BS EN 61784-3-6:2010

BSI Standards Publication

Industrial communication networks — Profiles

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

raising standards worldwide™

National foreword

This British Standard is the UK implementation of EN 61784-3-6:2010. It is identical to IEC 61784-3-6:2010. It supersedes BS EN 61784-3-6:2008 which is withdrawn.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 72030 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 61784-3-6

August 2010

ICS 25.040.40; 35.100.05

Supersedes EN 61784-3-6:2008

English version

Industrial communication networks - Profiles - Part 3-6: Functional safety fieldbuses - Additional specifications for CPF 6
(IEC 61784-3-6:2010)

Réseaux de communication industriels -
Partie 3-6: Bus de terrain à sécurité
fonctionnelle -
Spécifications complémentaires
pour le CPF 6
(CEI 61784-3-6:2010)

Industrielle Kommunikationsnetze -
Profile -
Teil 3-6: Funktional sichere Übertragung
bei Feldbussen -
Zusätzliche Festlegungen
für die Kommunikationsprofilfamilie 6
(IEC 61784-3-6:2010)

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 61784-3-6, 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 2010-07-01.

This European Standard supersedes EN 61784-3-6:2008.

The main changes with respect to EN 61784-3-6:2008 are listed below:

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

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 61784-3-6:2010 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:

EN 50170		
IEC 61131-2	NOTE	Harmonized as EN 61131-2.
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 61508-1:2010	NOTE	Harmonized as EN 61508-1:2010 (not modified).
IEC 61508-4:2010	NOTE	Harmonized as EN 61508-4:2010 (not 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 61784-5 series	NOTE	Harmonized in EN 61784-5 series (not modified).
IEC 61800-5-2	NOTE	Harmonized as EN 61800-5-2.
ISO 10218-1	NOTE	Harmonized as EN ISO 10218-1.
ISO 13849-2	NOTE	Harmonized as EN ISO 13849-2.

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 60204-1	-	Safety of machinery - Electrical equipment of machines - Part 1: General requirements	EN 60204-1	-
IEC 61131-3	-	Programmable controllers - Part 3: Programming languages	EN 61131-3	-
IEC 61158	Series	Industrial communication networks - Fieldbus specifications	EN 61158	Series
IEC 61158-2	-	Industrial communication networks - Fieldbus specifications - Part 2: Physical layer specification and service definition	EN 61158-2	-
IEC 61158-3-8	-	Industrial communication networks - Fieldbus specifications - Part 3-8: Data-link layer service definition - Type 8 elements	EN 61158-3-8	-
IEC 61158-4-8	-	Industrial communication networks - Fieldbus specifications - Part 4-8: Data-link layer protocol specification - Type 8 elements	EN 61158-4-8	-
IEC 61158-5-8	2007	Industrial communication networks - Fieldbus specifications - Part 5-8: Application layer service definition - Type 8 elements	EN 61158-5-8	2008
IEC 61158-6-8	-	Industrial communication networks - Fieldbus specifications - Part 6-8: Application layer protocol specification - Type 8 elements	EN 61158-6-8	-
IEC 61508	Series	Functional safety of electrical/electronic/programmable electronic safety-related systems	EN 61508	Series
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 61784-2	-	Industrial communication networks - Profiles - Part 2: Additional fieldbus profiles for real-time networks based on ISO/IEC 8802-3	EN 61784-2	-

Publication	Year	Title	EN/HD	Year
IEC 61784-3	2010	Industrial communication networks - Profiles - Part 3: Functional safety fieldbuses - General rules and profile definitions	EN 61784-3	2010
IEC 61784-5-6	-	Industrial communication networks - Profiles - Part 5-6: Installation of fieldbuses - Installation profiles for CPF 6	EN 61784-5-6	-
IEC 61918	-	Industrial communication networks - Installation of communication networks in industrial premises	EN 61918	-
IEC 62061	-	Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems	EN 62061	-
ISO 12100-1	-	Safety of machinery - Basic concepts, general principles for design - Part 1: Basic terminology, methodology	EN ISO 12100-1	-
ISO 13849-1	-	Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design	EN ISO 13849-1	-

This page deliberately left blank

CONTENTS

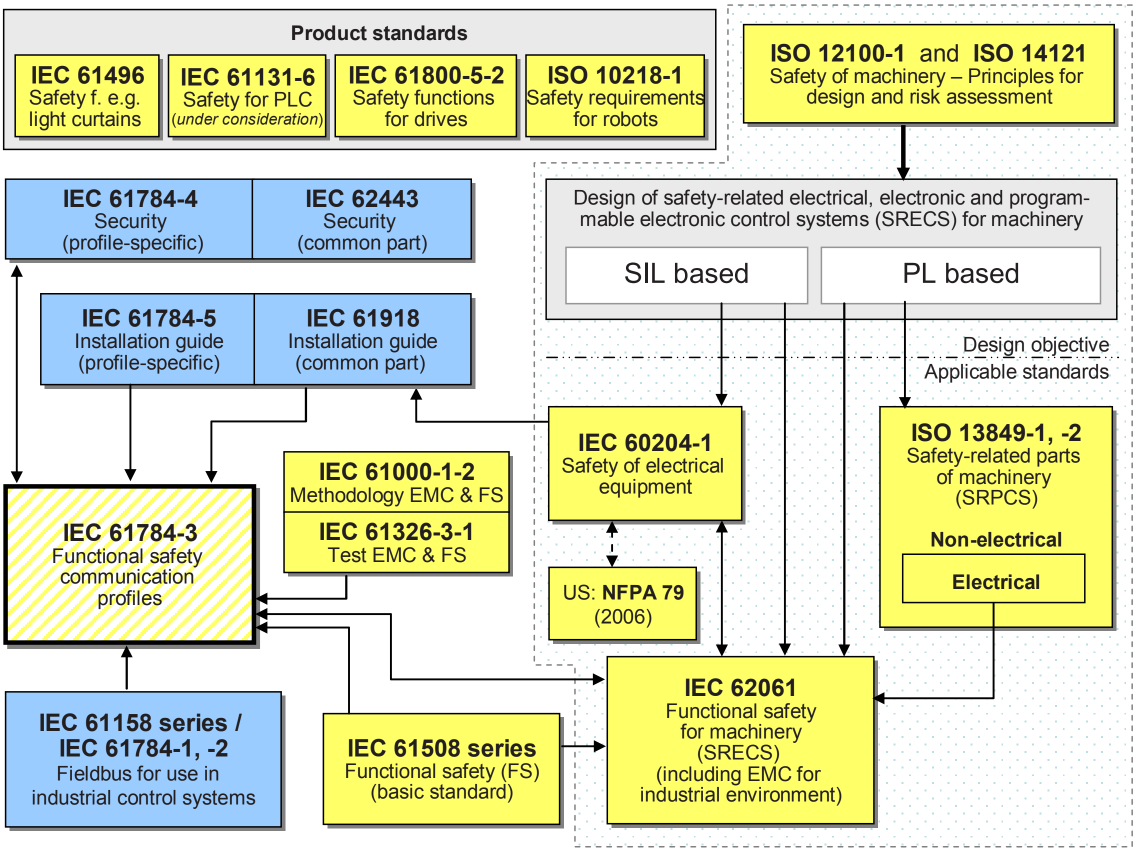
0 Introduction

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.



Key

🟨 (yellow) safety-related standards

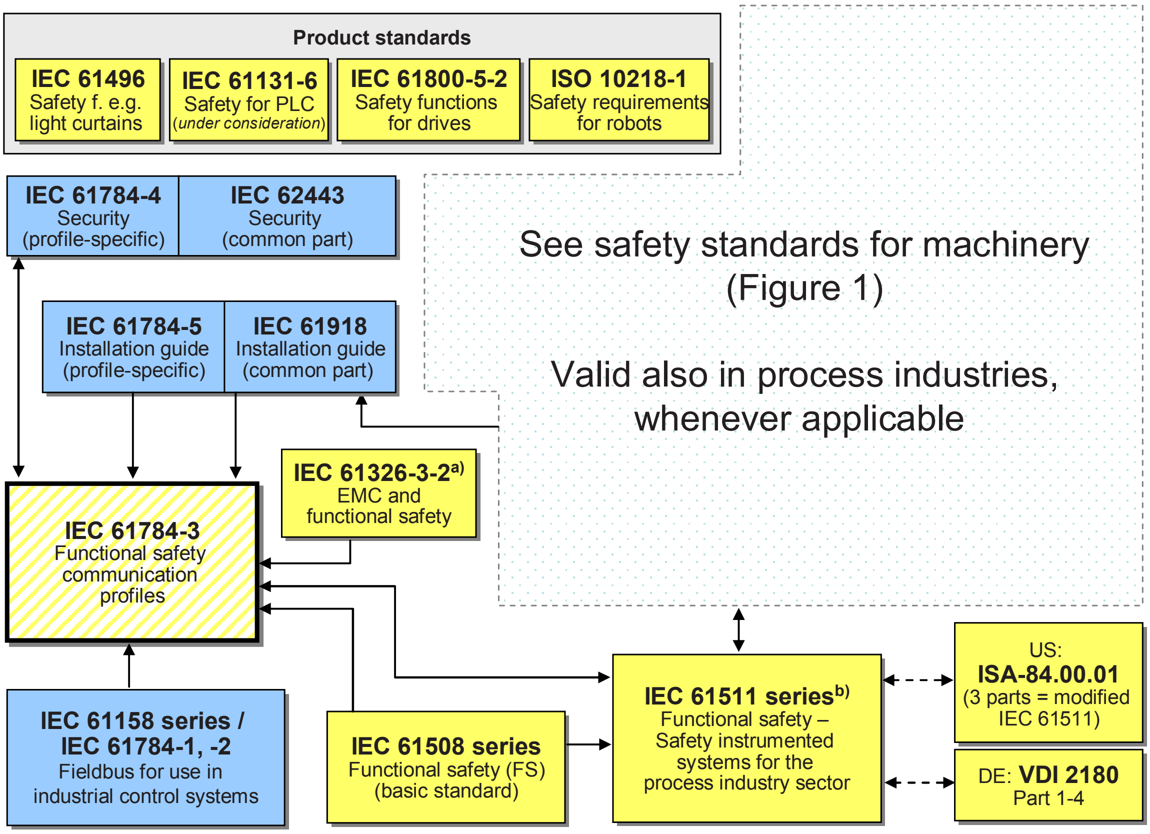
🟦 (blue) fieldbus-related standards

▨ (dashed yellow) this standard

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

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

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


Product standards
IEC 61496
Safety f. e.g. light curtains
IEC 61131-6
Safety for PLC
(under consideration)
IEC 61800-5-2
Safety functions for drives
ISO 10218-1
Safety requirements for robots
IEC 61784-4
Security (profile-specific)
IEC 62443
Security (common part)
See safety standards for machinery (Figure 1)
Valid also in process industries, whenever applicable
IEC 61784-5
Installation guide (profile-specific)
IEC 61918
Installation guide (common part)
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 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

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:

[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 shall not be held responsible for identifying any or all such patent rights.

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 part[1] defines mechanisms for the transmission of safety-relevant messages among participants within a distributed network using fieldbus technology in accordance with the requirements of IEC 61508 series[2] for functional safety. These mechanisms may be used in various industrial applications such as process control, manufacturing automation and machinery.

This part provides guidelines for both developers and assessors of compliant devices and systems.

NOTE 2 The resulting SIL claim of a system depends on the implementation of the selected functional safety communication profile within this system – implementation of a functional safety communication profile according to this part in a standard device is not sufficient to qualify it as a safety device.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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

IEC 61131-3, *Programmable controllers – Part 3: Programming languages*

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

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

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

IEC 61158-4-8, *Industrial communication networks – Fieldbus specifications – Part 4-8: Data-link layer protocol specification – Type 8 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 61158-5-8:2007, *Industrial communication networks – Fieldbus specifications – Part 5-8: Application layer service definition – Type 8 elements*

IEC 61158-6-8, *Industrial communication networks – Fieldbus specifications – Part 6-8: Application layer protocol specification – Type 8 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 61784-2, *Industrial communication networks – Profiles – Part 2: Additional fieldbus profiles for real-time networks based on ISO/IEC 8802-3*

IEC 61784-3:2010[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*

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

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

3 Terms, definitions, symbols, abbreviated terms and conventions

3.1 Terms and definitions

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

3.1.1 Common terms and definitions

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

3.1.1.2
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] In preparation.

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][4].

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

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

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

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

3.1.1.6
failure
termination of the ability of a functional unit to perform a required function or operation of a functional unit in any way other than as required

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

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

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

3.1.1.7
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 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]

3.1.1.8
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

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

[5] To be published.

3.1.1.10
frame
denigrated synonym for DLPDU

3.1.1.11
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 [32], [33].

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

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

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

[IEC/TR 62210, modified]

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

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

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

3.1.1.16
performance level (PL)
discrete level used to specify the ability of safety-related parts of control systems to perform a safety function under foreseeable conditions
[ISO 13849-1]

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

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

[IEC 61131-2]

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

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

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

3.1.1.19
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]

3.1.1.20
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]

3.1.1.21
risk
combination of the probability of occurrence of harm and the severity of that harm

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

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

3.1.1.22
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

3.1.1.23
safety connection
connection that utilizes the safety protocol for communications transactions

3.1.1.24
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.

3.1.1.25
safety device
device designed in accordance with IEC 61508 and which implements the functional safety communication profile

[6] To be published.

3.1.1.26
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]

3.1.1.27
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]

3.1.1.28
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 61784-3:2010[7], 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), corresponding to a range of safety integrity values, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest

NOTE 1 The target failure measures (see IEC 61508-4:2010, 3.5.17) for the four safety integrity levels are specified in Tables 2 and 3 of IEC 61508-1:2010[8].

NOTE 2 Safety integrity levels are used for specifying the safety integrity requirements of the safety functions to be allocated to the E/E/PE safety-related systems.

NOTE 3 A safety integrity level (SIL) is not a property of a system, subsystem, element or component. The correct interpretation of the phrase “SILn safety-related system” (where n is 1, 2, 3 or 4) is that the system is potentially capable of supporting safety functions with a safety integrity level up to n.

[IEC 61508-4:2010]

3.1.1.30
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 61784-3:2010, 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

[7] In preparation.

[8] To be published.

3.1.1.32
safety-related system
system performing *safety functions* according to IEC 61508

3.1.1.33
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]

3.1.1.34
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
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 t1 and t2

NOTE See IEC 61784-3:2010, 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 or 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	
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]
PELV	Protective Extra Low Voltage	
PES	Programmable Electronic System	[IEC 61508-4:2010]
PFH	Average frequency of dangerous failure [h^{-1}] per hour	[IEC 61508-6:2010[9]]
PhL	Physical Layer	[ISO/IEC 7498-1]
PL	Performance Level	[ISO 13849-1]
PLC	Programmable Logic Controller	
SCL	Safety Communication Layer	
SELV	Safety Extra Low Voltage	
SIL	Safety Integrity Level	[IEC 61508-4:2010]
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
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

[9] To be published.

Symbol	Definition	Unit
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
$\Lambda_{SL}(P_e)$	Residual error rate per hour of the safety communication layer with respect to the bit error probability	—
ν	Maximum number of safety messages per hour	—

3.3 Conventions

The conventions for service definitions of IEC 61158-5-8:2007, 3.8.4, are used.

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

4.1 General

Communication Profile Family 6 (commonly known as INTERBUS®[10]) 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™[10]) 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.

[10] 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.

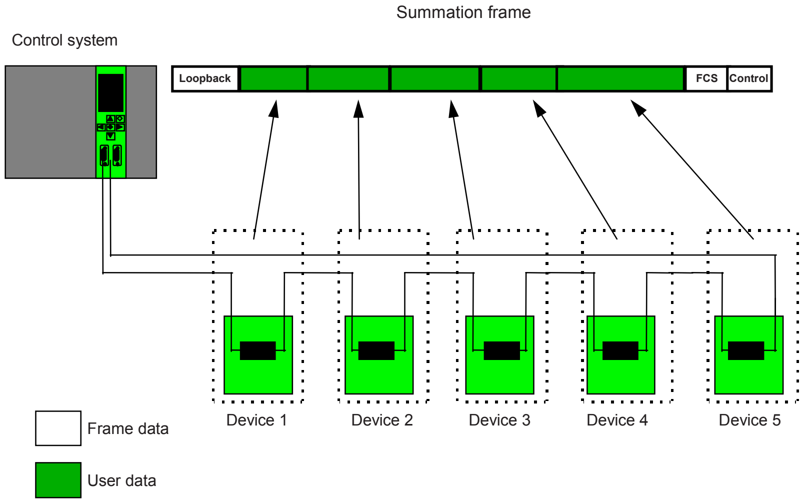


Figure 3 – FSCP 6/7 communication preconditions

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 [44] to [50] 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 elements according to IEC 61508 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 [c]	X [b]					
Insertion	X			X [a]				
Masquerade				X				X
Addressing				X				

NOTE Table adapted from IEC 62280-2 [18] and EN 954-1 [27].

[a] Only for sender identification. Detects only insertion of an invalid source.

[b] Required in all cases.

[c] Time stamp is created locally on SLCS 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 releated 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 ISO 13849-1.

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 12100-1. 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.

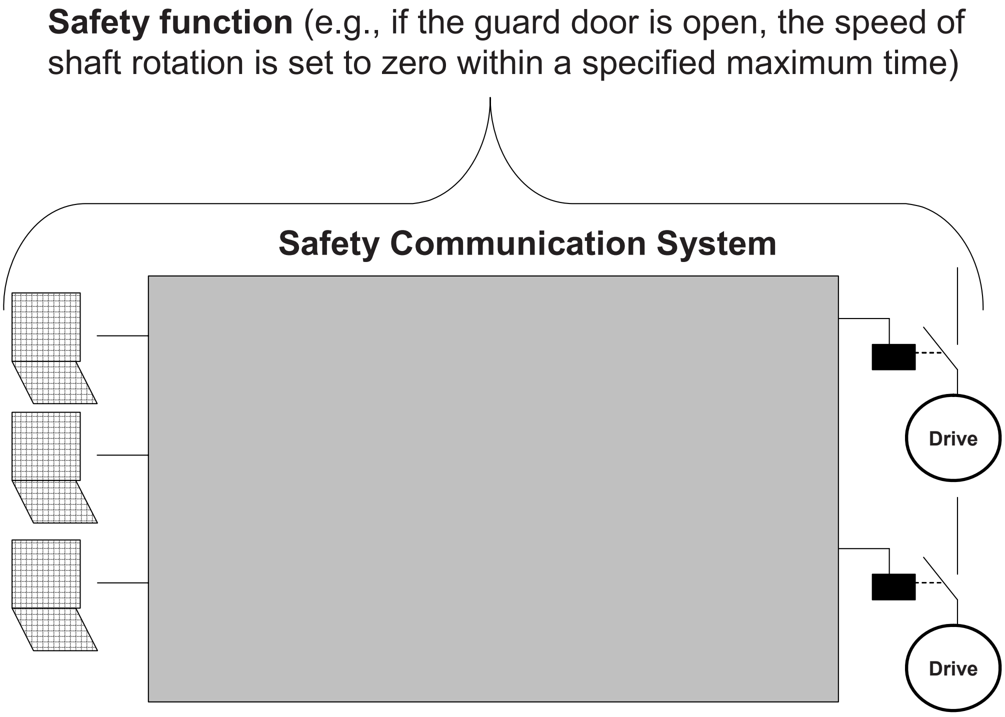

Safety function (e.g., if the guard door is open, the speed of shaft rotation is set to zero within a specified maximum time)
Safety Communication System
Drive
Drive

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.

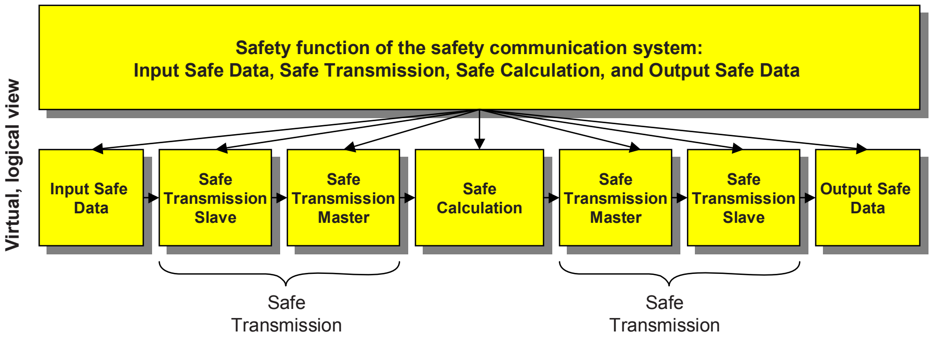


Figure 5 – Decomposition of safety function into function blocks

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.

5.4.3.3.3 Safe Transmission Master function block

The Safe Transmission Master function block performs the master-specific services of a safety control device within the functional safety communication system of this part.

5.4.3.4 Safe Calculation function block

The Safe Calculation function block performs the logic-solving task of the received input signals and generates new safety output data based on safety-related application software. The start of a new bus cycle shall be synchronized with this function block (see also 6.2). The specification of this function block is outside the scope of this part. Where necessary this part specifies requirements for the structure of the Safe Calculation function block.

5.4.3.5 Output Safe Data function block

The Output Safe Data function block reads the received output signals from the Safe Transmission Slave function block, transforms them into the physical output signal, and makes them available at the terminal block of a safety slave.

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

5.4.4 Assignment of the function blocks to subsystems

5.4.4.1 Overview

Table 3 provides an overview of the function blocks and the corresponding subsystems.

