IEC 61784-3-8

Edition 1.0 2010-06

INTERNATIONAL STANDARD

colour inside

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

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland
Email: inmail@iec.ch
Web: www.iec.ch

About the IEC

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

About IEC publications

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

- Catalogue of IEC publications: www.iec.ch/searchpub

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 It also gives information on projects, withdrawn and replaced publications.

- IEC Just Published: www.iec.ch/online_news/justpub

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

- Electropedia: www.electropedia.org

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

- Customer Service Centre: www.iec.ch/webstore/custserv

If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us:

Email: csc@iec.ch
Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00

IEC 61784-3-8

Edition 1.0 2010-06

INTERNATIONAL STANDARD

colour inside

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

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

PRICE CODE X

ICS 25.040.40; 35.100.05

ISBN 978-2-88910-980-7

CONTENTS

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.

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

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

FDIS	Report on voting
65C/591A/FDIS	65C/603/RVD

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

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

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

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

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

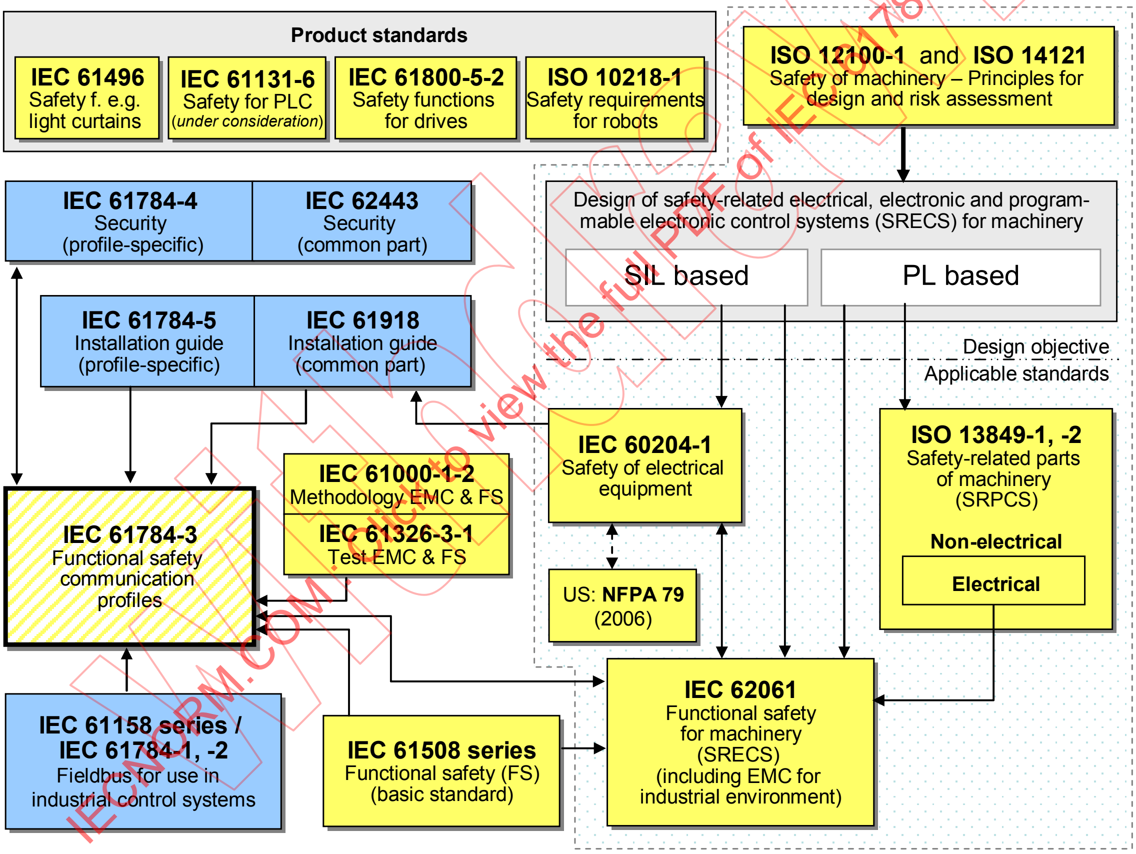
IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

The IEC 61158 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 many fieldbus enhancements are emerging, addressing not yet standardized areas such as real time, safety-related and security-related applications.

