



BSI Standards Publication

Industrial communication networks — Profiles

Part 3-8: Functional safety fieldbuses — Additional specifications for CPF8

National foreword

This British Standard is the UK implementation of EN IEC 61784-3-8:2021. It is identical to IEC 61784-3-8:2021. It supersedes BS EN 61784-3-8:2017, which will be withdrawn on 23 June 2024.

The UK participation in its preparation was entrusted to Technical Committee GEL/65/3, Industrial communications: process measurement and control, including fieldbus.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

© The British Standards Institution 2021
Published by BSI Standards Limited 2021

ISBN 978 0 539 18092 3

ICS 25.040.40; 35.100.05

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 July 2021.

Amendments/corrigenda issued since publication

Date	Text affected
------	---------------

English Version

**Industrial communication networks - Profiles - Part 3-8:
Functional safety fieldbuses - Additional specifications for CPF8
(IEC 61784-3-8:2021)**

Réseaux de communication industriels - Profils - Partie 3-8:
Bus de terrain de sécurité fonctionnelle - Spécifications
supplémentaires pour CPF 8
(IEC 61784-3-8:2021)

Industrielle Kommunikationsnetze - Profile - Teil 3-8:
Funktional sichere Übertragung bei Feldbussen -
Zusätzliche Festlegungen für die
Kommunikationsprofilfamilie 8
(IEC 61784-3-8:2021)

This European Standard was approved by CENELEC on 2021-06-23. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.



European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

European foreword

The text of document 65C/1083/FDIS, future edition 3 of IEC 61784-3-8, prepared by SC 65C "Industrial networks" of IEC/TC 65 "Industrial-process measurement, control and automation" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN IEC 61784-3-8:2021.

The following dates are fixed:

- latest date by which the document has to be implemented at national (dop) 2022-03-23 level by publication of an identical national standard or by endorsement
- latest date by which the national standards conflicting with the (dow) 2024-06-23 document have to be withdrawn

This document supersedes EN 61784-3-8:2017 and all of its amendments and corrigenda (if any).

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

Endorsement notice

The text of the International Standard IEC 61784-3-8:2021 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following notes have to be added for the standards indicated:

IEC 61000-1-2	NOTE	Harmonized as EN 61000-1-2
IEC 61000-6-7	NOTE	Harmonized as EN 61000-6-7
IEC 61010-2-201	NOTE	Harmonized as EN IEC 61010-2-201
IEC 61131-6	NOTE	Harmonized as EN 61131-6
IEC 61158-1	NOTE	Harmonized as EN IEC 61158-1
IEC 61158-5 (series)	NOTE	Harmonized as EN 61158-5 (series)
IEC 61496 (series)	NOTE	Harmonized as EN IEC 61496 (series)
IEC 61508-1:2010	NOTE	Harmonized as EN 61508-1:2010 (not modified)
IEC 61508-4:2010	NOTE	Harmonized as EN 61508-4:2010 (not modified)
IEC 61508-5:2010	NOTE	Harmonized as EN 61508-5:2010 (not modified)
IEC 61784-3 (series)	NOTE	Harmonized as EN 61784-3 (series)
IEC 61784-5 (series)	NOTE	Harmonized as EN IEC 61784-5 (series)
IEC 61800-5-2	NOTE	Harmonized as EN 61800-5-2
IEC 61918:2018	NOTE	Harmonized as EN IEC 61918:2018 (not modified)
IEC 62443 (series)	NOTE	Harmonized as EN IEC 62443 (series)
ISO 10218-1	NOTE	Harmonized as EN ISO 10218-1
ISO 13849 (series)	NOTE	Harmonized as EN ISO 13849 (series)
ISO 13849-1:2015	NOTE	Harmonized as EN ISO 13849-1:2015 (not modified)
ISO 13849-2	NOTE	Harmonized as EN ISO 13849-2

Annex ZA (normative)

Normative references to international publications with their corresponding European publications

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

NOTE 1 Where an International Publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

NOTE 2 Up-to-date information on the latest versions of the European Standards listed in this annex is available here: www.cenelec.eu.

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
IEC 61131-2	-	Industrial-process measurement and control - Programmable controllers - Part 2: Equipment requirements and tests	-	-
IEC 61158	series	Industrial communication networks - Fieldbus specifications	EN IEC 61158	series
IEC 61158-2	-	Industrial communication networks - Fieldbus specifications - Part 2: Physical layer specification and service definition	EN 61158-2	-
IEC 61158-3-18	-	Industrial communication networks - Fieldbus specifications - Part 3-18: Data-link layer service definition - Type 18 elements	EN 61158-3-18	-
IEC 61158-4-18	-	Industrial communication networks - Fieldbus specifications - Part 4-18: Data-link layer protocol specification - Type 18 elements	EN 61158-4-18	-
IEC 61158-5-18	-	Industrial communication networks - Fieldbus specifications - Part 5-18: Application layer service definition - Type 18 elements	EN 61158-5-18	-
IEC 61158-5-23	-	Industrial communication networks - Fieldbus specifications - Part 5-23: Application layer service definition - Type 23 elements	EN IEC 61158-5-23	-
IEC 61158-6-18	-	Industrial communication networks - Fieldbus specifications - Part 6-18: Application layer protocol specification - Type 18 elements	EN 61158-6-18	-
IEC 61158-6-23	-	Industrial communication networks - Fieldbus specifications - Part 6-23: Application layer protocol specification - Type 23 elements	EN IEC 61158-6-23	-

EN IEC 61784-3-8:2021 (E)

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
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	EN 61326-3-1	-
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	EN IEC 61326-3-2	-
IEC 61508	series	Functional safety of electrical/electronic/programmable electronic safety-related systems	EN 61508	series
IEC 61511	series	Functional safety - Safety instrumented systems for the process industry sector -	EN 61511	series
IEC 61784-1	-	Industrial communication networks - Profiles Part 1: Fieldbus profiles	EN IEC 61784-1	-
IEC 61784-2	-	Industrial communication networks - Profiles - Part 2: Additional fieldbus profiles for real-time networks based on ISO/IEC/IEEE 8802-3	EN IEC 61784-2	-
IEC 61784-3	2021	Industrial communication networks - Profiles - Part 3: Functional safety fieldbuses - General rules and profile definitions	EN IEC 61784-3	2021
IEC 62061	-	Safety of machinery - Functional safety of safety-related control systems	EN IEC 62061	-
ISO/IEC/IEEE 8802-3	-	Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 3: Standard for Ethernet	-	-