Table 3 – List of function blocks and subsystems

Function Block	Subsystem
Input Safe Data	Safety relevant peripheral (SRP)
Safe Transmission Master	Safety communication layer master (SCLM)
Safe Transmission Slave	Safety communication layer slave (SCLS)
Safe Calculation	Safety relevant controller (SRC)
Safe Transmission	Safety Communication Layer (SCL) Safety transmission profile
Output Safe Data	Safety relevant peripheral (SRP)

Figure 6 shows the results of the decomposition process with regard to the safety functions performed by a safety communication system.

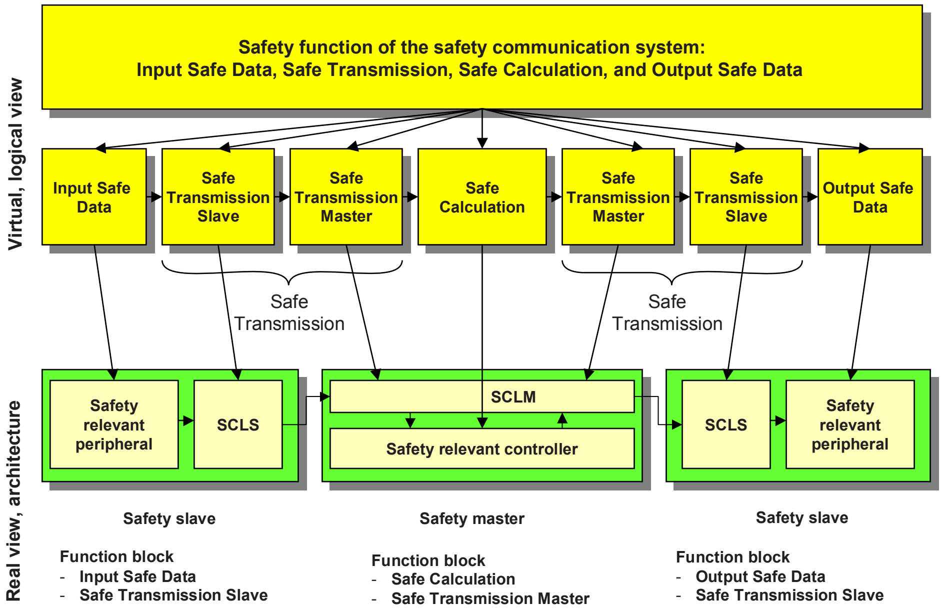


Figure 6 – Overview of the results of the decomposition process

The safety communication system is based on the following two main subsystems (devices):

- Safety slave (input, output, input and output);
- Safety master (with safety relevant controller).

Each of the subsystems (devices) performs one or more function blocks.

5.4.4.2 Description of the interfaces between the defined function blocks

5.4.4.2.1 Description of the signal flow

Figure 7 shows the signal flow between the defined function blocks.

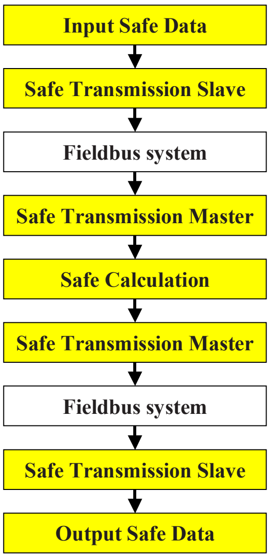


Figure 7 – Signal flow between the function blocks

Table 4 shows the signal flow between the function blocks.

Table 4 – Signal flow between the function blocks

Function block (source)	Function block (sink)	Required action
Input Safe Data	Safe Transmission Slave	The source function block transfers the recorded data at the terminal block of the safety slave performing the function block to the sink function block
Safe Transmission Slave	Safe Transmission Master	The source function block transfers the recorded data from the Input Safe Data function block to the subsequent Safe Transmission Master function block. The IEC 61158 Type 8 protocol is used as the transmission protocol. The Safe Transmission function block adds additional safety measures (deterministic remedial measures) to the transmitted safety data
Safe Transmission Master	Safe Calculation	The source function block extracts the received safety data by removing the additional safety measures (deterministic remedial measures) and transfers the data to the Safe Calculation function block
Safe Calculation	Safe Transmission Master	After processing the safety data, the Safe Calculation function block generates new safety output data and transfers this data to the subsequent Safe Transmission Master function block
Safe Transmission Master	Safe Transmission Slave	The Safe Transmission Master function block extracts all the safety data from the Safe Calculation function block and transfers it to the subsequent Safe Transmission Slave function block. The IEC 61158 Type 8 protocol is used as the transmission protocol. The function block adds additional safety measures (deterministic remedial measures) to the safety data
Safe Transmission Slave	Output Safe Data	The Safe Transmission Slave function block extracts the data from the received messages and transfers the data to the Output Safe Data function block

5.4.4.2.2 Interfaces between the function blocks and devices

Figure 8 shows the interfaces between the function blocks and devices.

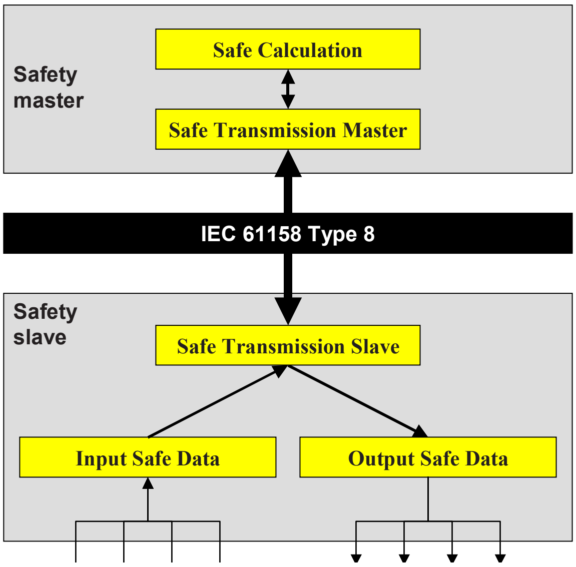


Figure 8 – Interfaces between the safety devices within the safety communication system

The safety relevant controller is parameterized and programmed using limited-variability language programming software (IEC 61131-3 -compatible, Windows-based programming system). All function blocks, subsystems, and devices can be programmed, parameterized, and configured using this software. This software is outside the scope of this part.

When performing a safety function, all the function blocks and all the interfaces between the function blocks are activated.

Where necessary this part specifies requirements for the design of the programming interface.

5.4.5 Safety requirements and safety integrity requirements

The safety requirements and the safety integrity requirements of a safety function are usually derived from a risk reduction process (see ISO 12100-1 and other appropriate standards). This is outside the scope of this part.

The safety communication layer is designed for high-demand mode of operation and up to a SIL CL of 3. Therefore the safety communication system consumes a maximum of 1 % of the overall PFH. Within the safety communication system $\Lambda < 10^{-7}$ is achieved.

NOTE 1 The safety requirements specification including the safety requirements and the safety integrity requirements is outside the scope of this part.

NOTE 2 The specification of this profile is suitable for a SIL CL up to 3. The resulting SIL CL of a subsystem that incorporates the safety communication layer depends on the safety relevant parameters of the actual subsystem. This is outside the scope of this part.

5.4.6 Specification of the safe state

5.4.6.1 General

If a dangerous failure is detected within the IEC 61158 Type 8 system or within the function blocks, the safety function and all related function blocks shall be set to their safe states.

In this context, the safe state is a value that a function block shall transfer to the subsequent function block in the event of a failure. A function block shall have measures to detect failures in the preceding function block. A function block shall have diagnostic measures to detect failures within itself. If a function block on a device has a direct interface to another device it shall have measures to detect failures in the preceding device.

A failure in a subsystem can result in a situation where the function block is not longer able to diagnose its own failure or to transfer the safe state to the subsequent function block. In the case of a function block failure, the function block of the subsequent device shall have measures to diagnose this failure. The function block that detected this failure shall transfer its safe state to the subsequent function block.

Only the value zero (representing the safe state) shall be transmitted to subsequent function blocks. Subsequent function blocks are not able to determine whether the reason for the safe state was the generation of a safe state due to a failure or the result of a request. The function block shall be always set to its safe state.

The system user should be informed by the diagnostics whether a request was detected or a failure. These diagnostics should be generated by the relevant function block or the following function block.

The section below provides information about the signal flow and all possible failures.

Figure 9 shows the signal flow and the safe states of the relevant function blocks.

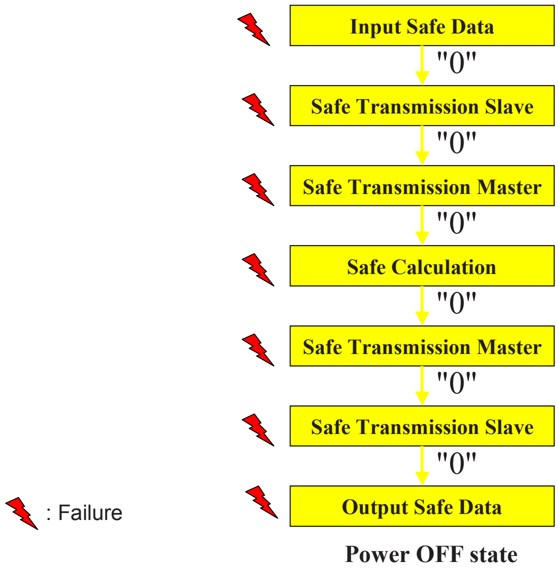


Figure 9 – Signal flow and safe states

5.4.6.2 Safe state of the Input Safe Data function block

The safe state of the function block is the transfer of the value zero for all sensor values.

5.4.6.3 Safe state of the Safe Transmission function block

The safe state of this function block depends on the error type. The safe state is defined as follows:

- Transfer of the value zero to the following function block
- No activation of the watchdog that represents the parameterized shutdown time

These measures apply to the Safe Transmission function block. They are incorporated in the Safe Transmission function block as well as the following function blocks:

- Safe Transmission Slave
- Safe Transmission Master

5.4.6.4 Safe state of the Safe Calculation function block

The safe state of the Safe Calculation function block is the transfer of the value zero for all output values.

NOTE The output values are transmitted to all output devices during the next data cycle.

5.4.6.5 Safe state of the Output Safe Data function block

The safe state of the Output Safe Data function block is the transfer of the value zero for all actuator values.

5.4.7 Response to a fault

5.4.7.1 Input Safe Data function block

In the event of a failure in the input interface of the Input Safe Data function block, the Input Safe Data function block transfers the value zero for each faulty input as an input to the subsequent Safe Transmission Slave function block.

The Input Safe Data function block transfers the value zero for all inputs to the Safe Transmission Slave function block in the event of a failure that the Input Safe Data function block has diagnosed itself.

5.4.7.2 Safe Transmission Slave function block

If this function block detects a failure in the preceding Input Safe Data function block, it transfers the value zero for all inputs to the Safe Transmission Master function block.

If this function block detects a failure in the preceding Safe Transmission Master function block, it transfers the value zero for all outputs to the subsequent Output Safe Data function block.

If this function block detects a failure within the messages being received from the preceding Safe Transmission Master function block, which indicate that the preceding function block has detected a failure, it transfers the value zero for all outputs to the subsequent Output Safe Data function block.

If this function block detects a failure in the IEC 61158 Type 8 system, it transfers the value zero for all outputs to the subsequent Output Safe Data function block.

If this function block detects a failure in the preceding device (safety relevant controller), it transfers the value zero for all outputs to the subsequent Output Safe Data function block.

5.4.7.3 Safe Transmission Master function block

If this function block detects a failure in the preceding Safe Transmission Slave function block, it transfers the value zero for all inputs of the relevant Safe Transmission Slave function block to the subsequent Safe Calculation function block.

If this function block detects a failure within the messages being received from the preceding Safe Transmission Slave function block, which indicate that the preceding function block has detected a failure, it transfers the value zero for all outputs of the related Safe Transmission Slave function block to the subsequent Safe Calculation function block.

If this function block detects a failure in the preceding Safe Calculation function block, it transfers the value zero for all outputs to the subsequent Safe Transmission Slave function block.

If this function block detects a failure in the IEC 61158 Type 8 system, it transfers the value zero for all inputs of the related device to the subsequent Safe Calculation function block.

If this function block detects a failure in the preceding safety input slave, it transfers the value zero for all related inputs of this slave to the subsequent Safe Calculation function block.

5.4.7.4 Safe Calculation function block

If this function block detects a failure in the preceding Safe Transmission Master function block, it sets the safety relevant controller to its safe state.

5.4.7.5 Output Safe Data function block

If this function block detects a failure in the preceding Safe Transmission Slave function block, it sets all outputs to the power OFF state.

If this function block detects a failure at one or more outputs on the device performing this function block, it sets the faulty outputs to their power OFF state.

5.4.8 Stop category

The specification of the safety communication layer in this part supports stop category 0 according to IEC 60204-1. In the event of a failure, the functional safety communication profile sets all or only the related outputs to zero. The output interfaces of the safety slaves are set to their power OFF state.

Stop category 1 or 2 can be implemented e. g. within an adequate application software and the safety slaves. For this, corresponding requirements shall be specified in the safety requirement specification of the devices. This is outside the scope of this part.

5.4.9 Safe Transmission

Deterministic remedial measures are based on the IEC 61158 Type 8 protocol and are implemented on the safety master as the safety communication layer master (SCLM) and on the safety slaves as the safety communication layer slave (SCLS) (Figure 10).

The safety communication layer master (SCLM) and the safety communication layer slave (SCLS) are specified within the safety communication layer specification.

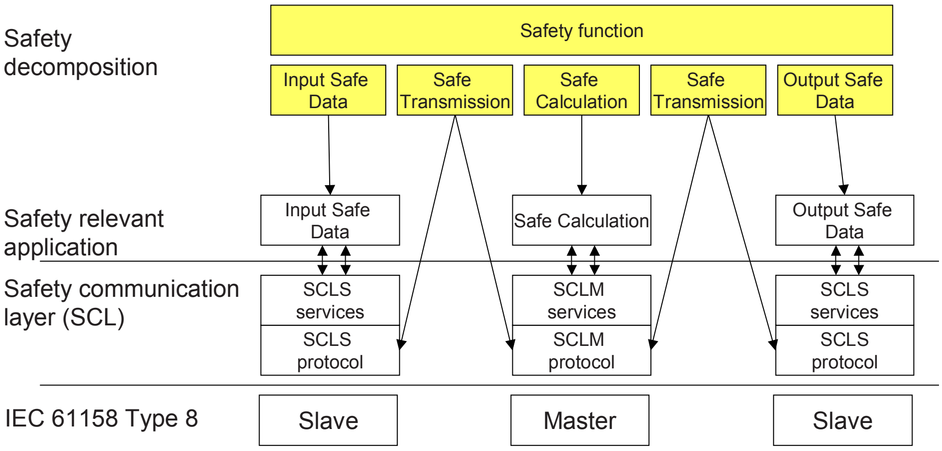


Figure 10 – Mapping of the Safe Transmission function block

5.5 Relationships with FAL (and DLL, PhL)

5.5.1 Overview

Subclause 5.5 describes how the SCL uses the FAL. Figure 11 shows the relationship between the SCL and the other layers of the IEC 61158 Type 8 communication stack.

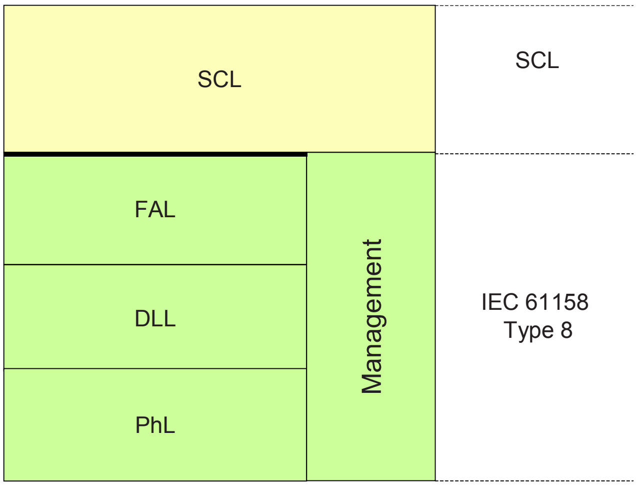


Figure 11 – Relationship between SCL and the other layers of IEC 61158 Type 8

The SCL defined in this part uses the AR-Unconfirmed Send service (AR-US) of IEC 61158-5-8 to transfer the SPDUs between the SCL entities.

In order to transmit the safety messages, the Start IEC 61158 Type 8 service shall be used by the SCLM according to the sequence charts in Clause 7. The sequence charts in Clause 7 show which safety messages are transmitted.

NOTE The SCL can be accessed either by the SRP (SCL: SCLS) or SRC (SCL: SCLM). The way to do this is implementation specific. It can be done for example according to Model D (Annex A of IEC 61784-3:2010).

5.5.2 Use of the AR-US service to initiate and parameterize

Figure 12 shows the use of the AR-Unconfirmed Send service with the following SCL services:

- Initiate;
- Send Application Parameter;
- Send Application Parameter ID;
- Parameterize Device.

These services have several AR-US request and AR-US indication service primitives. The exact sequences are shown in Clause 7.

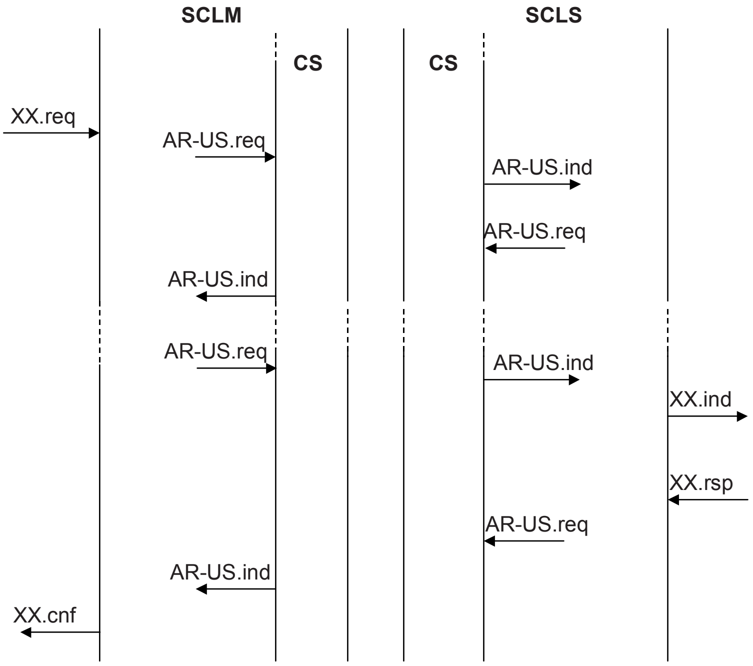


Figure 12 – Use of the AR-US service to initiate and parameterize

Figure 13 specifies the use of the AR-US service by the Transmit-Safety-Data service (TDS).

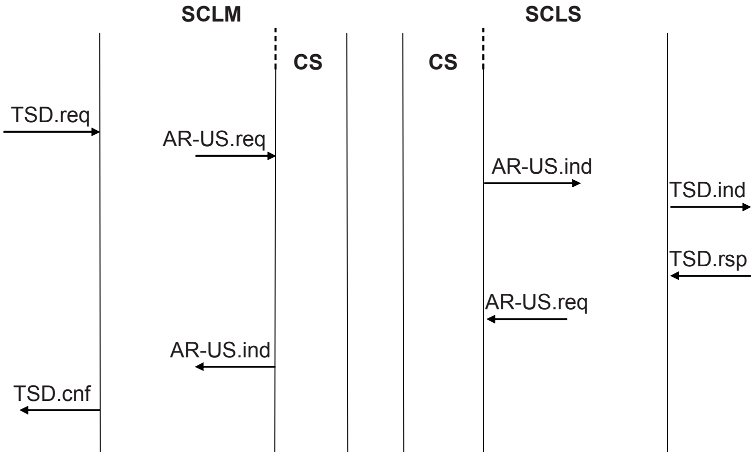


Figure 13 – Use of the AR-US service to transmit safety data

5.5.3 Use of the AR-US service to transmit safety data

Figure 14 specifies how the safety communication layer uses the AR-US service to abort.

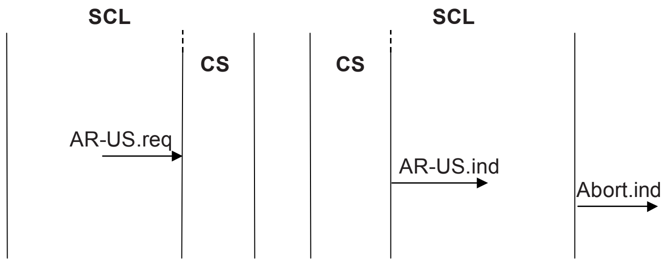


Figure 14 – Use of the AR-US service to abort

5.5.4 Use of the AR-US service to abort

Figure 15 specifies the use of the AR-US service by the Abort service.

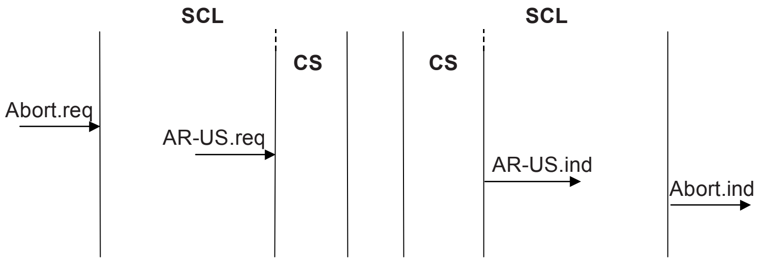


Figure 15 – Use of the AR-US service to abort

5.5.5 Data types

Data types of safety data are specified in IEC 61158-5-8:2007, Clause 5.

