

Industrial communication networks — Profiles —

Part 3-6: Functional safety fieldbuses — Additional specifications for CPF 6

ICS 25.040.40; 35.100.05

National foreword

This British Standard is the UK implementation of EN 61784-3-6:2008. It is identical to IEC 61784-3-6:2007.

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 61652 5

Amendments/corrigenda issued since publication

Date	Comments

**Industrial communication networks -
Profiles -
Part 3-6: Functional safety fieldbuses -
Additional specifications for CPF 6
(IEC 61784-3-6:2007)**

Réseaux de communication industriels -
Profils -
Partie 3-6: Bus de terrain
de sécurité fonctionnelle -
Spécification supplémentaire pour CPF 6
(CEI 61784-3-6:2007)

Industrielle Kommunikationsnetze -
Profile -
Teil 3-6: Funktional sichere Übertragung
bei Feldbussen -
Zusätzliche Festlegungen für die
Kommunikationsprofilfamilie 6
(IEC 61784-3-6:2007)

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 61784-3-6, 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 61784-3-6 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 6 as follows, where the [xx] notation indicates the holder of the patent right:

DE 103 25 263 A1 [PxC]	Sicherstellung von maximalen Reaktionszeiten in komplexen oder verteilten sicheren und/oder nicht sicheren Systemen
DE 103 18 068 A1 [PxC]	Verfahren und Vorrichtung zum Paket-orientierten Übertragen sicherheitsrelevanter Daten

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:

[PxC] Phoenix Contact GmbH & Co. KG
Intellectual Property Licenses & Standards
Flachsmarktstr. 8
D-32825 Blomberg,
Germany

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 61784-3-6:2007 was approved by CENELEC as a European Standard without any modification.

CONTENTS

INTRODUCTION.....	8
1 Scope.....	11
2 Normative references	11
3 Terms, definitions, symbols, abbreviated terms and conventions	12
3.1 Terms and definitions	12
3.1.1 Common terms and definitions	12
3.1.2 CPF 6: Additional terms and definitions	16
3.2 Symbols and abbreviated terms.....	17
3.2.1 Common symbols and abbreviated terms	17
3.2.2 CPF 6: Additional symbols and abbreviated terms	17
3.3 Conventions	18
4 Overview of FSCP 6/7 (INTERBUS™ Safety)	18
4.1 General.....	18
4.2 Technical overview.....	18
4.3 Functional Safety Communication Profile 6/7.....	19
5 General	20
5.1 External documents providing specifications for the profile	20
5.2 Safety functional requirements	20
5.3 Safety measures	20
5.3.1 General	20
5.3.2 Sequence number	21
5.3.3 Time stamp	21
5.3.4 Time expectation	21
5.3.5 Acknowledgement	21
5.3.6 Connection authentication	21
5.3.7 Distinction between safety relevant messages and non-safety relevant messages – different data integrity assurance system.....	22
5.3.8 Parameterized shutdown time.....	22
5.4 Safety communication layer structure	22
5.4.1 Decomposition process.....	22
5.4.2 Definition of the safety function of the safety communication system	23
5.4.3 Decomposition of the safety function of a safety communication system into function blocks.....	24
5.4.4 Assignment of the function blocks to subsystems	25
5.4.5 Safety requirements and safety integrity requirements.....	28
5.4.6 Specification of the safe state.....	28
5.4.7 Response to a fault	29
5.4.8 Stop category	31
5.4.9 Safe Transmission.....	31
5.5 Relationships with FAL (and DLL, PhL)	32
5.5.1 Overview	32
5.5.2 Use of the AR-US service to initiate and parameterize.....	32
5.5.3 Use of the AR-US service to transmit safety data	33
5.5.4 Use of the AR-US service to abort.....	34
5.5.5 Data types.....	34
6 Safety communication layer services	34

6.1	General	34
6.2	Transmission principle for safety messages between SCLM and SCLS	34
6.3	Function block requirements	35
6.3.1	Input Safe Data function block	35
6.3.2	Output Safe Data function block	35
6.3.3	Safe Calculation function block	35
6.4	Context management	36
6.4.1	Initiate service	36
6.4.2	Abort service	37
6.5	Function block parameterization	38
6.5.1	Send application parameter service	38
6.5.2	Send application parameter ID service	39
6.5.3	Parameterize device service	40
6.6	Safe Process Data Mode	40
6.6.1	Transmit-Safety-Data	40
6.6.2	Set-Diagnostic-Data service	42
6.6.3	Set-Acknowledgement-Data service	42
7	Safety communication layer protocol	43
7.1	Safety PDU format	43
7.1.1	Structure of safety messages	43
7.1.2	Description of the polynomial used	44
7.1.3	Structure of safety messages for safe parameterization and idle	44
7.1.4	Structure of safety messages for the transmission of safety data	50
7.1.5	Messages for synchronization	51
7.1.6	Structure of safety messages for aborting connections	52
7.2	State description	53
7.2.1	SCLM and SCLS state machines	53
7.2.2	Initiate	54
7.2.3	Parameterization	55
7.2.4	Process data mode	58
7.2.5	Process data mode with diagnostic data transmission	63
7.2.6	Process data mode with Acknowledgement-Data transmission	64
7.2.7	Connection aborted	65
7.3	Abort	65
7.3.1	Connection abort in the event of an error detected by the SCLM	65
7.3.2	Abort of all connections in the event of an error detected by the SCLS	66
7.3.3	Abort of all connections in the event of an error detected by the SCLM	68
8	Safety communication layer management	69
8.1	General	69
8.2	Requirements of safety communication layer management	69
8.3	Set-Safety-Configuration service	69
8.4	Start IEC 61158 Type 8 service	71
9	System requirements	71
9.1	Indicators and switches	71
9.2	Installation guidelines	71
9.3	Safety function response time	71
9.3.1	General	71