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

Figure 1 shows the relationships between this standard and relevant safety and fieldbus standards in a machinery environment.



Key

🟨 (yellow) safety-related standards

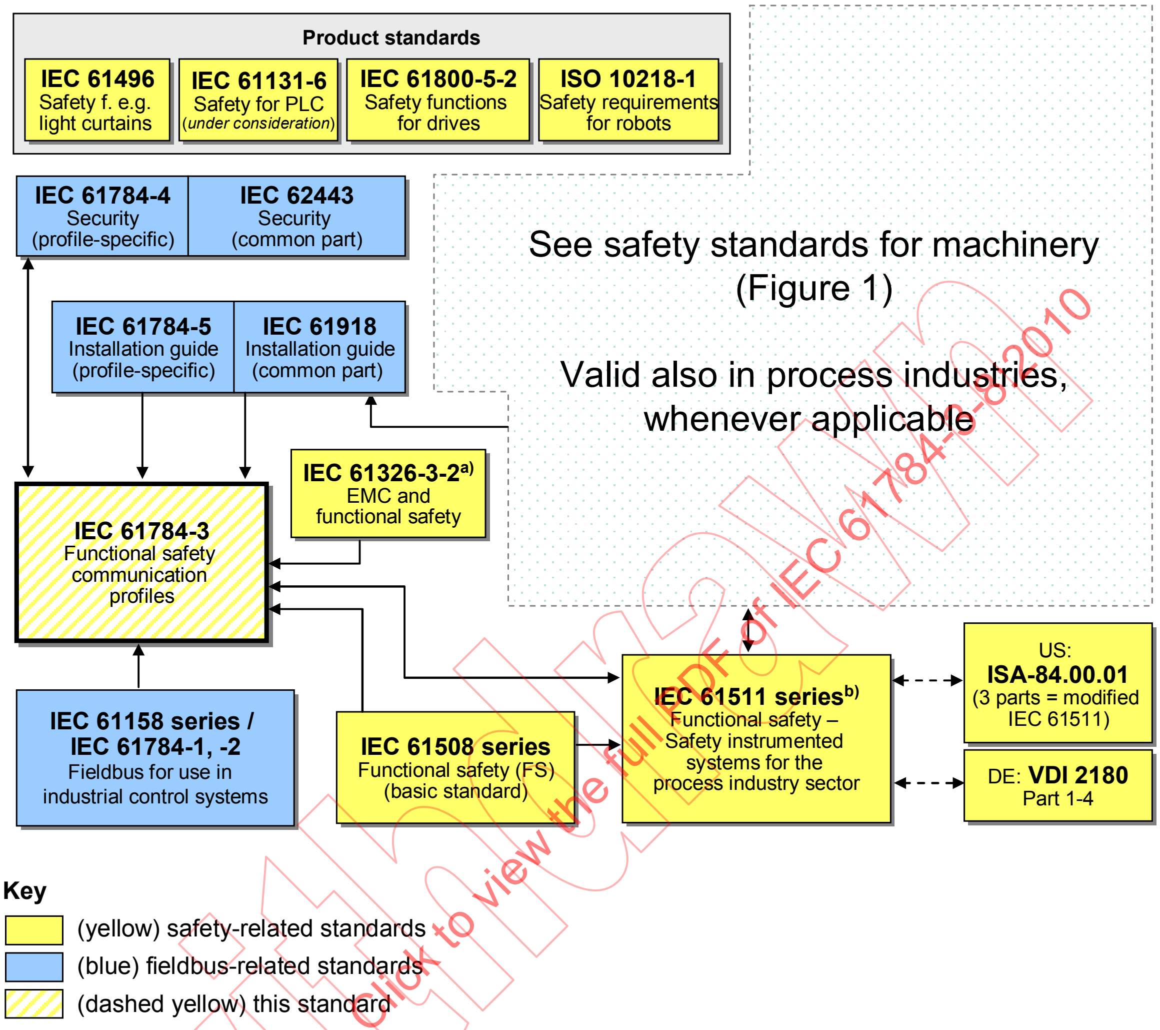
🟦 (blue) fieldbus-related standards

▨ (dashed yellow) this standard

NOTE Subclauses 6.7.6.4 (high complexity) and 6.7.8.1.6 (low complexity) of IEC 62061 specify the relationship between PL (Category) and SIL.

