

INTERNATIONAL STANDARD

NORME INTERNATIONALE



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

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



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2021 IEC, Geneva, Switzerland

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

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'IEC ou du Comité national de l'IEC du pays du demandeur. Si vous avez des questions sur le copyright de l'IEC ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de l'IEC de votre pays de résidence.

IEC Central Office
3, rue de Varembe
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 It also gives information on projects, replaced and withdrawn publications.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 online collection - oc.iec.ch

Discover our powerful search engine and read freely all the publications previews. 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 22 000 terminological entries in English and French, with equivalent terms in 18 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

A propos de l'IEC

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

A propos des publications IEC

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

Recherche de publications IEC -

webstore.iec.ch/advsearchform

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

IEC Just Published - webstore.iec.ch/justpublished

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

Service Clients - webstore.iec.ch/csc

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

IEC online collection - oc.iec.ch

Découvrez notre puissant moteur de recherche et consultez gratuitement tous les aperçus des publications. Avec un abonnement, vous aurez toujours accès à un contenu à jour adapté à vos besoins.

Electropedia - www.electropedia.org

Le premier dictionnaire d'électrotechnologie en ligne au monde, avec plus de 22 000 articles terminologiques en anglais et en français, ainsi que les termes équivalents dans 16 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

INTERNATIONAL STANDARD

NORME INTERNATIONALE



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

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

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 25.040.40; 35.100.05

ISBN 978-2-8322-9268-6

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

CONTENTS

FOREWORD.....	7
0 Introduction	9
0.1 General.....	9
0.2 Use of extended assessment methods in Edition 4.....	11
0.3 Patent declaration.....	11
1 Scope	12
2 Normative references	12
3 Terms, definitions, symbols, abbreviated terms and conventions	14
3.1 Terms and definitions.....	14
3.2 Symbols and abbreviated terms	21
3.2.1 Abbreviated terms	21
3.2.2 Symbols	22
4 Conformance	22
5 Basics of safety-related fieldbus systems	23
5.1 Safety function decomposition	23
5.2 Communication system	23
5.2.1 General	23
5.2.2 IEC 61158 fieldbuses.....	24
5.2.3 Communication channel types	24
5.2.4 Safety function response time.....	25
5.3 Communication errors	25
5.3.1 General	25
5.3.2 Corruption	25
5.3.3 Unintended repetition	26
5.3.4 Incorrect sequence	26
5.3.5 Loss	26
5.3.6 Unacceptable delay	26
5.3.7 Insertion	26
5.3.8 Masquerade.....	26
5.3.9 Addressing	26
5.4 Deterministic remedial measures	27
5.4.1 General	27
5.4.2 Sequence number.....	27
5.4.3 Time stamp.....	27
5.4.4 Time expectation	27
5.4.5 Connection authentication	27
5.4.6 Feedback message.....	27
5.4.7 Data integrity assurance	27
5.4.8 Redundancy with cross checking	28
5.4.9 Different data integrity assurance systems.....	28
5.5 Typical relationships between errors and safety measures.....	28
5.6 Communication phases	29
5.7 FSCP implementation aspects	30
5.8 Models for estimation of the total residual error rate	30
5.8.1 Applicability	30
5.8.2 General models for black channel communications	31

5.8.3	Identification of generic safety properties.....	31
5.8.4	Assumptions for residual error rate calculations.....	32
5.8.5	Residual error rates	33
5.8.6	Data integrity	35
5.8.7	Authenticity.....	36
5.8.8	Timeliness	38
5.8.9	Masquerade.....	41
5.8.10	Calculation of the total residual error rates	41
5.8.11	Total residual error rate and SIL	43
5.8.12	Configuration and parameterization for an FSCP	43
5.9	Relationship between functional safety and security	45
5.10	Boundary conditions and constraints.....	45
5.10.1	Electrical safety	45
5.10.2	Electromagnetic compatibility (EMC)	46
5.11	Installation guidelines	46
5.12	Safety manual.....	46
5.13	Safety policy	46
6	Communication Profile Family 1 (FOUNDATION™ Fieldbus) – Profiles for functional safety	47
7	Communication Profile Family 2 (CIP™) and Family 16 (SERCOS®) – Profiles for functional safety	47
8	Communication Profile Family 3 (PROFIBUS™, PROFINET™) – Profiles for functional safety	48
9	Communication Profile Family 6 (INTERBUS®) – Profiles for functional safety	48
10	Communication Profile Family 8 (CC-Link™) – Profiles for functional safety	49
10.1	Functional Safety Communication Profile 8/1	49
10.2	Functional Safety Communication Profile 8/2	49
11	Communication Profile Family 12 (EtherCAT™) – Profiles for functional safety.....	49
12	Communication Profile Family 13 (Ethernet POWERLINK™) – Profiles for functional safety	50
13	Communication Profile Family 14 (EPA®) – Profiles for functional safety.....	50
14	Communication Profile Family 17 (RAPIEnet™) – Profiles for functional safety.....	50
15	Communication Profile Family 18 (SafetyNET p™ Fieldbus) – Profiles for functional safety	51
Annex A (informative)	Example functional safety communication models	52
A.1	General.....	52
A.2	Model A (single message, channel and FAL, redundant SCLs).....	52
A.3	Model B (full redundancy)	52
A.4	Model C (redundant messages, FALs and SCLs, single channel)	53
A.5	Model D (redundant messages and SCLs, single channel and FAL)	53
Annex B (normative)	Safety communication channel model using CRC-based error checking	55
B.1	Overview.....	55
B.2	Channel model for calculations	55
B.3	Bit error probability P_e	56
B.4	Cyclic redundancy checking	57
B.4.1	General	57
B.4.2	Requirements for methods to calculate R_{CRC}	57
Annex C (informative)	Structure of technology-specific parts.....	59