9.3.2	Calculation of the parameterized shutdown time	72
9.4	Duration of demands	76
9.5	Constraints for calculation of system characteristics	76
9.5.1	System characteristics	76
9.5.2	Calculation of the number of telegrams per second	76
9.6	Maintenance	77
9.7	Safety manual	78
10	Certification	78

Annex ZA (normative)	Normative references to international publications with their corresponding European publications	82
----------------------	---	----

Bibliography	79
--------------------	----

Table 1 – Overview of profile identifier usable for FSCP 6/7	20
Table 2 – Selection of the various measures for possible errors	21
Table 3 – List of function blocks and subsystems	25
Table 4 – Signal flow between the function blocks	27
Table 5 – Initiate service parameters	36
Table 6 – Parameterization mode and related services	37
Table 7 – Abort service parameters	37
Table 8 – Abort of a point-to-point connection by the SRP or SRC	38
Table 9 – Send application parameter service	38
Table 10 – Send application parameter ID service	39
Table 11 – Parameterize device parameters	40
Table 12 – Transmit-Safety-Data service parameters	41
Table 13 – Set-Diagnostic-Data service parameters	42
Table 14 – Set-Acknowledgement-Data service parameters	43
Table 15 – Parameter ID	46
Table 16 – Block 0: Device ID	47
Table 17 – Block 1: Parameter record ID	48
Table 18 – Block 2: Application parameter	48
Table 19 – TIME encoding	51
Table 20 – Abort_Info: Connection abort in the event of an error detected by the SCLM	66
Table 21 – Abort_Info: Abort of all connections in the event of an error detected by the SCLS	67
Table 22 – Abort_Info: Abort of all connections in the event of an error detected by the SCLM	69
Table 23 – Set-Safety-Configuration service	70
Table 24 – Error_Info	70
Table 25 – Calculation of t_{IB}	75
Table 26 – Calculation of t_{SRC}	76
Table 27 – Calculation of t_{PST}	76

Figure 1 – Relationships of IEC 61784-3 with other standards (machinery)	8
--	---

Figure 2 – Relationships of IEC 61784-3 with other standards (process)	9
--	---

Figure 3 – FSCP 6/7 communication preconditions	19
Figure 4 – Example of a safety function	23
Figure 5 – Decomposition of safety function into function blocks	24
Figure 6 – Overview of the results of the decomposition process	26
Figure 7 – Signal flow between the function blocks	26
Figure 8 – Interfaces between the safety devices within the safety communication system	27
Figure 9 – Signal flow and safe states	29
Figure 10 – Mapping of the Safe Transmission function block	31
Figure 11 – Relationship between SCL and the other layers of IEC 61158 Type 8	32
Figure 12 – Use of the AR-US service to initiate and parameterize	33
Figure 13 – Use of the AR-US service to transmit safety data	33
Figure 14 – Use of the AR-US service to abort	34
Figure 15 – Use of the AR-US service to abort	34
Figure 16 – Structure of the safety PDU	43
Figure 17 – Integration of safety data and deterministic remedial measures in the summation frame	44
Figure 18 – Write_Parameter_Byte_Req message	45
Figure 19 – Read_Parameter_Byte_Req message	45
Figure 20 – Parameter_Byte_Con message	45
Figure 21 – Set_Safety_Connection_ID_Req message	49
Figure 22 – Set_Safety_Connection_ID_Con message of safety slaves	49
Figure 23 – Parameter_Idle_Req	49
Figure 24 – Parameter_Idle_Con	49
Figure 25 – Parameter_Check_Con	50
Figure 26 – Parameter_Loc_ID_Changed_Con	50
Figure 27 – Transmit Safety Data Message	50
Figure 28 – Sync_a message of the SCLM	51
Figure 29 – Req_b message of the SCLM	52
Figure 30 – Req_c message of the SCLM	52
Figure 31 – Req_d message of the SCLM	52
Figure 32 – Abort_Connection message	53
Figure 33 – Safety-Slave_Error message	53
Figure 34 – SCLM state machine	53
Figure 35 – SCLS state machine	54
Figure 36 – Initiate sequence	55
Figure 37 – Send Application Parameter sequence	56
Figure 38 – Send Application Parameter ID sequence	57
Figure 39 – Parameterize device sequence	58
Figure 40 – Simultaneous transmission of safety data to the safety slaves	59
Figure 41 – Use of the sequence number in the SCLM and SCLS	60
Figure 42 – Startup and error-free operation	61
Figure 43 – Resynchronization during operation	62
Figure 44 – Invalid CRC 24 checksum detected by the SCLS	63

Figure 45 – Process data mode with diagnostic data transmission	64
Figure 46 – Process data mode with Acknowledgement-Data transmission	65
Figure 47 – Error when initiating a connection	66
Figure 48 – Error at an SCLS when aborting all connections.....	67
Figure 49 – Abort of all connections in the event of an error detected by the SCLM	68
Figure 50 – Overview of the shutdown time.....	73

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.

