IEC 61784-3-6

Edition 2.0 2010-06

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Industrial communication networks – Profiles – Part 3-6: Functional safety fieldbuses – Additional specifications for CPF 6

Réseaux de communication industriels – Profils – Partie 3-6: Bus de terrain de sécurité fonctionnelle – Spécifications supplémentaires pour CPF 6

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

About the IEC

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

About IEC publications

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

- Catalogue of IEC publications: www.iec.ch/searchpub
The IEC on-line Catalogue enables you to search by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, withdrawn and replaced publications.
- IEC Just Published: www.iec.ch/online_news/justpub
Stay up to date on all new IEC publications. Just Published details twice a month all new publications released. Available on-line and also by email.
- Electropedia: www.electropedia.org
The world's leading online dictionary of electronic and electrical terms containing more than 20 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary online.
- Customer Service Centre: www.iec.ch/webstore/custserv
If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us:
Email: csc@iec.ch
Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00

A propos de la CEI

La Commission Electrotechnique Internationale (CEI) est la première organisation mondiale qui élabore et publie des normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications CEI

Le contenu technique des publications de la CEI est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

- Catalogue des publications de la CEI: www.iec.ch/searchpub/cur_fut-f.htm
Le Catalogue en-ligne de la CEI vous permet d'effectuer des recherches en utilisant différents critères (numéro de référence, texte, comité d'études,…). Il donne aussi des informations sur les projets et les publications retirées ou remplacées.
- Just Published CEI: www.iec.ch/online_news/justpub
Restez informé sur les nouvelles publications de la CEI. Just Published détaille deux fois par mois les nouvelles publications parues. Disponible en-ligne et aussi par email.
- Electropedia: www.electropedia.org
Le premier dictionnaire en ligne au monde de termes électroniques et électriques. Il contient plus de 20 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans les langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International en ligne.
- Service Clients: www.iec.ch/webstore/custserv/custserv_entry-f.htm
Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions, visitez le FAQ du Service clients ou contactez-nous:
Email: csc@iec.ch
Tél.: +41 22 919 02 11
Fax: +41 22 919 03 00

IEC 61784-3-6

Edition 2.0 2010-06

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Industrial communication networks – Profiles – Part 3-6: Functional safety fieldbuses – Additional specifications for CPF 6

Réseaux de communication industriels – Profils – Partie 3-6: Bus de terrain de sécurité fonctionnelle – Spécifications supplémentaires pour CPF 6

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

PRICE CODE XC
CODE PRIX

ICS 25.040.40; 35.100.05

ISBN 978-2-88912-812-9

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES –

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

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.

International Standard IEC 61784-3-6 has been prepared by subcommittee 65C: Industrial networks, of IEC technical committee 65: Industrial process measurement, control and automation.

This second edition cancels and replaces the first edition published in 2007. This edition constitutes a technical revision. The main changes with respect to the previous edition are listed below:

— updates in relation with changes in IEC 61784-3.

This bilingual version published in 2011-12, corresponds to the English version published in 2010-06.

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

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

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

The French version of this standard has not been voted upon.

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

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

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

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

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

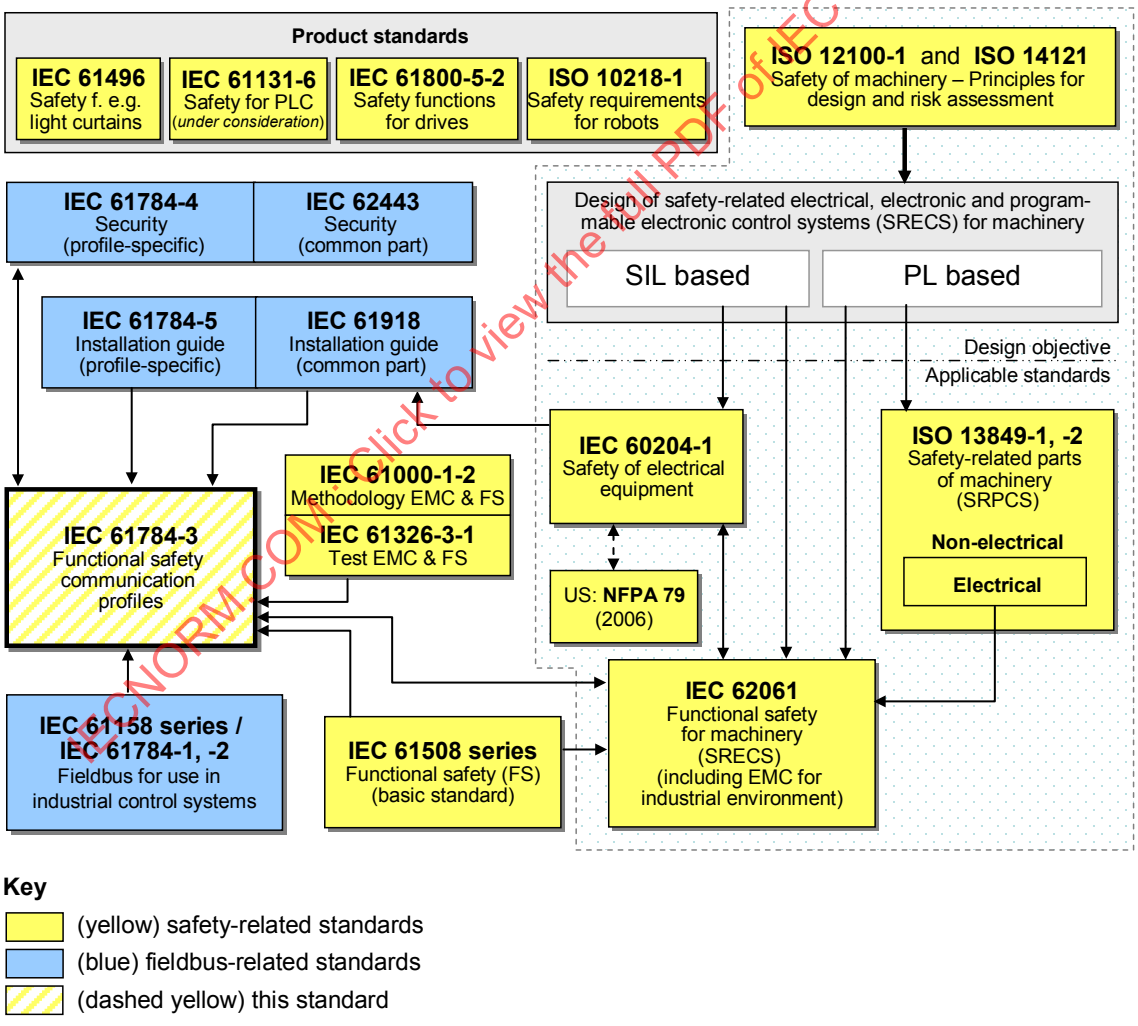
0 Introduction

0.1 General

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

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

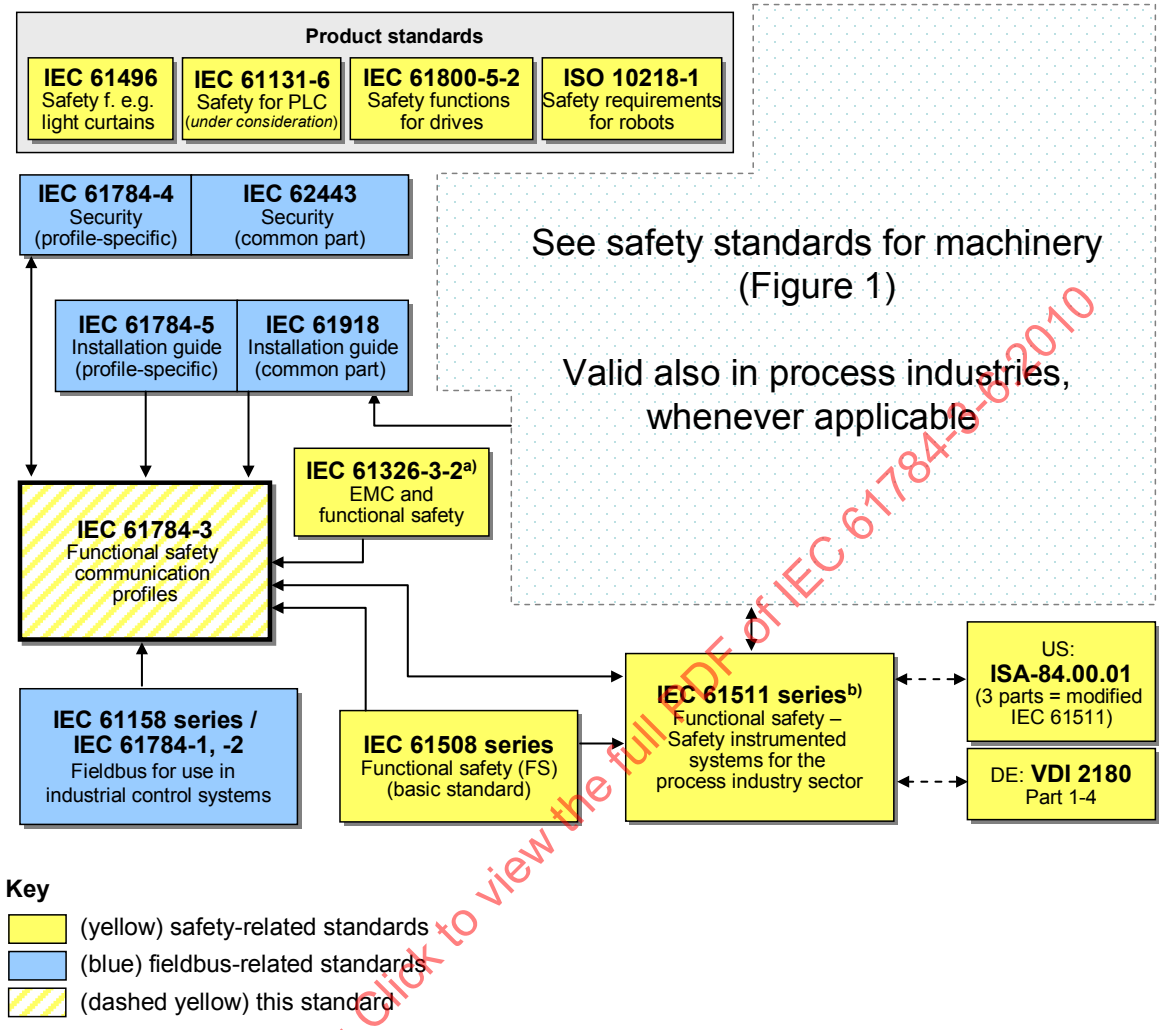
Figure 1 shows the relationships between this standard and relevant safety and fieldbus standards in a machinery environment.



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

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

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



[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.

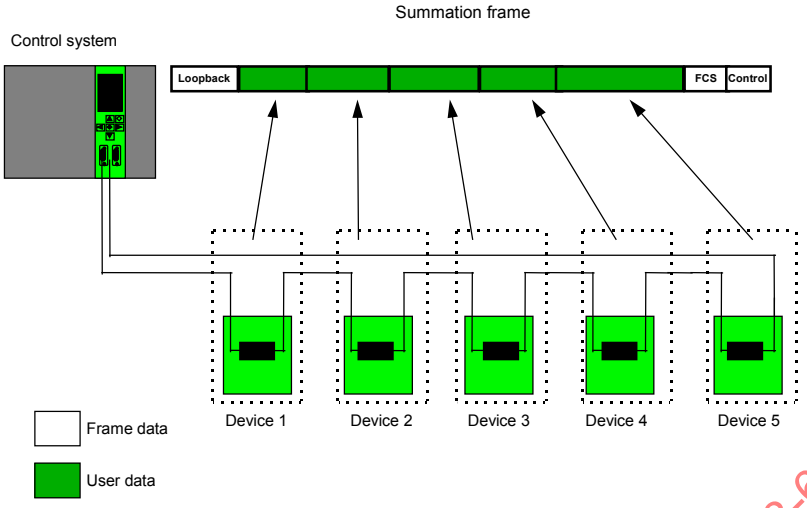


Figure 3 – FSCP 6/7 communication preconditions

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.

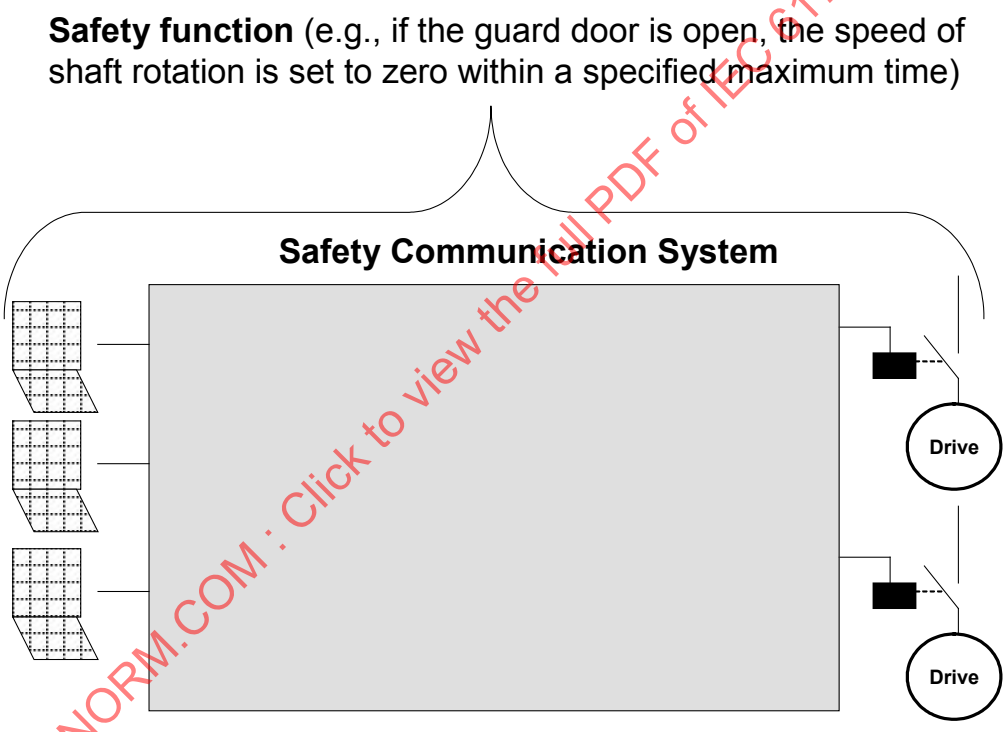


Figure 4 – Example of a safety function

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.

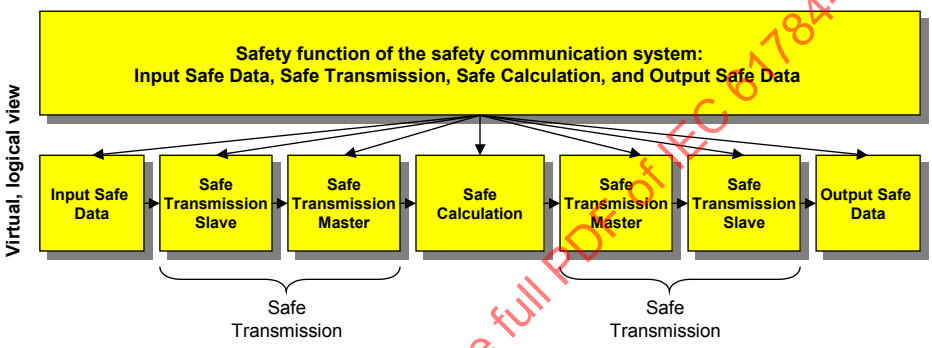


Figure 5 – Decomposition of safety function into function blocks

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.