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

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


Product standards
IEC 61496 Safety f. e.g. light curtains
IEC 61131-6 Safety for PLC (under consideration)
IEC 61800-5-2 Safety functions for drives
ISO 10218-1 Safety requirements for robots
IEC 61784-4 Security (profile-specific)
IEC 62443 Security (common part)
IEC 61784-5 Installation guide (profile-specific)
IEC 61918 Installation guide (common part)
See safety standards for machinery (Figure 1)
Valid also in process industries, whenever applicable
IEC 61326-3-2a) EMC and functional safety
IEC 61784-3 Functional safety communication profiles
IEC 61158 series / IEC 61784-1, -2 Fieldbus for use in industrial control systems
IEC 61508 series Functional safety (FS) (basic standard)
IEC 61511 seriesb) Functional safety – Safety instrumented systems for the process industry sector
US: ISA-84.00.01 (3 parts = modified IEC 61511)
DE: VDI 2180 Part 1-4
Key
(yellow) safety-related standards
(blue) fieldbus-related standards
(dashed yellow) this standard

[a] For specified electromagnetic environments; otherwise IEC 61326-3-1.

[b] EN ratified.

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

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

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

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

This standard describes:

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

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES –

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

1 Scope

This part of the IEC 61784-3 series specifies a safety communication layer (services and protocol) based on CPF 8 of IEC 61784-1 and IEC 61158 Type 18. It identifies the principles for functional safety communications defined in IEC 61784-3 that are relevant for this safety communication layer.

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 part[1] 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 series[2] for functional safety. These mechanisms may be used in various industrial applications such as process control, manufacturing automation and machinery.

This part 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 part in a standard device is not sufficient to qualify it as a safety device.

2 Normative references

The following referenced documents are indispensable for the application 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 60204-1, *Safety of machinery – Electrical equipment of machines – Part 1: General requirements*

IEC 61131-2, *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 standard, “this part” will be used for “this part of the IEC 61784-3 series”.

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

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

IEC 61158-6-18, *Industrial communication networks – Fieldbus specifications – Part 6-18: Application layer protocol specification – Type 18 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 61784-3: 2010[3] *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*

3 Terms, definitions, symbols, abbreviated terms and conventions

3.1 Terms and definitions

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

3.1.1 Common terms and definitions

3.1.1.1
availability
probability for an automated system that for a given period of time there are no unsatisfactory system conditions such as loss of production

3.1.1.2
black channel
communication channel without available evidence of design or validation according to IEC 61508

3.1.1.3
communication channel
logical connection between two end-points within a *communication system*

[3] In preparation.

3.1.1.4
communication system
arrangement of hardware, software and propagation media to allow the transfer of *messages* (ISO/IEC 7498 application layer) from one application to another

3.1.1.5
connection
logical binding between two application objects within the same or different devices

3.1.1.6
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 Terms “CRC code” and "CRC signature", and labels such as CRC1, CRC2, may also be used in this standard to refer to the redundant data.

NOTE 2 See also [32], [33][4].

3.1.1.7
error
discrepancy between a computed, observed or measured value or condition and the true, specified or theoretically correct value or condition

[IEC 61508-4:2010[5]], [IEC 61158]

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

NOTE 2 Errors do not necessarily result in a *failure* or a *fault*.

3.1.1.8
failure
termination of the ability of a functional unit to perform a required function or operation of a functional unit in any way other than as required

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

[IEC 61508-4:2010, modified], [ISO/IEC 2382-14.01.11, modified]

NOTE 2 Failure may be due to an *error* (for example, problem with hardware/software design or message disruption).

