $P(f^{UDS})$ is not known, the upper estimation of comprehensive data corruption residual error probability RP_I is applied, given by Equation (I.2).

$$RP_I \leq \max_{0 \leq p \leq 0,5} RP_I^{Binom}(p) \quad (I.2)$$

NOTE Equation (I.2) is the equivalent of an application of the BSC calculation with P_e up to 0,5.

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 ~~15~~14, *International Electrotechnical Vocabulary – Chapter 191: Dependability and quality of service*

[3] IEC 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*

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

[5] IEC 61158-2:2014, *Industrial communication networks – Fieldbus specifications – Part 2: Physical layer specification and service definition*

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

[7] IEC 61158-3-2, *Industrial communication networks – Fieldbus specifications – Part 3-2: Data-link layer service definition – Type 2 elements*

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

[9] IEC 61158-3-8, *Industrial communication networks – Fieldbus specifications – Part 3-8: Data-link layer service definition – Type 8 elements*

[10] IEC 61158-3-12, *Industrial communication networks – Fieldbus specifications – Part 3-12: Data-link layer service definition – Type 12 elements*

[11] IEC 61158-3-13, *Industrial communication networks – Fieldbus specifications – Part 3-13: Data-link layer service definition – Type 13 elements*

[12] IEC 61158-3-14, *Industrial communication networks – Fieldbus specifications – Part 3-14: Data-link layer service definition – Type 14 elements*

[13] IEC 61158-3-18, *Industrial communication networks – Fieldbus specifications – Part 3-18: Data-link layer service definition – Type 18 elements*

[14] IEC 61158-3-19, *Industrial communication networks – Fieldbus specifications – Part 3-19: Data-link layer service definition – Type 19 elements*

[15] IEC 61158-3-21, *Industrial communication networks – Fieldbus specifications – Part 3-21: Data-link layer service definition – Type 21 elements*

[16] IEC 61158-3-22, *Industrial communication networks – Fieldbus specifications – Part 3-22: Data-link layer service definition – Type 22 elements*

~~15~~14 Withdrawn

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

[18] IEC 61158-4-2, *Industrial communication networks – Fieldbus specifications – Part 4-2: Data-link layer protocol specification – Type 2 elements*

[19] IEC 61158-4-3, *Industrial communication networks – Fieldbus specifications – Part 4-3: Data-link layer protocol specification – Type 3 elements*

[20] IEC 61158-4-8, *Industrial communication networks – Fieldbus specifications – Part 4-8: Data-link layer protocol specification – Type 8 elements*

[21] IEC 61158-4-12, *Industrial communication networks – Fieldbus specifications – Part 4-12: Data-link layer protocol specification – Type 12 elements*

[22] IEC 61158-4-13, *Industrial communication networks – Fieldbus specifications – Part 4-13: Data-link layer protocol specification – Type 13 elements*

[23] IEC 61158-4-14, *Industrial communication networks – Fieldbus specifications – Part 4-14: Data-link layer protocol specification – Type 14 elements*

[24] IEC 61158-4-18, *Industrial communication networks – Fieldbus specifications – Part 4-18: Data-link layer protocol specification – Type 18 elements*

[25] IEC 61158-4-19, *Industrial communication networks – Fieldbus specifications – Part 4-19: Data-link layer protocol specification – Type 19 elements*

[26] IEC 61158-4-21, *Industrial communication networks – Fieldbus specifications – Part 4-21: Data-link layer protocol specification – Type 21 elements*

[27] IEC 61158-4-22, *Industrial communication networks – Fieldbus specifications – Part 4-22: Data-link layer protocol specification – Type 22 elements*

[28] IEC 61158-5 (all parts), *Industrial communication networks – Fieldbus specifications – Part 5: Application layer service definition*

[29] IEC 61158-5-2, *Industrial communication networks – Fieldbus specifications – Part 5-2: Application layer service definition – Type 2 elements*

[30] IEC 61158-5-3, *Industrial communication networks – Fieldbus specifications – Part 5-3: Application layer service definition – Type 3 elements*

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

[32] IEC 61158-5-8, *Industrial communication networks – Fieldbus specifications – Part 5-8: Application layer service definition – Type 8 elements*

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

[34] IEC 61158-5-10, *Industrial communication networks – Fieldbus specifications – Part 5-10: Application layer service definition – Type 10 elements*

[35] IEC 61158-5-12, *Industrial communication networks – Fieldbus specifications – Part 5-12: Application layer service definition – Type 12 elements*

[36] IEC 61158-5-13, *Industrial communication networks – Fieldbus specifications – Part 5-13: Application layer service definition – Type 13 elements*

[37] IEC 61158-5-14, *Industrial communication networks – Fieldbus specifications – Part 5-14: Application layer service definition – Type 14 elements*

[38] IEC 61158-5-18, *Industrial communication networks – Fieldbus specifications – Part 5-18: Application layer service definition – Type 18 elements*

[39] IEC 61158-5-19, *Industrial communication networks – Fieldbus specifications – Part 5-19: Application layer service definition – Type 19 elements*

[40] IEC 61158-5-21, *Industrial communication networks – Fieldbus specifications – Part 5-21: Application layer service definition – Type 21 elements*

[41] IEC 61158-5-22, *Industrial communication networks – Fieldbus specifications – Part 5-22: Application layer service definition – Type 22 elements*

[42] IEC 61158-5-23, *Industrial communication networks – Fieldbus specifications – Part 5-23: Application layer service definition – Type 23 elements*

[43] IEC 61158-6-2, *Industrial communication networks – Fieldbus specifications – Part 6-2: Application layer protocol specification – Type 2 elements*

[44] IEC 61158-6-3, *Industrial communication networks – Fieldbus specifications – Part 6-3: Application layer protocol specification – Type 3 elements*

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

[46] IEC 61158-6-8, *Industrial communication networks – Fieldbus specifications – Part 6-8: Application layer protocol specification – Type 8 elements*

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

[48] IEC 61158-6-10, *Industrial communication networks – Fieldbus specifications – Part 6-10: Application layer protocol specification – Type 10 elements*

[49] IEC 61158-6-12, *Industrial communication networks – Fieldbus specifications – Part 6-12: Application layer protocol specification – Type 12 elements*

[50] IEC 61158-6-13, *Industrial communication networks – Fieldbus specifications – Part 6-13: Application layer protocol specification – Type 13 elements*

[51] IEC 61158-6-14, *Industrial communication networks – Fieldbus specifications – Part 6-14: Application layer protocol specification – Type 14 elements*

[52] IEC 61158-6-18, *Industrial communication networks – Fieldbus specifications – Part 6-18: Application layer protocol specification – Type 18 elements*

[53] IEC 61158-6-19, *Industrial communication networks – Fieldbus specifications – Part 6-19: Application layer protocol specification – Type 19 elements*

[54] IEC 61158-6-21, *Industrial communication networks – Fieldbus specifications – Part 6-21: Application layer protocol specification – Type 21 elements*

[55] IEC 61158-6-22, *Industrial communication networks – Fieldbus specifications – Part 6-22: Application layer protocol specification – Type 22 elements*

[56] IEC 61158-6-23, *Industrial communication networks – Fieldbus specifications – Part 6-23: Application layer protocol specification – Type 23 elements*

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

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

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

[60] 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*

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

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

[63] IEC 62061:~~2005~~2021, *Safety of machinery – Functional safety of safety-related ~~electrical, electronic and programmable electronic~~ control systems*
~~IEC 62061:2005/AMD1:2012~~
~~IEC 62061:2005/AMD2:2015~~

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

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

[66] ISO/IEC 2382:2015, *Information technology – Vocabulary*

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

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

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

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

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

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

[73] 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

[74] 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

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

[76] 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

[77] D. KNUTH, *The Art of Computer Programming, Volume 2: Seminumerical Algorithms*, 3rd Edition, Addison-Wesley, 1997

[78] F. SCHILLER and T. MATTES, *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

[79] Francis SWARTS, *Undetected error behaviour of linear block codes on channels with memory*, PhD thesis, University of Johannesburg, 1994

[80] A. KUZNETSOV, Francis SWARTS, Hendrik C FERREIRA, et al, *On the undetected error probability of linear block codes on channels with memory*, IEEE Transactions on Information Theory, vol. 42, no. 1, pp:303-309, Jan. 1996

[81] SCHILLER F, et.al., *Enhancement of Safety Communication Model – Preserving the Black Channel Concept,* Automatisierungstechnik, vol. 70, no. 1, pp. 38-52. https://doi.org/10.1515/auto-2021-0098, De Gruyter, 2022

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES –

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

FOREWORD

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

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

IEC 61784-3 edition 4.1 contains the fourth edition (2021-02) [documents 65C/1067/FDIS and 65C/1072/RVD] and its amendment 1 (2024-02) [documents 65C/1284/FDIS and 65C/1291/RVD].

This Final version does not show where the technical content is modified by amendment 1. A separate Redline version with all changes highlighted is available in this publication.

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

This fourth edition constitutes a technical revision.

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

- Contents of previous Annex F were corrected based on feedback from peer review and subsequent analysis (in particular deletion of RP_U for data integrity, reduction of the Equation for RR_A, and clarifications on the values of RP_I and R_T).
- Additional assumptions for residual error rate calculations, clarification of assumption a).
- After correction, contents of previous Annex F were exchanged with the contents of previous Subclause 5.8.
- Contents of Subclause 5.9 on security replaced by a simple reference to IEC 62443 in accordance with Guide 120.
- Changes in Annex B: Dependency of this Annex B with the BSC model has been highlighted. First two paragraphs and figure in Clause B.2 have been deleted because of little relevance. The approximation Equation (B.4) has been deleted due to obsolescence, based on the observations that the CRC shall be anyway explicitly calculated in order to prove properness, and that it may produce optimistic results. Guidance for calculation of R_{CRC} in B.4.2 has been reviewed.
- Changes in Annex D: Formula D.1 was changed from an approximation to a proper Equation, with some adjustments, and contents of D.4.3 were clarified (default safety action).
- New informative Annex H, providing additional guidance for the calculation of RCRC.

This document 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 document and its amendment will remain unchanged until the stability date indicated on the IEC website under webstore.iec.ch in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn, or
- revised.

