

Industrial communication networks — Profiles —

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

ICS 25.040.40; 35.100.05

National foreword

This British Standard is the UK implementation of EN 61784-3-1:2008. It is identical to IEC 61784-3-1:2007.

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.

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 29 August 2008

© BSI 2008

ISBN 978 0 580 61648 8

Amendments/corrigenda issued since publication

Date	Comments

**Industrial communication networks -
Profiles -
Part 3-1: Functional safety fieldbuses -
Additional specifications for CPF 1
(IEC 61784-3-1:2007)**

Réseaux de communication industriels -
Profils -
Partie 3-1: Bus de terrain
de sécurité fonctionnelle -
Spécification supplémentaire pour CPF 1
(CEI 61784-3-1:2007)

Industrielle Kommunikationsnetze -
Profile -
Teil 3-1: Funktional sichere Übertragung
bei Feldbussen -
Zusätzliche Festlegungen
für die Kommunikationsprofilfamilie 1
(IEC 61784-3-1:2007)

This European Standard was approved by CENELEC on 2008-05-01. 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, 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

Central Secretariat: rue de Stassart 35, B - 1050 Brussels

Foreword

The text of document 65C/470/FDIS, future edition 1 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 2008-05-01.

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) 2009-02-01
- latest date by which the national standards conflicting
with the EN have to be withdrawn (dow) 2011-05-01

The International Electrotechnical Commission (IEC) and CENELEC draw 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

The IEC and CENELEC take no position concerning the evidence, validity and scope of these patent rights.

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

Information may be obtained from:

[FF] Fieldbus Foundation
9005 Mountain Ridge Drive
Bowie Bldg. - Suite 190
Austin, TX 78759-5316
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 and CENELEC shall not be held responsible for identifying any or all such patent rights.

Annex ZA has been added by CENELEC.

Endorsement notice

The text of the International Standard IEC 61784-3-1:2007 was approved by CENELEC as a European Standard without any modification.

CONTENTS

INTRODUCTION.....	7
1 Scope.....	10
2 Normative references	10
3 Terms, definitions, symbols, abbreviated terms and conventions	11
3.1 Terms and definitions	11
3.1.1 Common terms and definitions	11
3.1.2 CPF 1: Additional terms and definitions	15
3.2 Symbols and abbreviated terms.....	16
3.2.1 Common symbols and abbreviated terms	16
3.2.2 CPF 1: Additional symbols and abbreviated terms	17
3.3 Conventions	17
3.3.1 State Diagrams.....	17
3.3.2 Use of colors in figures	18
4 Overview of FSCP 1/1 (FOUNDATION Fieldbus™ SIS).....	19
4.1 General.....	19
4.2 Key concepts of FSCP 1/1.....	20
4.2.1 Black channel.....	20
4.2.2 Connection key.....	20
4.2.3 Cross-check	20
4.2.4 FSCP 1/1.....	20
4.2.5 Programmable electronic system	20
4.2.6 Queuing delays	20
4.2.7 Redundancy	21
4.2.8 SIL environment	21
4.3 Key components of FSCP 1/1	21
4.3.1 Overview	21
4.3.2 Black channel.....	21
4.4 Relationship to the ISO OSI basic reference model	22
5 General	22
5.1 External documents providing specifications for the profile	22
5.2 Safety functional requirements	22
5.2.1 Requirements for functional safety.....	22
5.2.2 Functional constraints.....	23
5.2.3 Device manufacturer requirements	23
5.3 Safety measures	24
5.3.1 Sequence number	24
5.3.2 Time stamp	24
5.3.3 Time expectation	24
5.3.4 Connection authentication	24
5.3.5 Data integrity assurance.....	24
5.3.6 Redundancy with cross checking	24
5.3.7 Different data integrity assurance systems	24
5.3.8 Relationships between errors and safety measures	24
5.4 Safety communication layer structure	25
5.4.1 Network topology and device connectivity.....	25