CONTENTS

FOREWORD	7
0 Introduction	9
0.1 General.....	9
0.2 Patent declaration	11
1 Scope	12
2 Normative references	12
3 Terms, definitions, symbols, abbreviated terms and conventions	13
3.1 Terms and definitions.....	13
3.1.1 Common terms and definitions.....	14
3.1.2 CPF 8: Additional terms and definitions	20
3.2 Symbols and abbreviated terms	21
3.2.1 Common symbols and abbreviated terms.....	21
3.2.2 CPF 8: Additional symbols and abbreviated terms	22
3.3 Conventions.....	22
4 Overview	22
5 General	22
6 Safety communication layer services	22
7 Safety communication layer protocol	23
8 Safety communication layer management.....	23
9 System requirements	23
10 Assessment.....	23
11 FSCP 8/1.....	23
11.1 Scope – FSCP 8/1	23
11.2 Normative references – FSCP 8/1.....	23
11.3 Terms, definitions, symbols, abbreviated terms and conventions – FSCP 8/1.....	23
11.4 Overview of FSCP 8/1 (CC-Link Safety™).....	23
11.5 General – FSCP 8/1.....	24
11.5.1 External documents providing specifications for the profile	24
11.5.2 Safety functional requirements	24
11.5.3 Safety measures.....	24
11.5.4 Safety communication layer structure	26
11.5.5 Relationships with FAL (and DLL, PhL).....	27
11.6 Safety communication layer services for FSCP 8/1	27
11.6.1 General	27
11.6.2 SASEs.....	27
11.6.3 SARs	28
11.6.4 Process data SAR ASEs	29
11.7 Safety communication layer protocol for FSCP 8/1.....	30
11.7.1 Safety PDU format.....	30
11.7.2 State description.....	38
11.8 Safety communication layer management for FSCP 8/1	43
11.8.1 General	43
11.8.2 Connection establishment and confirmation processing	43
11.8.3 Safety slave verification.....	43
11.9 System requirements for FSCP 8/1	44

11.9.1	Indicators and switches	44
11.9.2	Installation guidelines	45
11.9.3	Safety function response time	45
11.9.4	Duration of demands	47
11.9.5	Constraints for calculation of system characteristics	47
11.9.6	Maintenance	47
11.9.7	Safety manual	47
11.10	Assessment for FSCP 8/1	47
12	FSCP 8/2	48
12.1	Scope – FSCP 8/2	48
12.2	Normative references – FSCP 8/2	48
12.3	Terms, definitions, symbols, abbreviated terms and conventions – FSCP 8/2	48
12.4	Overview of FSCP 8/2 (CC-Link IE™ Safety communication function)	48
12.5	General – FSCP 8/2	48
12.5.1	External documents providing specifications for the profile	48
12.5.2	Safety functional requirements	49
12.5.3	Safety measures	49
12.5.4	Safety communication layer structure	54
12.5.5	Relationships with FAL (and DLL, PhL)	55
12.6	Safety communication layer services for FSCP 8/2	55
12.6.1	General	55
12.6.2	Connection reestablishment services	55
12.6.3	Data transmission services	56
12.6.4	Connection termination notification services	57
12.7	Safety communication layer protocol for FSCP 8/2	57
12.7.1	Safety PDU format	57
12.7.2	Safety FAL service protocol machine (SFSPM)	64
12.8	Safety communication layer management for FSCP 8/2	90
12.8.1	Parameter Definitions	90
12.8.2	Parameter Setup	94
12.8.3	Management Services	95
12.9	System requirements for FSCP 8/2	98
12.9.1	Indicators and switches	98
12.9.2	Installation guidelines	100
12.9.3	Safety function response time	100
12.9.4	Duration of demands	101
12.9.5	Constraints for calculation of system characteristics	101
12.9.6	Maintenance	102
12.9.7	Safety manual	102
12.10	Assessment for FSCP 8/2	103
Annex A (informative)	Additional information for functional safety communication profiles of CPF 8	104
A.1	Hash function calculation for FSCP 8/1	104
A.2	Hash function calculation for FSCP 8/2	104
A.3	Meaning of response time calculation formula for FSCP 8/2	105
Annex B (informative)	Information for assessment of the functional safety communication profiles of CPF 8	107
Bibliography		108

Figure 1 – Relationships of IEC 61784-3 with other standards (machinery)	9
Figure 2 – Relationships of IEC 61784-3 with other standards (process).....	10
Figure 3 – Relationship between SCL and the other layers of IEC 61158 Type 18.....	27
Figure 4 – State diagram	39
Figure 5 – Detection of unintended repetition.....	51
Figure 6 – Detection of incorrect sequence	51
Figure 7 – Detection of loss	52
Figure 8 – Detection of unacceptable delay by time stamps	53
Figure 9 – Detection of unacceptable delay by timer	53
Figure 10 – Protocol Hierarchy.....	54
Figure 11 – Safety PDU Structure	58
Figure 12 – CTRL Configuration.....	59
Figure 13 – SASE-M and SASE-S TS	62
Figure 14 – S-Data during safety refresh	62
Figure 15 – S-Data not during safety refresh.....	63
Figure 16 – S-Data header configuration.....	63
Figure 17 – CRC calculation	64
Figure 18 – Communication models	64
Figure 19 – SFSPM state transition diagram	65
Figure 20 – Connection establishment sequence	67
Figure 21 – Optional sequence during connection establishment sequence	68
Figure 22 – Communication sequence during safety refresh communication	68
Figure 23 – Offset measurement and generation sequence during safety refresh communication.....	69
Figure 24 – SFSPM-M state transition diagram	70
Figure 25 – Sequence other than during safety refresh	74
Figure 26 – S-Connect-req.....	74
Figure 27 – S-InitConfirmNetPrm-req	75
Figure 28 – net_prm_list	75
Figure 29 – S-InitVerifyStnPrm-req	75
Figure 30 – stn_prm_list	76
Figure 31 – S-InvokeFunc-req.....	76
Figure 32 – S-WriteErrorInfo-req.....	77
Figure 33 – date_and_time_of_occurrence.....	78
Figure 34 – SFSPM-S state transition diagram.....	79
Figure 35 – Sequence other than during safety refresh	84
Figure 36 – S-Connect-rsp.....	84
Figure 37 – S-InitConfirmNetPrm-rsp	85
Figure 38 – S-InitVerifyStnPrm-rsp	85
Figure 39 – S-InvokeFunc-rsp.....	86
Figure 40 – Offset calculation procedure of safety clock	87
Figure 41 – Relationship between transmission interval fluctuation and transmission_interval	91
Figure 42 – Calculation of allowable_refresh_interval	93

