BS EN 61784-3-1:2010

BSI Standards Publication

Industrial communication networks — Profiles -

Part 3-1: Functional safety fieldbuses — Additional specifications for CPF 1

raising standards worldwide™

National foreword

This British Standard is the UK implementation of EN 61784-3-1:2010. It is identical to IEC 61784-3-1:2010. It supersedes BS EN 61784-3-1:2008 which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee AMT/7, Industrial communications: process measurement and control, including fieldbus.

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

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

ISBN 978 0 580 72027 7

ICS 25.040.40; 35.100.05

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

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 September 2010.

Amendments issued since publication

Date	Text affected

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 61784-3-1

August 2010

ICS 25.040.40;35.100.05

Supersedes EN 61784-3-1:2008

English version

Industrial communication networks - Profiles - Part 3-1: Functional safety fieldbuses - Additional specifications for CPF 1 (IEC 61784-3-1:2010)

Réseaux de communication industriels -
Partie 3-1: Bus de terrain à sécurité
fonctionnelle -
Spécifications complémentaires
pour le CPF 1
(CEI 61784-3-1:2010)

Industrielle Kommunikationsnetze -
Profile -
Teil 3-1: Funktional sichere Übertragung
bei Feldbussen -
Zusätzliche Festlegungen
für die Kommunikationsprofilfamilie 1
(IEC 61784-3-1:2010)

This European Standard was approved by CENELEC on 2010-07-01. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

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

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

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

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

Management Centre: Avenue Marnix 17, B - 1000 Brussels

Foreword

The text of document 65C/591A/FDIS, future edition 2 of IEC 61784-3-1, prepared by SC 65C, Industrial networks, of IEC TC 65, Industrial-process measurement, control and automation, was submitted to the IEC-CENELEC parallel vote and was approved by CENELEC as EN 61784-3-1 on 2010-07-01.

This European Standard supersedes EN 61784-3-1:2008.

The main technical changes with respect to EN 61784-3-1:2008 are listed below:

– updates in relation with changes in EN 61784-3;

– adjustment of Figure 5;

– change of sequence number from two octets to four octets in 7.2.2 to match the final protocol from the consortium.

– addition of details for time synchronization in 7.2.4;

– addition of information for safety response time in 9.3;

– addition of information in constraints for calculation of system characteristics in 9.5.

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

The following dates were fixed:

– latest date by which the EN has to be implemented at national level by publication of an identical national standard or by endorsement	(dop)	2011-04-01
– latest date by which the national standards conflicting with the EN have to be withdrawn	(dow)	2013-07-01

Annex ZA has been added by CENELEC.

Endorsement notice

The text of the International Standard IEC 61784-3-1:2010 was approved by CENELEC as a European Standard without any modification.

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

IEC 60204-1	NOTE	Harmonized as EN 60204-1.
IEC 61158 series	NOTE	Harmonized in EN 61158 series (not modified).
IEC 61326-3-1	NOTE	Harmonized as EN 61326-3-1
IEC 61326-3-2	NOTE	Harmonized as EN 61326-3-2.
IEC 61496 series	NOTE	Harmonized in EN 61496 series (partially modified).
IEC 61508-5:2010	NOTE	Harmonized as EN 61508-5:2010 (not modified).
IEC 61508-6:2010	NOTE	Harmonized as EN 61508-6:2010 (not modified).
IEC 61784-2	NOTE	Harmonized as EN 61784-2.
IEC 61784-5 series	NOTE	Harmonized in EN 61784-5 series (not modified).
IEC 61800-5-2	NOTE	Harmonized as EN 61800-5-2.
IEC 62061	NOTE	Harmonized as EN 62061.
ISO 10218-1	NOTE	Harmonized as EN ISO 10218-1.
ISO 12100-1	NOTE	Harmonized as EN ISO 12100-1.
ISO 13849-1	NOTE	Harmonized as EN ISO 13849-1.
ISO 13849-2	NOTE	Harmonized as EN ISO 13849-2.
ISO 14121	NOTE	Harmonized as EN ISO 14121.

Annex ZA
(normative)

Normative references to international publications with their corresponding European publications

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.

NOTE When an international publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

Publication	Year	Title	EN/HD	Year
IEC 61131-2	-	Programmable controllers - Part 2: Equipment requirements and tests	EN 61131-2	-
IEC 61158-2	-	Industrial communication networks - Fieldbus specifications - Part 2: Physical layer specification and service definition	EN 61158-2	-
IEC 61158-3-1	-	Industrial communication networks - Fieldbus specifications - Part 3-1: Data-link layer service definition - Type 1 elements	EN 61158-3-1	-
IEC 61158-4-1	-	Industrial communication networks - Fieldbus specifications - Part 4-1: Data-link layer protocol specification - Type 1 elements	EN 61158-4-1	-
IEC 61158-5-5	-	Industrial communication networks - Fieldbus specifications - Part 5-5: Application layer service definition - Type 5 elements	EN 61158-5-5	-
IEC 61158-5-9	-	Industrial communication networks - Fieldbus specifications - Part 5-9: Application layer service definition - Type 9 elements	EN 61158-5-9	-
IEC 61158-6-5	-	Industrial communication networks - Fieldbus specifications - Part 6-5: Application layer protocol specification - Type 5 elements	EN 61158-6-5	-
IEC 61158-6-9	-	Industrial communication networks - Fieldbus specifications - Part 6-9: Application layer protocol specification - Type 9 elements	EN 61158-6-9	-
IEC 61508	Series	Functional safety of electrical/electronic/programmable electronic safety-related systems	EN 61508	Series
IEC 61508-1	2010	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1: General requirements	EN 61508-1	2010

Publication	Year	Title	EN/HD	Year
IEC 61508-2	2010	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems	EN 61508-2	2010
IEC 61508-3	2010	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 3: Software requirements	EN 61508-3	2010
IEC 61508-4	2010	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 4: Definitions and abbreviations	EN 61508-4	2010
IEC 61511	Series	Functional safety - Safety instrumented systems for the process industry sector	EN 61511	Series
IEC 61784-1	-	Industrial communication networks - Profiles - Part 1: Fieldbus profiles	EN 61784-1	-
IEC 61784-3	2010	Industrial communication networks - Profiles - Part 3: Functional safety fieldbuses - General rules and profile definitions	EN 61784-3	2010
IEC 61918	-	Industrial communication networks - Installation of communication networks in industrial premises	EN 61918	-
IEC 62280-1	-	Railway applications - Communication, signalling and processing systems - Part 1: Safety-related communication in closed transmission systems	-	-
ISO/IEC 8802-3	-	Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications	-	-

This page deliberately left blank

CONTENTS

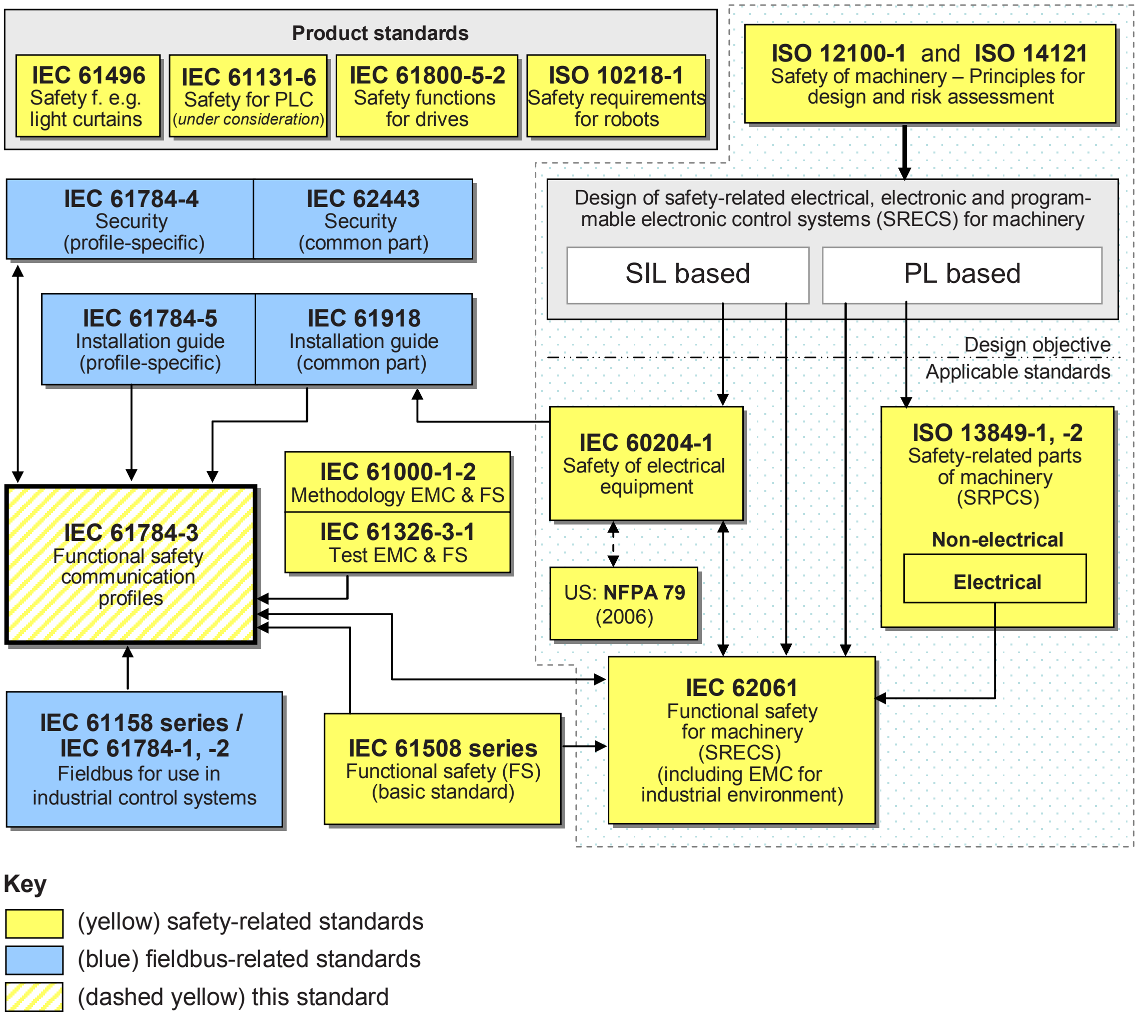
0 Introduction

0.1 General

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.

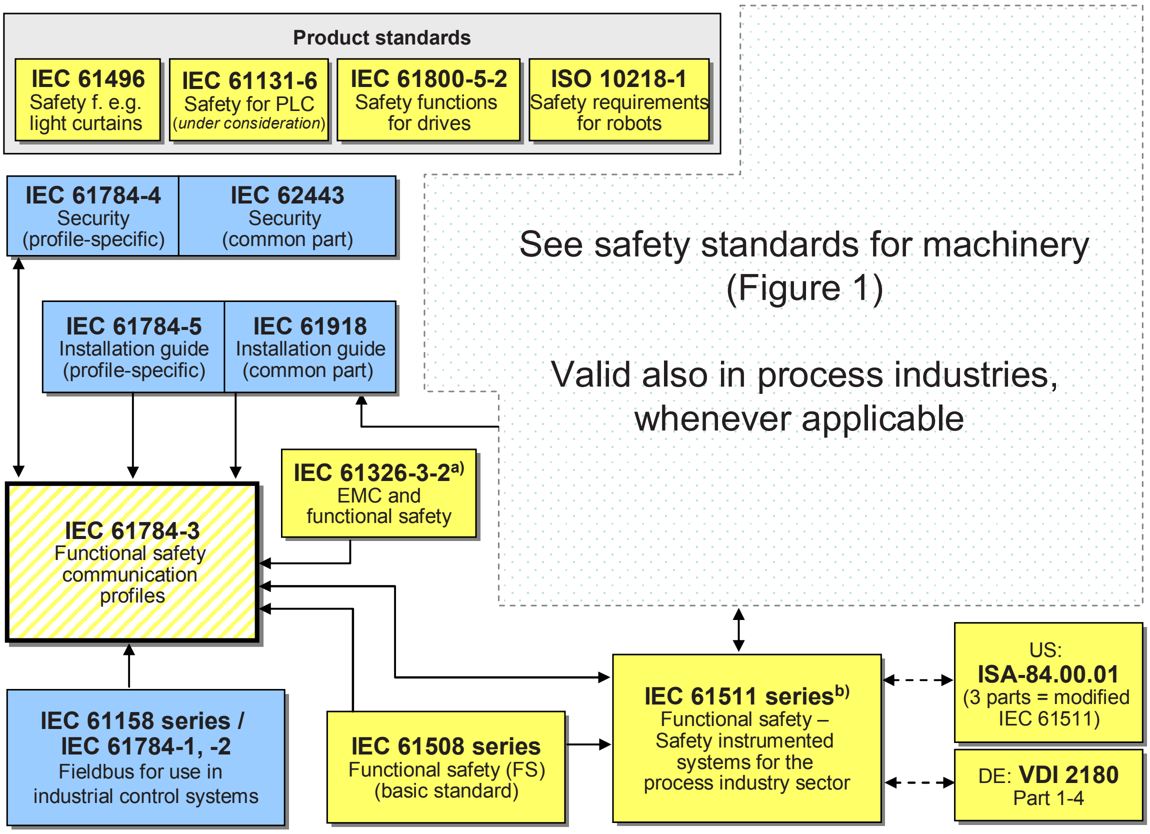
Figure 1 shows the relationships between this standard and relevant safety and fieldbus standards in a machinery environment.



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.

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 patents concerning the functional safety communication profiles for family 1 as follows, where the [xx] notation indicates the holder of the patent right:

US 6,999,824	[FF]	System and method for implementing safety instrumented systems in a fieldbus architecture

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

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

Information may be obtained from:

[FF] Fieldbus Foundation

9005 Mountain Ridge Drive
Bowie Bldg. - Suite 190
Austin, TX 78759-5316
USA
Tel: +1 512 794 8890

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

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES –

Part 3-1: Functional safety fieldbuses – Additional specifications for CPF 1

1 Scope

This part of the IEC 61784-3 series specifies a safety communication layer (services and protocol) based on CPF 1 of IEC 61784-1 and IEC 61158 Types 1 and 9. 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 61131-2, *Programmable controllers – Part 2: Equipment requirements and tests*

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

IEC 61158-3-1, *Industrial communication networks – Fieldbus specifications – Part 3-1: Data-link layer service definition – Type 1 elements*

IEC 61158-4-1, *Industrial communication networks – Fieldbus specifications – Part 4-1: Data-link layer protocol specification – Type 1 elements*

IEC 61158-5-5, *Industrial communication networks – Fieldbus specifications – Part 5-5: Application layer service definition – Type 5 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 61158-5-9, *Industrial communication networks – Fieldbus specifications – Part 5-9: Application layer service definition – Type 9 elements*

IEC 61158-6-5, *Industrial communication networks – Fieldbus specifications – Part 6-5: Application layer protocol specification – Type 5 elements*

IEC 61158-6-9, *Industrial communication networks – Fieldbus specifications – Part 6-9: Application layer protocol specification – Type 9 elements*

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

IEC 61508-1:2010[3], *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements*

IEC 61508-2:2010[3], *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*

IEC 61508-3:2010[3], *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements*

IEC 61508-4:2010[3], *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations*

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

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

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

ISO/IEC 8802-3, *Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications*

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] To be published.

[4] To be published.

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

3.1.1.4
communication channel
logical connection between two end-points within a *communication system*

3.1.1.5
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

3.1.1.6
connection
logical binding between two application objects within the same or different devices

3.1.1.7
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 [34], [35][5].

3.1.1.8
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[6]], [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*.

3.1.1.9
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

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

[6] To be published.