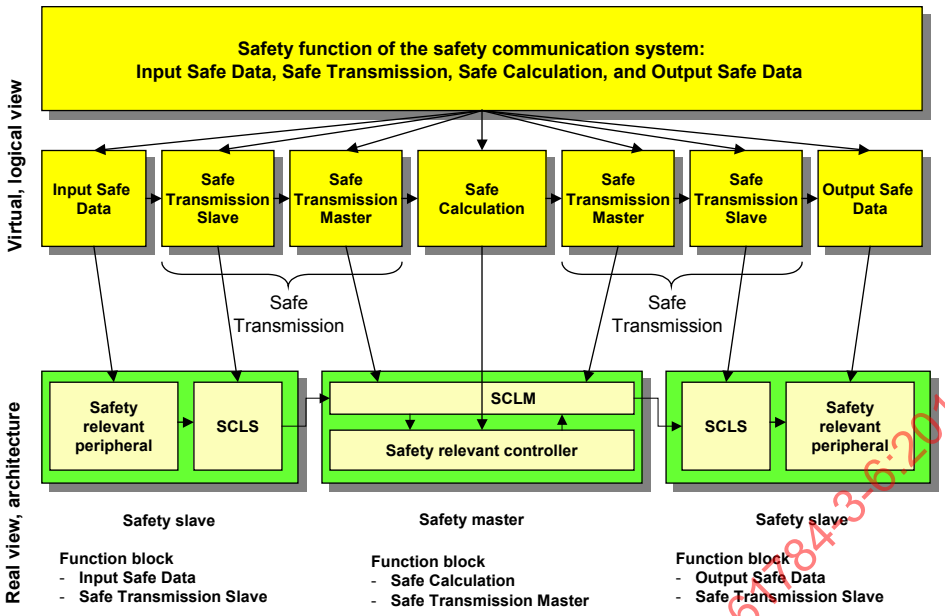


Figure 6 – Overview of the results of the decomposition process

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.

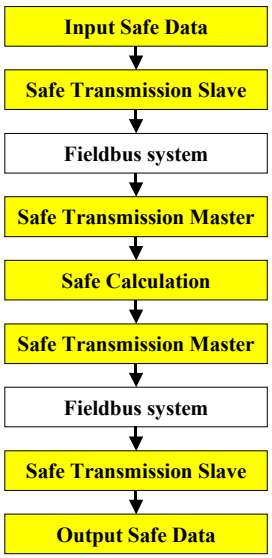


Figure 7 – Signal flow between the function blocks

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.

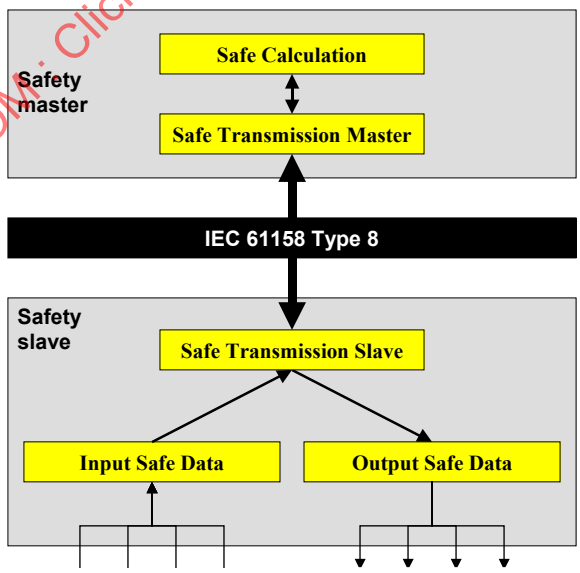


Figure 8 – Interfaces between the safety devices within the safety communication system

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.

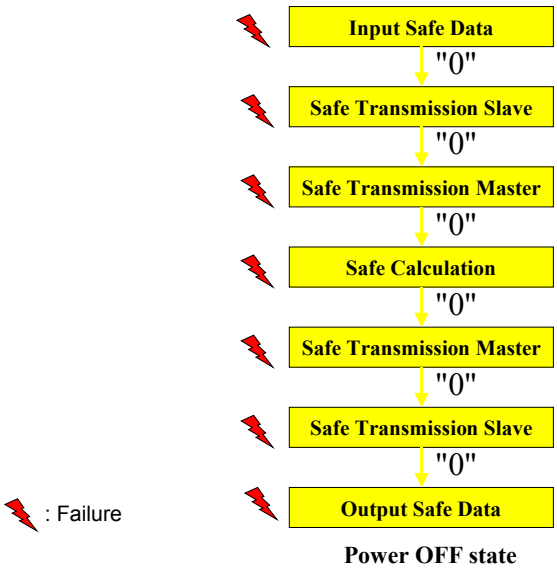


Figure 9 – Signal flow and safe states

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.

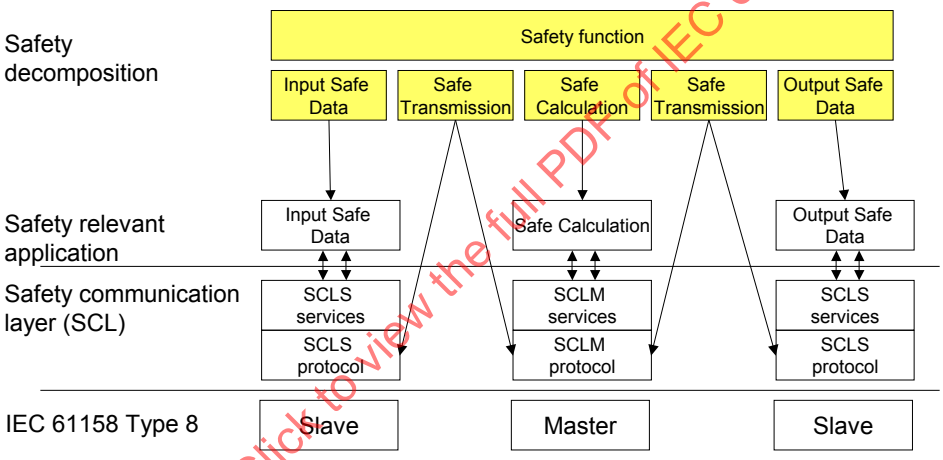


Figure 10 – Mapping of the Safe Transmission function block

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.

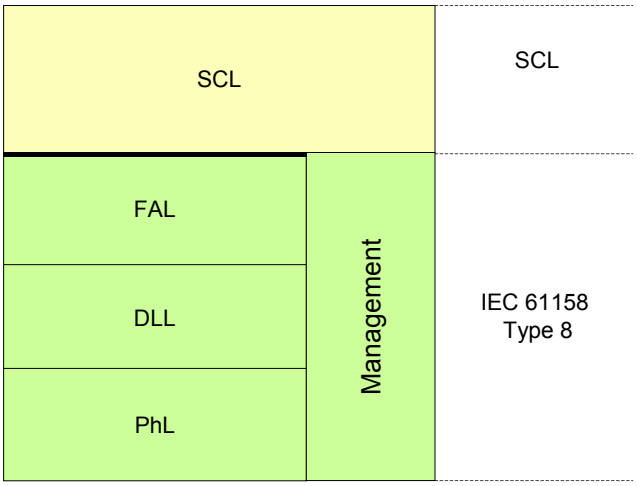


Figure 11 – Relationship between SCL and the other layers of IEC 61158 Type 8

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.

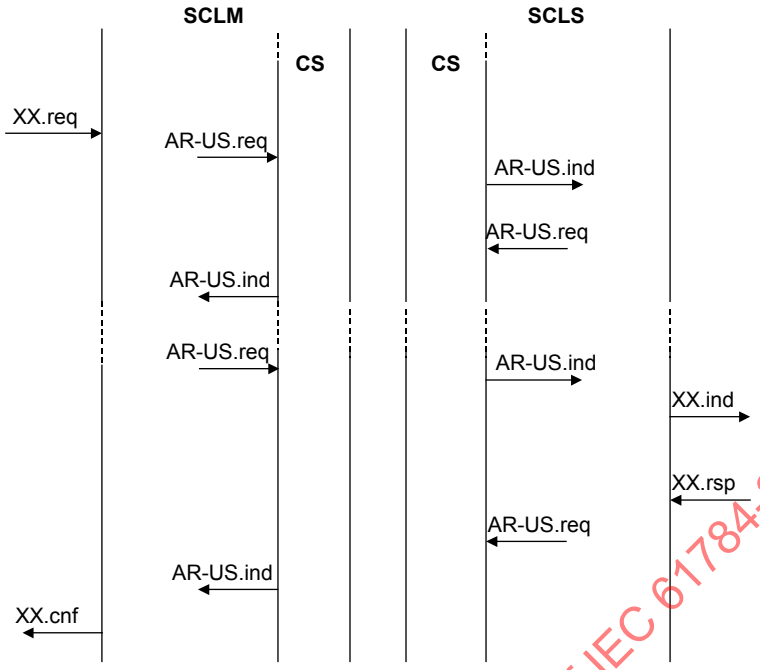


Figure 12 – Use of the AR-US service to initiate and parameterize

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

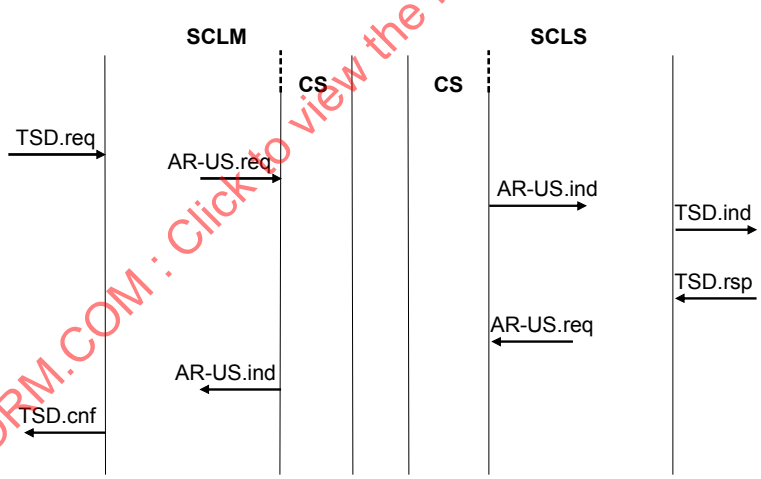


Figure 13 – Use of the AR-US service to transmit safety data

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.

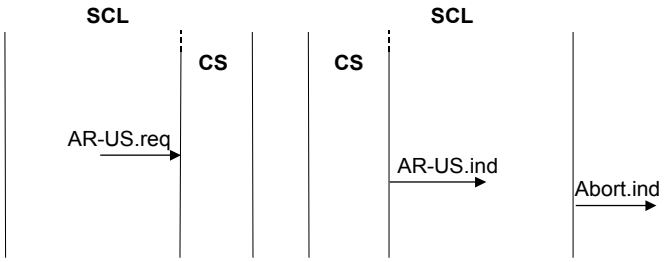


Figure 14 – Use of the AR-US service to abort

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.

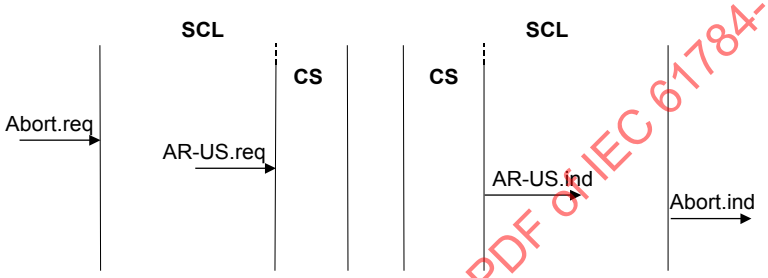


Figure 15 – Use of the AR-US service to abort

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.

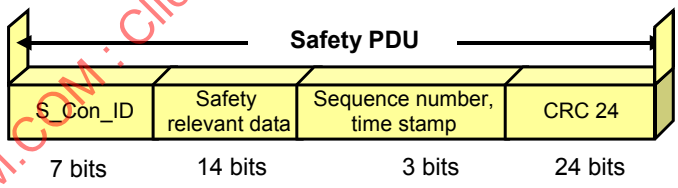


Figure 16 – Structure of the safety PDU

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.

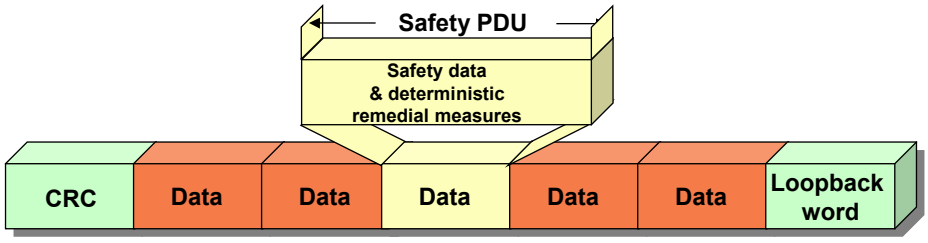


Figure 17 – Integration of safety data and deterministic remedial measures in the summation frame

7.1.2 Description of the polynomial used

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

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

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):

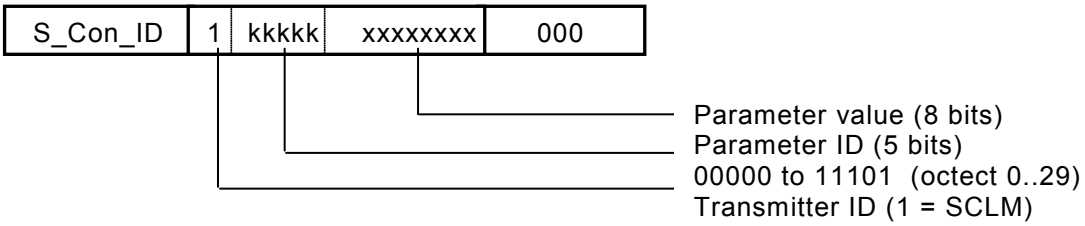


Figure 18 – Write_Parameter_Byte_Req message

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):

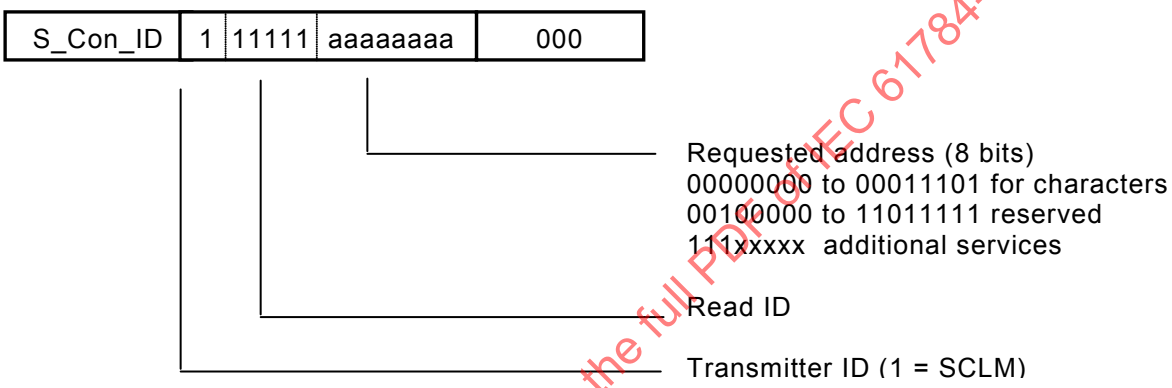


Figure 19 – Read_Parameter_Byte_Req message

7.1.3.2.3 Parameter_Byte_Con

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

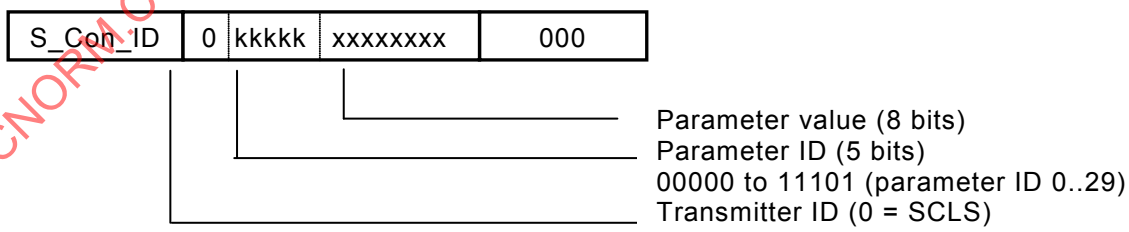


Figure 20 – Parameter_Byte_Con message

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.

