

INTERNATIONAL STANDARD

NORME INTERNATIONALE



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

**Réseaux de communication industriels – Profils –
Partie 3-8: Bus de terrain de sécurité fonctionnelle – Spécifications
supplémentaires pour CPF 8**



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2021 IEC, Geneva, Switzerland

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

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

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

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

About the IEC

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

About IEC publications

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

IEC publications search - webstore.iec.ch/advsearchform

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 It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

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

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

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

IEC online collection - oc.iec.ch

Discover our powerful search engine and read freely all the publications previews. With a subscription you will always have access to up to date content tailored to your needs.

Electropedia - www.electropedia.org

The world's leading online dictionary on electrotechnology, containing more than 22 000 terminological entries in English and French, with equivalent terms in 18 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

A propos de l'IEC

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

A propos des publications IEC

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

Recherche de publications IEC - webstore.iec.ch/advsearchform

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

IEC Just Published - webstore.iec.ch/justpublished

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

Service Clients - webstore.iec.ch/csc

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

IEC online collection - oc.iec.ch

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

Electropedia - www.electropedia.org

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

INTERNATIONAL STANDARD

NORME INTERNATIONALE



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

**Réseaux de communication industriels – Profils –
Partie 3-8: Bus de terrain de sécurité fonctionnelle – Spécifications
supplémentaires pour CPF 8**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 25.040.40; 35.100.05

ISBN 978-2-8322-9751-3

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

CONTENTS

FOREWORD	7
0 Introduction	9
0.1 General.....	9
0.2 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.

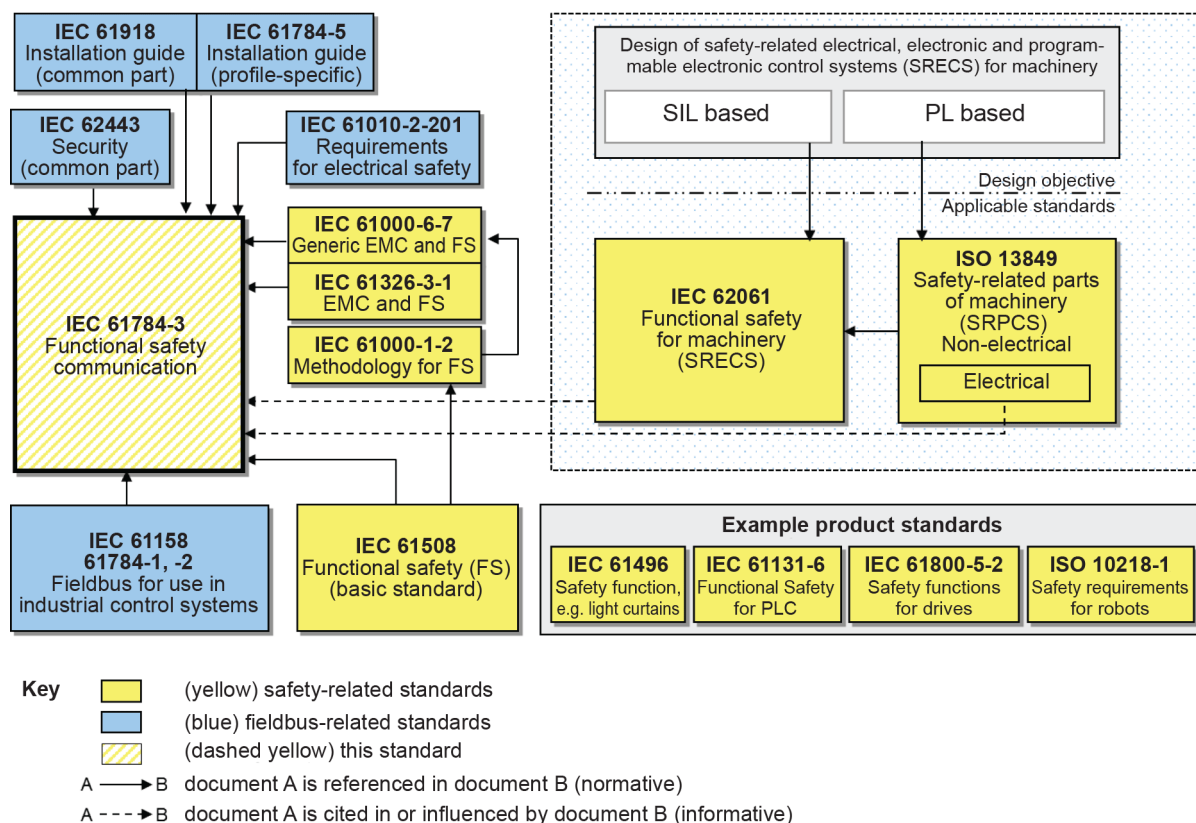
0 Introduction

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.

