

INTERNATIONAL STANDARD



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

Withhold



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2016 IEC, Geneva, Switzerland

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

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

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

About the IEC

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

About IEC publications

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

IEC Catalogue - webstore.iec.ch/catalogue

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

IEC publications search - www.iec.ch/searchpub

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 It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

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

Electropedia - www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing 20 000 terms and definitions in English and French, with equivalent terms in 15 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary

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

IEC Customer Service Centre - webstore.iec.ch/csc

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

INTERNATIONAL STANDARD



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

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 25.040.40; 35.100.05

ISBN 978-2-8322-3372-6

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

CONTENTS

FOREWORD.....	8
0 Introduction	10
0.1 General.....	10
0.2 Transition from Edition 2 to extended assessment methods in Edition 3.....	12
0.3 Patent declaration	12
1 Scope.....	14
2 Normative references.....	14
3 Terms, definitions, symbols, abbreviated terms and conventions.....	16
3.1 Terms and definitions	16
3.1.1 Common terms and definitions	
3.1.2 CPF 1: Additional terms and definitions	
3.1.3 CPF 2: Additional terms and definitions	
3.1.4 CPF 3: Additional terms and definitions	
3.1.5 CPF 6: Additional terms and definitions	
3.1.6 CPF 8: Additional terms and definitions	
3.1.7 CPF 12: Additional terms and definitions	
3.1.8 CPF 13: Additional terms and definitions	
3.1.9 CPF 14: Additional terms and definitions	
3.2 Symbols and abbreviated terms.....	24
3.2.1 Common symbols and abbreviated terms.....	
3.2.2 CPF 1: Additional symbols and abbreviated terms.....	
3.2.3 CPF 2: Additional symbols and abbreviated terms.....	
3.2.4 CPF 3: Additional symbols and abbreviated terms.....	
3.2.5 CPF 6: Additional symbols and abbreviated terms.....	
3.2.6 CPF 8: Additional symbols and abbreviated terms.....	
3.2.7 CPF 12: Additional symbols and abbreviated terms.....	
3.2.8 CPF 13: Additional symbols and abbreviated terms.....	
3.2.9 CPF 14: Additional symbols and abbreviated terms.....	
4 Conformance.....	26
5 Basics of safety-related fieldbus systems	26
5.1 Safety function decomposition	26
5.2 Communication system	27
5.2.1 General	27
5.2.2 IEC 61158 fieldbuses	27
5.2.3 Communication channel types	28
5.2.4 Safety function response time	28
5.3 Communication errors	29
5.3.1 General	29
5.3.2 Corruption.....	29
5.3.3 Unintended repetition	29
5.3.4 Incorrect sequence	30
5.3.5 Loss	30
5.3.6 Unacceptable delay.....	30
5.3.7 Insertion	30
5.3.8 Masquerade.....	30
5.3.9 Addressing.....	30

5.4	Deterministic remedial measures	31
5.4.1	General	31
5.4.2	Sequence number	31
5.4.3	Time stamp	31
5.4.4	Time expectation	31
5.4.5	Connection authentication	31
5.4.6	Feedback message	31
5.4.7	Data integrity assurance	32
5.4.8	Redundancy with cross checking	32
5.4.9	Different data integrity assurance systems	32
5.5	Typical relationships between errors and safety measures	32
5.6	Communication phases	33
5.7	FSCP implementation aspects	34
5.8	Data integrity considerations	34
5.8.1	Calculation of the residual error rate	34
5.8.2	Total residual error rate and SIL	37
5.9	Relationship between functional safety and security	38
5.10	Boundary conditions and constraints	39
5.10.1	Electrical safety	39
5.10.2	Electromagnetic compatibility (EMC)	39
5.11	Installation guidelines	40
5.12	Safety manual	40
5.13	Safety policy	40
6	Communication Profile Family 1 (FOUNDATION™ Fieldbus) – Profiles for functional safety	41
6.1	Functional Safety Communication Profile 1/1	
6.2	Technical overview	
7	Communication Profile Family 2 (CIP™) and Family 16 (SERCOS®) – Profiles for functional safety	42
7.1	Functional Safety Communication Profile 2/1	
7.2	Technical overview	
8	Communication Profile Family 3 (PROFIBUS™, PROFINET™) – Profiles for functional safety	44
8.1	Functional Safety Communication Profile 3/1	
8.2	Technical overview	
9	Communication Profile Family 6 (INTERBUS®) – Profiles for functional safety	46
9.1	Functional Safety Communication Profile 6/7	
9.2	Technical overview	
10	Communication Profile Family 8 (CC-Link™) – Profiles for functional safety	48
10.1	Functional Safety Communication Profile 8/1	48
10.2	Technical overview Functional Safety Communication Profile 8/2	48
11	Communication Profile Family 12 (EtherCAT™) – Profiles for functional safety	49
11.1	Functional Safety Communication Profile 12/1	
11.2	Technical overview	
12	Communication Profile Family 13 (Ethernet POWERLINK™) – Profiles for functional safety	50
12.1	Functional Safety Communication Profile 13/1	
12.2	Technical overview	

13	Communication Profile Family 14 (EPA®) – Profiles for functional safety	52
13.1	~~Functional Safety Communication Profile 14/1~~	~~52~~
13.2	~~Technical overview~~	~~52~~
14	Communication Profile Family 17 (RAPIEnet™) – Profiles for functional safety	53
15	Communication Profile Family 18 (SafetyNET p™ Fieldbus) – Profiles for functional safety	53
Annex A	(informative) Example functional safety communication models	54
A.1	General	54
A.2	Model A (single message, channel and FAL, redundant SCLs)	54
A.3	Model B (full redundancy)	54
A.4	Model C (redundant messages, FALs and SCLs, single channel)	55
A.5	Model D (redundant messages and SCLs, single channel and FAL)	55
Annex B	(~~informative~~ normative) Safety communication channel model using CRC-based error checking	57
B.1	Overview	57
B.2	Channel model for calculations	57
B.3	Bit error probability P_e	58
B.4	Cyclic redundancy checking	59
B.4.1	General	59
B.4.2	Considerations concerning CRC polynomials	60
Annex C	(informative) Structure of technology-specific parts	62
Annex D	(informative) Assessment guideline	64
D.1	Overview	64
D.2	Channel types	64
D.2.1	General	64
D.2.2	Black channel	64
D.2.3	White channel	64
D.3	Data integrity considerations for white channel approaches	65
D.3.1	General	65
D.3.2	Models B and C	65
D.3.3	Models A and D	66
D.4	Verification of safety measures	67
D.4.1	General	67
D.4.2	Implementation	67
D.4.3	"De-energize to trip" principle	67
D.4.4	Safe state	67
D.4.5	Transmission errors	67
D.4.6	Safety reaction and response times	67
D.4.7	Combination of measures	68
D.4.8	Absence of interference	68
D.4.9	Additional fault causes (white channel)	68
D.4.10	Reference test beds and operational conditions	68
D.4.11	Conformance tester	69
Annex E	(informative) Examples of implicit vs. explicit FSCP safety measures	70
E.1	General	70
E.2	Example fieldbus message with safety PDUs	70
E.3	Model with completely explicit safety measures	70
E.4	Model with explicit A-code and implicit T-code safety measures	71

E.5	Model with explicit T-code and implicit A-code safety measures	71
E.6	Model with split explicit and implicit safety measures	72
E.7	Model with completely implicit safety measures	73
E.8	Addition to Annex B – impact of implicit codes on properness	73
Annex F (informative)	Extended models for estimation of the total residual error rate	74
F.1	Applicability	74
F.2	General models for black channel communications	74
F.3	Identification of generic safety properties	75
F.4	Assumptions for residual error rate calculations	75
F.5	Residual error rates	76
F.5.1	Explicit and implicit mechanisms	76
F.5.2	Residual error rate calculations	76
F.6	Data integrity	78
F.6.1	Probabilistic considerations	78
F.6.2	Deterministic considerations	78
F.7	Authenticity	79
F.7.1	General	79
F.7.2	Residual error rate for authenticity (RR_A)	80
F.8	Timeliness	81
F.8.1	General	81
F.8.2	Residual error rate for timeliness (RR_T)	83
F.9	Masquerade	84
F.9.1	General	84
F.9.2	Other terms used to calculate residual error rate for masquerade rejection (RR_M)	84
F.10	Calculation of the total residual error rates	84
F.10.1	Based on the summation of the residual error rates	84
F.10.2	Based on other quantitative proofs	85
F.11	Total residual error rate and SIL	85
F.12	Configuration and parameterization for an FSCP	86
F.12.1	General	86
F.12.2	Configuration and parameterization change rate	88
F.12.3	Residual error rate for configuration and parameterization	88
Bibliography		89
Figure 1	– Relationships of IEC 61784-3 with other standards (machinery)	10
Figure 2	– Relationships of IEC 61784-3 with other standards (process)	11
Figure 3	– Transition from Edition 2 to Edition 3 assessment methods	12
Figure 4	– Safety communication as a part of a safety function	27
Figure 5	– Example model of a functional safety communication system	28
Figure 6	– Example of safety function response time components	29
Figure 7	– ~~Scope of FSCP 1/1~~	34
Figure 7	– Conceptual FSCP protocol model	34
Figure 8	– ~~Relationship of Safety Validators~~	34
Figure 8	– FSCP implementation aspects	34
Figure 9	– ~~Basic communication preconditions for FSCP 3/1~~	34