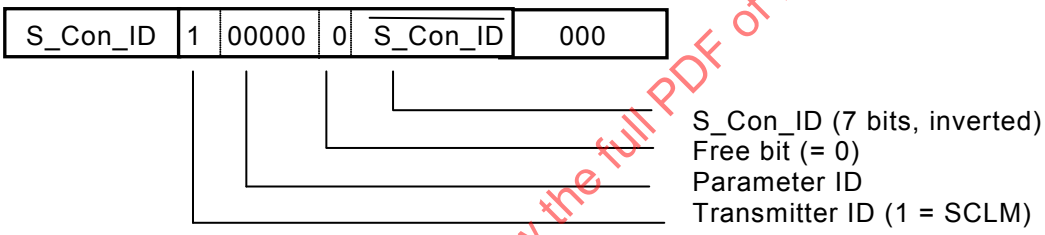


Figure 21 – Set_Safety_Connection_ID_Req message

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 .

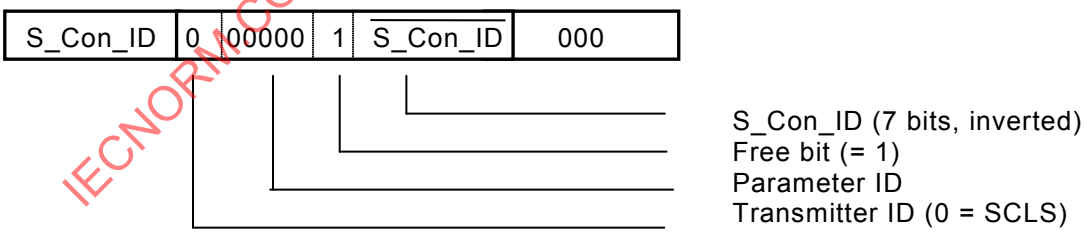


Figure 22 – Set_Safety_Connection_ID_Con message of safety slaves

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.

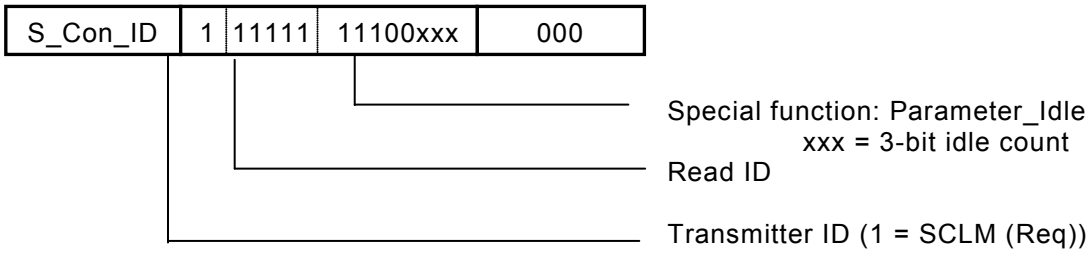


Figure 23 – Parameter_Idle_Req

7.1.3.2.8 Parameter_Idle_Con

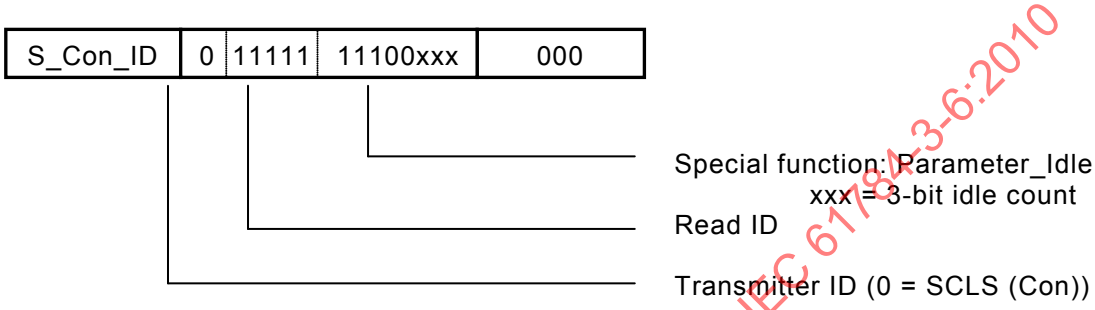


Figure 24 – Parameter_Idle_Con

7.1.3.2.9 Parameter_Check_Con

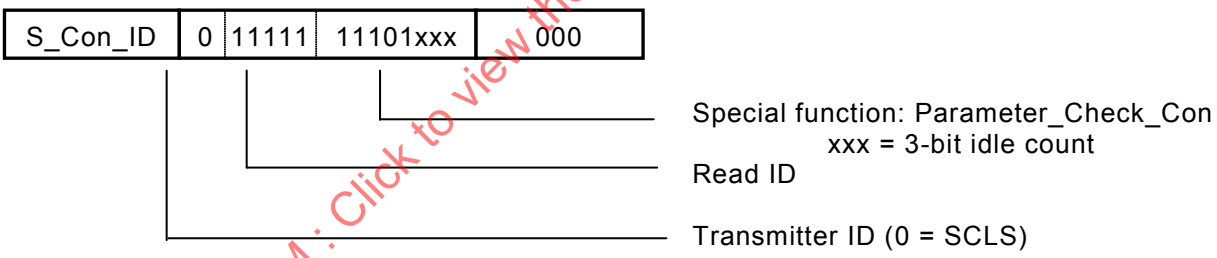


Figure 25 – Parameter_Check_Con

7.1.3.2.10 Parameter_Loc_ID_Changed_Con

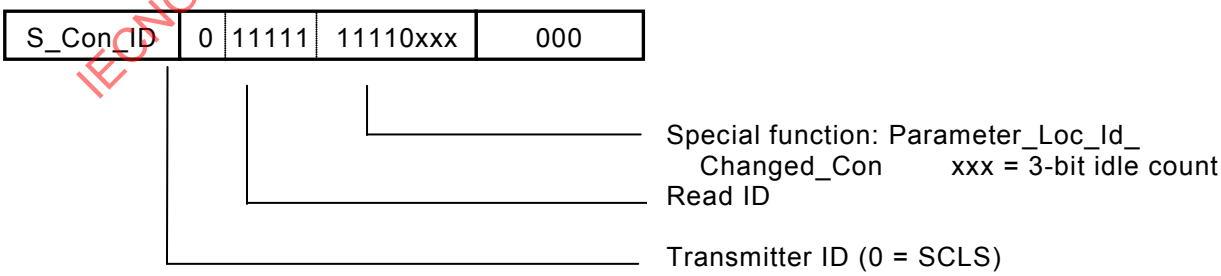


Figure 26 – Parameter_Loc_ID_Changed_Con

7.1.4 Structure of safety messages for the transmission of safety data

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

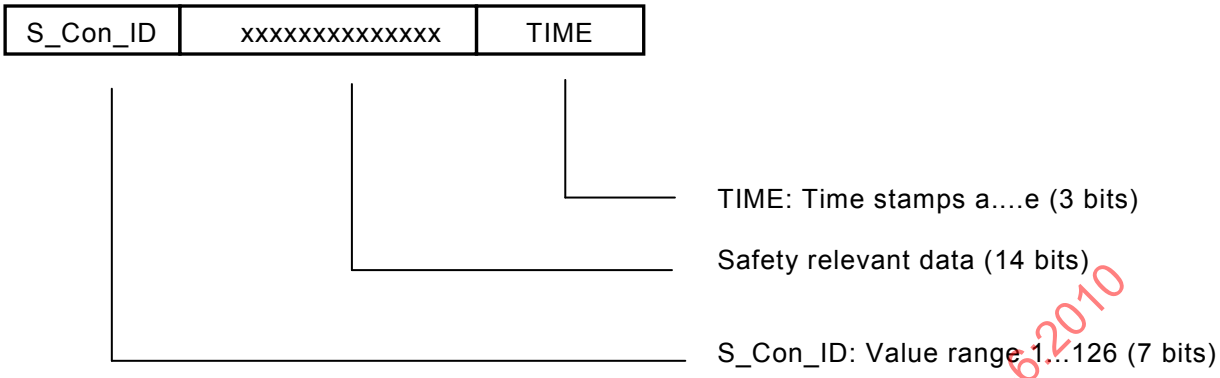


Figure 27 – Transmit Safety Data Message

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.

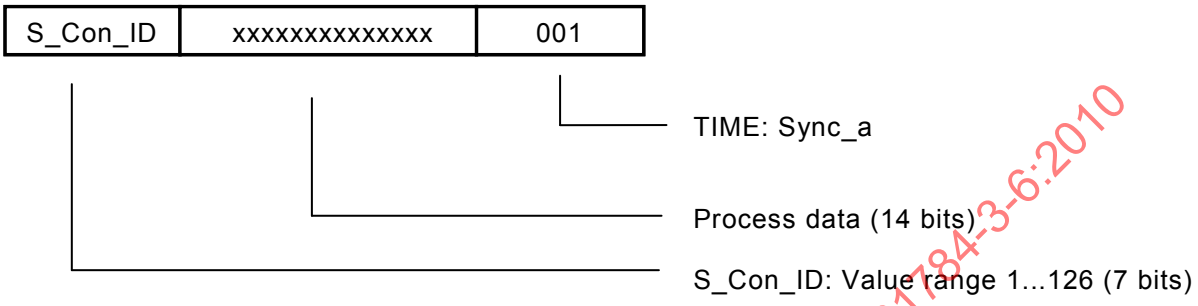


Figure 28 – Sync_a message of the SCLM

7.1.5.2 Req_b message of the SCLM

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

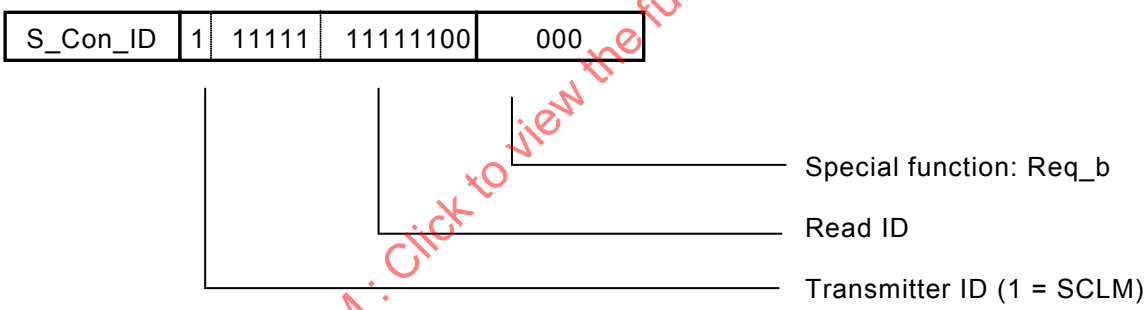


Figure 29 – Req_b message of the SCLM

7.1.5.3 Req_c message of the SCLM

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

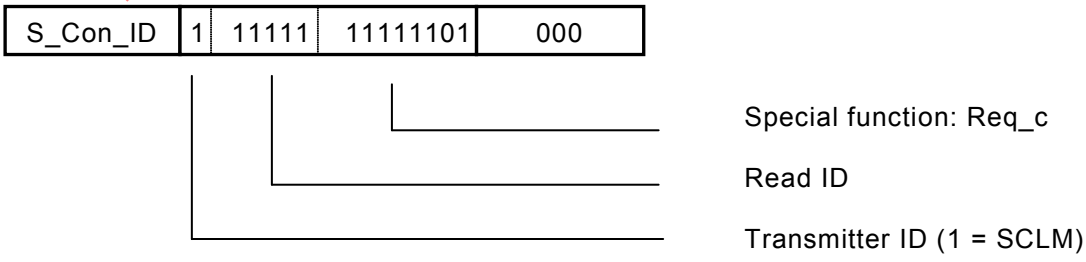


Figure 30 – Req_c message of the SCLM

7.1.5.4 Req_d message of the SCLM

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

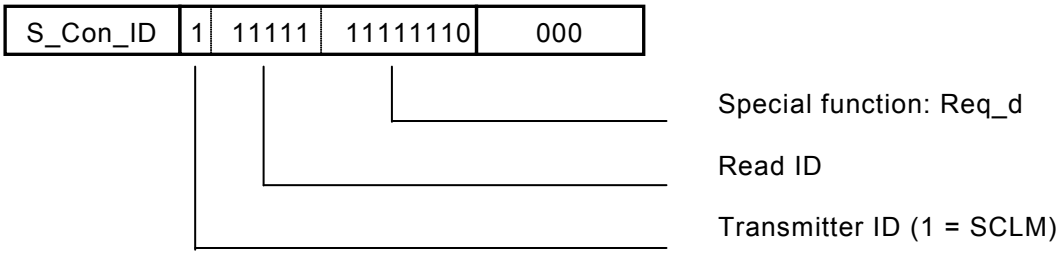


Figure 31 – Req_d message of the SCLM

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.

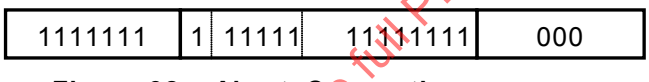
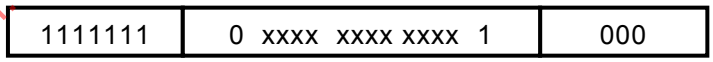


Figure 32 – Abort_Connection message

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.



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.