NOTE Only data types with the bit length lower than the safety data field can be applied. Actual used data types are device specific.

6 Safety communication layer services

6.1 General

Safety-related applications uses the following services to communicate via the safety communication layer:

- Initiate;
- Abort;
- Send Application Parameter;
- Send Application Parameter ID;
- Parameterize Device;
- Transmit-Safety-Data;
- Set-Diagnostic-Data;
- Set-Acknowledgement-Data.

6.2 Transmission principle for safety messages between SCLM and SCLS

The SCLM makes the safety messages for the individual SRPs of the connected slaves calculated by the SRC available to the IEC 61158 Type 8 master for transmission. The SRC then requests the IEC 61158 Type 8 master to start a data cycle.

The master assigns the data to be transmitted to the connected safety slaves and standard slaves, and starts a new data cycle. The data is then transmitted to the slaves, which at the same time return their own data to the master.

Once the data cycle has elapsed, the slaves transmit the received data to their application layers (Latch-OUT). At the same time, the master provides the SRC with the data received from the slaves in this data cycle and indicates the end of the data cycle. New data is then transferred to the communication equipment of the slaves for transmission in the next data cycle (Latch-IN). The safety slaves enter the calculated data from the previous data cycle in the communication equipment.

When the Latch-OUT signal is received, the SCLS receives the information that new data is available. The SCLS interprets the received message as a safety message and processes it. The SCLS has thus received safety messages.

After indicating the end of the data cycle, the SCLM reads the received messages. It interprets them as safety messages. The SCLM has thus received safety messages. However, the messages originate from a time earlier than the time the Latch-IN signal was detected.

Once the SCLS has received the safety messages from the SCLM, it creates a new safety message and makes it available for subsequent transmission. The new messages are not entered in the communication equipment of the safety slaves until the next data cycle. Thus the SCLM only receives the response to its sent safety message in the next but one data cycle.

6.3 Function block requirements

6.3.1 Input Safe Data function block

After receiving a Transmit-Safety-Data.ind (see 6.6.1), the current safety relevant physical input information shall be read. This data shall be sent with the Transmit-Safety-Data.res (see 6.6.1) via the Safety_In_Data parameter (see 6.6.1). This shall be done before the next Transmit-Safety-Data.ind is received.

Between two Transmit-Safety-Data.ind, each demand of a safety function shall be transmitted with the next Transmit-Safety-Data.res.

6.3.2 Output Safe Data function block

The demand of a safety function received with a Transmit-Safety-Data.ind (see 6.6.1) shall be performed immediately. If a Transmit-Safety-Data.ind (see 6.6.1) is not received within the parameterized shutdown time, the function block shall be placed in its safe state. For this the parameter Safety_In_Data_Time_Stamp in the Transmit-Safety-Data service (6.6.1) shall be used. The parameterized shutdown time can be transmitted with the application parameter record or is set in the function block.

6.3.3 Safe Calculation function block

To enable operation in process data mode, connections shall be initiated with the safety slaves and the application parameters shall be transmitted.

In process data mode, all safety slaves are now addressed cyclically with the Transmit-Safety-Data.req (see 6.6.1) service. The safety output data transmitted shall be calculated based on the safety input data of the previously received Transmit-Safety-Data.con (see 6.6.1).

When a Transmit-Safety-Data.con is received with the Safety_In_Data_Valid parameter = FALSE, the previously received data shall be used for the calculation.

When an Abort.ind (see 6.4.2) with Abort_Info from Table 8 and Table 20 (see 6.4.2) is received, the safe calculation function block shall use the value zero instead of the Safety_In_Data until a Transmit-Safety-Data.con (see 6.6.1) is received with the Safety_In_Data_Valid parameter = TRUE.

When an Abort.ind (see 6.4.2) with Abort_Info from Table 21 or Table 22, the Safe Calculation function block shall be placed in its safe state.

6.4 Context management

6.4.1 Initiate service

The Initiate service initiates the point-to-point connection. The initiate service parameters are specified in Table 5.

Table 5 – Initiate service parameters

Parameter name	Req	Ind	Rsp	Cnf
Argument	M	M		
Physical_Position	M			
Location_ID	M	M		
Parameterization_Mode	M	M		
Result(+)				M
Serial_Number			M	M
Vendor_ID			M	
Device_Type			M	
Device_Revision			M	
User_Data			M	M
SCLS_Revision			M	M

Argument

The argument contains the parameters of the service request.

Physical_Position

This parameter specifies the number of the safety device with which the connection is to be initiated.

Location_ID

This parameter contains the location ID of the device [1 … 126]. It is used to address the slave.

Parameterization_Mode

This parameter contains the parameterization mode. Parameterization shall be performed according to the set mode (1, 2, 3). Table 6 specifies the services that shall be performed according to the set parameterization mode.

Table 6 – Parameterization mode and related services

Parameterization mode	Service
1	Send Application Parameter
2	Send Application Parameter ID
3	Parameterize Device

Result(+)

This selection type parameter indicates that the service request was successful. It thus confirms that the addressed device has the correct device ID and location ID.

Serial_Number

This parameter contains the unique serial number of the addressed device.

Vendor_ID

This parameter contains the vendor ID of the addressed device.

Device_Type

This parameter contains the device type of the addressed device.

Device_Revision

This parameter contains the device revision of the addressed device.

User_Data

This parameter contains the application data (2 octets) read back by the addressed device.

SCLS_Revision

This parameter contains the SCLS revision.

6.4.2 Abort service

The Abort service aborts a point-to-point connection. The abort service parameters are specified in Table 7.

Table 7 – Abort service parameters

Parameter name	Req	Ind
Argument	M	M(=)
Location_ID	M	M(=)
Abort_Info	M	M
Additional_Info	M	M

Argument

The argument contains the parameters of the service request.

Location_ID

This parameter contains the location ID of the addressed device [1 … 126]. It is used to address the device.

Abort_Info

In the event of an abort, this parameter contains:

- The reason for calling the service (see Table 8), or
- The reason for aborting (Table 8, Table 20, Table 21, and Table 22)

Additional_Info

If specific values appear in Abort_Info, this parameter contains additional information.

Table 8 – Abort of a point-to-point connection by the SRP or SRC

Abort_Info	Called By	Meaning
SRP_Detected_Error_Para	SRP	The parameter record is not consistent.
SRP_Detected_Error_Para_ID	SRP	The parameter record ID is invalid.
SRP_Detected_Error_Loc_ID_Not_Saved	SRP	The location ID could not be stored permanently.
Abort_Connection	SRC	Initiated abort of a point-to-point connection.

6.5 Function block parameterization

6.5.1 Send application parameter service

This service transmits the application parameter record of safety devices. The send application parameter service parameters are specified in Table 9.

Table 9 – Send application parameter service

Parameter name	Req	Ind	Rsp	Cnf
Argument	M	M(=)		
Location_ID	M		M(=)	
Application_Parameter_Record	M	M		
Result(+)			M	M
Location_ID_Changed			M	M

Argument

The argument contains the parameters of the service request.

Location_ID

This parameter contains the location ID of the addressed device [1 … 126]. It is used to address the device.

Application_Parameter_Record

This parameter contains the application parameter and its number.

Result(+)

This selection type parameter indicates that the service request was successful.

Location_ID_Changed

This parameter contains the value TRUE or FALSE. If TRUE, the location ID was different and the new ID was accepted. If FALSE, the location ID was correct.

6.5.2 Send application parameter ID service

This service transmits the application parameter record ID. If the existing application parameter record currently stored on the device has the same application parameter record ID, this application parameter record is used. The send application parameter ID service parameters are specified in Table 10.

Table 10 – Send application parameter ID service

Parameter name	Req	Ind	Rsp	Cnf
Argument	M	M(=)		
Location_ID	M		M(=)	
Application_Parameter_Record_ID	M	M		
Result(+)			M	M
Location_ID_Changed			M	M

Argument

The argument contains the parameters of the service request.

Location_ID

This parameter contains the location ID of the addressed device [1 … 126]. It is used to address the device.

Application_Parameter_Record_ID

This parameter contains the ID of a parameter record.

Result(+)

This selection type parameter indicates that the service request was successful.

Location_ID_Changed

This parameter contains the value TRUE or FALSE. If TRUE, the location ID was different and the new ID was accepted. If FALSE, the location ID was correct.

6.5.3 Parameterize device service

This service activates the parameter record of the SRP for the safety devices with the application parameter record ID if it has the same application parameter record ID as the received application parameter record ID.

This service transmits both the application parameter and the application parameter record ID. The parameterize device service parameters are specified in Table 11.

Table 11 – Parameterize device parameters

Parameter name	Req	Ind	Rsp	Cnf
Argument	M	M(=)		
Location_ID	M		M(=)	
Application_Parameter_Record	M	M		
Application_Parameter_Record_ID	M	M		
Result(+)			M	M
Location_ID_Changed			M	M

Argument

The argument contains the parameters of the service request.

Location_ID

This parameter contains the location ID of the addressed device [1 … 126]. It is used to address the device.

Application_Parameter_Record

This parameter contains the application parameter and its number.

Application_Parameter_Record_ID

This parameter contains the ID of a parameter record.

Result(+)

This selection type parameter indicates that the service request was successful.

Location_ID_Changed

This parameter contains the value TRUE or FALSE. If TRUE, the location ID was different and the new ID was accepted. If FALSE, the location ID was correct.

6.6 Safe Process Data Mode

6.6.1 Transmit-Safety-Data

The Safe Transmission function block uses this service to transmit safety output data from the SRC to the SRP and from the SRP to the SRC. The Output Safe Data function block uses both time stamps to determine the age of the safety input data used to calculate the safety output data. The Transmit-Safety-Data service parameters are specified in Table 12.

Table 12 – Transmit-Safety-Data service parameters

Parameter name	Req	Ind	Res	Cnf
Argument	M	M(=)		
Location_ID	M			
Safety_Out_Data	O	O		
Safety_Out_Data_Valid		M		
Safety_In_Data_Time_Stamp		C		
Safety_In_Data_ACK		M		
Result			S	S
Location_ID				M(=)
Safety_In_Data			O	O
Safety_In_Data_Valid				C
Actual_Time_Stamp			C	

Argument

The argument contains the parameters of the service request.

Location_ID

This parameter contains the location ID of the addressed device [1 … 126]. It is used to address the device.

Safety_Out_Data

This parameter contains the safety output data.

Safety_Out_Data_Valid

This parameter specifies whether the data in the Safety_Out_Data parameter is valid and may be used.

Safety_In_Data_Time_Stamp

The Output Safe Data function block uses this parameter to read out the time at which the safety input data used to calculate this safety output data was read in from its own SCLS. If the time stamp = 0, only the zeros in Safety_Out_Data may be forwarded to the outputs.

Safety_In_Data_ACK

This parameter contains a copy of Safety_In_Data. Those bits within the Safety_In_Data which are “1” will be copied to Safety_In_Data_ACK immediately, those who are “0” will be copied to Safety_In_Data_ACK when the SRC has received them. The SCLS can be sure that these bits have been received if the sequence number has been changed 3 steps correctly.

Result

This selection type parameter indicates that the service request was successful.

Safety_In_Data

This parameter contains the safety input data.

Safety_In_Data_Valid

This parameter specifies whether the data in the Safety_In_Data parameter is valid and may be used.

Actual_Time_Stamp

This parameter contains the time at which the request was sent.

The Output Safe Data function block uses this parameter to transmit the time of the request call to its own SCLS.

6.6.2 Set-Diagnostic-Data service

The Set-Diagnostic-Data service transmits the SCLS diagnostic data to the SCLM. The Set-Diagnostic-Data service parameters are shown in Table 13.

Table 13 – Set-Diagnostic-Data service parameters

Parameter name	Req	Ind
Argument	M	M(=)
Location_ID		M
Diagnostic_Data	M	M(=)

Argument

The argument contains the parameters of the service request.

Location_ID

This parameter contains the location ID of the addressed device [1 … 126]. It is used to address the device.

Diagnostic_Data

This parameter contains the diagnostic data of a safety device with the specified location ID.

6.6.3 Set-Acknowledgement-Data service

The Set-Acknowledgement-Data service is used to transmit the SCLM acknowledgement data to the SCLS. The Set-Acknowledgement-Data service parameters are specified in Table 14.

Table 14 – Set-Acknowledgement-Data service parameters

Parameter name	Req	Ind
Argument	M	M(=)
Location_ID	M	
Acknowledgement_Data	M	M(=)

Argument

The argument contains the parameters of the service request.

Location_ID

This parameter contains the location ID of the addressed device [1 … 126]. It is used to address the device.

Acknowledgement_Data

This parameter contains the acknowledgements for the diagnostic data of the safety device with the specified location ID.

7 Safety communication layer protocol

7.1 Safety PDU format

7.1.1 Structure of safety messages

The structure of the safety PDU comprising the deterministic remedial measures and the safety data is specified in Figure 16.

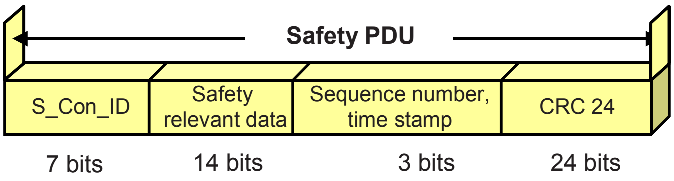


Figure 16 – Structure of the safety PDU

The safety message consists of 24 information bits (14 bits of safety data + 7-bit safety connection ID + 3-bit sequence number) and a 24-bit checksum.

The safety PDU (SPDU) for each safety slave is integrated in the IEC 61158 Type 8 PhPDU, as shown in Figure 17.

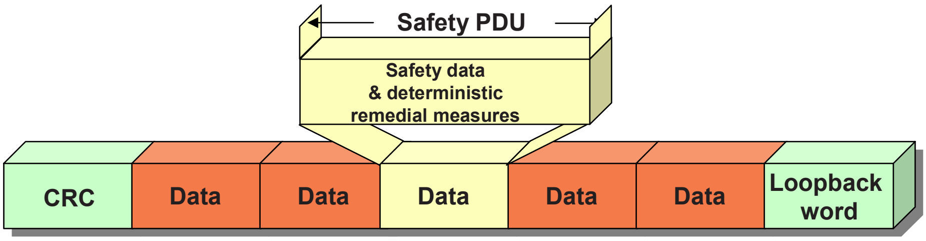


Figure 17 – Integration of safety data and deterministic remedial measures in the summation frame

7.1.2 Description of the polynomial used

Equation (1) specifies the polynomial used to calculate the CRC.

$$G(X) = X24 + X23 + X18 + X17 + X12 + X11 + X10 + X8 + X6 + X4 + X2 + 1 \qquad (1)$$

The description of the properties of the selected code is outside the scope of this part.

7.1.3 Structure of safety messages for safe parameterization and idle

7.1.3.1 General

The transmission of all parameters is safety relevant. Therefore, equally high requirements should be placed on the parameter messages as on the messages for transmitting safety data.

The following messages are used in the parameterization phase:

- Write_Parameter_Byte_Req
- Read_Parameter_Byte_Req
- Parameter_Byte_Con
- Set_Safety_Connection_ID_Req
- Set_Safety_Connection_ID_Con
- Parameter_Idle_Req
- Parameter_Idle_Con
- Parameter_Check_Con
- Parameter_Loc_ID_Changed_Con

7.1.3.2 Description of the Messages

7.1.3.2.1 Write_Parameter_Byte_Req

If the SCLM wants to send a parameter octet to an SCLS, the **Write_Parameter_Byte_Req** message is used (Figure 18):

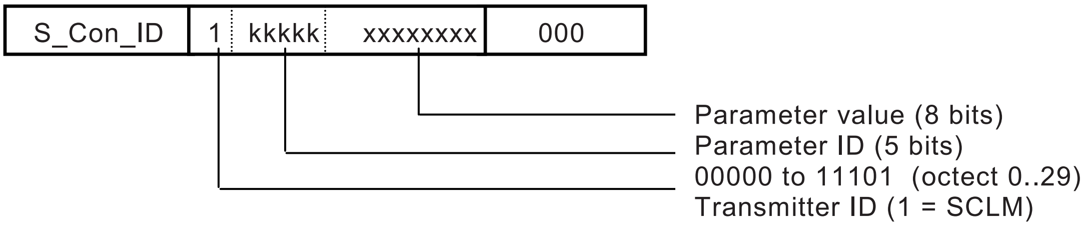


Figure 18 – Write_Parameter_Byte_Req message

7.1.3.2.2 Read_Parameter_Byte_Req

If the SCLM wants to read a parameter octet from an SCLS, the **Read_Parameter_Byte_Req** message is used (Figure 19):

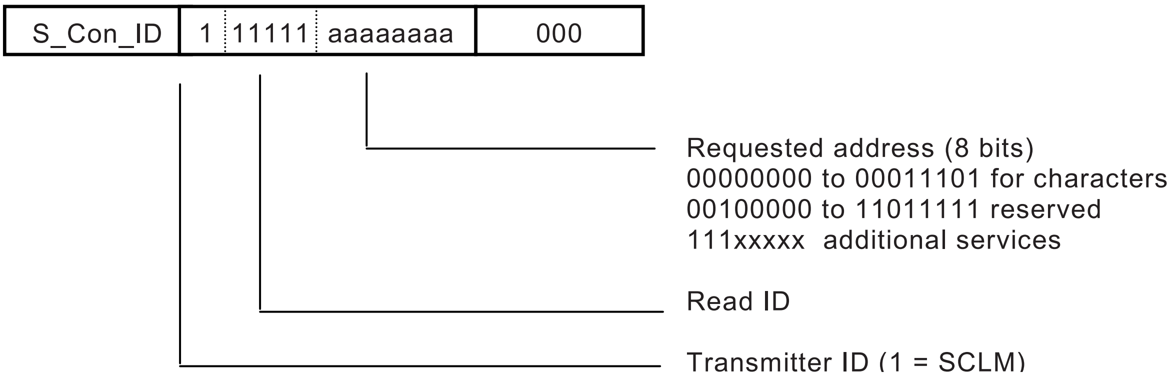

S_Con_ID
1
11111
aaaaaaaa
000
Requested address (8 bits)
00000000 to 00011101 for characters
00100000 to 11011111 reserved
111xxxxx additional services
Read ID
Transmitter ID (1 = SCLM)

Figure 19 – Read_Parameter_Byte_Req message

7.1.3.2.3 Parameter_Byte_Con

The SCLS responds in both cases with a **Parameter_Byte_Con** message (Figure 20).

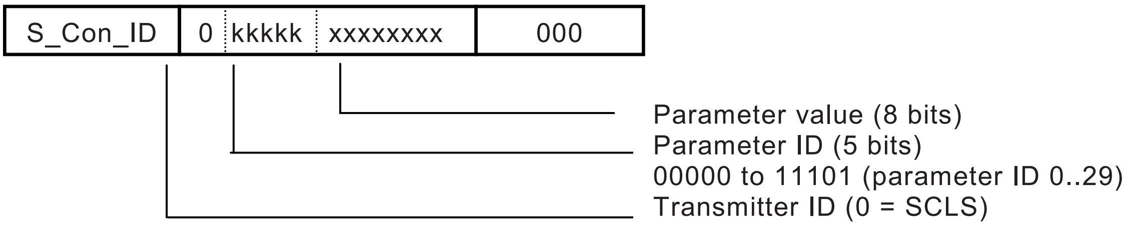


Figure 20 – Parameter_Byte_Con message

7.1.3.2.4 Use of the parameter messages

When an octet with the corresponding Parameter ID is written, a response is always sent by returning the written value.

Table 15 specifies the parameter IDs on the safety devices.

Table 15 – Parameter ID

Parameter ID	Parameter ID	Meaning
00000	0	Reserved for safety connection ID
00001	1	SCLS_Revision
00010	2	Location ID
00011	3	Parameterization mode
00100	4	reserved, shall not be used
00101	5	reserved, shall not be used
00110	6	reserved, shall not be used
00111	7	reserved, shall not be used
01000	8	reserved, shall not be used
01001	9	Block ID (n)
01010	10	Data from block n
:	:	: :
11101	29	Data from block n
11110	30	Reserved
11111	31	Read request and additional messages with special services

Octets with parameter ID 0 to 9 contain parameters that are required for safe communication.

Octets with parameter ID 10 to 29 are referred to as a block and are available 256 times. The block, which can currently be addressed via parameter IDs 01010 (10 dec) to 11101 (29 dec), is specified by the block ID (octet 9). The block ID thus represents an extension of the parameter ID.

Blocks 0 and 1 are reserved for the device ID and the parameter record ID. This is specified Table 16 and Table 17. The Parameter record ID allows a unique identification of the parameter records.

NOTE For information concerning the generation of the Parameter record ID it is highly recommended to contact the INTERBUS-Club.

Octets with parameter IDs which are reserved, shall not be used. The user shall be informed, if the octet field of a parameter ID is nevertheless used, and an error message shall be generated.