Figure 43 – Calculation of allowable_delay	94
Figure 44 – Calculation of response time between safety PLCs	100
Figure 45 – Constraints on N_{SE} and m	102
Figure A.1 – Allowable_delay and offset calculation deviation	105
Table 1 – Selection of the various measures for possible errors	25
Table 2 – M1 safety device manager attribute format	31
Table 3 – S1 safety device manager attribute format	31
Table 4 – M1 safety connection manager attribute format	31
Table 5 – S1 safety connection manager attribute format	31
Table 6 – M1 safety cyclic transmission attribute format	32
Table 7 – S1 safety cyclic transmission attribute format	33
Table 8 – M1 safety device manager attribute encoding	33
Table 9 – S1 safety device manager attribute encoding	34
Table 10 – M1 safety connection manager attribute encoding	34
Table 11 – S1 safety connection manager attribute encoding	34
Table 12 – M1 safety cyclic transmission attribute encoding	35
Table 13 – S1 safety cyclic transmission attribute encoding	37
Table 14 – Safety master monitor timer operation	41
Table 15 – Safety slave monitor timer operation	41
Table 16 – Safety data monitor timer operation	41
Table 17 – Details of connection establishment and confirmation processing	43
Table 18 – Details of slave information verification processing	43
Table 19 – Details of safety slave parameter transmission processing	44
Table 20 – Monitor LEDs	45
Table 21 – Safety function response time calculation	46
Table 22 – Safety function response time definition of terms	46
Table 23 – Selection of the various measures for possible errors	50
Table 24 – SS-Start	55
Table 25 – SS-Restart	55
Table 26 – SS-InvokeFunc	56
Table 27 – SS-Read	56
Table 28 – SS-Write	57
Table 29 – SS-Terminate	57
Table 30 – Safety PDU elements	58
Table 31 – CTRL Elements	59
Table 32 – State list	65
Table 33 – SFSPM-M timers	70
Table 34 – SFSPM-M state transition table	71
Table 35 – support_functions	74
Table 36 – error_category	77
Table 37 – error_category for AL errors	77
Table 38 – error_code	78

Table 39 – SFSPM-S timers.....	79
Table 40 – SFSPM-S state transition table.....	80
Table 41 – Parameters used by safety communication layer	90
Table 42 – SM-SetSafetyStationInfo	95
Table 43 – Safety station information setting parameters of SM-SetSafetyStationInfo	95
Table 44 – SM-SetSafetyNetworkParameter	96
Table 45 – Safety network parameters of SM-SetSafetyNetworkParameter	96
Table 46 – SM-GetSafetyStationInfo	96
Table 47 – Safety station information parameters of SM-GetSafetyStationInfo (Request).....	97
Table 48 – Safety station information parameters of SM-GetSafetyStationInfo (Response)	97
Table 49 – SM-GetSafetyNetworkParameter	97
Table 50 – Parameters of SM-GetSafetyNetworkParameter request.....	97
Table 51 – Parameters of SM-GetSafetyNetworkParameter response	98
Table 52 – Monitor LEDs	99
Table 53 – Communication port monitor LEDs	99
Table A.1 – Residual error probability for FSCP 8/1 CRC.....	104
Table A.2 – Residual error probability for FSCP 8/2 CRC.....	105

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**INDUSTRIAL COMMUNICATION NETWORKS –
PROFILES –****Part 3-8: Functional safety fieldbuses –
Additional specifications for CPF 8****FOREWORD**

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

IEC 61784-3-8 has been prepared by subcommittee 65C: Industrial networks, of IEC technical committee 65: Industrial-process measurement, control and automation. It is an International Standard.

This third edition cancels and replaces the second edition published in 2016. This edition constitutes a technical revision.

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

- structured for compliance with IEC 61784-3 Ed.4;
- general editorial changes and clarifications;
- safety measures (11.5.3);

- safety application service elements (11.6.2);
- safety PDU format (11.7.1);
- constraints for calculations of system characteristics (11.9.5);
- safety measures (12.5.3);
- safety PDU format (12.7.1);
- behaviour (12.7.2);
- constraints for calculations of system characteristics (12.9.5);
- hash function calculations (Annex A).

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

FDIS	Report on voting
65C/1083/FDIS	65C/1087/RVD

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

The language used for the development of this International Standard is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/standardsdev/publications.