3.1.1.9
fault
abnormal condition that may cause a reduction in, or loss of, the capability of a functional unit to perform a required function

NOTE IEV 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.

[IEC 61508-4:2010, modified], [ISO/IEC 2382-14.01.10, modified]

3.1.1.10
fieldbus
communication system based on serial data transfer and used in industrial automation or process control applications

[4] Figures in square brackets refer to the bibliography.

[5] To be published.

3.1.1.11
frame
denigrated synonym for DLPDU

3.1.1.12
hash function
(mathematical) function that maps values from a (possibly very) large set of values into a (usually) smaller range of values

NOTE 1 Hash functions can be used to detect data corruption.

NOTE 2 Common hash functions include parity, checksum or CRC.

[IEC/TR 62210, modified]

3.1.1.13
hazard
state or set of conditions of a system that, together with other related conditions will inevitably lead to harm to persons, property or environment

3.1.1.14
master
active communication entity able to initiate and schedule communication activities by other stations which may be masters or slaves

3.1.1.15
message
ordered series of octets intended to convey information
[ISO/IEC 2382-16.02.01, modified]

3.1.1.16
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
[ISO 13849-1]

3.1.1.17
protective extra-low-voltage (PELV)
electrical circuit in which the voltage cannot exceed a.c. 30 V r.m.s., 42,4 V peak or d.c. 60 V in normal and single-fault condition, except earth faults in other circuits

NOTE A PELV circuit is similar to an SELV circuit that is connected to protective earth.

[IEC 61131-2]

3.1.1.18
redundancy
existence of means, in addition to the means which would be sufficient for a functional unit to perform a required function or for data to represent information

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

[IEC 61508-4:2010, modified], [ISO/IEC 2382-14.01.12, modified]

3.1.1.19
reliability
probability that an automated system can perform a required function under given conditions for a given time interval (t1,t2)

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

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

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

NOTE 4 Reliability differs from availability.

[IEC 62059-11, modified]

3.1.1.20
risk
combination of the probability of occurrence of harm and the severity of that harm

NOTE For more discussion on this concept see Annex A of IEC 61508-5:2010[6].

[IEC 61508-4:2010], [ISO/IEC Guide 51:1999, definition 3.2]

3.1.1.21
safety communication layer (SCL)
communication layer that includes all the necessary measures to ensure safe transmission of data in accordance with the requirements of IEC 61508

3.1.1.22
safety connection
connection that utilizes the safety protocol for communications transactions

3.1.1.23
safety data
data transmitted across a safety network using a safety protocol

NOTE The Safety Communication Layer does not ensure safety of the data itself, only that the data is transmitted safely.

3.1.1.24
safety device
device designed in accordance with IEC 61508 and which implements the functional safety communication profile

3.1.1.25
safety extra-low-voltage (SELV)
electrical circuit in which the voltage cannot exceed a.c. 30 V r.m.s., 42,4 V peak or d.c. 60 V in normal and single-fault condition, including earth faults in other circuits

NOTE An SELV circuit is not connected to protective earth.

[IEC 61131-2]

3.1.1.26
safety function
function to be implemented by an E/E/PE safety-related system or other risk reduction measures, that is intended to achieve or maintain a safe state for the EUC, in respect of a specific hazardous event

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

[IEC 61508-4:2010, modified]

[6] To be published.

3.1.1.27
safety function response time
worst case elapsed time following an actuation of a safety sensor connected to a fieldbus, before the corresponding safe state of its safety actuator(s) is achieved in the presence of errors or failures in the safety function channel

NOTE This concept is introduced in IEC 61784-3:2010 [7], 5.2.4 and addressed by the functional safety communication profiles defined in this part.

3.1.1.28
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 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[8].

NOTE 2 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 A safety integrity level (SIL) is not a property of a system, subsystem, element or component. The correct interpretation of the phrase “SILn 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.