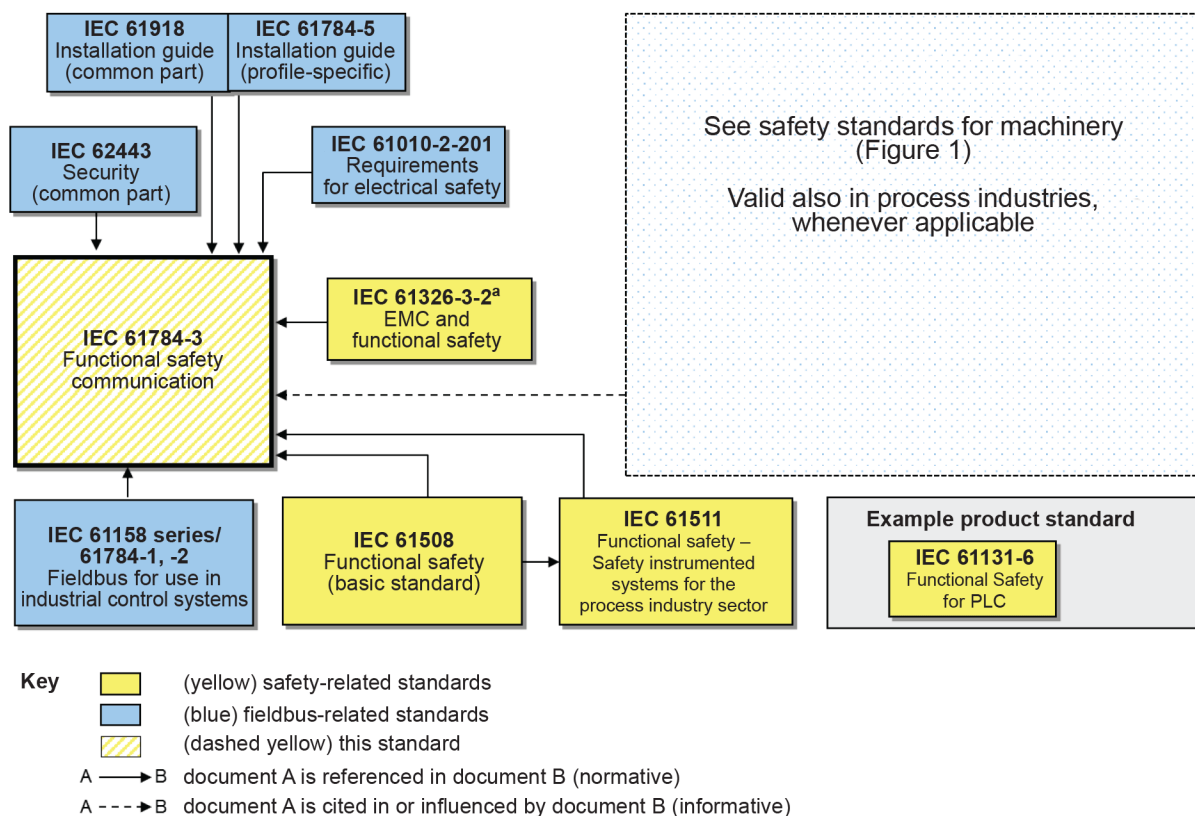


IEC

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.

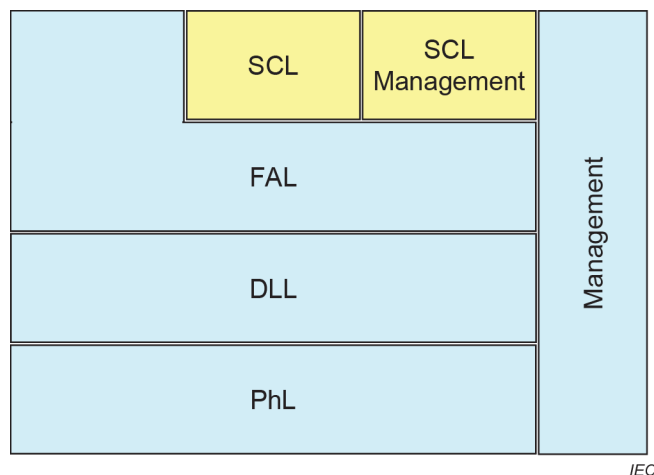


Figure 3 – Relationship between SCL and the other layers of IEC 61158 Type 18

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.

Table 2 – M1 safety device manager attribute format

Attribute	Format	Size (bits)
Management information	Structure of 2 elements:	11
Link id	Unsigned3	3
Software/protocol version	1 octet, bit mapped	8
Connected slave management information	Array of 64 members:	64 octets
Software/protocol version	1 octet, bit mapped	8

11.7.1.2.2 S1 safety device manager PDU abstract syntax

The abstract syntax for attributes belonging to this class is described in Table 3.

Table 3 – S1 safety device manager attribute format

Attribute	Format	Size (bits)
Management information	Structure of 3 elements:	11
Link id	Unsigned3	3
Software/protocol version	1 octet, bit mapped	8

11.7.1.2.3 M1 safety connection manager PDU abstract syntax

The abstract syntax for attributes belonging to this class is described in Table 4.

Table 4 – M1 safety connection manager attribute format

Attribute	Format	Size (bits)
Parameter information	Structure of 5 elements:	2 004 octets
Safety monitor timer value	Unsigned16	16
Safety data monitor timer value	Unsigned16	16
Safety slave specification	8 octets, bit mapped	64
Safety slave specification source	8 octets, bit mapped	64
Safety slave product information	Array of 64 members:	1 984 octets
Safety product information 1 – 64	Word oriented data structure	31 octets
Safety slave parameter data	16 – 52 224 octets	16 – 52 224 octets
Safety slave link status	8 octets, bit mapped	64

11.7.1.2.4 S1 safety connection manager PDU abstract syntax

The abstract syntax for attributes belonging to this class is described in Table 5.

Table 5 – S1 safety connection manager attribute format

Attribute	Format	Size (bits)
Safety product information 1 – 64	Word oriented data structure	31 octets
Safety slave parameter data	16 – 816 octets	16 – 816 octets

11.7.1.2.5 M1 safety cyclic transmission PDU abstract syntax

The abstract syntax for attributes belonging to this class is described in Table 6.