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

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

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

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

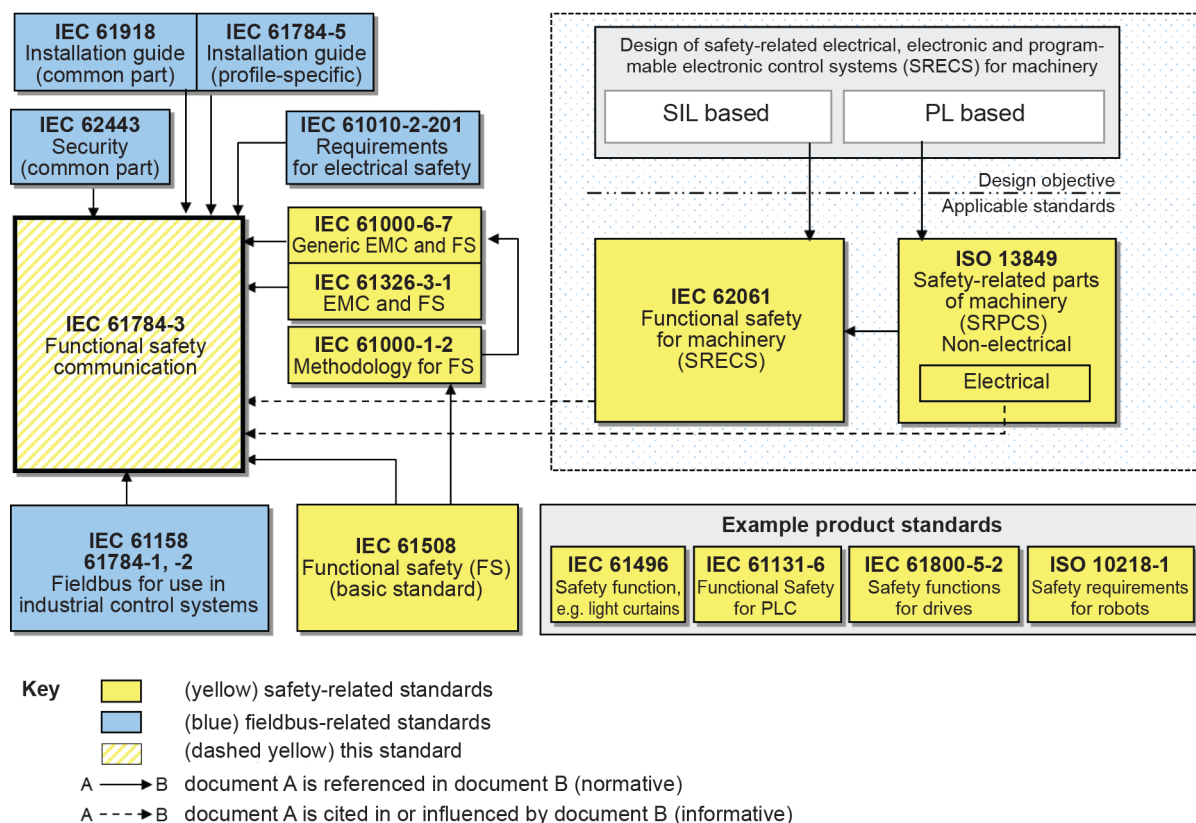
0 Introduction

0.1 General

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

IEC 61784-3 (all parts) explains the relevant principles for functional safety communications with reference to IEC 61508 (all parts) and specifies several safety communication layers (profiles and corresponding protocols) based on the communication profiles and protocol layers of IEC 61784-1, IEC 61784-2 and IEC 61158 (all parts). It does not cover electrical safety and intrinsic safety aspects. It also does not cover security aspects, nor does it provide any requirements for security.

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

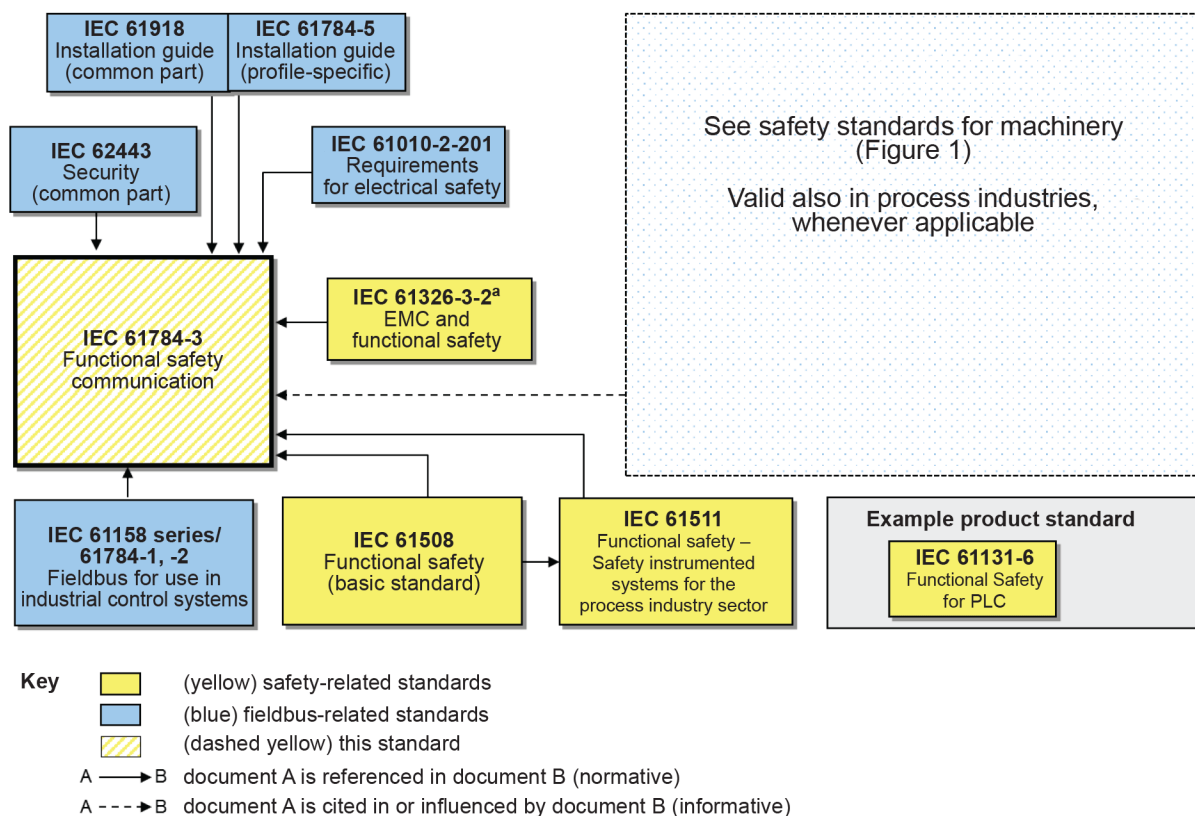


IEC

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

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

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



IEC

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

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

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

Safety communication layers specified in IEC 61784-3 (all parts) do this in such a way that a fieldbus can be used for applications requiring functional safety up to the Safety Integrity Level (SIL) specified by its corresponding functional safety communication profile.