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

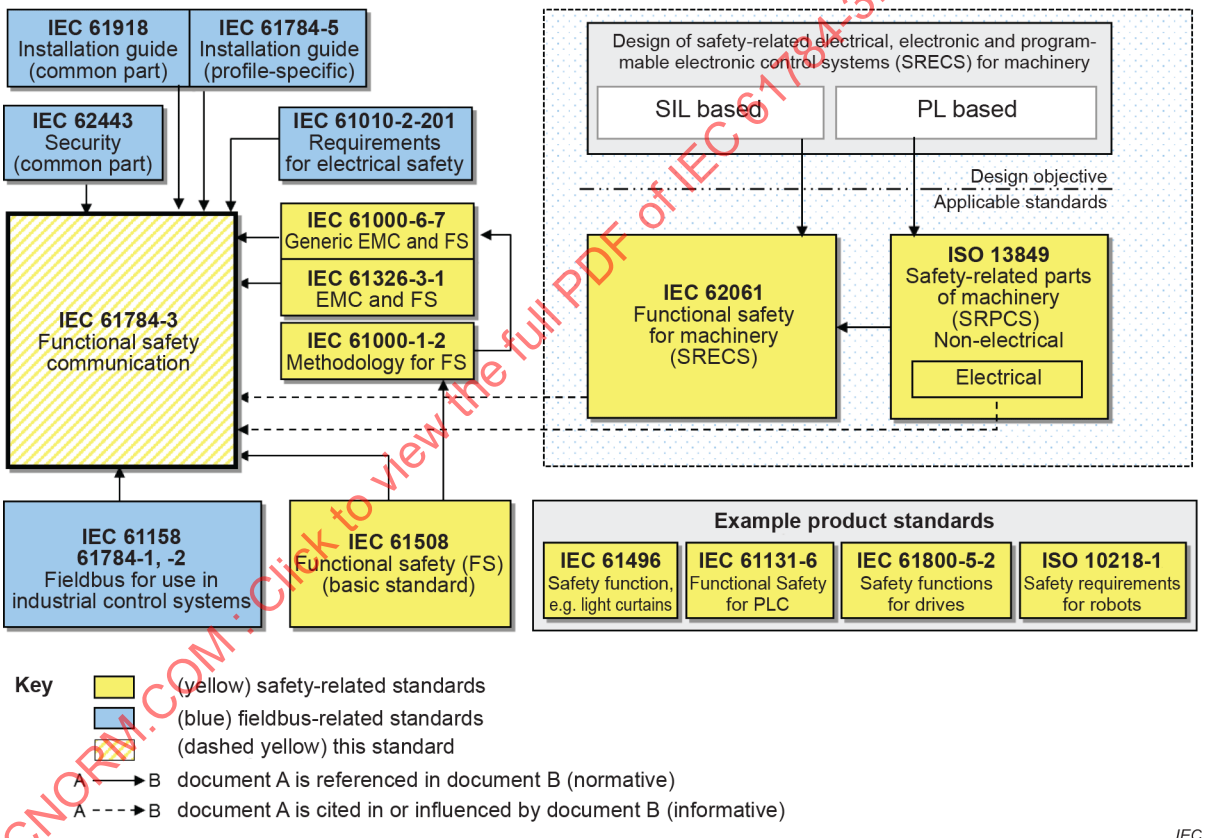
0 Introduction

0.1 General

The IEC 61158 (all parts) 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 and safety-related applications.

IEC 61784-3 (all parts) explains the relevant principles for functional safety communications with reference to IEC 61508 (all parts) 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 IEC 61158 (all parts). It does not cover electrical safety and intrinsic safety aspects. It also does not cover security aspects, nor does it provide any requirements for security.

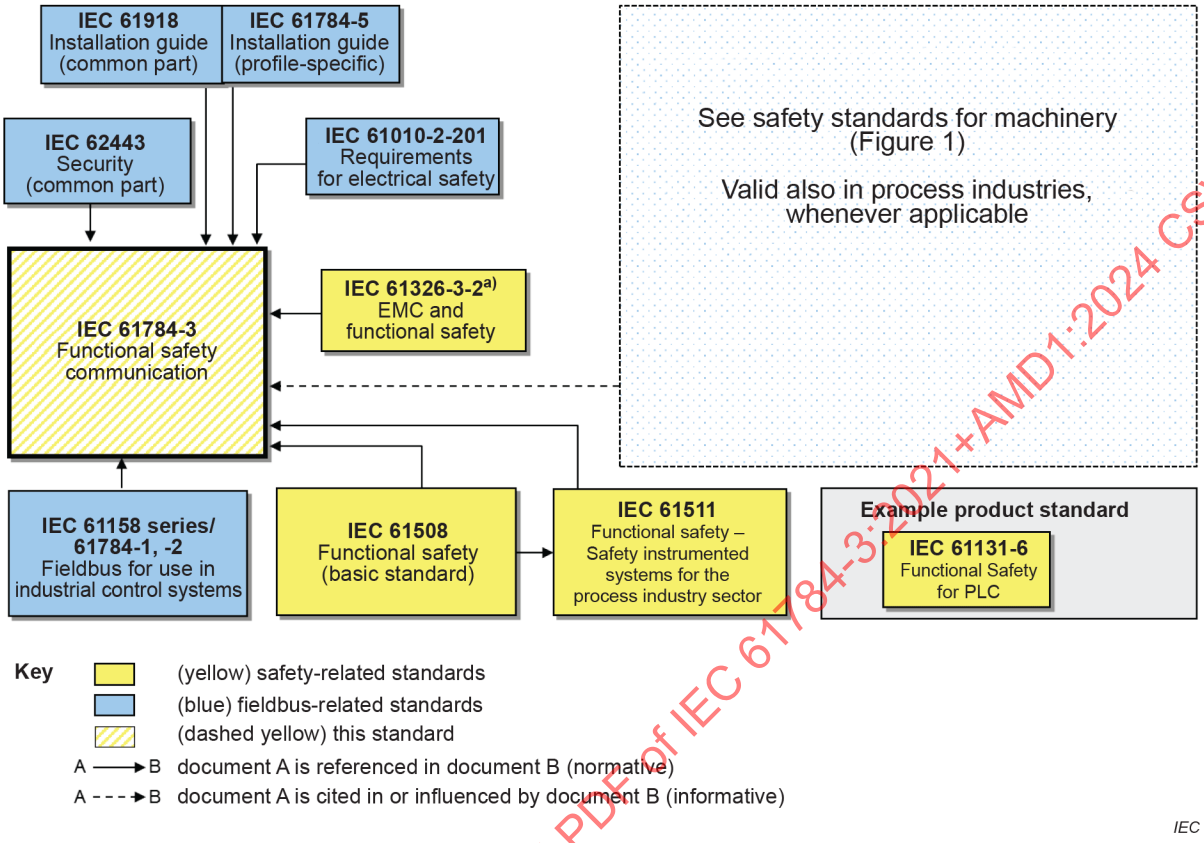
Figure 1 shows the relationships between IEC 61784-3 (all parts) and relevant safety and fieldbus standards in a machinery environment.



NOTE IEC 62061 specifies the relationship between PL (Category) and SIL.

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

Figure 2 shows the relationships between IEC 61784-3 (all parts) and relevant safety and fieldbus standards in a process environment.



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

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

Safety communication layers which are implemented as parts of safety-related systems according to IEC 61508 (all parts) 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 IEC 61784-3 (all parts) 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.

IEC 61784-3 (all parts) describes:

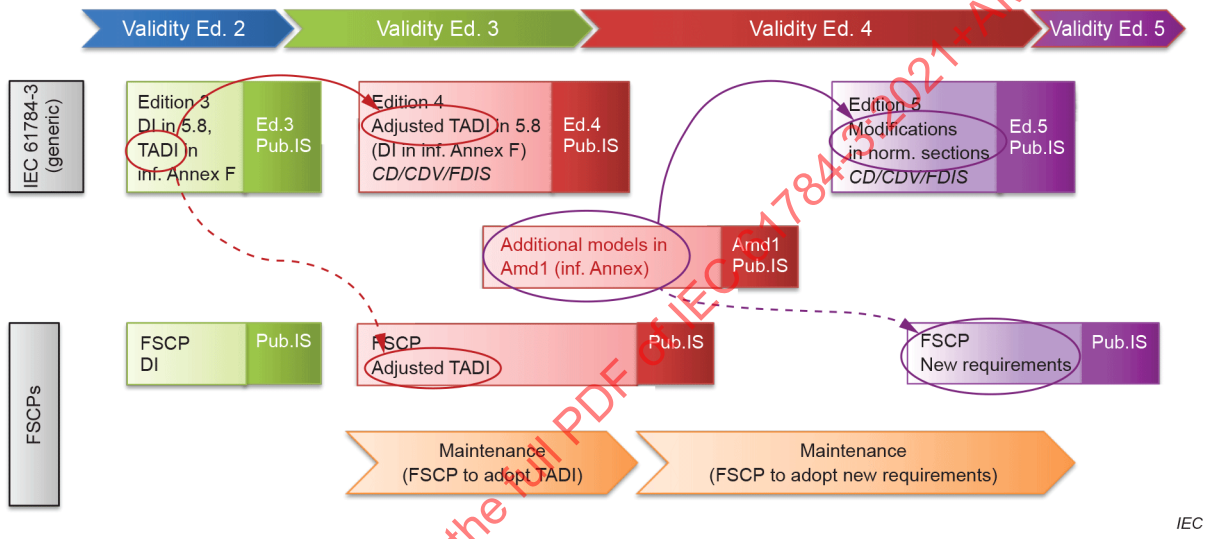
- basic principles for implementing the requirements of IEC 61508 (all parts) for safety-related data communications, including possible transmission faults, remedial measures and considerations affecting data integrity;
- functional safety communication profiles for several communication profile families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

0.2 Use of extended assessment methods in Edition 4

This edition of the generic part of IEC 61784-3 (all parts) includes extended models for 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 5.8.

Upon publication of this new edition of the generic part, FSCPs shall be assessed using the methods from this Edition 4, based on the extended models specified in 5.8 (derived from a modified version of Annex F of Edition 3). The informative Annex F contains the legacy models for reference purpose only.

Figure 3 shows the transitions from original assessment methods of Edition 2 to extended assessment methods in this Edition 4 and the future Edition 5.



Key

DI Data Integrity

TADI Timeliness, Authenticity, Data Integrity

Figure 3 – Transitions from Ed. 2 to Ed. 4 and future Ed. 5 assessment methods

0.3 Patent declaration

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

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

The holders of these patent rights have assured IEC that they are willing to negotiate licences under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statements of the holders of these patent rights are registered with IEC. Information may be obtained from the patent database available at http://patents.iec.ch.

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

INTRODUCTION to Amendment 1

This Amendment 1 discusses the concepts of a comprehensive channel model for data integrity calculations for functional safety communications protocols (FSCPs) as specified in IEC 61784-3:2021. The comprehensive channel model addresses data corruption error types where multiple contiguous bits are affected by a single fault.

It also reviews typical relationships between the possible errors and the various safety measures which can be implemented.

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 (all parts)[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 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 IEC 61158 (all parts). 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 (all parts) can exist that are not included in IEC 61784-3 (all parts).

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

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

NOTE 3 Implementation of a functional safety communication profile according to this document in a device is not sufficient to qualify it as a safety device, as defined in IEC 61508 (all parts).