Table 6 – M1 safety cyclic transmission attribute format

Attribute	Format	Size (bits)
Data out	Structure of 2 elements:	192 × n
Safety RY data	Bit-oriented data structure	32 × n
RWw data	Word-oriented data structure	64 × n
Safety RWw data	Word-oriented data	64 × (n – m)
Safety TPI-T	Safety transmission packet information	64 × m
Safety RY-r data	Bit-oriented data structure	32 × n
RWw-r data	Word-oriented data structure	64 × n
Safety RWw-r data	Word-oriented data	64 × (n – m)
Safety TPI-T-r	Safety transmission packet information	64 × m
Data in	Structure of n elements	192 × n
Safety data in 1	Structure of 2 elements	192
Safety RX data	Bit-oriented data structure	64
RWr data	Word-oriented data structure	128
Safety RWr data	Word-oriented data	64
Safety TPI-R	Safety transmission packet information	64
Safety RX-r data	Bit-oriented data structure	32
RWr-r data	Word-oriented data structure	64
Safety RWr-r data	Word-oriented data	64
Safety TPI-R-r	Safety transmission packet information	64
...	...	...
Safety data in n	Structure of 2 elements	192
NOTE The values of n and m are dependent upon the values of the corresponding configuration settings in the master status.		

11.7.1.2.6 S1 safety cyclic transmission PDU abstract syntax

The abstract syntax for attributes belonging to this class is described in Table 7.

Table 7 – S1 safety cyclic transmission attribute format

Attribute	Format	Size (bits)
Data out	Structure of 2 elements:	192
Safety RY data	Bit-oriented data structure	32
RWw data	Word-oriented data structure	64
Safety RWw data	Word-oriented data	64
Safety TPI-T	Safety transmission packet information	64
Safety RY-r data	Bit-oriented data structure	32
RWw-r data	Word-oriented data structure	64
Safety RWw-r data	Word-oriented data	64
Safety TPI-T-r	Safety transmission packet information	64
Data in	Structure of 2 elements:	192
Safety RX data	Bit-oriented data structure	64
RWr data	Word-oriented data structure	128
Safety RWr data	Word-oriented data	64
Safety TPI-R	Safety transmission packet information	64
Safety RX-r data	Bit-oriented data structure	64
RWr-r data	Word-oriented data structure	128
Safety RWr-r data	Word-oriented data	64
Safety TPI-R-r	Safety transmission packet information	64

11.7.1.3 Transfer syntax

11.7.1.3.1 M1 safety device manager PDU encoding

The specific PDU encoding for attributes belonging to this class is described in Table 8.

Table 8 – M1 safety device manager attribute encoding

Attribute	Encoding		
Management information	Specifies the configuration of the master device		
Link id	0 – 7 = allowable range		
Software/protocol version	Bit	Description	Value
	5 – 0	Software version	1 – 63 = allowable range
	7 – 6	Protocol version	0 = Version 1 1 = Version 2 2 = Version 3 3 = Version 4
Connected slave management information	Specifies the configuration of the connected slaves		
Slave information 1 – 64	Array of 64 elements, each encoded as:		
Software/protocol version	Bit	Description	Value
	5 – 0	Software version	1 – 63 = allowable range
	7 – 6	Protocol version	0 = Version 1 1 = Version 2 2 = Version 3 3 = Version 4

11.7.1.3.2 S1 safety device manager PDU encoding

The specific PDU encoding for attributes belonging to this class is described in Table 9.

Table 9 – S1 safety device manager attribute encoding

Attribute	Encoding		
Management information	Specifies the configuration of the master device		
Link id	0 – 7 = allowable range		
Software/protocol version	Bit	Description	Value
	5 – 0	Software version	1 – 63 = allowable range
	7 – 6	Protocol version	0 = Version 1 1 = Version 2 2 = Version 3 3 = Version 4

11.7.1.3.3 M1 safety connection manager PDU encoding

The specific PDU encoding for attributes belonging to this class is described in Table 10.

Table 10 – M1 safety connection manager attribute encoding

Attribute	Encoding
Parameter information	Specifies the connection configuration
Safety monitor timer value	1 – 65 535 = ms
Safety data monitor timer value	1 – 65 535 = ms
Safety slave specification	Bit 0 – 63 correspond to slot 1 – 64, where: 0 = SCL not supported 1 = SCL supported
Safety slave specification source	Bit 0 – 63 correspond to slot 1 – 64, where: 0 = SCL-user specification not supported 1 = SCL-user specification supported
Safety slave product information 1 – 64	Array of 64 elements, each encoded as:
Safety product information	31 octets of data for safety product information
Safety parameter data	0 – 52 224 octets of data for slave memory access
Safety slave link status	Bit 0 – 63 correspond to slot 1 – 64, where: 0 = Safety slave station not running 1 = Safety slave station running

11.7.1.3.4 S1 safety connection manager PDU encoding

The specific PDU encoding for attributes belonging to this class is described in Table 11.

Table 11 – S1 safety connection manager attribute encoding

Attribute	Encoding
Safety product information	31 octets of data for safety product information
Safety parameter data	0 – 816 octets of data for slave memory access

11.7.1.3.5 M1 safety cyclic transmission PDU encoding

The specific PDU encoding for attributes belonging to this class is described in Table 12.