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

IEC 61784-3 (all parts) describes:

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

0.2 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 a patent concerning the functional safety communication profiles for family 8. IEC takes no position concerning the evidence, validity, and scope of this patent right.

The holder of this patent right has assured IEC that s/he is willing to negotiate licences under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statement of the holder of this patent right is registered with IEC. Information may be obtained from the patent database available at <http://patents.iec.ch>.

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

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES –

Part 3-8: Functional safety fieldbuses – Additional specifications for CPF 8

1 Scope

This part of IEC 61784-3 (all parts) specifies a safety communication layer (services and protocol) based on CPF 8 of IEC 61784-1, IEC 61784-2 and IEC 61158 Type 18 and Type 23. It identifies the principles for functional safety communications defined in IEC 61784-3 that are relevant for this safety communication layer. This safety communication layer is intended for implementation in safety devices only.

NOTE 1 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.

This document defines mechanisms for the transmission of safety-relevant messages among participants within a distributed network using fieldbus technology in accordance with the requirements of IEC 61508 (all parts)¹ for functional safety. These mechanisms may be used in various industrial applications such as process control, manufacturing automation and machinery.

This document provides guidelines for both developers and assessors of compliant devices and systems.

NOTE 2 The resulting SIL claim of a system depends on the implementation of the selected functional safety communication profile within this system – implementation of a functional safety communication profile according to this document in a standard device is not sufficient to qualify it as a safety device.

2 Normative references

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

IEC 61131-2, *Industrial-process measurement and control – Programmable controllers – Part 2: Equipment requirements and tests*

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

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

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

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

¹ In the following pages of this document, "IEC 61508" will be used for "IEC 61508 (all parts)".

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

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

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

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

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

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

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

IEC 61784-3:2021, *Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions*

IEC 62061, *Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems*

ISO/IEC/IEEE 8802-3, *Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 3: Standard for Ethernet*

3 Terms, definitions, symbols, abbreviated terms and conventions

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC 61784-3 and the following apply.

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

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

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



3.1.1 Common terms and definitions

NOTE These common terms and definitions are inherited from IEC 61784-3:2021.

3.1.1.1

absolute time stamp

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

[SOURCE: IEC 62280:2014, 3.1.1, modified – use of "devices" and "fieldbus" instead of "entities" and "transmission system"]

3.1.1.2

active network element

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

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

[SOURCE: IEC 61918:2018, 3.1.2]

3.1.1.3

bit error probability

P_e

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

3.1.1.4

black channel

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

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

3.1.1.5

bridge

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

3.1.1.6

closed communication system

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

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

3.1.1.7

communication channel

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

3.1.1.8

communication system

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

3.1.1.9

connection

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

3.1.1.10**Cyclic Redundancy Check****CRC**

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

<method> procedure used to calculate the redundant data

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

Note 2 to entry: See also [26], [27]².

3.1.1.11**defined communication system****defined channel**

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

3.1.1.12**diversity**

different means of performing a required function

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

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

3.1.1.13**DLPDU**

DEPRECATED: frame

Data Link Protocol Data Unit

3.1.1.14**error**

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

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

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

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

3.1.1.15**failure**

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

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

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

² Figures in square brackets refer to the bibliography.

3.1.1.16

fault

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

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

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

3.1.1.17

fieldbus

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

3.1.1.18

fieldbus system

system using a *fieldbus* with connected devices

3.1.1.19

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 [26], [27].

3.1.1.20

hash function

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

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

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

3.1.1.21

hazard

potential source of harm

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

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

3.1.1.22

master

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

3.1.1.23

message

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

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

3.1.1.24**message sink**

information sink

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

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

3.1.1.25**message source**

information source

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

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

3.1.1.26**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]

3.1.1.27**redundancy**

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

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

3.1.1.28**relative time stamp***time stamp* referenced to the local clock of an entity

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

[SOURCE: IEC 62280:2014, 3.1.43, modified – format adjusted]

3.1.1.29**residual error probability**

RP

probability of an *error* undetected by the SCL *safety measures***3.1.1.30****residual error rate**statistical rate at which the SCL *safety measures* fail to detect *errors***3.1.1.31****risk**

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

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

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

3.1.1.32

safety communication channel

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*.

3.1.1.33

safety communication layer

SCL

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

3.1.1.34

safety connection

connection that utilizes the safety protocol for communications transactions

3.1.1.35

safety data

data transmitted across a safety network using a safety protocol

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

3.1.1.36

safety device

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

3.1.1.37

safety function

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

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

3.1.1.38

safety function response time

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

Note 1 to entry: This concept is introduced in IEC 61784-3:2021, 5.2.4 and addressed by the functional safety communication profiles defined in this document.

3.1.1.39

safety integrity level

SIL

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

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

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

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

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

3.1.1.40

safety measure

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

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

Note 2 to entry: Communication *errors* and related safety measures are detailed in IEC 61784-3:2021, 5.3 and 5.4.

3.1.1.41

safety PDU

SPDU

PDU transferred through the *safety communication channel*

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

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

3.1.1.42

safety-related application

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

3.1.1.43

safety-related system

system performing *safety functions* according to IEC 61508

3.1.1.44

slave

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

3.1.1.45

spurious trip

trip caused by the safety system without a process demand

3.1.1.46

timeliness code

time information included in a *message*

3.1.1.47

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.