NOTE 4 The resulting SIL claim of a system depends on the implementation of the selected functional safety communication profile within this system.

NOTE 5 Annex C explains the numbering scheme used for the technology-specific parts (IEC 61784-3-x) as well as their common general structure.

NOTE 6 Annex D provides a guideline for the assessment and test of safety communication profiles as well as safety-related devices using these profiles.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 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 document, “IEC 61508” will be used for “IEC 61508 (all parts)”.

IEC 61010-2-201, *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/IEEE 8802-3*

IEC 61784-3 (all parts), *Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses*

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

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

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

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

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

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

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

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

IEC 61784-3-17, *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 61918:2018, *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.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp

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 of "devices" and "fieldbus" instead of "entities" and "transmission system"]

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 61918:2018, 3.1.2]

3.1.3
bit error probability
Pe
probability for a given bit to be received with the incorrect value

3.1.4
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.

3.1.5
bridge
abstract device that connects multiple network segments along the data link layer

3.1.6
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]

3.1.7
communication channel
logical connection between two end-points within a *communication system*

3.1.8
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

3.1.9
connection
logical binding between two application objects within the same or different devices

3.1.10
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 document to refer to the redundant data.

Note 2 to entry: See also [71], [72][2].

3.1.11
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 (all parts), using for example zones and conduits

3.1.12
device
physical entity connected to the fieldbus composed of communication element and possibly other functional elements

[SOURCE: IEC 61158-2:2014, 3.1.13, modified – Note to entry and some details have been deleted.]

2 Figures in square brackets refer to the bibliography.

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]

3.1.14
DLPDU
DEPRECATED: frame
Data Link Protocol Data Unit

3.1.15
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]

3.1.16
explicit code
code for safety measure that is actually transmitted within the SPDU and is known to the sender and receiver

3.1.17
explicit data
data that is transmitted

Note 1 to entry: Explicit data is defined in contrast to implicit data.

3.1.18
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]

3.1.19
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]

3.1.20
fieldbus
communication system based on serial data transfer and used in industrial automation or process control applications

3.1.21
fieldbus system
system using a *fieldbus* with connected devices

3.1.22
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 [71], [72].

3.1.23
functional safety communication profile
FSCP
technology specification for the implementation of an SCL

3.1.24
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.

3.1.25
hazard
potential source of harm

Note 1 to entry: The term includes danger to persons arising within a short time scale (for example, fire and explosion) and also those that have a long-term effect on a person's health (for example, release of a toxic substance).

[SOURCE: IEC 61508-4:2010, 3.1.2 and ISO/IEC Guide 51:2014, definition 3.2]

3.1.26
implicit code
code for safety measure that is not transmitted within the SPDU but is known to the sender and receiver

3.1.27
implicit data
additional data that is not transmitted but is known to the sender and receiver, and used in the encoding and decoding of the message/SPDU

Note 1 to entry: Implicit data is defined in contrast to explicit data.

[SOURCE: IEC 62280:2014, 3.1.25, modified – addition of ", and used in the encoding and decoding of the message/SPDU" and of Note 1 to entry]

3.1.28
master
communication entity able to initiate and schedule communication activities by other stations which may be masters or slaves

3.1.29
message
<information theory and communication theory> ordered sequence of characters (usually octets) intended to convey information

[SOURCE: ISO/IEC 2382:2015, 2123205, modified – insertion of "(usually octets)", deletion of notes and source]

3.1.30
message sink
information sink
part of a *communication system* in which *messages* are considered to be received

[SOURCE: ISO/IEC 2382:2015, 2123207, modified – deletion of notes and source]

3.1.31
message source
information source
part of a *communication system* from which *messages* are considered to originate

[SOURCE: ISO/IEC 2382:2015, 2123206, modified – deletion of notes and source]

3.1.32
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]

3.1.33
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]

3.1.34
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]

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

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

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

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

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

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

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

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

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

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

3.1.44
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 document.

3.1.45
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.

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

3.1.46
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.

3.1.47
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.

3.1.48
safety-related application
programs designed in accordance with IEC 61508 to meet the SIL requirements of the application

3.1.49
safety-related system
system performing *safety functions* according to IEC 61508

3.1.50
slave
communication entity able to receive messages and send them in response to another communication entity which may be a master or a slave, but not to initiate communication activities

3.1.51
spurious trip
trip caused by the safety system without a process demand

3.1.52
time stamp
time information included in a *message*

3.1.53
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.

3.1.54
white channel
defined communication system in which all relevant hardware and software elements are designed, implemented and validated according to IEC 61508

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

3.1.55
uniformly distributed segment
UDS
segment of a message consisting of contiguous bits within which error patterns are uniformly distributed

3.2 Symbols and abbreviated terms

3.2.1 Abbreviated terms

A-code	Authenticity code	
BSC	Binary Symmetric Channel	(see Clause B.2)
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 (all parts)]
FCS	Frame Check Sequence	
FIT	Failure In Time (equals 10^{-9} failure per hour)	
FS	Functional Safety	
FSCP	Functional Safety Communication Profile	
IACS	Industrial Automation and Control System	
MTBF	Mean Time Between Failures	
MTTF	Mean Time To Failure	
NSR	Non Safety Related	
PDU	Protocol Data Unit	[ISO/IEC 7498-1]
PELV	Protective Extra Low Voltage	[IEC 61010-2-201]
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	
SC	Safety Communication Channel	
SCL	Safety Communication Layer	
SELV	Safety Extra Low Voltage	[IEC 61010-2-201]
SIS	Safety Instrumented Systems	

SIL	Safety Integrity Level	[IEC 61508-4:2010]
SMS	Security Management System	[IEC 62443 (all parts)]
SPDU	Safety PDU	
SR	Safety Related	
T-code	Timeliness code	
UDS	uniformly distributed segment	

3.2.2 Symbols

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

4 Conformance

Each functional safety communication profile within IEC 61784-3 (all parts) is based on communication profiles of IEC 61784-1 or IEC 61784-2 and protocol layers of IEC 61158 (all parts).

A statement of conformance to a Functional Safety Communication Profile (FSCP) of IEC 61784-3 (all parts) shall be stated as either

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

or

conformance to IEC 61784-3 (Ed.y.z) 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.y.z)

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 document performs transmission of safety data. To simplify system calculations, it is recommended that any logical connection of the 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 5.8.11).

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.

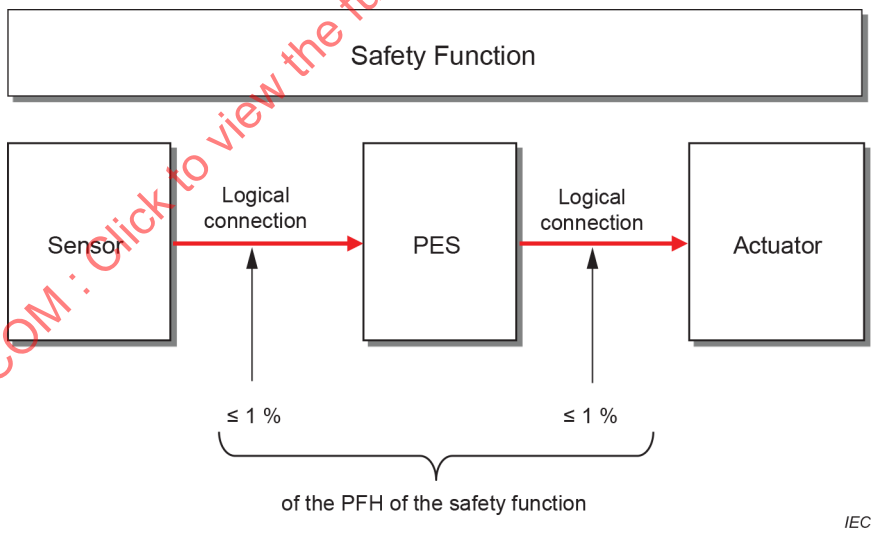


Figure 4 – Safety communication as a part of a safety function

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.

In any case, the safety manual for this FSCP shall provide guidance on the calculations of the PFH or PFD_{avg} for a safety function (see 5.8.10).

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 document focuses on the use of fieldbus based functional safety communication systems. Figure 5 shows an example model of the use of functional safety communications with a fieldbus based on the black channel approach.

When using IEC 61158 based fieldbus structures without modifications in the definition of each communication layer, all the measures necessary to implement transmission of safety data in accordance with the requirements of IEC 61508 shall be performed by an additional "safety communication layer", positioned as shown in Figure 5.

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

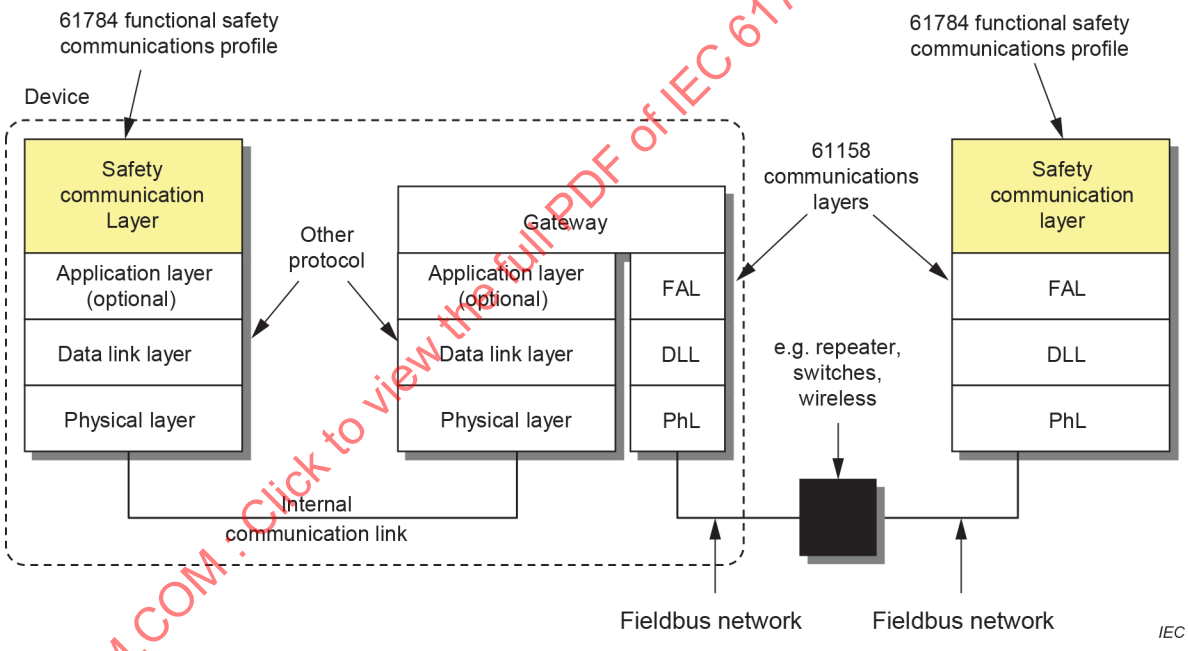


Figure 5 – Example model of a functional safety communication system

While implementation of the Fieldbus Application Layer (FAL) is required for functional safety communication systems according to this document, 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 "black channel" or "white channel" to define the requirements of the base fieldbus for transmission of safety data. This document 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 (all parts).