Figure 9 – Example application 1 (m=4)	36
~~Figure 10 – Structure of a FSCP 3/1 safety PDU~~	
Figure 10 – Example application 2 (m = 2)	37
~~Figure 11 – Safe communication modes~~	
Figure 11 – Zones and conduits concept for security according to IEC 62443	39
~~Figure 12 – FSCP 6/7 communication preconditions~~	
~~Figure 13 – Basic FSCP 12/1 system~~	
~~Figure 14 – Producer consumer example~~	
~~Figure 15 – Client server example~~	
~~Figure 16 – FSCP 14/1 safety communication architecture~~	
Figure A.1 – Model A	54
Figure A.2 – Model B	55
Figure A.3 – Model C	55
Figure A.4 – Model D	56
Figure B.1 – Communication channel with perturbation	57
Figure B.2 – Binary symmetric channel (BSC)	58
Figure B.3 – Example of a block with a message part and a CRC bits (redundancy code) signature	59
Figure B.4 – Block codes for error detection	60
Figure B.5 – Proper and improper CRC polynomials	61
Figure D.1 – Basic Markov model	66
Figure E.1 – Example safety PDUs embedded in a fieldbus message	70
Figure E.2 – Model with completely explicit safety measures	70
Figure E.3 – Model with explicit A-code and implicit T-code safety measures	71
Figure E.4 – Model with explicit T-code and implicit A-code safety measures	72
Figure E.5 – Model with split explicit and implicit safety measures	72
Figure E.6 – Model with completely implicit safety measures	73
Figure F.1 – Black channel from an FSCP perspective	74
Figure F.2 – Model for authentication considerations	79
Figure F.3 – Fieldbus and internal address errors	80
Figure F.4 – Example of slowly increasing message latency	82
Figure F.5 – Example of an active network element failure	83
Figure F.6 – Example application 1 (m = 4)	85
Figure F.7 – Example application 2 (m = 2)	85
Figure F.8 – Example of configuration and parameterization procedures for FSCP	87
Table 1 – Overview of the effectiveness of the various measures on the possible errors	33
Table 2 – Definition of items used for calculation of the residual error rates	36
Table 3 – Typical relationship of residual error rate to SIL level	37
Table 4 – Typical relationship of residual error on demand to SIL	37
Table 5 – Overview of profile identifier usable for FSCP 6/7	47
Table B.1 – Example dependency $d_{\min}$ and block bit length n	60
Table C.1 – Common subclause structure for technology-specific parts	62

Table F.1 – Typical relationship of residual error rate to SIL	86
Table F.2 – Typical relationship of residual error on demand to SIL.....	86

Withdrawn

INTERNATIONAL ELECTROTECHNICAL COMMISSION

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES –

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

FOREWORD

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

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

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

This third edition cancels and replaces the second edition published in 2010. This edition constitutes a technical revision.

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

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

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

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

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

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

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

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

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

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

0.1 General

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

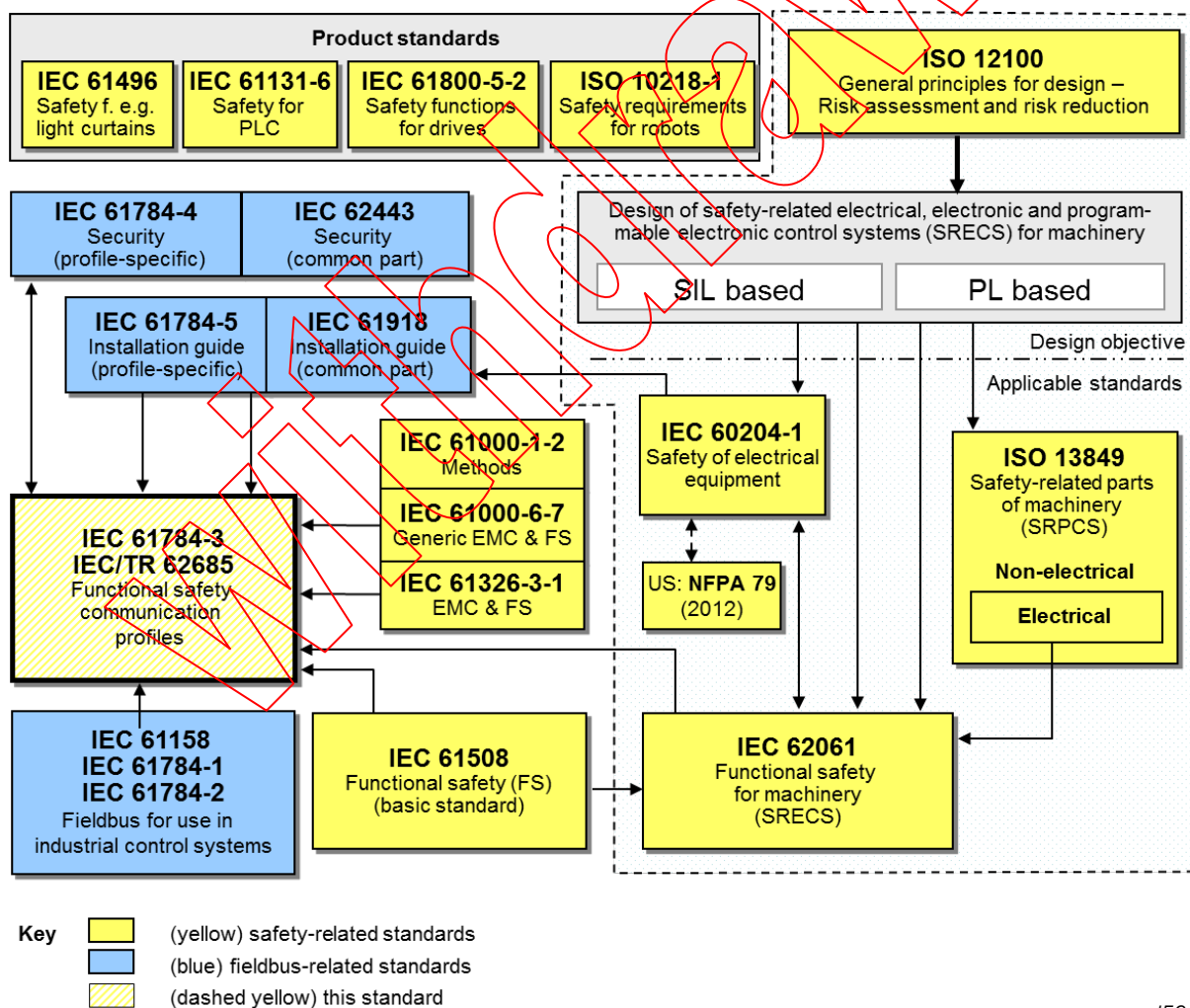
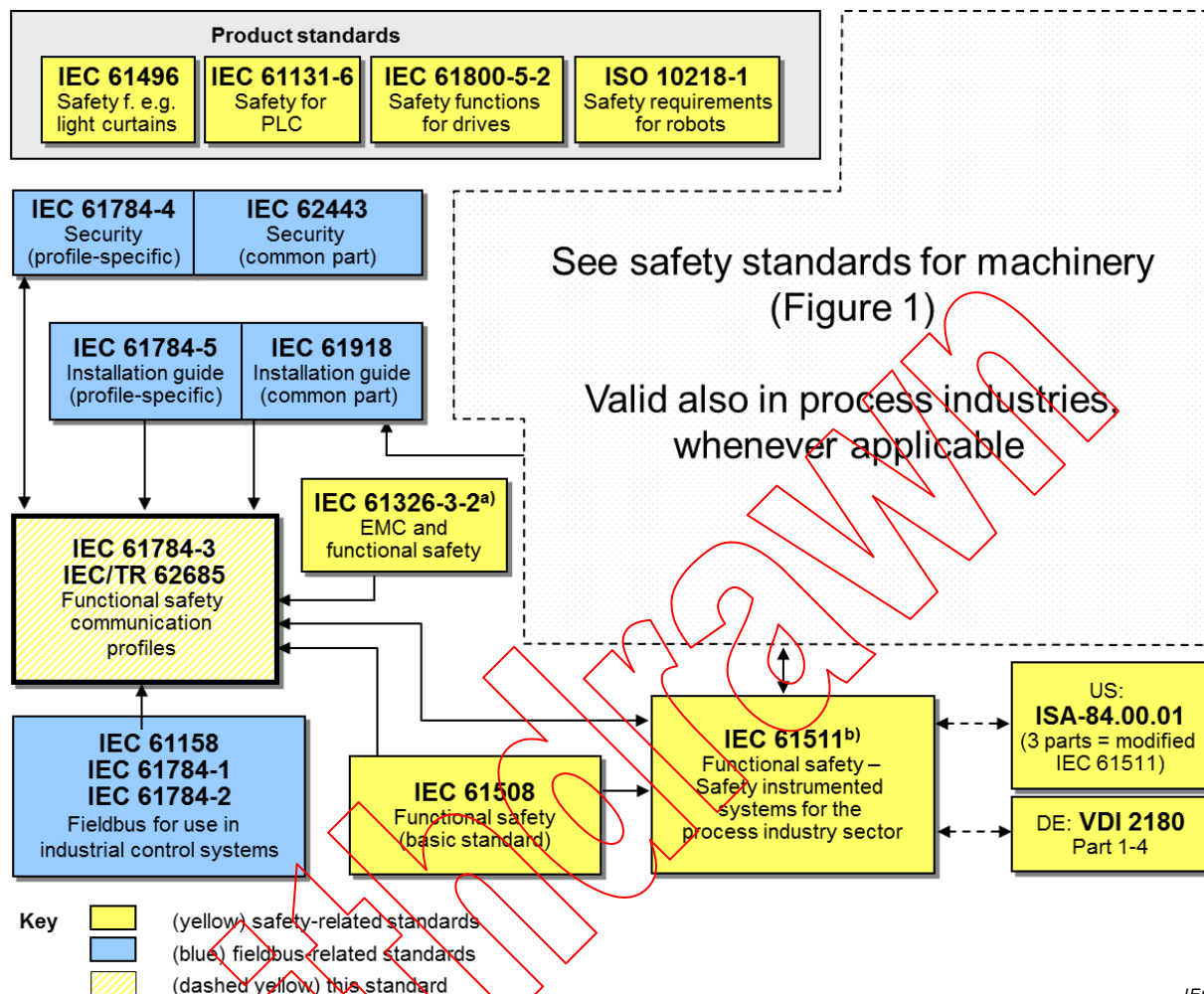