3.1.1.48

white channel

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

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

3.1.2 CPF 8: Additional terms and definitions

3.1.2.1

cycle

interval at which an activity is repetitively and continuously executed

3.1.2.2

safety application relationship

SAR

application relationship between two or more safety related application relationship endpoints

3.1.2.3

safety application service element

SASE

safety related application service element

3.1.2.4

safety clock

clock (counter) for recording the time of occurrence of events such as the transmission and reception of safety communication related messages

3.1.2.5

safety data monitor timer

timer used by the time expectation function for safety data transmission

3.1.2.6

safety monitor timer

timer used by the time expectation function for safety connection management

3.1.2.7

safety refresh

periodic transmission and reception of safety data between master and slave stations

3.1.2.8

slot

one quantum (granularity) of the position dependent mapping of the cyclic data fields

3.1.2.9

station

device and its corresponding SAREP associated with the transmission and reception of safety data

Note 1 to entry: The station number is used in the position dependent mapping of the cyclic data fields (a station occupies one or more slots).

3.1.2.10

safety protocol transmission information

information distinguishing safety relevant messages

3.2 Symbols and abbreviated terms

3.2.1 Common symbols and abbreviated terms

A-code	Authentication code	
CP	Communication Profile	[IEC 61784-1]
CPF	Communication Profile Family	[IEC 61784-1]
CRC	Cyclic Redundancy Check	
DLL	Data Link Layer	[ISO/IEC 7498-1]
DLPDU	Data Link Protocol Data Unit	
EMC	Electromagnetic Compatibility	
EUC	Equipment Under Control	[IEC 61508-4:2010]
E/E/PE	Electrical/Electronic/Programmable Electronic	[IEC 61508-4:2010]
FAL	Fieldbus Application Layer	[IEC 61158-5 (all parts)]
FS	Functional Safety	
FSCP	Functional Safety Communication Profile	
FSPM	FAL Service Protocol Machine	[IEC 61158-1]
MTBF	Mean Time Between Failures	
MTTF	Mean Time To Failure	
PDU	Protocol Data Unit	[ISO/IEC 7498-1]
Pe	Bit error probability	
PhL	Physical Layer	[ISO/IEC 7498-1]
PL	Performance Level	[ISO 13849-1]
PLC	Programmable Logic Controller	
SCL	Safety Communication Layer	
SIL	Safety Integrity Level	[IEC 61508-4:2010]
SPDU	Safety PDU	
T-code	Timeliness code	

3.2.2 CPF 8: Additional symbols and abbreviated terms

AR	Application Relationship
ASE	Application Service Element
CC	Carry Counter
CID	Connection Identifier
CMD	Command Data
LED	Light Emitting Diode
LID	Link Identifier
OBL	Offset Baseline
RNO	Running Number
SAR	Safety Application Relationship
SAREP	Safety Application Relationship Endpoint
SARPM	Safety Application Relationship Protocol State Machine
SASE	Safety Application Service Element
SFSPM	Safety FSPM (appended with -S Slave or -M Mater)
SRC	Safety Relevant Controller
SRP	Safety Relevant Peripheral
TPI	Safety Transmission Packet Information
TPI-T	Safety Transmission Packet Information from master
TPI-R	Safety Transmission Packet Information from slave
TS	Time Stamp

3.3 Conventions

Conventions used in this document are defined in IEC 61158 Type 18 and Type 23, IEC 61784-1 CPF 8 and IEC 61784-2 CPF 8.

In order to assist the reader familiar with the standard clause numbering and for the purpose of consistency and alignment with IEC 61784-3, Clauses 4 to 10 reference Clauses 11 to 17 for FSCP 8/1 and Clauses 18 to 24 for FSCP 8/2.

4 Overview

For overview information pertaining to FSCP 8/1, see 11.4. For overview information pertaining to FSCP 8/2, see 12.4.

5 General

For general information pertaining to FSCP 8/1, see 11.5. For general information pertaining to FSCP 8/2, see 12.5.

6 Safety communication layer services

For safety communication layer services information pertaining to FSCP 8/1, see 11.6. For safety communication layer services information pertaining to FSCP 8/2, see 12.6.

7 Safety communication layer protocol

For safety communication layer protocol information pertaining to FSCP 8/1, see 11.7. For safety communication layer protocol information pertaining to FSCP 8/2, see 12.7.

8 Safety communication layer management

For safety communication layer management information pertaining to FSCP 8/1, see 11.8. For safety communication layer management information pertaining to FSCP 8/2, see 12.8.

9 System requirements

For system requirements information pertaining to FSCP 8/1, see 11.9. For system requirements information pertaining to FSCP 8/2, see 12.9.

10 Assessment

For assessment information pertaining to FSCP 8/1, see 11.10. For assessment information pertaining to FSCP 8/2, see 12.10.

11 FSCP 8/1

11.1 Scope – FSCP 8/1

See Clause 1.

11.2 Normative references – FSCP 8/1

See Clause 2.

11.3 Terms, definitions, symbols, abbreviated terms and conventions – FSCP 8/1

See Clause 3.

11.4 Overview of FSCP 8/1 (CC-Link Safety™)

Communication Profile Family 8 (commonly known as CC-Link™³) 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™³) is based on the CPF 8 basic profiles in IEC 61784-1 and the safety communication layer specifications defined in this document.

³ CC-Link™ and CC-Link Safety™ are trade names of the non-profit organization CC-Link Partner Association. This information is given for the convenience of users of this document and does not constitute an endorsement by IEC of the trade name holder or any of its products. Compliance to this document does not require use of the trade names CC-Link™ or CC-Link Safety™. Use of the trade names CC-Link™ or CC-Link Safety™ requires permission of CC-Link Partner Association and compliance with conditions for their use (such as testing and validation).

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 is 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 ASEs as specified in this document. However, since inheriting 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.

11.5 General – FSCP 8/1

11.5.1 External documents providing specifications for the profile

Manufacturers of FSCP 8/1 safety devices are encouraged to check documents [30], [31] and [32] which provide additional specifications relevant for implementation of the SCL defined in this document.

11.5.2 Safety functional requirements

This document specifies the services and protocols for a functional safety communication system based on IEC 61158 Type 18. The communication technologies specified in this document shall only be implemented in devices designed in accordance with the requirements of IEC 61508.

The following requirements shall apply to the development of devices that implement FSCP 8/1 protocols. The same requirements were used in the development of FSCP 8/1.