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

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

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

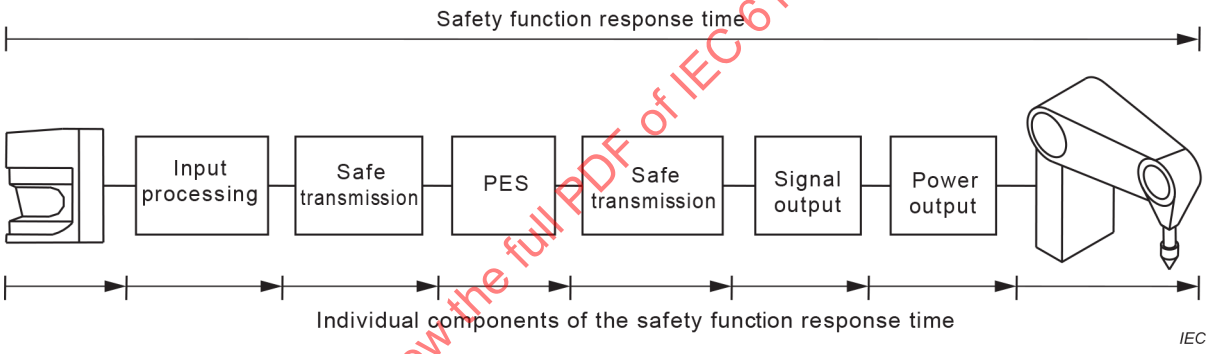


Figure 6 – Example of safety function response time components

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

5.3 Communication errors

5.3.1 General

Subclauses 5.3.2 to 5.3.9 specify possible communication errors. Additional notes are provided to indicate the typical behaviour of a black channel.

5.3.2 Corruption

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

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

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

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

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

5.3.3 Unintended repetition

Due to an error, fault or interference, messages are repeated.

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

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

5.3.4 Incorrect sequence

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

NOTE 1 This "incorrect sequence" error is also referred to as "out-of-sequence" error.

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

NOTE 3 When multiple sequences are active, such as messages from different source entities or reports relating to different object types, these sequences are monitored separately, and errors can be reported for each sequence.

5.3.5 Loss

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

5.3.6 Unacceptable delay

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

5.3.7 Insertion

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

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

5.3.8 Masquerade

Due to a fault or interference, a message from a non-safety related source is interpreted in such a way that it appears to originate from a valid safety related source entity. Non-safety related data would therefore 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 passphrases 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 5.4.8 list measures commonly used to detect deterministic errors and failures of a communication system, as contrasted to stochastic errors like message corruption due to electromagnetic interference.

5.4.2 Sequence number

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

5.4.3 Time stamp

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

NOTE Relative time stamps and absolute time stamps can be used.

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

5.4.4 Time expectation

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

EXAMPLE

Time-slot-oriented access method:

– the exchange of messages takes place within fixed cycles and predetermined time slots for every participant;

– optionally, every participant sends his data within its time slot even if there is no value change (this is an example of cyclic communication);

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

5.4.5 Connection authentication

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

5.4.6 Feedback message

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

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

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

5.4.7 Data integrity assurance

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

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

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

5.4.8 Redundancy with cross checking

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

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

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

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

5.5 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.

The effectiveness of a measure against errors depends on the specific implementation of this measure.

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

Table 1 – Typical relationships between errors and safety measures

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)
Corruption (see 5.3.2)					X [d]	X	X
Unintended repetition (see 5.3.3)	X	X					
Incorrect sequence (see 5.3.4)	X	X					
Loss (see 5.3.5)	X				X		
Unacceptable delay (see 5.3.6)		X	X [b]				
Insertion (see 5.3.7)	X [e]	X [e]		X [a]	X		
Masquerade (see 5.3.8)	X	X		X	X [d]	X	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] Void

[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 acknowledging of the feedback message.

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

5.6 Communication phases

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

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

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

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

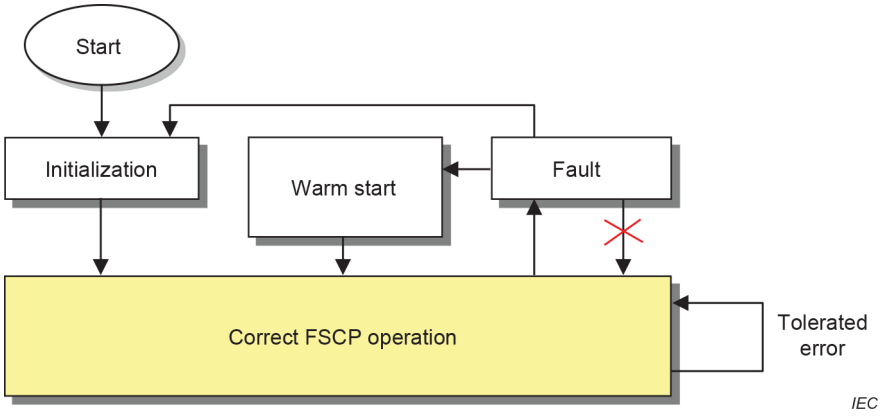


Figure 7 – Conceptual FSCP protocol model

5.7 FSCP implementation aspects

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

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

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

This document 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 endpoints (using only basic assumptions on the black channel performance as stated in the safety manuals of the individual FSCPs).

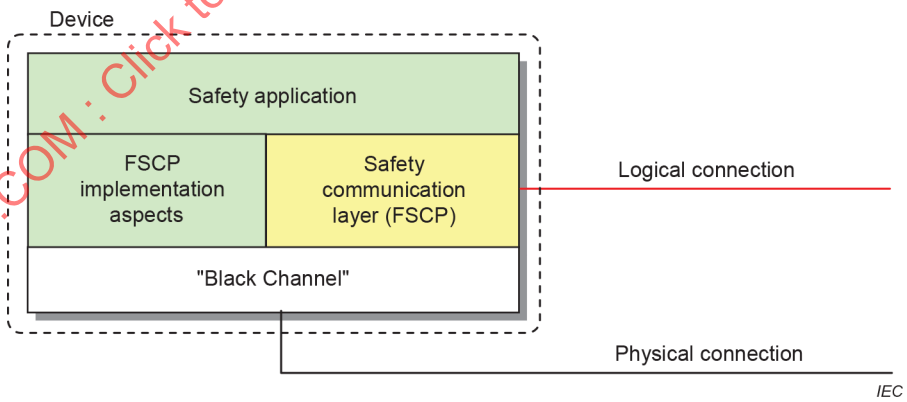


Figure 8 – FSCP implementation aspects

5.8 Models for estimation of the total residual error rate

5.8.1 Applicability

Subclause 5.8 specifies models for estimating the total residual error rate for an FSCP, for the purpose of assessing this FSCP.

5.8.2 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 9 shows a black channel that contains different types of communication: Fieldbus messages with safety and non-safety PDUs.

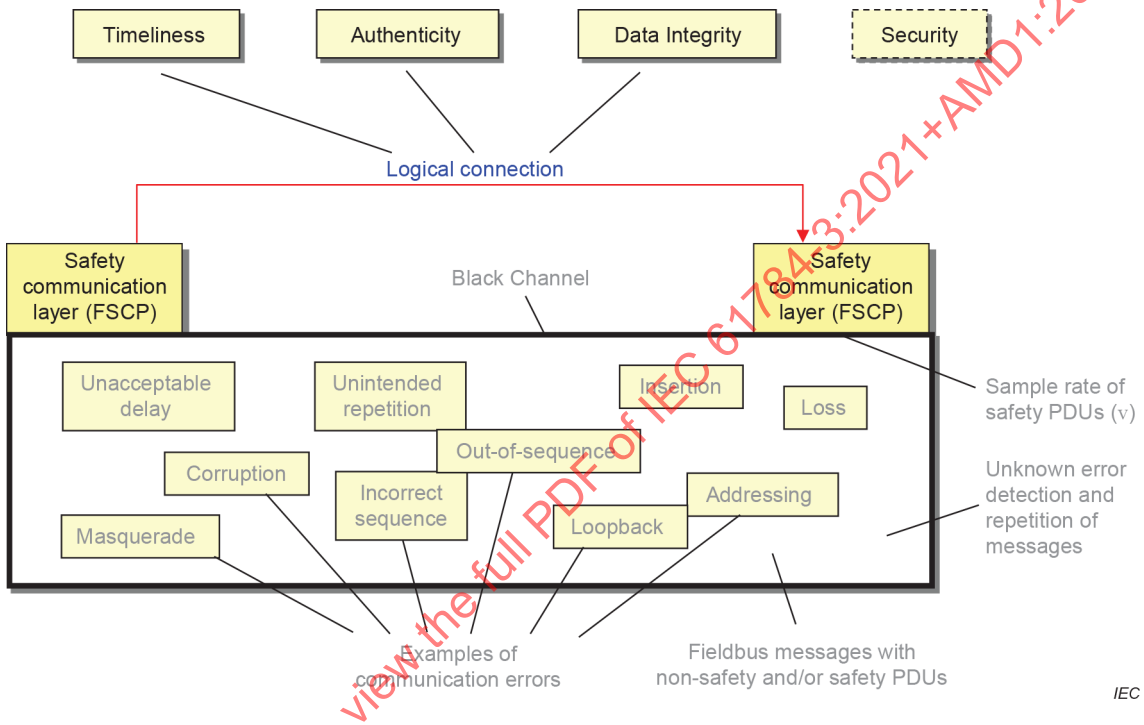


Figure 9 – Black channel from an FSCP perspective

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.

5.8.3 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 9):

- data integrity;
- authentication;
- 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 correct 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 document. Security issues are addressed in IEC 62443 (all parts).

Another generic safety aspect that shall be considered is the configuration and/or parameterization of the FSCP (see 5.8.12).

A fault in any of these generic safety measures may result in a hazard.

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 5.8.10.

5.8.4 Assumptions for residual error rate calculations

Subclause 5.8 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 5.8:

a) assuming a failure rate of an average black channel device to be 10^{-7}/h (100 FIT), the black channel device failure rate is taken to be 10 000 times this value for SCL calculations. Therefore, the 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 The error rate of 10^{-3} for a non-safety device is derived from ISO 13849-1:2015, Table 7, using a conservative margin compared to the weakest performance level.