Annex D (informative) Assessment guideline	62
D.1 Overview.....	62
D.2 Channel types.....	62
D.2.1 General	62
D.2.2 Black channel	62
D.2.3 White channel.....	62
D.3 Data integrity considerations for white channel approaches	63
D.3.1 General	63
D.3.2 Models B and C	63
D.3.3 Models A and D	64
D.4 Verification of safety measures	64
D.4.1 General	64
D.4.2 Implementation.....	65
D.4.3 Default safety action	65
D.4.4 Safe state	65
D.4.5 Transmission errors	65
D.4.6 Safety reaction and response times	65
D.4.7 Combination of measures	65
D.4.8 Absence of interference	66
D.4.9 Additional fault causes (white channel)	66
D.4.10 Reference test beds and operational conditions	66
D.4.11 Conformance tester	66
Annex E (informative) Examples of implicit vs. explicit FSCP safety measures.....	67
E.1 General.....	67
E.2 Example fieldbus message with safety PDUs	67
E.3 Model with completely explicit safety measures	67
E.4 Model with explicit A-code and implicit T-code safety measures.....	68
E.5 Model with explicit T-code and implicit A-code safety measures.....	68
E.6 Model with split explicit and implicit safety measures	69
E.7 Model with completely implicit safety measures	70
E.8 Addition to Annex B – impact of implicit codes on properness	70
Annex F (informative) Legacy models for estimation of the total residual error rate	71
F.1 General.....	71
F.2 Calculation of the residual error rate	71
F.3 Total residual error rate and SIL	73
Annex G (informative) Implicit data safety mechanisms for IEC 61784-3 functional safety communication profiles (FSCPs).....	74
G.1 Overview.....	74
G.2 Basic principles.....	74
G.3 Problem statement: constant values for implicit data	75
G.4 RP for FSCPs with random, uniformly distributed err_{impl}	78
G.4.1 General	78
G.4.2 Uniform distribution within the interval $[0;2^i-1]$, $i \geq r$	79
G.4.3 Uniform distribution in the interval $[1;2^r-1]$, $i = r$	81
G.5 General case	83
G.6 Calculation of P_{ID}	83
Annex H (informative) Residual error probability for example CRC codes (tables for verification of calculation methods)	85
H.1 Overview.....	85

H.2	Example of a 32-bit CRC.....	85
H.3	Example of a 16-bit CRC.....	90
H.4	Conclusion.....	94
	Bibliography.....	96
	Figure 1 – Relationships of IEC 61784-3 with other standards (machinery).....	9
	Figure 2 – Relationships of IEC 61784-3 with other standards (process).....	10
	Figure 3 – Transitions from Ed. 2 to Ed. 4 and future Ed. 5 assessment methods	11
	Figure 4 – Safety communication as a part of a safety function	23
	Figure 5 – Example model of a functional safety communication system	24
	Figure 6 – Example of safety function response time components.....	25
	Figure 7 – Conceptual FSCP protocol model.....	30
	Figure 8 – FSCP implementation aspects.....	30
	Figure 9 – Black channel from an FSCP perspective	31
	Figure 10 – Model for authentication considerations	36
	Figure 11 – Fieldbus and internal address errors	37
	Figure 12 – Example of slowly increasing message latency	39
	Figure 13 – Example of an active network element failure.....	40
	Figure 14 – Example application 1 ($m = 4$).....	42
	Figure 15 – Example application 2 ($m = 2$).....	42
	Figure 16 – Example of configuration and parameterization procedures for FSCP.....	44
	Figure A.1 – Model A	52
	Figure A.2 – Model B	53
	Figure A.3 – Model C	53
	Figure A.4 – Model D	54
	Figure B.1 – Binary symmetric channel (BSC).....	55
	Figure B.2 – Block codes for error detection	56
	Figure B.3 – Example of a block with a message part and a CRC signature	57
	Figure B.4 – Proper and improper CRC polynomials	58
	Figure D.1 – Basic Markov model	64
	Figure E.1 – Example safety PDUs embedded in a fieldbus message	67
	Figure E.2 – Model with completely explicit safety measures	67
	Figure E.3 – Model with explicit A-code and implicit T-code safety measures.....	68
	Figure E.4 – Model with explicit T-code and implicit A-code safety measures.....	69
	Figure E.5 – Model with split explicit and implicit safety measures	69
	Figure E.6 – Model with completely implicit safety measures	70
	Figure F.1 – Example application 1 ($m = 4$).....	72
	Figure F.2 – Example application 2 ($m = 2$).....	73
	Figure G.1 – FSCP with implicit transmission of authenticity and/or timeliness codes	75
	Figure G.2 – Example of an incorrect transmission with multiple error causes.....	76
	Figure G.3 – Impact of errors in implicit data on the residual error probability	77
	Figure H.1 – Residual error probabilities (example of a 32-bit CRC – result 1).....	87
	Figure H.2 – Residual error probabilities (example of a 32-bit CRC – result 2).....	87

Figure H.3 – Residual error probabilities (example of a 32-bit CRC – result 3)	88
Figure H.4 – Residual error probabilities (example of a 32-bit CRC – result 4)	88
Figure H.5 – Residual error probabilities (example of a 32-bit CRC – result 5)	89
Figure H.6 – Residual error probabilities (example of a 32-bit CRC – result 6)	89
Figure H.7 – Residual error probabilities (example of a 16-bit CRC – result 1)	92
Figure H.8 – Residual error probabilities (example of a 16-bit CRC – result 2)	92
Figure H.9 – Residual error probabilities (example of a 16-bit CRC – result 3)	93
Figure H.10 – Residual error probabilities (example of a 16-bit CRC – result 4)	93
Figure H.11 – Residual error probabilities (example of a 16-bit CRC – result 5)	94
Figure H.12 – Example 1 of improper polynomial	94
Figure H.13 – Example 2 of improper polynomial	95
Table 1 – Overview of the effectiveness of the various measures on the possible errors	29
Table 2 – Typical relationship of residual error rate to SIL	43
Table 3 – Typical relationship of residual error on demand to SIL	43
Table 4 – Overview of profile identifier usable for FSCP 6/7	48
Table B.1 – Example dependency $d_{\min}$ and block bit length n	56
Table C.1 – Common subclause structure for technology-specific parts	59
Table F.1 – Definition of items used for calculation of the residual error rates	72
Table F.2 – Typical relationship of residual error rate to SIL	73
Table F.3 – Typical relationship of residual error on demand to SIL	73
Table H.1 – Residual error probabilities (R_{CRC1}) for example CRC32 polynomial	86
Table H.2 – Residual error probabilities (R_{CRC2}) for example CRC16 polynomial	91

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) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

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 cancels and replaces the third edition, published in 2016 and its Amendment 1, published in 2017. This 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 R_{CRC} .