- The FSCP 8/1 protocols are designed to support Safety Integrity Level SIL3 (refer to IEC 61508).
- Implementations of FSCP 8/1 shall comply with IEC 61508.
- The basic requirements for the development of the FSCP 8/1 protocol are specified in IEC 61784-3.
- The safety state for discrete data is the de-energized state (0). For analog values the de-energized state shall be defined by the safety-related application.
- Environmental conditions shall be according to IEC 61131-2 for the basic levels and IEC 61326-3-1, IEC 61326-3-2 for the safety margin tests, unless there are specific product standards.
- Unless specified in this document, the CPF 8 requirements shall be unchanged for safety.

11.5.3 Safety measures

11.5.3.1 General

The safety communication layer described in this document provides the following deterministic remedial measures to implement its safety communication layer:

- sequence number;
- time expectation;
- connection authentication;
- feedback message;

- data integrity assurance;
- redundancy with cross-checking;
- different data integrity assurance systems.

The selection of the various measures for possible errors is shown in Table 1.

Table 1 – Selection of the various measures for possible errors

Communication errors	Deterministic Remedial Measures							
	Sequence Number	Time Stamp	Time Expectation	Connection Authentication	Feedback Message	Data Integrity Assurance	Redundancy With Cross Checking	Different Data Integrity Assurance Systems
Corruption						X	X	
Unintended repetition	X							
Incorrect sequence	X							
Loss	X							
Unacceptable delay			X					
Insertion	X			X	X			
Masquerade				X	X		X	X
Addressing				X				
NOTE Table adapted from IEC 62280:2014								

11.5.3.2 Sequence number

Safety messages contain a sequence number (RNO) with a width of 24 bits and a specified sequence (see 11.7.1 and 11.7.2). This RNO is a combination of RNO-1 (4 bits) RNO-2 (4 bits) and RNO-3 (16 bits). If the sequence is not followed, all safety related output signals shall be set to their safe states.

11.5.3.3 Time expectation

An integrated watchdog timer providing the time expectation of each output channel on each safety output slave ensures a safety function response time, which is the time between the detection of an event at the safety input slave and the response at the corresponding output channel(s) on the safety output slave(s) without the processing time of the safety input. For details see also 11.9.3.

The safety function response time comprises the fieldbus transmission time from a safety input slave to the master and from the safety master to the safety output slave, including possible repetitions of the safety PDU due to transmission errors, the processing time on safety output slave, and the processing time within the safety relevant controller (SRC).

If the safety function response time 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 power OFF state. This shall be observed by the application layer of the SRP.

11.5.3.4 Connection authentication

The connection authentication is implemented by a set of a safety connection ID (Link ID) and a station number. Each safety slave uses a 3 bit Link ID which specifies its safety network system. This provides the SRC with up to 8 safety network systems. The assignment of Link ID values shall be unique within a functional safety communication system. The safety messages always contain the Link ID.

11.5.3.5 Feedback message

A feedback message is provided from each slave that confirms receipt of messages from the master. The feedback message contains error status information from the slave as well as acknowledgment of the RNO, link ID, and command ID.

11.5.3.6 Data integrity assurance

Data integrity is assured using the CRCs included in the safety PDU. The transmitting node sends the safety PDU including its calculated CRCs. The receiving node compares the CRCs included in the received safety PDU with the CRCs calculated from the received safety PDU, and determines if corruption occurred.

11.5.3.7 Redundancy with cross checking

The receiving node cross checks the redundant portions of the received safety PDU to verify that these portions match each other bit-for-bit.

11.5.3.8 Different data integrity assurance system

Distinction between safety relevant messages and non-safety relevant messages: Safety messages contain a CRC checksum (32 bits). The IEC 61158 Type 18 protocol uses a different CRC algorithm (16-bit CRC). Additionally, each telegram contains an 8-bit command ID, a 3-bit link ID and a 24-bit RNO and each of these components shall conform to the restrictions as defined for these fields.

11.5.4 Safety communication layer structure

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 herein. Since they inherit directly from the parent classes defined for CPF 8, these SASEs specify additions to CPF 8. The SASEs are implemented based on the following:

- Device manager – ASE class specifications for M1 and S1 type device manager;
- Connection manager – AR class definition for M1 and S1 type connection manager;
- Cyclic transmission – Process data AR ASE class specification for M1 and S1 type cyclic transmission.

The SCL augments these ASE definitions with:

- M1 and S1 type safety device manager;
- M1 and S1 type safety connection manager;
- M1 and S1 type safety cyclic transmission.

All management, behaviors and functions of the SCL are handled with these safety application service elements.

11.5.5 Relationships with FAL (and DLL, PhL)

11.5.5.1 Overview

Figure 3 shows the relationship between the SCL and the other layers of the IEC 61158 Type 18 communication stack.

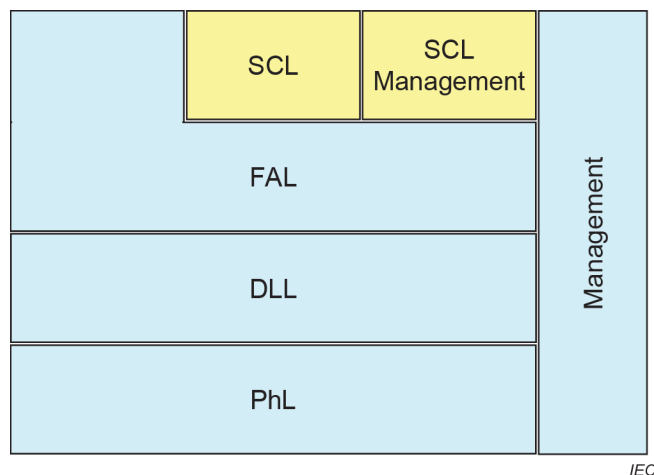


Figure 3 – Relationship between SCL and the other layers of IEC 61158 Type 18

11.5.5.2 Data types

Data types of safety data are specified in IEC 61158-5-18.