5.4.2	Device architecture.....	25
5.5	Relationships with FAL (and DLL, PhL)	26
5.5.1	General	26
5.5.2	Data Types.....	27
6	Safety communication layer services	27
6.1	Application Process (AP).....	27
6.1.1	Overview	27
6.1.2	Network visible objects	28
6.1.3	Application layer interface	28
6.1.4	Object dictionary	28
6.1.5	Application program directory	28
6.2	Function block application processes	28
6.2.1	General	28
6.2.2	Function block model.....	28
6.2.3	Application process	31
6.3	Device to device communications	33
6.3.1	General	33
6.3.2	Client/server.....	33
6.3.3	Publisher/subscriber	34
6.3.4	Report distribution	34
6.3.5	FBAP operation in a linking device	34
6.3.6	System management kernel protocol (SMKP) communications	34
6.4	Profiles.....	34
6.4.1	General	34
6.4.2	FSCP 1/1 profile	34
6.5	Device descriptions	35
6.6	Common file formats	36
6.7	Configuration information	36
6.7.1	Overview	36
6.7.2	Level 1 configuration: manufacturer device definition.....	36
6.7.3	Level 2 configuration: network definition	36
6.7.4	Level 3 configuration: distributed application definition	36
6.7.5	Level 4 configuration: device configuration	36
7	Safety communication layer protocol	36
7.1	Safety PDU format	36
7.1.1	General	36
7.1.2	Safety communication layer CRC	37
7.1.3	Black channel time synchronization monitoring.....	37
7.1.4	Sequence number	37
7.1.5	Virtual header.....	38
7.1.6	Connection key.....	38
7.1.7	Redundancy and cross-check	39
7.2	Protocol extensions for use in safety-related systems.....	39
7.2.1	Overview	39
7.2.2	Publisher-subscriber interactions	39
7.2.3	Client-server interactions.....	45
7.2.4	Time synchronization.....	50
7.2.5	Device start-up	51
7.3	Communications entity	51

7.3.1	General	51
7.3.2	Network management	51
7.3.3	FMS	51
7.3.4	H1 stack	51
8	Safety communication layer management	52
8.1	Overview	52
8.2	SMK communications	52
8.3	FMS services	52
8.4	SMK services	52
8.4.1	General	52
8.4.2	Address assignment	52
8.4.3	Time synchronization	52
8.5	Safety communication layer configuration and start-up	52
8.5.1	H1 configuration and start-up	52
8.5.2	FSCP 1/1 FBAP	53
8.5.3	Testing	53
9	System requirements	53
9.1	Indicators and switches	53
9.2	Installation guidelines	53
9.3	Safety function response time	53
9.4	Duration of demands	54
9.5	Constraints for calculation of system characteristics	54
9.5.1	Message rate	54
9.5.2	SIL level	54
9.6	Maintenance	54
9.7	Safety manual	54
10	Certification	54
Annex A (informative)	Additional information for functional safety communication profiles of CPF 1	55
A.1	Hash function calculation	55
A.2	Fault conditions arising from locations beyond the output function block	57
Annex ZA (normative)	Normative references to international publications with their corresponding European publications	62
Bibliography		59
Table 1	– Example state transition table	18
Table 2	– Safety measures and possible communication errors	25
Table 3	– Data types used within FSCP 1/1	27
Table 4	– Fault state behaviour	30
Table 5	– Publisher states	40
Table 6	– Publisher state table - Received transitions	41
Table 7	– Publisher state table - Internal transitions	41
Table 8	– Subscriber states	43
Table 9	– Subscriber state table - Received transitions	44
Table 10	– Subscriber state table - Internal transitions	44
Table 11	– Server states during read operations	46
Table 12	– Received transitions for a FSCP 1/1 Server during read operations	47