[IEC 61508-4:2010]

3.1.1.29
safety measure
<this standard> measure to control possible communication *errors* that is designed and implemented in compliance with the requirements of IEC 61508

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

NOTE 2 Communication *errors* and related safety measures are detailed in IEC 61784-3:2010, 5.3 and 5.4.

3.1.1.30
safety-related application
programs designed in accordance with IEC 61508 to meet the SIL requirements of the application

3.1.1.31
safety-related system
system performing *safety functions* according to IEC 61508

3.1.1.32
slave
passive communication entity able to receive messages and send them in response to another communication entity which may be a master or a slave

3.1.1.33
time stamp
time information included in a *message*

[7] In preparation.

[8] To be published.

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 data monitor timer
timer used by the time expectation function for safety data transmission

3.1.2.5
safety monitor timer
timer used by the time expectation function for safety connection management

3.1.2.6
safety PDU
synonym for safety-related DLPDU

3.1.2.7
slot
one quantum (granularity) of the position dependent mapping of the cyclic data fields

3.1.2.8
station
device and its corresponding SAREP associated with the transmission and reception of safety data

NOTE The station number is used in the position dependent mapping of the cyclic data fields (a station occupies one or more slots).

3.1.2.9
safety protocol transmission information
information distinguishing safety relevant messages

3.2 Symbols and abbreviated terms

3.2.1 Common symbols and abbreviated terms

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]
FS	Functional Safety	
FSCP	Functional Safety Communication Profile	

MTBF	Mean Time Between Failures	
MTTF	Mean Time To Failure	
PDU	Protocol Data Unit	[ISO/IEC 7498-1]
PELV	Protective Extra Low Voltage	
PhL	Physical Layer	[ISO/IEC 7498-1]
PL	Performance Level	[ISO 13849-1]
PLC	Programmable Logic Controller	
SCL	Safety Communication Layer	
SELV	Safety Extra Low Voltage	
SIL	Safety Integrity Level	[IEC 61508-4:2010]

3.2.2 CPF 8: Additional symbols and abbreviated terms

AR	Application Relationship
ASE	Application Service Element
CMD	Command Data
LED	Light Emitting Diode
LID	Link Identifier
PSD	Protocol Support Data
RNO	Running Number
SAR	Safety Application Relationship
SAREP	Safety Application Relationship Endpoint
SARPM	Safety Application Relationship Protocol State Machine
SASE	Safety Application Service Element
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

3.3 Conventions

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

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

Communication Profile Family 8 (commonly known as CC-Link™ [9]) 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™ [9]) is based on the CPF 8

[9] CC-Link™ and CC-Link Safety™ are trade names of the non-profit organization CC-Link Partner Association. This information is given for the convenience of users of this International Standard and does not constitute an endorsement by IEC of the trade name holder or any of its products. Compliance to this standard does not require use of the trade names CC-Link™ or CC-Link Safety™. Use of the trade names CC-Link™ or CC-Link Safety™ requires permission of CC-Link Partner Association.

basic profiles in IEC 61784-1 and the safety communication layer specifications defined in this part.

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

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

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

5 General

5.1 External documents providing specifications for the profile

Manufacturers of FSCP 8/1 safety devices are encouraged to check documents [43], [44] and [45] which provide additional specifications relevant for implementation of the SCL defined in this part.

5.2 Safety functional requirements

This standard specifies the services and protocols for a functional safety communication system based on IEC 61158 Type 18.

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 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 part, the CPF 8 requirements shall be unchanged for safety.

5.3 Safety measures

5.3.1 General

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

— sequence number;

- time expectation;
- connection authentication;
- feedback message;
- data integrity assurance (CRC 32);
- 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		
Unintended repetition	X							
Incorrect sequence	X							
Loss	X				X			
Unacceptable delay			X					
Insertion	X			X	X			
Masquerade				X	X			X
Addressing				X				
NOTE Table adapted from IEC 62280-2 [16] and EN 954-1 [27].								

5.3.2 Sequence number

Safety messages contain a sequence number (RNO) with a width of 4 bits and a specified sequence (see 7.1 and 7.2). If the sequence is not followed, all safety related output signals shall be set to their safe states.