11.6 Safety communication layer services for FSCP 8/1

11.6.1 General

The FSCP 8/1 SAR uses buffered transport for process data inputs and outputs. Transmission triggering type services are required depending upon the configuration of the instantiated objects. Connection management is handled by the safety connection manager class. Safety-related applications use safety application service elements to communicate via the safety communication layer. The formal model of these service elements is defined in 11.6.

11.6.2 SASEs

11.6.2.1 M1 safety device manager class specification

The M1 safety device manager class supports a master type SCL user on a polled type DL implementation.

SCL ASE:			Management SASE
CLASS:			M1 safety device manager
CLASS ID:			not used
PARENT CLASS:			M1 device manager
ATTRIBUTES:			
1	(m)	Attribute:	Management information
1.1	(m)	Attribute:	Link id
1.2	(o)	Attribute:	Software/protocol version
2	(m)	Attribute:	Connected slaves management information
2.1	(m)	Attribute:	Software/protocol version 1
...	...	...	...
2.n	(m)	Attribute:	Software/protocol version n

...	...	...	...
2.64	(m)	Attribute:	Software/protocol version 64

11.6.2.2 S1 safety device manager class specification

The S1 safety device manager class supports a slave type SCL user on a polled type DL implementation.

SCL ASE:			Management SASE
CLASS:			S1 safety device manager
CLASS ID:			not used
PARENT CLASS:			S1 device manager
ATTRIBUTES:			
1	(m)	Attribute:	Management information
1.1	(m)	Attribute:	Link id
1.2	(m)	Attribute:	Software/protocol version

11.6.3 SARs

11.6.3.1 M1 safety connection manager class

The M1 safety connection manager class supports a master type SCL user on a polled type DL implementation.

SCL ASE:			Management SASE
CLASS:			M1 safety connection manager
CLASS ID:			not used
PARENT CLASS:			M1 connection manager
ATTRIBUTES:			
1	(m)	Attribute:	Parameter information
1.1	(m)	Attribute:	Safety monitor timer value
1.2	(m)	Attribute:	Safety data monitor timer value
1.3	(m)	Attribute:	Safety slave specification
1.4	(m)	Attribute:	Safety slave specification source
1.5	(m)	Attribute:	Safety slave product information
2	(m)	Attribute:	Safety slave parameter data
3	(m)	Attribute:	Safety slave link status

11.6.3.2 S1 safety connection manager class

The S1 safety connection manager class supports a slave type SCL user on a polled type DL implementation.

SCL ASE:	Management SASE
CLASS:	S1 safety connection manager
CLASS ID:	not used
PARENT CLASS:	S1 connection manager
ATTRIBUTES:	
1	(m) Attribute: Safety product information
2	(m) Attribute: Safety slave parameter data

11.6.4 Process data SAR ASEs

11.6.4.1 M1 safety cyclic transmission class specification

The M1 safety cyclic transmission class supports a master type SCL user in association with an M1 safety connection manager.

SCL ASE:	Process Data SAR ASE
CLASS:	M1 safety cyclic transmission
CLASS ID:	not used
PARENT CLASS:	M1 cyclic transmission
ATTRIBUTES:	
1.	(m) Attribute: Data out
1.1.	(m) Attribute: Safety RY data
1.2.	(m) Attribute: RWw data
1.2.1.	(m) Attribute: Safety RWw data
1.2.2.	(m) Attribute: Safety TPI-T
1.3.	(m) Attribute: Safety RY-r data
1.4.	(m) Attribute: RWw-r data
1.4.1.	(m) Attribute: Safety RWw-r data
1.4.2.	(m) Attribute: Safety TPI-T-r
2.	(m) Attribute: Data in
2.1.	(m) Attribute: Safety data in 1
2.1.1.	(m) Attribute: Safety RX data 1
2.1.2.	(m) Attribute: RWr data 1
2.1.2.1	(m) Attribute: Safety RWr data 1
2.1.2.2	(m) Attribute: Safety TPI-R 1
2.1.3.	(m) Attribute: Safety RX-r data 1
2.1.4.	(m) Attribute: RWr-r data 1
2.1.4.1	(m) Attribute: Safety RWr-r data 1
2.1.4.2	(m) Attribute: Safety TPI-R-r 1
...	...
2.n.	(m) Attribute: Safety data in n
...	...
2.64.	(m) Attribute: Safety data in 64

11.6.4.2 S1 safety cyclic transmission class specification

The S1 safety cyclic transmission class supports a slave type SCL user in association with an S1 safety connection manager.

SCL ASE:		Process Data SAR ASE
CLASS:		S1 safety cyclic transmission
CLASS ID:		not used
PARENT CLASS:		S1 cyclic transmission
ATTRIBUTES:		
1.	(m)	Attribute: Data out
1.1	(m)	Attribute: Safety RY data
1.2	(m)	Attribute: RWw data
1.2.1.	(m)	Attribute: Safety RWw data
1.2.2.	(m)	Attribute: Safety TPI-T
1.3	(m)	Attribute: Safety RY-r data
1.4	(m)	Attribute: RWw-r data
1.4.1.	(m)	Attribute: Safety RWw-r data
1.4.2.	(m)	Attribute: Safety TPI-T-r
2.	(m)	Attribute: Data in
2.1	(m)	Attribute: Safety RX data
2.2	(m)	Attribute: RWr data
2.2.1	(m)	Attribute: Safety RWr data
2.2.2	(m)	Attribute: Safety TPI-R
2.3	(m)	Attribute: Safety RX-r data
2.4	(m)	Attribute: RWr-r data
2.4.1	(m)	Attribute: Safety RWr-r data
2.4.2	(m)	Attribute: Safety TPI-R-r

11.7 Safety communication layer protocol for FSCP 8/1

11.7.1 Safety PDU format

11.7.1.1 General

The safety PDU syntax and encoding is described as in IEC 61158-6-18 in terms of abstract syntax and transfer syntax.

11.7.1.2 Abstract syntax

11.7.1.2.1 M1 safety device manager PDU abstract syntax

The abstract syntax for attributes belonging to this class is described in Table 2.