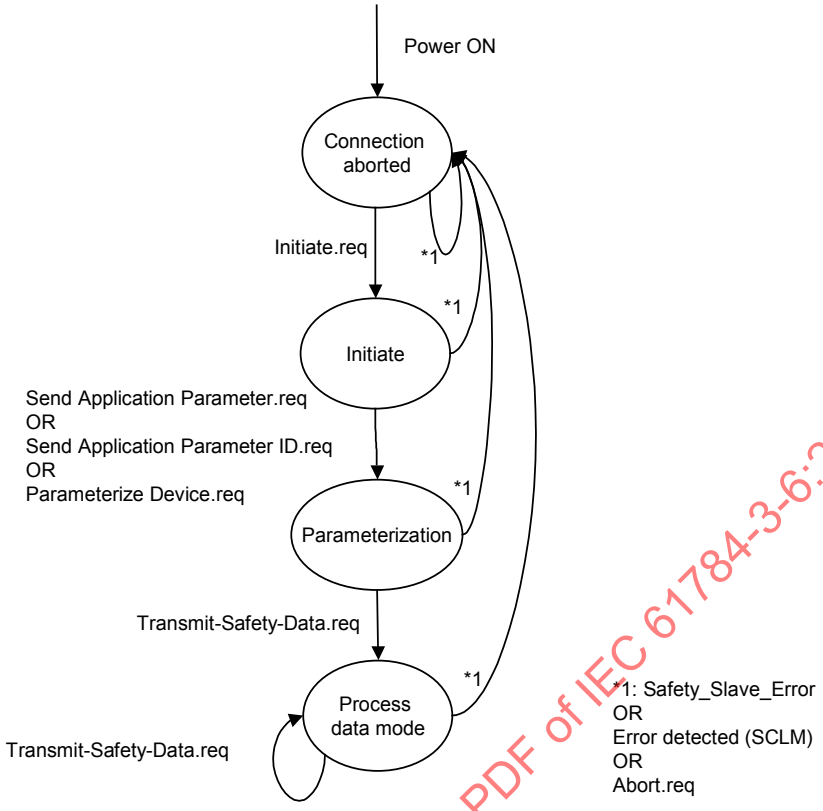


Figure 34 – SCLM state machine

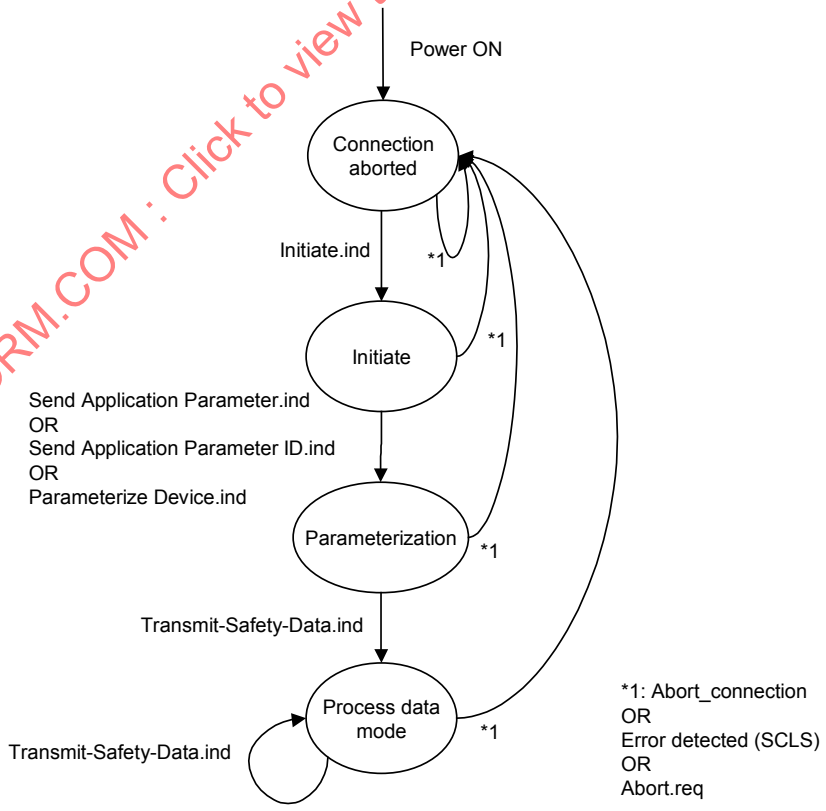


Figure 35 – SCLS state machine

7.2.2 Initiate

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

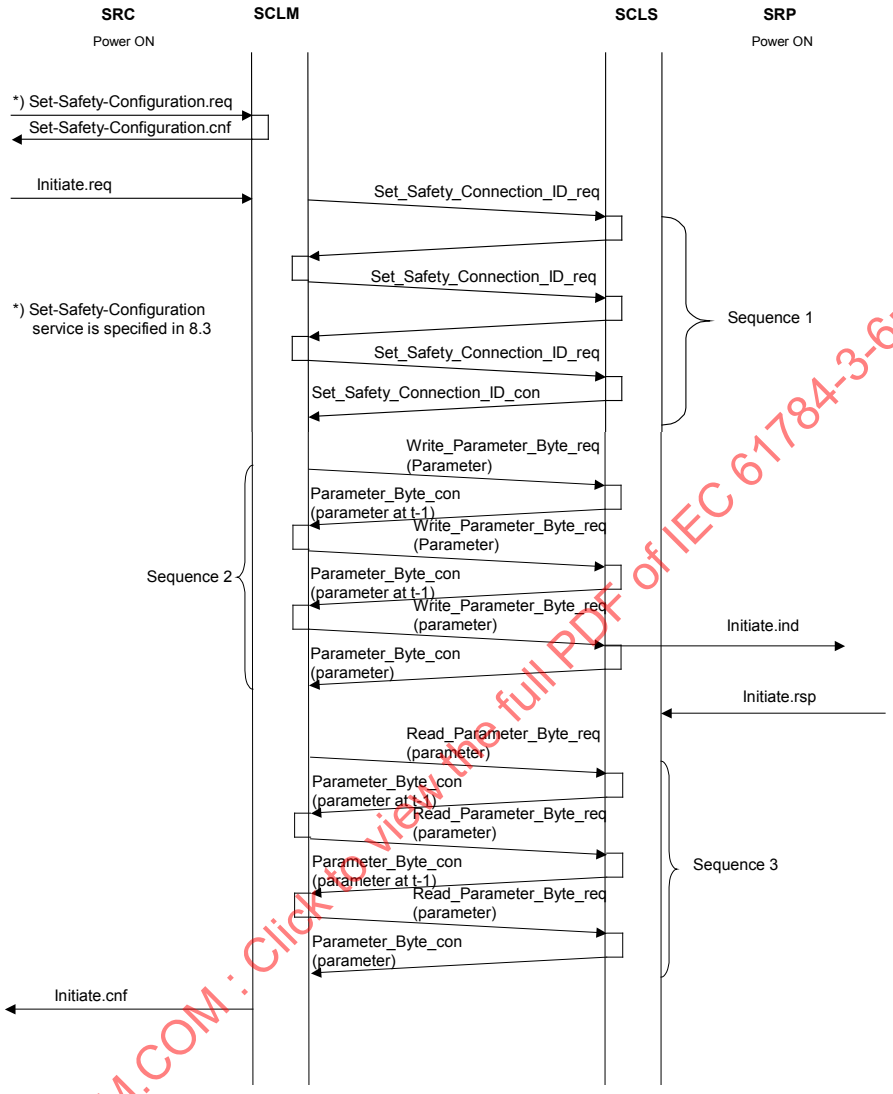


Figure 36 – Initiate sequence

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.