The text of this International Standard is based on the following documents:

FDIS	Report on voting
65C/1067/FDIS	65C/1072/RVD

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

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 will remain unchanged until the stability date indicated on the IEC website under "<http://webstore.iec.ch>" in the data related to the specific document. At this date, the document will be

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

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

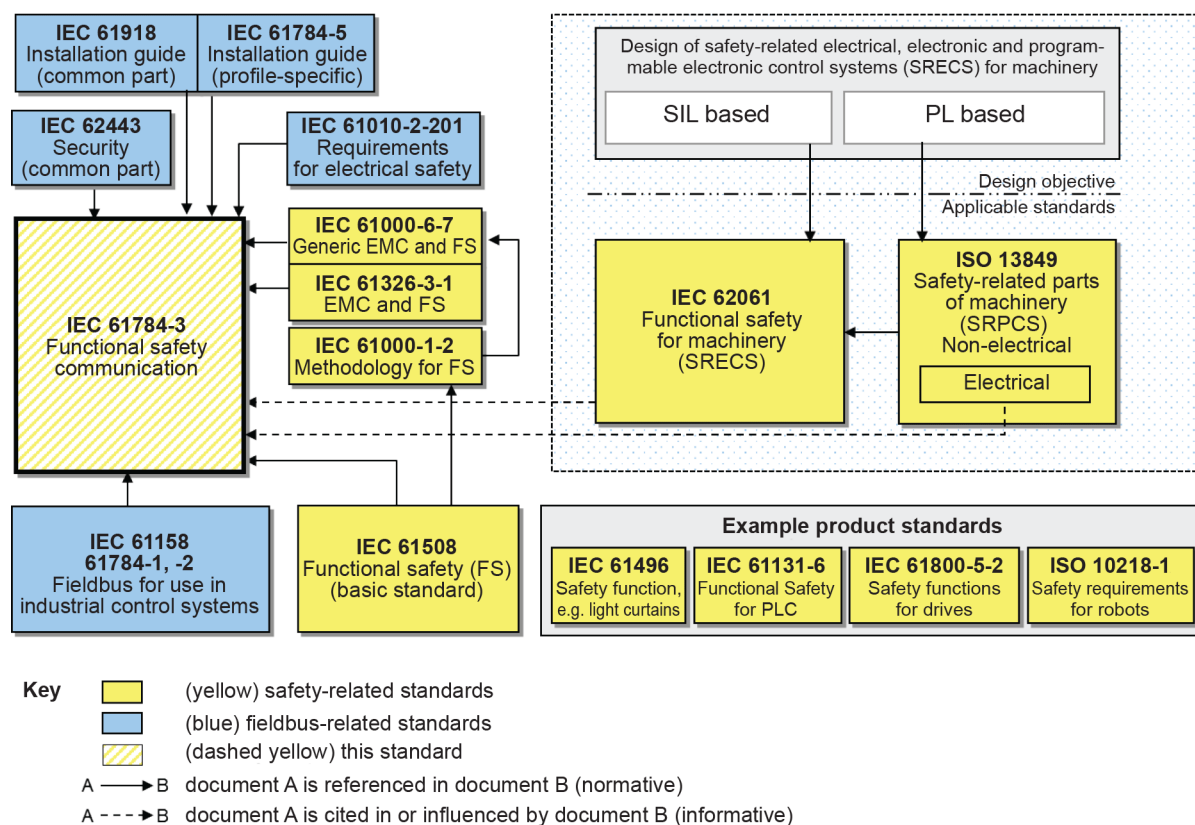
0 Introduction

0.1 General

The IEC 61158 (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.