Figure 1 – Relationships of IEC 61784-3 with other standards (machinery)

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



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

^b EN ratified.

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

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

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

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

This standard describes:

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

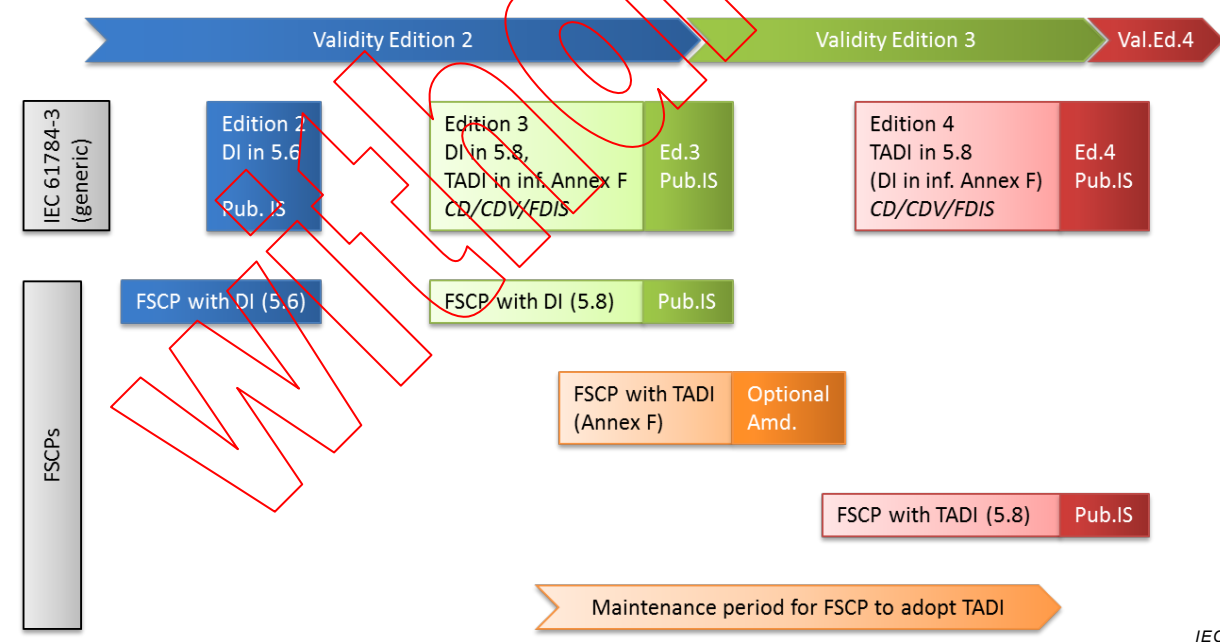
0.2 Transition from Edition 2 to extended assessment methods in Edition 3

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

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

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

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



IEC

Key

- DI Data Integrity
- TADI Timeliness, Authenticity, Data Integrity

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

0.3 Patent declaration

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

in IEC 61784-3-1, IEC 61784-3-2, IEC 61784-3-3, IEC 61784-3-6, IEC 61784-3-8, IEC 61784-3-12, IEC 61784-3-13, IEC 61784-3-14, IEC 61784-3-17 and IEC 61784-3-18.

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

The holders of these patent rights have assured the IEC that they are willing to negotiate licences either free of charge or under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statements of the holders of these patent rights are registered with IEC.

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

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

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

Withdrawn

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 series¹ 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 part² and the IEC 61784-3-x parts specify several functional safety communication profiles based on the communication profiles and protocol layers of the fieldbus technologies in IEC 61784-1, IEC 61784-2 and the IEC 61158 series. These functional safety communication profiles use the black channel approach, as defined in IEC 61508. These functional safety communication profiles are intended for implementation in safety devices exclusively.

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

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

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

NOTE 3 Additional profile specific requirements for security ~~may~~ can also be specified in IEC 61784-4³ ~~(40)~~.

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

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

2 Normative references

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

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

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

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

³ Proposed new work item under consideration.

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

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

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

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

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

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

IEC 61508-1:2010⁴, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements*

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

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

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

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

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

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

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

IEC 61784-3-8⁵, *Industrial communication networks – Profiles – Part 3-8: Functional safety fieldbuses – Additional specifications for CPF 8*

IEC 61784-3-12⁵, *Industrial communication networks – Profiles – Part 3-12: Functional safety fieldbuses – Additional specifications for CPF 12*

IEC 61784-3-13⁵, *Industrial communication networks – Profiles – Part 3-13: Functional safety fieldbuses – Additional specifications for CPF 13*

⁴ ~~To be published.~~

⁵ ~~To be published.~~

IEC 61784-3-14⁵, *Industrial communication networks – Profiles – Part 3-14: Functional safety fieldbuses – Additional specifications for CPF 14*

IEC 61784-3-17⁶, *Industrial communication networks – Profiles – Part 3-17: Functional safety fieldbuses – Additional specifications for CPF 17*

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

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

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

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

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

3 Terms, definitions, symbols, abbreviated terms and conventions

3.1 Terms and definitions

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

~~3.1.1 Common terms and definitions~~

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

3.1.1

absolute time stamp

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

[SOURCE: IEC 62280-2:2014, 3.1.1, modified – use *devices* and *fieldbus*]

3.1.2

active network element

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

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

[SOURCE: IEC 61918:2013, 3.1.2]

3.1.3

availability

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

3.1.4

bit error probability

P_e

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

⁶ To be published

3.1.5**black channel**

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

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

3.1.6**bridge**

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

3.1.7**closed communication system**

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

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

3.1.8**communication channel**

logical connection between two end-points within a communication system

3.1.9**communication system**

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

3.1.10**connection**

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

3.1.11**Cyclic Redundancy Check****CRC**

<value> redundant data derived from, and stored or transmitted together with, a block of data in order to detect data corruption

<method> procedure used to calculate the redundant data

Note 1 to entry: Terms "CRC code" and "CRC signature", and labels such as CRC1, CRC2, may also be used in this standard to refer to the redundant data.

Note 2 to entry: See also [28], [29], ~~[30]~~⁷.

3.1.12**defined communication system****defined channel**

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

⁷ Figures in square brackets refer to the bibliography.

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, 3.3.7⁸]

3.1.14

error

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

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

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

[SOURCE: IEC 61508-4:2010, 3.6.11, modified – notes added] ~~[IEC 61158]~~

3.1.15

explicit code

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

3.1.16

failure

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

~~NOTE 1 – The definition in IEC 61508-4 is the same, with additional notes.~~

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

[SOURCE: IEC 61508-4:2010, 3.6.4, modified – notes and figures replaced]₇
~~[ISO/IEC 2382-14.01.11, modified]~~

3.1.17

fault

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

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

[SOURCE: IEC 61508-4:2010, 3.6.1, modified – figure reference deleted]₇
~~[ISO/IEC 2382-14.01.10, modified]~~

3.1.18

fieldbus

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

3.1.19

fieldbus system

system using a *fieldbus* with connected devices

⁸ ~~To be published.~~

3.1.20**DLPDU**

DEPRECATED: frame

~~denigrated synonym for DLPDU~~

Data Link Protocol Data Unit

3.1.21**Frame Check Sequence**

FCS

redundant data derived from a block of data within a DLPDU (frame), using a hash function, and stored or transmitted together with the block of data, in order to detect data corruption

Note 1 to entry: An FCS can be derived using for example a CRC or other hash function.

Note 2 to entry: See also [28], [29], ~~[30]~~.