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)

3.1.1.10
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]

3.1.1.11
fieldbus
communication system based on serial data transfer and used in industrial automation or process control applications

3.1.1.12
frame
denigrated synonym for DLPDU

3.1.1.13
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 An FCS can be derived using for example a CRC or other hash function.

NOTE 2 See also [34], [35].

3.1.1.14
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]

3.1.1.15
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

3.1.1.16
master
active communication entity able to initiate and schedule communication activities by other stations which may be masters or slaves

3.1.1.17
message
ordered series of octets intended to convey information
[ISO/IEC 2382-16.02.01, modified]

3.1.1.18
message sink
part of a *communication system* in which *messages* are considered to be received
[ISO/IEC 2382-16.02.03]

3.1.1.19
message source
part of a *communication system* from which *messages* are considered to originate
[ISO/IEC 2382-16.02.02]

3.1.1.20
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]

3.1.1.21
proof test
periodic test performed to detect failures in a *safety-related system* so that, if necessary, the system can be restored to an “as new” condition or as close as practical to this condition

NOTE A proof test is intended to confirm that the safety-related system is in a condition that assures the specified safety integrity.

[IEC 61508-4 and IEC 62061, modified]

3.1.1.22
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]

3.1.1.23
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]

3.1.1.24
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[7].

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

[7] To be published.

3.1.1.25
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

3.1.1.26
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.

3.1.1.27
safety device
device designed in accordance with IEC 61508 and which implements the functional safety communication profile

3.1.1.28
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]

3.1.1.29
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[8], 5.2.4 and addressed by the functional safety communication profiles defined in this part.

3.1.1.30
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[9].

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]

3.1.1.31
safety measure
<this standard> measure to control possible communication *errors* that is designed and implemented in compliance with the requirements of IEC 61508

[8] In preparation.

[9] To be published.

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.

3.1.1.32
safety-related application
programs designed in accordance with IEC 61508 to meet the SIL requirements of the application

3.1.1.33
safety-related system
system performing *safety functions* according to IEC 61508

3.1.1.34
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

3.1.1.35
spurious trip
trip caused by the safety system without a process demand

3.1.1.36
time stamp
time information included in a *message*

3.1.2 CPF 1: Additional terms and definitions

3.1.2.1
client
connection entity that requests information from a server

3.1.2.2
cross-check
verification that the redundantly transmitted data are identical

3.1.2.3
H1
fieldbus standard communication data link

3.1.2.4
host
information processing unit that is able to perform the safety profile mechanisms, and services the black channel

3.1.2.5
macro cycle
single iteration of the link level schedule

3.1.2.6
masquerade
error due to mistaken identification information

3.1.2.7
publisher
message source that transmits messages on a periodic basis

3.1.2.8
queuing
sequential handling of items

3.1.2.9
server
communication entity that handles messages from a client

3.1.2.10
SIL environment
hardware and software suitable for SIS functions

3.1.2.11
subscriber
message sink that receives messages from a publisher

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	
EMI	Electromagnetic Interference	
EUC	Equipment Under Control	[IEC 61508-4:2010]
E/E/PE	Electrical/Electronic/Programmable Electronic	[IEC 61508-4:2010]
FAL	Fieldbus Application Layer	[IEC 61158-5]
FCS	Frame Check Sequence	
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]
PES	Programmable Electronic System	[IEC 61508-4:2010]
PFD	Probability of dangerous Failure on Demand	[IEC 61508-6:2010[10]]
PFH	Average frequency of dangerous failure [h^{-1}] per hour	[IEC 61508-6:2010]
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]
SR	Safety Relevant	

3.2.2 CPF 1: Additional symbols and abbreviated terms

AP	Application Process

[10] To be published.

ASIC	Application Specific Integrated Circuit
CAS	Cascade
CF	Common File
CFF	Common File Format
DD	Device Description
DO	Digital Output
FBAP	Function Block Application Process
FMS	Fieldbus Message Specification
LAS	Link Active Scheduler
LO	Local Override
LRSN	Last Sequence Number Received
MAU	Medium Attachment Unit
MD5	Message Digest Algorithm 5
MIB	Management Information Base
NMA	Network Management Agent
NMIB	Network Management Information Base
OD	Object Dictionary
OOS	Out Of Service
SIS	Safety Instrumented System
SMIB	System Management Information Base
SMK	System Management Kernel
SMKP	System Management Kernel Protocol
VCR	Virtual Communication Relationship

3.3 Conventions

3.3.1 State diagrams

Figure 3 shows an example state diagram which will be used in this part. A state is indicated by an oval with the state name in the center of the oval. In Figure 3, “Not Connected”, “Connected/Good”, and “Connected/Bad” are all states. A transition is indicated by a line or curve with an arrow indicating the direction of the transition. Each transition is named with a label on the line or curve. In Figure 3, “R1”, “R2”, “R3”, and “R4” are transitions.

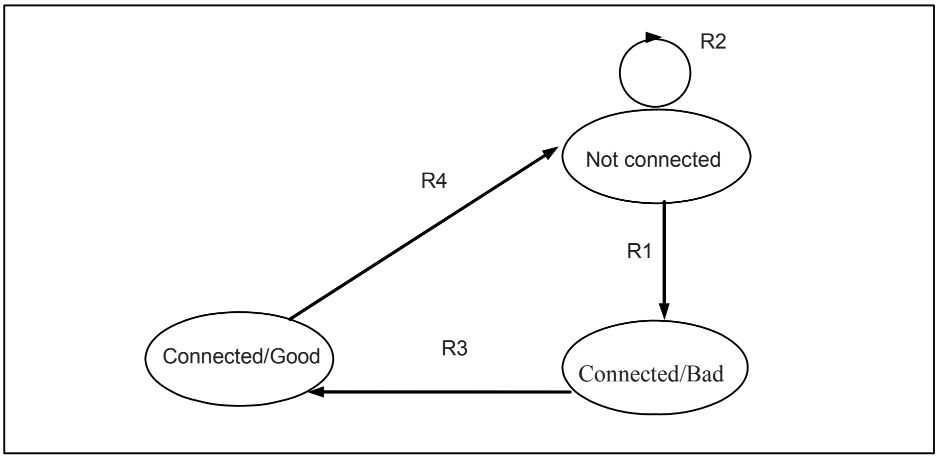


Figure 3 – Example state diagram

For each state diagram there will be a corresponding table as shown in Table 1. The first column labelled "#" contains the transition name. The second column labelled "Current state" contains the state that this transition applies to. The third column labelled "Event and condition action" contains the event, any conditions for the transition, and any actions. The actions are indented from the conditions. In Table 1, "RcvMsg() = "FMS Initiate.cnf"" is a condition where a "SET Sequence Number = MCN" is an action. The fourth column labelled "Next state" contains the new state after this transition.

Table 1 – Example state transition table

#	Current state	Event and condition action	Next state
R1	Not connected	RcvMsg() = "FMS Initiate.cnf" SET Sequence Number = MCN	Connected/ Bad
R2	Not connected	RcvMsg() = "Any message (not FMS Initiate.cnf)"	Same
R3	Connected/ Bad	RcvMsg() = "Abort.ind" OR RcvMsg() = "Abort.req"	Not connected
R4	Connected/ Good	RcvMsg() = "Abort.ind" OR RcvMsg() = "Abort.req"	Not connected

3.3.2 Use of colors in figures

The use of colors in figures is not normative and is used only for clarity of the figure. The convention for use of colors is described in Figure 4. Any colors not shown are used for clarity of the figure only.

🟨 = Safety-related

⬛ = Black Channel

🟧 = FSCP 1/1 Protocol

Figure 4 – Use of colors in figures

4 Overview of FSCP 1/1 (FOUNDATION Fieldbus™ SIS)

4.1 General

Communication Profile Family 1 (commonly known as FOUNDATION™ Fieldbus[11]) defines communication profiles based on IEC 61158-2 Type 1, IEC 61158-3-1, IEC 61158-4-1, IEC 61158-5-5, IEC 61158-5-9, IEC 61158-6-5, and IEC 61158-6-9.

The basic profiles CP 1/1, CP 1/2, and CP 1/3 are defined in IEC 61784-1. The CPF 1 functional safety communication profile FSCP 1/1 (FF-SIS™[11]) is based on the CP 1/1 basic profile in IEC 61784-1 and the safety communication layer specifications defined in this part.

[11] FOUNDATION™ Fieldbus and FF-SIS™ are trade names of the non-profit organization Fieldbus Foundation. This information is given for the convenience of users of this International Standard and does not constitute an endorsement by IEC of the trade name holder or any of its products. Compliance to this part of IEC 61784-3 does not require use of the trade names Foundation Fieldbus™ or FF-SIS™. Use of the trade names FOUNDATION™ Fieldbus or FF-SIS™ requires permission from the Fieldbus Foundation.

NOTE 1 The FOUNDATION™ Fieldbus Specifications AG-180 [45], FF-807 [46], FF-884 [47], and FF-895 [48] are applicable to this protocol.

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

NOTE 2 These safety-related applications are also called safety instrumented systems (SIS) (see IEC 61511 series).

The FSCP 1/1 safety communication layer specified in this part makes it possible to use intelligent devices in a safety-related system adding more capability to the system, yet the system can meet its safety integrity level requirements. The safety communication layer specified in this part is only applicable to CP 1/1 as described in IEC 61784-1. The scope of this part is defined in Figure 5.

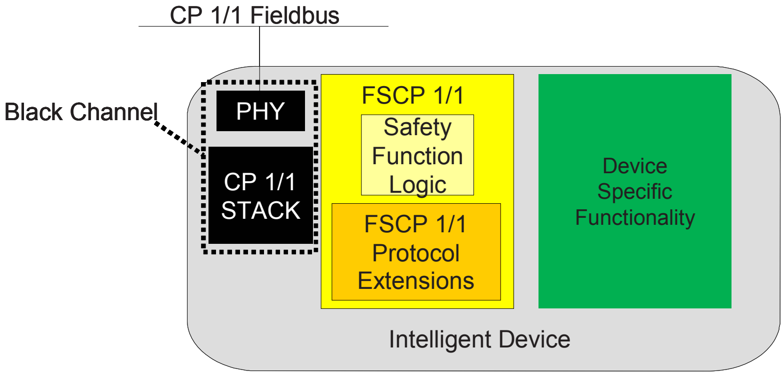


Figure 5 – Scope of FSCP 1/1

This part does not define requirements for engineering tools or internal measurement functionality of devices. The safety communication layer ensures that a configuration created using an engineering tool is downloaded into the safety devices without the protocol impacting the safety integrity level.

FSCP 1/1 alone does not ensure functional safety. In addition to FSCP 1/1 protocol interoperability registration, the vendor will also obtain functional safety assessment for the products, systems, and software. The user shall ascertain the suitability of use of all safety-related equipment in the safety function in accordance with IEC 61508.

4.2 Key concepts of FSCP 1/1

4.2.1 Black channel

This is the concept of using a non-trusted communication system (for example wires, fiber optics, repeater, barrier, ASIC, communication stack, linking device, interface) to provide a reliable communication channel. The black channel includes the part in a device known as the communications entity as well as the SMK and SMKP. FSCP 1/1 diagnostics control faults in the black channel. The black channel can fail any time but communications failures are detected so as to control faults within the process safety time. The failure detection diagnostics shall comply with IEC 61508, the black channel needs not. The FSCP 1/1 protocol does not rely on the 16-bit CRC in the H1 data-link layer FCS.

4.2.2 Connection key

The connection key is a unique number for each connection, a source-destination relationship "codeword", which is given by the host to each safety link object at configuration time. Unlike the black channel address, the connection key is protected by the safety communication layer CRC. The connection key is unique within the safety communication layer. When devices are replaced, the same connection key may be reused and downloaded to the new device. The device configuration including the connection key is cleared in a removed device before it is connected on a FSCP 1/1 network again in another service. Devices may automatically clear their configuration when the black channel address is changed; alternatively, devices may have a reset button or equivalent to clear their configuration.

4.2.3 Cross-check

This is a comparison of the application data, sequence number, and CRC that have been redundantly transmitted (twice within the same message) to ascertain that the two copies are identical.

4.2.4 FSCP 1/1

FSCP 1/1 provides a closed transmission system suitable for use in a safety-related system. It achieves trusted communication between safety-related applications.
(Adapted from IEC 62280-1).

4.2.5 Programmable electronic system

This is a system for control, protection or monitoring based on one or more programmable electronic devices. It includes all elements of the system such as power supplies, sensors and other input devices, data highways and other communication paths, and actuators and other output devices. The structure of a PES may have the programmable electronics as a unit distinct from sensors and actuators on the EUC and their interfaces, but the programmable electronics could exist at several places in the PES.
(Adapted from IEC 61508-4:2010, 3.3.1).

4.2.6 Queuing delays

One possible fault is that messages are held up in the black channel due to queuing in the device communication stack or in intelligent network hardware including repeaters, hubs, bridges, switches, and linking devices. Unconfirmed published messages may be coming through the black channel successfully, even at an acceptable rate, but may, due to long or multiple queuing at various stages along the black channel path, be older than the process safety time allows. This fault is a type of delay fault, where the delay is introduced by devices in the black channel queuing messages.

4.2.7 Redundancy

Redundancy is the use of additional hardware, software or data above that needed in an error free environment.

EXAMPLE Duplicated functional components and the addition of parity bits are both instances of redundancy.

NOTE Redundancy is used primarily to improve reliability or availability (IEC 61508-4:2010, 3.4.6).

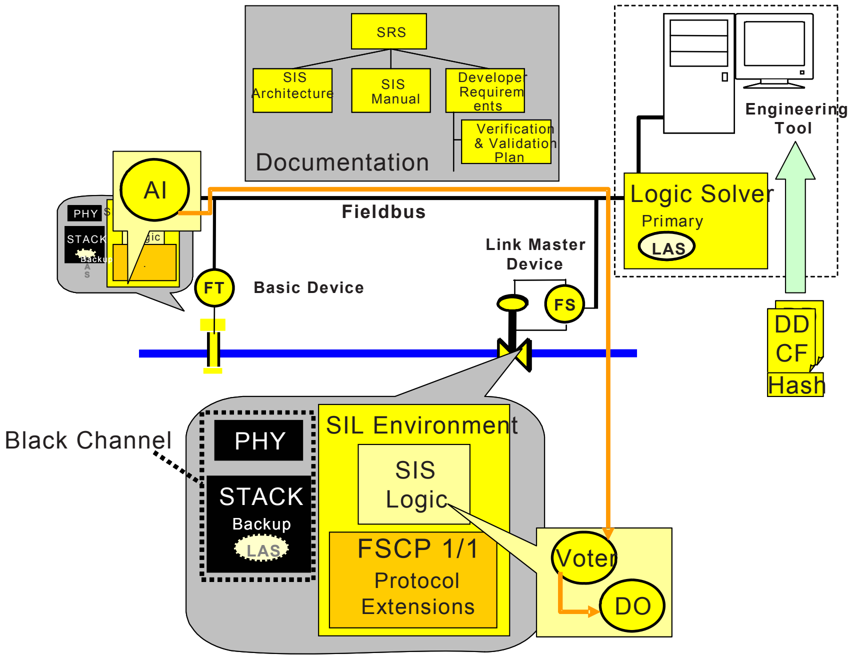
4.2.8 SIL environment

FSCP 1/1 compliant hardware and software components may be built into a system that is a suitable environment for implementation of safety-related applications.

4.3 Key components of FSCP 1/1

4.3.1 Overview

The fieldbus communication hardware and stack are not trusted. A safety communication layer above the communication stack ensures trustworthy communication over the fieldbus, and a safety link object in the FBAP contains the additional information required by the FSCP 1/1 protocol. These are shown in Figure 6. In a safety device the application process and safety communication layer will execute in a SIL environment. A set of simplified function blocks suitable for safety-related applications have been created.