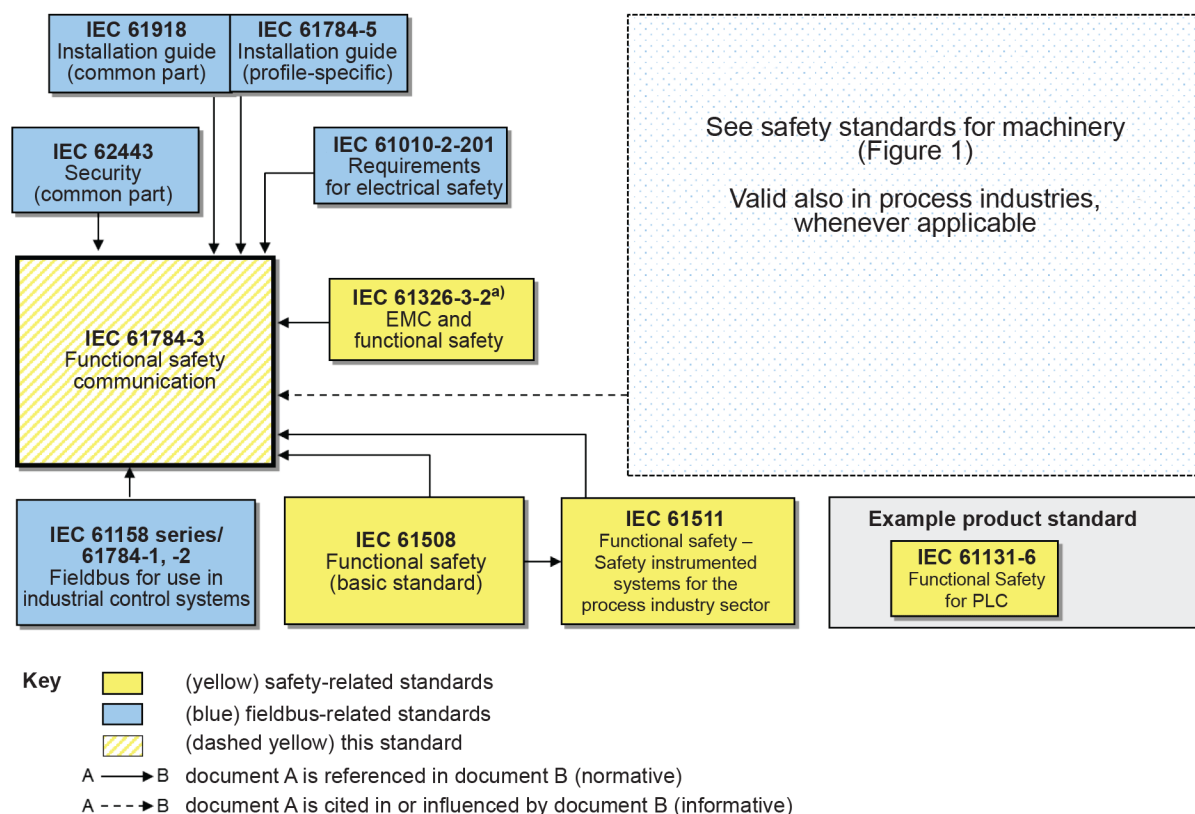


IEC

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.



IEC

^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:

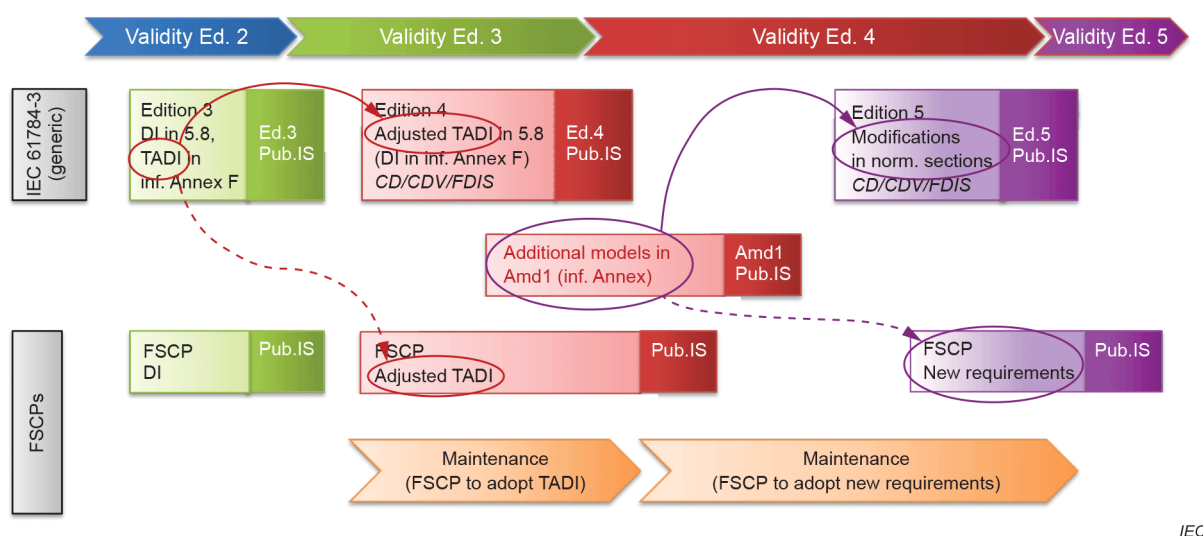
- basic principles for implementing the requirements of IEC 61508 (all parts) for safety-related data communications, including possible transmission faults, remedial measures and considerations affecting data integrity;
- functional safety communication profiles for several communication profile families 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.



IEC

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.

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

P_e

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.

3.2 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	

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).

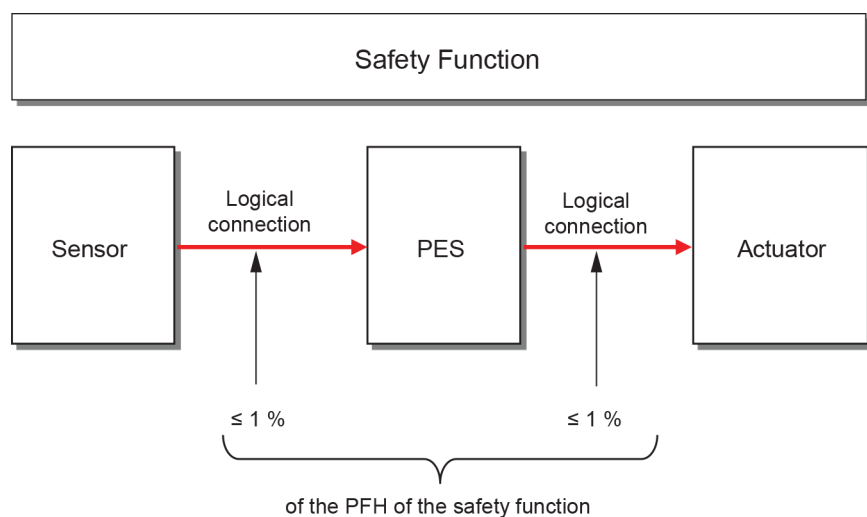
5 Basics of safety-related fieldbus systems

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.



IEC

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.