Table 16 – Block 0: Device ID

Parameter ID	Meaning
10	Serial number octet 1
11	Serial number octet 2
12	Serial number octet 3
13	Serial number octet 4
14	Serial number octet 5
15	Serial number octet 6
16	Vendor ID octet 1
17	Vendor ID octet 2
18	Vendor ID octet 3

Parameter ID	Meaning
19	Vendor ID octet 4
20	Device type ID octet 1
21	Device type ID octet 2
22	Device type ID octet 3
23	Device type ID octet 4
24	Device type ID octet 5
25	Device type ID octet 6
26	Device type ID octet 7
27	Device revision octet 1
28	Read parameter octet 1 (device-specific)
29	Read parameter octet 2 (device-specific)

Table 17 – Block 1: Parameter record ID

Parameter ID	Meaning
10	Parameter record ID octet 1
11	Parameter record ID octet 2
12	Parameter record ID octet 3
13	Parameter record ID octet 4
14	Parameter record ID octet 5
15	Parameter record ID octet 6
16	Parameter record ID octet 7
17	Parameter record ID octet 8
18	Parameter record ID octet 9
19	Parameter record ID octet 10
20	Parameter record ID octet 11
21	Parameter record ID octet 12
22	reserved, shall not be used
23	reserved, shall not be used
24	reserved, shall not be used
25	reserved, shall not be used
26	reserved, shall not be used
27	reserved, shall not be used
28	reserved, shall not be used
29	reserved, shall not be used

Blocks 2 to 255 can be used freely for the application parameters. For block 2, the first two octets shall contain the number of subsequent parameters (including all additional blocks). This is specified in Table 18.

Table 18 – Block 2: Application parameter

Parameter ID	Meaning
10	Number of subsequent parameter octets (high)
11	Number of subsequent parameter octets (low)
12	Application parameter
13	Application parameter
:	:
:	:
29	Application parameter

Therefore the maximum number of parameters which can be transmitted is:
254 × 20 - 2 = 5 078 octets.

7.1.3.2.5 Set_Safety_Connection_ID_Req message

The SCLM uses the Set_Safety_Connection_ID_Req message (specified in Figure 21) to transmit the safety connection ID to the SCLS of the safety slaves.

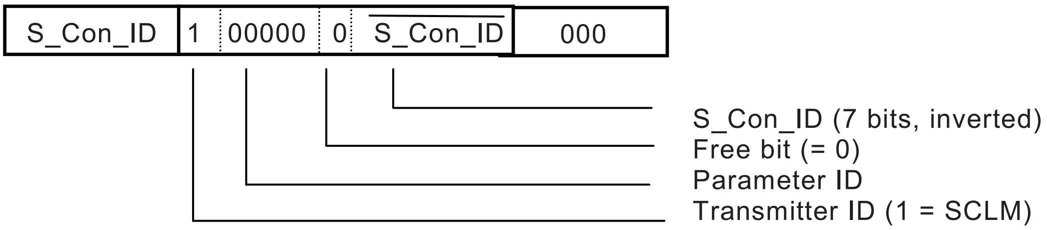


Figure 21 – Set_Safety_Connection_ID_Req message

7.1.3.2.6 Set_Safety_Connection_ID_Con message of safety slaves

The SCLS uses the Set_Safety_Connection_ID_Con message (specified in Figure 22) to transmit his safety connection ID to the SCLM .

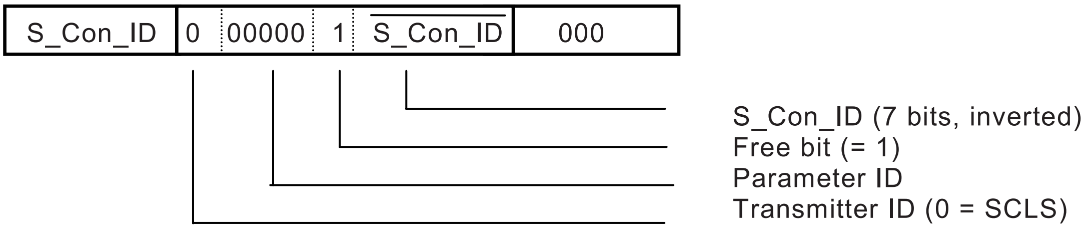


Figure 22 – Set_Safety_Connection_ID_Con message of safety slaves

7.1.3.2.7 Parameter_Idle_Req

Once the last parameter has been transmitted, the SCLM sends Parameter_Idle_Req messages. The SCLS responds with Parameter_Idle_Con and, after checking the parameter, with Parameter_Check_Con and Parameter_Loc_ID_Changed_Con messages. The structure of the messages is specified in Figure 23 to Figure 26.

The 3-bit idle-count is used to make changes to subsequent message encoding.

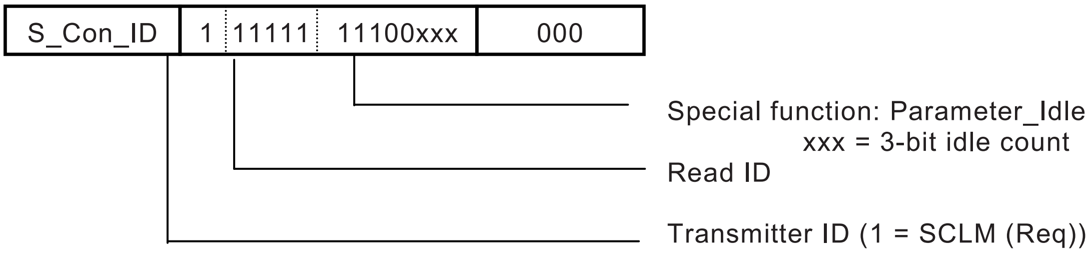

S_Con_ID
1
11111
11100xxx
000
Special function: Parameter_Idle
xxx = 3-bit idle count
Read ID
Transmitter ID (1 = SCLM (Req))

Figure 23 – Parameter_Idle_Req

7.1.3.2.8 Parameter_Idle_Con

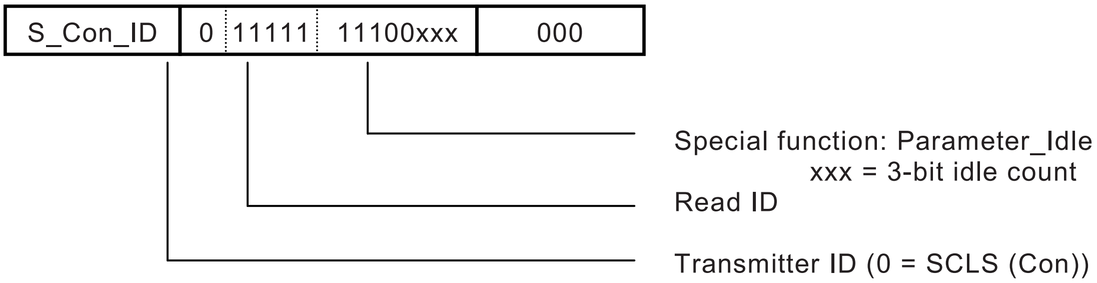

S_Con_ID
0
11111
11100xxx
000
Special function: Parameter_Idle
xxx = 3-bit idle count
Read ID
Transmitter ID (0 = SCLS (Con))

Figure 24 – Parameter_Idle_Con

7.1.3.2.9 Parameter_Check_Con

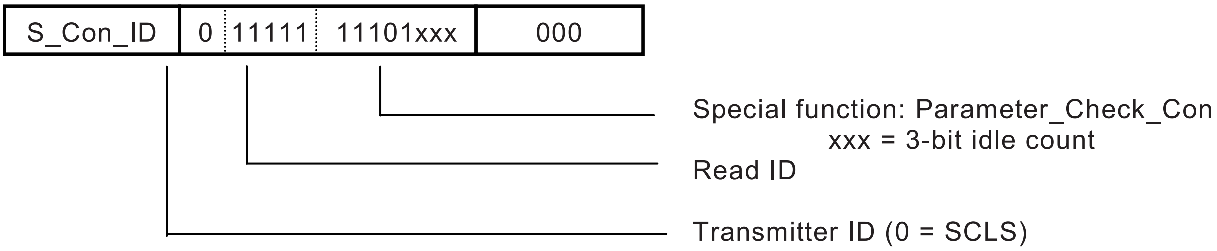

S_Con_ID
0
11111
11101xxx
000
Special function: Parameter_Check_Con
xxx = 3-bit idle count
Read ID
Transmitter ID (0 = SCLS)

Figure 25 – Parameter_Check_Con

7.1.3.2.10 Parameter_Loc_ID_Changed_Con

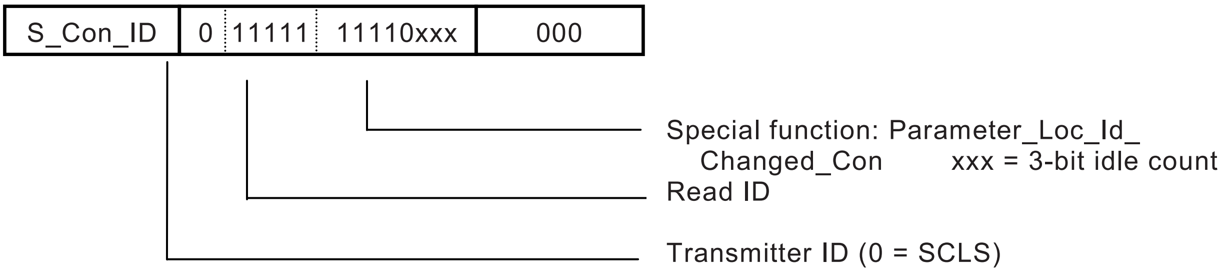


Figure 26 – Parameter_Loc_ID_Changed_Con

7.1.4 Structure of safety messages for the transmission of safety data

Figure 27 specifies the structure of the Transmit Safety Data Message.

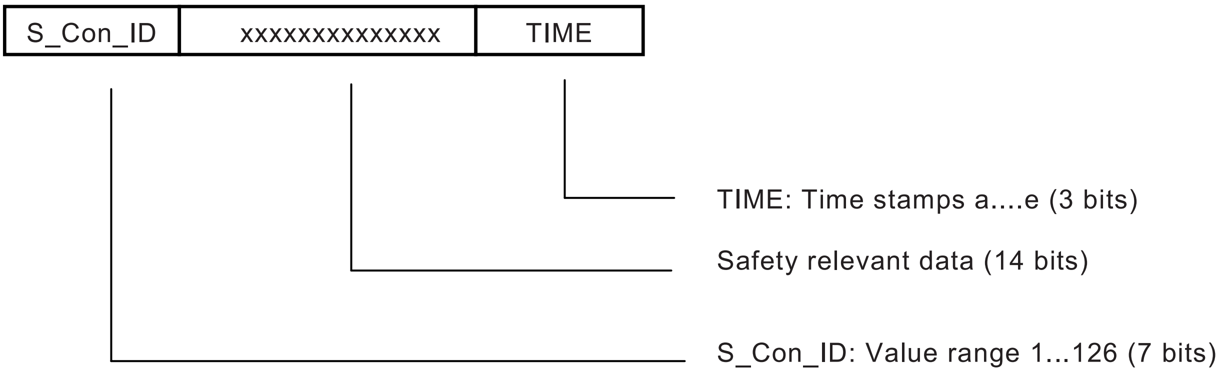

S_Con_ID
xxxxxxxxxxxxxx
TIME
TIME: Time stamps a....e (3 bits)
Safety relevant data (14 bits)
S_Con_ID: Value range 1...126 (7 bits)

Figure 27 – Transmit Safety Data Message

Safety messages contain a sequence number (TIME), which is encoded using a 3-bit value as specified in Table 19.

Table 19 – TIME encoding

Sequence number	Encoding in time	Remarks
-	000	
Sync_a	001	
a	010	Transmission of sequence number a and process data
b	011	Transmission of sequence number b and process data
c	100	Transmission of sequence number c and process data
d	101	Transmission of sequence number d and process data
e	110	Transmission of sequence number e and process data
e	111	Transmission of sequence number e and diagnostic/acknowledgement and unchanged process data

These messages transmit safety data from the SCLS to the SCLM and safety data from the SCLM to the SCLS of the safety slaves. The transmitter/receiver ID is specified by the sequence of values for the TIME.

The sequence number is incremented from a to e. When reaching e the SCLM/SCLS compares the process data to be transmitted with the process data which were sent with sequence number d. If the process data are unchanged the SCLM/SCLS may send Acknowledgement/Diagnostic data instead of process data. This should be done if a Set-Acknowledgement-Data.req / Set-Diagnostic-Data.req is pending.

7.1.5 Messages for synchronization

7.1.5.1 Sync_a message of the SCLM

The SCLM uses Sync_a messages to synchronize the time stamp of all "valid" safety slaves (Figure 28). This message is always sent to all the safety slaves simultaneously. A safety slave is synchronized for the first time following parameterization. By receiving the Sync_a message, it then switches from the "safe parameterization" state to the "safe process data transmission" state.

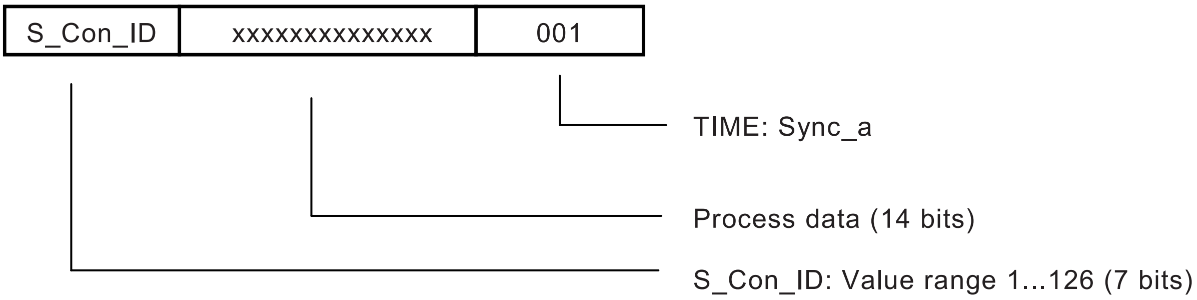


Figure 28 – Sync_a message of the SCLM

7.1.5.2 Req_b message of the SCLM

The Req_b message of the SCLM is specified in Figure 29.

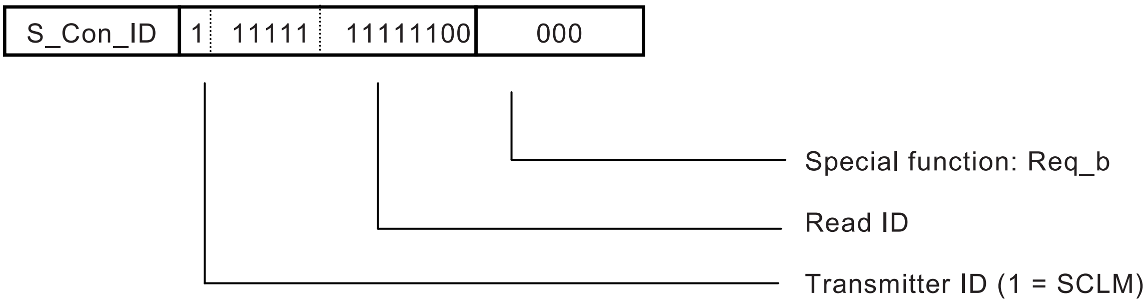


Figure 29 – Req_b message of the SCLM

7.1.5.3 Req_c message of the SCLM

The Req_c message of the SCLM is specified in Figure 30.

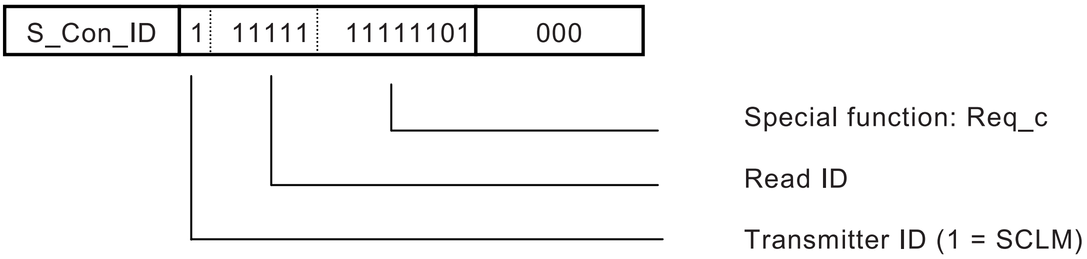


Figure 30 – Req_c message of the SCLM

7.1.5.4 Req_d message of the SCLM

The Req_d message of the SCLM is specified in Figure 31.

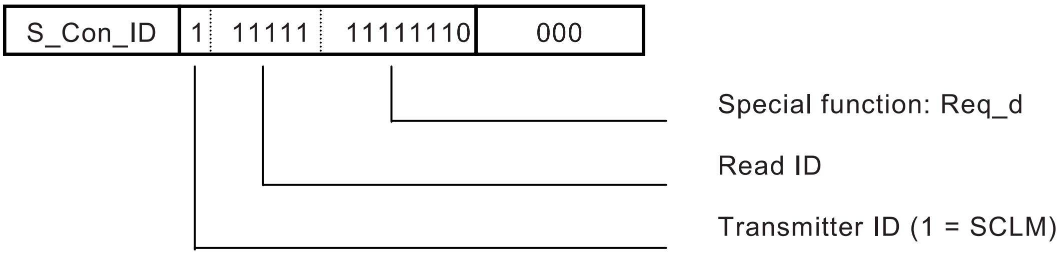


Figure 31 – Req_d message of the SCLM

These safety messages (Figure 28 through Figure 31) are used at the start and during safe process data transmission from the SCLM to synchronize the time stamp (TIME) in the SCLS of the safety slaves. The sequence of the messages is predefined. In the event of errors, the affected SCLS enters the connection aborted state and responds with a Safety_Slave_Error message.

7.1.6 Structure of safety messages for aborting connections

7.1.6.1 Abort_Connection Message of the SCLM

This message (Figure 32) is used to send an Abort.ind to the safety slave. This message transmits the Abort_Info = Abort_Connection.

1111111	1 11111 11111111	000

Figure 32 – Abort_Connection message

7.1.6.2 Safety_Slave_Error Message of safety slaves

The safety slaves send this message (Figure 33) if an error was detected in the parameterization sequence or during operation of the safety slaves, which results in the need for reparameterization. The error type is also transmitted.

This state can only be left if a Set_Safety_Connection_ID message is received from the SCLM.

1111111	0 xxxx xxxx xxxx 1	000

NOTE xxxx xxxx xxxx is the Abort_Info.

Figure 33 – Safety-Slave_Error message

7.2 State description

7.2.1 SCLM and SCLS state machines

Figure 34 specifies the SCLM state machine and Figure 35 specifies the SCLS state machine.

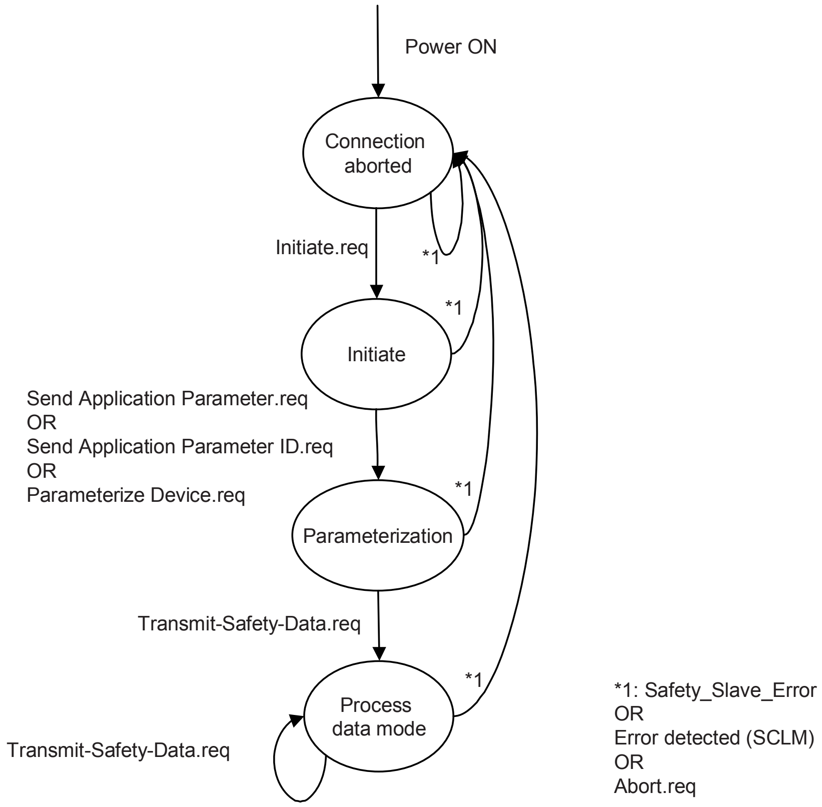


Figure 34 – SCLM state machine

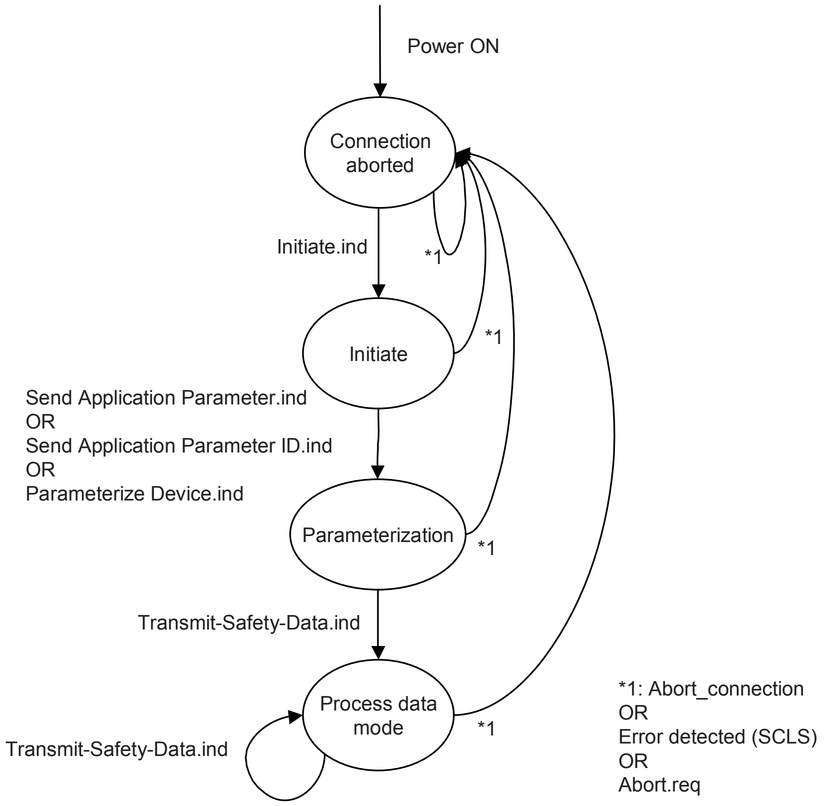


Figure 35 – SCLS state machine

7.2.2 Initiate

Figure 36 specified the service primitive sequence of the initiate service and the transmitted messages.