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

3.1.22**hash function**

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

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

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

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

3.1.23**hazard**

state or set of conditions of a system that, together with other related conditions will inevitably lead to harm to persons, property or environment

3.1.24**implicit code**

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

3.1.25**master**

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

3.1.26**message**

ordered series of octets intended to convey information

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

3.1.27**message sink**

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

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

3.1.28**message source**

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

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

3.1.29

nuisance trip

spurious trip with no harmful effect

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

3.1.30

performance level

PL

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

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

3.1.31

protective extra-low-voltage

PELV

electrical circuit in which the voltage cannot exceed a.c. 30 V r.m.s., 42,4 V peak or d.c. 60 V in normal and single-fault condition, except earth faults in other circuits

Note 1 to entry: A PELV circuit ~~is similar to an SELV circuit that is connected~~ incorporates a connection to protective earth. Without the protective earth connection or if there is a fault in the protective earth connection, the circuit voltages are not controlled.

[SOURCE: IEC ~~61131-2~~ 61010-2-201:2013, 3.109, modified – deletion of "circuit" from term, and deletion of second note to entry]

3.1.32

redundancy

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

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

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

[SOURCE: IEC 61508-4:2010, 3.4.6, modified – example and notes deleted];
[ISO/IEC 2382-14:01.12, modified]

3.1.33

relative time stamp

time stamp referenced to the local clock of an entity

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

[SOURCE: IEC 62280-2:2014, ~~modified~~, 3.1.43]

3.1.34

reliability

probability that an automated system can perform a required function under given conditions for a given time interval (t_1, t_2)

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

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

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

Note 4 to entry: Reliability differs from availability.

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

3.1.35

residual error probability

RP

probability of an error undetected by the SCL safety measures

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

3.1.36

residual error rate

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

3.1.37

risk

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

Note 1 to entry: For more discussion on this concept see Annex A of IEC 61508-5:2010⁹.

[SOURCE: IEC 61508-4:2010, 3.1.6, and ISO/IEC Guide 51:1999 2014, definition ~~3.2~~ 3.9, modified – different note]

3.1.38

safety communication channel

SC

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

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

3.1.39

safety communication layer

SCL

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

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

3.1.40

safety connection

connection that utilizes the safety protocol for communications transactions

3.1.41

safety data

data transmitted across a safety network using a safety protocol

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

⁹ ~~To be published.~~

3.1.42

safety device

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

3.1.43

safety extra-low-voltage

SELV

electrical circuit in which the voltage cannot exceed a.c. 30 V r.m.s., 42,4 V peak or d.c. 60 V in normal and single-fault condition, including earth faults in other circuits

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

[SOURCE: IEC ~~61131-2~~ 61010-2:2013, 3.110, modified – deletion of "circuit" from term, and deletion of note to entry]

3.1.44

safety function

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

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

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

3.1.45

safety function response time

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

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

3.1.46

safety integrity level

SIL

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

Note 1 to entry: The target failure measures (see IEC 61508-4:2010, 3.5.17) for the four safety integrity levels are specified in Tables 2 and 3 of IEC 61508-1:2010 ~~40~~.

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

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

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

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

3.1.47 safety measure

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

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

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

3.1.48 safety PDU SPDU PDU transferred through the safety communication channel

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

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

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

3.1.49 safety-related application

programs designed in accordance with IEC 61508 to meet the SIL requirements of the application

3.1.50 safety-related system

system performing *safety functions* according to IEC 61508

3.1.51 slave

passive communication entity able to receive messages and send them in response to another communication entity which may be a master or a slave

3.1.52 spurious trip

trip caused by the safety system without a process demand

3.1.53 time stamp

time information included in a *message*

3.1.54 uniform distribution

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

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

3.1.55 white channel

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

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

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

~~None required for this part.~~

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

~~None required for this part.~~

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

~~None required for this part.~~

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

~~None required for this part.~~

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

~~None required for this part.~~

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

~~None required for this part.~~

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

~~None required for this part.~~

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

~~None required for this part.~~

3.2 Symbols and abbreviated terms

~~3.2.1 Common symbols and abbreviated terms~~

BSC	Binary Symmetric Channel	
CP	Communication Profile	[IEC 61784-1]
CPF	Communication Profile Family	[IEC 61784-1]
CRC	Cyclic Redundancy Check	
DLL	Data Link Layer	[ISO/IEC 7498-1]
DLPPDU	Data Link Protocol Data Unit	
EMC	Electromagnetic Compatibility	
EMI	Electromagnetic Interference	
EUC	Equipment Under Control	[IEC 61508-4:2010]
E/E/PE	Electrical/Electronic/Programmable Electronic	[IEC 61508-4:2010]
FAL	Fieldbus Application Layer	[IEC 61158-5]
FCS	Frame Check Sequence	
FIT	Failure In Time (equals 10^{-9} failure per hour)	
FS	Functional Safety	
FSCP	Functional Safety Communication Profile	
IACS	Industrial Automation and Control System	
MTBF	Mean Time Between Failures	

MTTF	Mean Time To Failure	
NSR	Non Safety- ~~Relevant~~ Related	
PDU	Protocol Data Unit	[ISO/IEC 7498-1]
Pe	Bit error probability	
PELV	Protective Extra Low Voltage	
PES	Programmable Electronic System	[IEC 61508-4:2010]
PFD _{avg}	Average probability of dangerous Failure on Demand	[IEC ~~61508-6~~ 61508-4:2010 ¹⁴]
PFH	Average frequency of dangerous failure [h ⁻¹] per hour	[IEC ~~61508-6~~ 61508-4:2010]
PhL	Physical Layer	[ISO/IEC 7498-1]
PL	Performance Level	[ISO 13849-1]
PLC	Programmable Logic Controller	
RP	Residual Error Probability	
SCL	Safety Communication Layer	
SELV	Safety Extra Low Voltage	
SIS	Safety Instrumented Systems	
~~SIL~~	~~Safety Integrity Level~~	~~[IEC 61508-4:2010]~~
SL	Security Level	[IEC 62443]
SMS	Security Management System	[IEC 62443]
SPDU	Safety PDU	
SR	Safety- ~~Relevant~~ Related	

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

~~SIS Safety Instrumented Systems~~

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

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

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

~~DP Decentralized Peripherals~~

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

~~None required for this part.~~

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

~~ASE Application Service Element~~

~~SASE Safety Application Service Element~~

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

~~FSoE Failsafe over CPF 12~~

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

~~None required for this part.~~

¹⁴ ~~To be published.~~

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

~~IP~~ ~~Internet Protocol~~

~~UDP~~ ~~User Datagram Protocol~~

4 Conformance

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

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

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

or

conformance to IEC 61784-3 (Ed. ~~2.0~~ 3.0) FSCP n/m <Type>

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

Alternatively, a statement of conformance may be stated as either

conformance to IEC 61784-3-N:20xx

or

conformance to IEC 61784-3-N (Ed. ~~2.0~~ 3.0)

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

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

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

5 Basics of safety-related fieldbus systems

5.1 Safety function decomposition

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

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

EXAMPLE

In Figure 3, the PFH of the safety function is $PFH_{\text{sensor}} + PFH_{\text{PES}} + PFH_{\text{actuator}} + 2 \times PFH_{\text{safety-communication-channel}}$

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

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

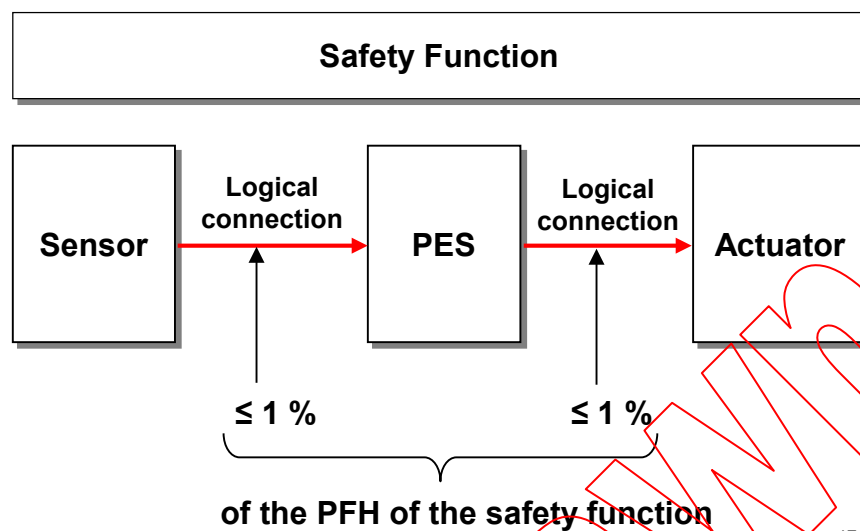


Figure 4 – Safety communication as a part of a safety function

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

5.2 Communication system

5.2.1 General

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

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

5.2.2 IEC 61158 fieldbuses

While IEC 61508 is not restricting the use of communication technologies, this standard focuses on the use of fieldbus based functional safety communication systems. Figure 5 shows an example model of the use of functional safety communications with a fieldbus based on the black channel approach.