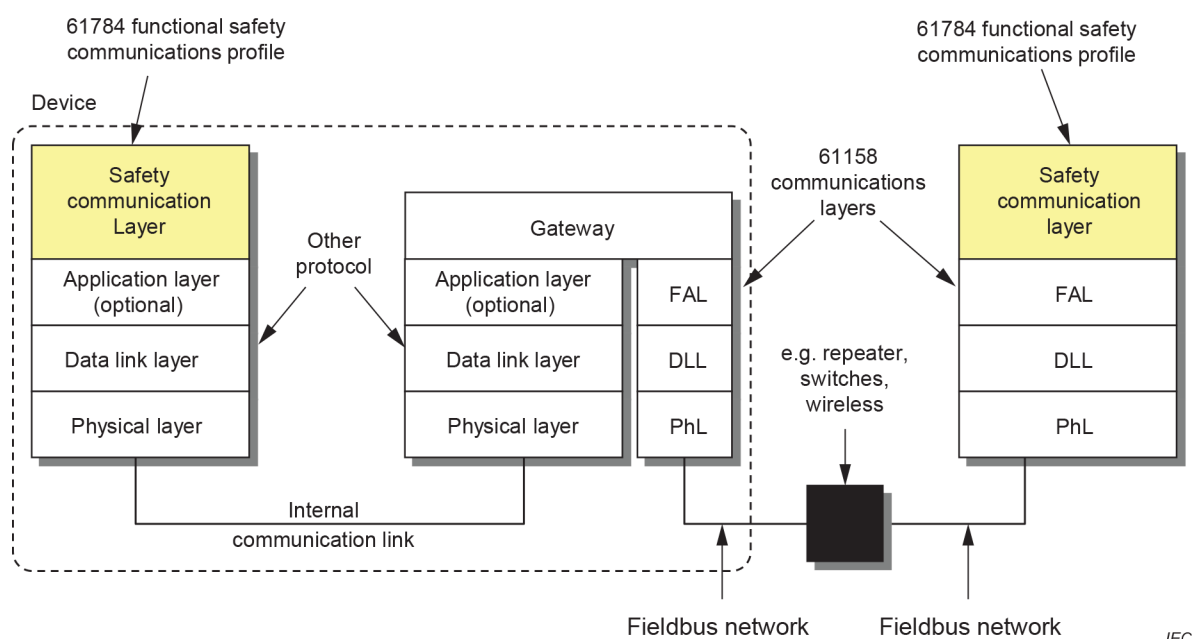


Figure 5 – Example model of a functional safety communication system

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.

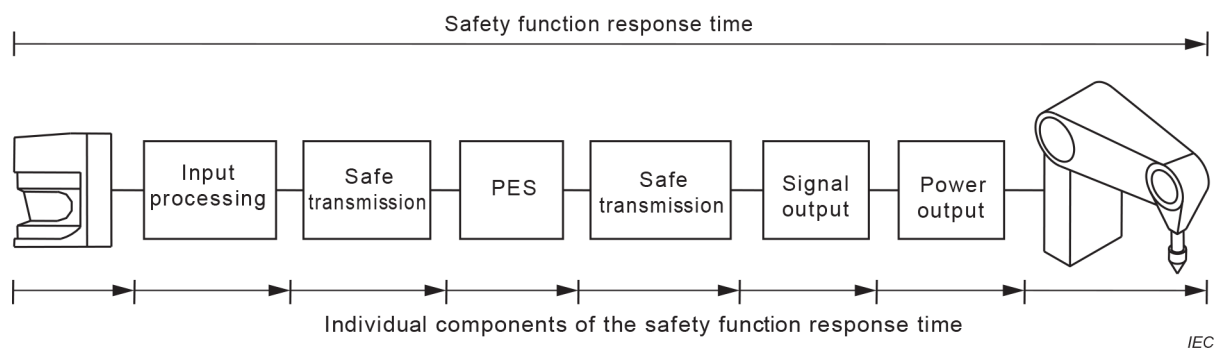


Figure 6 – Example of safety function response time components

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

5.4.2 Sequence number

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

5.4.3 Time stamp

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

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

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

5.4.4 Time expectation

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

EXAMPLE

Time-slot-oriented access method:

- the exchange of messages takes place within fixed cycles and predetermined time slots for every participant;
- optionally, every participant sends his data within its time slot even if there is no value change (this is an example of cyclic communication);
- to identify a participant who did not transmit within its associated time slot, a source identification is added.

5.4.5 Connection authentication

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

5.4.6 Feedback message

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

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

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

5.4.7 Data integrity assurance

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

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

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

5.4.8 Redundancy with cross checking

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

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

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

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

5.4.9 Different data integrity assurance systems

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

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

5.5 Typical relationships between errors and safety measures

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

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

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

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

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

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

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

^b Required in all cases.

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

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

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

5.6 Communication phases

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

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

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

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

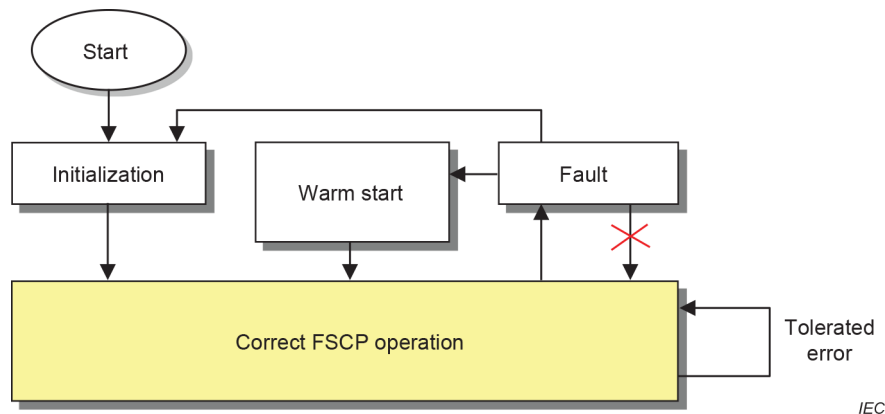


Figure 7 – Conceptual FSCP protocol model

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).