Table 12 – M1 safety cyclic transmission attribute encoding

Attribute	Encoding			
Data out	Process data registers set by the master for slave device output			
Safety RY data	A position mapped field of bit-oriented output data for all connected slave devices ordered by slot with 32 bits			
RWw data	A position mapped field into which is mapped: word-oriented output data for all connected safety slave devices and the safety transmission packet information for transmission to the safety slave devices			
Safety RWw data	A position mapped field of word-oriented output data for all connected slave devices. Contains 4 words per slot beginning with the second slot. This is because the following field occupies the space allocated for the first slot in a non-safety slave			
Safety TPI-T	Octet	Bit	Description	Values
	0 – 1	–	RNO-3	0 – 65 535
	2 – 3	0 – 3	RNO-1	0 – 15
		4 – 6	Link id	0 – 7
		7	reserved	0
		8 – 11	Transmission data type	0 – 15
		12	Busy flag	0 = busy 1 = not busy
		13	reserved	0
		14	Read request	0 = no request 1 = request
		15	SCL-user application mode	0 = test mode 1 = safety mode
	4 – 7	–	CRC32-A	CRC32-A
Safety RY-r data	same as RY			
RWw-r data	same as RWw			
Safety RWw-r data	same as Safety RWw			
Safety TPI-T-r	Octet	Bit	Description	Values
	0 – 1	–	Tx/Rx (A-code)	255 / 1 – 64
	2 – 3	0 – 3	RNO-2	0 – 15
		4 – 15	same as Safety TPI-T	
	4 – 7	–	CRC32-B	CRC32-B
Data in	Process data registers read by the master representing slave device inputs			
Safety data in	Process data registers read by the master representing safety slave device inputs			
Safety RX data	A field containing the bit-oriented input data from slave device n ordered by slot with 32 bits			
RWr data	A field containing the word-oriented input data from slave device n ordered by slot with 4 words			

Attribute	Encoding		
Safety RWr data	A position mapped field of word-oriented input data from slave device n. Contains 4 words per slot beginning with the second slot. This is because the following field occupies the space allocated for the first slot in a non-safety slave		
Safety TPI-R	Bit	Description	Values
	0 – 15	RNO-3	0 – 65 535
	16 – 19	RNO-1	0 – 15
	20 – 22	Link id	0 – 7
	23	reserved	0
	24 – 27	Transmission data type	0 – 15
	28	Busy flag	0 = busy 1 = not busy
	29	Error notification	0 = no error 1 = error
	30	reserved	0
	31	SCL-user application mode	0 = test mode 1 = safety mode
	32 – 63	CRC32-A	CRC32-A
Safety RX-r data	same as Safety RX		
RWr-r data	same as RWr		
Safety RWr-r data	same as Safety RWr		
Safety TPI-R-r	Bit	Description	Values
	0 – 15	Tx/Rx (A-code)	255 / 1 – 64
	16 – 19	RNO-2	0 – 15
	20 – 31	same as Safety TPI-R	
	32 – 63	CRC32-B	CRC32-B
NOTE The value of RNO is derived by combining the RNO subparts as follows: RNO-1 = RNO bits 0-3 RNO-2 = RNO bits 4-7 RNO-3 = RNO bits 8-23			

11.7.1.3.6 S1 safety cyclic transmission PDU encoding

The specific PDU encoding for attributes belonging to this class is described in Table 13.