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

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

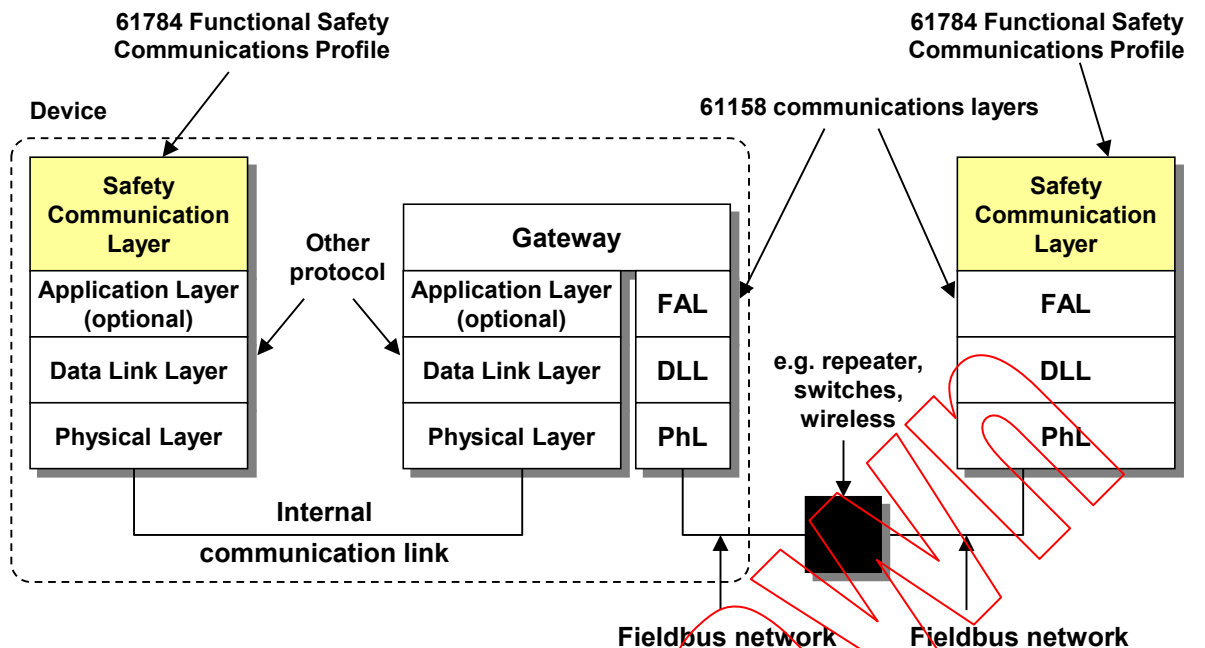


Figure 5 – Example model of a functional safety communication system

NOTE 1 While implementation of the Fieldbus Application Layer (FAL) is required, while the AL for functional safety communication systems according to this standard, the Application Layer may be omitted for communication links internal to a device (for example with a gateway).

NOTE 2 Functions of the user layer that are not safety-related may bypass the SCL and access the FAL directly.

5.2.3 Communication channel types

IEC 61508 uses the concepts of the so called “black channel” or “white channel” to define the requirements of the base fieldbus for transmission of safety data. Whether a communication channel is white or black is determined by where the safety measures are accomplished with respect to the base fieldbus. This standard specifies functional safety communication profiles that use the black channel approach.

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

5.2.4 Safety function response time

The safety function response time is the worst case elapsed time following an actuation of a safety sensor (for example switch, pressure transmitter, light curtain) connected to a fieldbus, before until the corresponding safe state of its safety actuator(s) (for example relay, valve, drive) is achieved in the presence of errors or failures in the safety function-channel.

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

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

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

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

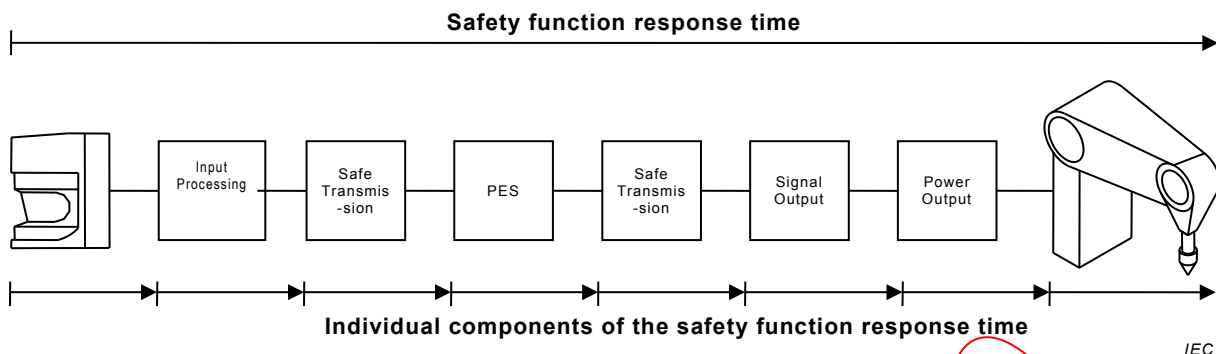


Figure 6 – Example of safety function response time components

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 ~~should~~ will not be classed as 'Loss' until recovery or repetition procedures have failed or are not used.

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

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

5.3.3 Unintended repetition

Due to an error, fault or interference, ~~old not updated~~ messages are repeated ~~at an incorrect point in time~~.

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

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

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

5.3.4 Incorrect sequence

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

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

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

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

5.3.5 Loss

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

5.3.6 Unacceptable delay

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

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

~~a) immediate repetition;~~

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

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

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

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

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

5.3.7 Insertion

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

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

5.3.8 Masquerade

Due to a fault or interference, a message is inserted that relates to an apparently valid source entity, so a non-safety ~~relevant~~ related message may be received by a safety ~~relevant~~ related participant, which then treats it as safety ~~relevant~~ related.

NOTE Communication systems used for safety-related applications ~~may~~ can use additional checks to detect Masquerade, such as authorised source identities and pass-phrases or cryptography.

5.3.9 Addressing

Due to a fault or interference, a safety ~~relevant~~ related message is ~~sent~~ delivered to the ~~wrong incorrect~~ safety ~~relevant~~ related participant, which then treats reception as correct. This

includes the so-called loopback error case, where the sender receives back its own sent message.

5.4 Deterministic remedial measures

5.4.1 General

Subclauses 5.4.2 to 5.4.9 list measures commonly used to detect deterministic errors and failures of a communication system, as contrasted to stochastic errors like message corruption due to electromagnetic interference.

5.4.2 Sequence number

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

5.4.3 Time stamp

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

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

NOTE 2 Time stamping ~~implicitly~~ requires the time base to be synchronized. For safety applications, synchronization ~~needs to~~ shall be regularly monitored, and the probability of this mechanism failing shall be included in the assessment of the overall safety function.

5.4.4 Time expectation

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

EXAMPLE

Time-slot-oriented access method:

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

5.4.5 Connection authentication

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

5.4.6 Feedback message

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

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

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

5.4.7 Data integrity assurance

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

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

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

5.4.8 Redundancy with cross checking

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

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

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

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

5.4.9 Different data integrity assurance systems

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

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

5.5 Typical relationships between errors and safety measures

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

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

NOTE A safety measure ~~can~~ shall only be listed in the corresponding table for a given FSCP if this measure takes effect before the ~~guaranteed~~ 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 62280-2:2014 [15] and [28], Table 1.								
^a Only for sender identification. Detects only insertion of an invalid source. ^b Required in all cases. ^c This measure is only comparable with a high quality data assurance mechanism if a calculation can show that the residual error rate Λ reaches the values required in 5.4.9 when two messages are sent through independent transceivers. ^d Effective only if feedback message includes original data or information about the original data, and if the receiver only acts on the data after acknowledge of the feedback message. ^e Effective only if the sequence numbers or time stamps of the source entities are different.								

5.6 Communication phases

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

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

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

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

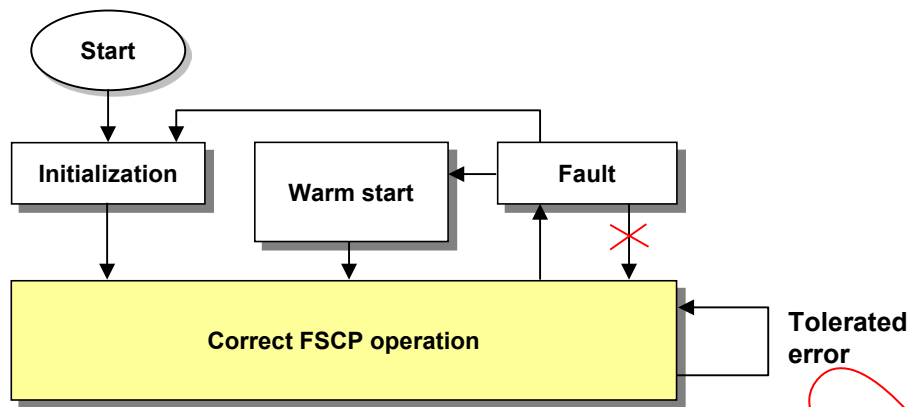


Figure 7 – Conceptual FSCP protocol model

5.7 FSCP implementation aspects

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

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

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

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

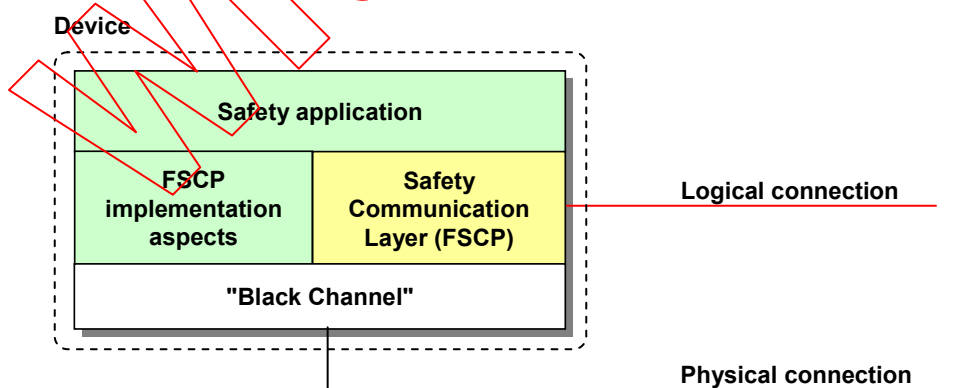


Figure 8 – FSCP implementation aspects

5.8 Data integrity considerations

5.8.1 Calculation of the residual error rate

Even when the messages are arriving in a correct (deterministic) manner the ~~safety data~~ SPDU still may be corrupted. Thus data integrity assurance is a fundamental component of

the safety communication layer to reach a required safety integrity level. Suitable hash functions like parity bits, cyclic redundancy check (CRC), message repetition, and similar forms of message redundancy shall be applied.