Table 13 – States of a FSCP 1/1 server during write operations.....	48
Table 14 – Received transitions for a FSCP 1/1 Server during write operations	49
Table A.1 – Fault conditions arising from locations beyond the output function block	58
Figure 1 – Relationships of IEC 61784-3 with other standards (machinery)	7
Figure 2 – Relationships of IEC 61784-3 with other standards (process).....	8
Figure 3 – Example state diagram.....	18
Figure 4 – Use of colors in figures	18
Figure 5 – Scope of FSCP 1/1	19
Figure 6 – FSCP 1/1 architecture (H1)	21
Figure 7 – Black channel	22
Figure 8 – FSCP 1/1 in system architecture	25
Figure 9 – FSCP 1/1 H1 device.....	26
Figure 10 – FSCP 1/1 protocol layers	26
Figure 11 – Relationship between FSCP 1/1 and the other layers of IEC 61158 Type 1	27
Figure 12 – Key write-lock	29
Figure 13 – Password write-lock	29
Figure 14 – Example of FSCP 1/1 communication.....	33
Figure 15 – Example of device description.....	35
Figure 16 – Safety PDU showing virtual content.....	40
Figure 17 – Safety PDU showing duplication of data and addition of CRC.....	40
Figure 18 – State transition diagram for a FSCP 1/1 Publisher.....	41
Figure 19 – Safety PDU showing duplication of data and addition of CRC.....	42
Figure 20 – Safety PDU showing virtual content.....	42
Figure 21 – State transition diagram for a FSCP 1/1 subscriber	43
Figure 22 – Safety PDU showing virtual content.....	45
Figure 23 – Safety PDU showing virtual content with sub index	45
Figure 24 – Safety PDU showing duplication of data, addition of sequence number and CRC.....	46
Figure 25 – State transition diagram for a FSCP 1/1 Server during read operations	46
Figure 26 – Safety PDU showing duplication of data and addition of sequence number and CRC.....	47
Figure 27 – Example of FSCP 1/1 write	48
Figure 28 – Example of FSCP 1/1 write with sub index	48
Figure 29 – State transition diagram for a FSCP 1/1 Server during write operations.....	49
Figure 30 – Safety PDU showing duplication of data and CRC	50
Figure 31 – Example of safety function response time components.....	53

INTRODUCTION

The IEC 61158 fieldbus standard together with its companion standards IEC 61784-1 and IEC 61784-2 defines a set of communication protocols that enable distributed control of automation applications. Fieldbus technology is now considered well accepted and well proven. Thus many fieldbus enhancements are emerging, addressing not yet standardized areas such as real time, safety-related and security-related applications.