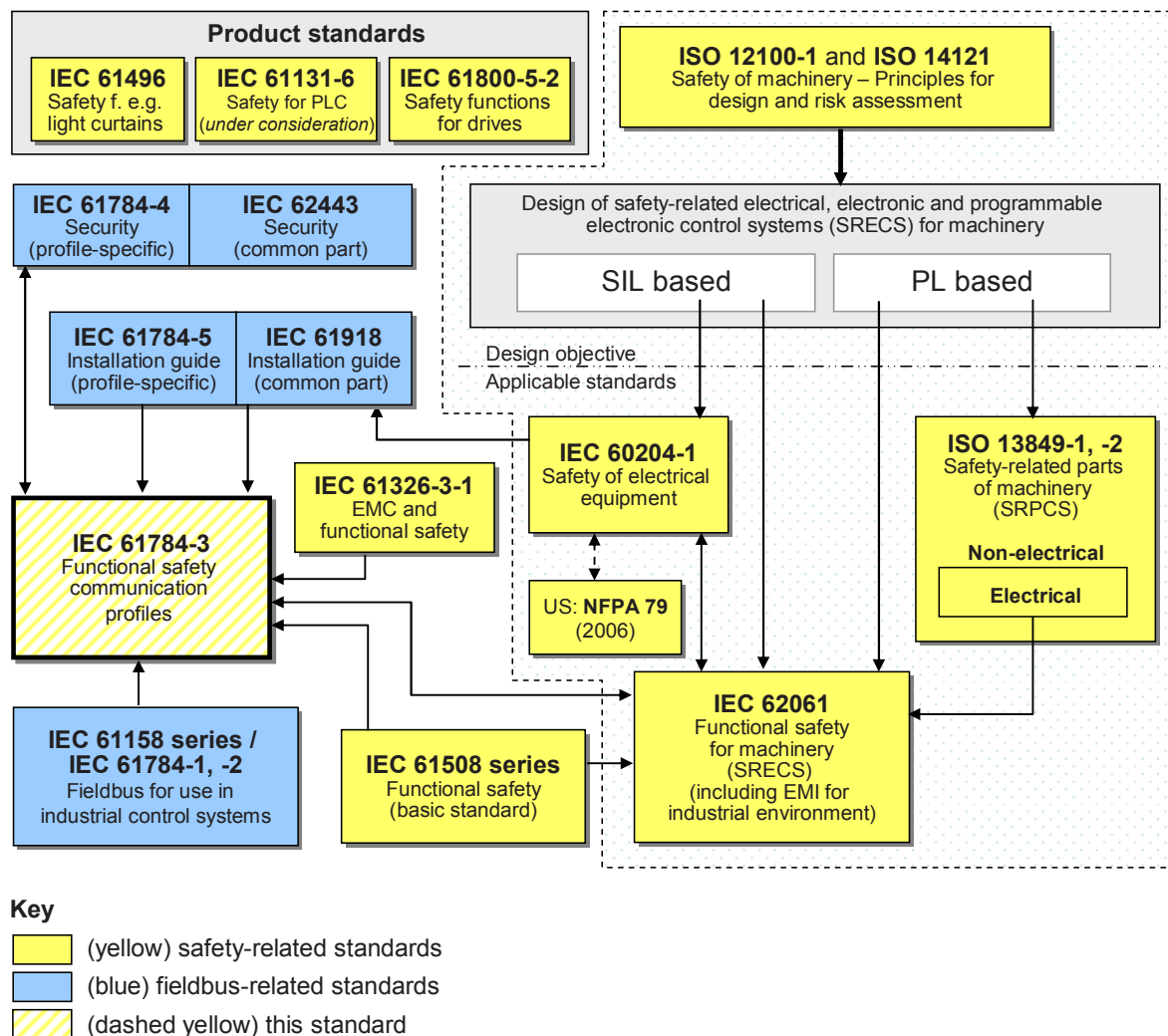
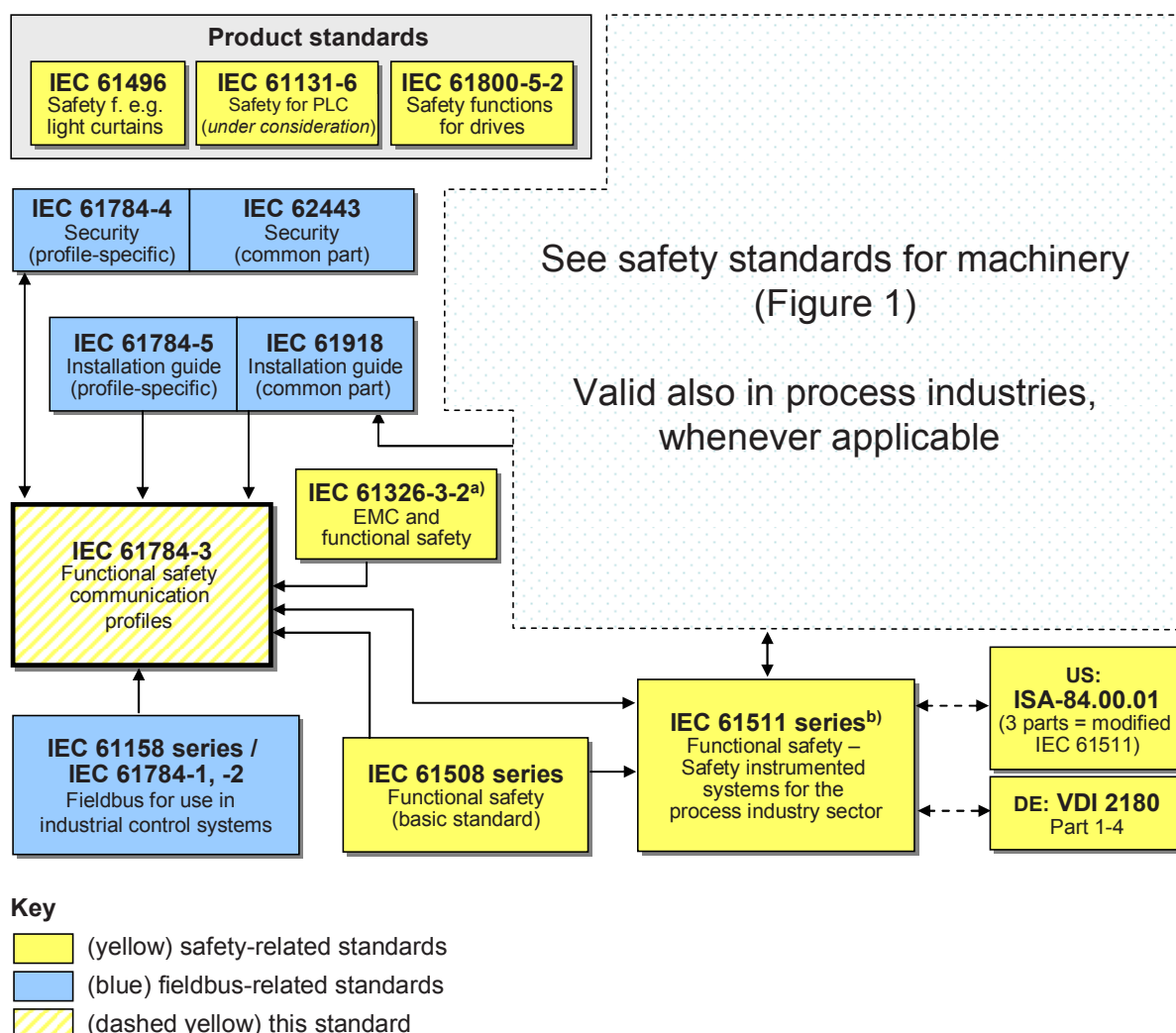