LAS = Link Active Scheduler

Figure 6 – FSCP 1/1 architecture (H1)

The FSCP 1/1 protocol controls failures such as device or wire malfunctions as well as sporadic disturbances such as EMI. The safety communication layer detects the following types of communication error: repetition, deletion, insertion, re-sequencing, data corruption, masquerading, and delay.

4.3.2 Black channel

The black channel concept as shown in Figure 7 permits safety data to be transmitted across a non-trusted bus. There is no need for physical separation of safety functions and non-safety hardware. Safety and non-safety devices and data can share the bus, as shown in Figure 7.

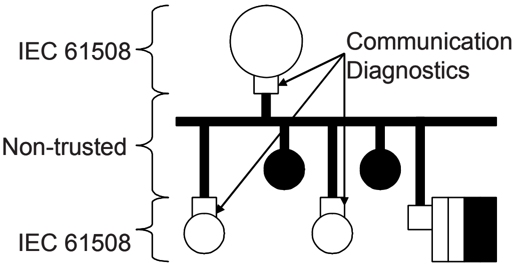


Figure 7 – Black channel

Only one LAS is permitted on an H1 network. Safety-related and non-safety-related applications can exist in the same device. FSCP 1/1 transmission is logically separated from non-FSCP 1/1 transmission. A single-channel configuration, that is a non-redundant bus, is sufficient. A safety device can provide both safety and non-safety function blocks. FSCP 1/1 protocol is used with safety function block links. Regular CP 1/1 is used with non-safety function block links. Thus a safety device can be used for safety or non-safety functions.

Failures may result from effects other than actual failures of hardware components (for example electromagnetic interference, decoding errors), however, such failures are

considered to be random hardware failures.
(Adapted from IEC 61508-2:2010[12], 7.4.5.2).

To increase availability, hot-standby bus redundancy may be used. A single channel is expected to be used between instruments and a logic-solver. Redundant channels are expected to be used for communication between logic-solvers.

4.4 Relationship to the ISO OSI basic reference model

The safety communication layer is implemented above the communication stack in the application layer.

5 General

5.1 External documents providing specifications for the profile

The following documents provide additional specifications which may be relevant for the design of FSCP 1/1:

- FOUNDATION™ Fieldbus AG-180 [45];
- FOUNDATION™ Fieldbus FF-807 [46];
- FOUNDATION™ Fieldbus FF-884 [47];
- FOUNDATION™ Fieldbus FF-895 [48].

5.2 Safety functional requirements

5.2.1 Requirements for functional safety

The following list are the functional safety requirements used in the development of the FSCP 1/1 protocol.

- FSCP 1/1 shall be designed to permit vendors to develop products suitable for use in SIL 2 (IEC 61508) applications, SIL 3 is recommended.
- The protocol shall support the publisher/subscriber and client/server connection.
- The safety related protocol shall prevent interference from non-safety related devices. For example a non-safety related handheld shall not be permitted to change parameters in a safety related device.
- The protocol shall protect against unintended or non-authorized configuration changes to a safety device.
- The contribution of the FSCP 1/1 protocol to PFD/PFH shall be less than 1 % of the value required by the SIL level.
- PFD/PFH calculations shall be based on demand mode and high demand mode (as defined in IEC 61508).
- The protocol shall implement measures to control the following faults:
  - transmission bit failure/falsifying;
  - retransmission;
  - omission;
  - insertion/expansion;
  - wrong order;
  - delay;

[12] To be published.

- addressing failures/masquerading;
- queuing.

NOTE A queuing fault is a type of delay fault.

- It shall be possible to calculate the reaction time for the application.
- The function block implementation shall be in accordance with IEC 61508-3 to the required SIL.
- Devices with different SIL levels shall be possible on the same network.
- It shall be possible to by-pass the devices in a safe manner.

5.2.2 Functional constraints

The following is a list of functional constraints used in the development of FSCP 1/1.

- Using safety communication and standard communication by means of standard devices and safety devices at the same CP 1/1 bus shall be possible.
- ASICs, communication stack, repeaters, wiring hardware, power supplies, and accessories shall remain unmodified (black channel) safety functions above OSI layer 7.
- The protocol shall have the mechanisms to permit a host to detect a mismatch in the device type or device revision or DD revision or capability file revision or SIL level.

5.2.3 Device manufacturer requirements

The following list is the set of requirements that FSCP 1/1 places on the device vendor.

- Environmental conditions and electrical safety according to IEC 61131-2 requirements.
- The hardware shall be in accordance with IEC 61508-2 to the required SIL.
- The software shall be in accordance with IEC 61508-3 to the required SIL.
- Hardware and software assessment shall be done by a competent and independent test organization according to IEC 61508-1.

5.3 Safety measures

5.3.1 Sequence number

Each safety protocol data unit has an incrementing sequence number which is the macro cycle number when the message was generated.

5.3.2 Time stamp

The sequence number included in the safety protocol data unit is also a time stamp, since it is the macro cycle number.

5.3.3 Time expectation

The sequence number/time stamp is used to verify that messages are delivered in a timely manner. There is also a stale counter for each connection that detects when messages have not been received within the expected time frame.

5.3.4 Connection authentication

There is a connection key associated with each connection that is used to verify that a safety protocol data unit is from the correct message source.

5.3.5 Data integrity assurance

Each safety protocol data unit has a CRC to insure data integrity.

5.3.6 Redundancy with cross checking

Each safety protocol data unit contains two copies of the data and CRC. The duplication of the data and CRC is used to cross check the data.

5.3.7 Different data integrity assurance systems

The safety protocol data unit has additional CRCs that are different from the black channel data integrity system.

5.3.8 Relationships between errors and safety measures

The safety measures outlined in 5.3.1 to 5.3.7 can be related to the set of possible errors. This relationship is shown in Table 2. Each safety measure can provide protection against one or more errors in transmission. It shall be demonstrated that there is at least one corresponding safety measure or combination of safety measures for the defined possible errors in accordance with Table 2.

Table 2 – Safety measures and possible communication errors

Communication errors	Safety 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	X						
Incorrect sequence	X	X						
Loss	X							
Unacceptable Delay		X	X					
Insertion	X							
Masquerade								X
Addressing				X				
NOTE Table adapted from IEC 61784-3.								

5.4 Safety communication layer structure

5.4.1 Network topology and device connectivity

5.4.1.1 General

Safety and non-safety devices can share the same fieldbus, as shown in Figure 8. The entire safety function from sensor to actuator shall be taken into account. The fieldbus link is designed to consume no more than 1 % of the PFD budget.

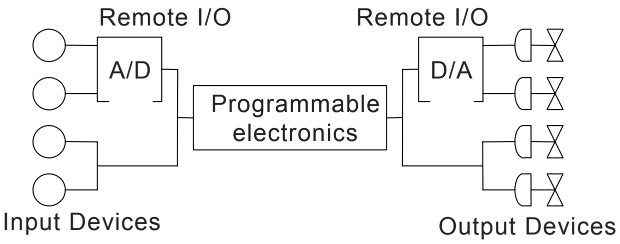


Figure 8 – FSCP 1/1 in system architecture

NOTE The programmable electronics are shown centrally located but could exist at several places in the PES.

5.4.1.2 Single H1 link topology

A safety function consists of a single H1 link. The link is part of the black channel. Safety devices and non-safety H1 devices are networked identically.

5.4.2 Device architecture

5.4.2.1 General

The black channel concept permits the communication hardware (including ASIC and MAU) and communication software stack to be non-trusted while the FSCP 1/1 protocol communications diagnostics and function block application executes in a SIL environment consisting of SIL hardware and software. The safety communication layer is the interface between the SIL application process and the non-trusted black channel communication entity, as shown in Figure 9.

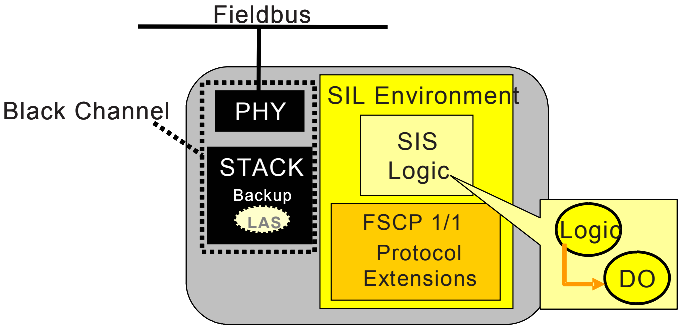


Figure 9 – FSCP 1/1 H1 device

Care needs to be taken when implementing the black channel concept to ensure that non-SIL hardware and software does not interfere with the SIL hardware and software.

5.4.2.2 H1 device architecture

Application processes are safety related and will be executed in a SIL environment. The communications entity consists of the communication stack, FMS, NMA, and NMIB which are non-trusted. The communications entity, as well as SMK and SMKP, are part of the black channel. Their relationship is shown in Figure 10.

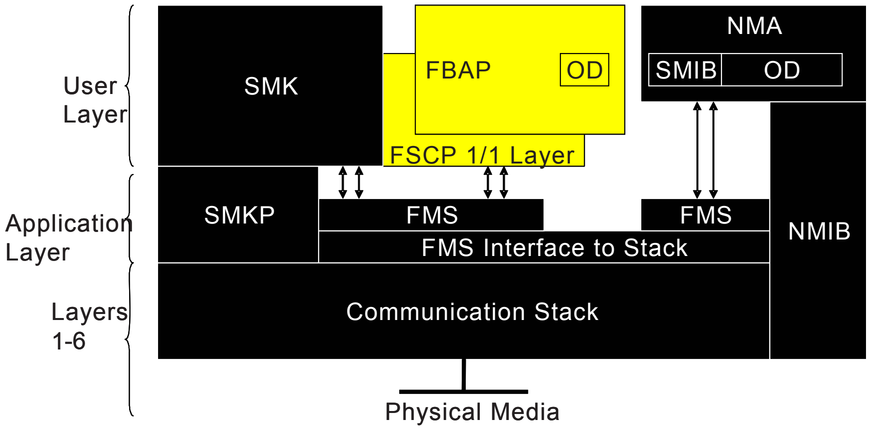


Figure 10 – FSCP 1/1 protocol layers

5.5 Relationships with FAL (and DLL, PhL)

5.5.1 General

Figure 11 shows the relationship between FSCP 1/1 and the other layers of IEC 61158 Type 1.

FBAP	FSCP 1/1
FSCP 1/1	
FMS	IEC 61158 Type 1
FAL	
DLL	
PhL	

Figure 11 – Relationship between FSCP 1/1 and the other layers of IEC 61158 Type 1

5.5.2 Data types

FSCP 1/1 uses the basic data types listed in Table 3 according to CPF 1 in IEC 61784-1.

Table 3 – Data types used within FSCP 1/1

Data type name	Number of octets
Integer8	1
Integer16	2
Integer32	4
Unsigned8 (used as bits)	1
Unsigned16 (used as bits)	2
Unsigned32 (used as bits)	4
Unsigned16	2
Unsigned32	4
Floating Point 32	4
Date	
TimeOfDay with date indication	
TimeOfDay without date indication	
TimeDifference with date indication	
TimeDifference without date indication	
Visible string	1,2,3, …

6 Safety communication layer services

6.1 Application Process (AP)

6.1.1 Overview

Safety and non-safety functions can be allocated in the same or different application processes in a device. The AP for safety functions requires a SIL environment and is not part of the black channel.

The FSCP 1/1 layer is independent of the application process and therefore can be used with the function block application process or another kind of application process.

6.1.2 Network visible objects

The application process accesses the application layer in the black channel communication stack, not directly, but through the FSCP 1/1 layer.

6.1.3 Application layer interface

The same set of messaging services provided by FMS for non-safety objects is provided by the safety communication layer for the safety objects.

6.1.4 Object dictionary

There is no change to the fieldbus Object dictionary to support the black channel.

6.1.5 Application program directory

There is no change the Application Process directory to support the black channel.

6.2 Function block application processes

6.2.1 General

Simple function blocks have been defined and are suitable for safety-related applications. A FBAP containing safety objects will execute in a SIL environment.

The use of function blocks is optional. A host will probably not implement function blocks.

6.2.2 Function block model

6.2.2.1 Stale count

The end-to-end stale count check, which is based on sequence number mismatch, controls faults in scheduling and execution of the logic chain up to the output function block. A stale data timer after the output function block controls faults in scheduling and execution of the output function block itself. If update from the output function block is not received within the set time limit due to a scheduling or execution error, the output will go to the fault state. The use of a stale data timer after the output function block is a safety measure independent of the non-SIL SMK that checks that the function blocks are executing. If a function block is not executing, the outputs are not propagated to the black channel. The missing publication is a fault controlled downstream, the sequence number mismatch will cause a preconfigured fault state action. The sequence number for the link used in the FSCP 1/1 protocol is computed from the macro cycle number based on data link time and therefore changes for every new PDU delivered to the black channel. If the black channel misbehaves and is publishing old data, the sequence number will not match making it possible to detect such faults downstream.

The end-to-end stale-count mechanism detects faults such as: function block stopping executing, executing in the wrong order, at the wrong time, or with too much jitter. These faults may be due to faults in scheduling, in the function block itself, or longer than the worst expected function block execution time.

6.2.2.2 Simulation

To enable simulation, the write-lock in the resource block and simulation protection will be off. If the write-lock is turned back on, simulation is automatically disabled. In addition, simulation enable is required to be in non-volatile memory. When power is turned on simulation is always disabled.

A non-safety function alarm is issued when simulation is enabled. The host needs to check periodically to determine if simulation is enabled in any of the devices.

6.2.2.3 Write-lock

A write-lock protects the device configuration. When the write-lock in the safety device resource block is set, all writes to the resource are disabled, including the MIB but excluding the write-lock itself. Protected contents of the MIB include object (blocks, links, VCRs), address, parameters and device tag.

A safety lock function block in every safety device is able to write to the write-lock parameter in the resource block of the same device. The safety lock function block has a write-lock input which accepts a safety function block link. This permits writes to several devices to be enabled or disabled remotely from a central location. The safety lock function block can activate and deactivate the write-lock in the device using key switch though a DI function block. Figure 12 shows the architecture of this lock.

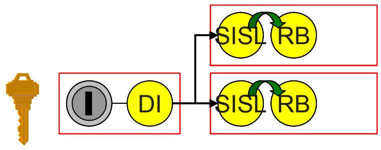


Figure 12 – Key write-lock

Write-lock can also be activated and deactivated by writing a parameter in the safety lock function block. Writing this parameter is usually protected by appropriate passwords in the host. Figure 13 shows the architecture of this lock.

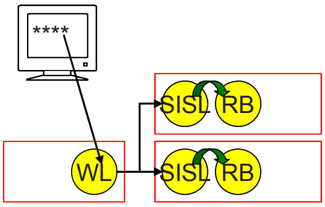


Figure 13 – Password write-lock

6.2.2.4 Trip and reset

For the FSCP 1/1 output function block the fault state can be configured de-energized-to-trip, energized-to-trip, or hold last value. If the cascade input of an output function block has a Bad status, for example due to lost communication, this is also reflected as a Bad::non-specific substatus on the feedback output of the output function block. The physical output may trigger on a genuine process demand from the logic solver logic, communication or upstream function block execution error, through operator intervention, or on device fault.

There is a distinction between preconfigured fault state action in response to process demand, communication or upstream function block execution error and trip due to device and power fault. On a process demand the output function block acts on its input signal where zero (0) always means preconfigured fault state action, and one (1) always means OK to run. For energize-to-trip the signal is inverted in the output function block. On a communication error the output function block does not take action until fault-state time has elapsed, and then it either holds its last position or goes to the fault value as set by the fault-state option and fault-state value.