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

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

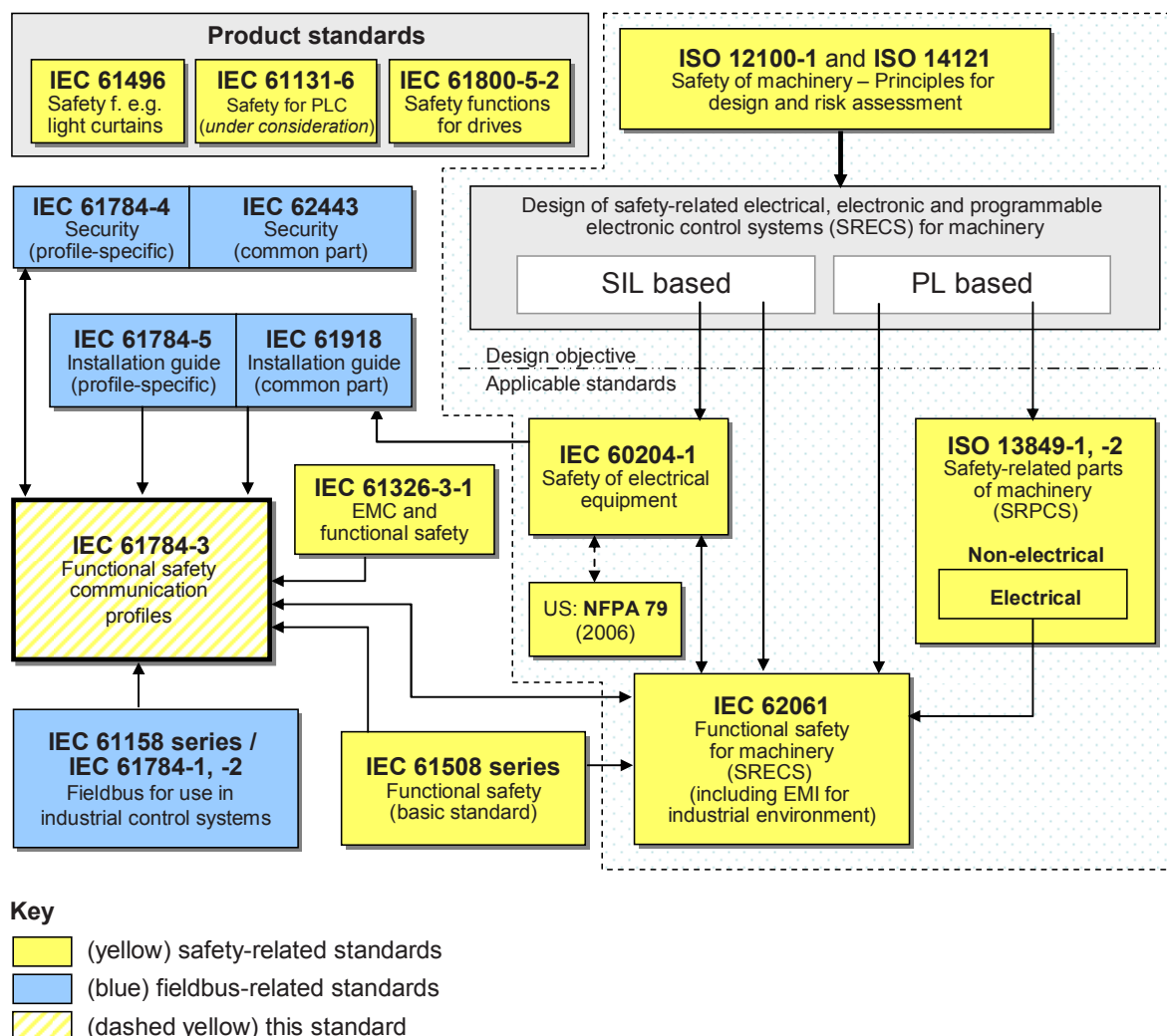
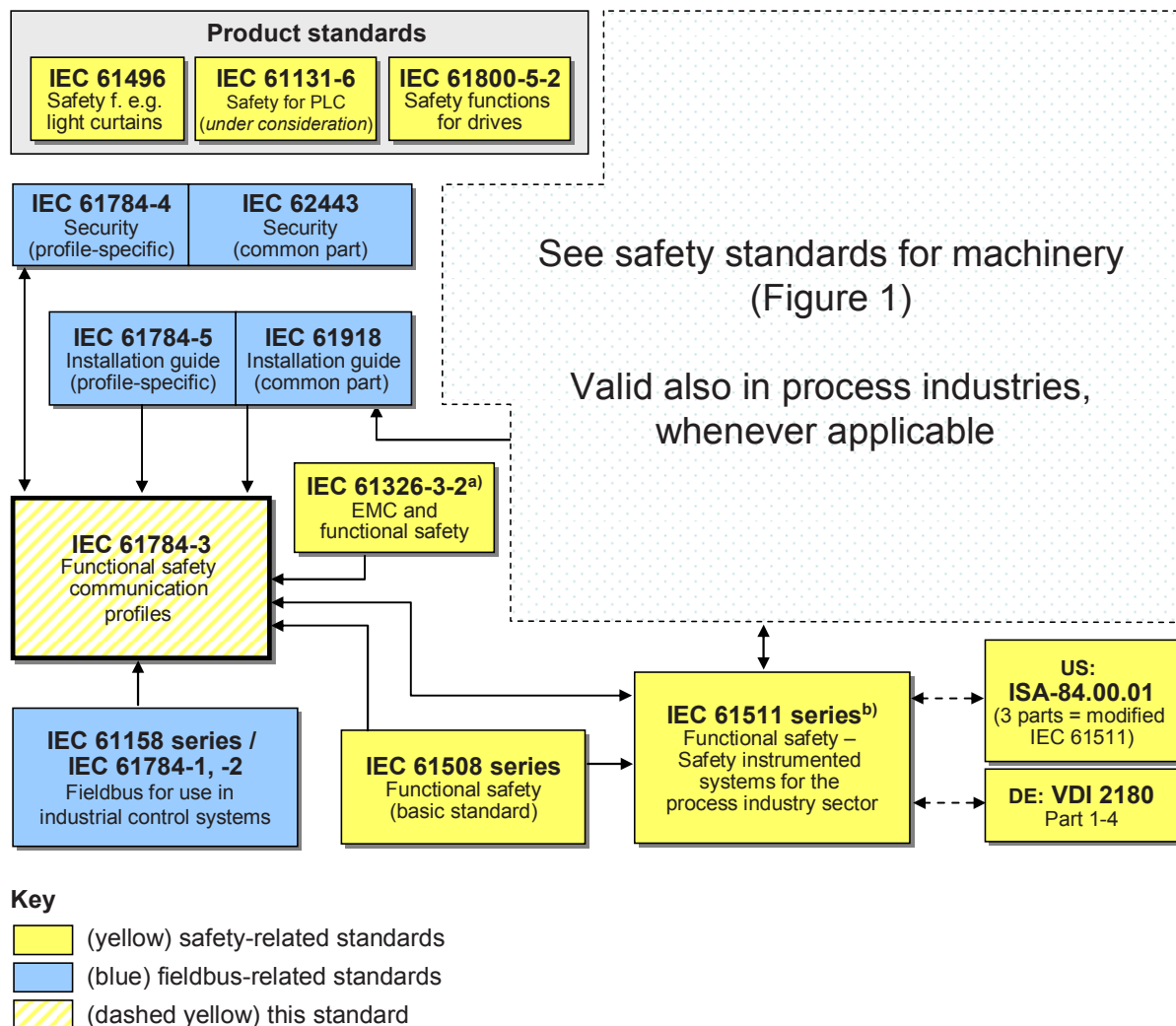