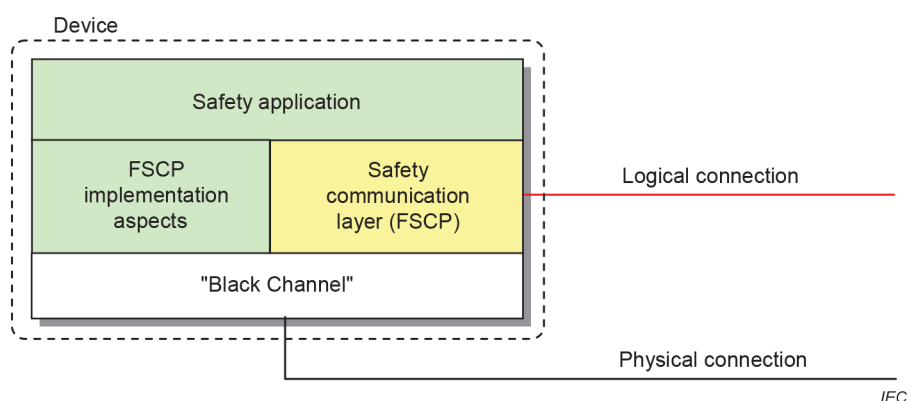


Figure 8 – FSCP implementation aspects

5.8 Models for estimation of the total residual error rate

5.8.1 Applicability

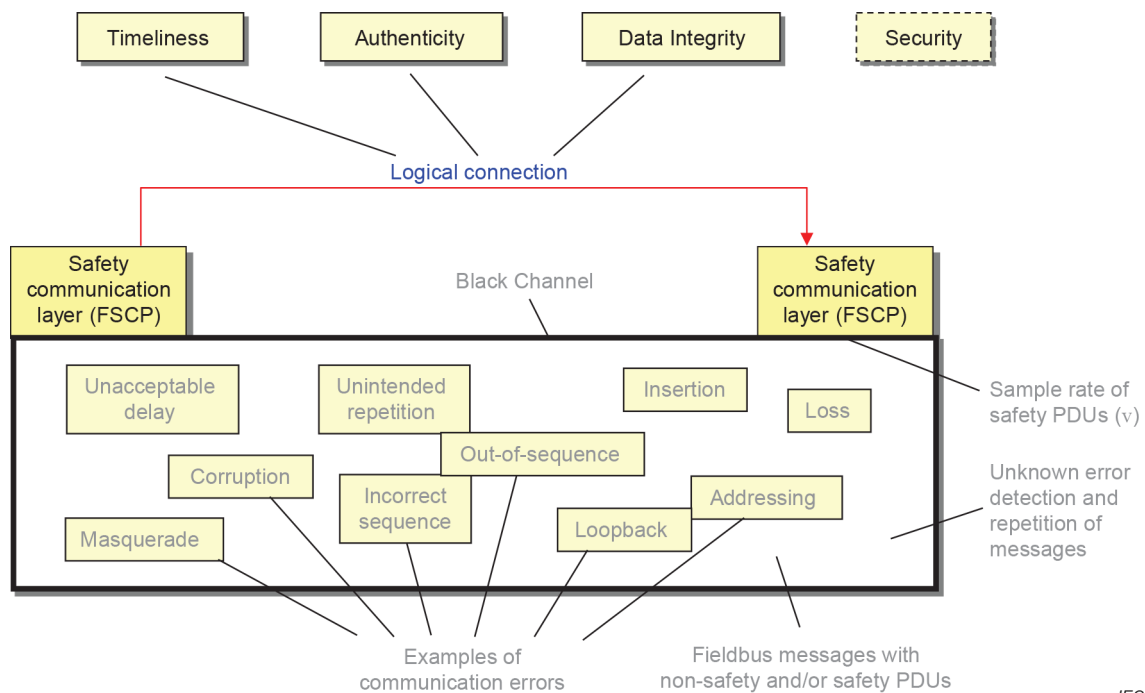
Subclause 5.8 specifies models for estimating the total residual error rate for an FSCP, for the purpose of assessing this FSCP.

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.



IEC

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).

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

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 ($i = 1 \dots N$);
- V_{Ri} is the number of values representing the total range for data field i ($i = 1 \dots N$).

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.

5.8.7 Authenticity

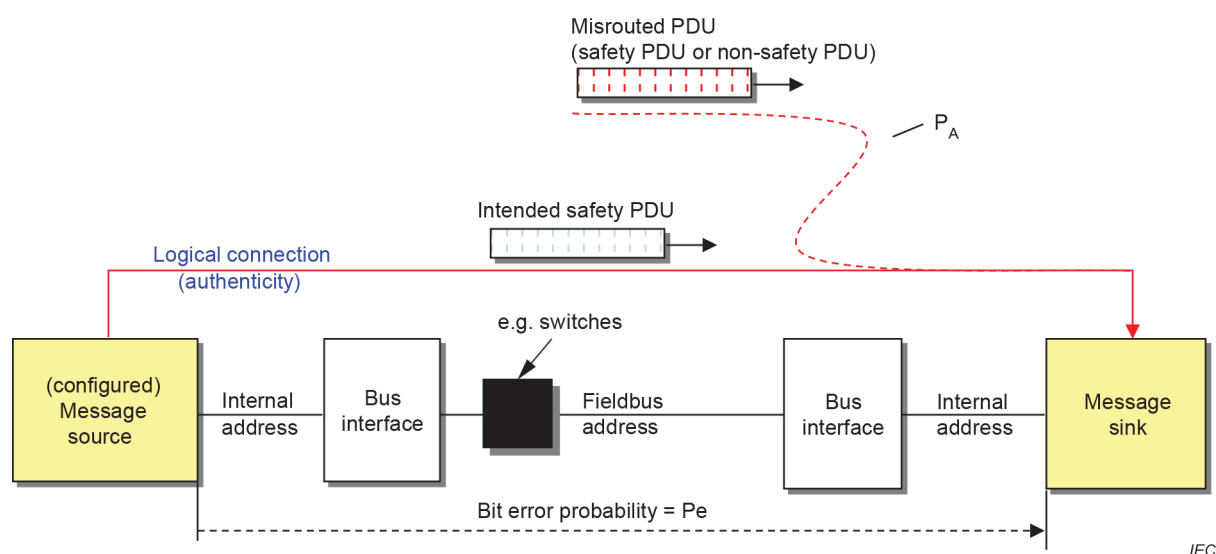
5.8.7.1 General

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).