Figure 1 – Relationships of IEC 61784-3 with other standards (machinery)

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 3-6: Functional safety fieldbuses – Additional specifications for CPF 6

1 Scope

This part of the IEC 61784-3 series specifies a safety communication layer (services and protocol) based on CPF 6 of IEC 61784-1, IEC 61784-2 and IEC 61158 Type 8. 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 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 61131-3, *Programmable controllers – Part 3: Programming languages*

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

IEC 61158-3-8, *Industrial communication networks – Fieldbus specifications – Part 3-8: Data-link layer service definition*

IEC 61158-4-8, *Industrial communication networks – Fieldbus specifications – Part 4-8: Data-link layer protocol specification*

IEC 61158-5-8, *Industrial communication networks – Fieldbus specifications – Part 5-8: Application layer service definition*

IEC 61158-6-8, *Industrial communication networks – Fieldbus specifications – Part 6-8: Application layer protocol specification*

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

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

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

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

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

IEC 61784-5-6, *Industrial communication networks – Profiles – Part 5: Installation of fieldbuses – Installation profiles for CPF 6*

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

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

3 Terms, definitions, symbols, abbreviated terms and conventions

3.1 Terms and definitions

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

3.1.1 Common terms and definitions

3.1.1.1

availability

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

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

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

3.1.1.3

connection

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

3.1.1.4

Cyclic Redundancy Check (CRC)

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

<method> procedure used to calculate the redundant data

NOTE 1 Terms “CRC code” and “CRC signature”, and labels such as CRC1, CRC2, may also be used in this standard to refer to the redundant data.

NOTE 2 See also [32], [33]².

² Figures in square brackets refer to the bibliography.

3.1.1.5

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*.