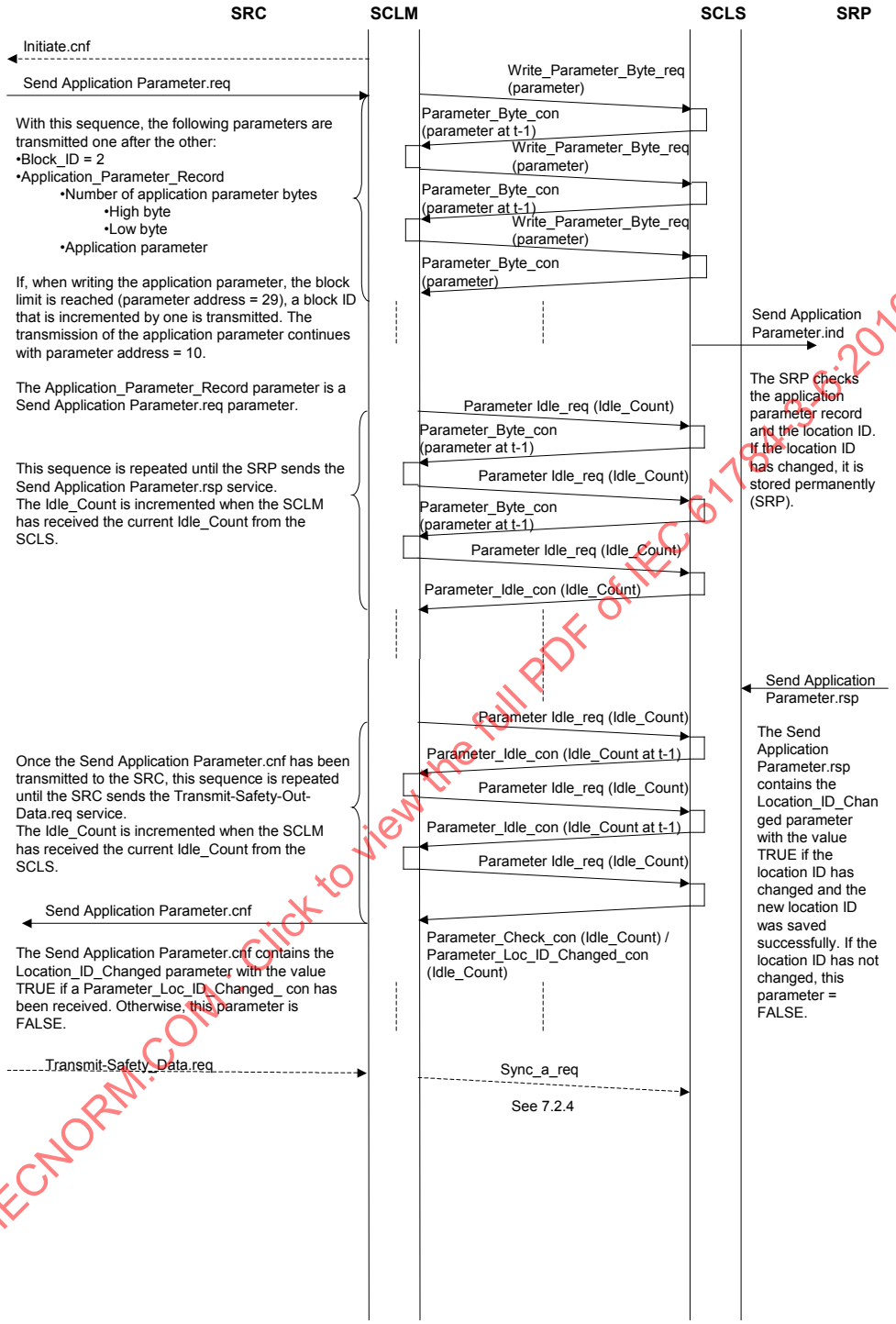


Figure 37 – Send Application Parameter sequence

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

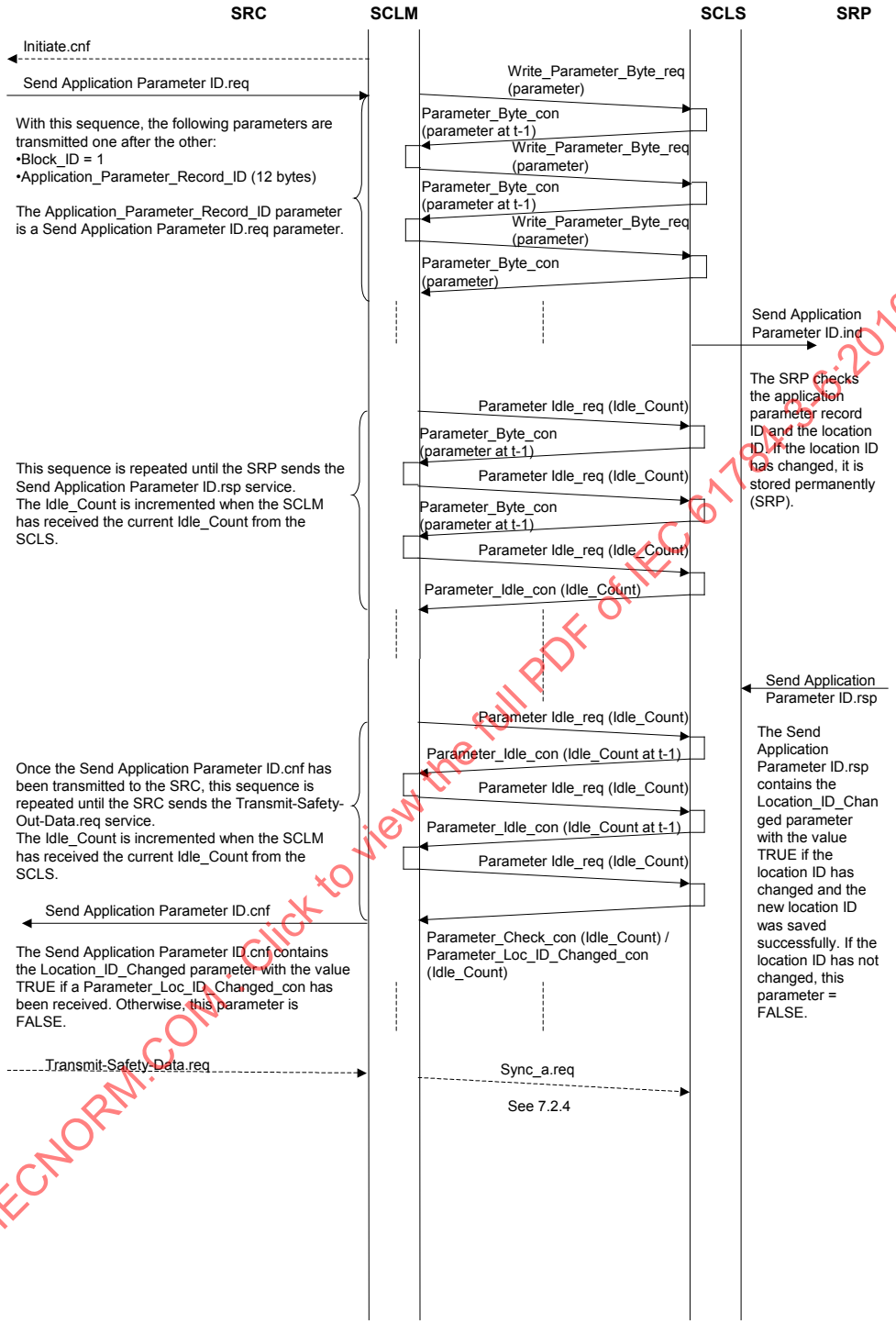


Figure 38 – Send Application Parameter ID sequence

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

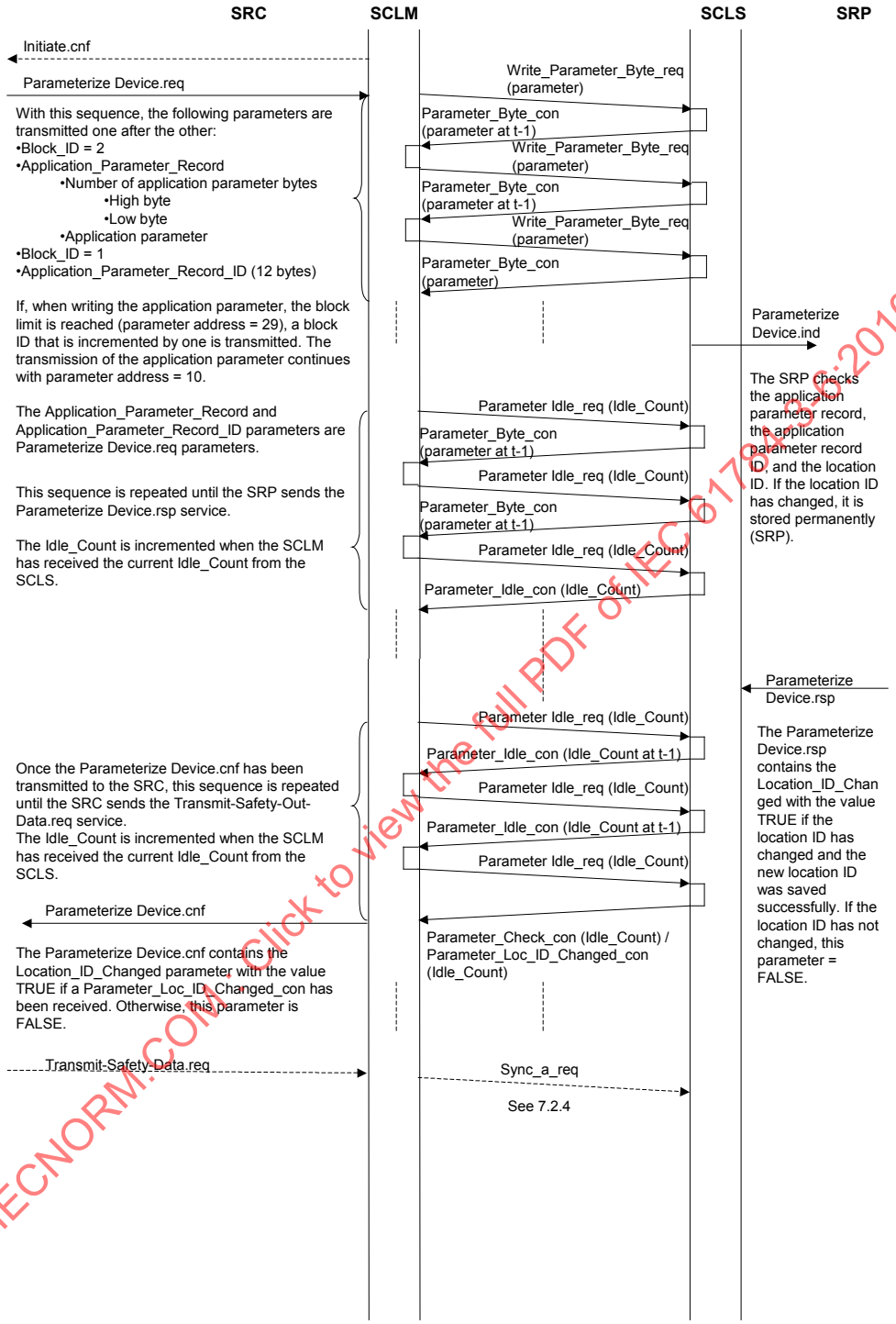


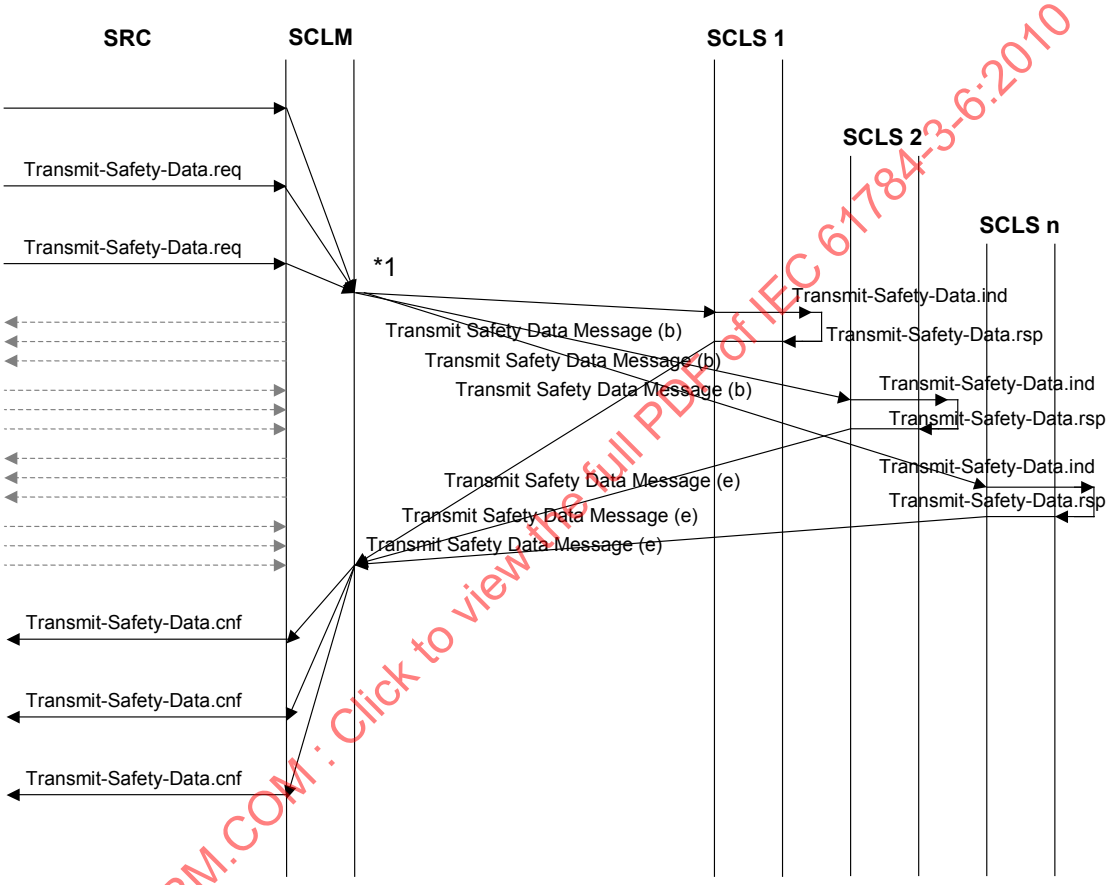
Figure 39 – Parameterize device sequence

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.

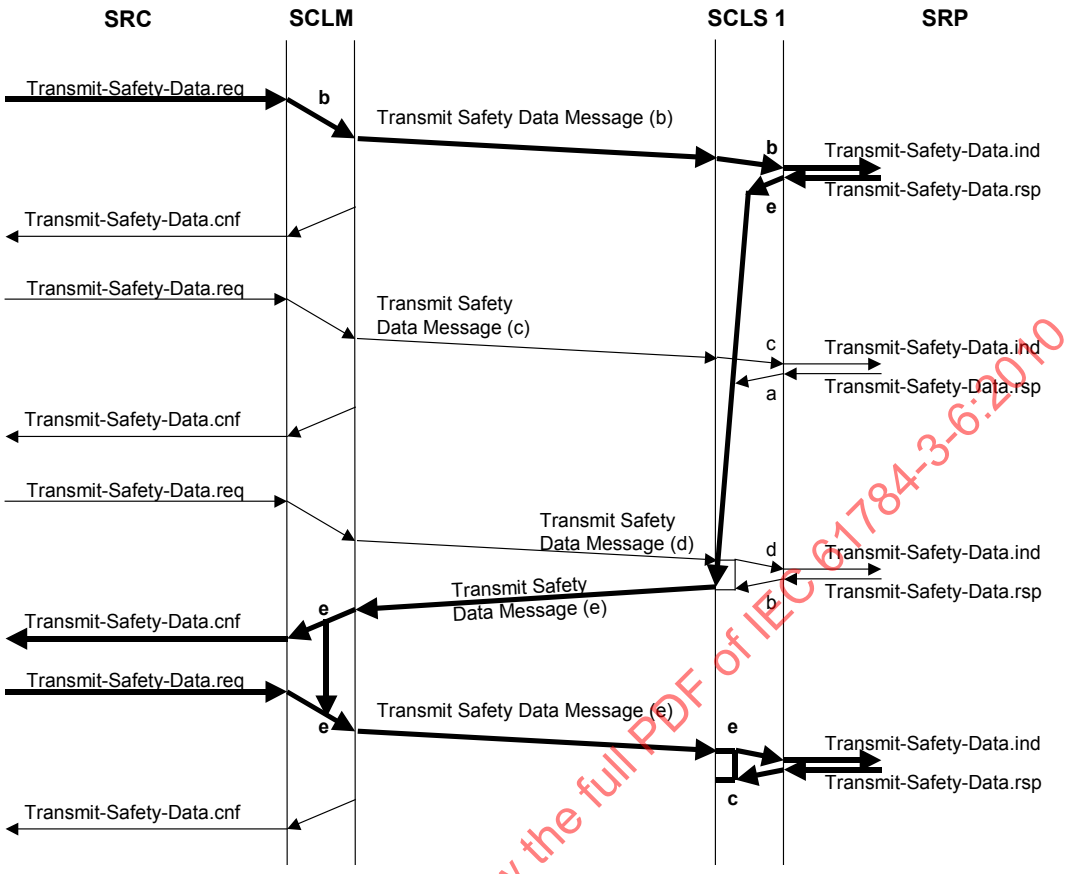


Figure 41 – Use of the sequence number in the SCLM and SCLS

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.

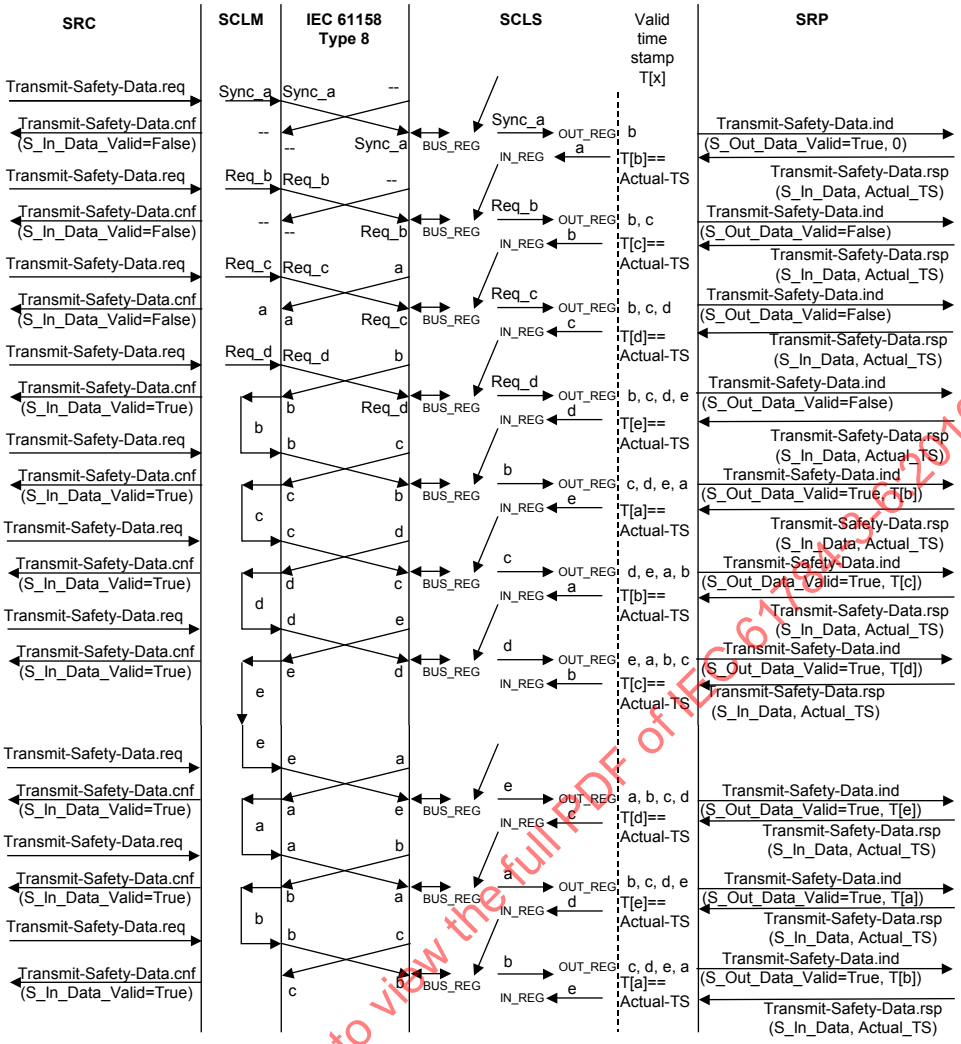


Figure 42 – Startup and error-free operation

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.