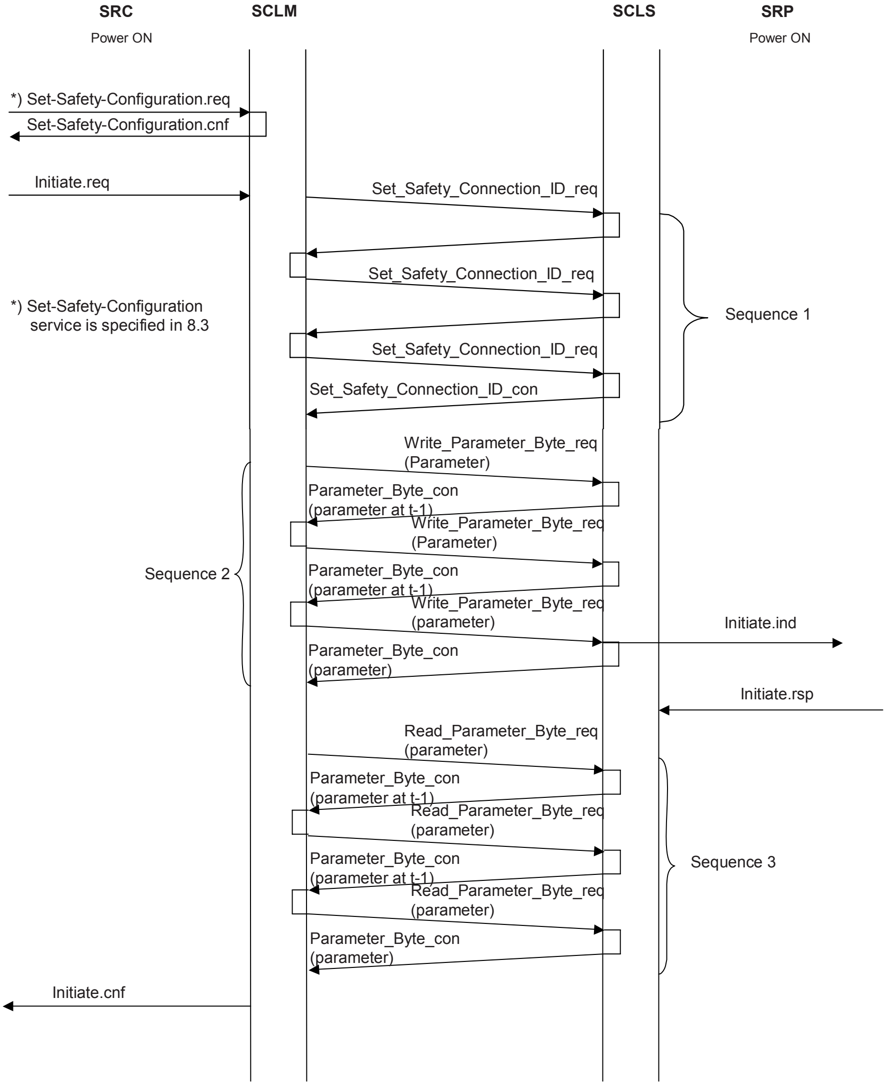

SRC
Power ON
SCLM
SCLS
SRP
Power ON
*) Set-Safety-Configuration.req
Set-Safety-Configuration.cnf
Initiate.req
Set_Safety_Connection_ID_req
Set_Safety_Connection_ID_req
*) Set-Safety-Configuration service is specified in 8.3
Set_Safety_Connection_ID_req
Set_Safety_Connection_ID_con
Sequence 1
Write_Parameter_Byte_req (Parameter)
Parameter_Byte_con (parameter at t-1)
Write_Parameter_Byte_req (Parameter)
Sequence 2
Parameter_Byte_con (parameter at t-1)
Write_Parameter_Byte_req (parameter)
Initiate.ind
Parameter_Byte_con (parameter)
Initiate.rsp
Read_Parameter_Byte_req (parameter)
Parameter_Byte_con (parameter at t-1)
Read_Parameter_Byte_req (parameter)
Parameter_Byte_con (parameter at t-1)
Sequence 3
Read_Parameter_Byte_req (parameter)
Parameter_Byte_con (parameter)
Initiate.cnf

Figure 36 – Initiate sequence

In sequence 1 (Figure 36), the safety connection ID is transmitted to the safety slave.

In sequence 2 (Figure 36), the following parameters are transmitted one after the other:

- Parameterization_Mode
- Block_ID = 0
- Location_ID

The Parameterization_Mode and Location_ID parameters are Initiate.req parameters.

In sequence 3 (Figure 36), the following Initiate.res parameters are read one after the other:

- SCLS_Revision
- Serial_Number (6 octets)
- Vendor_ID (4 octets)
- Device_Type (7 octets)
- Device_Revision (1 octet)
- User_Data (2 octets)

7.2.3 Parameterization

The parameterization phase is initiated with one of the following services:

- Send Application Parameter
- Send Application Parameter ID
- Parameterize Device

Figure 37 specifies the protocol sequence for the Send Application Parameter service.

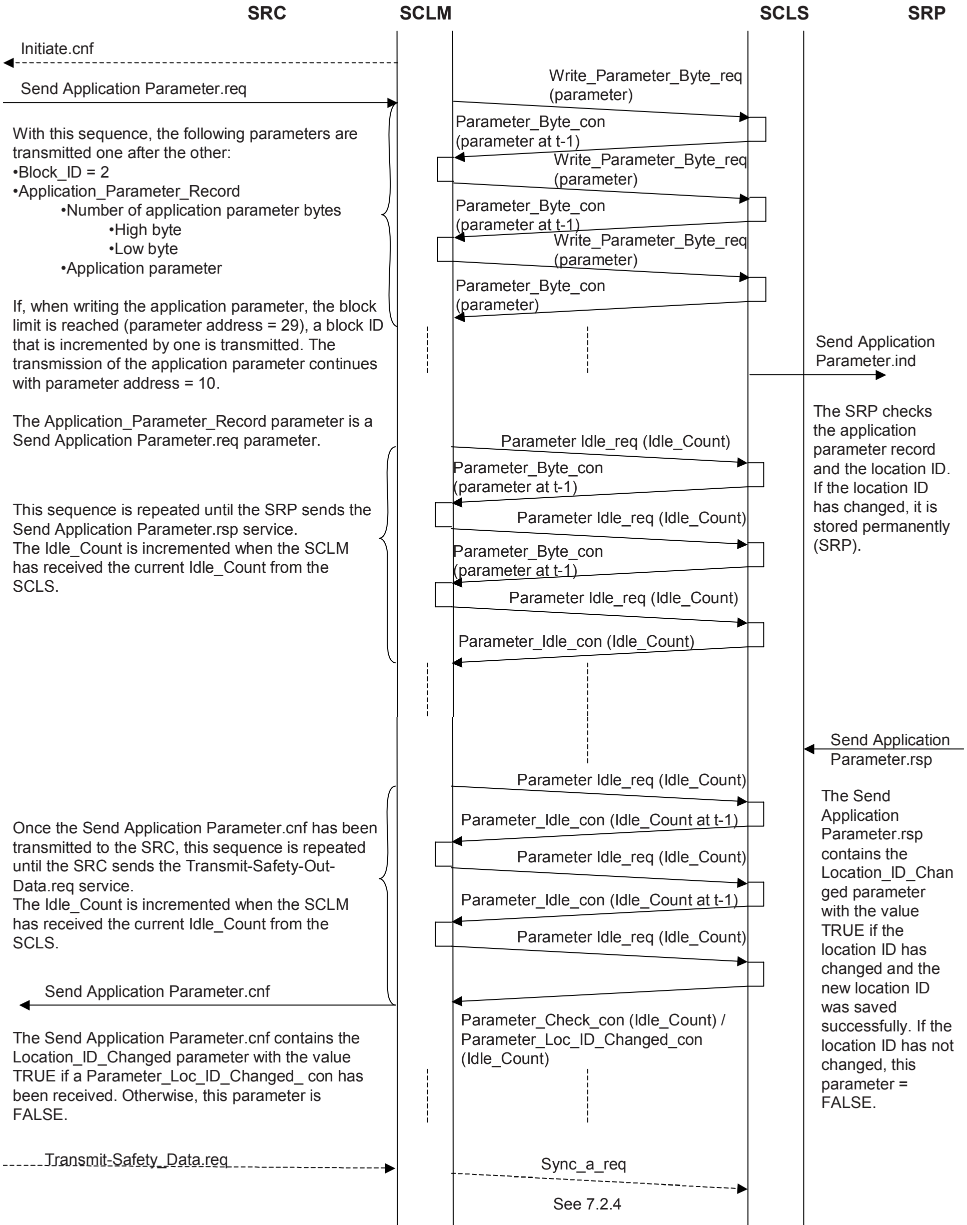
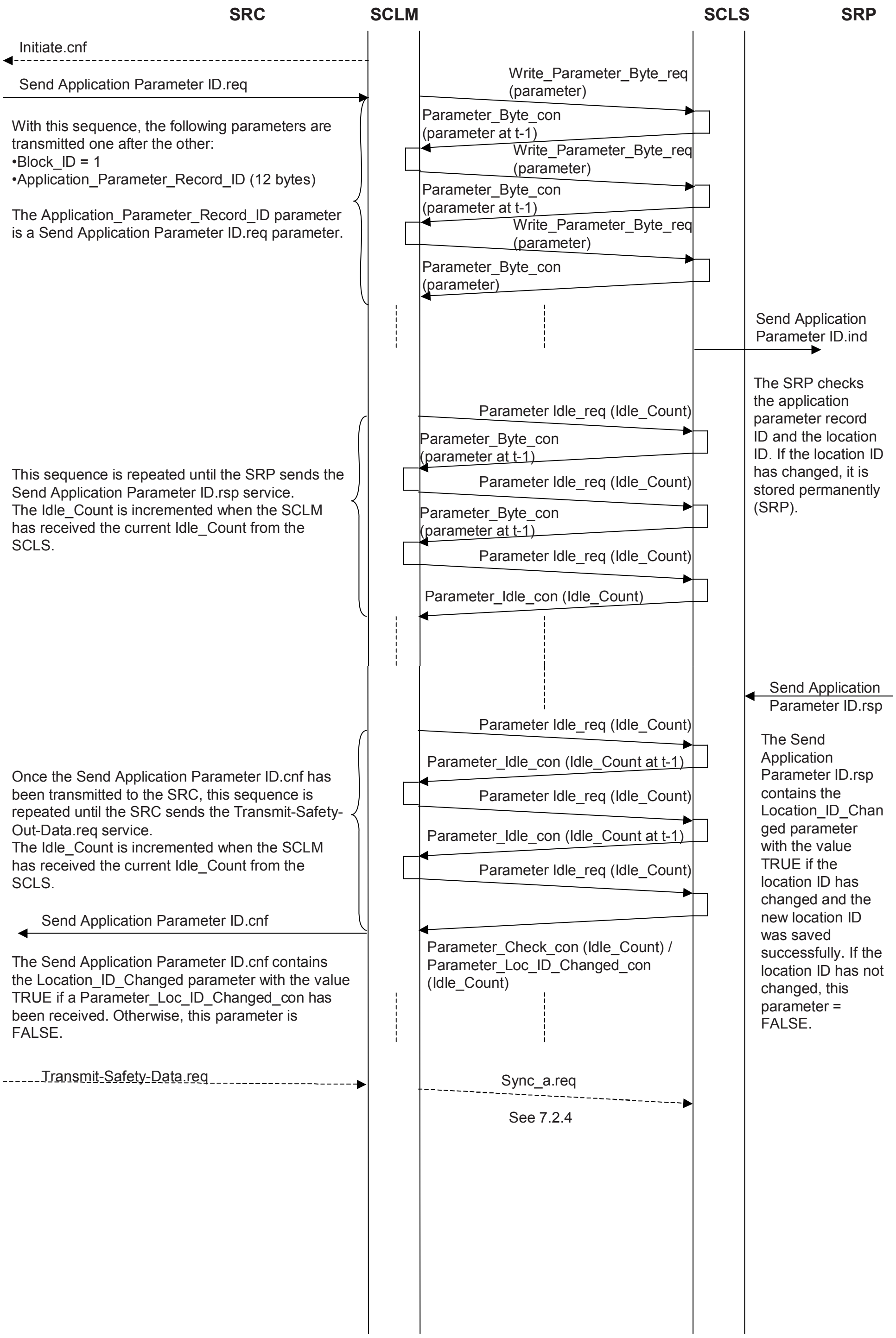

SRC
SCLM
SCLS
SRP
Initiate.cnf
Send Application Parameter.req
Write_Parameter_Byte_req (parameter)
Parameter_Byte_con (parameter at t-1)
Write_Parameter_Byte_req (parameter)
Parameter_Byte_con (parameter at t-1)
Write_Parameter_Byte_req (parameter)
Parameter_Byte_con (parameter)
With this sequence, the following parameters are transmitted one after the other:
•Block_ID = 2
•Application_Parameter_Record
•Number of application parameter bytes
•High byte
•Low byte
•Application parameter
If, when writing the application parameter, the block limit is reached (parameter address = 29), a block ID that is incremented by one is transmitted. The transmission of the application parameter continues with parameter address = 10.
The Application_Parameter_Record parameter is a Send Application Parameter.req parameter.
Send Application Parameter.ind
The SRP checks the application parameter record and the location ID. If the location ID has changed, it is stored permanently (SRP).
Parameter Idle_req (Idle_Count)
Parameter_Byte_con (parameter at t-1)
Parameter Idle_req (Idle_Count)
Parameter_Byte_con (parameter at t-1)
Parameter Idle_req (Idle_Count)
Parameter_Idle_con (Idle_Count)
This sequence is repeated until the SRP sends the Send Application Parameter.rsp service.
The Idle_Count is incremented when the SCLM has received the current Idle_Count from the SCLS.
Send Application Parameter.rsp
The Send Application Parameter.rsp contains the Location_ID_Changed parameter with the value TRUE if the location ID has changed and the new location ID was saved successfully. If the location ID has not changed, this parameter = FALSE.
Parameter Idle_req (Idle_Count)
Parameter_Idle_con (Idle_Count at t-1)
Parameter Idle_req (Idle_Count)
Parameter_Idle_con (Idle_Count at t-1)
Parameter Idle_req (Idle_Count)
Parameter_Check_con (Idle_Count) / Parameter_Loc_ID_Changed_con (Idle_Count)
Once the Send Application Parameter.cnf has been transmitted to the SRC, this sequence is repeated until the SRC sends the Transmit-Safety-Out-Data.req service.
The Idle_Count is incremented when the SCLM has received the current Idle_Count from the SCLS.
Send Application Parameter.cnf
The Send Application Parameter.cnf contains the Location_ID_Changed parameter with the value TRUE if a Parameter_Loc_ID_Changed_ con has been received. Otherwise, this parameter is FALSE.
Transmit-Safety_Data.req
Sync_a_req
See 7.2.4

Figure 37 – Send Application Parameter sequence

Figure 38 specifies the protocol sequence for the Send Application Parameter ID service.


SRC
SCLM
SCLS
SRP
Initiate.cnf
Send Application Parameter ID.req
Write_Parameter_Byte_req (parameter)
Parameter_Byte_con (parameter at t-1)
Write_Parameter_Byte_req (parameter)
Parameter_Byte_con (parameter at t-1)
Write_Parameter_Byte_req (parameter)
Parameter_Byte_con (parameter)
Send Application Parameter ID.ind
Parameter Idle_req (Idle_Count)
Parameter_Byte_con (parameter at t-1)
Parameter Idle_req (Idle_Count)
Parameter_Byte_con (parameter at t-1)
Parameter Idle_req (Idle_Count)
Parameter_Idle_con (Idle_Count)
Send Application Parameter ID.rsp
Parameter Idle_req (Idle_Count)
Parameter_Idle_con (Idle_Count at t-1)
Parameter Idle_req (Idle_Count)
Parameter_Idle_con (Idle_Count at t-1)
Parameter Idle_req (Idle_Count)
Send Application Parameter ID.cnf
Parameter_Check_con (Idle_Count) / Parameter_Loc_ID_Changed_con (Idle_Count)
Transmit-Safety-Data.req
Sync_a.req
See 7.2.4

With this sequence, the following parameters are transmitted one after the other:

- Block_ID = 1
- Application_Parameter_Record_ID (12 bytes)

The Application_Parameter_Record_ID parameter is a Send Application Parameter ID.req parameter.

The SRP checks the application parameter record ID and the location ID. If the location ID has changed, it is stored permanently (SRP).

This sequence is repeated until the SRP sends the Send Application Parameter ID.rsp service. The Idle_Count is incremented when the SCLM has received the current Idle_Count from the SCLS.

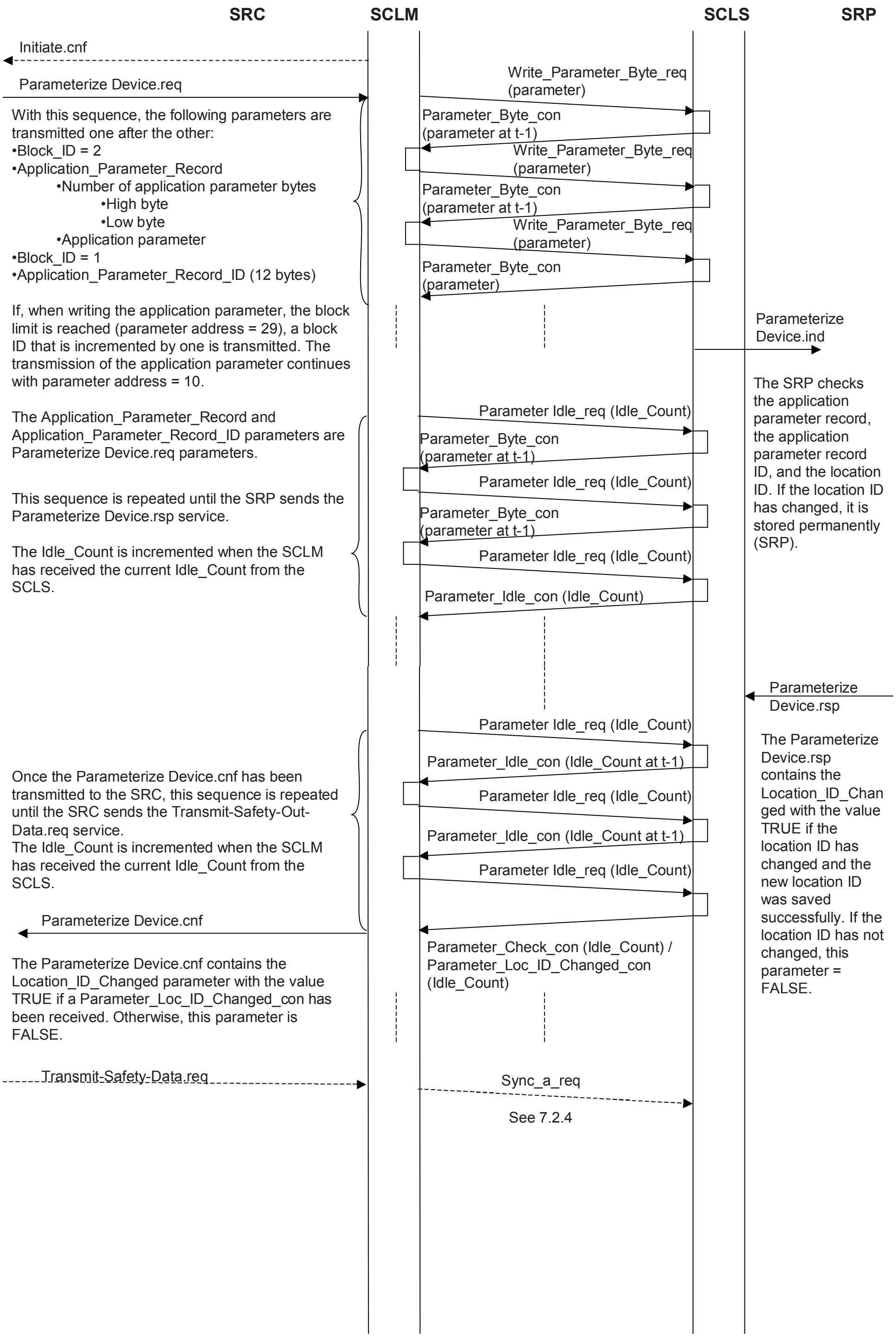
The Send Application Parameter ID.rsp contains the Location_ID_Changed parameter with the value TRUE if the location ID has changed and the new location ID was saved successfully. If the location ID has not changed, this parameter = FALSE.