In normal operation the output function block is in cascade mode. By default the mode will remain in cascade on a process demand. Optionally for process demand and for communication error, the output can be latched in its fault state. When the latch fault state option is enabled and a process demand or communication error occurs, the DO function block goes to local-override (LO) mode. Even if the demand or fault condition is cleared, the output remains in its fault state until reset by the user. A logic solver can monitor the output from the feedback output of the output function block and optionally alarm on Bad status. If latched, operator will unlatch it, either through resource block fault state clear or through the reset input of the output function block. If a device is configured for a de-energized fault state this may through the hardware result in, for example, a valve opening or closing. Table 4 lists this behaviour.

If the input status is Bad or Good::Initiate-fault-state the output will also take preconfigured fault state action.

Table 4 – Fault state behaviour

Condition	Example	DO Fault State Delay	DO Fault State Option	DO Fault State Latch	Remark
Bad status, communication or upstream function block execution error	Cascade input bad due to safety communication layer CRC failure, sequence number mismatch or redundancy cross-check mis-comparison	Yes	Energized		
De-energized					
Hold	Optional LO mode				
Initiate fault-state	Substatus received from another function block or logic solver	Yes	Energized		
De-energized					
Hold	Optional LO mode				
Operator intervention	Set fault-state from resource block	No	Energized		
De-energized					
Hold	Always LO mode				
Process demand from logic solver	Discrete cascade input is zero (0)	No	No	Optional LO mode	Usually CAS mode
Black channel failure	Time synchronization error	Yes	Energized		
De-energized					
Hold	Optional LO mode				

Provided the condition that caused the preconfigured fault state action has cleared, the user can reset the latched output by using the clear fault state parameter in the resource block or a clear fault state input in the output function block itself.

6.2.3 Application process

6.2.3.1 General

Standard FSCP 1/1 function blocks have been defined. Manufacturers can create enhanced and custom safety function blocks. All FSCP 1/1 blocks are identified by profile numbers within a specified range. This permits the host to interact with FSCP 1/1 blocks as required.

6.2.3.2 Block types

6.2.3.2.1 General

Additional standard function blocks and resource block have been created for FSCP 1/1. The standard FSCP 1/1 function blocks are identified by profile numbers within a specified range. The FSCP 1/1 function blocks have fewer permitted mode and parameter options than their regular counterparts. The manual mode is only allowed while the device is not write-locked, the same applies to the automatic mode for output function blocks. When the device writes are unlocked, the function block modes will go to the operational automatic and cascade modes respectively.

Fault state behaviour in safety output function blocks is mandatory.

6.2.3.2.2 Safety device resource block

The resource block write-lock parameter has the important function of a lockout mechanism that prevents writing to the entire resource.

The current safety communication layer statistics can be accessed through the safety device resource block. FSCP 1/1 protocol statistics consist of a counter of the number bad safety communication layer CRC faults detected.

The safety communication layer statistics also contain a black channel error parameter with a flag indicating that a time synchronization fault occurred.

The safety device resource block contains a parameter to unlock write protection of the device. This will be done before parameters and other objects can be written. The safety lock function block simplifies the locking and unlocking of writes in multiple devices.

The safety device resource block contains a parameter to clear all tripped outputs that have been latched in fault state output.

The safety device resource block contains a macro cycle duration parameter since the data in the black channel cannot be relied on.

The safety device resource block contains parameters informing the hardware revision and firmware revision as well as checksums for the firmware and the configuration.

6.2.3.2.3 Additional function blocks

6.2.3.2.3.1 General

Safety applications require inputs, outputs, and logic. Therefore a new set of safety function blocks providing these capabilities is provided. The new safety function blocks include:

- safety analog input;
- safety discrete input;
- safety lock;
- safety discrete output;
- safety logic;
- safety analog comparator.

The SR-AI, SR-DI, and SR-DO function blocks have reduced functionality as compared to their regular counterparts so as to simplify implementation for implementers and reduce mistakes and make verification easier for users. Simplification includes fewer supported modes and no alarms.

6.2.3.2.3.2 Safety output function blocks

The safety output function blocks are important because these are where the preconfigured fault state action is taken. Apart from preconfigured fault state action on the process demand value received on the cascade input, the output function block will also take preconfigured fault state action on bad status, initiate fault state, upstream function block execution error, and stale communication. The output transducer will trip on the failure of its associated output function block in the safety function to execute. The output transducer controls scheduling and communication faults for the safety function by tripping if it has not been updated with fresh data within the stale data timer setting. When the output function block takes preconfigured fault state action due to a genuine process demand, status, or communication fault, the mode will by default remain in cascade. Safety output function blocks include optional functionality to latch tripped outputs. A feedback output on the output function block shows Bad::non-specific status if the cascade input has bad communication. Other faults in the output will also be reflected by the status. Optionally a non-safety alert may be sent on fault state if the device supports it. The feedback status and alarm details will indicate if the fault state is a genuine process demand or due to a fault. From the mode parameter in the output function block it is possible to see if the output is in a fault state condition using FSCP 1/1 communication. An individual latched output can be cleared using a reset input parameter in each output function block. The reset input accepts a safety function block link thus permitting the fault state to be reset remotely and through logic from another function block. All tripped outputs can be cleared using a parameter contained in the resource block.

Advanced valve diagnostics such as partial stroke testing, analog position feedback on discrete valves, and position deviation alarms, are expected to be implemented in transducer blocks by vendor specific means. Future transducer block profile teams may define standard parameters for these devices.

6.2.3.2.3.3 Safety lock function block

The safety lock function block unlocks write-protection based on link inputs enabling central locking and unlocking of several devices.

Before parameters can be written the resource will be unlocked. This is equivalent to a lockout key on a safety system console. Because there may be many safety devices, and they are often inconveniently mounted in hazardous areas and otherwise inaccessible, unlocking and lockdown will be possible through FSCP 1/1 communication. Soft write-lock is mandatory in the safety resource block.

6.2.3.2.4 Safety link object

The FSCP 1/1 protocol extensions are reflected in the safety link object. A different link object storing additional information is used for FSCP 1/1 function block links. The safety link object contains the connection key and end-to-end stale count limit required for safety applications. Multiple independent safety function chains can exist on the same network or in same device or logic-solver, a failure in one safety function chain shall not require a shutdown in the other safety function chains on the same bus or in the same devices or logic solver. To ensure interoperability with existing equipment in non-safety-related applications it is mandatory that a device also supports the non-safety link object.

6.2.3.2.5 Stale data timer

The end-to-end stale count mechanism catches function block execution errors up to, but excluding, the output function block. A second mechanism, the Stale Data Timer trips the output if the output transducer block does not get updated by the output function block in a timely manner, such as due to output function block execution failure. The output stale data time is configured through the output function block. The stale data time shall not be confused with the fault-state time.

Similarly a manufacturer specific mechanism monitors execution of other blocks, including transducer blocks.

EXAMPLE If the input transducer block is not executed properly then the input function block output status is bad.

6.3 Device to device communications

6.3.1 General

FSCP 1/1 communication is supported for publisher/subscriber and client/server communications but not for report distribution. A safety device can still use the report distribution VCR to transmit alerts, but the mechanism cannot be trusted. Figure 14 illustrates this communication.

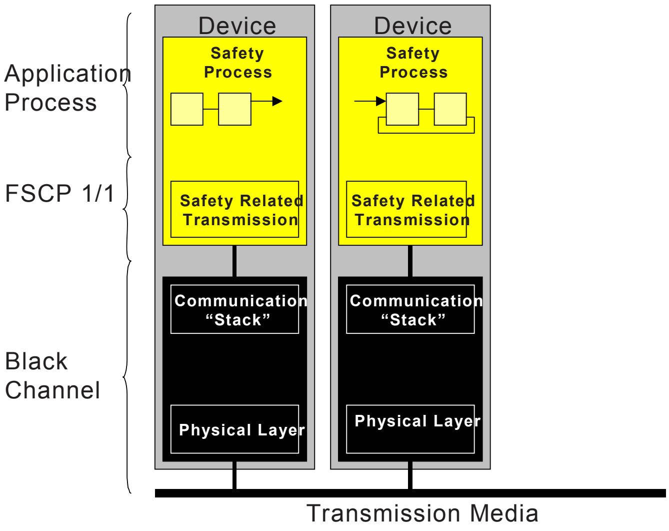


Figure 14 – Example of FSCP 1/1 communication

6.3.2 Client/server

Client/server read and write is supported in a safety device. Client/server is used by the user to write parameters. After changes are made, a functional test should be done by the user as defined in IEC 61508.

The client/server VCR is not deterministic and not truly timed. Client/server VCRs are not suitable for the shutdown path.

Parameters and objects can be written, but FSCP 1/1 communications is first required to enable writes. A write-lock exists in the resource block that protects all the objects in the resource. After a configuration change the user is required to perform a proof test. FSCP 1/1 communications is then used to disable the further writing.

Read-requests and write-responses use the regular CP 1/1 protocol. Write-requests and read-responses use the FSCP 1/1 protocol. A client/server link object (with connection key etc.) shall be created for each client (interface) that will be permitted to read/write a device. Every message will have a CRC. The connection key is included as part of the virtual header, which is used in the calculation of the CRC.

FSCP 1/1 function blocks have FSCP 1/1 links configured in safety link objects. The FSCP 1/1 protocol is an extension of the PDU, not a new data type.

FSCP 1/1 uses redundant transmission, meaning that data, sequence number, and CRC are transmitted twice and cross-checked at the receiving end.

6.3.3 Publisher/subscriber

FSCP 1/1 function blocks have FSCP 1/1 links configured in safety link objects. The FSCP 1/1 protocol is an extension of the PDU, not a new data type. In addition to the safety communication layer CRC, the published safety PDU also includes a sequence number that permits the subscribers control of additional faults.

FSCP 1/1 uses redundant transmission, meaning that data, sequence number, and CRC are transmitted twice and cross-checked at the receiving end.

6.3.4 Report distribution

There is no FSCP 1/1 protocol extension for the report distribution VCR and therefore it is not trusted. A safety device can send non-safety alerts.

6.3.5 FBAP operation in a linking device

An application process in a linking device is accessed in the same way as a FSCP 1/1 FBAP.

6.3.6 System management kernel protocol (SMKP) communications

SMKP is part of the black channel. Faults in the local interface between the SMKP and the application process are controlled by manufacturer specific means.

6.4 Profiles

6.4.1 General

A profile is a subset, a selection, chosen from a larger general specification. An FSCP 1/1 profile is thus a restricted version of the full FSCP 1/1 functionality. New profiles are created for FSCP 1/1.

6.4.2 FSCP 1/1 profile

6.4.2.1 General

FSCP 1/1 H1 devices can also be categorized into classes based on their capabilities. FSCP 1/1 H1 devices belong to one or more of the following sets of classes:

- H1 FSCP 1/1 Field devices - control devices that reside on H1 links;
- FSCP 1/1 Host devices - perform user interface and configuration functions - a logic solver with configuration tool.

6.4.2.2 Block parameterization

All parameters in safety blocks can be written either using non-FSCP 1/1 client/server VCR, before the FSCP 1/1 client/server link object has been created, or FSCP 1/1 client/server VCR once the FSCP 1/1 client/server link object has been created. FSCP 1/1 requires the resource block to be "unlocked" before anything in the resource can be written. After changes are made a functional test should be done.

6.4.2.3 Block parameterization lockout

Before parameters can be written the resource needs to be unlocked. This is equivalent to a lockout key on a safety-related system console. Because there may be many safety devices, and they are often mounted in hazardous areas or otherwise inaccessible, unlocking and locking will also be possible through FSCP 1/1 communication. Soft write-lock is mandatory in the safety resource block.

One of many conceivable implementations of this is a function block which, when an input is activated, writes the write-lock parameter in the device in order to enable configuration. A function block is provided for this purpose.

6.4.2.4 User authentication

The host software has to ensure that only authorized users are given access to programming and parameterization.

6.4.2.5 Programming lockout

Before objects can be changed the resource needs to be unlocked. This is equivalent to a lockout key on a safety-related system console. Because there may be many safety devices, and they are often mounted in hazardous areas and otherwise inaccessible, unlocking and locking will be possible through FSCP 1/1 communication. The programming lockout is based on the resource write-lock parameter in the resource block. Objects other than blocks, such as link objects, can only be written when the resource is unlocked.

Program changes should be done with the process shutdown (the devices will still be executing blocks) where the host communicates with the devices.

6.5 Device descriptions

Device descriptions are an integral part of the configuration tool. An MD5 hash will be generated for each of the DD and capabilities files to ensure the integrity of the file. The MD5 hash for the DD/CF files will be stored under a special keyword in the FSCP 1/1 capabilities file. This is shown in Figure 15.

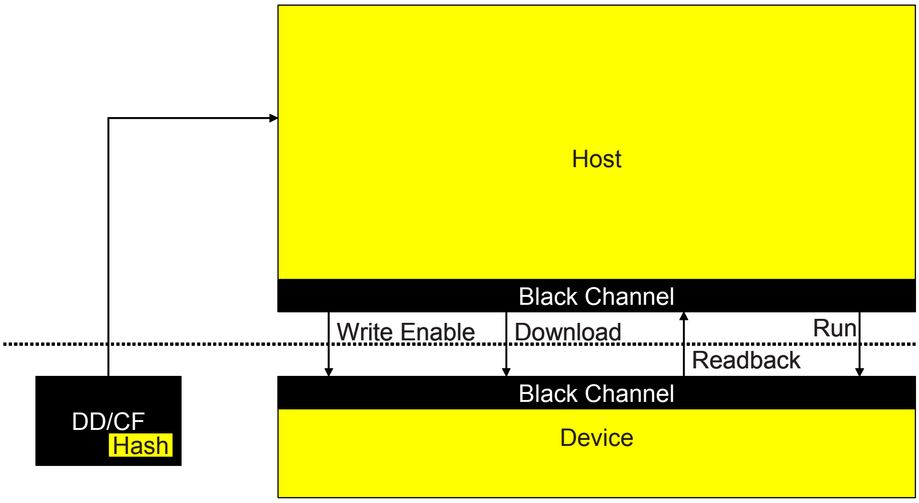


Figure 15 – Example of device description

6.6 Common file formats

Capabilities files are an integral part of the configuration tool. The hash mechanism is described for DD and is the same for CF.

The digest of the MD5 hash over the DD and CFF files is stored in the end of the CFF file.

The capabilities file contains parameters that inform the failure rates of the device. There are also parameters for product design level, that is, the fault avoidance gained (for example during the design process requirements for a SIL 2 device may have been followed, even though failure rates are good for SIL 3).

6.7 Configuration information

6.7.1 Overview

FSCP 1/1 configuration will be largely the same as non-safety configuration but with the addition of writing safety function block parameters such as the Stale Data Timer, end-to-end stale count limit, and macro cycle. FSCP 1/1 function block links use the safety link object where the connection key needs to be set. It is expected that the configuration tool will automatically manage the configuration of the connection key and macro cycle. Once a device is operational, changes to any function blocks are not permitted.

6.7.2 Level 1 configuration: manufacturer device definition

Implementation issues for safety devices include measures for physical or logical separation of safety (application process and safety communication layer) and non-trusted (black channel stack) functions in order to ensure of non-interference. Function block applications for safety-related and non-safety-related applications may reside in same or different VFDs.

6.7.3 Level 2 configuration: network definition

Configuration of the black channel is unchanged.

6.7.4 Level 3 configuration: distributed application definition

A special link object is used for safety function blocks. The expected propagation time for the channel shall be calculated.

The user defines the process safety time. The macro cycle, end-to-end stale count limits and stale data timer needs to be configured accordingly.

6.7.5 Level 4 configuration: device configuration

The macro cycle time shall be set using the parameter in the resource block.