   NOTE 3 A failure rate less conservative than 10^{-3}/h 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}/h would therefore render the safety communication channel inoperable.

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

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

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

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

f) each logical connection is assigned a unique authentication code, which is known to both sender and receiver prior to transmission of SPDUs;

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;

i) the CRC calculation is performed on the entire SPDU, including A-code and T-code.

5.8.5 Residual error rates

5.8.5.1 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 1 Implicit mechanism is typically used to accommodate limited systems with fixed black channel message sizes, slow transmission rates, or low-cost implementations.

The FSCPs specified in IEC 61784-3 (all parts) 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. Proof of sufficiently low residual error probability shall be demonstrated specifically for each FSCP. Therefore, Subclause 5.8 only deals with the explicit category.

NOTE 2 Annex G presents formulae examples for special cases, in order to provide guidance for the development of additional formulae for the residual error probabilities of FSCPs using implicit data safety mechanisms.

5.8.5.2 Residual error rate calculations

5.8.5.2.1 General

Subclauses 5.8.5.2.2 to 5.8.5.2.5 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.

5.8.5.2.2 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 (1).

$$RR_I = RP_I \times v \times RP_{FSCP\_I} \quad (1)$$

where

RR_I is the residual error rate for Data Integrity;

RP_I is the residual error probability for Data Integrity (see 5.8.6.3);

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

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

The measures used for RP_{FSCP_I} shall be independent of the data integrity measure.

5.8.5.2.3 Contribution of authenticity errors (RR_A)

There are three conditions necessary for this residual rate:

a) a misdirected PDU;

b) bit errors in the received authentication code resulting in a match with the expected authentication code, and

c) these bit errors are not detected by CRC.

Since the A-code is transmitted explicitly, bit errors in the received authentication code are already considered in the calculation of RP_I.

Since v is the maximum message sample rate, R_A (rate of occurrence for misdirected safety PDUs, see 5.8.7.2) is included in v.

As a result, a value of 0 (zero) will be used for RR_A in all equations where this term appears.

5.8.5.2.4 Contribution of timeliness errors (RR_T)

An example for the calculation of the residual error rate for Timeliness RR_T is shown in Equation (2).

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

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 (see 5.8.8.2) (value cannot exceed v, as specified in 5.8.5.2.2);

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

The measures used for RP_{FSCP_T} shall be independent of the timeliness measure.

Unlike the A-code, the T-code value changes over time, and therefore data integrity measures are necessary but not sufficient to detect timeliness errors.

5.8.5.2.5 Contribution of masquerade errors (RR_M)

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 (3). This Equation (3) assumes the SPDU structure differs from the structure of non-safety PDUs in terms of location of the fields of uniqueness.

$$RP_U = \frac{V_{A1}}{V_{R1}} \times \frac{V_{A2}}{V_{R2}} \times \ldots \times \frac{V_{AN}}{V_{RN}} \quad (3)$$

where

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

V_{Ai} is the number of values accepted by a sink in data field i (i = 1…N);

V_{Ri} is the number of values representing the total range for data field i (i = 1…N).

An example for the calculation of the residual error rate for Masquerade RR_M is shown in Equation (4).

$$RR_M = 2^{-LA} \times 2^{-LT} \times w \times 2^{-r} \times RP_U \times 2^{-LR} \times R_M \quad (4)$$

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 (see 5.8.9.2).

5.8.6 Data integrity

5.8.6.1 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;

– measures to assure that each SPDU checked by the black channel CRC is also checked by the SCL CRC since additional trials in the black channel with identical check would increase the Residual Error Rate.

5.8.6.2 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.

5.8.6.3 Residual error probability for data integrity RP_I

RP_I is the residual error probability for Data Integrity.

EXAMPLE See R_{CRC} in Annex B.

Annex B provides information on CRC-based error checking to address data integrity. Example literature is listed in B.4.2.

NOTE Annex I complements Annex B by providing a comprehensive data integrity model using CRC-based error checking.

5.8.7 Authenticity

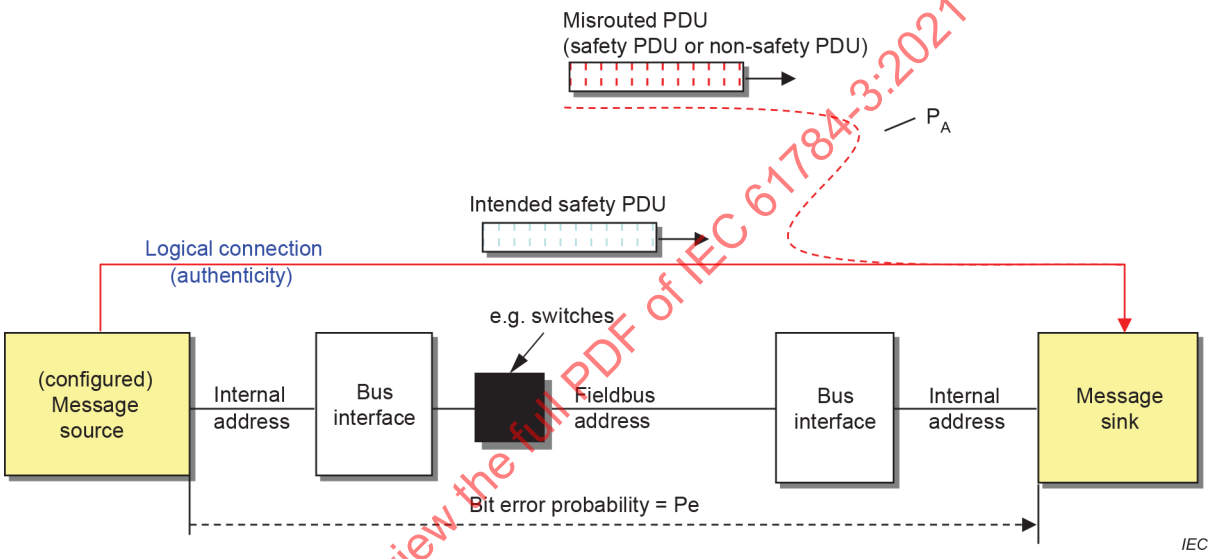
5.8.7.1 General

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 10):

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



Key

PA Probability of an authenticity error for logical connections

Figure 10 – Model for authentication considerations

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

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

NOTE

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

– falsification of an address within the message or an error within an internal communication link (see Figure 11) 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 11 shows typical locations of addressing errors due to corrupted addresses within the fieldbus communication system or possible internal addressing errors (for example due to corrupted pointers within modular remote I/O devices).

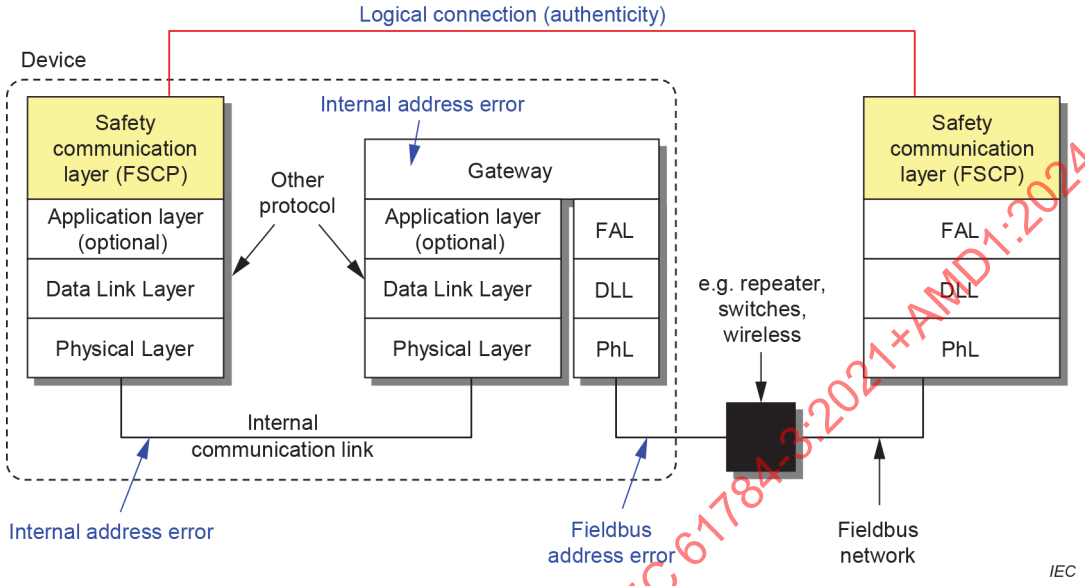


Figure 11 – Fieldbus and internal address errors

Additional systematic causes for incorrect authenticity may be identified within configuration and parameterization procedures as shown in 5.8.12. 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.

5.8.7.2 Rate of occurrence of misdirected SPDUs (R_A)

In accordance with 5.8.4 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 technical measures for the authentication can be supplemented by organizational measures, which shall be practical for the user to perform (see 5.8.12).

5.8.8 Timeliness

5.8.8.1 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 act as a message source and a message sink at the same time.

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

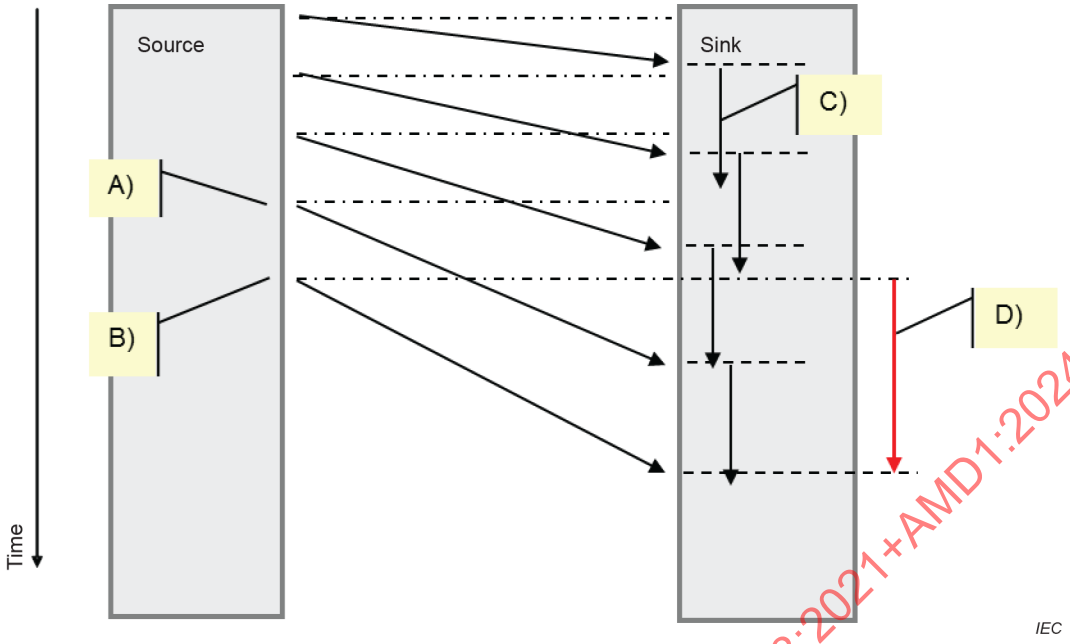
Typical causes for non-timely communication which shall be considered during the design of the FSCP are variable performances of the black channel.