Once the Send Application Parameter ID.cnf has been transmitted to the SRC, this sequence is repeated until the SRC sends the Transmit-Safety-Out-Data.req service. The Idle_Count is incremented when the SCLM has received the current Idle_Count from the SCLS.

The Send Application Parameter ID.cnf contains the Location_ID_Changed parameter with the value TRUE if a Parameter_Loc_ID_Changed_con has been received. Otherwise, this parameter is FALSE.

Figure 38 – Send Application Parameter ID sequence

Figure 39 specifies the protocol sequence for the Parameterize Device service.


SRC
SCLM
SCLS
SRP
Initiate.cnf
Parameterize Device.req
Write_Parameter_Byte_req (parameter)
Parameter_Byte_con (parameter at t-1)
Write_Parameter_Byte_req (parameter)
Parameter_Byte_con (parameter at t-1)
Write_Parameter_Byte_req (parameter)
Parameter_Byte_con (parameter)
Parameterize Device.ind
Parameter Idle_req (Idle_Count)
Parameter_Byte_con (parameter at t-1)
Parameter Idle_req (Idle_Count)
Parameter_Byte_con (parameter at t-1)
Parameter Idle_req (Idle_Count)
Parameter_Idle_con (Idle_Count)
Parameterize Device.rsp
Parameter Idle_req (Idle_Count)
Parameter_Idle_con (Idle_Count at t-1)
Parameter Idle_req (Idle_Count)
Parameter_Idle_con (Idle_Count at t-1)
Parameter Idle_req (Idle_Count)
Parameterize Device.cnf
Parameter_Check_con (Idle_Count) / Parameter_Loc_ID_Changed_con (Idle_Count)
Transmit-Safety-Data.req
Sync_a_req
See 7.2.4

With this sequence, the following parameters are transmitted one after the other:
- Block_ID = 2
- Application_Parameter_Record
    - Number of application parameter bytes
        - High byte
        - Low byte
    - Application parameter
- Block_ID = 1
- Application_Parameter_Record_ID (12 bytes)

If, when writing the application parameter, the block limit is reached (parameter address = 29), a block ID that is incremented by one is transmitted. The transmission of the application parameter continues with parameter address = 10.

The Application_Parameter_Record and Application_Parameter_Record_ID parameters are Parameterize Device.req parameters.

This sequence is repeated until the SRP sends the Parameterize Device.rsp service.

The Idle_Count is incremented when the SCLM has received the current Idle_Count from the SCLS.

The SRP checks the application parameter record, the application parameter record ID, and the location ID. If the location ID has changed, it is stored permanently (SRP).

Once the Parameterize Device.cnf has been transmitted to the SRC, this sequence is repeated until the SRC sends the Transmit-Safety-Out-Data.req service.
The Idle_Count is incremented when the SCLM has received the current Idle_Count from the SCLS.

The Parameterize Device.rsp contains the Location_ID_Changed with the value TRUE if the location ID has changed and the new location ID was saved successfully. If the location ID has not changed, this parameter = FALSE.

The Parameterize Device.cnf contains the Location_ID_Changed parameter with the value TRUE if a Parameter_Loc_ID_Changed_con has been received. Otherwise, this parameter is FALSE.

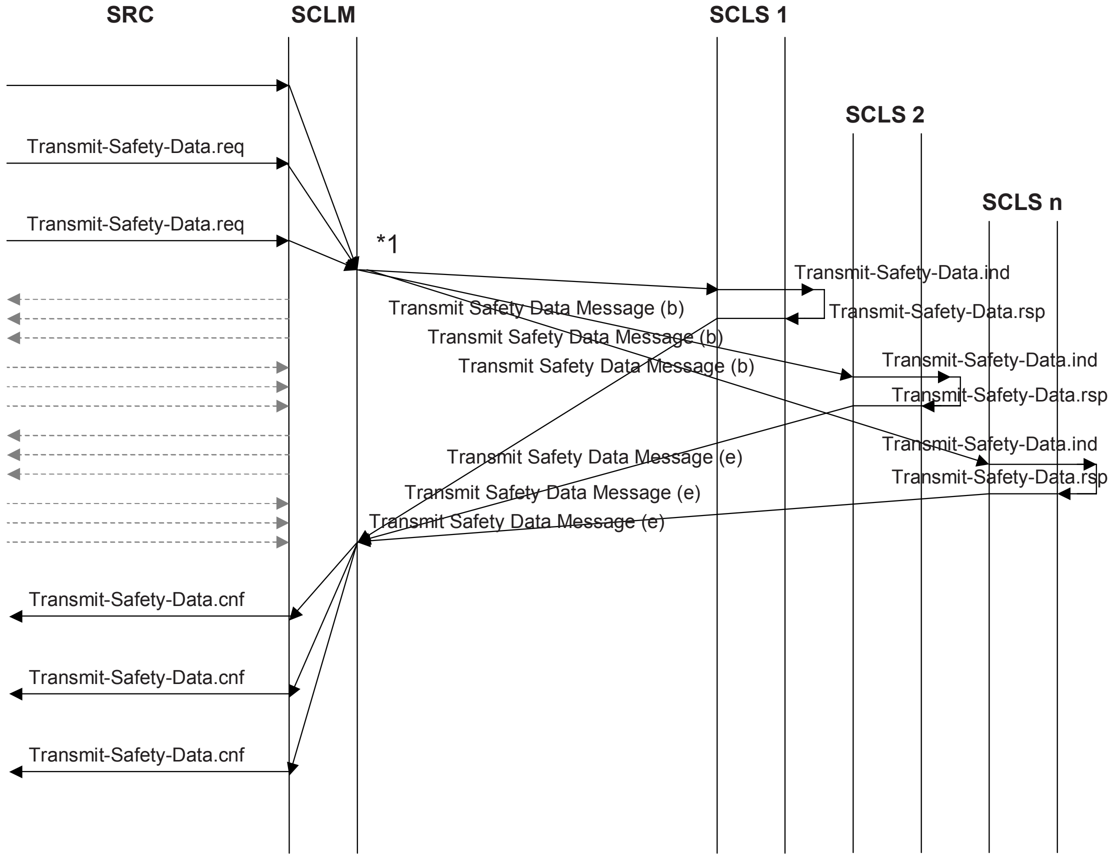
Figure 39 – Parameterize device sequence

7.2.4 Process data mode

This subclause describes the transmission of safety data. The SRC creates all the Transmit-Safety-Data.req for safety slaves. The safety data are transmitted simultaneous (in one cycle) to the safety relevant slaves (Figure 40, *1).

For connections in the parameterization state, a Transmit-Safety-Data.req can be sent to enter the process data mode state.

If no Transmit-Safety-Data.req or Abort.req are sent for connections in the process data mode state, all the connections shall be aborted with an Abort.req.



*1: Start IEC 61158 Type 8 service

Figure 40 – Simultaneous transmission of safety data to the safety slaves

Figure 41 specifies the use of the sequence number in the SCLM and SCLS.

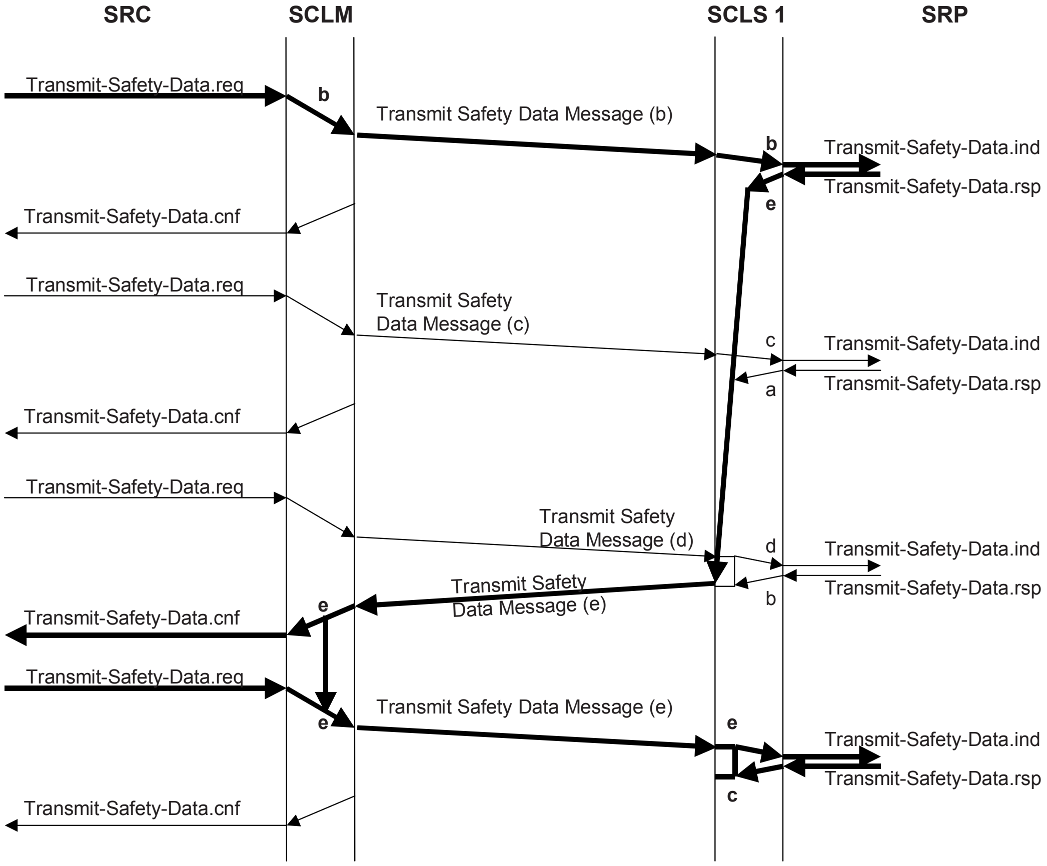


Figure 41 – Use of the sequence number in the SCLM and SCLS

In the process data mode state, all the safety slaves are synchronized with the first Transmit-Safety-Data.req. Once synchronization is complete, the safety data are transmitted with the next Transmit-Safety-Data.req. Figure 42 specifies this relationship.

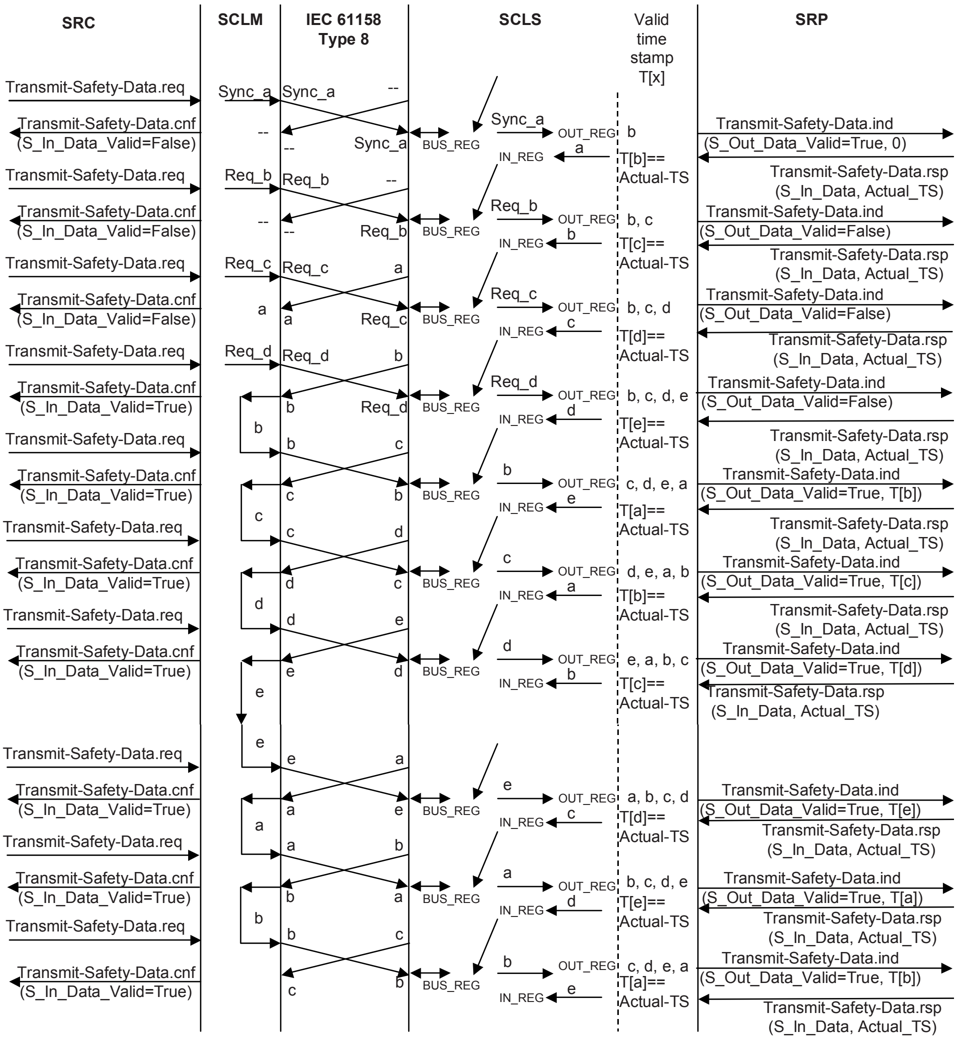


Figure 42 – Startup and error-free operation

Figure 43 specified the communication sequence for resynchronization during operation in the event of a transmission error in the IEC 61158 Type 8 communication system. The sequence is implemented simultaneously with all the safety slaves in the event of the following:

- error in the IEC 61158 Type 8 communication system;
- removal and addition of safety slaves;
- invalid CRC 24 checksum detected by the SCLM.

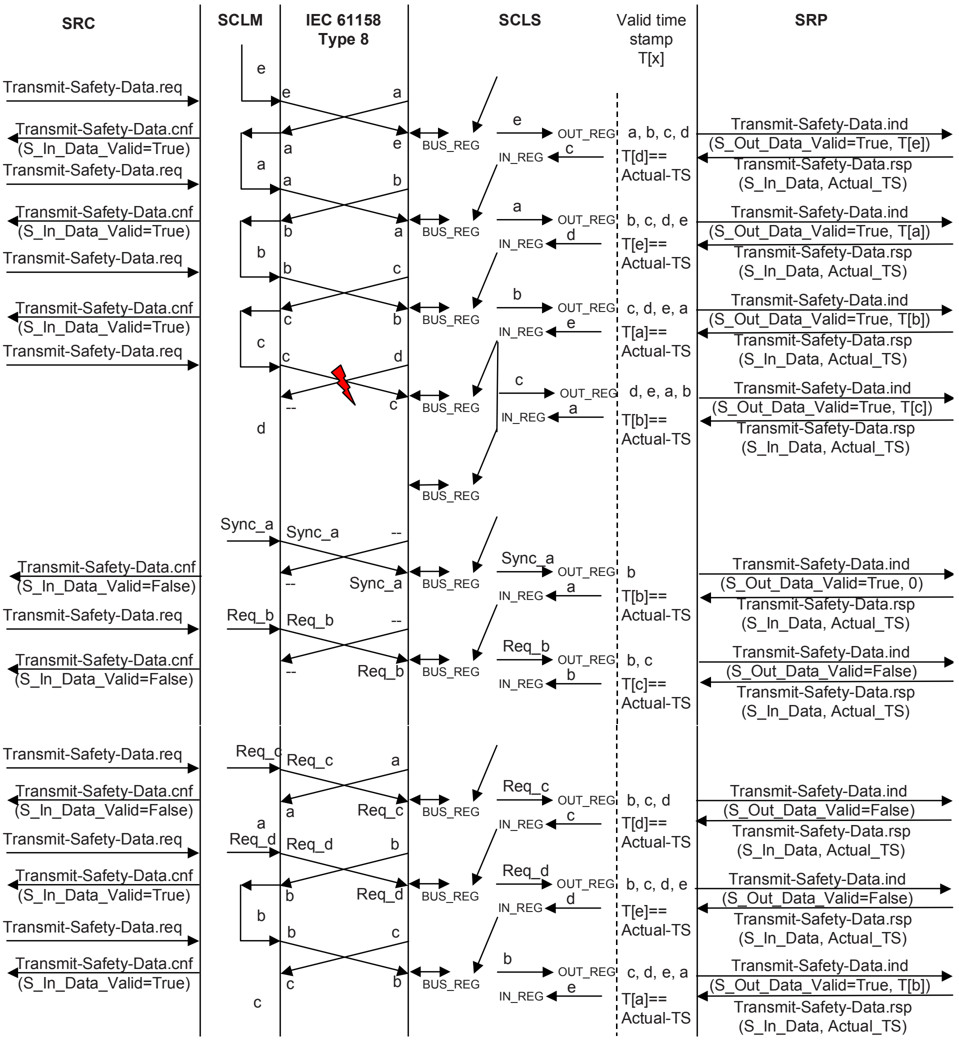

SRC
SCLM
IEC 61158 Type 8
SCLS
Valid time stamp T[x]
SRP
Transmit-Safety-Data.req
Transmit-Safety-Data.cnf (S_In_Data_Valid=True)
Transmit-Safety-Data.cnf (S_In_Data_Valid=False)
Transmit-Safety-Data.ind (S_Out_Data_Valid=True, T[e])
Transmit-Safety-Data.ind (S_Out_Data_Valid=True, T[a])
Transmit-Safety-Data.ind (S_Out_Data_Valid=True, T[b])
Transmit-Safety-Data.ind (S_Out_Data_Valid=True, T[c])
Transmit-Safety-Data.ind (S_Out_Data_Valid=True, 0)
Transmit-Safety-Data.ind (S_Out_Data_Valid=False)
Transmit-Safety-Data.rsp (S_In_Data, Actual_TS)
BUS_REG
OUT_REG
IN_REG
a, b, c, d
T[d]== Actual-TS
b, c, d, e
T[e]== Actual-TS
c, d, e, a
T[a]== Actual-TS
d, e, a, b
T[b]== Actual-TS
b
b, c
T[c]== Actual-TS
b, c, d
b, c, d, e
Sync_a
Req_b
Req_c
Req_d
--
a
b
c
d
e

Figure 43 – Resynchronization during operation

Figure 44 specifies the communication sequence in the event of an invalid CRC 24 checksum detected by the SCLS.

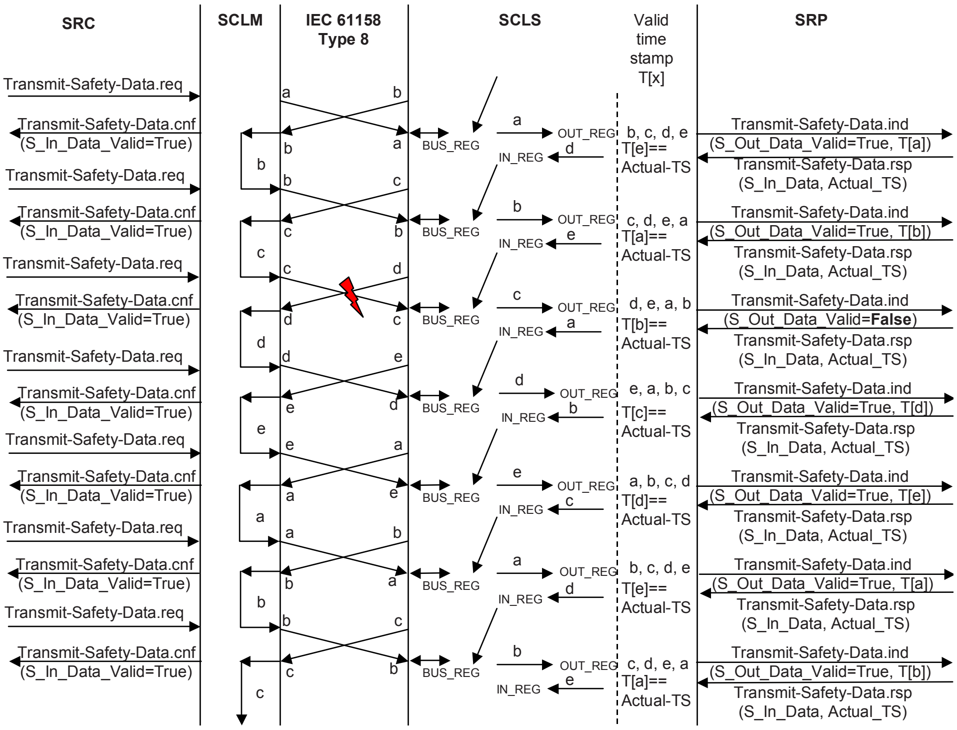

SRC
SCLM
IEC 61158 Type 8
SCLS
Valid time stamp T[x]
SRP
Transmit-Safety-Data.req
Transmit-Safety-Data.cnf (S_In_Data_Valid=True)
a
b
BUS_REG
OUT_REG
IN_REG
b, c, d, e T[e]== Actual-TS
Transmit-Safety-Data.ind (S_Out_Data_Valid=True, T[a])
Transmit-Safety-Data.rsp (S_In_Data, Actual_TS)
c, d, e, a T[a]== Actual-TS
Transmit-Safety-Data.ind (S_Out_Data_Valid=True, T[b])
d, e, a, b T[b]== Actual-TS
Transmit-Safety-Data.ind (S_Out_Data_Valid=False)
e, a, b, c T[c]== Actual-TS
Transmit-Safety-Data.ind (S_Out_Data_Valid=True, T[d])
a, b, c, d T[d]== Actual-TS
Transmit-Safety-Data.ind (S_Out_Data_Valid=True, T[e])
b, c, d, e T[e]== Actual-TS
Transmit-Safety-Data.ind (S_Out_Data_Valid=True, T[a])
c, d, e, a T[a]== Actual-TS
Transmit-Safety-Data.ind (S_Out_Data_Valid=True, T[b])
c
d
e

Figure 44 – Invalid CRC 24 checksum detected by the SCLS

7.2.5 Process data mode with diagnostic data transmission

Figure 45 specifies the process data mode with diagnostic data transmission sequence.