Table 13 – S1 safety cyclic transmission attribute encoding

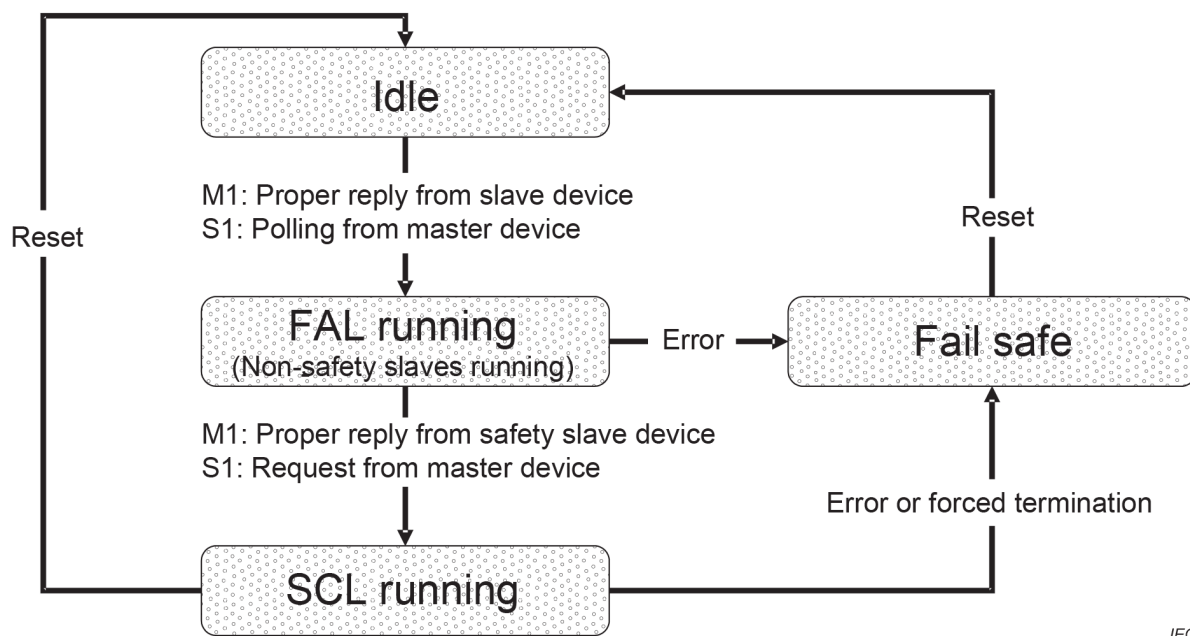
Attribute	Encoding		
Data out	The process data received from the master		
Safety RY data	A field containing the bit-oriented input data ordered by slot with 32 bits		
RWw data	A position mapped field into which is mapped: word-oriented output data (optionally) and the safety transmission packet information as received from the master		
Safety RWw data	A position mapped field of word-oriented output data for the slave device. Contains 4 words per slot beginning with the second slot. This is because the following field occupies the space allocated for the first slot in a non-safety slave		
Safety TPI-T	Bit	Description	Values
	0 – 15	RNO-3	0 – 65 535
	16 – 19	RNO-1	0 – 15
	20 – 22	Link id	0 – 7
	23	reserved	0
	24 – 27	Transmission data type	0 – 15
	28	Busy flag	0 = busy 1 = not busy
	29	reserved	0
	30	Read request	0 = no request 1 = request
	31	SCL-user application mode	0 = test mode 1 = safety mode
	32 – 63	CRC32-A	CRC32-A
Safety RY-r data	same as Safety RY		
RWw-r data	same as RWw		
Safety RWw-r data	same as Safety RWw		
Safety TPI-T-r	Bit	Description	Values
	0 – 15	Tx/Rx (A-code)	1 – 64 / 255
	16 – 19	RNO-2	0 – 15
	20 – 31	same as Safety TPI-T	
	32 – 63	CRC32-B	CRC32-B
Data in	The process data transmitted to the master		
Safety RX data	A field containing the bit-oriented input data ordered by slot with 32 bits		
RWr data	A field containing the word-oriented input data from the master.		
Safety RWr data	A position mapped field of word-oriented input data for the slave device. Contains 4 words per slot beginning with the second slot. This is because the following field occupies the space allocated for the first slot in a non-safety slave		

Attribute	Encoding		
Safety TPI-R	Bit	Description	Values
	0 – 15	RNO-3	0 – 65 535
	16 – 19	RNO-1	0 – 15
	20 – 22	Link id	0 – 7
	23	reserved	0
	24 – 27	Transmission data type	0 – 15
	28	Busy flag	0 = busy 1 = not busy
	29	Error notification	0 = no error 1 = error
	30	reserved	0
	31	SCL-user application mode	0 = test mode 1 = safety mode
	32 – 63	CRC32-A	CRC32-A
Safety RX-r data	same as Safety RX		
RWr-r data	same as RWr		
Safety RWr-r data	same as Safety RWr		
Safety TPI-R-r	Bit	Description	Values
	0 – 15	Tx/Rx (A-code)	1 – 64 / 255
	16 – 19	RNO-2	0 – 15
	20 – 31	same as Safety TPI-R	
	32 – 63	CRC32-B	CRC32-B
NOTE The value of RNO is derived by combining the RNO subparts as follows: RNO-1 = RNO bits 0-3 RNO-2 = RNO bits 4-7 RNO-3 = RNO bits 8-23			

11.7.2 State description

11.7.2.1 Overview

The SCL state model is extended from IEC 61158 Type 18 with a safe state, shown in Figure 4 as Fail safe state. The safe state is entered upon error conditions and is configured to ensure all outputs are maintained in safe states: digital outputs are low, zero, or off, and analog outputs are held at a safe level previously configured by the SCL user. The M1 safety master device manages the states of each safety slave device individually.



IEC

Figure 4 – State diagram

The general method of connection establishment, slave verification, and data refresh is also extended beyond that of IEC 61158 Type 18 and includes safety parameter transmission and processing (see SCL management in 11.8) and safety data transmission and confirmation monitoring.

11.7.2.2 Idle

11.7.2.2.1 Overview

The idle state exists prior to any FAL communications among devices.

11.7.2.2.2 Transition

Upon an appropriate request from the FAL user to the M1 safety master device, receipt of a proper reply from the S1 safety slave device yields a transition from the idle state to the FAL running state.

Upon the receipt of polling communications from the M1 safety master, the S1 safety slave device transitions to the FAL running state.

11.7.2.3 FAL running

11.7.2.3.1 Overview

In the FAL running state, the M1 safety master devices and S1 safety slave devices have established non-safety communications.

11.7.2.3.2 Transition

Upon receipt of request from the M1 safety master, the S1 safety slave transitions to the SCL running state.

Upon receipt of appropriate responses from the S1 safety slave devices, the M1 safety master transitions to the SCL running state.

Any condition of error or fault while in the FAL running state or failed attempt to transition to the SCL running state causes a FSCP 8/1 device to transition to the fail safe state.

11.7.2.4 SCL running

11.7.2.4.1 Overview

The details of the SCL running state are explained in 11.8.

11.7.2.4.2 Transition

As explained in 11.7.2.6, a FSCP 8/1 device transitions to the fail safe state upon detection of an error by any of the following safety measures:

- sequence number;
- time expectation;
- connection authentication;
- feedback message;
- data integrity assurance;
- redundancy with cross checking;
- different data integrity assurance systems.

As explained in 11.7.2.7, a FSCP 8/1 device transitions to the fail safe state upon receipt of a forced termination request.