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 12);
– 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 12 shows an example of a slowly increasing message latency of the black channel.



Key

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

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

C) Timeout check in sink

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

Figure 12 – 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 13).

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

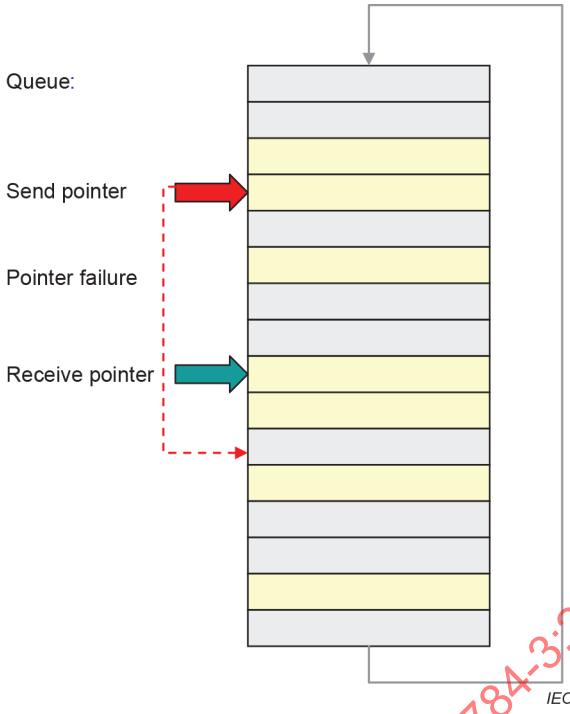


Figure 13 – Example of an active network element failure

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:

- 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.

5.8.8.2 Rate of occurrence of incorrect sequence SPDUs (R_T)

In a safety-related network with message storing elements (see Figure 13), in accordance with 5.8.4 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.

R_T shall be multiplied by 1 in case the SCL enters the safe state after detecting the first communication error. Otherwise R_T shall be multiplied with the maximum number of SPDUs sampled (checked by the receiving SCL) until the safe state has been entered by the SCL.

NOTE The multiplication is necessary because when an active network element fails as described in Figure 13, multiple erroneous SPDUs will be received, all potentially having a different timeliness code.

5.8.9 Masquerade

5.8.9.1 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).

5.8.9.2 Rate of occurrence for masqueraded SPDUs (R_M)

In accordance with 5.8.4 bullet a), a value of 10^{-3}/h per device (both safety related and non-safety related) shall be assumed for the rate of occurrence for masqueraded safety PDUs (R_M), unless otherwise specified.

5.8.10 Calculation of the total residual error rates

5.8.10.1 General

The total residual error rate λ_{SC} for the safety communication channel is needed to calculate the PFH or PFD_{avg} contributions, as explained in 5.1.

5.8.10.2 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 (5).

$$\lambda_{SC} = RR_T + RR_A + RR_I + RR_M \quad (5)$$

where

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

RR_T is the residual error rate per hour for Timeliness (see 5.8.5.2.4);

RR_A is the residual error rate per hour for Authenticity (see 5.8.5.2.3);

RR_I is the residual error rate per hour for Data Integrity (see 5.8.5.2.2);

RR_M is the residual error rate per hour for Masquerade (see 5.8.5.2.5).

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 (6) and in Figure 14 and Figure 15.

$$\lambda_{SCL} = \lambda_{SC} \times m \quad (6)$$

where

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

λ_{SC} is the total residual error rate per hour for the safety communication channel of one logical connection (see Equation (5));

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 14 and Figure 15 illustrate how this number can be determined.

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

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

Figure 14 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.

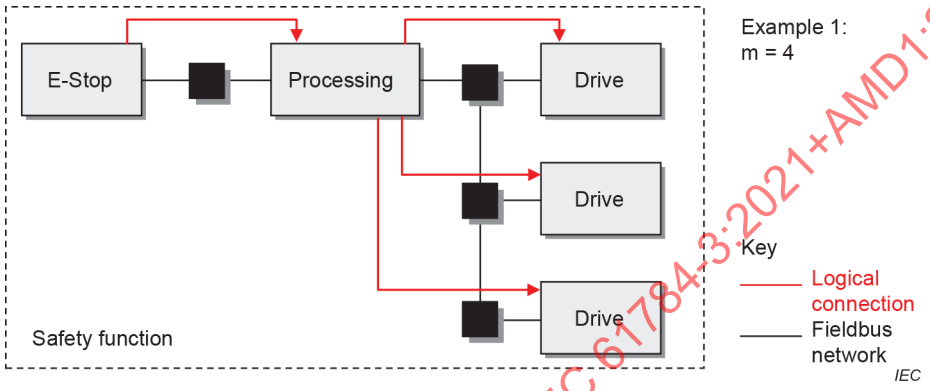


Figure 14 – Example application 1 (m = 4)

Figure 15 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.

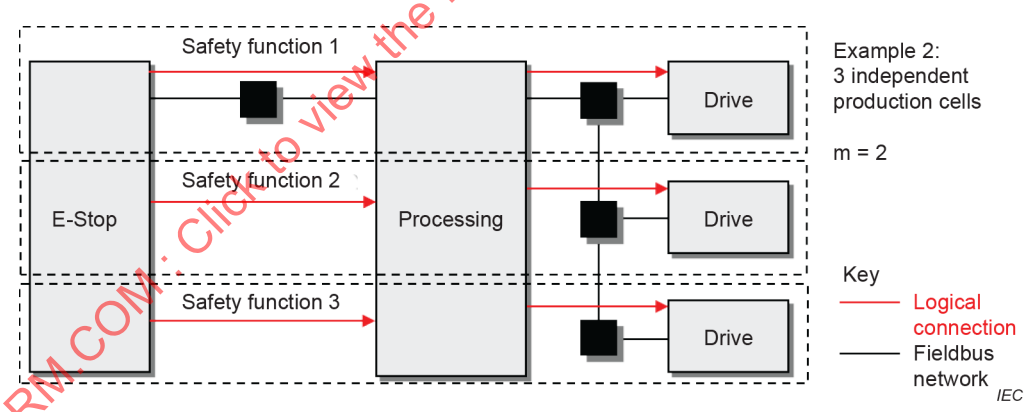


Figure 15 – Example application 2 (m = 2)

5.8.10.3 Based on other quantitative proofs

The summation of the residual error rates of the generic safety properties as shown in 5.8.10.1 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 directly use the methods of the IEC 61508 and to determine the Safe Failure Fraction and the Diagnostic Coverage of the FSCP.

5.8.11 Total residual error rate and SIL

A functional safety communication system shall provide a residual error rate in accordance with this document. Table 2 and Table 3 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 2 – 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 3 – 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 (PFD_{avg})	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}

5.8.12 Configuration and parameterization for an FSCP

5.8.12.1 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 16.

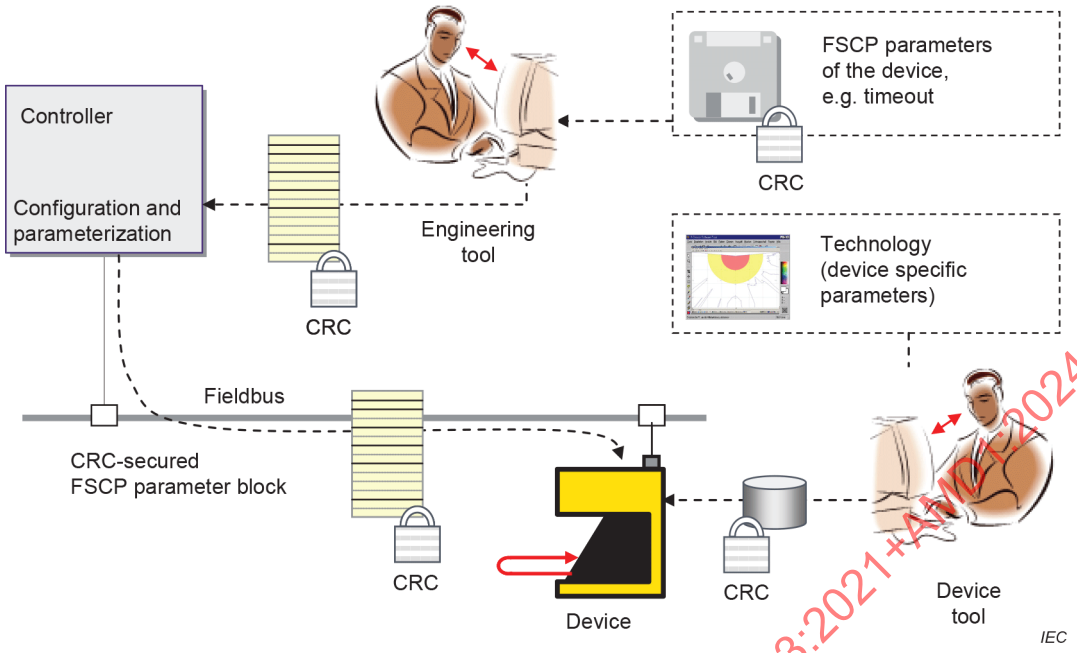


Figure 16 – Example of configuration and parameterization procedures for FSCP

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 62061:2021, 6.7.3 and IEC 62061:2021, 6.7.4 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.
– Detection of conflict between safety technology limits and FSCP parameters (such as safety technology cycle time longer than FSCP watchdog time).

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 62061:2021, 6.7.3 and IEC 62061:2021, 6.7.4 and ISO 13849-1:2015, 4.6.4.

5.8.12.2 Configuration and parameterization change rate

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

5.8.12.3 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 5.8.12.2.

5.9 Relationship between functional safety and security

Security shall be considered for safety-related applications that include functional safety communication systems. However, this document does not cover security aspects, nor does it provide any requirements for security. Security of industrial automation and control systems (IACS) is addressed in IEC 62443 (all parts).

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 (all parts).

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 (all parts).

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 IEC 61784-3 (all parts) are specified in IEC 61918 and the profile specific parts of IEC 61784-5 (all parts), 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), 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 IEC 61784-3 (all parts) 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.

Table 5 lists the summary of topics to be added in the safety manual of products implementing IEC 61784-3-x, if relevant.