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 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.

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.

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, command ID and protocol support data field.

5.3.6 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 a 16-bit protocol support data field, an 8-bit command ID, a 3-bit link ID and a 4-bit RNO.

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 manger;
- 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 manger;
- M1 and S1 type safety cyclic transmission.

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

5.5 Relationships with FAL (and DLL, PhL)

5.5.1 Overview

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

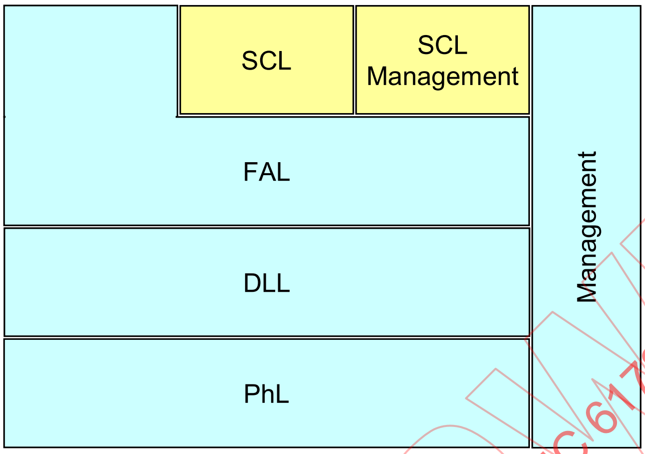


Figure 3 – Relationship between SCL and the other layers of IEC 61158 Type 18

5.5.2 Data types

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

6 Safety communication layer services

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 are defined in this clause.

6.2 SASEs

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

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

6.3 SARs

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

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

6.4 Process data SAR ASEs

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
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.n.	(m)	Attribute:	Safety data in n
…	…	…	…
2.64.	(m)	Attribute:	Safety data in 64

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 manger.

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
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

7 Safety communication layer protocol

7.1 Safety PDU format

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.

7.1.2 Abstract syntax

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

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

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

Attribute	Format	Size (bits)
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

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

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:	96 × 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
Data in	Structure of n elements	96 × n
Safety data in 1	Structure of 2 elements	96 x p_1
Safety RX data	Bit-oriented data structure	32 x p_1
RWr data	Word-oriented data structure	64 x p_1
Safety RWr data	Word-oriented data	64 × (p_1 - 1)
Safety TPI-R	Safety transmission packet information	64
…	…	…
Safety data in n	Structure of 2 elements	96 x p_n
NOTE The values of n and m are dependent upon the values of the corresponding configuration settings in the master status. The value of p depends on the number of slots occupied by the slave station.		

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:	96 × p
Safety RY data	Bit-oriented data structure	32 × p
RWw data	Word-oriented data structure	64 × p
Safety RWw data	Word-oriented data	64 × (p - 1)
Safety TPI-T	Safety transmission packet information	64
Data in	Structure of 2 elements:	96 × p
Safety RX data	Bit-oriented data structure	32 × p
RWr data	Word-oriented data structure	64 × p
Safety RWr data	Word-oriented data	64 × (p - 1)
Safety TPI-R	Safety transmission packet information	64
NOTE The value of p depends on the number of slots occupied by the slave station.		