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

NOTE 1 EXAMPLE When CRC is used as the hash function, the ~~communication channel~~ fieldbus DLL shall not use the same CRC polynomial as the superimposed safety communication layer.

All these methodologies provide a means of achieving low residual error rates. All measures of data integrity assurance shall be implemented within the superimposed parts (safety communication layer) of the controls designed to the required SIL claim.

A supplier may choose various calculation methods for providing estimates for the data integrity mechanisms of fieldbus networks. The results of these calculations may lead to either more effort in the design of hardware and software to provide integrity or more effort in the calculation and proof of the reliability of the overall control system.

The residual error rate is calculated from the residual error probability of the superimposed (safety) data integrity assurance mechanism and the ~~transmission rate of safety messages~~ sample rate of SPDUs. In ~~addition~~ case of calculation of PFH / PFD_{avg} per safety function, one shall take into account for the assessment the maximum number of information sinks (m) that is permitted in a single safety function.

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

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

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

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

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

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

Equation items	Definition
$\lambda_{SC} (Pe)$	Residual error rate per hour of the safety communication ~~layer~~ channel with respect to the bit error probability (see 3.1.36)
$\lambda_{SCL} (Pe)$	Residual error rate per hour of the safety communication layer with respect to the bit error probability (see 3.1.36)
Pe	Bit error probability (see Clause B.3). ~~Unless a better error probability can be proven, a value of 10^{-2} shall be used.~~ ^a
$R_{SC} (Pe)$	Residual error probability of the safety ~~message~~ communication channel with respect to the bit error probability (see 3.1.35)
v	Maximum ~~number of safety messages~~ sample rate of SPDUs per hour
m	Maximum number of ~~information sinks that is permitted in a single safety function (see Figure 6)~~ logical connections that is permitted in a single safety function (see Figure 9 and Figure 10)

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

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

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

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

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

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

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

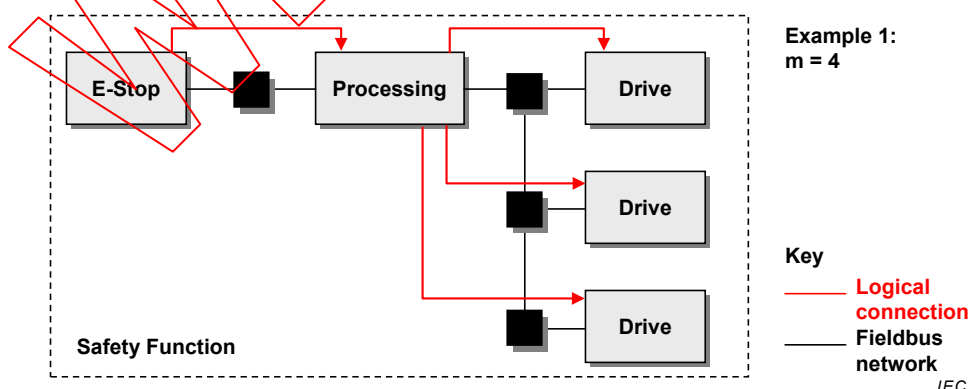


Figure 9 – Example application 1 ($m=4$)

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

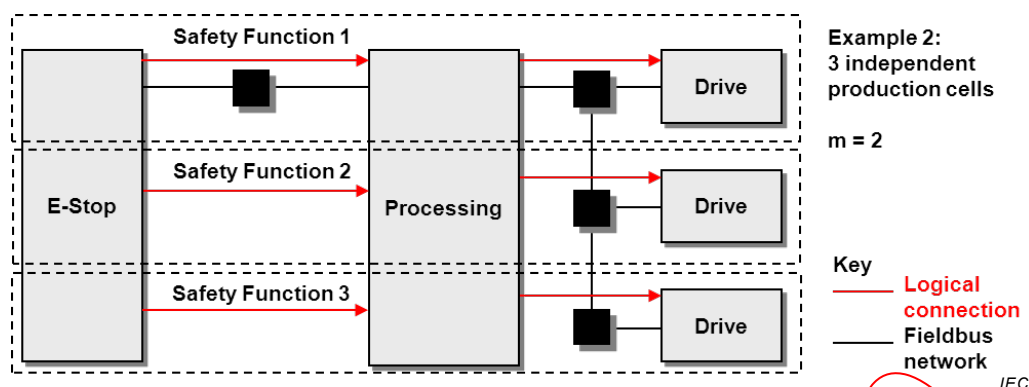


Figure 10 – Example application 2 (m = 2)

5.8.2 Total residual error rate and SIL

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

Both low demand and high demand mode systems shall have a defined safety function response time, so a necessary ~~number of safety messages per second~~ rate of SPDUs shall be guaranteed. ~~The calculation of the error rate is based on high demand mode, and is therefore also applicable to the low demand mode.~~ The PFH for a certain SIL shall be provided in all cases, while the PFD_{avg} is optional.

Table 3 – Typical relationship of residual error rate to SIL ~~level~~

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

~~NOTE – Values in this table are based on the assumption that the functional safety communication system contributes no more than 1 % of the total failures of the safety function.~~

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

Applicable for safety functions up to SIL	Average probability of a dangerous failure on demand for the safety function (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	$< 10^{-1}$	$< 10^{-3}$

5.9 Relationship between functional safety and security

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

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

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

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

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

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

IEC 62443 also addresses the requirements to secure system components.

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

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

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

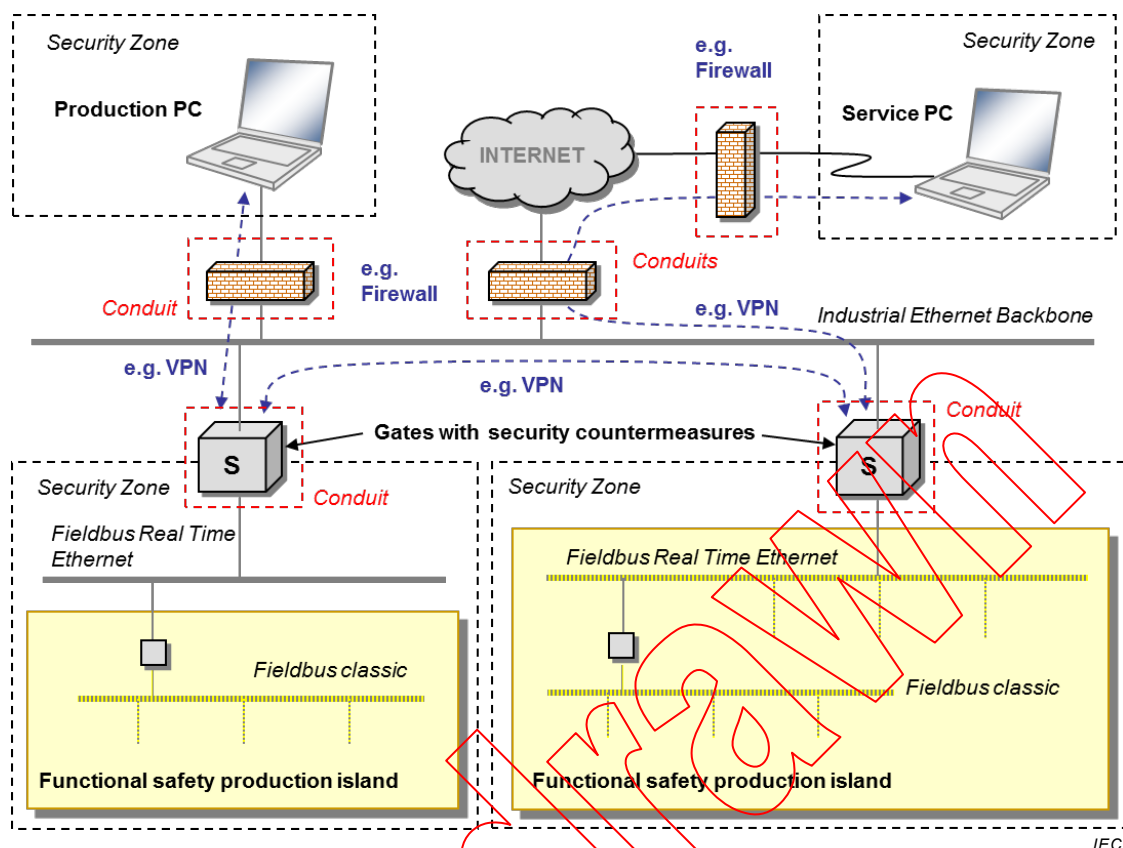


Figure 11 – Zones and conduits concept for security according to IEC 62443

5.10 Boundary conditions and constraints

5.10.1 Electrical safety

Electrical safety is a precondition for a functional safety communication system. Therefore, all safety devices connected to it shall conform to the relevant ~~SELV/PELV IEC specifications (for example IEC 61131-2)~~ IEC electrical safety standards (for example SELV/PELV as specified in IEC 61010-2-201). The Safety Manual shall specify the constraints required of the devices connected in a functional safety communication system, whether safety devices or non-safety devices, including active network elements.