Table 5 – Topics for the safety manual of products implementing IEC 61784-3-x

#	Item	Reference	Notes
1	Safety function decomposition PFH, PFDavg	5.1 and 5.8.10	Guidance on the calculations of the PFH or PFDavg for a safety function shall be provided.
2	FSCP installation aspects	5.7 5.8.4	If the safe behaviour of an FSCP or its provided PFH and PFDavg values depend on prerequisites made for the underlying communication channel, these prerequisites should be mentioned in the manual. Potential prerequisites include, but are not limited to: • maximum number of safe network endpoints; • maximum number of non-safe network endpoints; • maximum number of network devices (routers, switches); • maximum or minimum safety PDU and non-safety PDU rates; • watchdog time. Where appropriate, it should be explained in the manual how the end user can verify whether the prerequisites are fulfilled or not.
3	Installation guideline	5.11	The requirements for installation of equipment using the communication technologies specified in IEC 61784-3 are specified in IEC 61918 and IEC 61784-5-x.

#	Item	Reference	Notes
4	Authenticity	5.8.7.1	According to 5.8.7.1, authenticity requirements shall be met during all communication phases in 5.6 for which connection authentication is relevant. If automatic authenticity checks are not possible for certain phases (e.g. at first-time connection establishment), this shall be documented.
5	Configuration and parameterization	5.8.12.1	Systematic configuration and parameterization errors can only be safely prevented by verification and validation. The safety manuals shall provide the necessary instructions. (Relevant information see IEC 62061:2021, 6.7.3, 6.7.4 and ISO 13849-1:2015, 4.6.4)
6	Electrical safety	5.10.1	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.
7	Security	5.9	Security shall be considered for safety-related applications that include functional safety communication systems. Security of industrial automation and control systems (IACS) is addressed in IEC 62443 (all parts).
8	Safety function response time (SFRT)	D.4.6	Maximum safety function response time specified by the manufacturer and time required to complete a safety-related reaction shall not be exceeded, even in the presence of errors and failures.

5.13 Safety policy

Users of this document 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 IEC 61784-3 (all parts) shall only be implemented in devices designed in accordance with the requirements of IEC 61508.

The use of communication technologies specified in IEC 61784-3 (all parts) 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 IEC 61784-3 (all parts) 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 IEC 61784-3 (all parts) is responsible for the correct implementation of the standard, the correctness and completeness of the device documentation and information.

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

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

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

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

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

---

3 FOUNDATION™ Fieldbus and FF-SIS™ are trade names of the non-profit organization FieldComm Group. This information is given for the convenience of users of this document and does not constitute an endorsement by IEC of the trade name holder or any of its products. Compliance to this document 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 FieldComm Group and compliance with conditions for their use (such as testing and validation).

4 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 document and does not constitute an endorsement by IEC of the trade name holder or any of its products. Compliance to this document 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).

5 SERCOS® is a trade name of SERCOS International e.V. This information is given for the convenience of users of this document and does not constitute an endorsement by IEC of the trademark holder or any of its products. Compliance to this document 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).

6 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 document and does not constitute an endorsement by IEC of the trade name holder or any of its products. Compliance to this document 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™[6]) 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®[7]) 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™[7]) is based on the CPF 6 basic profiles in IEC 61784-1 and the safety communication layer specifications defined in IEC 61784-3-6.

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

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

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

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

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™[8]) 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™[8]) is based on the CPF 8 basic profiles in IEC 61784-1 and the safety communication layer specifications defined in IEC 61784-3-8.

---

7 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 document and does not constitute an endorsement by IEC of the trade name holder or any of its products. Compliance to this document 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).

8 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 document and does not constitute an endorsement by IEC of the trade name holder or any of its products. Compliance to this document 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™[9]) 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™[10]) 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™[10]) 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 Communication Profile Family 13 (Ethernet POWERLINK™) – Profiles for functional safety

Communication Profile Family 13 (commonly known as Ethernet POWERLINK™[11]) 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™[11]) 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®[12]) defines communication profiles based on IEC 61158-3-14, IEC 61158-4-14, IEC 61158-5-14, and IEC 61158-6-14.

---

9 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 document and does not constitute an endorsement by IEC of the trade name holder or any of its products. Compliance to this document 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).

10 EtherCAT™ and Safety-over-EtherCAT™ are trade names of Beckhoff, Verl. This information is given for the convenience of users of this document and does not constitute an endorsement by IEC of the trade name holder or any of its products. Compliance to this document 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).

11 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 document and does not constitute an endorsement by IEC of the trade name holder or any of its products. Compliance to this document 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 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 document and does not constitute an endorsement by

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®[12]) 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™ [13]) 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™[13]) is based on the CPF 17 basic profile in IEC 61784-2 and the safety communication layer specifications defined in IEC 61784-3-17.

IEC of the trade name holder or any of its products. Compliance to this document 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).

13 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 document and does not constitute an endorsement by IEC of the trade name holder or any of its products. Compliance with this document 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).

Annex A
(informative)

Example functional safety communication models

A.1 General

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

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

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

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

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

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

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

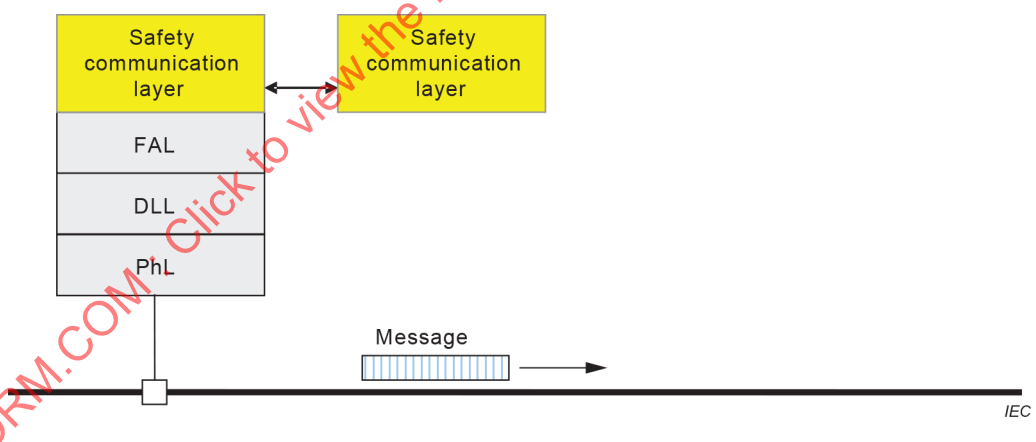


Figure A.1 – Model A

A.3 Model B (full redundancy)

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

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

Transmission layers and transmission media may be of different types.

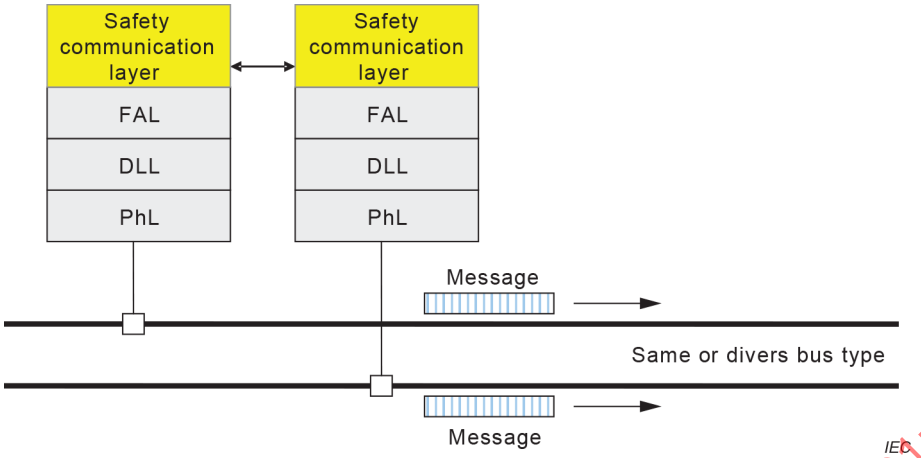


Figure A.2 – Model B

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

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

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

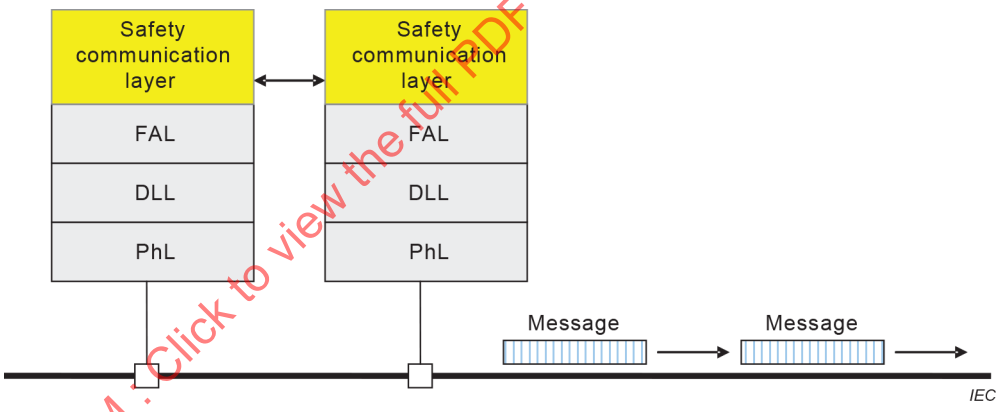


Figure A.3 – Model C

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

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

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

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

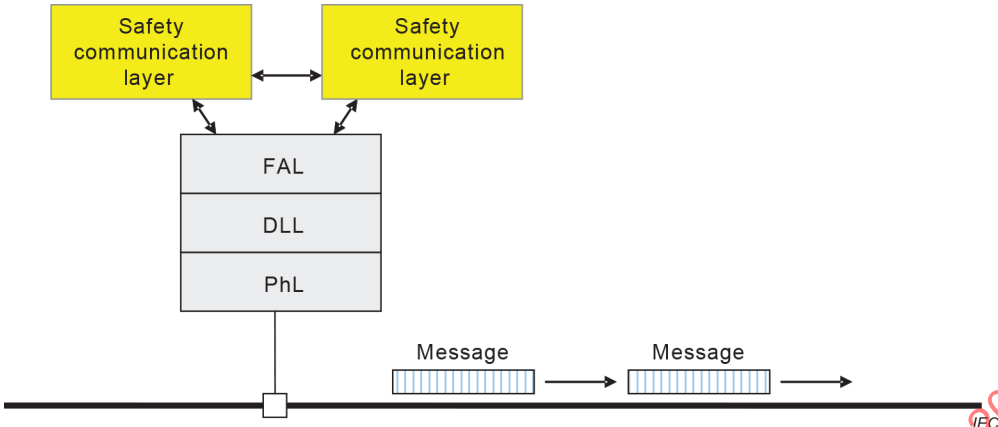


Figure A.4 – Model D

Annex B
(normative)

Safety communication channel model using CRC-based error checking

B.1 Overview

Annex B contains a black channel model for data integrity calculations based on binary symmetric channel. Use of the binary symmetric channel model is recommended unless a different model can be proven more applicable for a particular FSCP.