11.7.2.5 Fail safe

11.7.2.5.1 Overview

The fail safe state is one where all outputs are held in their safe state. For digital outputs, unless otherwise specified, this is the off (or zero or low) state, and for analog outputs, unless otherwise specified, this is the zero output (i.e., no voltage and/or no current) state. Typically, analog outputs will be configured with a safe value that is imposed on the output when in the fail safe state.

11.7.2.5.2 Transition

Exit from the fail safe state is only possible via slave reset.

11.7.2.6 Safety data transmission and processing

11.7.2.6.1 Overview

The SCL of FSCP 8/1 provides the following safety measures:

- sequence number;
- time expectation;
- connection authentication;
- feedback message;
- data integrity assurance;
- redundancy with cross checking;
- different data integrity assurance systems.

The safety master and each safety slave manages and analyzes safety transmissions in order to verify their integrity.

11.7.2.6.2 Sequence number

Safety messages contain a sequence number (RNO) with a width of 24 bits and a specified sequence. The RNO is incremented and transmitted by the safety master. The safety slave echoes the received RNO. If an out of sequence RNO is received, the safety slave is transitioned to the safe state.

11.7.2.6.3 Time expectation

The SCL uses a safety monitor timer and safety data monitor timers to ensure reliable and continuous communications. SLC management configures the timer with a value in the range of 1 ms to 65 535 ms.

The safety monitor timer is used for confirming that safety cyclic communication is being performed normally, and the safety data monitor timers are used for confirming that successive safety cyclic communications are being performed normally. Safety stations monitor the reception interval of the cyclic data that is protected by the normal safety data protection information by this safety monitor timer. Additionally, safety slave stations monitor the reception intervals of the cyclic data that are protected by the normal safety data protection information by the safety data monitor timers.

Table 14, Table 15, and Table 16 describe the operation of the safety monitor timer for both safety master and safety slave devices.

Table 14 – Safety master monitor timer operation

Startup	Termination	Error termination
Sending of safety data (RNO ≠ 0)	Reception of slave response (refresh) data (of the same RNO as send RNO) to which safety data protection information has been properly added	(1) At occurrence of a monitoring timeout (2) At detection of an RNO error

Table 15 – Safety slave monitor timer operation

Startup	Reset	Termination
Reception of safety data (CMD ID=01h)	Reception of master station polling and refresh data (previously RNO+1) to which safety data protection information has been properly added	(1) At occurrence of a monitoring timeout (2) At detection of an RNO error (3) At reception of a forced termination request

Table 16 – Safety data monitor timer operation

Startup	Reset	Termination
Reception of safety cyclic I/O data (CMD ID = 0Fh)	Reception of master station polling and refresh data (previously RNO+2) to which safety data protection information has been properly added	(1) At occurrence of a monitoring timeout (2) At detection of an RNO error (3) At reception of a forced termination request
NOTE Safety slave stations have two safety data monitor timers. A safety data monitor timer starts up upon reception of safety cyclic I/O data (CMS ID=0Fh and RNO=n), and reception of two successive data (RNO=n+2) resets it. The other safety data monitor timer starts up upon reception of safety cyclic I/O data (CMD ID=0Fh and RNO=n+1), and reception of two successive data (RNO=n+3) reset it.		

The behavior of a safety master upon expiration of the safety monitor timer is specified as:

- 1) Failsafe processing such as the clearing of S-RX delivered to the SCL user to zero.
- 2) Error notification to SCL user.
- 3) Transition to the idle state.

The behavior of a safety slave upon expiration of the safety monitor timer is specified as:

- 1) Failsafe processing such as the termination of output to external devices.
- 2) Error notification to SCL user.
- 3) Transition to the safe state.

11.7.2.6.4 Connection authentication

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.

Additionally, the transmitted 16-bit logical connection ID is appended to the SPDU for validation. This field, which is comprised of Tx (8-bit source ID) and Rx (8-bit destination ID), is checked for correctness and also included in the data integrity measures.

11.7.2.6.5 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.

11.7.2.6.6 Data integrity

The CRC32 for FSCP 8/1 is calculated as described in Annex A. The residual error rate for FSCP 8/1 is calculated in accordance with IEC 61784-3.

11.7.2.6.7 Redundancy with cross checking

The redundant data fields are compared bit-for-bit to their counterparts.

11.7.2.6.8 Different data integrity assurance system

The distinction between safety relevant and non-safety relevant messages is ensured by validating the uniqueness of safety messages to contain a properly formatted CRC checksum (32 bits), an 8-bit command ID, a 3-bit link ID and a 24-bit RNO.

The IEC 61158 Type 18 protocol uses a different CRC algorithm (16-bit CRC) and no inclusion of command ID, link ID or RNO.

11.7.2.7 Forced termination

Forced termination processing is used when the safety master requests a safety slave to terminate communication. The safety slave that receives the forced termination request transitions to the fail safe state (stopping external output) and then immediately terminates communication.

11.8 Safety communication layer management for FSCP 8/1

11.8.1 General

Safety-related applications use the following services to configure the safety communication system:

- establish connection;
- verify slave configuration;
- safety slave parameter transmission.

11.8.2 Connection establishment and confirmation processing

Upon connection establishment, initial configuration is confirmed by validating that the SAREPs reside in safety devices and that safety cyclic transmission is supported. This process is described in Table 17.