7 Safety communication layer protocol

7.1 Safety PDU format

7.1.1 General

The FSCP 1/1 protocol controls failures during communication. The FSCP 1/1 protocol is applied to the FMS communications protocol. Faults in the local interface between the application process and the SMK as well as the SMIB in the NMA are controlled by manufacturer specific means. The FSCP 1/1 protocol is applied to FMS communications across the fieldbus.

7.1.2 Safety communication layer CRC

Cyclic redundancy check is used to control data corruption failures in fieldbus communication. Data is transmitted together with a calculated CRC checksum for each safety PDU. The safety communication layer CRC is defined by CCITT 32 V.42 and ISO/IEC 8802-3 (IEEE 802.3). It is a 32 bit polynomial calculated as follows:

$(x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^{8} + x^{7} + x^{5} + x^{4} + x^{2} + x + 1)$.

The receiver safety communication layer re-calculates the checksum of the received data and compares the result with the received checksum. Corrupted messages are rejected.

7.1.3 Black channel time synchronization monitoring

The sequence number is based on the macro cycle number derived from the data link time for each publication. The sequence number is in effect a sort of timestamp. All devices on the H1 network have a common sense of macro cycle. Devices on an H1 network thus rely on a common sense of time based on a correctly working time synchronization mechanism. Synchronized time is required to ensure synchronous execution of function blocks and communications thus ensuring the shortest safety function response time possible. The time synchronization mechanism corrects the data link time and frequency and resides in the black channel but it is monitored by the safety communication layer. The safety communication layer has an independent safety time source and detects loss of time synchronization in the black channel by comparing the frequency of FSCP 1/1 clock with the frequency of black channel clock at clock synchronization. If deviation is more than a permitted value, a preconfigured fault state action is triggered by setting function block inputs and outputs to bad status. The resource block has a black channel error parameter with time synchronization error flag.

Time distribution from the time master (LAS) to the other devices could be affected by communication queuing delays, just like other link publications. The local black channel includes a function that measures the roundtrip delay through the black channel to compensate for queuing delays. This is done periodically including start-up and LAS change. This is not a safety function. This is a function to avoid spurious trips thus ensuring better availability.

The black channel time synchronization monitor controls faults such as:

- LAS time fast, slow or jump;
- queuing fault (publisher/subscriber or time distribution);
- device restart;
- safety function restart;
- LAS switch over;
- LAS restart;
- schedule corruption (LAS or field device);
- initial start-up (configuration) (same as safety function restart);
- communication (lost time distribution, compel data, or publishing).

7.1.4 Sequence number

For publisher/subscriber VCRs the sequence number for each publication is based on macro cycle number which is computed by the safety communication layer from the data link time at the beginning of each macro cycle. The black channel time synchronization monitoring function in the safety communication layer ensures the data link time is good. The publisher/subscriber sequence number is in effect a timestamp. All devices on the H1 network have a common sense of macro cycle. There can be no sub-schedules, that is, function blocks can only be executed once per macro cycle. The result is that during normal operation the sequence number increments by one for each new link publication. The sequence number is included with the message and compared against an expected sequence number in the safety communication layer at the receiving end. If a maximum permitted difference is exceeded it will provide a bad status to the input of the function block so that the application process knows that the data is stale.

If the overall response time from sensor to actuator is compromised due to communication errors, function block execution, scheduling faults or any other reason the output will take the preconfigured fault state action. When there is a chain of linked function blocks making up a safety function it would be possible for several individual link stale counts to add up to a long response time before detection. Rather than a stale count per link as used for non-FSCP 1/1 communications, the stale counts are diagnosed end-to-end. This is effectively a propagation delay measurement. The maximum response time from sensor to actuator permitted by the application (expressed in macro cycle units) shall be configured in the end-to-end stale count limit of the link object. If the end-to-end stale count limit is exceeded the safety communication layer sets the input status to the function block to BAD. Because the safety communication layer derives the sequence number from the macro cycle number only when function block outputs have been updated, and each individual function block only updates its output if input conditions are right (the subsequent publication thus triggering the generation of the sequence number), stale counts are propagated downstream and added up. That is, when all links are working and all function blocks execute as they should, the sequence number (based on macro cycle number at sensor) propagated from end to end matches the macro cycle (expected sequence number) in the valve. When compared to the macro cycle in the output device, it indicates the total missed communications and executions in the chain of function blocks making up the safety function. This results in a much shorter worst case response time. The criteria to refresh with a new output or not is function block specific. A new sequence number is only generated by the safety communication layer as the message is published. Certain function blocks may require all used inputs to be current while other function blocks may have voting capability that only requires a certain number of the used inputs to be current.

The FSCP 1/1 layer requires one sequence number counter for each client/server VCR. The client/server sequence number is incremented by one for each new transaction. For a client-server VCR if the sequence number is out of synch then the connection is aborted. The sequence numbers are reset when a new connection is established.

7.1.5 Virtual header

The protocol header, such as address, in the black channel frame is not protected by the safety communication layer CRC and therefore cannot be relied upon in safety-related applications. There is therefore a need to use a different mechanism to uniquely identify the source-destination relationship within the FSCP 1/1 message, but protected by the safety communication layer CRC. The connection key is used for this purpose. Sending the connection key in every message, however, would create overhead. To reduce the overhead, the safety communication layer CRC is calculated on the safety data and a virtual header including the connection key and object index. The connection key is not transmitted on the bus but the safety communication layer CRC in the recipient will fail if the connection key is wrong. The safety link object contains the connection key making it possible to compute the CRC.

7.1.6 Connection key

The protocol contains a mechanism to uniquely identify FSCP 1/1 messages so one FSCP 1/1 message is not masquerading as another FSCP 1/1 message: FSCP 1/1 function block links will be identified by a unique 32-bit connection key. The connection key will be administered by the host and written in the safety link objects. The connection key is part of the virtual header embedded in the safety communication layer CRC, but is not communicated. Any mismatch in the connection key is not explicitly checked in the subscriber or server, but a mismatch will cause a safety communication layer CRC error. That is, a safety communication layer CRC error could indicate data corruption or a connection key mismatch.

7.1.7 Redundancy and cross-check

The safety communication layer protocol contains a mechanism that transmits two copies of the whole data including sequence number and CRC in a single frame. At the receiving end the two copies are cross-checked to detect whether corruption has occurred.

One possible implementation is that in a device containing two redundant microcontrollers, each controller builds its transmission message completely independently. The two independent data messages are added together by the black channel interface and transmitted together as a single frame. Conversely, when receiving the two independent data messages in the frame from the black channel are unpacked to its respective microcontroller, which then perform the cross-check.

7.2 Protocol extensions for use in safety-related systems

7.2.1 Overview

In order to use fieldbus devices in a safety-related system, it is necessary to extend the fieldbus protocol to ensure that the process can be taken to a safe state when failures occur. FMS and all other communication layers, including the SMK are treated as a black channel. Hence, all the protocol extensions are implemented in the User Layer or Function Block Application Process.

No new data types are specified, other than the safety link object. The data that is communicated using FMS will include the protocol extensions. The extensions are specific to the type of interaction.

NOTE The CRC 32 is described in 7.1.2.

7.2.2 Publisher-subscriber interactions

7.2.2.1 General

There is only one macro cycle for the whole H1 segment. All devices in an H1 segment, including the LAS shall be configured with the same macro cycle count. A function block in a device shall be scheduled to execute only once during the macro cycle.

At the beginning of execution of a function block, the current macro cycle number (MCN) shall be calculated as follows:

MCN = DL - Time DIV macro cycle duration

MCN shall be a 16-bit unsigned integer.

NOTE If a device has multiple function blocks, if feasible, the MCN may be calculated at the beginning of the macro cycle rather than at the beginning of execution of every function block.

7.2.2.2 Publisher

7.2.2.2.1 Connection establishment

The publishing of a safety function block parameter to be used in a safety function is indicated by the presence of a safety link object. If a safety link object exists for publishing, the publisher FBAP shall establish the publisher connection in a manner identical to non-safety publisher connections.

7.2.2.2.2 Publishing of data

At the end of execution, the safety function block shall determine which of its output parameters are to be published. The output parameters to be published are dependent on the type of the function block and the status of its input parameters. The parameters published are outside the scope of this part.

A function block publishes its selected output parameters (if so configured) using the extended protocol. The publishing of safety function block parameters to be used in a safety function is indicated by the presence of a safety link object. The published parameter value will be protected from possible corruption, duplication, and out of sequence reception caused by the black channel. To protect the data from corruption, a CRC 32 is used. A virtual PDU is formed as shown in Figure 16.

Connection key (4 octets)	Object index (4 octets)	Sequence number (4 octets)	Object value & status (2-120 octets)

Figure 16 – Safety PDU showing virtual content

Only the lower two octets of the Object Index are used. The higher two octets are set to zero. The CRC32 is calculated over the Virtual Safety PDU. The data on the call for the Information Report is modified to include a sequence number and CRC32 and is duplicated. The data format is shown in Figure 17.

Data 1			Data 2		
Original data	Sequence number	CRC32	Original data	Sequence number	CRC32

Figure 17 – Safety PDU showing duplication of data and addition of CRC

The “Original Data” is identical in format to the data that would have been contained in the data portion of the information report for non-safety data. The sequence number and the CRC32 are appended to this data. The function block shall set the sequence number to be the macro cycle number.

The function block shall set the status of the published output parameter to bad::black channel failure if the black channel time synchronization is not working properly i.e. BLK_CHN_ERR is non-zero.

Figure 18, Table 5, Table 6 and Table 7 define the state machine for the publisher.

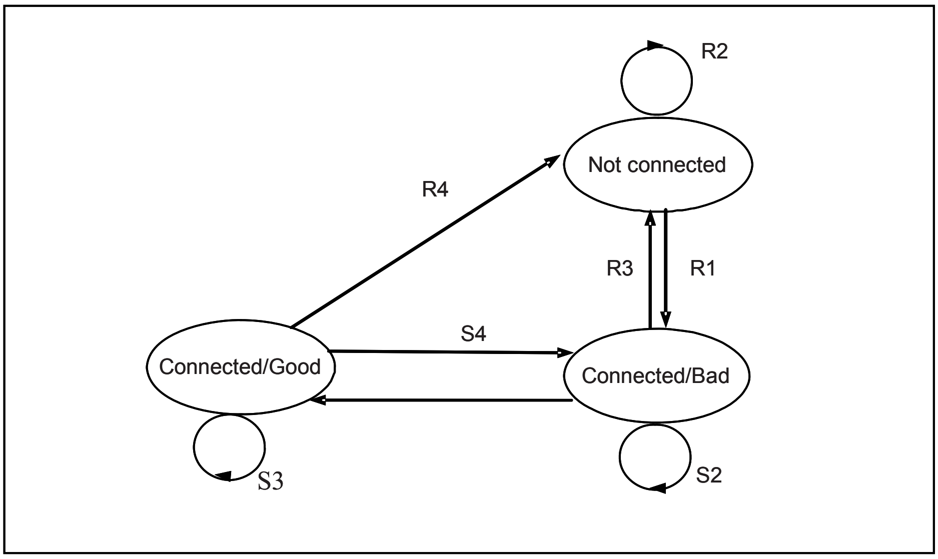


Figure 18 – State transition diagram for a FSCP 1/1 Publisher

Table 5 – Publisher states

State	Description
Not connected	No VCR for publishing established
Connected/Bad	VCR established but black channel errors not cleared
Connected/Good	VCR established, normal publications occurring

Table 6 – Publisher state table - Received transitions

#	Current State	Event & Condition Action	Next State
R1	Not connected	RcvMsg() = “FMS Initiate.cnf"	Connected/ Bad
R2	Not connected	RcvMsg() = "Any message (not FMS Initiate.cnf)"	Same
R3	Connected/ Bad	RcvMsg() = "Abort.ind" OR RcvMsg() = "Abort.req"	Not connected
R4	Connected/G Good	RcvMsg() = "Abort.ind" OR RcvMsg() = "Abort.req"	Not connected

Table 7 – Publisher state table - Internal transitions

#	Current State	Event & Condition Action	Next State

S1	Connected/ bad	BLK_CHN_ERR = 0
		SET Sequence Number = MCN
			Connected/ Good

S2	Connected/ Bad	BLK_CHN_ERR <> 0
		SET Black Channel Failure
		SET Sequence Number = MCN
			Same

S3	Connected/ Good	BLK_CHN_ERR = 0
		SET Sequence Number = MCN
			Same

S4	Connected/ Good	BLK_CHN_ERR <> 0
		SET Black Channel Failure
		SET Sequence Number = MCN
		NOTE The Function Block determines if its output parameters will be published or not. The logic is dependent on the sequence numbers received on its input parameters.
			Connected/ Bad

7.2.2.3 Subscriber

7.2.2.3.1 Connection establishment

The subscription of a safety function block parameter to be used in a safety function is indicated by the presence of a safety link object. If a safety link object exists for subscribing, the subscriber FBAP shall establish the subscriber connections in manner identical to non-safety subscriber connections.

7.2.2.3.2 Subscribing of data

The MCN, calculated at the beginning of block execution, is the sequence number that is expected from the publisher of each of the publisher-subscriber connections in the block. If the published data is not state or if there are no accumulated delays in the black channel then the received sequence numbers will match the MCN.

When the FBAP receives FMS data, as shown in Figure 19, for a VCR associated with a safety link object,

a) The two copies of the original data are compared (Data 1 and Data 2), if they are identical proceed to b), otherwise the message is discarded and increment the Stale Count by 1.

Data 1			Data 2		
Original data	Sequence number	CRC32	Original data	Sequence number	CRC32

Figure 19 – Safety PDU showing duplication of data and addition of CRC

b) A Virtual Safety PDU, identical to the VSPDU used in the Publication of the data, is formed as shown in Figure 20.

Expected connection key (4 octets)	Expected object index (4 octets)	Received sequence number (4 octets)	Received object value & status (2-120 octets)

Figure 20 – Safety PDU showing virtual content

The expected connection key and the expected object index are extracted from the safety link object. For H1, only the lower two octets of the object index are used. The higher two octets are set to zero. The sequence number and the object value and status are filled in from the received data. The sequence number, and the duplicate data indication provided by the black channel are ignored.

c) A CRC 32 is calculated over the VSPDU. The CRC 32 is then compared with the CRC 32 received in the data portion of the FMS PDU. If the calculated CRC 32 does not match the received CRC 32, the PDU will be discarded. If the CRC does not match, the stale count is incremented by 1.

d) If CRC32 is valid and the sequence number matches the MCN, the received data is used.

e) If CRC 32 is valid, and the sequence number does not match the MCN, the stale count is incremented by 1. Data is discarded.

f) If stale count exceeds the configured end-to-end stale count limit, the status of the Input parameter shall be set to bad::black channel failure. The data is discarded.

g) If the black channel time synchronization is not working i.e. BLK_CHN_SYNC_ERR bit in the BLK_CHN_ERR parameter in resource block is TRUE, the status of the input parameters shall be set to bad::black channel failure. The data is discarded.

Table 8, Figure 21, Table 9 and Table 10 define the state machine for the subscriber.