3.1.1.6

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)

3.1.1.7

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]

3.1.1.8

fieldbus

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

3.1.1.9

fieldbus system

system using a *fieldbus* with connected devices

3.1.1.10

frame

denigrated synonym for DLPDU

3.1.1.11

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]

3.1.1.12**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

3.1.1.13**master**

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

3.1.1.14**message**

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

3.1.1.15**protective extra-low-voltage (PELV)**

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

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

[IEC 61131-2]

3.1.1.16**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]

3.1.1.17**relative time stamp**

time stamp referenced to the local clock of an entity

NOTE In general, there is no relationship to clocks of other entities.

[IEC 62280-2, modified]

3.1.1.18**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]

3.1.1.19

risk

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

3.1.1.20

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

3.1.1.21

safety connection

connection that utilizes the safety protocol for communications transactions

3.1.1.22

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.

3.1.1.23

safety device

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

3.1.1.24

safety extra-low-voltage (SELV)

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

NOTE An SELV circuit is not connected to protective earth.

[IEC 61131-2]

3.1.1.25

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]

3.1.1.26

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.

3.1.1.27

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]

3.1.1.28

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.

3.1.1.29

safety-related application

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

3.1.1.30

safety-related system

system performing *safety functions* according to IEC 61508

3.1.1.31

SIL claim limit (SIL CL)

maximum SIL that can be claimed for a *safety-related system* in relation to architectural constraints and systematic safety integrity

[IEC 62061, modified]

3.1.1.32

slave

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

3.1.1.33

time stamp

time information included in a *message*

3.1.2 CPF 6: Additional terms and definitions

3.1.2.1

cycle

interval at which an activity is repetitively and continuously executed

3.1.2.2

parameterized shutdown time

safety function response time (worst-case response time for each safety function) without t_1 and t_2

NOTE See IEC 61784-3, 5.2.4, Figure 4.

3.1.2.3

safety PDU

synonym for safety-related DLPDU

3.1.2.4

safety (input/output) data

data that is input/output safely at the external interfaces (terminal blocks) of the function blocks

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]
FSCP	Functional Safety Communication Profile	
E/E/PE	Electrical/Electronic/Programmable Electronic	[IEC 61508-4:1998]
PDU	Protocol Data Unit	[ISO/IEC 7498-1]
PELV	Protective Extra Low Voltage	
PES	Programmable Electronic System	[IEC 61508-4:1998]
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	
SELV	Safety Extra Low Voltage	
SIL	Safety Integrity Level	[IEC 61508-4:1998]
SIL CL	SIL Claim Limit	[IEC 62061]

3.2.2 CPF 6: Additional symbols and abbreviated terms

3.2.2.1 Additional abbreviated terms

SCLM	Safety Communication Layer Master
SCLS	Safety Communication Layer Slave
SRC	Safety Relevant Controller
SRP	Safety Relevant Peripheral
S_CON_ID	Safety Connection ID

3.2.2.2 Additional symbols

Symbol	Definition	Unit
a	Number of all slaves	—
AF	Availability factor	—
I _s	Number of safety slaves	
M	Type 8 master implementation factor	—
n	Number of data octets	octet
n _{as}	Number of safety slaves	—
n _{FBS}	Number of used function blocks (in the safety-related application software)	—
P _e	Bit error probability	—
R _{SL} (P _e)	residual error probability of a safety message	—
t _A	Response time of the actuator	ms
t _{CTSCS}	Cycle time of the functional safety communication system	ms
t _G	Guaranteed shutdown time	ms

Symbol	Definition	Unit
T_{bit}	Nominal bit duration	ms
t_{IB}	Cycle time of the IEC 61158 Type 8 communication system	ms
t_{IN}	Processing time of the safety input	ms
t_{FBS}	Average function block processing time (in the safety-related application software)	ms
t_{OD}	Processing time of the safety output device	ms
t_{PST}	Parameterized shutdown time of a safety output	ms
t_{S}	Sensor response time	ms
t_{SF}	Safety function response time	ms
t_{SRC}	Processing time of the SRC	ms
t_{Stop}	Machine stopping time	ms
t_{SW}	Software processing time of the master (application specific)	ms
$\Lambda_{\text{SL}}(P_e)$	Residual error rate per hour of the safety communication layer with respect to the bit error probability	—
v	Maximum number of safety messages per hour	—

3.3 Conventions

The conventions for service definitions of IEC 61158-5-8, 3.8.4, are used.

4 Overview of FSCP 6/7 (INTERBUS™ Safety)

4.1 General

Communication Profile Family 6 (commonly known as INTERBUS®³) defines communication profiles based on IEC 61158-2 Type 8, IEC 61158-3-8, IEC 61158-4-8, IEC 61158-5-8, and IEC 61158-6-8.

The basic profiles CP 6/1, CP 6/2, CP 6/3 are defined in IEC 61784-1. The CPF 6 functional safety communication profile FSCP 6/7 (INTERBUS Safety™³) is based on the CPF 6 basic profiles in IEC 61784-1 and the safety communication layer specifications defined in this part.