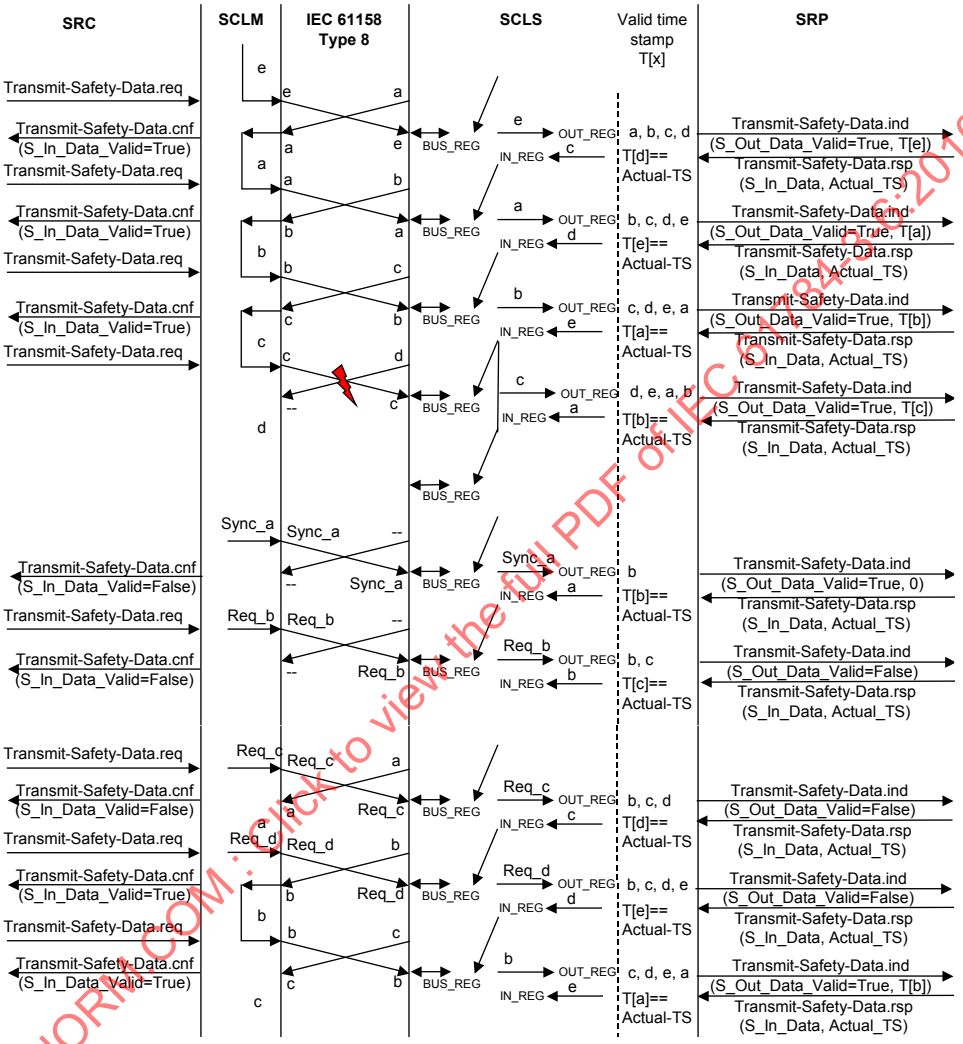


Figure 43 – Resynchronization during operation

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

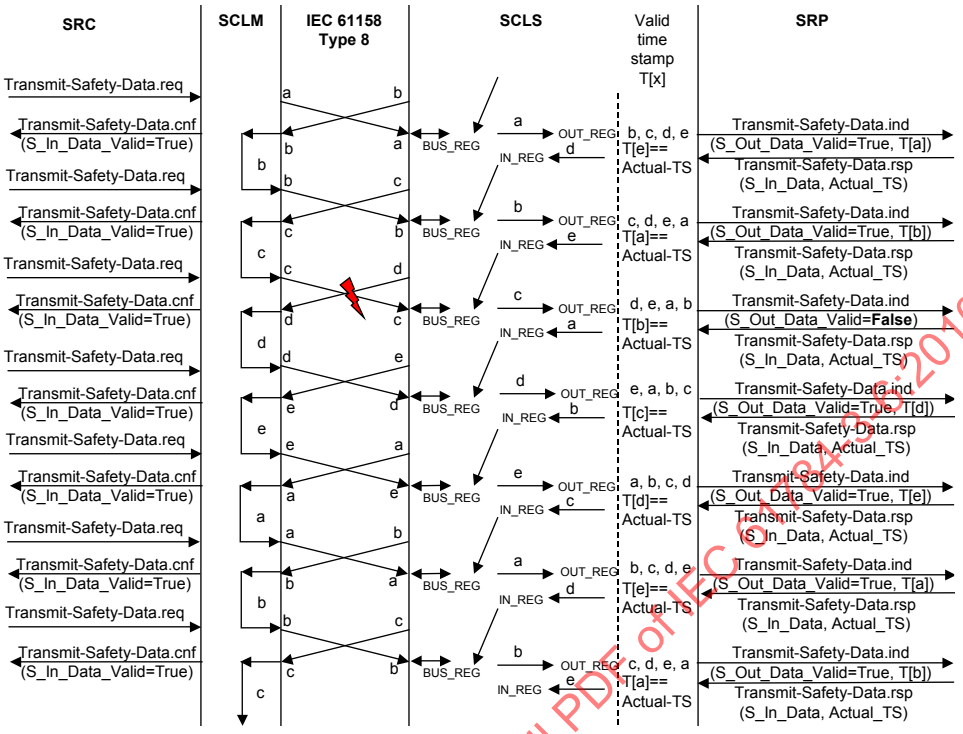


Figure 44 – Invalid CRC 24 checksum detected by the SCLS

7.2.5 Process data mode with diagnostic data transmission

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

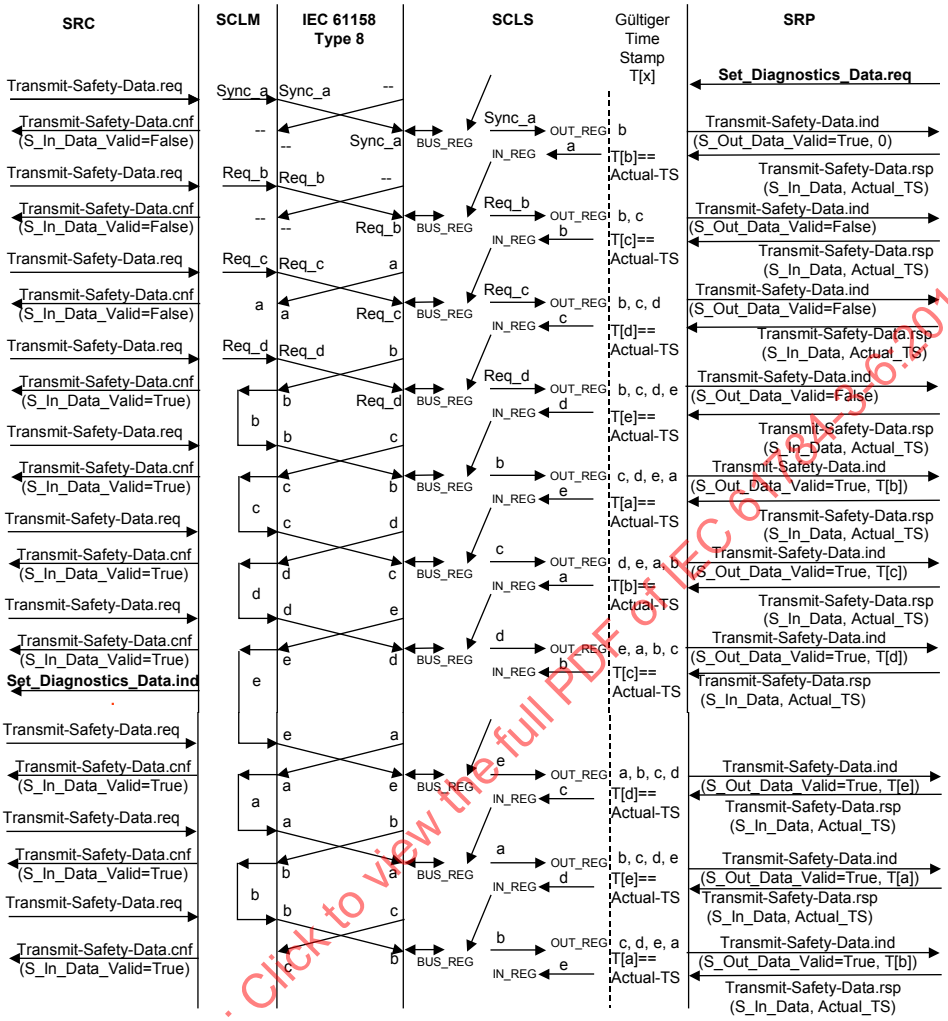


Figure 45 – Process data mode with diagnostic data transmission

7.2.6 Process data mode with Acknowledgement-Data transmission

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

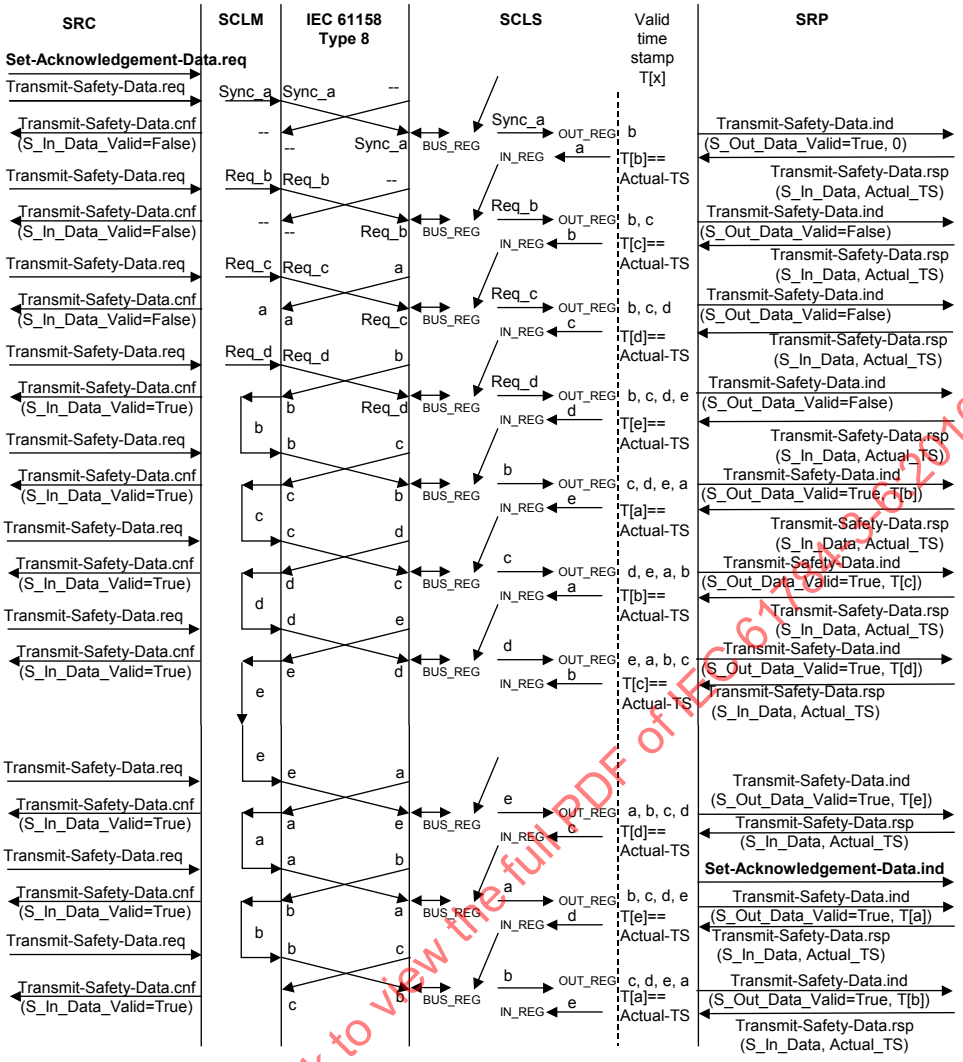


Figure 46 – Process data mode with Acknowledgement-Data transmission

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.

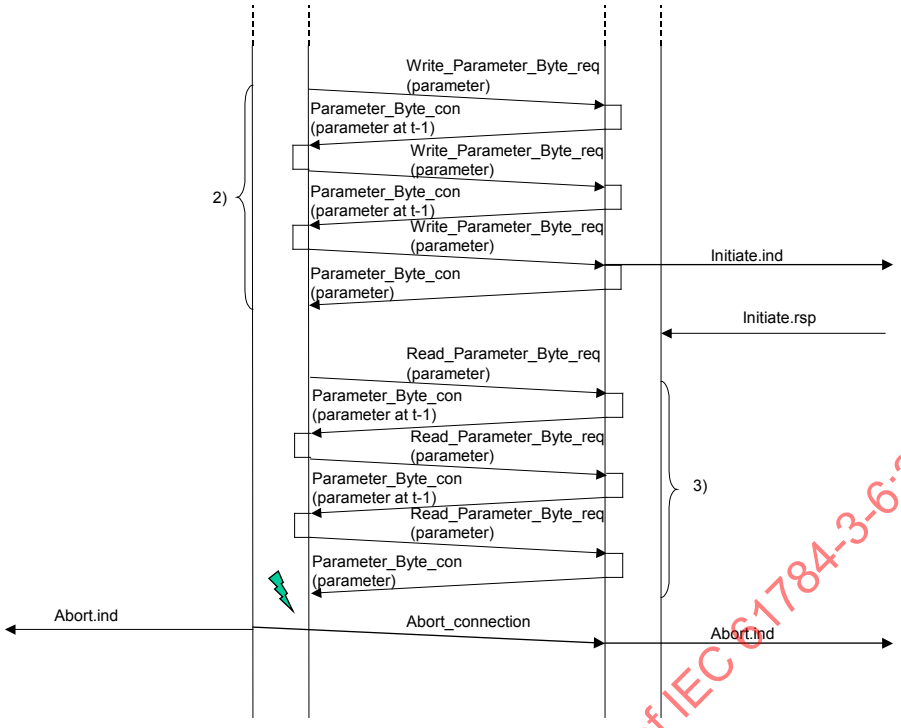


Figure 47 – Error when initiating a connection

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.

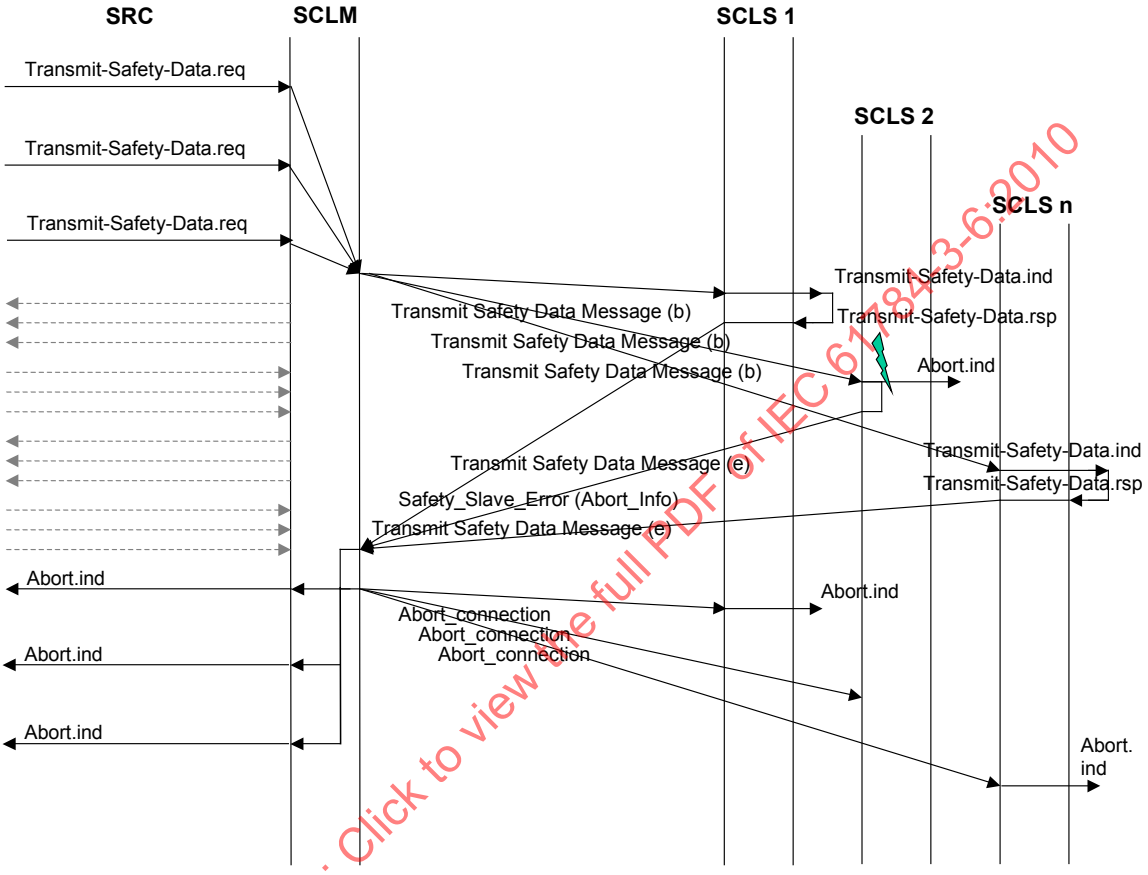


Figure 48 – Error at an SCLS when aborting all connections

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.