Table 8 – Subscriber states

State	Description
Not connected	No VCR for subscribing established
Connected/Stale	VCR established but black channel errors or stale count not cleared
Connected/Good	VCR established, normal publications occurring

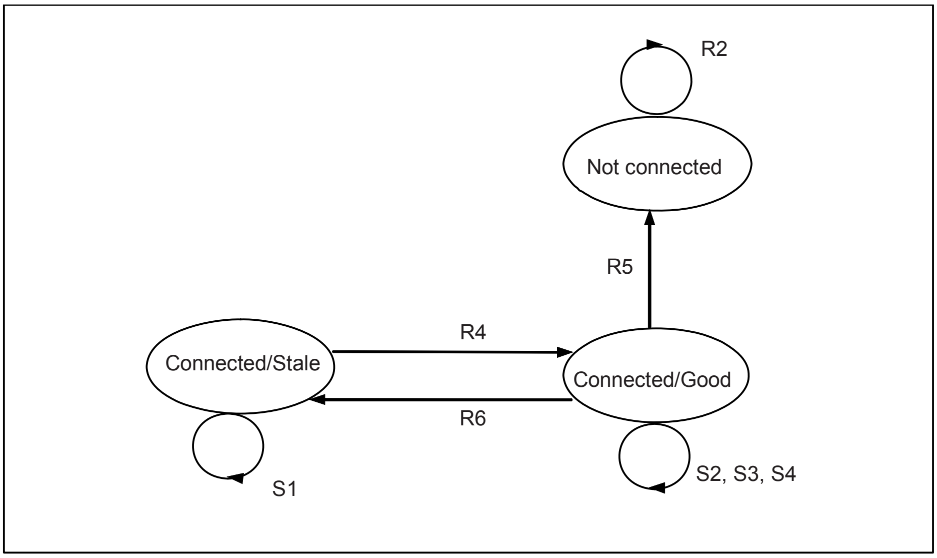


Figure 21 – State transition diagram for a FSCP 1/1 subscriber

Table 9 – Subscriber state table - Received transitions

#	Current State	Event and condition action	Next State
R1	Not connected	RcvMsg() = “FMS Initiate.cnf"	Connected/ stale
R2	Not connected	RcvMsg() = "Any message (not FMS Initiate.cnf)"	Same
R3	Connected/ Stale	RcvMsg() = "Abort.ind" OR RcvMsg() = "Abort.req"	Not connected

R4	Connected/ Stale	Sequence Number = MCN
		AND
		BLK_CHN_ERR = 0
		SET Use Data Stale Count = 0
			Connected/ Good

R5	Connected/ Good	RcvMsg() = "Abort.ind" OR RcvMsg() = "Abort.req"	Not connected
R6	Connected/ Good	Stale Count > End-to-end stale count OR BLK_CHN_ERR <> 0 SET Status = Bad::Black channel failure Discard data	Connected/ Stale

Table 10 – Subscriber state table - Internal transitions

#	Current state	Event and condition action	Next state
S1	Connected/ Stale	Sequence Number = MCN OR Data 1 <> Data 2 OR BLK_CHN_ERR <> 0 SET Status = Bad::Black channel failure Discard data	Connected/ Good
S2	Connected/ Good	(Sequence Number <> MCN OR Data 1 <> Data 2) AND Stale Count <= End-to-end stale count AND BLK_CHN_ERR = 0 Increment Stale Count Discard data	Same
S3	Connected/ Good	CRC 32 is invalid AND BLK_CHN_ERR = 0 Increment Stale Count Discard data	Same
S4	Connected/ Good	Sequence Number = MCN AND Data 1 = Data 2 AND BLK_CHN_ERR = 0 SET Stale Count = 0 Use data	Same

7.2.3 Client-server interactions

7.2.3.1 General

Client-Server VCRs to read data from safety function blocks shall be set up with maximum concurrency of 1. The device shall reject all FMS Initiate requests to VCRs set up with a concurrency greater than 1.

7.2.3.2 Read

The read request for reading data from safety function blocks (i.e. data to be used in a safety function) is identical to that of reading data from non safety function blocks.

FMS supplies the index of the object (and the optional sub index) that is being read. If the read is for a safety function block, the device shall check if a valid safety link object, with service operation set to SIS_ACCESS, exists for that block. If a valid link object does not exist, the device responds to the read just like a read of a non-safety function block parameter.

If a valid safety link object exists, and there is already a read or write request pending, the device shall reject the read or write request and send a negative response.

If a valid safety link object exists, and there is no other outstanding read/write request, the device responds to the data using the extended protocol. This data will be protected from possible corruption, duplication, and out of sequence reception caused by the black channel. To protect the data from corruption, a CRC 32 is used and to calculate the CRC 32, a virtual PDU is formed as shown in Figure 22. If the read is a read by sub index, the sub index is also used in calculating the CRC 32. For H1, only the lower two octets of the object index are used. The higher two octets are set to zero.

Connection key (4 octets)	Object index (4 octets)	Sequence number (4 octets)	Object value & status (2-120 octets)

Figure 22 – Safety PDU showing virtual content

If the read is by sub index, the VSPDU shall include the sub index. The sub index shall be included in the calculation of CRC 32. This virtual PDU is shown in Figure 23.

Connection key (4 octets)	Object index (4 octets)	Sub index (1 octets)	Sequence number (4 octets)	Object value & status (2-120 octets)

Figure 23 – Safety PDU showing virtual content with sub index

The CRC 32 is calculated over the Virtual Safety PDU. The data on the call for the FMS Read.res is modified to duplicate the data and to include a sequence number and CRC 32. The data format is shown in Figure 24.

Data 1			Data 2		
Original data	Sequence number	CRC32	Original data	Sequence number	CRC32

Figure 24 – Safety PDU showing duplication of data, addition of sequence number and CRC

The “Original data” is identical in format to the data that would have been contained in the data portion of the FMS Read.res for non safety function blocks. The Sequence Number and the CRC32 are appended to this data. The sequence number is incremented for every PDU handed over to the black channel for communication.

The sequence number count is maintained for each safety communication layer connection, i.e. connection key. The sequence number is reset to zero after connection establishment. The sequence number rolls over to 1.

NOTE The Invoke ID is not included in the CRC 32 calculation.

If the device is responding with a negative response, the response is identical to negative response for non-safety function blocks. That is, the sequence number is not incremented; virtual safety PDU need not be formed.

The state machine for processing reads is shown in Table 11, Figure 25 and Table 12.

Table 11 – Server states during read operations

State	Description
Not connected	No Connection established
Connected	Connection established

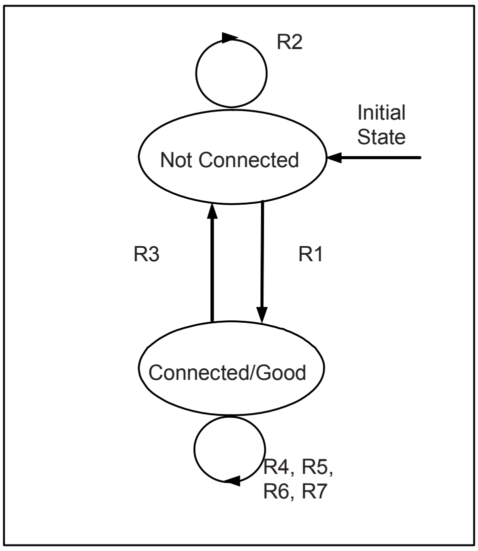


Figure 25 – State transition diagram for a FSCP 1/1 Server during read operations

Table 12 – Received transitions for a FSCP 1/1 Server during read operations

#	Current state	Event and condition action	Next state
R1	Not connected	RcvMsg() = “Connection Request valid response" Set Sequence number = o	Connected
R2	Not connected	RcvMsg() = "Any message (not connection request valid response)"	Same
R3	Connected	RcvMsg() = "Abort.ind" OR RcvMsg() = "Abort.req"	Not connected
R4	Connected	Valid Read request AND safety link object exists AND No other FMS requests outstanding Respond using safety communication layer protocol	Connected
R5	Connected	Valid Read request AND safety link object does not exist Respond using FMS protocol	Connected
R6	Connected	Valid Read request AND safety link object exists AND Other FMS requests outstanding Return negative response	Connected
R7	Connected	Invalid Read request Return negative response	Connected

7.2.3.3 Write

The request for writing data to safety function blocks will follow the extended protocol. Clients initiating the write request shall format the data according to the safety PDU format described below and shown in Figure 26.

FMS supplies the index of the object that is being written. If the write is for a safety function block, the device shall check if the write is formatted according to the extended protocol.

That is it checks to see if Data 1 is identical to Data 2. If identical it determines if the packet has a valid sequence number and a CRC32 added. If not identical the data is discarded and a negative response is returned. A sequence is valid if it is 1 more (using unsigned arithmetic) than the last sequence number received on that connection (LRSN) i.e. sequence numbers have to be tracked per connection key. If the sequence number is incorrect, the device shall discard the write and abort the connection. If the sequence number is correct, the device shall increment the LRSN.

Data 1			Data 2		
Original data	Sequence number	CRC32	Original data	Sequence number	CRC32

Figure 26 – Safety PDU showing duplication of data and addition of sequence number and CRC

The “Original data” is identical in format to the data that would have been contained in the data portion of the FMS Write.ind for non safety function blocks.

The device then determines if a valid safety link object, with Service Operation set to SIS_ACCESS, exists for that block. If a valid link object does not exist, the device discards the write request and returns a negative response.

If a valid Link object exists, the device constructs a virtual Safety PDU (VSPDU) as shown in Figure 27 . The expected Connection Key is taken from the safety link object. If the write is by sub index, the sub index shall also be included as shown in Figure 28. The lower two octets of the Object Index are used. The higher two octets are set to zero.

Expected connection key (4 octets)	Object index (4 octets)	Sequence number (4 octets)	Object value & status (2-120 octets)

Figure 27 – Example of FSCP 1/1 write

Expected connection Key (4 octets)	Object index (4 octets)	Sub index (1 octets)	Sequence number (4 octets)	Object value & status (2-120 octets)

Figure 28 – Example of FSCP 1/1 write with sub index

The CRC 32 is calculated over the Virtual Safety PDU, and compared with the CRC 32 in the received data. If it does not match, the device shall discard the data, and return a negative response.

If all the checks pass, the device honours the write request. A positive or negative response is returned by the specific block that is being written to.

A positive or negative write response has the same format as a write response from a non-safety function block.

The state machine for processing writes is shown in Table 13, Figure 29 and Table 14.

Table 13 – States of a FSCP 1/1 server during write operations

State	Description
Not connected	No connection established
Connected	Connection established

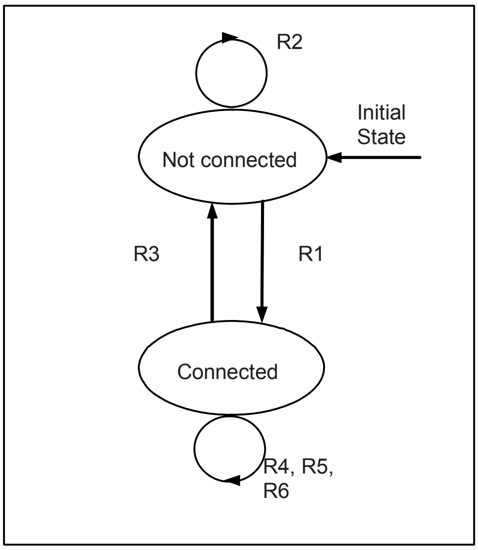


Figure 29 – State transition diagram for a FSCP 1/1 Server during write operations

Table 14 – Received transitions for a FSCP 1/1 Server during write operations

#	Current state	Event and condition action	Next state
R1	Not connected	RcvMsg() = “Connection Request valid response" Set LRSN = 0	Connected
R2	Not connected	RcvMsg() = "Any message (not connection request valid response)"	Same
R3	Connected	RcvMsg() = "Abort.ind" OR RcvMsg() = "Abort.req"	Not connected
R4	Connected	Valid Write request AND safety link object exists AND CRC 32 is OK AND Sequence Number OK AND No other FMS requests outstanding Increment LRSN Respond using safety related communication layer protocol	Connected
R5	Connected	Data 1 not identical to Data 2 OR safety link object does not exist OR CRC 32 not OK OR Invalid Write request Return negative response	Connected

#	Current state	Event and condition action	Next state
R6	Connected	Valid Write request AND safety link object exists AND Sequence Number OK AND Other FMS requests outstanding Return negative response	Connected

7.2.3.4 Writes to safety link object

Writes to the safety link object shall be according to the extended protocol as specified below.

The request for writing data to safety function blocks will follow the extended protocol. The client shall compute CRC 32 over the index of the safety link object and Link Object data, in that order.

FMS supplies the index of the object that is being written. If the write is for a safety link object, the device shall check if the write is formatted according to the extended PDU content shown in Figure 30. That is it compares Data 1 to Data 2 and if identical it checks to see if the packet has a valid CRC 32 added. If not identical the write is discarded and a negative response is returned. CRC 32 is computed over the index of the safety link object and safety link object data, in that order. If the calculated CRC does not match the received CRC, the device shall discard the write and return a negative response. The device shall not support write by sub index to the safety link object. If a device receives a write by sub index, it shall discard the request and return a negative response.

Data 1		Data 2	
Safety link object data	CRC32	Safety link object data	CRC32

Figure 30 – Safety PDU showing duplication of data and CRC

The device then determines if the safety link object is formatted correctly. If it is not the device shall discard the write and return a negative response.

The safety object shall be written only when the resource block is OOS. If the resource block is not in OOS, the device shall discard the write and return a negative response.

If all the checks pass, the device honours the write request and returns a positive response.

A positive or negative write response has the same format as a write response from a non-safety function block.

With respect to connection management, a successful write to safety link object shall trigger the same behaviour as a successful write to non-safety link objects. In addition, a successful write shall reset (set to 0) the sequence number associated with the connection key that is written.

The device shall store the CRC in its non-volatile storage as part of the safety link object. The device is expected to check the integrity of its entire configured link objects on a periodic basis and immediately after start-up in accordance with IEC 61508 requirements. If the integrity is bad, the device shall set its resource block to OOS.

7.2.4 Time synchronization

Time (DL-time) is synchronized by the black channel. The safety communication layer time sync monitor shall monitor whether the black channel time synchronization is working correctly or not. The safety communication layer shall have a dedicated hardware timer with a crystal of at least 10^{-4} accuracy and a resolution of at least 100 µs.

a) The safety communication layer time sync monitor shall execute after the black channel has processed a received Time Distribution PDU. It shall determine if the drift between black channel time and the safety communication layer time is greater than the allowable drift.

Allowable drift = $(TLCTD_n - TLCTD_{n-1}) \times SF\_SYNC\_DRIFT) / (60 \times 32\,000)$

NOTE 1 The (60 × 32 000) factor has units (1/32 ms)/min

NOTE 2 The ordering of computation is significant to maintain precision.

Actual drift = $(TTD_n - TTD_{n-1}) - (TLCTD_n - TLCTD_{n-1})$

Total Error = Total Error + Actual Drift

```
If |Total Error| > (Allowable Drift + SIF_SYNC_JITTER)
        Time Sync Error = 1
else
        Time Sync Error = 0
```

The next equations take into account the allowable drift in Total Error.

```
if (|Total Error| > Allowable Drift) then
        If (Total Error > 0) then
                // Total Error is positive
                // Subtract the allowable drift from the total error
                Total Error = Total Error – Allowable Drift
        else
                // Add the allowable drift to the total error
                Total Error = Total Error + Allowable Drift
else
        // The magnitude of Total Error is less than Allowable Drift
        Total Error = 0
```

Where:

$TLCTD_n$ is the time of safety communication layer clock after processing of the current TD;

$TLCTD_{n-1}$ is the time of safety communication layer clock after processing of the previous TD;

SIF_SYNC_DRIFT is a parameter that defines the acceptable rate of drift;

NOTE 3 The units for SIF_SYNC_DRIFT are (1/32 ms)/min.

NOTE 4 The valid range for SIF_SYNC_DRIFT is 100 – 1000.

NOTE 5 The default value for SIF_SYNC_DRIFT is 384.

SIF_SYNC_JITTER is a parameter that defines the acceptable jitter;

NOTE 6 The units for SIF_SYNC_JITTER is 1/32 ms.

NOTE 7 The default value for SIF_SYNC_JITTER is 160.

NOTE 8 The valid range for SIF_SYNC_JITTER is 0-320.