4.2 Technical overview

FSCP 6/7 uses the existing conveyance path for cyclic transmission of data (for process data). This is in principle a master slave concept with a physical ring topology and logical one-to-one relationships between one master and each of its slaves (Figure 3). The data is transmitted via a PDU – commonly known as summation frame – from which each slave extracts its output data and insert its input data.

³ INTERBUS® and INTERBUS Safety™ are trade names of Phoenix Contact GmbH & Co. KG, control of trade name use is given to the non profit organization INTERBUS Club. 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 does not require use of the trade names INTERBUS® or INTERBUS Safety™. Use of the trade names INTERBUS® or INTERBUS Safety™ requires permission of the INTERBUS Club.

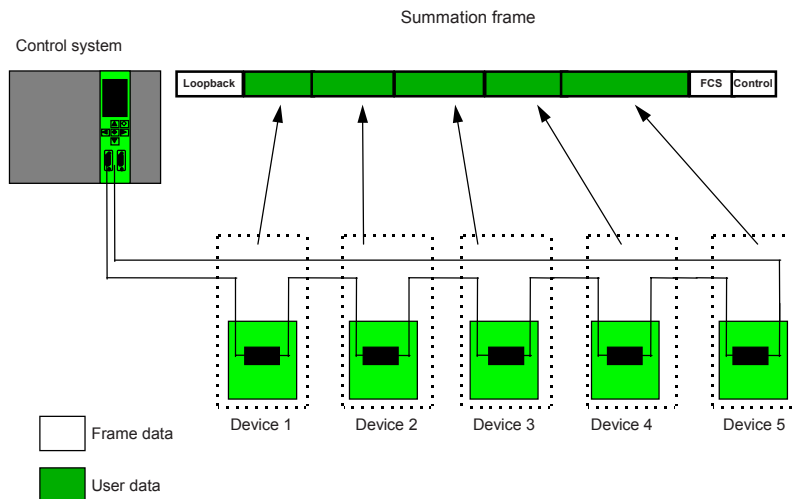


Figure 3 – FSCP 6/7 communication preconditions

The safety communication layer of FSCP 6/7 provides the following safety measures to realize its safety communication layer:

- sequence number;
- time stamp;
- connection authentication;
- cyclic redundancy checking for safety data integrity.

Sequence numbering uses the range from 001 to 111 without 000. The connection authentication (sender/receiver information) consists of 7 bits so that up to 126 slaves can be integrated in the safety fieldbus. Safety data can be conveyed from the safety master to each safety slave and from each safety slave to the safety master within a single data cycle. A separate watchdog timer in each safety output slave ensures a safety function response time for each safety function and can be widely parameterized. The watchdog timer can be adjusted for each safety output channel of a safety output slave.

The safety communication layer of FSCP 6/7 can be used for safety functions up to SIL 3. Therefore the safety fieldbus consumes at a maximum 1 % of the overall PFH. Within the safety fieldbus $\Lambda < 10^{-7}$ is achieved. An integrated watchdog timer providing the time expectation of each output channel on each safety output slave ensures a functional safety response time. The functional safety response time comprises the fieldbus transmission time from a safety input slave to the master and from the master to the safety output slave including also possible repetitions of the safety PDU due to transmission errors, the processing time on each safety slave (input and output) and the processing time within the PES (usually realized as a safety PLC with an integrated master) and the stopping time of a machine. If the configured time of the integrated watchdog timer of a specific output channel of a safety output slave is exceeded the corresponding output channel is set to its safe state which is usually the powerless state.

The structure of the safety PDU comprises the safety measures (sequence number, time stamp, connection authentication, CRC) and the safety data. The safety data and the safety measures for each safety slave will be integrated in the summation frame.

4.3 Functional Safety Communication Profile 6/7

The CPF 6 functional safety communication profile FSCP 6/7 is based on the CPF 6 profiles CP 6/1, CP 6/2 and CP 6/3 specified in IEC 61784-1. The profiles CP 6/1, CP 6/2 and CP 6/3 contain optional services, which are specified by profile identifiers. The suitable profile identifiers for CP 6/7 are shown in Table 1.

Table 1 – Overview of profile identifier usable for FSCP 6/7

Profile	Master		Slave		
	cyclic	cyclic and non cyclic	cyclic	non cyclic	cyclic and non cyclic
Profile 6/1	618	619	611	—	613
Profile 6/2	—	629	—	—	623
Profile 6/3	—	639	—	—	633

The safety communication layer specification given in this part fully applies.

5 General

5.1 External documents providing specifications for the profile

Manufacturers of a safety device are recommended to check the documents [31], and [42] to [48] that provide additional specifications which may be relevant for implementation of the SCL defined in this part.

5.2 Safety functional requirements

Requirements for the design of safety devices such as safety master and safety slaves are outside the scope of this part. The designer of such devices shall have take into account the requirements of IEC 61508.

Some of the requirements for the function blocks which shall be implemented on the safety devices are specified in 6.3. The requirements for the function blocks used in this part for specification of services and protocols are specified in 5.4.

Specifications of subsystems or subsystem elements are implementation specific and therefore outside the scope of this part. This part only specifies the services and protocols for a functional safety communication system based on IEC 61158 series Type 8.