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

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

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

5.10.2 Electromagnetic compatibility (EMC)

~~IEC 61508 requires "Increase of interference immunity", but does not specify how to achieve this. Functional safety communication profiles in this standard will use for that purpose the increased test levels and corresponding performance criteria specified in IEC 61326-3-1.~~ Safety devices shall comply with the increased test levels and durations, as well as corresponding performance criteria specified in IEC 61326-3-1 or the generic standard IEC 61000-6-7. IEC 61326-3-2 may be used as an exception, if the intended application exactly matches the specific scope and pre-conditions of IEC 61326-3-2.

NOTE Certain applications ~~may~~ can require higher levels than those specified in IEC 61326-3-1, according to Safety Requirements Specification (SRS).

5.11 Installation guidelines

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

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

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

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

5.12 Safety manual

According to IEC 61508-2, device suppliers shall provide a safety manual. A description of the minimum information required by the profile to be included in the safety manual is provided in the relevant profile specific parts.

5.13 Safety policy

Users of this standard shall take into account the following constraints to avoid misunderstanding, wrong expectations or legal actions regarding safety-related developments and applications.

NOTE 1 This includes for example use for training, seminars, workshops and consultancy.

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

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

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

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

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

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

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

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

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

6.1 Functional Safety Communication Profile 1/1

Communication Profile Family 1 (commonly known as FOUNDATION™ Fieldbus¹²) defines communication profiles based on IEC 61158-2 Type 1, IEC 61158-3-1, IEC 61158-4-1, IEC 61158-5-5, IEC 61158-5-9, IEC 61158-6-5, and IEC 61158-6-9.

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

6.2 Technical overview

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

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

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

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

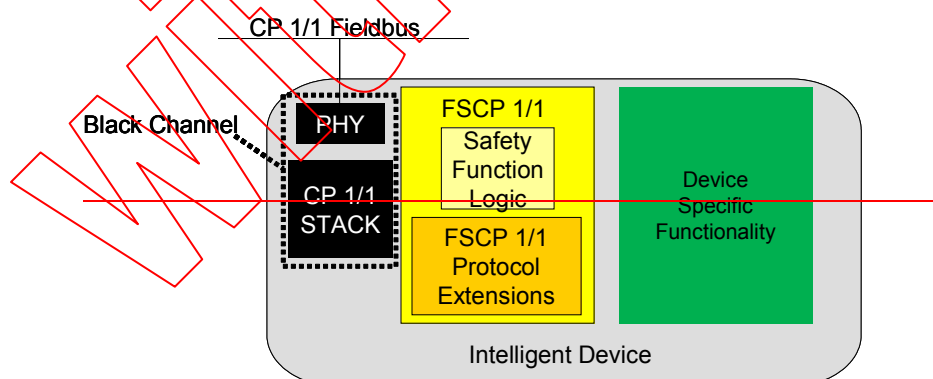


Figure 7 – Scope of FSCP 1/1

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

¹² FOUNDATION™ Fieldbus and FF-SIS™ are trade names of the non-profit organization Fieldbus Foundation. This information is given for the convenience of users of this International Standard and does not constitute an endorsement by IEC of the trade name holder or any of its products. Compliance to this standard does not require use of the trade names Foundation Fieldbus™ or FF-SIS™. Use of the trade names FOUNDATION™ Fieldbus or FF-SIS™ requires permission of Fieldbus Foundation and compliance with conditions for their use (such as testing and validation).

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

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

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

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

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

Communication Profile Family 16 (commonly known as SERCOS®¹⁴) defines a communication profile CP 16/3 based on IEC 61158-3-19, IEC 61158-4-19, IEC 61158-5-19, and IEC 61158-6-19.

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

~~7.2 Technical overview~~

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

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

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

¹⁴ SERCOS® is a trade name of SERCOS International e.V. This information is given for the convenience of users of this International Standard and does not constitute an endorsement by IEC of the trademark holder or any of its products. Compliance to this standard does not require use of the trade name SERCOS®. Use of the trade name SERCOS® requires permission of the trade name holder and compliance with conditions for its use (such as testing and validation).

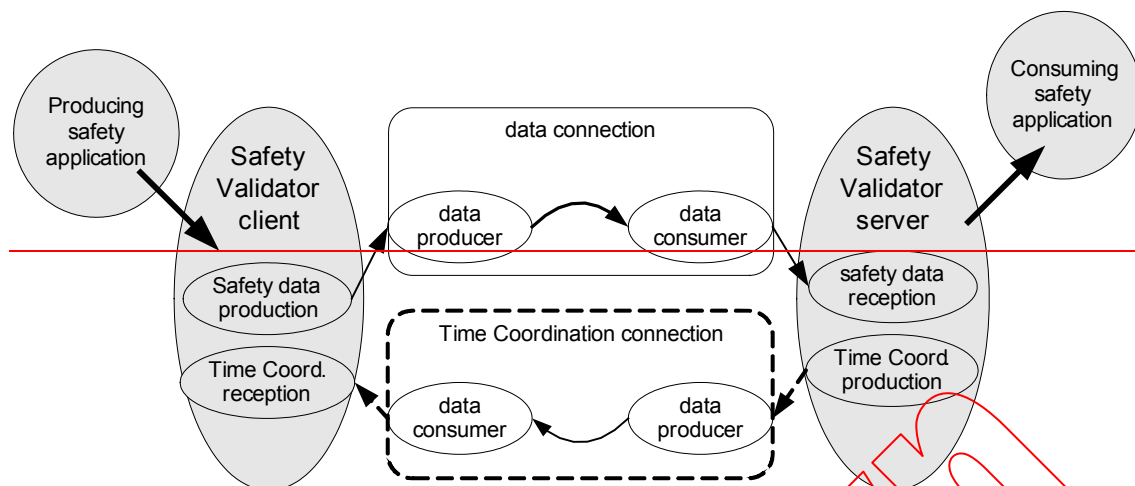


Figure 8 — Relationship of Safety Validators

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

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

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

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

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

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

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

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

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

Communication Profile Family 3 (commonly known as PROFIBUS™, PROFINET™¹⁵) defines communication profiles based on IEC 61158-2 Type 3, IEC 61158-3-3, IEC 61158-4-3, IEC 61158-5-3, IEC 61158-5-10, IEC 61158-6-3, and IEC 61158-6-10.

The basic profiles CP 3/1 and CP 3/2 are defined in IEC 61784-1; CP 3/4, CP 3/5 and CP 3/6 are defined in IEC 61784-2. The CPF 3 functional safety communication profile FSCP 3/1 (PROFIsafe™⁹) is based on the CPF 3 basic profiles in IEC 61784-1 and IEC 61784-2 and the safety communication layer specifications defined in IEC 61784-3-3.