7.1.3 Transfer syntax

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

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

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

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

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

<table>
<tr><th>Attribute</th><th colspan="4">Encoding</th></tr>
<tr><td>Data out</td><td colspan="4">Process data registers set by the master for slave device output</td></tr>
<tr><td>Safety RY data</td><td colspan="4">A position mapped field of bit-oriented output data for all connected slave devices ordered by slot with 32 bits per slot</td></tr>
<tr><td>RWw data</td><td colspan="4">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</td></tr>
<tr><td>Safety RWw data</td><td colspan="4">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</td></tr>
<tr><td rowspan="11">Safety TPI-T</td><td><b>Octet</b></td><td><b>Bit</b></td><td><b>Description</b></td><td><b>Values</b></td></tr>
<tr><td>0 - 1</td><td>–</td><td>Protocol support data (PSD) which is used by SCL management</td><td>0 - 65 535</td></tr>
<tr><td rowspan="8">2 - 3</td><td>0 - 3</td><td>Running number</td><td>0 - 15</td></tr>
<tr><td>4 - 6</td><td>Link id</td><td>0 - 7</td></tr>
<tr><td>7</td><td>reserved</td><td>0</td></tr>
<tr><td>8 - 11</td><td>Transmission data type</td><td>0 - 15</td></tr>
<tr><td>12</td><td>Busy flag</td><td>0 = busy
1 = not busy</td></tr>
<tr><td>13</td><td>reserved</td><td>0</td></tr>
<tr><td>14</td><td>Read request</td><td>0 = no request
1 = request</td></tr>
<tr><td>15</td><td>SCL-user application mode</td><td>0 = test mode
1 = safety mode</td></tr>
<tr><td>4 - 7</td><td>–</td><td>CRC32</td><td>CRC32</td></tr>
<tr><td>Data in</td><td colspan="4">Process data registers read by the master representing slave device inputs</td></tr>
<tr><td>Safety data in</td><td colspan="4">Process data registers read by the master representing safety slave device inputs</td></tr>
<tr><td>Safety RX data</td><td colspan="4">A field containing the bit-oriented input data from slave device n ordered by slot with 32 bits per slot. The number of slots occupied by the slave device determines the total length of this field</td></tr>
<tr><td>RWr data</td><td colspan="4">A field containing the word-oriented input data from slave device n ordered by slot with 4 words per slot. The number of slots occupied by the slave device determines the total length of this field</td></tr>
<tr><td>Safety RWr data</td><td colspan="4">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</td></tr>
<tr><td rowspan="2">Safety TPI-R</td><td><b>Bit</b></td><td colspan="2"><b>Description</b></td><td><b>Values</b></td></tr>
<tr><td>0 - 15</td><td colspan="2">Protocol support data (PSD) which is used by SCL management</td><td>0 - 65 535</td></tr>
</table>

Attribute	Encoding		
	16 - 19	Running number	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	CRC32

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 per slot. The number of slots occupied by the slave device determines the total length of this field		
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	Protocol support data (PSD) which is used by SCL management	0 - 65 535
	16 - 19	Running number	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	CRC32

Attribute	Encoding		
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 per slot. The number of slots occupied by the slave device determines the total length of this field		
RWr data	A field containing the word-oriented input data from the master. The number of slots occupied by the slave device determines the total length of this field		
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		
Safety TPI-R	**Bit**	**Description**	**Values**
	0 - 15	Protocol support data (PSD) which is used by SCL management	0 - 65 535
	16 - 19	Running number	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	CRC32

7.2 State description

7.2.1 Overview

The SCL state model is extended from IEC 61158 Type 18 with a safe state, as shown in Figure 4. 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.