The description of safe states is given in 5.4.6.

5.3 Safety measures

5.3.1 General

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

- Sequence number
- Time stamp
- Connection authentication
- Cyclic redundancy check for safety data integrity (CRC 24)
- Different data integrity assurance systems.

The selection of the various measures for possible errors is shown in Table 2.

Table 2 – Selection of the various measures for possible errors

Communication errors	Deterministic Remedial Measures							
	Sequence number	Time stamp	Time expectation	Connection authentication	Feedback message	Data Integrity assurance	Redundancy with cross checking	Different data integrity assurance systems
Corruption						X		
Unintended repetition	X							
Incorrect sequence	X							
Loss	X							
Unacceptable delay		X ^d	X ^c					
Insertion	X			X ^{a,b}				
Masquerade				X ^a				X
Addressing				X				
NOTE Table adapted from IEC 62280-2 and EN 954-1.								
^a Depends on application. ^b Only for transmitter identification. Only detects insertion of an invalid source. ^c Required in all cases. ^d Time stamp is created locally on SCLS side. Detection of unintended repetition and incorrect sequence can not be done with this. IEC 61158 series Type 8 specific.								

5.3.2 Sequence number

Safety messages contain a sequence number with a width of 3 bits and a specified sequence (see 7.1 and 7.2). If the sequence is not followed, all safety related output signals shall be set to their safe states (Figure 47, Figure 48). All safety slaves shall have the same sequence number at all times (see 7.1 and 7.2).

5.3.3 Time stamp

The sequence number and a local clock can be used to generate a local relative time stamp for each SCLS. This relative time stamp refers to all safety input and output data in the system.

5.3.4 Time expectation

The SCLS can use the time stamp to determine whether or not the safety input data that is used to link the safety output data is too old.

5.3.5 Acknowledgement

An acknowledgement is provided when the sequence number is updated correctly.

5.3.6 Connection authentication

The connection authentication is implemented by a safety connection ID (S_CON_ID), which consists of 7 bits so that up to 126 slaves can be integrated in the functional safety

communication system. The assignment of safety connection IDs shall be unique within a functional safety communication system.

The safety messages always contain the safety connection ID.

5.3.7 Distinction between safety relevant messages and non-safety relevant messages – different data integrity assurance system

Safety messages (48 bits) contain a CRC checksum (24 bits). The IEC 61158 Type 8 protocol uses a different CRC algorithm (16-bit CRC). In addition, each telegram contains a 7-bit safety connection ID.

5.3.8 Parameterized shutdown time

An integrated watchdog timer providing the time expectation of each output channel on each safety output slave ensures a parameterized shutdown time, which is the time between the detection of an event at the safety input slave and the response at the corresponding output channel(s) on the safety output slave(s) without the processing time of the safety input. For details see also 9.3.2.2.

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

If the parameterized shutdown time of a specific output channel of a safety output slave is exceeded, the corresponding output channel is set to its safe state, which is usually the power OFF state. This shall be observed by the application layer of the SRP.

5.4 Safety communication layer structure

5.4.1 Decomposition process

The IEC 61158 Type 8 system was designed for short response times and foreseeable transmission times. Both qualities are needed in safety-related applications.

EXAMPLE 1 A dangerous movement needs to be stopped as quickly as possible. For this, a safety communication system with short transmission times is required.

EXAMPLE 2 Protective devices have to be installed at a safe distance so that people are not able to access the machine before the movement has stopped. To calculate this safe distance, a definition of a worst-case response time is required.

To perform safety functions, devices are usually used, which incorporate neither complex electronics nor programmable electronics. The failure modes of these devices are very well defined. Conventional technologies are limited if the application requirements increase with regard to flexibility, functionality, and diagnostics. The aim of the development of a safety communication system based on an IEC 61158 Type 8 system was to transfer the advantages of a standard fieldbus system to safety technology.

The design of the safety communication layer follows the principles of IEC 61508, IEC 62061, and EN 954-1.

NOTE 1 Following the principles of IEC 62061 does not mean that it is limited to machinery only.

The first step after determining the limits of a machine and defining a suitable machinery concept is usually to perform a risk reduction process according to ISO 12100. Safety functions that are needed to ensure the required level of functional safety for each hazard determined are specified later on.

EXAMPLE 3 A safety function can be "If the guard door is open, the speed of shaft rotation is set to zero within a specified time".

The decomposition process of the overall application-specific safety function down to the fieldbus system is shown below. The result of this process is the specification of function blocks and the interfaces between them.

NOTE 2 The term "safety function block" is used in the same manner as in IEC 62061, but does not limit the scope of this part to the machinery sector alone.

5.4.2 Definition of the safety function of the safety communication system

A fieldbus system performs only part of a safety function specified for a safety relevant control system by itself. For this, sensors, actuators (for example, guard door switch, contactor), and usually application software are also required.

The safety function of a safety communication system is to transmit safety data from an input to an output within a specified time. Figure 4 provides an example of a safety function within a machine. The black box in the middle can be represented by a conventional safety device (for example, safety relay) or a safety communication system. The sensors and actuators are connected at the interfaces outside the safety communication system.