Table 17 – Details of connection establishment and confirmation processing

SAREP type	Details of processing
Safety master	(1) Confirm that the slave is a safety slave device. (This is confirmed by communicating the safety cyclic data.) (2) Confirm that the safety slave has received the establish connection command. (This is confirmed by checking that the CMD of the response data are identical with the send data.) (3) Transmit the safety monitor timer value.
Safety slave	(1) Confirm that the master is a safety master device. (This is confirmed by communicating the safety cyclic data.) (2) Receive the safety monitor timer value and registers the value internally.

The safety master station transmits $RNO = 0$ when sending the establish connection command.

11.8.3 Safety slave verification

11.8.3.1 General

Product information verification processing confirms that the connected safety slave stations match the safety slave stations currently set to the network parameters of the safety master station to detect misconnections and misconfiguration. A replacement slave device that is not a safety slave, is detected and disabled at start-up.

11.8.3.2 Safety slave information verification process

The safety slave information verification process is described in Table 18.

Table 18 – Details of slave information verification processing

SAREP type	Details of processing
Safety master	(1) Read the product information from safety slaves, and verify that information against product information set to network parameters. (2) After verification, send the product information to safety slave stations.
Safety slave	(1) Verify the product information of the slave against the product information received from the safety master.

Slave information verification processing verifies safety slave product information.

11.8.3.3 Safety slave parameter transmission

Safety slave configuration parameters are transmitted from the safety master to each safety slave. This process is described in Table 19.

Table 19 – Details of safety slave parameter transmission processing

SAREP type	Details of processing
Safety master	(1) Read the CRC32 of the ROM storage parameters from the safety slave stations, and verify this CRC32 with the CRC32 of the ROM storage parameters registered from the SCL user. (2) Send the safety slave parameters to the safety slave.
Safety slave	(1) Receive the safety slave parameters from the safety master, confirm the setting values, and perform internal registration processing.

11.9 System requirements for FSCP 8/1

11.9.1 Indicators and switches

11.9.1.1 Switches

Each safety device shall provide physical means for setting the following:

- Online – Set this mode to establish a data link.
- Station number – 0: Safety master, 1 to 64: Safety slave – required for safety slave only.
- Link ID – 0 to 7
- Baud rate – 156 kbit/s, 625 kbit/s, 2,5 Mbit/s, 5 Mbit/s, 10 Mbit/s – required for safety master only.
- Reset – required for safety slave only

and optionally provides physical means for setting the following:

- Number of occupied slots – Station slots (1 or 2) occupied by one safety slave station.
- Line test 1 – Verifies that the master is able to connect to all slave stations.
- Line test 2 – Verifies that the master is able to connect to a specific slave station.
- Parameter check test – Verifies the parameter content.
- Hardware test – Verifies each individual module for normal operation.

11.9.1.2 Indicators

Indicator requirements are specified in Table 20 with the following interpretation:

- M = mandatory
- O = optional

Indicator type, color and shape are not specified. Also, where computers or other devices with screens are used, indication may be supported via indication on the screen.

Table 20 – Monitor LEDs

No.	LED Name	Description	Safety master station	Safety remote device station	Safety remote I/O station
1	RUN	Lit: Module normal Out: Watchdog timer error	M	O	O
2	ERR	Lit: Communication with all stations error This LED lights when one of the following occurs: · Switch setting error · Master station duplicated on same line · Parameter content error · Data link monitor timer activated · Cable wire break Or cable influenced by noise on the transmission path Flashing: Communication error	M	O	O
3	L RUN	Lit: Data link execution in progress	M	O	O
4	L ERR.	Lit: Communication error (self station) Flashing: Switch type setting was changed with power ON	M	O	O

11.9.2 Installation guidelines

This document specifies protocol and services for a safety communication system based on IEC 61158 Type 18. Usage of safety devices with the safety protocol specified in this document requires proper installation.

Additional installation information is also given in [30] and [31] in the Bibliography.

11.9.3 Safety function response time

11.9.3.1 General

As mentioned in 11.5.3, an integrated watchdog timer is used which provides the time expectation of each output channel on each safety output slave. It ensures a safety function response time.

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.

11.9.3.2 Time calculation

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.

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 SRC.

The safety function response time is calculated as the sum of (a) through (f) from Table 21 with the terms as defined in Table 22.

NOTE 1 The safety master calculates the timeout based on: the safety refresh monitoring time – $((WDT \times n) \times 2)$.

NOTE 2 $(WDT \times n) \times 2$ is the time required for the safety master to send communication data.

Table 21 – Safety function response time calculation

Item	Maximum
(a) Input device response time	DT1
(b) Safety slave input processing time	Time of noise removal filter + Processing time of remote input station
(c) Monitoring time from safety input to safety output	Safety data monitor time
(d) Safety slave output processing time	Processing time of remote output station
(e) Output device response time	DT2
Total	(a)+(b)+(c)+(d)+(e)