8.2 ~~Technical overview~~

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

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

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

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

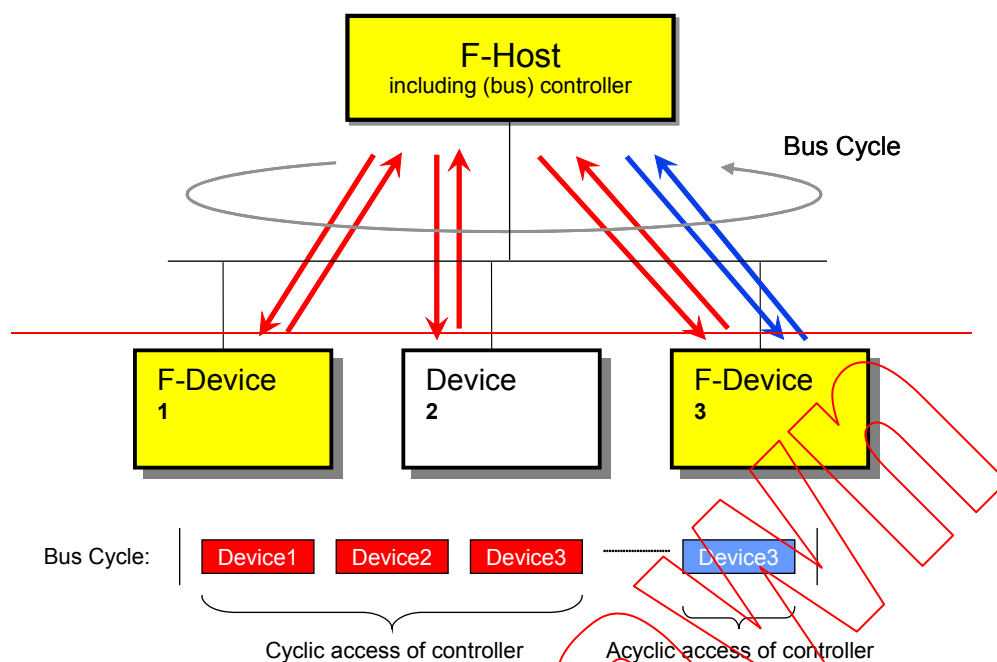


Figure 9 – Basic communication preconditions for FSCP 3/1

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

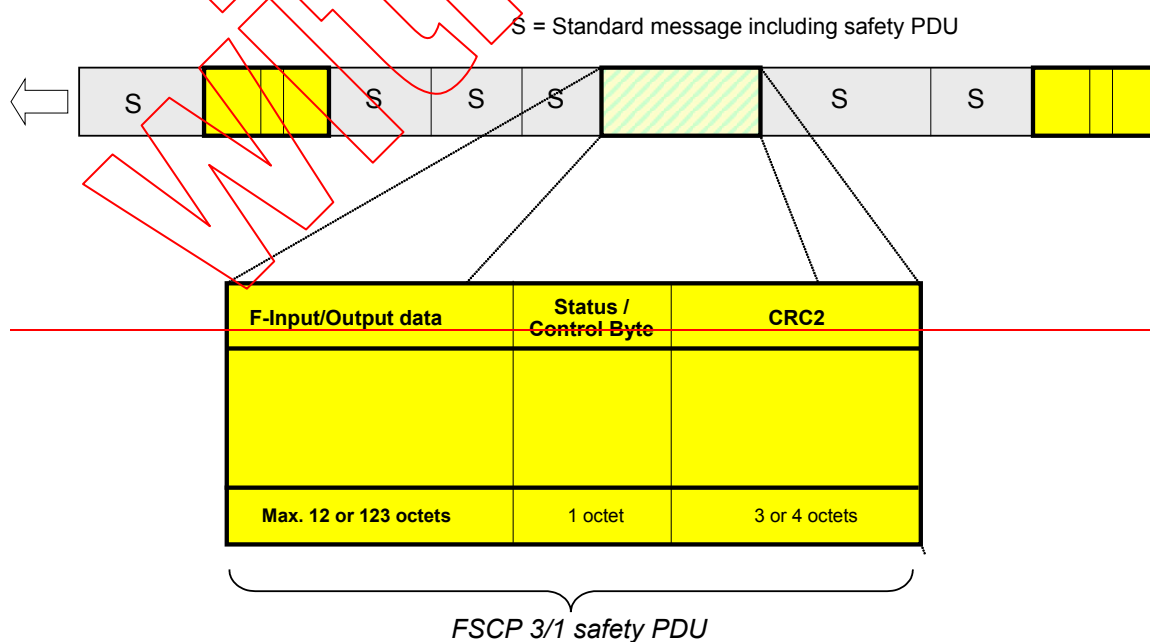


Figure 10 – Structure of a FSCP 3/1 safety PDU

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

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

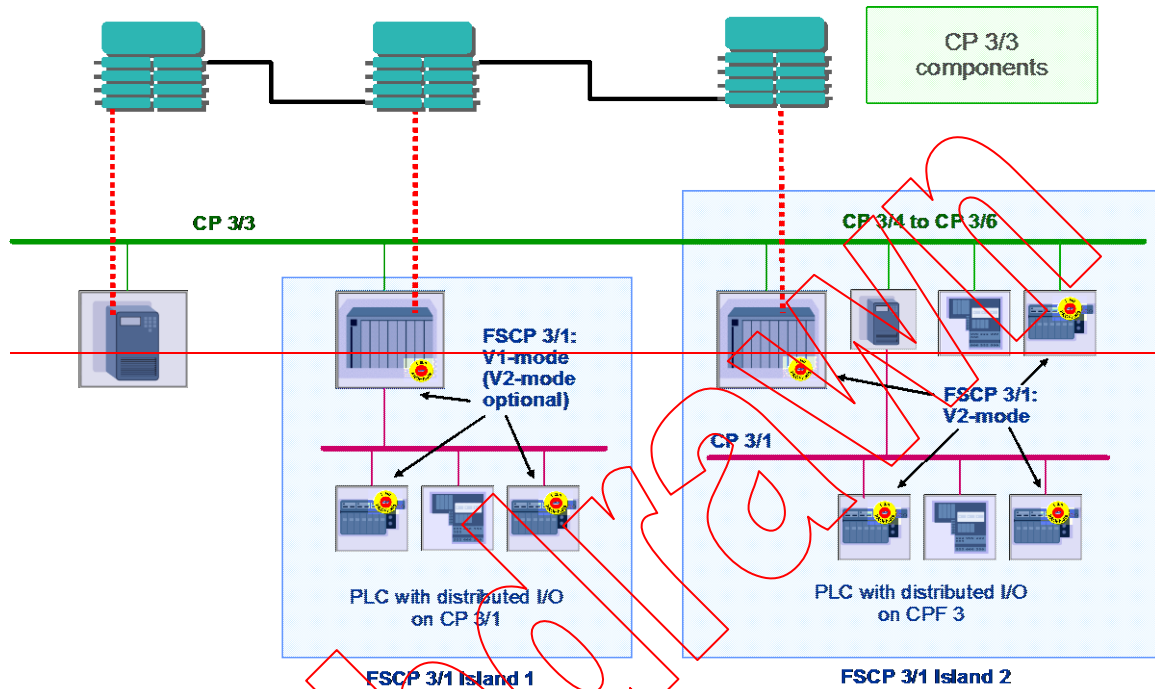


Figure 11 – Safe communication modes

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

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

9.1 Functional Safety Communication Profile 6/7

Communication Profile Family 6 (commonly known as INTERBUS®¹⁶) defines communication profiles based on IEC 61158-2 Type 8, IEC 61158-3-8, IEC 61158-4-8, IEC 61158-5-8, and IEC 61158-6-8.

The basic profiles CP 6/1, CP 6/2, CP 6/3 are defined in IEC 61784-1. The CPF 6 functional safety communication profile FSCP 6/7 (INTERBUS Safety™¹⁰) is based on the CPF 6 basic profiles in IEC 61784-1 and the safety communication layer specifications defined in IEC 61784-3-6.

The profiles CP 6/1, CP 6/2 and CP 6/3 contain optional services, which are specified by profile identifiers. The suitable profile identifiers for CP 6/7 are shown in Table 5.

¹⁶ INTERBUS® and INTERBUS Safety™ are trade names of Phoenix Contact GmbH & Co. KG, control of trade name use is given to the non profit organization INTERBUS Club. This information is given for the convenience of users of this International Standard and does not constitute an endorsement by IEC of the trade name holder or any of its products. Compliance to this standard does not require use of the trade names INTERBUS® or INTERBUS Safety™. Use of the trade names INTERBUS® or INTERBUS Safety™ requires permission of the INTERBUS Club and compliance with conditions for their use (such as testing and validation).

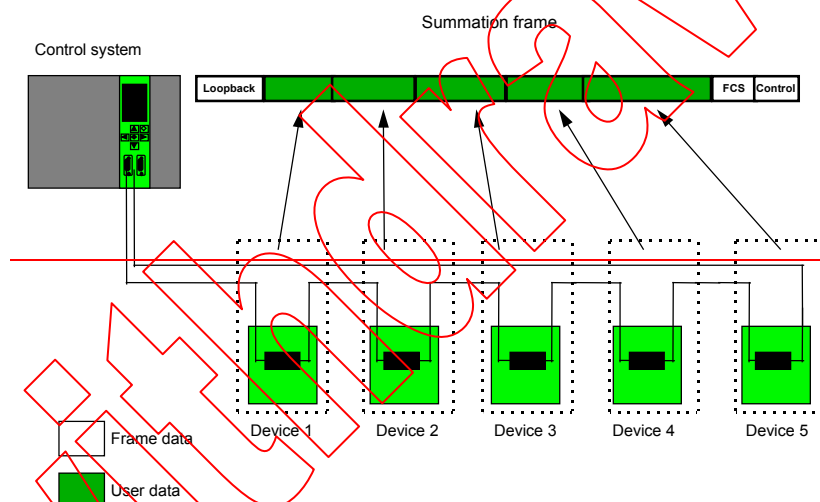
Table 5 – Overview of profile identifier usable for FSCP 6/7

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

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

9.2 Technical overview

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

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

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

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

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

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

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

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

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

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

10.1 Functional Safety Communication Profile 8/1

Communication Profile Family 8 (commonly known as CC-Link™¹⁷) defines communication profiles based on IEC 61158-2 Type 18, IEC 61158-3-18, IEC 61158-4-18, IEC 61158-5-18, and IEC 61158-6-18.

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

10.2 ~~Technical overview~~ Functional Safety Communication Profile 8/2

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

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

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

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

¹⁷ CC-Link™ and CC-Link Safety™ are trade names of the non-profit organization CC-Link Partner Association. This information is given for the convenience of users of this International Standard and does not constitute an endorsement by IEC of the trade name holder or any of its products. Compliance to this standard does not require use of the trade names CC-Link™ or CC-Link Safety™. Use of the trade names CC-Link™ or CC-Link Safety™ requires permission of CC-Link Partner Association and compliance with conditions for their use (such as testing and validation).