Figure 1 – Relationships of IEC 61784-3 with other standards (machinery)

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



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

^b EN ratified.

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

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

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

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

This standard describes

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

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES

Part 3-1: 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 Type 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 part¹ 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 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*

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*

¹ In the following pages of this standard, “this part” will be used for “this part of the IEC 61784-3 series”.

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

3 Terms, definitions, symbols, abbreviated terms and conventions

3.1 Terms and definitions

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

3.1.1 Common terms and definitions

3.1.1.1

availability

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

NOTE Availability depends on MTBF (mean time between failure) and MDT (mean down time):
 $\text{Availability} = \text{MTBF} / (\text{MTBF} + \text{MDT})$.

3.1.1.2

black channel

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

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 [28], [29]².

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

NOTE 1 An error can be caused by a faulty item, e.g. a computing error made by faulty computer equipment.

[IEV 191-05-24], [IEC 61508-4:1998], [IEC 61158]

NOTE 2 Errors may be due to design mistakes within hardware/software and/or corrupted information due to electromagnetic interference and/or other effects.

NOTE 3 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

NOTE 1 The definition in IEV 191-04-01 is the same, with additional notes.

[IEC 61508-4:1998], [ISO/IEC 2382-14.01.11]

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 preventative maintenance or other planned actions, or due to lack of external resources.

[IEC 61508-4:1998], [ISO/IEC 2382-14.01.10]

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

² Figures in square brackets refer to the bibliography.

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 [28], [29].

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 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

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]

3.1.1.21

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

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

NOTE 1 Redundancy is used primarily to improve reliability or availability.

NOTE 2 The definition in IEC 191-15-01 is less complete.

[IEC 61508-4:1998], [ISO/IEC 2382-14.01.12]

3.1.1.22

reliability

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

NOTE 1 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]

3.1.1.23

risk

combination of the probability of occurrence of harm and the severity of that harm
[IEC 61508-4:1998]

3.1.1.24

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

3.1.1.25

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.