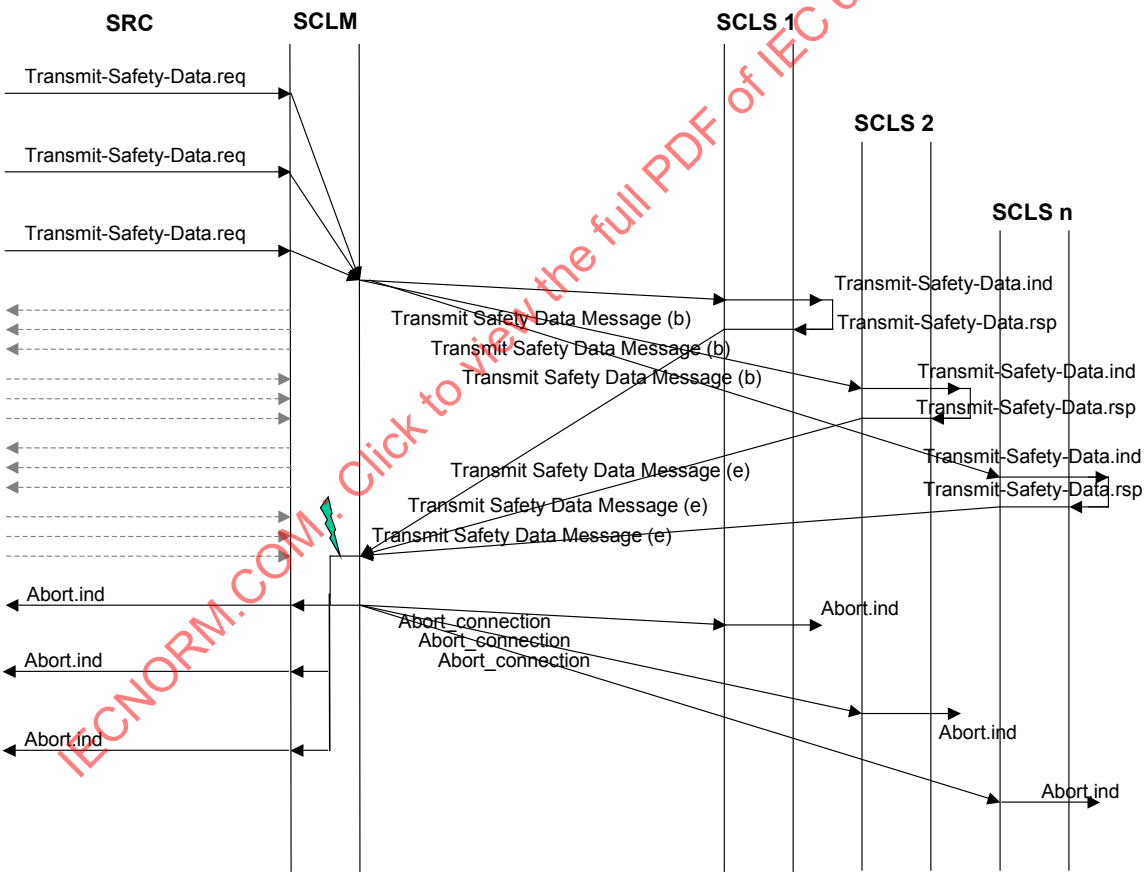


Figure 49 – Abort of all connections in the event of an error detected by the SCLM

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.

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

where

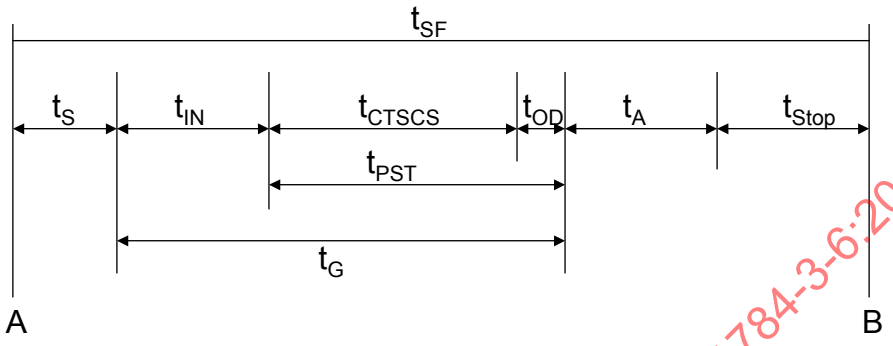
tSF	is the safety function response time (application specific);
tS	is the sensor response time (see information for use of the sensor);
tIN	is the processing time of the safety input (shall be specified from the manufacturer of the safety device and shall be part of the information for use of the safety 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).

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

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).

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

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).

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

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).

$$tPST \geq AF \times tCTSCS + tOD \quad (6)$$

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).

$$tPST \geq AF \times 2\ ms + tOD \quad (7)$$

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).

$$\Lambda SL(Pe) = RSL(Pe) \times \nu \times m \quad (8)$$

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).

$$tIB = 13 \times 6 \times nas \times Tbit \quad (9)$$

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 $\nu \times m$.

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

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)

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

RÉSEAUX DE COMMUNICATION INDUSTRIELS – PROFILS –

Partie 3-6: Bus de terrain de sécurité fonctionnelle – Spécifications supplémentaires pour CPF 6

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (CEI) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de la CEI). La CEI a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, la CEI – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de la CEI"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec la CEI, participent également aux travaux. La CEI collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de la CEI concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de la CEI intéressés sont représentés dans chaque comité d'études.
3) Les Publications de la CEI se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de la CEI. Tous les efforts raisonnables sont entrepris afin que la CEI s'assure de l'exactitude du contenu technique de ses publications; la CEI ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de la CEI s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de la CEI dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de la CEI et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) La CEI elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de la CEI. La CEI n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à la CEI, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de la CEI, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de la CEI ou de toute autre Publication de la CEI, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.

La Norme internationale CEI 61784-3-6 a été établie par le sous-comité 65C: Réseaux de communication industriels, du comité d'études 65 de la CEI: Mesure, commande et automation dans les processus industriels.

Cette seconde édition annule et remplace la première édition publiée en 2007. Cette édition constitue une révision technique. Les principales modifications par rapport à l'édition précédente sont énumérées ci-dessous:

— mises à jour par rapport aux changements apportés à la CEI 61784-3.

La présente version bilingue, correspond à la version anglaise monolingue publiée en 2010-06.

Le texte anglais de cette norme est issu des documents 65C/591A/FDIS et 65C/603/RVD.

Le rapport de vote 65C/603/RVD donne toute information sur le vote ayant abouti à l'approbation de cette norme.

La version française de cette norme n'a pas été soumise au vote.

Cette publication a été rédigée selon les Directives ISO/CEI, Partie 2.

Une liste de toutes les parties de la série CEI 61784-3, présentées sous le titre général *Réseaux de communication industriels – Profils – Bus de terrain de sécurité fonctionnelle*, peut être consultée sur le site Web de la CEI.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de stabilité indiquée sur le site web de la CEI sous "http://webstore.iec.ch" dans les données relatives à la publication recherchée. A cette date, la publication sera

- reconduite,
- supprimée,
- remplacée par une édition révisée, ou
- amendée.

IMPORTANT – Le logo "colour inside" qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

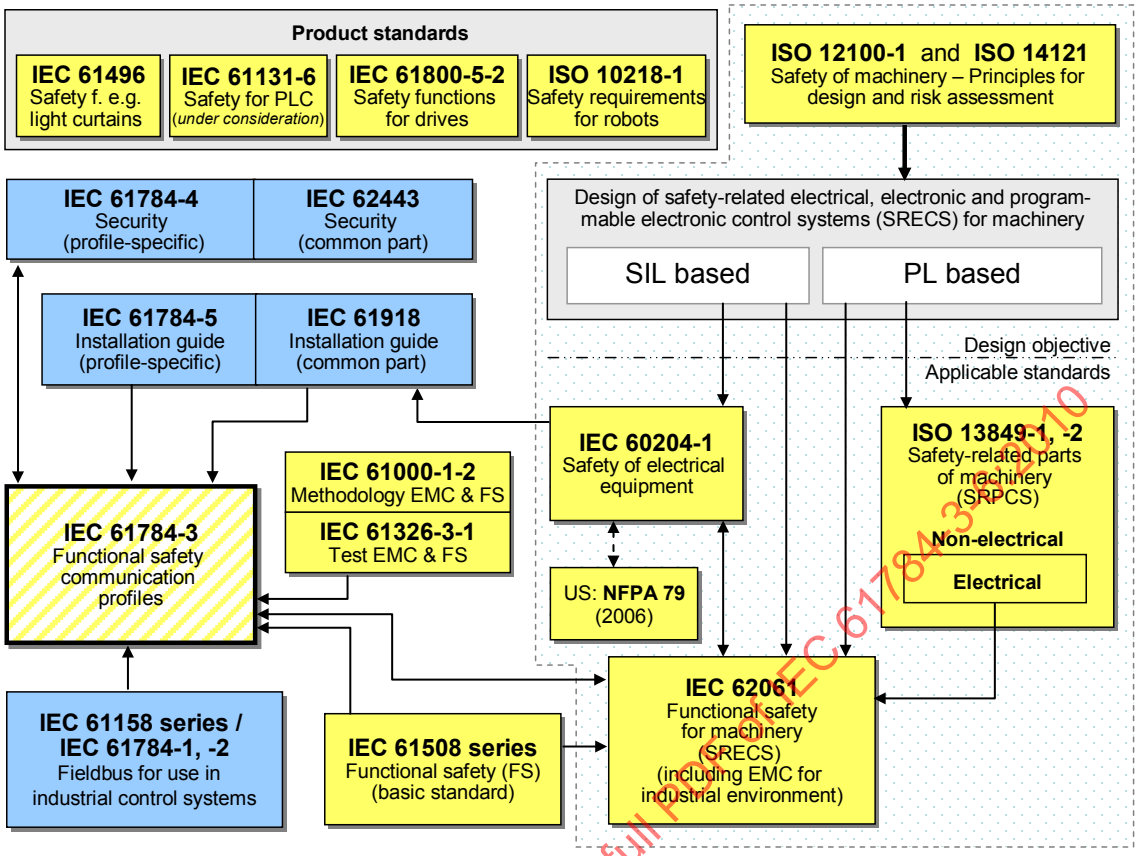
0 Introduction

0.1 Généralités

La norme CEI 61158 relative aux bus de terrain, ainsi que ses normes associées CEI 61784-1 et CEI 61784-2, définit un ensemble de protocoles de communication qui assurent la commande répartie d'applications automatisées. La technologie de bus de terrain est désormais reconnue et bien éprouvée. Ainsi de nombreuses améliorations des bus de terrain se développent pour traiter de domaines non encore normalisés tels que les applications en temps réel relatives à la sécurité et à la sûreté.

La présente norme définit les principes pertinents applicables aux communications en termes de sécurité fonctionnelle en référence à la série CEI 61508, et spécifie plusieurs couches de communication de sécurité (profils et protocoles correspondants) basées sur les profils de communication et les couches de protocole de la CEI 61784-1, la CEI 61784-2 et la série CEI 61158. Elle ne couvre pas les aspects relatifs à la sécurité électrique et à la sécurité intrinsèque.

La Figure 1 illustre les relations entre la présente norme et les normes pertinentes relatives à la sécurité et au bus de terrain dans un environnement machines.



Key

(yellow) safety-related standards

(blue) fieldbus-related standards

(dashed yellow) this standard

Légende

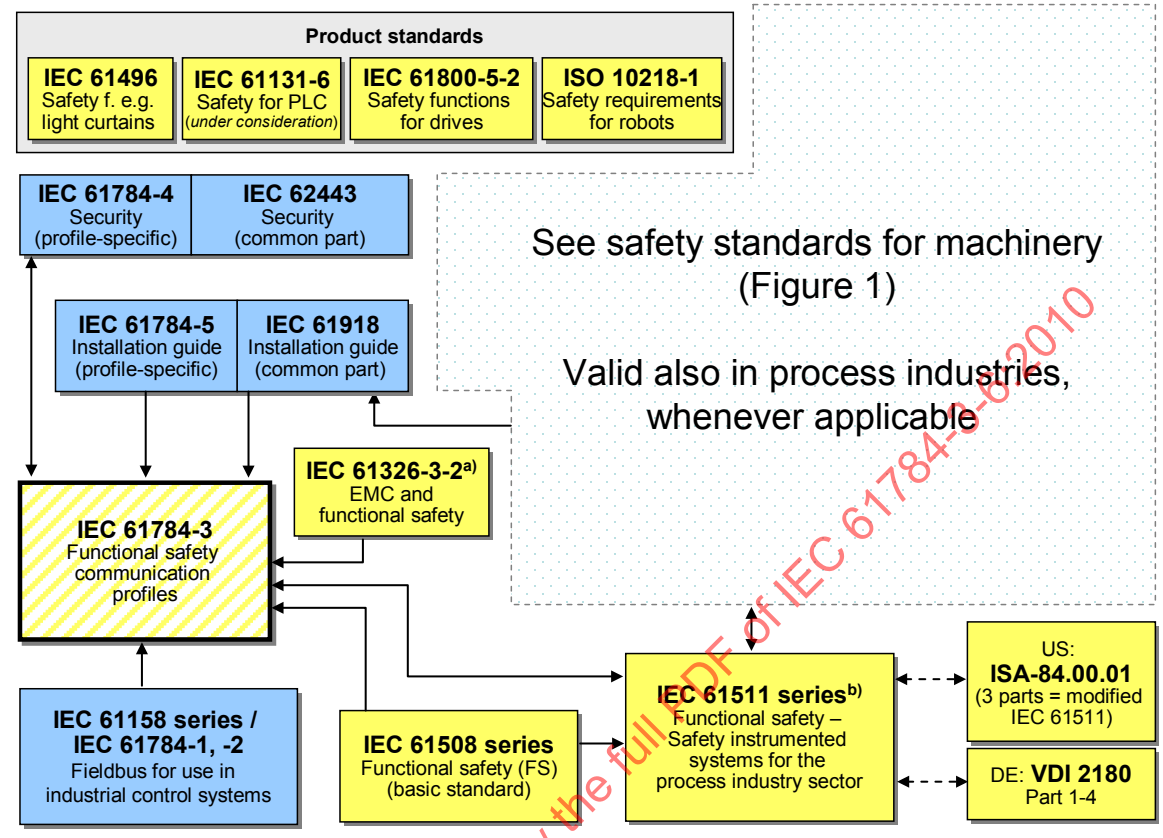
Anglais	Français
Product standards	Normes de produits
Safety function, e.g. light curtains	Fonction de sécurité, par exemple barrières photo électriques
Safety for PLC (under consideration)	Sécurité relative aux automates programmables (à l'étude)
Safety functions for drives	Fonctions de sécurité applicables aux entraînements
Safety requirements for robots	Exigences de sécurité applicables aux robots
Safety of machinery – principles for design and risk assessment	Sécurité des machines – principes généraux de conception et d'appréciation du risque
Security (profile-specific)	Sûreté (spécifique au profil)
Security (common part)	Sûreté (partie commune)
Design of safety-related electrical, electronic and programmable electronic control systems for machinery	Conception des systèmes de commande électriques, électroniques et électroniques programmables relatifs à la sécurité pour les machines
SIL based	Basé sur SIL
PL based	Basé sur PL
Installation guide (profile-specific)	Guide d'installation (spécifique au profil)
Installation guide (common part)	Guide d'installation (partie commune)

Anglais	Français
Design objective	Objectif de conception
Applicable standards	Normes applicables
Safety of electrical equipment	Sécurité des équipements électriques
Safety-related parts of machinery	Parties des systèmes de commande relatives à la sécurité
Non-electrical	Non électrique
Electrical	Electrique
Methodology EMC & functional safety	Méthodologie en matière de compatibilité électromagnétique & sécurité fonctionnelle
Test EMC & functional safety	Essai CEM et sécurité fonctionnelle
Functional safety communication profiles	Profils de communication de sécurité fonctionnelle
IEC 61158 series / IEC 61784-1,-2 Fieldbus for use in industrial control systems	Série CEI 61158 / CEI 61784-1,-2 Bus de terrain pour utilisation dans des systèmes de commande industriels
IEC 61508 series, Functional safety (basic standard)	Série CEI 61508 Sécurité fonctionnelle (norme de base)
Functional safety for machinery (SRECS) including EMC for industrial environment)	Sécurité fonctionnelle des systèmes de commande électriques, électroniques et électroniques programmables (y compris les interférences électromagnétiques dans l'environnement industriel)
Key	Légende
(yellow) safety-related standards	(jaune) normes relatives à la sécurité
(blue) fieldbus-related standards	(bleu) normes relatives au bus de terrain
(dashed) yellow) this standard	(jaune pointillé) la présente norme

NOTE Les paragraphes 6.7.6.4 (haute complexité) et 6.7.8.1.6 (faible complexité) de la CEI 62061 spécifient la relation entre PL (catégorie) et SIL.

Figure 1 - Relation entre la CEI 61784–3 et d'autres normes (machines)

La Figure 2 illustre les relations entre la présente norme et les normes pertinentes relatives à la sécurité et au bus de terrain dans un environnement de transformation.