TTD_n is the DL-Time after processing of the current TD;

TTD_{n-1} is the DL-Time after processing of the previous TD;

Total Error is the total accumulated error in 1/32 ms contained in a signed 32 bit value;

Time Sync Error is a flag indicating a time synchronization error;

b) If Time Sync Error is 1, the monitor shall set the BLK_CHN_SYNC_ERR bit of the BLK_CHN_ERROR parameter in the Resource Block to TRUE; otherwise the flag shall be set to FALSE.

c) If the black channel does not receive a valid TD in 6 consecutive Time Distribution Periods, the monitor shall set the BLK_CHN_SYNC_ERR bit of the BLK_CHN_ERROR parameter in the Resource Block to TRUE.

d) If the BLK_CHN_SYNC_ERR is TRUE, the Time Sync Monitor shall require the black channel to attempt to synchronize time — periodically (once every TD period) command the black channel to send out CT sequences.

e) When the resource block's CLR_FAULT_STATE is written, a DL_RESET primitive shall be sent to the data link layer if the BLK_CHN_SYNC_ERR is TRUE.

7.2.5 Device start-up

The resource block in the safety communication layer shall be in OOS mode until the following have been completed:

a) The device is on the live list (the device is either LAS or the device has received a valid PN/PR/Activation PDU sequence;

b) The black channel DL -Time is valid — the device is LAS, or the device has updated the time based on valid TD and RR PDUs.

7.3 Communications entity

7.3.1 General

The communications entity and the SMK are the parts of the black channel that exist in a device and, therefore, do not have to execute in a SIL environment.

No changes are made to the communications entity.

7.3.2 Network management

Network management is part of the black channel. No change is needed.

7.3.3 FMS

FMS is part of the black channel. No change is needed.

7.3.4 H1 stack

The H1 stack is part of the black channel. No change is needed.

8 Safety communication layer management

8.1 Overview

The SMK is not trusted and is defined to be part of the black channel. Therefore, SMK need not be executed in a SIL environment. Internal manufacturer specific checks that meet the requirements of IEC 61508 are required for any local interface interaction between the SMK and the application process.

It is only possible to set an address when the write enable mode is set in the device resource block. When the address is changed the link objects are deleted. The address and tag of a device can only be written when the resource is in out-of-service mode.

8.2 SMK communications

The SMK is part of the black channel and its communications with the application layer are not trusted. Communications between SMK and the application process are on a local interface and verifications are internal using manufacturer specific means.

8.3 FMS services

The SMIB is part of the black channel, but exchanges information with the application process via SMK through a local interface. The manufacturer specific diagnostics shall verify this local interface. These internal faults can be controlled by manufacturer specific means.

8.4 SMK services

8.4.1 General

SMK services are part of the black channel and therefore not trusted. Verifications are internal between SMK and the application process on a local interface. These internal faults can be controlled by manufacturer specific means.

The resource block contains a macro cycle parameter since the data in the black channel cannot be relied on.

8.4.2 Address assignment

Address is part of the black channel. Address duplication masquerading faults are controlled using the connection key. It is expected that devices will automatically clear their configuration when the black channel address is changed.

8.4.3 Time synchronization

Time synchronization is a black channel function. A black channel time synchronization monitor function in the safety communication layer diagnoses the integrity of the H1 time synchronization mechanism. FSCP 1/1 protocol extensions, stale data timer, and end-to-end stale count limit will indirectly control the faults caused by any synchronization problems.

8.5 Safety communication layer configuration and start-up

8.5.1 H1 configuration and start-up

MIB is part of the black channel. There are no changes to its configuration. FBAP is different, (see 8.5.2). The safety communication layer is configured from data in link objects and the resource block transferred by internal vendor specific means.

8.5.2 FSCP 1/1 FBAP

Function block objects and parameters may be configured according to the Function Block AP specification.

8.5.3 Testing

After a device configuration has been changed it is necessary to test and verify the correct function.

9 System requirements

9.1 Indicators and switches

There are no indicators or switches that are required for a device.

9.2 Installation guidelines

The installation guidelines of IEC 61918 shall apply.

NOTE Specific amendments to the installation guidelines of IEC 61918 may also be defined in a future IEC 61784-5-1 [13] for CPF 1.

9.3 Safety function response time

9.3.1 Overview

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

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

Figure 31 shows an example of typical components making up a safety function response time.

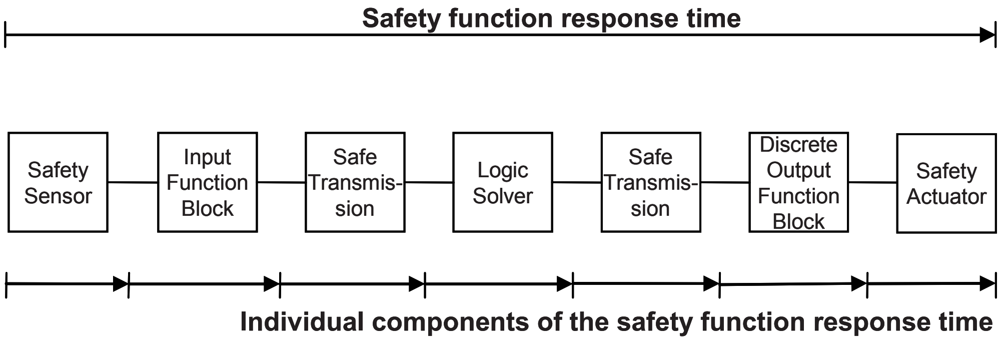

Safety function response time
Safety Sensor
Input Function Block
Safe Transmis-sion
Logic Solver
Safe Transmis-sion
Discrete Output Function Block
Safety Actuator
Individual components of the safety function response time

Figure 31 – Example of safety function response time components

The safety function response time is the sum of all the times show in Figure 31.

9.3.2 Safety Sensor

The response time of the Safety Sensor will be specified by the vendor of the sensor.

9.3.3 Input Function Block

The Input Function Block response time will be defined in the Safety Manual supplied with the device containing the Input Function Block.

9.3.4 Safe Transmission

The Safe transmission time = 2 x macro cycle + ((stale count) x macro cycle)

9.3.5 Logic Solver

The Logic Solver response time will be defined in the Safety Manual for the Logic Solver.

9.3.6 Discrete Output Function Block

The Discrete Output Function Block response time will be defined in the Safety Manual supplied with the device containing the Discrete Output Function Block.

9.3.7 Safety Actuator

The response time of the Safety Actuator will be supplied with the Safety Manual for the Safety Actuator.

9.4 Duration of demands

The demand has to exist for at least 2 macro cycles to guarantee that the functional safety communication system detects the demand.

9.5 Constraints for calculation of system characteristics

9.5.1 System characteristics

Figure 32 shows the FSCP 1/1 network topology defined for FSCP 1/1. In this topology, all input and output devices are connected to a logic solver. The input device publishes its data to the logic solver subscriber. The output device will subscribe to data published by the logic solver.

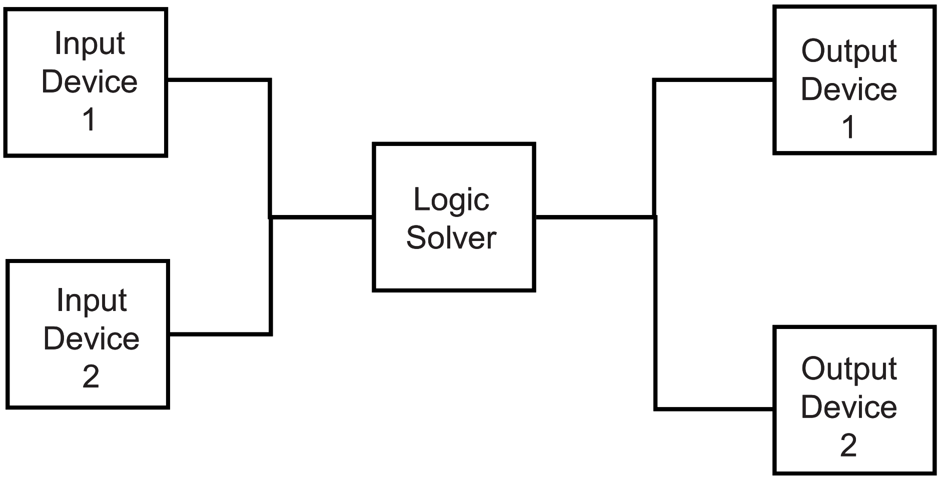


Figure 32 – Example FSCP 1/1 network topology

9.5.2 Message rate

FSCP 1/1 has a physical maximum rate for publishing of data of 100 messages per second. The maximum message rate used in calculations of the safety integrity level for FSCP 1/1 was 10 000 messages per second. Since the message rate used far exceeds the possible message rate on a H1 segment, there are no constraints on the message rate on a H1 segment.

9.5.3 SIL level

The FSCP 1/1 protocol technology is designed for use in a SIL 3 safety function and to use up no more than 1 % of the PFD budget (1 % of 10^{-7} in continuous high-demand mode). It is possible to use FSCP 1/1 in products designed for safety functions up to SIL 3, suitable for logic solvers.

9.5.4 Mixing FSCP 1/1 devices and CP 1/1 devices

The FSCP 1/1 protocol was designed to allow the mixing of CP 1/1 and FSCP 1/1 on the same H1 segment. The CP 1/1 devices cannot effect the safety of the FCSP 1/1 protocol, but the CP 1/1 devices may affect the availability of the H1 segment. It is not recommended mixing CP 1/1 and FSCP 1/1 devices on the same H1 segment.

9.5.5 Devices on a segment

There are no limits beyond the limits already specified in CP 1/1 on the number of devices on a H1 segment imposed by FSCP 1/1.

9.5.6 Residual error rate calculations

The results of calculating the residual error rate according to IEC 61784-3:2010 equation (1) and the values used for the calculation are shown in Table 15.

Table 15 – Values used for calculation of residual error rate

Equation items	FSCP 1/1 value
Λ_{SL} (Pe)	$1{,}04 \times 10^{-14}$
Pe	10^{-2}
R_{SL} (Pe)	$5{,}42 \times 10^{-20}$
v	6 000
m	32
n	32 to 1 024

R_{SL} (Pe) was calculated using equation (D.1) of IEC 61784-3:2010. The results are shown in Table 16.

Table 16 – Values of R_{SL} (Pe) for different values of n

n	R_{SL} (Pe)
32	$5{,}42 \times 10^{-20}$
64	$1{,}26 \times 10^{-29}$
96	$2{,}94 \times 10^{-39}$
128	$6{,}84 \times 10^{-49}$
160	$1{,}59 \times 10^{-58}$
192	$3{,}70 \times 10\text{-}^{68}$
224	$8{,}63 \times 10^{-78}$
256	$2{,}01 \times 10^{-87}$
288	$4{,}68 \times 10\text{-}^{97}$
320	$1{,}09 \times 10^{-106}$

n	R_{SL} (Pe)
352	2,54 x 10^{-116}
384	6,99 x 10^{-127}
416	3,03 x 10^{-138}
448	2,59 x 10^{-150}
480	5,51 x 10^{-163}
512	3,56 x 10^{-176}

9.6 Maintenance

There are no specific maintenance requirements for FSCP 1/1.

9.7 Safety manual

The safety device manufacturer shall supply a safety manual that is appropriate to the device.

The safety manual shall include the methods necessary for calculating the safety response time for the safety-related system that includes the safety device.

10 Assessment

FSCP 1/1 alone does not make a safety-related system or safety device. In addition to FSCP 1/1 protocol interoperability registration, the device, systems, and software, etc. will also have applicable SIL assessment. The user shall ascertain the suitability of use of every Safety device in the safety function in accordance with IEC 61508. In addition to Fieldbus considerations, the user will also take the IEC 61508 safety aspects into consideration. It shall be the manufacturer's responsibility to develop the device to the appropriate development process according to the safety standards (see IEC 61508, IEC 61511 series) and assessment by an appropriate agency shall be achieved.

Annex A
(informative)