3.1.1.26

safety device

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

3.1.1.27

safety function

function to be implemented by an E/E/PE safety-related system, other technology *safety-related system* or external risk reduction facilities, which is intended to achieve or maintain a safe state for the EUC, in respect of a specific hazardous event
[IEC 61508-4:1998]

3.1.1.28

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, 5.2.4 and addressed by the functional safety communication profiles defined in this part.

3.1.1.29

safety integrity level (SIL)

discrete level (one out of a possible four) for specifying the safety integrity requirements of the *safety functions* to be allocated to the E/E/PE safety-related systems, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest

NOTE The target failure measures for the four safety integrity levels are specified in Tables 2 and 3 of IEC 61508-1.

[IEC 61508-4:1998]

3.1.1.30

safety measure

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

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

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

3.1.1.31

safety-related application

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

3.1.1.32

safety-related system

system performing *safety functions* according to IEC 61508

3.1.1.33

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

3.1.1.34

spurious trip

trip caused by the safety system without a process demand

3.1.1.35

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	
EMI	Electro-Magnetic Interference	
EUC	Equipment Under Control	[IEC 61508-4:1998]
FAL	Fieldbus Application Layer	[IEC 61158-5]
FCS	Frame Check Sequence	
FSCP	Functional Safety Communication Profile	
E/E/PE	Electrical/Electronic/Programmable Electronic	[IEC 61508-4:1998]
PDU	Protocol Data Unit	[ISO/IEC 7498-1]
PES	Programmable Electronic System	[IEC 61508-4:1998]
PFD	Average Probability of Failure on Demand	[IEC 61508-6:1998]
PFH	Probability of Failure per Hour	[IEC 61508-6:1998]
PhL	Physical Layer	[ISO/IEC 7498-1]

PLC	Programmable Logic Controller	
SCL	Safety Communication Layer	
SIL	Safety Integrity Level	[IEC 61508-4:1998]
SR	Safety Relevant	

3.2.2 CPF 1: Additional symbols and abbreviated terms

AP	Application Process
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
FIFO	First-In First-Out
FMS	Field 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.

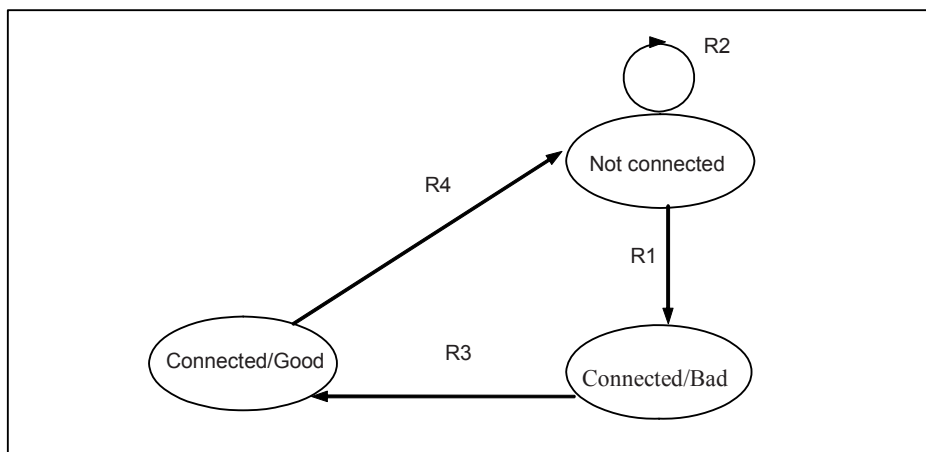


Figure 3 – Example state diagram

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.

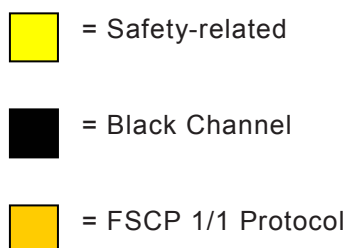


Figure 4 – Use of colors in figures