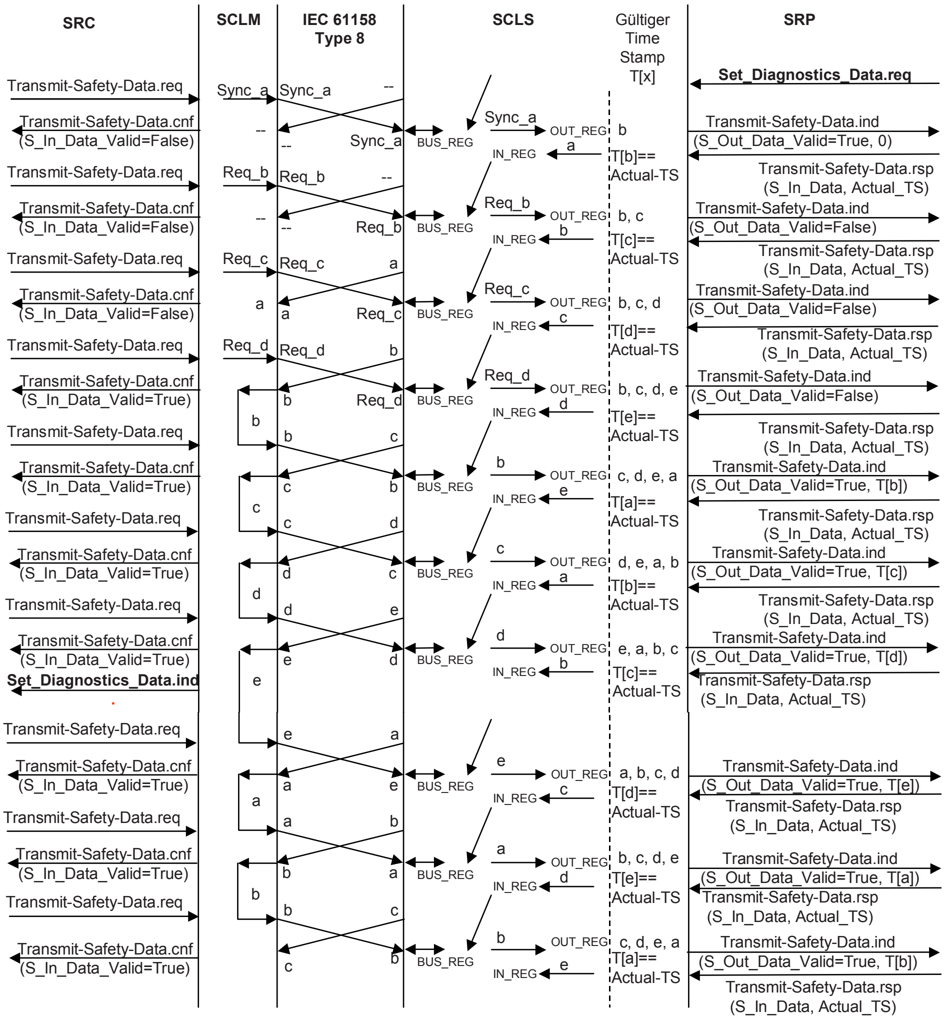

SRC
SCLM
IEC 61158 Type 8
SCLS
Gültiger Time Stamp T[x]
SRP
Set_Diagnostics_Data.req
Transmit-Safety-Data.req
Sync_a
Sync_a
--
Transmit-Safety-Data.cnf (S_In_Data_Valid=False)
--
--
Sync_a
BUS_REG
Sync_a
OUT_REG
IN_REG
a
b
T[b]== Actual-TS
Transmit-Safety-Data.ind (S_Out_Data_Valid=True, 0)
Transmit-Safety-Data.rsp (S_In_Data, Actual_TS)
Transmit-Safety-Data.req
Req_b
Req_b
Transmit-Safety-Data.cnf (S_In_Data_Valid=False)
Req_b
b, c
T[c]== Actual-TS
Transmit-Safety-Data.ind (S_Out_Data_Valid=False)
Transmit-Safety-Data.rsp (S_In_Data, Actual_TS)
Transmit-Safety-Data.req
Req_c
Req_c
Transmit-Safety-Data.cnf (S_In_Data_Valid=False)
Req_c
b, c, d
T[d]== Actual-TS
Transmit-Safety-Data.req
Req_d
Req_d
Transmit-Safety-Data.cnf (S_In_Data_Valid=True)
Req_d
b, c, d, e
T[e]== Actual-TS
c, d, e, a
T[a]== Actual-TS
d, e, a, b
T[b]== Actual-TS
e, a, b, c
T[c]== Actual-TS
Transmit-Safety-Data.ind (S_Out_Data_Valid=True, T[b])
Transmit-Safety-Data.ind (S_Out_Data_Valid=True, T[c])
Transmit-Safety-Data.ind (S_Out_Data_Valid=True, T[d])
Set_Diagnostics_Data.ind
a, b, c, d
T[d]== Actual-TS
Transmit-Safety-Data.ind (S_Out_Data_Valid=True, T[e])
b, c, d, e
T[e]== Actual-TS
Transmit-Safety-Data.ind (S_Out_Data_Valid=True, T[a])
c, d, e, a
T[a]== Actual-TS
Transmit-Safety-Data.ind (S_Out_Data_Valid=True, T[b])
Transmit-Safety-Data.rsp (S_In_Data, Actual_TS)

Figure 45 – Process data mode with diagnostic data transmission

7.2.6 Process data mode with Acknowledgement-Data transmission

Figure 46 specifies the process data mode with Acknowledgement-Data transmission sequence.

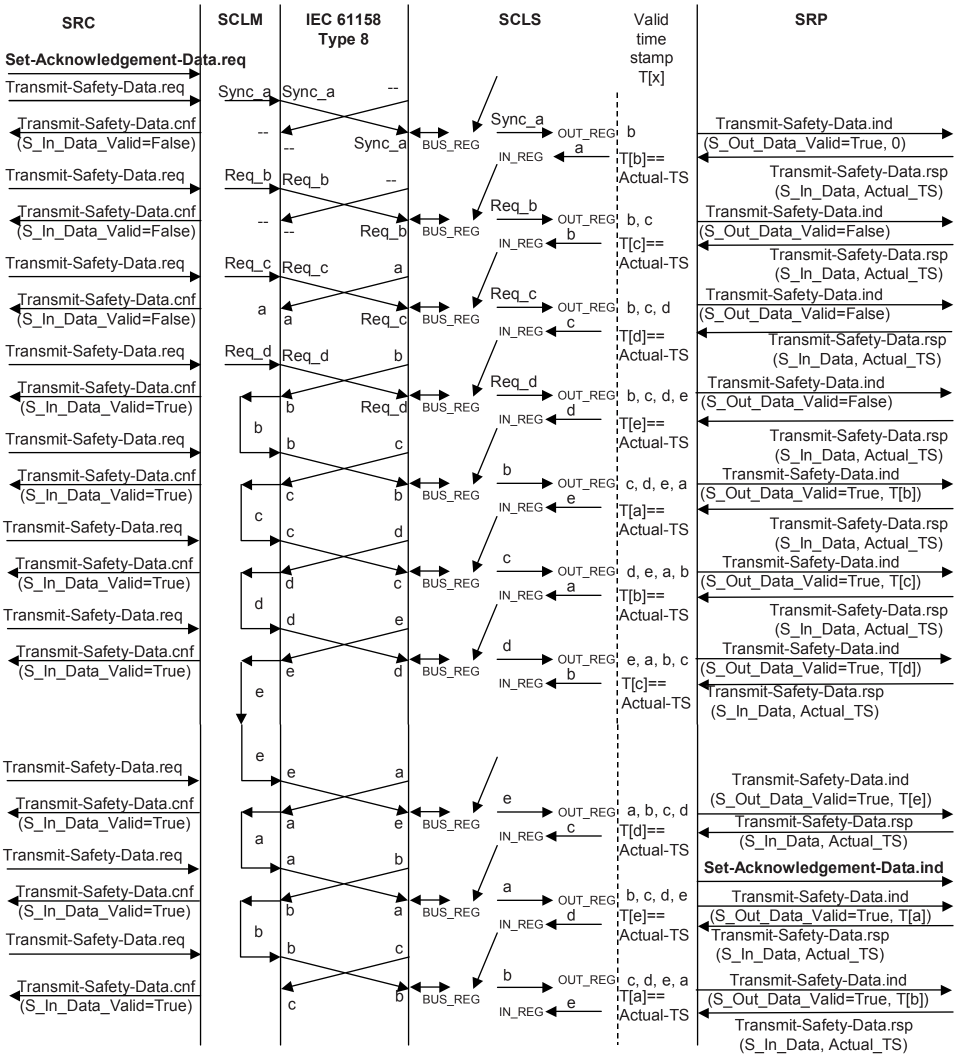


Figure 46 – Process data mode with Acknowledgement-Data transmission

7.2.7 Connection aborted

In this state, the connection to the safety slave is aborted.

An abort can be triggered by the following:

- Safety_Slave_Error
- Error detected (SCLM)
- Abort.req

7.3 Abort

7.3.1 Connection abort in the event of an error detected by the SCLM

Figure 47 specifies the connection abort in the event of an error when initiating a connection.

When one of the errors listed in Table 20 is detected in the SCLM, the SCLM transmits the Abort_Connection message to the SCLS and aborts the initiation of the connection to the SCLS. At the SCLM, an Abort.ind with the corresponding Abort_Info from Table 20 is sent to the SRC.

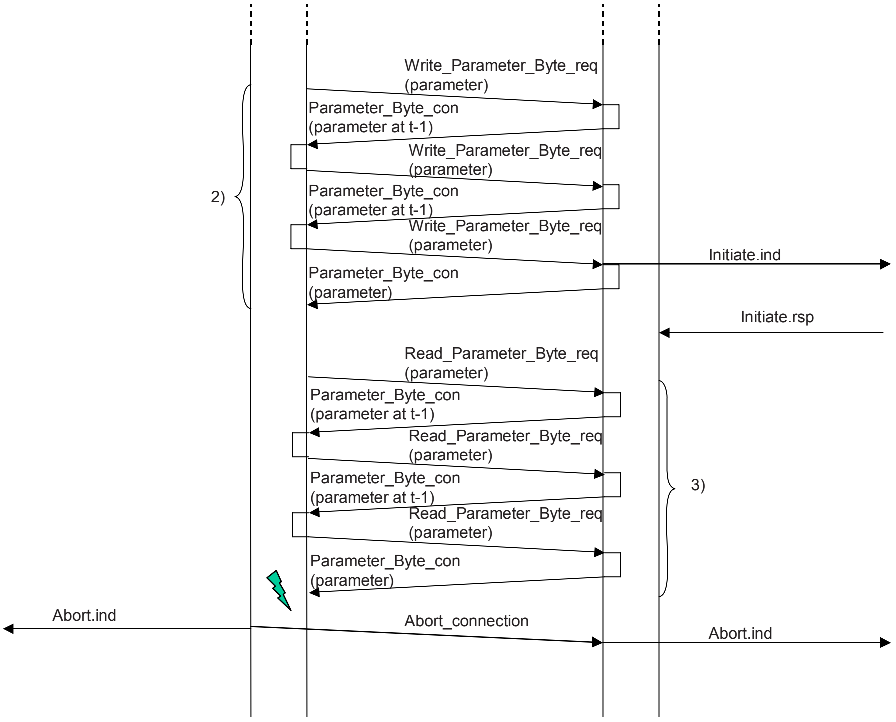


Figure 47 – Error when initiating a connection

Table 20 – Abort_Info: Connection abort in the event of an error detected by the SCLM

Abort_Info	Generated by	All Point-to-Point Connections aborted	Meaning
Invalid_Serial_Number	SCLM	No	**Additional_Info** contains the serial number received from the safety slave.
Invalid_Vendor_ID	SCLM	No	
Invalid_Device_Type	SCLM	No	
Invalid_Device_Revision	SCLM	No	

7.3.2 Abort of all connections in the event of an error detected by the SCLS

Figure 48 shows that one of the errors listed in Table 21 has been detected on the SCLS side. The behavior is shown by the Transmit-Safety-Data service. This method also applies to the following services:

- Initiate
- Send Application Parameter
- Send Application Parameter ID
- Parameterize Device

The SCLS indicates the error with the Abort.ind (Abort_Info = Abort_Connection) at its SRP and with the Safety_Slave_Error message (Abort_Info) at the SCLM. The SCLS then enters the connection aborted state.

After receiving the Safety_Slave_Error message (Abort_Info), the SCLM transmits an Abort.ind (Abort_Info) for each established connection to the SRC and sends the Abort_Connection message to all the SCLS. It then enters the connection aborted state for all connections.

All SCLS, whose connections have not yet been aborted, transmit an Abort.ind (Abort_Info = Abort_Connection) to their SRP and then enter the connection aborted state.

In the connection aborted state, the SCLS that detected the error responds to the messages from the SCLM with the last sent Safety_Slave_Error (Abort_Info) until an IEC 61158 Type 8 bus reset or power ON occurs. It then transmits the Safety_Slave_Error (No_Safety_Connection_ID). A new connection can now be initiated by the SCLM.

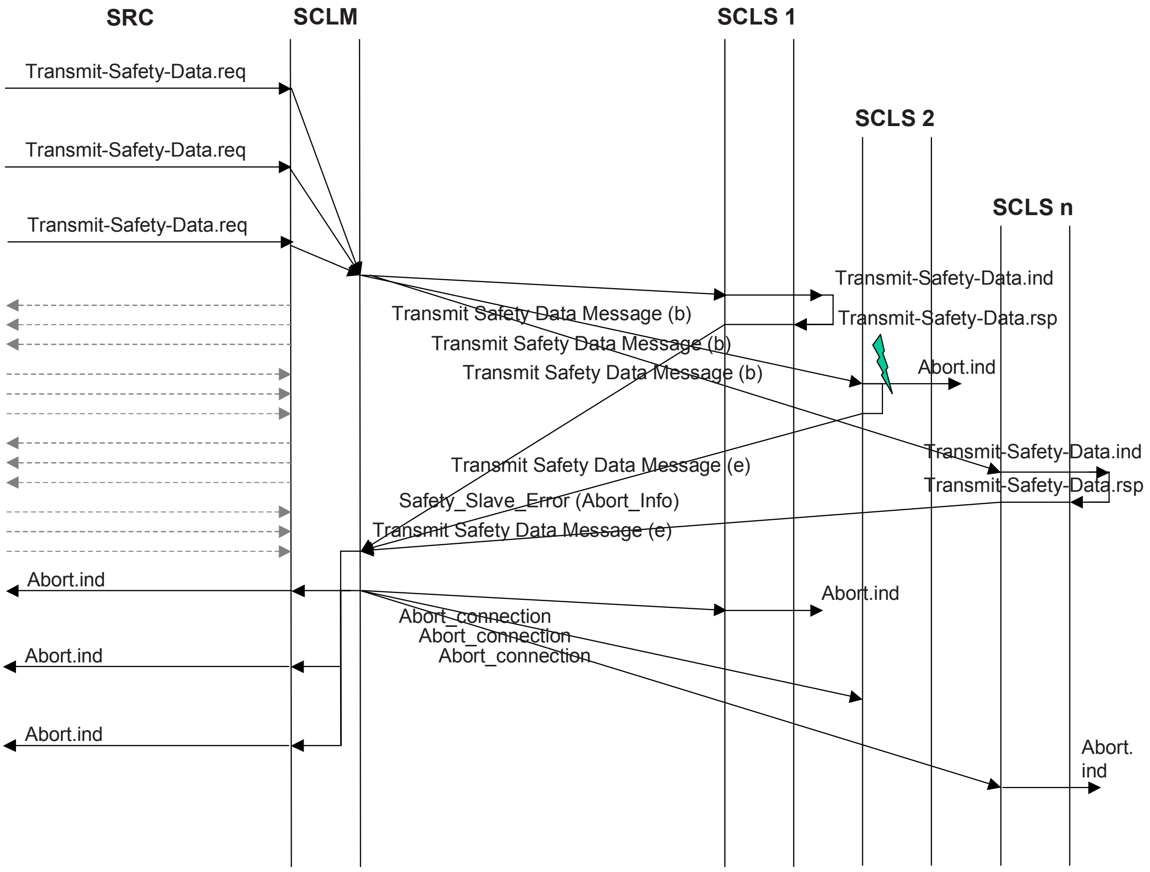


Figure 48 – Error at an SCLS when aborting all connections

Table 21 – Abort_Info: Abort of all connections in the event of an error detected by the SCLS

Abort_Info	Abort_Info in 7.1.6.2	Meaning
State_Error Max_Retry_Exceeded_SCLS	$6fc_{hex}$	Error in the program sequence. A Read_Parameter_Req or a Byte_Parameter_Req was received 10 times in succession
Invalid_Safety_Connection_ID	$6fd_{hex}$	Safety message received with an invalid safety connection ID
Invalid_Sequence_Num	$6fe_{hex}$	Safety message received with an invalid sequence number
Invalid_Message	$6fb_{hex}$	The specified sequence for safety messages was not observed (for example Sync_a message in a wrong state)
CRC_24_Error	$6ff_{hex}$	An invalid CRC 24 was detected by an SCLS when initiating a connection or during the parameterization phase. During parameterization mode, invalid CRC 24 sequences were detected in consecutive safety messages, whereby the correct order of sequence numbers is no longer guaranteed

7.3.3 Abort of all connections in the event of an error detected by the SCLM

Figure 49 shows that one of the errors listed in Table 22 has been detected on the SCLM side. The behavior is shown by the Transmit-Safety-Data service. This method also applies to the following services:

- Initiate
- Send Application Parameter
- Send Application Parameter ID
- Parameterize Device

When one of the errors listed in Table 22 is detected in the SCLM, the SCLM transmits an Abort.ind (Abort_Info) for each established connection to the SRC and sends the Abort_Connection message to all the SCLS. It then enters the connection aborted state for all connections.

All SCLS transmit an Abort.ind (Abort_Info = Abort_Connection) to their SRP and then enter the connection aborted state.

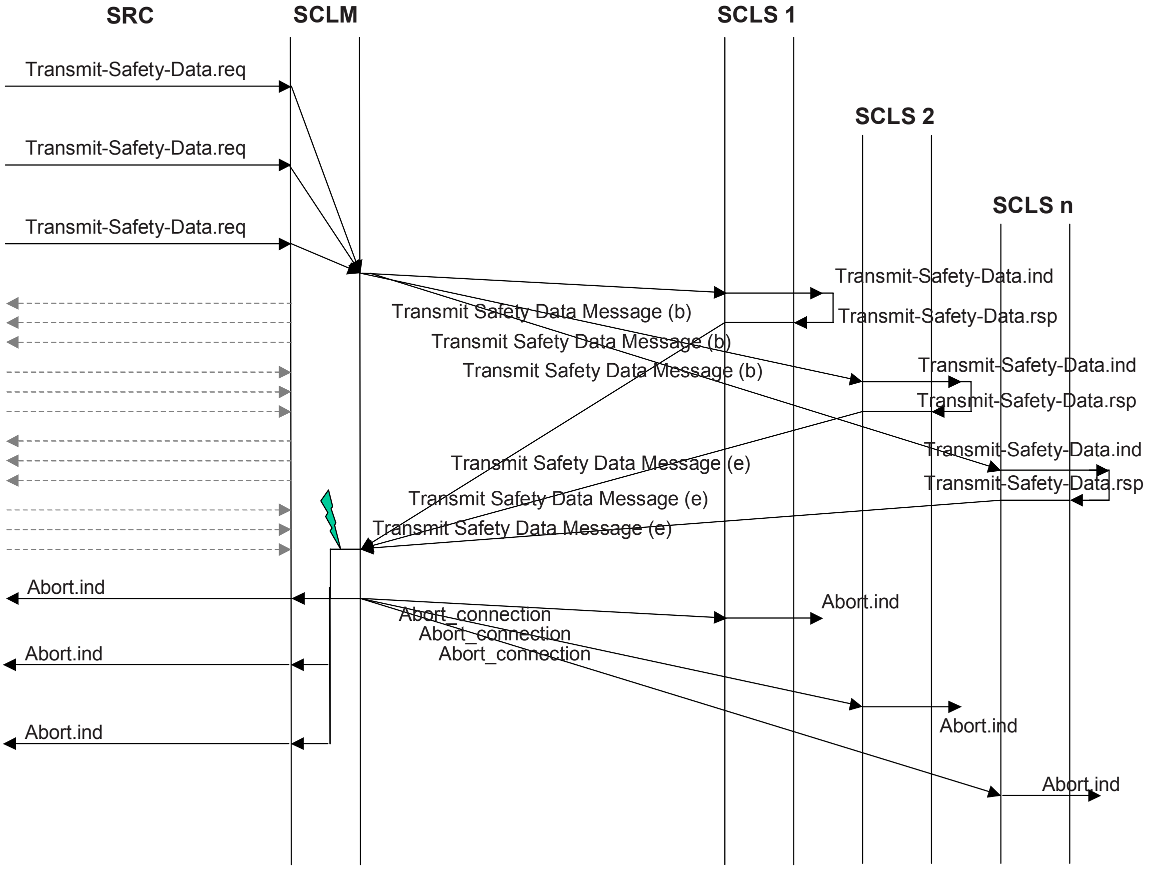


Figure 49 – Abort of all connections in the event of an error detected by the SCLM

Table 22 – Abort_Info: Abort of all connections in the event of an error detected by the SCLM

Abort_Info	Meaning
State_Error	Error in the program sequence
Invalid_Safety_Connection_ID	Safety message received with an invalid safety connection ID
Invalid_Sequence_Num	Safety message received with an invalid sequence number
Invalid_Message	The specified sequence for safety messages was not observed
Invalid_SCLS_Version	The SCLS version number does not match the SCLM version number
Max_Retry_Exceeded_SCLM	In the initiate or parameterization sequence, no corresponding confirmation was received after 10 attempts to send a Read_Parameter_Byte.req or Write_Parameter.req.