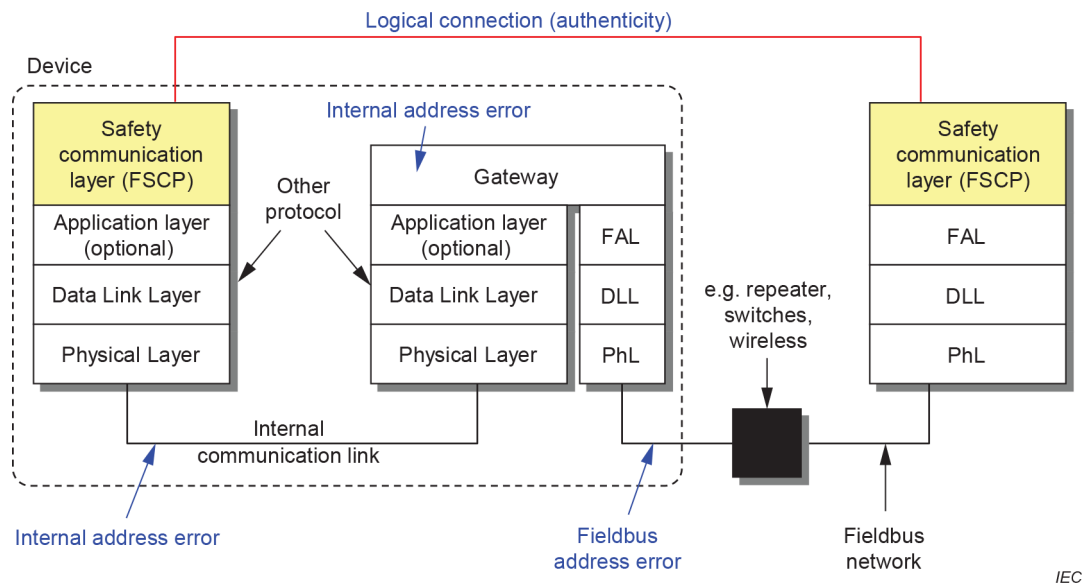


Figure 11 – Fieldbus and internal address errors

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.

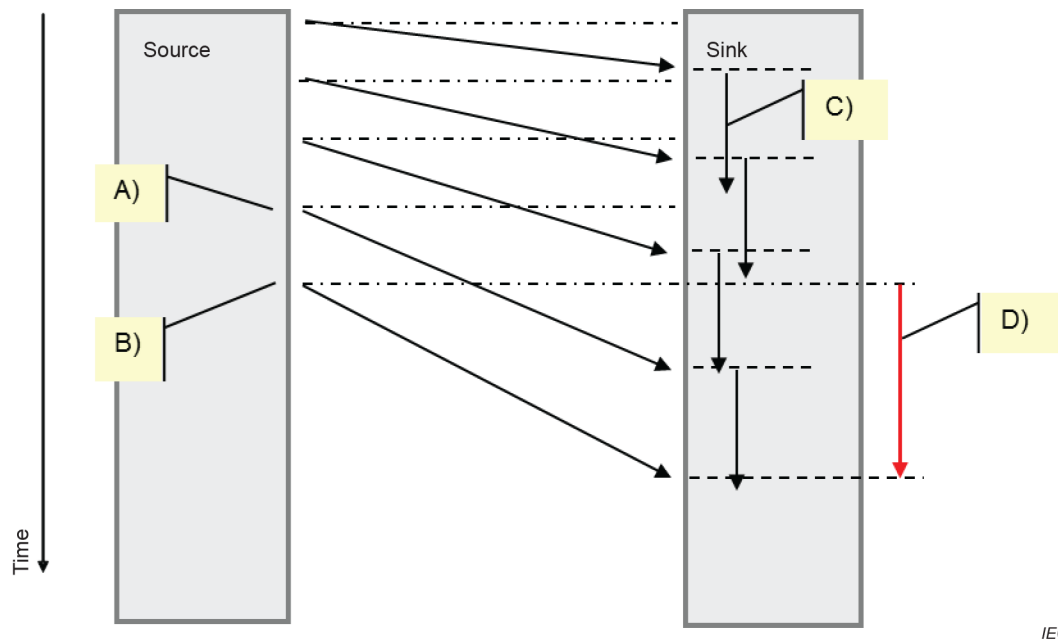
Typical causes for non-timely communication which shall be considered during the design of the FSCP are variable performances of the black channel.

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.



IEC

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.