Table 22 – Safety function response time definition of terms

Item	Definition
LS	Link Scan Time as specified by the manufacturer
n	Value after the decimal point of LS/WDT (rounded up)
SRRP	Safety refresh response processing time. As specified by the manufacturer
m	Value after the decimal point of $SRRP/(WDT \times n)$ (rounded up)
Time of noise removal filter	Configured in safety remote station settings (Setting value: 1 ms to 50 ms)
DT1, DT2	Response time of sensor or output destination controlling device. As specified by the manufacturer.
Safety data monitor time	Time set in network parameter. Use the value derived from the following formula as the measure: Safety refresh monitor time $\times 2 - ((WDT \times n) \times m) - 10$ [ms]
Safety refresh monitor time	Time set in network parameter. Use the value gained by the following calculation formula as the measure. In triggered mode: $(WDT \times n) \times 3 + (WDT \times n) \times m \times 2 + (WDT \times \alpha)$ [ms] In free-running mode: $(WDT \times n) \times 3 + LS + (WDT \times n) \times m \times 2 + (WDT \times \alpha)$ [ms] where: $\alpha = 0$, for $LS \leq 1,5$ ms $\alpha = 1$, for $LS > 1,5$ ms
WDT (Watchdog timer)	Time set in configuration parameter.
Triggered mode	Mode which performs data link when sequence scan is synchronized with link scan. In the triggered mode, sequence scan and link scan start simultaneously
Free-running mode	Mode which performs data link without synchronizing sequence program

11.9.4 Duration of demands

The duration of demand by the safety-related application to the safety communication layer shall be sufficient in duration such that demand is detected within the longest safety function response time by the application.

11.9.5 Constraints for calculation of system characteristics

An FSCP 8/1 safety system shall comply with the following constraints:

- IEC 61158 Type 18: No restrictions
- Maximum number of safety slots: 64
- Minimum scan cycle time: 10 ms
- Maximum number of safety relevant I/O bits per safety PDU – slave to master: 208
- Maximum number of safety relevant I/O bits per safety PDU – master to slave: 7 168

11.9.6 Maintenance

There are no SCL specific requirements for maintenance.

Specifications for system behavior in case of device repair and replacement are outside the scope of this document. The specification of these activities and the responsibilities are not relevant for the specification of services and protocols. Usually this will be part of a functional safety management plan. However, repair, replacement as well as maintenance, overall safety validation, overall operation, modifications, retrofits and decommissioning or disposal according to IEC 61508 are important issues which have to be taken into account. It is recommended to contact the device or system supplier also.

For information on programming the SRP and setting the parameters of safety devices, it is strongly recommended to contact the device or system supplier. Also, it is recommended to take into account the documents [30] and [31]. In these documents additional information, e.g. checklists, is given for the user of a CC-LINK-Safety system.

NOTE Additional requirements for maintenance – as well as other requirements – are specified in IEC 61508, IEC 61511 and/or IEC 62061.

11.9.7 Safety manual

The supplier of safety slaves that incorporate the SCL according to the SCL specifications given in this document shall prepare an appropriate safety manual according to IEC 61508. This safety manual shall also include the installation requirements as specified in 11.9.2 as well as guidelines for the configuration of device switches. In addition to switches common with IEC 61158 Type 18, these guidelines shall include the statement that all safety devices on the same network shall be configured with the same Link ID. See 11.9.1.1.

According to the safety communication system based on IEC 61158 Type 18, it is strongly recommended to take into account the specifications [30], [31] and [32].

NOTE Before starting the implementation of a safety device it is good engineering practice to contact the CLPA to determine if there are amendments to implementation guidelines and/or implementation requirements.

11.10 Assessment for FSCP 8/1

It is the manufacturer's responsibility to develop the device to the appropriate development process according to the safety standards (see IEC 61508, IEC 61511, IEC 62061, ...) and relevant legal regulations (e. g. European machinery directive). Additional information is provided in Annex B.

12 FSCP 8/2

12.1 Scope – FSCP 8/2

See Clause 1.

12.2 Normative references – FSCP 8/2

See Clause 2.

12.3 Terms, definitions, symbols, abbreviated terms and conventions – FSCP 8/2

See Clause 3.

12.4 Overview of FSCP 8/2 (CC-Link IE™ Safety communication function)

Communication Profile 8/4 and 8/5 (commonly known as CC-Link IE™⁴) defines communication profiles based on ISO/IEC/IEEE 8802-3, IEC 61158-5-23, and IEC 61158-6-23.

The basic profiles CP 8/4, and CP 8/5 are defined in IEC 61784-2. The CPF 8 functional safety communication profile FSCP 8/2 (CC-Link IE™ Safety communication function³) is based on the CP 8/4 and CP 8/5 basic profiles in IEC 61784-2 and the safety communication layer specifications defined in this document.

FSCP 8/2 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 8/2 protocol is designed to support Safety Integrity Level SIL3 (IEC 61508) using CP 8/4 and CP 8/5 by additionally specifying mechanisms for the implementation of time stamp, time expectation, connection authentication, feedback message, data integrity assurance and different data integrity assurance safety measures.

SCL capabilities for FSCP 8/2 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 CP 8/4 and CP 8/5, these SASEs specify required additions to CP 8/4 and CP 8/5 for functional safety using a black channel approach.

The master and slave construct yields two SASEs, the SASE-M and SASE-S respectively. Each are managed by an safety FAL service protocol machine, the SFSPM-M and the SFSPM-S respectively.

12.5 General – FSCP 8/2

12.5.1 External documents providing specifications for the profile

Manufacturers of FSCP 8/2 safety devices are encouraged to review CC-Link Safety Specifications which provide additional specifications relevant for implementation of the SCL defined in this document.

NOTE Documents [30] and [31] contain important information related to FSCP 8/2.

⁴ CC-Link IE™ is a trade name of the non-profit organization CC-Link Partner Association. This information is given for the convenience of users of this document and does not constitute an endorsement by IEC of the trade name holder or any of its products. Compliance to this document does not require use of the trade name CC-Link IE™. Use of the trade name CC-Link IE™ requires permission of CC-Link Partner Association and compliance with conditions for their use (such as testing and validation).