B.2 Channel model for calculations

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.1). Furthermore, it is assumed all bit cells have the same bit error probability $P_e = P$.

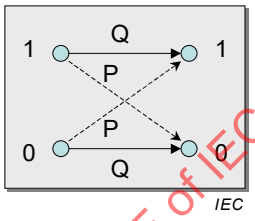


Figure B.1 – Binary symmetric channel (BSC)

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.

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

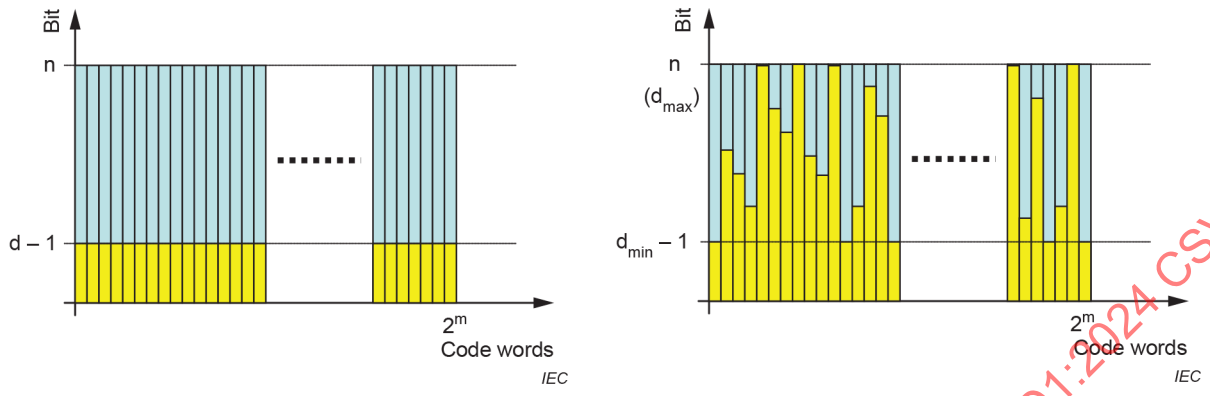
In case the block contains a fictive coding to detect error patterns up to d-1 such as shown in Figure B.2 with a minimum Hamming distance d_{min}, an upper limit residual error probability $R_{UL}(P_e)$ can be calculated with the Equation (B.2) shown below.

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

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

However, this simplified equation does not take into account that even a simple parity bit (minimum Hamming distance $d_{min} = 2$) 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.

Figure B.2 illustrates the background for the Equation (B.2).



a) Fictive code

b) CRC coding

Key

	detectable number of perturbed bits
n	block length
d	Hamming distance
d_{min}	minimum Hamming distance
m	message length

Figure B.2 – 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.

EXAMPLE

Table B.1 shows the block bit length n for different d_{min} values for a specific polynomial (0x1F29F in this case). Different polynomials will result in different values.

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

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

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 (spurious 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 spurious trips normally can be mitigated.

The design of a safety layer assuming a Pe of 10^{-4} is not recommended, as 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 all values up to 100 times higher Pe than 10^{-4}, that is 10^{-2}.

Therefore, unless a better lower bit error probability can be undeniably justified (beyond physical measurements on systems in actual installations and theoretical considerations based on arguments regarding the availability or long term stability of network connections), a maximum value of 10^{-2} shall be used for the bit error probability.

B.4 Cyclic redundancy checking

B.4.1 General

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

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

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.

NOTE For all i from 1 to (d_{min}-1), the value of A_i is equal to 0.

For a high bit error probability (close to 0,5), the worst case value for R_{CRC} is 2^{-r} for proper CRC polynomials (see for example [73]).

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.

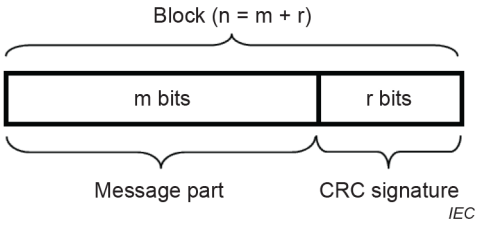


Figure B.3 – Example of a block with a message part and a CRC signature

B.4.2 Requirements for methods to calculate R_{CRC}

Various methods for calculating R_{CRC} have been provided in existing literature (for example [74], [76], [77], [78], [79], [80]). However, polynomial evaluations from published literature should be used with caution as some results have been questioned by subsequent analysis.

In addition, there are no known conservative approximation formulas, which would allow for a general calculation of R_{CRC}. Not even the "conservative" bound 2^{-r} is valid for all polynomials and all values of R_{CRC}.

NOTE 1 As a guidance for the calculation of R_{CRC}, Annex H provides numerical results which can be compared to the output values of algorithms in order to verify them.

Therefore, the R_{CRC} for the selected generator polynomial shall be explicitly calculated, as specified below.

- R_{CRC} shall be calculated for all values of n in use.

  NOTE 2 Calculating R_{CRC} e.g. for the longest telegram length is not sufficient. For example, the polynomial CCITT16 ($x^{16}+x^{12}+x^5+1$ or 0x11021) has a very high R_{CRC} for some small values of n.

  NOTE 3 If a polynomial is proper for a given data length n, it can still be improper for other data lengths (be it smaller or larger).

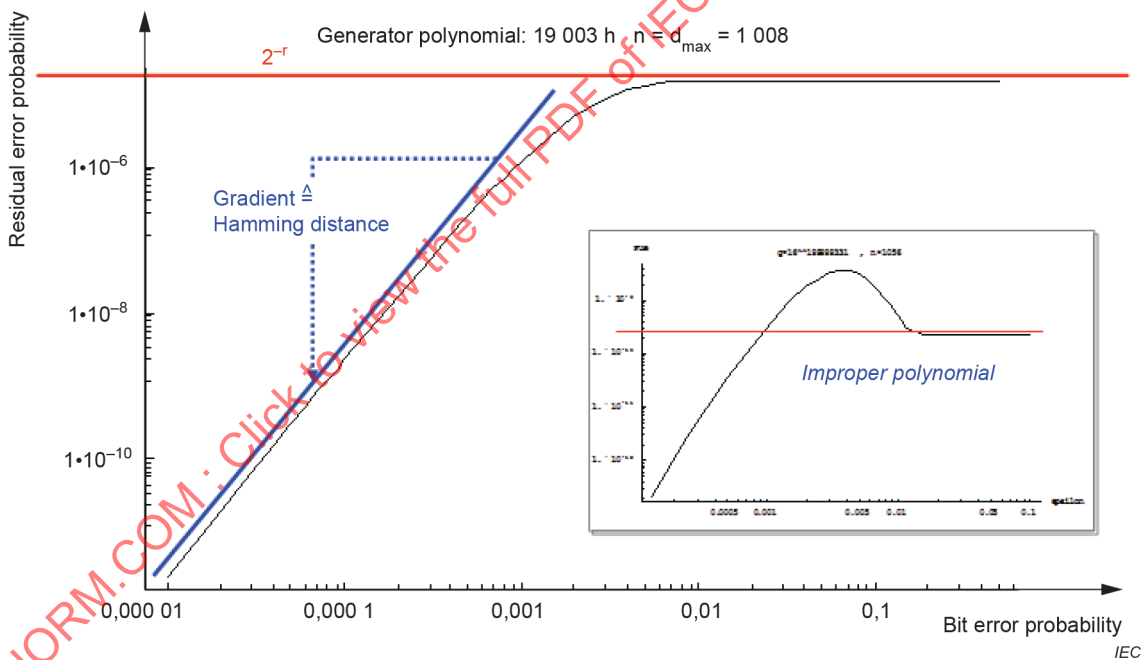
- R_{CRC} shall be calculated for all relevant values of P_e in the interval [2/n to 0,01].

  NOTE 4 In some cases, R_{CRC} does not grow monotonously with the P_e (so-called improper polynomials, see Figure B.4).

  NOTE 5 See [33] for a justification on using 2/n as the lowest P_e.

- Subsequently, it follows that:
  - if n<=200, it is sufficient to evaluate the single value P_e = 0,01;
  - if n>200, multiple values within this interval shall be evaluated (at least 2/n, 4/n, 8/n, 16/n, and so on until 0,01).

When choosing and implementing an algorithm for calculating R_{CRC}, numerical stability (for example ranges, precision, resolution, error propagation) shall be considered in order to avoid incorrect results. For instance, the subtraction of values of the same magnitude and the summation of many small values are problematic, when using floating point numbers.



Key

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

Figure B.4 – Proper and improper CRC polynomials

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

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

Annex C
(informative)

Structure of technology-specific parts

All technology-specific parts of IEC 61784-3 (all parts) 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

Clause and subclause No.	Title	Contents
5.5	Relationships with FAL (and DLL, PhL)	May include existing diagnostics, expected services, constraints (for example, "to be used in conjunction with FSCP x/y")
5.5.1	Data Types	List of the IEC 61158 data types used by the profile
6	Safety communication layer services	May include application objects used, diagnostic services
7	Safety communication layer protocol	First subclause is listed below, others may be added as needed. May include specific time mechanisms, state machines, sequence charts, reaction on power off/power down, diagnostic protocol and corresponding diagnosis
7.1	Safety PDU format	Includes detailed definition of safety PDU (message) formats. Will include several subclauses to specify the various format elements (for example safety CRC specification)
8	Safety communication layer management	Includes specifications for the following aspects of parameterization: – safe parameter data supplied by another safety device (for example a parameter server) – safe parameter data supplied by a tool (for example device description) (including any required measure to secure the storage, handling and transfer)
9	System requirements	First subclauses are listed below, others may be added as needed
9.1	Indicators and switches	Specifications for device indicators and switch function and behaviour
9.2	Installation guidelines	Detailed clause references within IEC 61918 or other relevant documents
9.3	Safety function response time	Calculations and related examples of reaction times relevant for the technology (for example worst case reaction time of safety loop)
9.4	Duration of demands	Specifications for the duration of demands within devices
9.5	Constraints for calculation of system characteristics	Includes black channel retries, number of telegrams 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

Clause and subclause No.	Title	Contents
Annex A (informative)	Additional information for functional safety communication profiles of CPF X	Mandatory informative annex used to provide additional non-normative information on the protocol. If there is none, then this will contain the following sentence: "There is no additional information for this FSCP".
A.1	Hash function calculation	For example, algorithms for CRC calculation
	Bibliography	Bibliographic references relevant for this part

Annex D
(informative)

Assessment guideline

D.1 Overview

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

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

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

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

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 3.1.4, 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 3.1.54, 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.