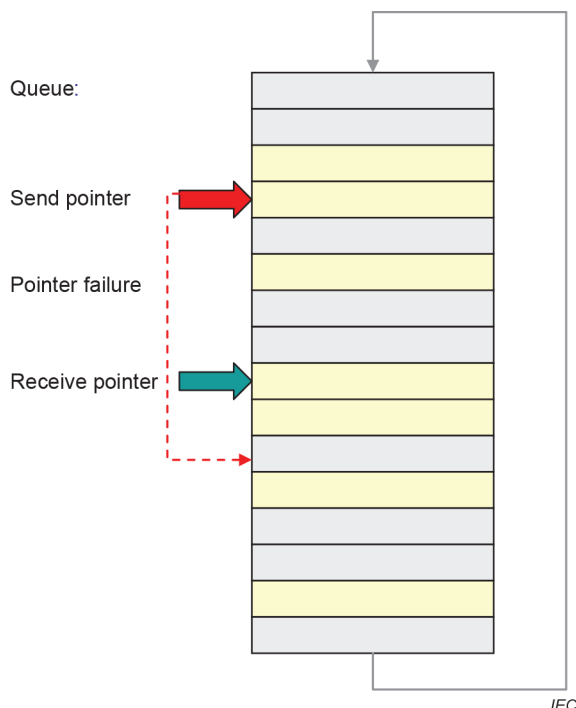


Figure 13 – Example of an active network element failure

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.

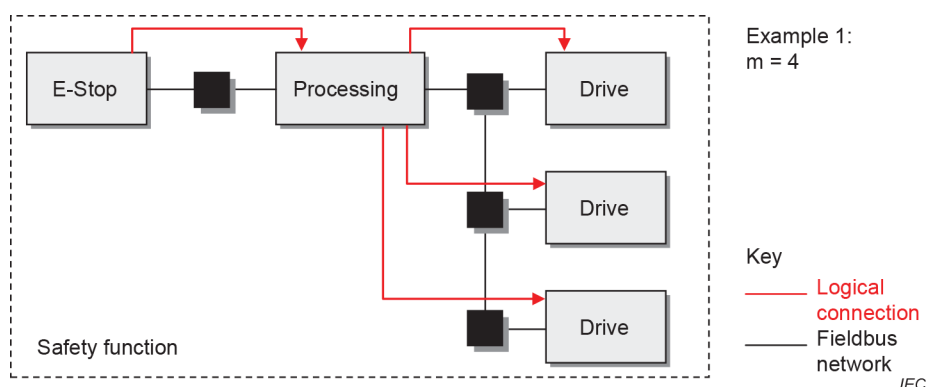


Figure 14 – Example application 1 ($m = 4$)

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.

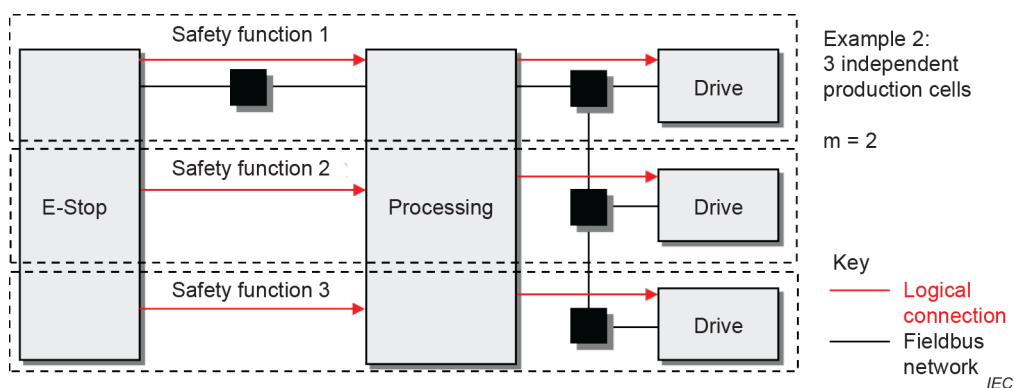


Figure 15 – Example application 2 ($m = 2$)

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.

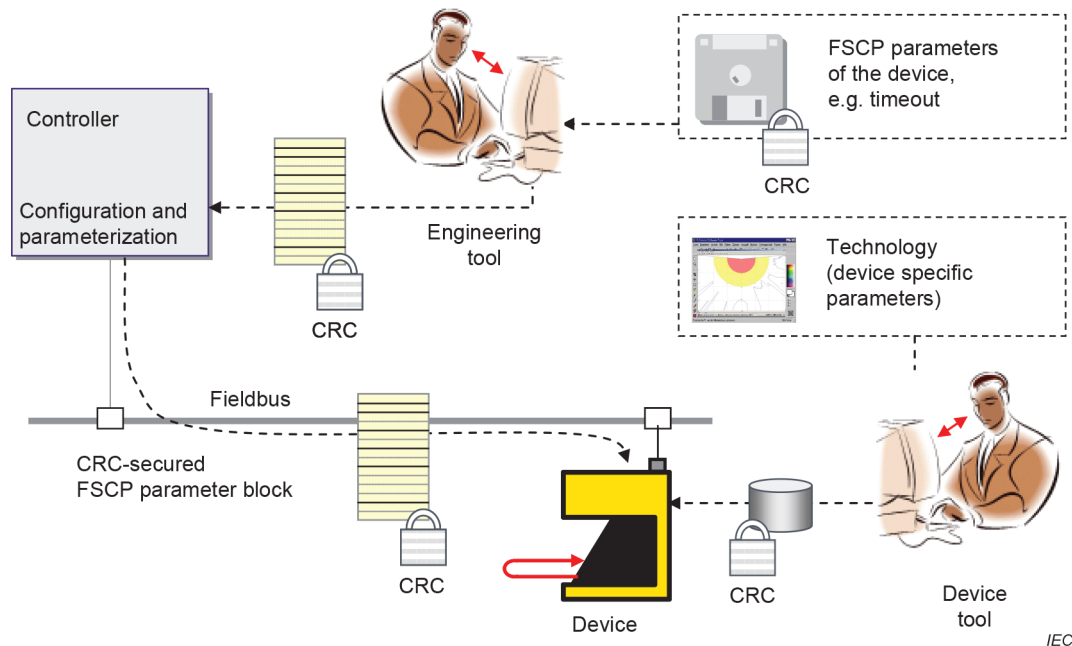


Figure 16 – Example of configuration and parameterization procedures for FSCP

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 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 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.

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™ Fieldbus³) 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.

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).

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.

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.

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).

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).