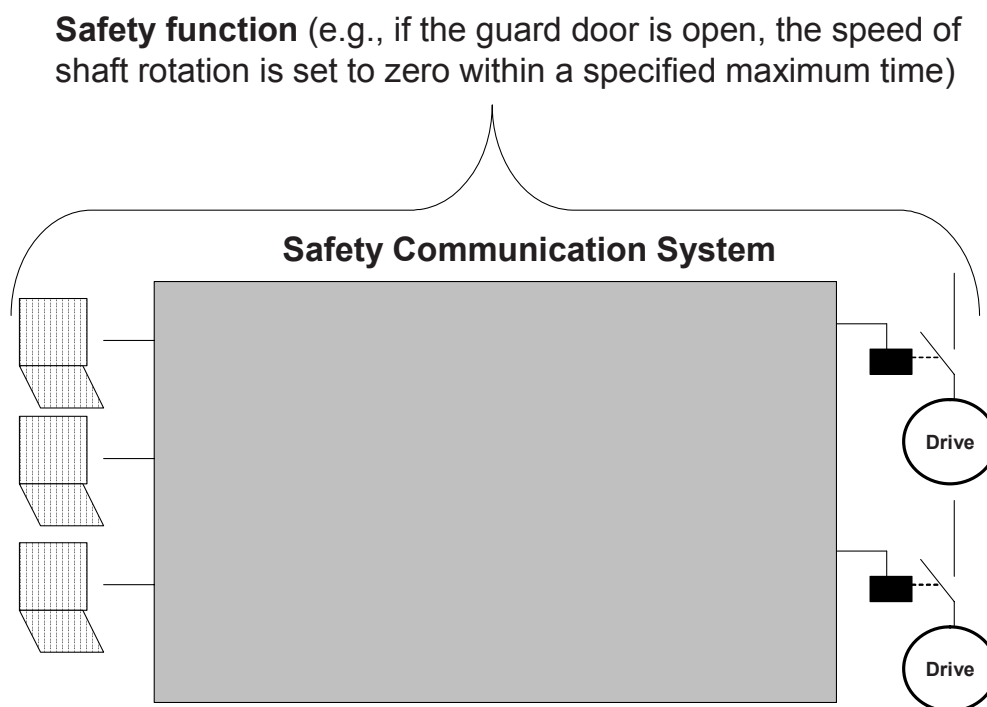


Figure 4 – Example of a safety function

5.4.3 Decomposition of the safety function of a safety communication system into function blocks

5.4.3.1 Overview of the safety function decomposition process

The safety function performed by the safety communication system can be decomposed into the following function blocks (Figure 5):

- Input Safe Data
- Safe Transmission (based on IEC 61158 Type 8 protocol)
- Safe Calculation
- Output Safe Data.

NOTE Implementation of a function block usually requires a detailed safety requirement specification. Also a safety requirements specification for the subsystems performing the function blocks is needed. These specifications are outside of the scope of this part.

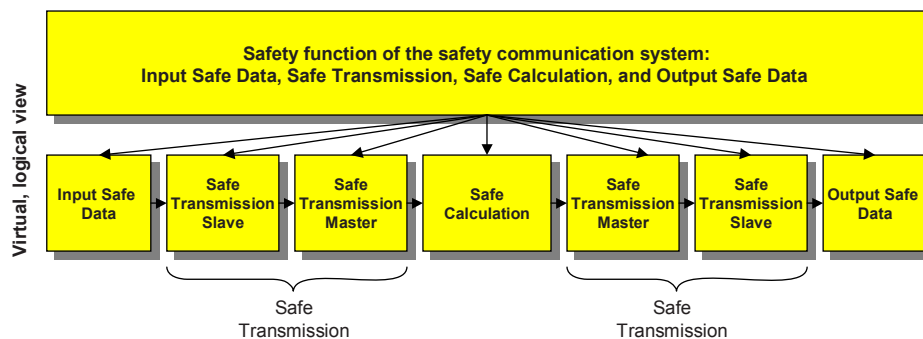


Figure 5 – Decomposition of safety function into function blocks

5.4.3.2 Input Safe Data function block

The Input Safe Data function block reads the physical input signals from different sensors that can be connected to the input terminal block of a safety slave. It prepares the data for transmission via the Safe Transmission function block.

This function block is application-specific and outside the scope of this part.

5.4.3.3 Safe Transmission function blocks

5.4.3.3.1 Overview of Safe Transmission

Two Safe Transmission function blocks ensure the safe transmission of safety data from a source to a sink (for example, transmitter to receiver):

- Safe Transmission Master function block
- Safe Transmission Slave function block

NOTE According to IEC 62061, a function block is performed by a single subsystem (for example, device) only. Each function block is assigned to a subsystem within the architecture of the safety function. Several function blocks may be assigned to a single subsystem. A function block is only performed by a single subsystem.

5.4.3.3.2 Safe Transmission Slave function block

The Safe Transmission Slave function block performs the slave-specific services of an input or output device within the safety communication system and the additional safety profile of this part.