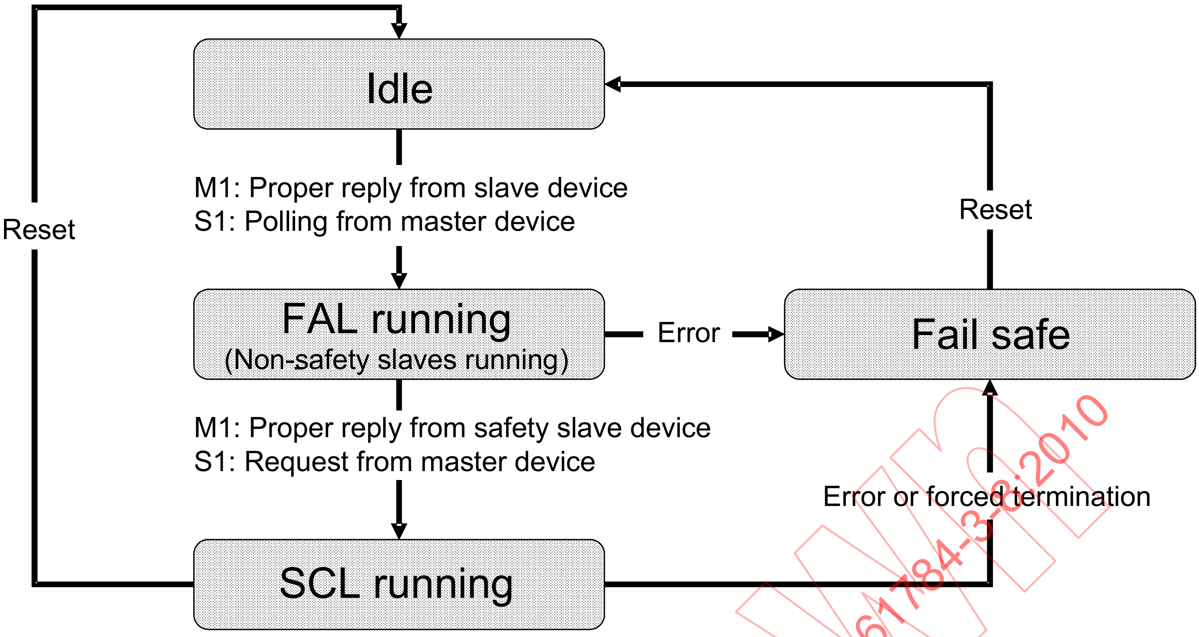

Idle
M1: Proper reply from slave device
S1: Polling from master device
Reset
Reset
FAL running
(Non-safety slaves running)
Error
Fail safe
M1: Proper reply from safety slave device
S1: Request from master device
Error or forced termination
SCL running

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 Clause 8) and safety data transmission and confirmation monitoring.

7.2.2 Idle

7.2.2.1 Overview

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

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.

7.2.3 FAL running

7.2.3.1 Overview

The M1 safety master devices and S1 safety slave devices have established non-safety communications.

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.

7.2.4 SCL running

7.2.4.1 Overview

The details of the SCL running state are explained in Clause 8.

7.2.4.2 Transition

As explained in 7.2.6, a FSCP 8/1 device transitions to the fail safe state upon detection of any of the following error types:

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

As explained in 7.2.7, a FSCP 8/1 device transitions to the fail safe state upon receipt of a forced termination request.

7.2.5 Fail safe

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.

7.2.5.2 Transition

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

7.2.6 Safety data transmission and processing

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;
- different data integrity assurance systems.

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

7.2.6.2 Sequence number

Safety messages contain a sequence number (RNO) with a width of 4 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.

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 value to a value 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 and Table 15 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.

7.2.6.4 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.

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, command ID and protocol support data field.

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 discussed in 9.5.2.

7.2.6.7 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), a 16-bit protocol support data field, an 8-bit command ID, a 3-bit link ID and a 4-bit RNO.

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

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.

8 Safety communication layer management

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.

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 and PSD 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.

8.3 Safety slave verification

8.3.1 General

Product information verification processing confirms that the actually 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.

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.

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.

9 System requirements

9.1 Indicators and switches

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.

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

No.	LED Name	Description	Safety master station	Safety remote device station	Safety remote I/O station
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

9.2 Installation guidelines

This standard specifies protocol and services for a safety communication system based on IEC 61158 Type 18. However, usage of safety devices with the safety protocol specified in this standard requires proper installation. All devices connected to a safety communication system defined in this part shall fulfill SELV/PELV requirements, which are specified in the relevant IEC standards such as IEC 60204-1.

Additional installation information is also given in [43] and [44] in the Bibliography.

9.3 Safety function response time

9.3.1 General

As mentioned in 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, 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).

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 each safety slave (input and output), and the processing time within the 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.

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 x n) x 2)

NOTE 2 (WDT x n) x 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 x 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 x 2 - ((WDT x n) x 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 x n) x 3 + (WDT x n) x m x 2 + (WDT x α) [ms] In free-running mode: (WDT x n) x 3 + LS + (WDT x n) x m x 2 + (WDT x α) [ms] where: α = 0, for LS ≤ 1,5 ms α = 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