8 Safety communication layer management

8.1 General

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

- Set-Safety-Configuration
- Start IEC 61158 Type 8

8.2 Requirements of safety communication layer management

The services shall be used in a defined way (see Sequences in 7.2) so that the safety communication system is prepared for the safety function to be performed.

8.3 Set-Safety-Configuration service

The Set-Safety-Configuration service (Table 23) is used to configure the SCLM subsystem.

Table 23 – Set-Safety-Configuration service

Parameter name	Req	Cnf
Argument	M	
List_of_Configuration_Data	M	
Physical_Position	M	
Location_ID	M	
Serial_Number	M	
Vendor_ID	M	
Device_Type	M	
Device_Revision	M	
Result(+)		S
Result(-)		S
Error_Info		M

Argument

The argument contains the parameters of the service request.

List_of_Configuration_Data

This parameter record contains the configuration data for all safety devices.

Physical_Position

This parameter specifies the number of the safety device in the communication system with which the connection is to be initiated.

Location_ID

This parameter contains the location ID of the addressed device [1 … 126]. It is used to address the device.

Serial_Number

This parameter contains the unique serial number of the addressed device.

Vendor_ID

This parameter contains the vendor ID of the addressed device.

Device_Type

This parameter contains the device type of the addressed device.

Device_Revision

This parameter contains the device revision of the addressed device.

Error_Info

This parameter contains the description of the error as specified in Table 24.

Table 24 – Error_Info

Error_Info	Meaning
Invalid_Physical_Position	Each of the used values for the parameter Physical_Position shall be unique within the safety communication system
Invalid_Location_ID	Each Location_ID shall be unique. None of them shall have the value zero

8.4 Start IEC 61158 Type 8 service

The Start IEC 61158 Type 8 service starts the transmission of safety data.

This service has no parameters.

9 System requirements

9.1 Indicators and switches

Each safety slave device shall have a red colored LED. This LED shall represent the following states:

- **Off**: If power supply is connected: no error of the safety slave; device in process data mode
- **Flashing** (1 Hz): Device not parameterized
- **On**: Failure state of the device; device fails; SCLS in connection aborted state

Each safety master device shall have a red colored LED. This LED shall represent the following states:

- **Off**: If power supply is connected: no error of the safety master device; device in process data mode
- **Flashing** (1 Hz): safety master is in the initiate state or initiate state was left with a failure or debug state of the safety relevant controller
- **On**: Failure state of the device; device fails; SCLM in connection aborted state

9.2 Installation guidelines

This part specifies protocol and services for a safety communication system based on IEC 61158 series Type 8. However, usage of safety devices with the safety protocol specified in this part requires proper installation. All devices connected to a safety communication system defined in this part shall fulfil SELV/PELV requirements, which are specified in the relevant IEC standards such as IEC 60204-1. Further relevant installation guidelines are specified in IEC 61918 and IEC 61784-5-6.

Additional installation information is also given in [44] and [45] in the bibliography.

9.3 Safety function response time

9.3.1 General

As mentioned in 5.3 an integrated watchdog timer is used which provides the time expectation of each output channel on each safety output slave. It ensures a 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).

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 each safety slave (input and output), 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.

9.3.2 Calculation of the parameterized shutdown time

9.3.2.1 General

The typical response time of a fieldbus system is the time between the recognition of an input signal at the terminal block of a safety input slave and the time at which a corresponding reaction at the terminal block of a safety output slave is detected. This time can usually only be reached and measured during error-free operation of the IEC 61158 Type 8 communication system.

The processing times for the standard control system are irrelevant for determining the typical response time of the IEC 61158 Type 8 communication system.

The typical response time of the IEC 61158 Type 8 communication system is irrelevant and not suitable for determining the guaranteed shutdown time or for dimensioning safe distances.

9.3.2.2 Shutdown times

The safety function response time comprises the following times

- Response time of the sensor
- Response time of the functional safety communication system (including also processing times on safety slave, safety master and safety relevant controller)
- Response time of the actuator
- Machine stopping time

EXAMPLE Machine stopping time could be e. g. time to stop a fast rotating paper roll

The guaranteed shutdown time (t_G) of the functional safety communication system performing the safety function comprises the

- processing time of the safety inputs involved in the safety function (maximum value of all safety input slaves used by the safety function)
- parameterized shutdown time of a safety output involved

The manufacturers of the safety input slaves shall document the processing time of the safety input slave within the information for use of this device.

For the calculation of the safety function response time Equation (2) shall be used.

$$tSF = tS + tIN + tCTSCS + tOD + tA + tStop \qquad (2)$$

where

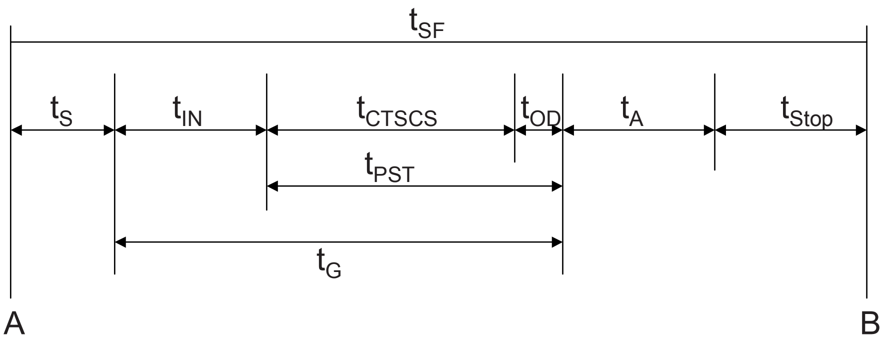
tSF	is the safety function response time (application specific);
tS	is the sensor response time (see information for use of the sensor);
tIN	is the processing time of the safety input (shall be specified from the manufacturer of the safety device and shall be part of the information for use of the safety device);
tCTSCS	is the cycle time of the functional safety communication system;
tOD	is the processing time of the safety output device;
tA	is the tesponse time of the actuator (see information for use of the actuator);
tStop	is the machine stopping time (shall be measured).

NOTE 1 If several sensors are involved in the safety function, the longest response time of the sensors involved is used in the calculation.

NOTE 2 If several inputs are involved in the safety function, the longest processing time of the inputs involved is used in the calculation.

NOTE 3 Instead of a stopping time the time needed for achieving the safe state of a machine or plant can be used too. Usually this time can be reduced by using a category 1 or 2 stop.

The parameterized shutdown time (t_{PST}) of a safety output shall be determined according to 9.3.2.4. Figure 50 gives an overview of the shutdown time.



Key

A is the demand of a safety function

B is the safe state of the machine or plant

t_{PST} is the parameterized shutdown time of a safety output

Figure 50 – Overview of the shutdown time

9.3.2.3 Cycle Times of the IEC 61158 Type 8 communication system and the functional safety communication system

The cycle time of the functional safety communication system t_{CTSCS} is calculated as shown in Equation (3).

$$tCTSCS = tIB + tSRC \qquad (3)$$

where

tCTSCS	is the cycle time of the functional safety communication system;
tIB	is the cycle time of the IEC 61158 Type 8 communication system;
tSRC	is the processing time of the SRC.

The minimum cycle time of the IEC 61158 Type 8 communication system t_{IB} is application specific and outside the scope of this part. If there is a value given in the information for use of the functional safety communication system, this value shall be used for the calculation.

The time t_{IB} is also application specific. Usually it is calculated with Equation (4).

$$tIB = [M \times 13 \times (8 + n) + 3 \times a] \times Tbit + tSW \qquad (4)$$

where

tIB is the cycle time of the IEC 61158 Type 8 communication system;

M is the master implementation factor;

n is the number of data octets (user data; payload);

a is the number of all slaves;

Tbit is the nominal bit duration (see 27.2 in IEC 61158-2);

tSW is the software processing time of the master (application specific).

NOTE 1 The formula for calculation of t_{IB} depends on the implementation of the master. A typical value for M is 1,15.

NOTE 2 The value of t_S is implementation specific. A typical value for t_S is 0,7 ms. For more details see relevant information for use documents of the manufacturer of the used master device.

NOTE 3 The minimum cycle time of an IEC 61158 Type 8 communication system is implementation specific. For more details see relevant information for use documents of the manufacturer of the used master device.

The processing time of the SRC can be approximately calculated with Equation (5).

$$tSRC = nFBS \times tFBS + nas \times tFBS + 0{,}3\ ms \qquad (5)$$

where

tSRC is the processing time of the SRC;

nFBS is the number of used function blocks (in the safety-related application software);

tFBS is the average function block processing time (in the safety-related application software);

nas is the number of safety slaves.

NOTE 4 A typical value for t_{FBS} is 0,01 ms may be longer or shorter in a specific implementation. Therefore is is recommended to take into account the information for use documents of the manufacturer of the used master or safety relevant controller device for an exact calculation.

9.3.2.4 Parameterized shutdown time t_{PST} of a safety output

Usually the safety function response time is limited by the application (e. g. application specific standard, safety requirements specification). The following text describes the procedure for the safety communication system for determining the parameterized shutdown time that can be implemented in this system.

If the required shutdown time is based on the system design, the specifications in this subclause shall be used to determine whether these times can be observed by the planned structure of the functional safety communication system.

In the following calculation, it is assumed that the structure of the functional safety communication system and the transmission speed are specified. These are the controlling factors for the cycle time of the functional safety communication system t_{CTSCS} and therefore also for the parameterized shutdown time of the safety outputs that can be implemented in this system.

The parameterized shutdown time of the safety outputs if t_{CTSCS} is greater or equal than 2 ms T_{PST} is calculated as shown in Equation (6).

$$tPST \geq AF \times tCTSCS + tOD \tag{6}$$

where

tPST	is the parameterized shutdown time;
AF	is the availability factor;
tCTSCS	is the cycle time of the functional safety communication system;
tOD	is the processing time of the safety output device.

The parameterized shutdown time of the safety outputs if t_{CTSCS} is less than 2 ms t_{PST} is calculated as shown in Equation (7).

$$tPST \geq AF \times 2\ ms + tOD \tag{7}$$

where

tPST	is the parameterized shutdown time;
AF	is the availability factor;
tOD	is the processing time of the safety output device.

The factor AF (availability factor) takes into account permissible and typical errors, for example, EMI and associated single errors in the IEC 61158 Type 8 communication system.

NOTE The value of AF is implementation and applications specific. The value may be adjusted between 5 and 14. For the examples in this subclause AF = 14 is used. Doing this e. g. EMI conditions do not limit the availability of the functional safety communication system. With a good installation of the functional safety communication system AF = 5 may be sufficient too.

If communication in the functional safety communication system is affected longer than calculated for t_{PST}, this shall result in the shutdown of the corresponding safety output(s), so that the guaranteed shutdown time for the safety function is always observed. This shutdown shall be diagnosed and should be acknowledged if an acknowledgement procedure is programmed in the safety-related application program.

9.3.2.5 Example for calculating the parameterized shutdown time t_{PST} of the safety outputs

The parameterized shutdown time in the example is calculated as shown in Equation (3) up to Equation (7). The way to calculate the parameterized shutdown time taking into account intermediate results and the result of the calculation is shown in Table 25 up to Table 27.

The calculation of t_{IB} is shown in Table 25.

Table 25 – Calculation of tIB

Parameter	Description	Value	(sub) total
N	Number of data octets	13	
A	Number of all slaves	4	
T_{bit}	Nominal bit duration	500 ns	
t_{SW}	Software processing time of the master	0,7 ms	
t_{IB}	Cycle time of the IEC 61158 Type 8 communication system. Applying Equation (4)		0,86 ms

Table 26 shows the calculation of t_{SRC}.

Table 26 – Calculation of tSRC

n_{FBS}	Number of used function blocks (in the safety-related application software)	6	
n_{as}	number of safety slaves	2	
t_{FBS}	average function block processing time (in the safety-related application software)	0,01 ms	
t_{SRC}	Processing time of the SRC Applying Equation (5)		0,38 ms

With this values the calculation of t_{PST} can be performed. This is shown in Table 27.

Table 27 – Calculation of tPST

t_{OD}	Processing time of the safety output device. In this example t_{OD} is neglected.	-	
t_{CTSCS}	Cycle time of the functional safety communication system Applying Equation (3) Result is t_{CTSCS} = 1,24 ms, which is less than 2 ms. Therefore t_{CTSCS} = 2 ms is used.	1,24 ms	2 ms
t_{PST}	**Result for parameterized shutdown time of a safety output applying Equation (7):** **$t_{PST} \geq 14 \times 2$ ms**		28 ms

The user shall always check the value of the parameterized shutdown time of a safety output.

9.4 Duration of demands

The requirements of 6.3.1 shall be taken into account.

9.5 Constraints for calculation of system characteristics

9.5.1 System characteristics

The following basic data have to be adhered:

- IEC 61158 Type 8: No restrictions
- Maximum number of safety devices: 126
- Maximum number of safety relevant Bits per Safety PDU: 14
- Maximum of parameters per a functional safety slave: 254 × 20 octets

NOTE Each safety relevant Bit is protected according to SIL 3

9.5.2 Calculation of the number of telegrams per second

Safety messages will be transmitted with each data cycle, so all safety messages have to be taken into account calculating Λ according to Equation (8).

$$\Lambda SL(Pe) = RSL(Pe) \times \nu \times m \tag{8}$$

where

$\Lambda SL(Pe)$ is the residual error rate per hour of the safety communication layer with respect to the bit error probability;

$RSL(Pe)$ is the residual error probability of a safety message;

ν is the maximum number of safety messages per hour;

m is the maximum number of information sinks that is permitted in a single safety function;

Pe is the bit error probability.

For IEC 61158 Type 8 the product n × m shall take into account the maximum of all safety messages per second within the system. With each IEC 61158 Type 8 data cycle for each of the existing safety slaves (I_s: number of safety slaves) the safety master sends a message.

At the same time (with each IEC 61158 Type 8 data cycle) the safety slaves send back their messages to the safety master. In one IEC 61158 Type 8-Cycle ($2 \times I_s$) safety messages are transmitted. The worst-case scenario is that a functional safety system consists only of safety slaves. A safety message consists of 6 octets, so calculation of the cycle time is as shown in Equation (9).

$$tIB = 13 \times 6 \times nas \times Tbit, \tag{9}$$

where

tIB is the cycle time of the IEC 61158 Type 8 communication system;

nas is the number of safety slaves;

$Tbit$ is the time for the transmission of one bit.

Equation (10) shows how to calculate $\nu \times m$.

$$\nu \times m = (2 \times nas) / (13 \times 6 \times nas \times Tbit) = 1 / (39 \times Tbit) \tag{10}$$

where

ν is the maximum number of safety messages per hour;

m is the maximum number of information sinks that is permitted in a single safety function;

nas is the number of safety slaves;

$Tbit$ is the time for the transmission of one bit.

EXAMPLE Within a functional safety communication system with 2 Mbit/s: $\nu \times m$ = 51 282 safety messages/s

NOTE The product $\nu \times m$ effects the response time of the functional safety communication system and the maximum SIL CL of this system. A higher SIL CL may than lead to longer response times and vice versa. A value of 51 282 safety messages/s allows a very short response time (based on a low bit duration time) as well as a SIL CL of 3.

9.6 Maintenance

No SCL specific requirements for maintenance.

NOTE 1 Specifications for system behavior in case of device repair and replacement are outside the scope of this part. The specification of these activities and the responsibilities are not relevant for the specification of services and protocols. Usually this will be part of a functional safety management plan. However, repair, replacement as well as maintenance, overall safety validation, overall operation, modifications, retrofits and decommissioning or disposal according to IEC 61508 are important issues which have to be taken into account. It is recommended to contact the device or system supplier also.

NOTE 2 For information for programming of the SRP and the parameterization of safety devices it is strongly recommended to contact the device or system supplier. Beside this it is recommended to take into account the documents [47] or [48] from the bibliography. In this part additional information e. g. checklists are given for the user of an INTERBUS-Safety system.

NOTE 3 Additional requirements for maintenance – as well as other requirements – are specified in IEC 61508, IEC 61511 and / or IEC 62061.

9.7 Safety manual

The supplier of safety slaves that incorporate the SCL according to the SCL specifications given in this part shall prepare an appropriate safety manual according to IEC 61508. This safety manual shall also include the installation requirements as specified in 9.2.

According to the safety communication system based on IEC 61158 Type 8 it is strongly recommended to take into account the specifications [47] and [48] of the bibliography.

NOTE 1 Before starting the implementation of a safety device it is good engineering practice to contact the INTERBUS-Club to figure out, if there are amendments to implementation guidelines and/or implementation requirements.

NOTE 2 For general information concerning functional safety mainly in Europe see [49] and [50].

10 Assessment

It is the manufacturers responsibility to develop the devices to the appropriate development process according to the safety standards (see IEC 61508, IEC 61511, IEC 62061, ...) and relevant legal regulations (e. g. European machinery directive).

NOTE For validation and/or assessment of safety devices specific requirements outside of this part exists. Further information for validation and/or assessment of safety devices can be obtained by the INTERBUS-Club (www.interbusclub.com).

Annex A
(informative)

Additional information for functional safety communication profiles of CPF 6

There is no additional information for this FSCP.

Annex B
(informative)

Information for assessment of the functional safety communication profiles of CPF 6

Information about test laboratories which test and validate the conformance of FSCP 6/7 products with IEC 61784-3-6 can be obtained from the National Committees of the IEC or from the following organization:

INTERBUS Club Deutschland e.V.
Flachsmarktstrasse 28
32817 Blomberg
GERMANY

Phone: +49 5235/34 2100
Fax: +49 5235/34 1234
E-mail: germany@interbusclub.com
URL: www.interbusclub.com

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/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*

[3] IEC 61131-2, *Programmable controllers – Part 2: Equipment requirements and tests*

[4] IEC 61131-6[11], *Programmable controllers – Part 6: Functional safety*

[5] 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*

[6] 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*

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

[8] IEC 61508-1:2010[12], *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements*

[9] IEC 61508-4:2010[12], *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations*

[10] IEC 61508-5:2010[12], *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 5: Examples of methods for the determination of safety integrity levels*

[11] IEC 61508-6:2010[12], *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3*

[12] IEC 61784-4[13], *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/TR 62210, *Power system control and associated communications – Data and communication security*

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

[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*

[11] In preparation.

[12] To be published.

[13] 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 13849-2, *Safety of machinery – Safety-related parts of control systems – Part 2: Validation*

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

[27] EN 954-1:1996[14], *Safety of machinery – Safety related parts of control systems – General principles for design*

[28] EN 50170, *General purpose field communication system*

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

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

[31] GS-ET-26[15], *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*")

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

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

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

[35] *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.

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

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

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

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

[40] 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

[41] 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

[42] 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

[43] Machinery directive 98/37/EC

[44] IBS SYS PRO INST UM E; *Configuring and Installing INTERBUS*; Phoenix Contact GmbH & Co KG; Prod.-Id. 27 43 802 (can be downloaded from www.phoenixcontact.com)

[45] IBS IL SYS PRO UM E; *Configuring and Installing the INTERBUS Inline product range*; Phoenix Contact GmbH & Co KG; Prod.-Id. 27 43 048 (can be downloaded from www.phoenixcontact.com)

[14] To be replaced by ISO 13849-1 and/or IEC 62061.

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

[46] IBS SYS INTRO G4 UM; *Allgemeine Einführung in das INTERBUS-System*; Phoenix Contact GmbH & Co KG; Prod.-Id. 27 45 10 1

[47] UM EN INTERBUS-SAFETY SYS; *INTERBUS-Safety system description*; Phoenix Contact GmbH & Co KG; Prod.-ID. 26 99 49 3 (can be downloaded from www.phoenixcontact.com)

[48] UM DE INTERBUS-SAFETY SYS; *INTERBUS-Safety Systembeschreibung*; Phoenix Contact GmbH & Co KG; Prod.-ID. 26 99 48 0 (can be downloaded from www.phoenixcontact.com)

[49] SAFETY INTRO UM; *Einführung in die Sicherheitstechnik*; Phoenix Contact GmbH & Co KG; Prod.-ID. 26 98 96 0 (can be downloaded from www.phoenixcontact.com)

[50] SAFETY INTRO UM E; *Introduction to Safety Technology*; Phoenix Contact GmbH & Co KG; Prod.-ID. 26 99 20 2 (can be downloaded from www.phoenixcontact.com)

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

Copyright subsists in all BSI publications. BSI also holds the copyright, in the UK, of the publications of the international standardization bodies. Except as permitted under the Copyright, Designs and Patents Act 1988 no extract may be reproduced, stored in a retrieval system or transmitted in any form or by any means – electronic, photocopying, recording or otherwise – without prior written permission from BSI. This does not preclude the free use, in the course of implementing the standard of necessary details such as symbols, and size, type or grade designations. If these details are to be used for any other purpose than implementation then the prior written permission of BSI must be obtained. Details and advice can be obtained from the Copyright & Licensing Manager.

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™

BSi®