Additional information for functional safety communication profiles of CPF 1

A.1 Hash function calculation

```
//
// Usage:
//   crc32eth [infile]
//   calculates Ethernet-CRC32 over the content of file [infile]
//
// Compile:
//   (this source should compile on any C++ compiler)
//   g++ -Wall -o crc32eth crc32eth.cc                  #GNU-C++ under Linux
//   g++ -Wall -mno-cygwin -o crc32eth.exe crc32eth.cc   #with cygwin GNU-C++
//
// ---------------------------------------------------------------------------------------------
// CRC calculation is mathematically the evaluation of the remainder of a polynomial division

// with the generator polynomial as divisor.
// For Ethernet-CRC32 the generator polynomial is 0xedb88320, the bits correspond (f.l.t.r.)

// with the coefficients fuer x^0, x^1 .. x^31, the coefficient for x^32 ist implicitly 1.
// This "unnatural" bit order (least significant bit left) is also applied to any single
// octet of the input data block and to the result of the polynomial division.
// ---------------------------------------------------------------------------------------------

#include <iostream>
#include <iomanip>
#include <fstream>

// ---------------------------------------------------------------------------------------------

const unsigned long maCRC32Ether[256] = {
  // Table for generator polynom 0xedb88320
  0x00000000, 0x77073096, 0xee0e612c, 0x990951ba,
  0x076dc419, 0x706af48f, 0xe963a535, 0x9e6495a3,
  0x0edb8832, 0x79dcb8a4, 0xe0d5e91e, 0x97d2d988,
  0x09b64c2b, 0x7eb17cbd, 0xe7b82d07, 0x90bf1d91,
  0x1db71064, 0x6ab020f2, 0xf3b97148, 0x84be41de,
  0x1adad47d, 0x6ddde4eb, 0xf4d4b551, 0x83d385c7,
  0x136c9856, 0x646ba8c0, 0xfd62f97a, 0x8a65c9ec,
  0x14015c4f, 0x63066cd9, 0xfa0f3d63, 0x8d080df5,
  0x3b6e20c8, 0x4c69105e, 0xd56041e4, 0xa2677172,
  0x3c03e4d1, 0x4b04d447, 0xd20d85fd, 0xa50ab56b,
  0x35b5a8fa, 0x42b2986c, 0xdbbbc9d6, 0xacbcf940,
  0x32d86ce3, 0x45df5c75, 0xdcd60dcf, 0xabd13d59,
  0x26d930ac, 0x51de003a, 0xc8d75180, 0xbfd06116,
  0x21b4f4b5, 0x56b3c423, 0xcfba9599, 0xb8bda50f,
  0x2802b89e, 0x5f058808, 0xc60cd9b2, 0xb10be924,
  0x2f6f7c87, 0x58684c11, 0xc1611dab, 0xb6662d3d,
  0x76dc4190, 0x01db7106, 0x98d220bc, 0xefd5102a,
  0x71b18589, 0x06b6b51f, 0x9fbfe4a5, 0xe8b8d433,
  0x7807c9a2, 0x0f00f934, 0x9609a88e, 0xe10e9818,
  0x7f6a0dbb, 0x086d3d2d, 0x91646c97, 0xe6635c01,
  0x6b6b51f4, 0x1c6c6162, 0x856530d8, 0xf262004e,
  0x6c0695ed, 0x1b01a57b, 0x8208f4c1, 0xf50fc457,
  0x65b0d9c6, 0x12b7e950, 0x8bbeb8ea, 0xfcb9887c,
  0x62dd1ddf, 0x15da2d49, 0x8cd37cf3, 0xfbd44c65,
  0x4db26158, 0x3ab551ce, 0xa3bc0074, 0xd4bb30e2,
  0x4adfa541, 0x3dd895d7, 0xa4d1c46d, 0xd3d6f4fb,
  0x4369e96a, 0x346ed9fc, 0xad678846, 0xda60b8d0,
  0x44042d73, 0x33031de5, 0xaa0a4c5f, 0xdd0d7cc9,
  0x5005713c, 0x270241aa, 0xbe0b1010, 0xc90c2086,
  0x5768b525, 0x206f85b3, 0xb966d409, 0xce61e49f,
  0x5edef90e, 0x29d9c998, 0xb0d09822, 0xc7d7a8b4,
  0x59b33d17, 0x2eb40d81, 0xb7bd5c3b, 0xc0ba6cad,
  0xedb88320, 0x9abfb3b6, 0x03b6e20c, 0x74b1d29a,
  0xead54739, 0x9dd277af, 0x04db2615, 0x73dc1683,
  0xe3630b12, 0x94643b84, 0x0d6d6a3e, 0x7a6a5aa8,
  0xe40ecf0b, 0x9309ff9d, 0x0a00ae27, 0x7d079eb1,
  0xf00f9344, 0x8708a3d2, 0x1e01f268, 0x6906c2fe,
  0xf762575d, 0x806567cb, 0x196c3671, 0x6e6b06e7,
  0xfed41b76, 0x89d32be0, 0x10da7a5a, 0x67dd4acc,
  0xf9b9df6f, 0x8ebeeff9, 0x17b7be43, 0x60b08ed5,
  0xd6d6a3e8, 0xa1d1937e, 0x38d8c2c4, 0x4fdff252,
  0xd1bb67f1, 0xa6bc5767, 0x3fb506dd, 0x48b2364b,
  0xd80d2bda, 0xaf0a1b4c, 0x36034af6, 0x41047a60,
  0xdf60efc3, 0xa867df55, 0x316e8eef, 0x4669be79,
  0xcb61b38c, 0xbc66831a, 0x256fd2a0, 0x5268e236,
  0xcc0c7795, 0xbb0b4703, 0x220216b9, 0x5505262f,
  0xc5ba3bbe, 0xb2bd0b28, 0x2bb45a92, 0x5cb36a04,
  0xc2d7ffa7, 0xb5d0cf31, 0x2cd99e8b, 0x5bdeae1d,
  0x9b64c2b0, 0xec63f226, 0x756aa39c, 0x026d930a,
  0x9c0906a9, 0xeb0e363f, 0x72076785, 0x05005713,
  0x95bf4a82, 0xe2b87a14, 0x7bb12bae, 0x0cb61b38,
  0x92d28e9b, 0xe5d5be0d, 0x7cdcefb7, 0x0bdbdf21,
  0x86d3d2d4, 0xf1d4e242, 0x68ddb3f8, 0x1fda836e,
  0x81be16cd, 0xf6b9265b, 0x6fb077e1, 0x18b74777,
  0x88085ae6, 0xff0f6a70, 0x66063bca, 0x11010b5c,
  0x8f659eff, 0xf862ae69, 0x616bffd3, 0x166ccf45,
  0xa00ae278, 0xd70dd2ee, 0x4e048354, 0x3903b3c2,
  0xa7672661, 0xd06016f7, 0x4969474d, 0x3e6e77db,
  0xaed16a4a, 0xd9d65adc, 0x40df0b66, 0x37d83bf0,
  0xa9bcae53, 0xdebb9ec5, 0x47b2cf7f, 0x30b5ffe9,
  0xbdbdf21c, 0xcabac28a, 0x53b39330, 0x24b4a3a6,
  0xbad03605, 0xcdd70693, 0x54de5729, 0x23d967bf,
  0xb3667a2e, 0xc4614ab8, 0x5d681b02, 0x2a6f2b94,
  0xb40bbe37, 0xc30c8ea1, 0x5a05df1b, 0x2d02ef8d
};

// GetCRC32Ether() calculates the CRC over a data block located at address [pStart] with a
size
// of [len] octets. GetCRC32Ether() works incrementally with the result of the last portion given

// as [preset] value for the subsequent portion. For the first portion a preset value of 0xffffffff

// (=CRC32ETHER_PRESET) has to be used.
// GetCRC32Ether() implements the highly efficient table technique for CRC calculation.

enum {CRC32ETHER_PRESET= 0xffffffff};

unsigned long GetCRC32Ether(const void*   pStart,
                            size_t        len,
                            unsigned long preset) {
  size_t bytecount;
  unsigned char * buf= (unsigned char *) pStart;
  unsigned long crcword= preset;
  for (bytecount= len; (bytecount > 0); bytecount--, buf++) {
    crcword= maCRC32Ether[(crcword ^ *buf) & 0x0ff] ^ ( crcword >> 8L );
  }
  return crcword;
};

// -------------------------------------------------------------------------------------------
enum {BUFSIZE= 1024}; //Groesse des Read-Buffers

int main(int argc, char * argv[]) {

  if (argc != 2) {
    std::cerr << "Usage:" << std::endl;
    std::cerr << "  "  << argv[0] << " infile" << std::endl;
    return 2;
  }

  std::ifstream infile;
  infile.open(argv[1], std::ios_base::in | std::ios_base::binary);
  if (!infile) {
    std::cerr << "ERR: unable to open file " << argv[1] << std::endl;
    exit(1);
  }

  char buf[BUFSIZE];                    //Read-Buffer
  size_t totalCount= 0;                 //Laenge in Bytes
  unsigned long sig= CRC32ETHER_PRESET; //Preset of the signatur

  while (infile) {
    infile.read(&buf[0], BUFSIZE);
    size_t portionCount= infile.gcount();
    totalCount+= portionCount;
    sig= GetCRC32Ether(&buf[0], portionCount, sig);
  }
  if (!infile.eof()) {
    std::cerr << "ERR: error while reading file " << argv[1] << std::endl;
    exit(1);
  }
  infile.close();
  std::cout << argv[0] << ": bytes read from file " << argv[1] << ": " << totalCount << std::endl;

  std::cout << argv[0] << ": CRC: 0x" << std::hex << std::setw(8) << std::setfill('0') << sig <<
std::endl;

return 0;
}
```

A.2 Fault conditions arising from locations beyond the output function block

When diagnostics on the device output detect a field fault arising from locations beyond the output function block or beyond the device itself, for example a connected actuator, the action taken is not defined in the output function block, but rather in the transducer block or hardware. On a device failure the output goes to the de-energized state just as if power to the device itself was lost. Some output devices may use auxiliary power to drive the actuator, and if this is lost the physical output goes to its de-energized state. Since these faults occur after the output function block, the fault state configuration is not applicable. Table A.1 shows this behaviour.

A device failure will always result in a latched output that will need to be reset by the user.

Table A.1 – Fault conditions arising from locations beyond the output function block

Condition	Example	Remark
Field fault	Partial stroke testing failure (valve or actuator fault), solenoid wiring open or short circuit	Diagnostics and action determined by transducer block and hardware. Feedback through output function block
Auxiliary power failure	Loss of supply air, line power, or hydraulic pressure	Action determined by hardware. Feedback through output function block
Device power failure	Bus power or separate power lost	Action determined by hardware
Device failure	Memory fault or CPU watchdog	Action determined by hardware
Stale data timer	Output block execution or scheduling fault	Diagnostics and action determined by transducer block and hardware. Feedback through output function block

Annex B
(informative)
Information for assessment of the functional safety communication profiles of CPF 1

Information about test laboratories which test and validate the conformance of FSCP 1/1 products with IEC 61784-3-1 can be obtained from the National Committees of the IEC or from the following organization:

Fieldbus Foundation
9005 Mountain Ridge Drive
Bowie Bldg - Suite 200
Austin, TX 78759-5316
USA

Phone: +1 512 794 8890
Fax: +1 512 794 8893
E-mail: info@fieldbus.org
URL:http://www.fieldbus.org

Bibliography

[1] IEC 60050 (all parts), *International Electrotechnical Vocabulary*

NOTE See also the IEC Multilingual Dictionary – Electricity, Electronics and Telecommunications (available on CD-ROM and at <http://www.electropedia.org>)

[2] IEC 60204-1, *Safety of machinery – Electrical equipment of machines – Part 1: General requirements*

[3] IEC/TS 61000-1-2*, Electromagnetic compatibility (EMC) – Part 1-2: General – Methodology for the achievement of the functional safety of electrical and electronic equipment with regard to electromagnetic phenomena*

[4] IEC 61131-6[13], *Programmable controllers – Part 6: Functional safety*

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

[6] 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*

[7] 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*

[8] IEC 61496 (all parts), *Safety of machinery – Electro-sensitive protective equipment*

[9] IEC 61508-5:2010[14], *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 5: Examples of methods for the determination of safety integrity levels*

[10] IEC 61508-6:2010[14], *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3*

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

[12] IEC 61784-4[15], *Industrial communication networks – Profiles – Part 4: Secure communications for fieldbuses*

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

[14] IEC 61800-5-2, *Adjustable speed electrical power drive systems – Part 5-2: Safety Requirements – Functional*

[15] IEC/TR 62059-11, *Electricity metering equipment – Dependability – Part 11: General concepts*

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

[17] IEC/TR 62210, *Power system control and associated communications – Data and communication security*

[18] IEC 62280-2, *Railway applications – Communication, signalling and processing systems – Part 2: Safety-related communication in open transmission systems*

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

[20] ISO/IEC Guide 51:1999, *Safety aspects — Guidelines for their inclusion in standards*

[21] ISO/IEC 2382-14, *Information technology – Vocabulary – Part 14: Reliability, maintainability and availability*

[13] Under consideration.

[14] To be published.

[15] Proposed new work item under consideration.

[22] ISO/IEC 2382-16, *Information technology – Vocabulary – Part 16: Information theory*

[23] ISO/IEC 7498 (all parts), *Information technology – Open Systems Interconnection – Basic Reference Model*

[24] ISO 10218-1, *Robots for industrial environments – Safety requirements – Part 1: Robot*

[25] ISO 12100-1, *Safety of machinery – Basic concepts, general principles for design – Part 1: Basic terminology, methodology*

[26] ISO 13849-1, *Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design*

[27] ISO 13849-2, *Safety of machinery – Safety-related parts of control systems – Part 2: Validation*

[28] ISO 14121, *Safety of machinery – Principles of risk assessment*

[29] ITU-T(CCITT) V.42, *Error-correcting procedures for DCEs using asynchronous-to-synchronous conversion,* available at < http://www.itu.int/rec/T-REC-V.42/e>

[30] IEEE 802.3, *IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications*

[31] ANSI/ISA-84.00.01-2004 (all parts), *Functional Safety: Safety Instrumented Systems for the Process Industry Sector*

[32] VDI/VDE 2180 (all parts), *Safeguarding of industrial process plants by means of process control engineering*

[33] GS-ET-26[16], *Grundsatz für die Prüfung und Zertifizierung von Bussystemen für die Übertragung sicherheitsrelevanter Nachrichten*, May 2002. HVBG, Gustav-Heinemann-Ufer 130, D-50968 Köln ("*Principles for Test and Certification of Bus Systems for Safety relevant Communication*")

[34] ANDREW S. TANENBAUM, *Computer Networks*, 4th Edition, Prentice Hall, N.J., ISBN-10:0130661023, ISBN-13: 978-0130661029

[35] W. WESLEY PETERSON, *Error-Correcting Codes*, 2nd Edition 1981, MIT-Press, ISBN 0-262-16-039-0

[36] BRUCE P. DOUGLASS, *Doing Hard Time*, 1999, Addison-Wesley, ISBN 0-201-49837-5

[37] *New concepts for safety-related bus systems*, 3rd International Symposium "Programmable Electronic Systems in Safety Related Applications", May 1998, from Dr. Michael Schäfer, BG-Institute for Occupational Safety and Health.

[38] DIETER CONRADS, *Datenkommunikation*, 3rd Edition 1996, Vieweg, ISBN 3-528-245891

[39] German IEC subgroup DKE AK 767.0.4: *EMC and Functional Safety*, Spring 2002

[40] NFPA79 (2002), *Electrical Standard for Industrial Machinery*

[41] GUY E. CASTAGNOLI, *On the Minimum Distance of Long Cyclic Codes and Cyclic Redundancy-Check Codes*, 1989, Dissertation No. 8979 of ETH Zurich, Switzerland

[42] GUY E. CASTAGNOLI, STEFAN BRÄUER, and MARTIN HERRMANN, *Optimization of Cyclic Redundancy-Check Codes with 24 and 32 Parity Bits*, June 1993, IEEE Transactions On Communications, Volume 41, No. 6

[43] SCHILLER F and MATTES T: *An Efficient Method to Evaluate CRC-Polynomials for Safety-Critical Industrial Communication*, Journal of Applied Computer Science, Vol. 14, No 1, pp. 57-80, Technical University Press, Łódź,Poland, 2006

[44] SCHILLER F and MATTES T: *Analysis of CRC-polynomials for Safety-critical Communication by Deterministic and Stochastic Automata*, 6th IFAC Symposium on Fault Detection, Supervision and Safety for Technical Processes, SAFEPROCESS 2006, pp. 1003-1008, Beijing, China, 2006

[45] Foundation™ Fieldbus AG-180, *User Application Guide for FF-SIS*

[16] This document has been one of the starting points for this part. It is currently undergoing a major revision.

[46] Foundation™ Fieldbus FF-807, *FS-SIS Application Model – Phase 1*

[47] Foundation™ Fieldbus FF-884, *FF-SIS Protocol Specification*

[48] Foundation™ Fieldbus FF-895, *FF-SIS Function Block Application Process – Phase 1*

____

This page deliberately left blank

British Standards Institution (BSI)

BSI is the independent national body responsible for preparing British Standards and other standards-related publications, information and services. It presents the UK view on standards in Europe and at the international level.

It is incorporated by Royal Charter.

Revisions

British Standards are updated by amendment or revision. Users of British Standards should make sure that they possess the latest amendments or editions.

It is the constant aim of BSI to improve the quality of our products and services. We would be grateful if anyone finding an inaccuracy or ambiguity while using this British Standard would inform the Secretary of the technical committee responsible, the identity of which can be found on the inside front cover.

Tel: +44 (0)20 8996 9001 Fax: +44 (0)20 8996 7001

BSI offers Members an individual updating service called PLUS which ensures that subscribers automatically receive the latest editions of standards.

Tel: +44 (0)20 8996 7669 Fax: +44 (0)20 8996 7001
Email: plus@bsigroup.com

Buying standards

You may buy PDF and hard copy versions of standards directly using a credit card from the BSI Shop on the website **www.bsigroup.com/shop.** In addition all orders for BSI, international and foreign standards publications can be addressed to BSI Customer Services.

Tel: +44 (0)20 8996 9001 Fax: +44 (0)20 8996 7001
Email: orders@bsigroup.com

In response to orders for international standards, it is BSI policy to supply the BSI implementation of those that have been published as British Standards, unless otherwise requested.

Information on standards

BSI provides a wide range of information on national, European and international standards through its Knowledge Centre.

Tel: +44 (0)20 8996 7004 Fax: +44 (0)20 8996 7005
Email: knowledgecentre@bsigroup.com

Various BSI electronic information services are also available which give details on all its products and services.

Tel: +44 (0)20 8996 7111 Fax: +44 (0)20 8996 7048
Email: info@bsigroup.com

BSI Subscribing Members are kept up to date with standards developments and receive substantial discounts on the purchase price of standards. For details of these and other benefits contact Membership Administration.

Tel: +44 (0)20 8996 7002 Fax: +44 (0)20 8996 7001
Email: membership@bsigroup.com

Information regarding online access to British Standards via British Standards Online can be found at **www.bsigroup.com/BSOL**

Further information about BSI is available on the BSI website at **www.bsigroup.com/standards**

Copyright

Tel: +44 (0)20 8996 7070
Email: copyright@bsigroup.com

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

Tel +44 (0)20 8996 9001
Fax +44 (0)20 8996 7001
www.bsigroup.com/standards

raising standards worldwide™