Key

(yellow) safety-related standards
(blue) fieldbus-related standards
(dashed yellow) this standard

Légende

Anglais	Français
Product standards	Normes de produits
Safety function, e.g. light curtains	Fonction de sécurité, par exemple barrières photo électriques
Safety for PLC (under consideration)	Sécurité relative aux automates programmables (à l'étude)
Safety functions for drives	Fonctions de sécurité applicables aux entraînements
Safety requirements for robots	Exigences de sécurité applicables aux robots
Security (profile-specific)	Sûreté (spécifique au profil)
Security (common part)	Sûreté (partie commune)
Installation guide (profile-specific)	Guide d'installation (spécifique au profil)
Installation guide (common part)	Guide d'installation (partie commune)
See safety standards for machinery (Figure 1)	Voir normes de sécurité pour les machines (Figure 1)
Valid also in process industries, whenever applicable	Valable également dans les industries de transformation, le cas échéant
Functional safety communication profiles	Profils de communication de sécurité fonctionnelle

Anglais	Français
IEC 61326-3-2 [a)] EMC and functional safety	CEI 61326-3-2 [a)] CEM & sécurité fonctionnelle
IEC 61158 series/ IEC 61784-1-2, Fieldbus for use in industrial control systems	Série CEI 61158/ CEI 61784-1,-2 Bus de terrain pour utilisation dans des systèmes de commande industriels
IEC 61508 series, Functional safety (basic standard)	Série CEI 61508 Sécurité fonctionnelle (norme de base)
IEC 61511 series[b)] Functional safety–safety instrumented systems for the process industry sector	Série CEI 61511[b)] sécurité fonctionnelle – systèmes instrumentés de sécurité pour le secteur des industries de transformation
US: ISA 84.00.1 (3 parts = modified IEC 61511)	US: ISA 84.00.1 (3 parties = CEI 61511 modifiée)
DE : VDI 2180 Part 1 –4	DE : VDI 2180 Parties 1 à 4
Key	Légende
(yellow) safety-related standards	(jaune) normes relatives à la sécurité
(blue) fieldbus-related standards	(bleu) normes relatives au bus de terrain
(dashed) yellow) this standard	(jaune pointillé) la présente norme

[a] Pour des environnements électromagnétiques spécifiés, sinon CEI 61326-3-1.

[b] EN ratifiée.

Figure 2 - Relations entre la CEI 61784–3 et d'autres normes (transformation)

Les couches de communication de sécurité mises en œuvre dans la trame de systèmes relatifs à la sécurité conformément à la série CEI 61508, assurent la confiance nécessaire à accorder à la transmission de messages (information) entre deux participants ou plus sur un bus de terrain dans un système relatif à la sécurité, ou une fiabilité suffisante dans le comportement de sécurité en cas d'erreurs ou de défaillances du bus de terrain.

Les couches de communication de sécurité spécifiées dans la présente norme permettent de garantir cette assurance en utilisant un bus de terrain dans des applications nécessitant une sécurité fonctionnelle jusqu'au niveau d'intégrité de sécurité (SIL) spécifié par son profil de communication de sécurité fonctionnelle correspondant.

La revendication du SIL qui en résulte pour un système dépend de la mise en œuvre du profil de communication de sécurité fonctionnelle retenu au sein du système – la mise en œuvre du profil de communication de sécurité fonctionnelle dans un dispositif normal ne suffit pas à le qualifier de dispositif de sécurité.

La présente norme décrit:

— les principes de base de mise en œuvre des exigences de la série CEI 61508 pour les communications de données relatives à la sécurité, y compris les défauts de transmission potentiels, les mesures correctives et les considérations concernant l'intégrité des données;

— la description individuelle des profils de sécurité fonctionnelle pour plusieurs familles de profils de communication dans les CEI 61784-1 et CEI 61784-2;

— les extensions de la couche de sécurité aux sections relatives au service et aux protocoles de communication de la série CEI 61158.

0.2 Déclaration de droits de propriété

La commission électrotechnique internationale (CEI) attire l'attention sur le fait qu'il est déclaré que la conformité avec le présent document peut impliquer l'utilisation de brevets concernant les profils de communication de sécurité fonctionnelle pour la famille 6, où la notation [xx] désigne le détenteur des droits de propriété.

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

La CEI ne prend pas position eu égard à la preuve, la validité et la portée de ces droits de propriété.

Les détenteurs de ces droits de propriété ont donné l'assurance à la CEI qu'ils consentent à négocier des licences avec des demandeurs du monde entier, en des termes et à des conditions raisonnables et non discriminatoires. A ce propos, la déclaration des détenteurs de ces droits de propriété est enregistrée à la CEI.

Des informations peuvent être obtenues auprès de:

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

L'attention est attirée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété autres que ceux mentionnés ci-dessus. La CEI ne doit pas être tenue pour responsable de ne pas avoir dûment signalé tout ou partie de ces droits de propriété.

RÉSEAUX DE COMMUNICATION INDUSTRIELS – PROFILS –

Partie 3-6: Bus de terrain de sécurité fonctionnelle – Spécifications supplémentaires pour CPF 6

1 Domaine d'application

La présente partie de la série CEI 61784-3 spécifie une couche de communication relative à la sécurité (services et protocole) fondée sur la CPF 6 de la CEI 61784-1, de la CEI 61784-2 et le Type 8 de la CEI 61158. Elle identifie les principes applicables aux communications de sécurité fonctionnelle définies dans la CEI 61784-3, et appropriés à cette couche de communication de sécurité.

NOTE 1 Elle ne couvre pas les aspects relatifs à la sécurité électrique et à la sécurité intrinsèque. La sécurité électrique concerne les dangers tels que les chocs électriques. La sécurité intrinsèque concerne les dangers associés aux atmosphères explosibles.

La présente partie[1] définit les mécanismes de transmission des messages propres à la sécurité entre les participants d'un réseau réparti, en utilisant la technologie de bus de terrain conformément aux exigences de la série CEI 61508[2] concernant la sécurité fonctionnelle. Ces mécanismes peuvent être utilisés dans diverses applications industrielles, telles que la commande de processus, l'usinage automatique et les machines.

La présente partie fournit des lignes directrices tant pour les développeurs que pour les évaluateurs de dispositifs et systèmes conformes.

NOTE 2 La revendication du SIL qui en résulte pour un système dépend de la mise en œuvre du profil de communication de sécurité fonctionnelle retenu au sein du système – la mise en œuvre du profil de communication de sécurité fonctionnelle, conforme à la présente partie, dans un dispositif normal ne suffit pas à le qualifier de dispositif de sécurité.

2 Références normatives

Les documents de référence suivants sont indispensables pour l'application du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

CEI 60204-1, *Sécurité des machines – Équipement électrique des machines – Partie 1 : Règles générales*

IEC 61131-3, *Programmable controllers – Part 3: Programming languages* (disponible en anglais uniquement)

IEC 61158 (all parts), *Industrial communication networks – Fieldbus specifications* (disponible uniquement en anglais)

CEI 61158-2, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 2 : Spécification de couche physique et définition des services*

---

1 Dans les pages suivantes de la présente norme, "la présente partie" se substitue à "cette partie de la série CEI 61784-3".

2 Dans les pages suivantes de la présente norme, "CEI 61508" se substitue à "série CEI 61508".

IEC 61158-3–8, *Industrial communication networks – Fieldbus specifications – Part 3-8: Data-link layer service definition – Type 8 elements* (disponible uniquement en anglais)

IEC 61158-4–8, *Industrial communication networks – Fieldbus specifications – Part 4-8: Data-link layer protocol specification – Type 8 elements* (disponible uniquement en anglais)

IEC 61158-5–8 :2007, *Industrial communication networks – Fieldbus specifications – Part 5-8: Application layer service definition – Type 8 elements* (disponible uniquement en anglais)

IEC 61158-6–8, *Industrial communication networks – Fieldbus specifications – Part 6-8: Application layer protocol specification – Type 8 elements* (disponible uniquement en anglais)

CEI 61508 (toutes parties), *Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité*

CEI 61511 (toutes parties), *Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur des industries de transformation*

CEI 61784-1, *Réseaux de communication industriels – Profils – Partie 1: Profils de bus de terrain*

CEI 61784-2, *Réseaux de communication industriels – Profils – Partie 2 : Profils de bus de terrain supplémentaires pour les réseaux en temps réel basés sur l'ISO/CEI 8802-3*

CEI 61784-3:2010[3], *Réseaux de communication industriels – Profils – Partie 3 : Bus de terrain de sécurité fonctionnelle – Règles générales et définitions de profil*

IEC 61784-5-6, *Industrial communication networks – Profiles – Part 5: Installation of fieldbuses – Installation profiles for CPF 6* (disponible uniquement en anglais)

IEC 61918, *Industrial communication networks – Installation of communication networks in industrial premises* (disponible uniquement en anglais)

CEI 62061, *Sécurité des machines – Sécurité fonctionnelle des systèmes de commande électriques, électroniques et électroniques programmables relatifs à la sécurité*

ISO 12100-1, *Sécurité des machines – Notions fondamentales, principes généraux de conception – Partie 1: Terminologie de base, méthodologie*

ISO 13849-1, *Sécurité des machines – Parties des systèmes de commande relatives à la sécurité – Partie 1 : Principes généraux de conception*

3 Termes, définitions, symboles, abréviations et conventions

3.1 Termes et définitions

Pour les besoins du présent document, les termes et définitions suivants s'appliquent.

---

3 En cours d'élaboration.

3.1.1 Termes et définitions communs

3.1.1.1
disponibilité
probabilité, pour un système automatisé, qu'il ne se produise pas de conditions opérationnelles non satisfaisantes, telles que la perte de production, pendant une période donnée

3.1.1.2
système de communication
disposition de matériels, logiciels et vecteurs de propagation destinée à permettre la transmission de *messages* (ISO/CEI 7498, couche d'application) d'une application à une autre

3.1.1.3
connexion
liaison logique entre deux objets d'application de dispositifs identiques ou différents

3.1.1.4
contrôle de redondance cyclique (CRC[4])
<valeur> donnée redondante déduite, et enregistrée ou transmise simultanément, d'un bloc de données afin de détecter toute corruption des données

<méthode> procédure utilisée pour calculer les données redondantes

NOTE 1 Les termes « code CRC » et « signature CRC », et les étiquettes telles que CRC1, CRC2, peuvent également être utilisés dans la présente norme pour se référer aux données redondantes.

NOTE 2 Voir également [32], [33][5].

3.1.1.5
erreur
écart ou discordance entre une valeur ou une condition calculée, observée ou mesurée, et la valeur ou la condition vraie, prescrite ou théoriquement correcte

[CEI 61508-4:2010[6]], [CEI 61158]

NOTE 1 Les erreurs peuvent être causées par des erreurs de conception du matériel/logiciel et/ou des informations altérées du fait de perturbations électromagnétiques et/ou autres effets.

NOTE 2 Les erreurs ne produisent nécessairement pas une *défaillance* ou une *panne*.

3.1.1.6
défaillance
cessation de l'aptitude d'une unité fonctionnelle à accomplir une fonction requise ou fonctionnement d'une unité fonctionnelle d'une toute autre manière que celle requise

NOTE 1 La définition de la CEI 61508-4 est identique avec des notes complémentaires.

[CEI 61508-4:2010, modifiée], [ISO/CEI 2382-14.01.11, modifiée]

NOTE 2 Une défaillance peut être causée par une *erreur* (par exemple, problème de conception matérielle/logicielle ou rupture de message).

3.1.1.7
panne
condition anormale susceptible de provoquer la réduction ou la perte de la capacité d'une unité fonctionnelle à accomplir une fonction requise

---

4 CRC = *Cyclic Redundancy Check*

5 Les chiffres entre crochets font référence à la bibliographie.

6 A publier.

NOTE Le VEI 191-05-01 définit la « panne » comme un état caractérisé par l'incapacité à accomplir une fonction requise, à l'exclusion de l'incapacité au cours de la période de maintenance préventive ou autres actions planifiées, ou du fait de l'absence de ressources externes.

[CEI 61508-4:2010, modifiée], [ISO/CEI 2382-14.01.10, modifiée]

3.1.1.8
bus de terrain
système de communication basé sur le transfert de données en série et utilisé dans des applications d'automatisation industrielle ou de commande de processus

3.1.1.9
système de bus de terrain
système utilisant un *bus de terrain* avec des dispositifs reliés

3.1.1.10
trame
synonyme discrédité de DLPDU

3.1.1.11
séquence de contrôle de trame (FCS[7])
données redondantes issues d'un bloc de données d'un DLPDU (trame), utilisant une fonction de hachage, et enregistrées ou transmises avec le bloc de données, afin de déterminer l'altération des données

NOTE 1 Il est possible de calculer une FCS à l'aide, par exemple, d'un CRC ou d'une autre fonction de hachage.

NOTE 2 Voir également [32], [33].

3.1.1.12
fonction de hachage
fonction (mathématique) de mise en correspondance des valeurs d'un ensemble (éventuellement) très grand de valeurs en une plage de valeurs (habituellement) plus petite

NOTE 1 Les fonctions de hachage peuvent être utilisées pour déterminer l'altération des données.

NOTE 2 Les fonctions de hachage courantes incluent la parité, la somme de contrôle ou le CRC.

[CEI/TR 62210, modifiée]

3.1.1.13
danger
état ou ensemble de conditions d'un système qui, avec d'autres conditions associées, entraîne inévitablement un préjudice pour les personnes, les biens ou l'environnement

3.1.1.14
maître
entité de communication active capable d'initier et de programmer des activités de communication effectuées par d'autres stations qui peuvent être des maîtres ou des esclaves

3.1.1.15
message
série ordonnée d'octets destinée à communiquer des informations
[ISO/CEI 2382-16.02.01, modifiée]

7 FCS = *Frame Check Sequence*

3.1.1.16
niveau de performance (PL[8])
niveau discret utilisé pour spécifier la capacité des parties relatives à la sécurité des systèmes de commande à accomplir une fonction de sécurité dans des conditions prévisibles [ISO 13849-1]

3.1.1.17
très basse tension de protection (TBTP)
circuit électrique dans lequel la tension ne peut pas dépasser 30 V eff. en c.a., 42,4 V crête ou 60 V en c.c. dans des conditions normales de premier défaut, à l'exception des défauts à la terre dans d'autres circuits

NOTE Un circuit TBTP est similaire à un circuit TBTS relié à la terre de protection.

[CEI 61131-2]

3.1.1.18
redondance
existence de moyens, outre les moyens qui se révèleraient suffisants pour qu'une unité fonctionnelle accomplisse une fonction requise ou que des données représentent une information

NOTE La définition de la CEI 61508-4 est identique, avec des exemples et des notes supplémentaires.

[CEI 61508-4:2010, modifiée], [ISO/CEI 2382-14.01.12, modifiée]

3.1.1.19
datation (horodatage) relative
datation référencée par rapport à l'horloge locale d'une entité

NOTE En général, il n'y a pas de relation avec les horloges des autres entités.

[CEI 62280-2, modifiée]

3.1.1.20
fiabilité
probabilité qu'un système automatisé puisse accomplir une fonction requise, dans des conditions données, pendant un intervalle de temps donné (t1, t2)

NOTE 1 On suppose en général que le système automatisé est en état d'accomplir la fonction requise au début de l'intervalle de temps donné.

NOTE 2 Le terme "fiabilité" est aussi employé pour désigner l'aptitude caractérisée par cette probabilité.

NOTE 3 Au cours de la période MTBF ou MTTF, la probabilité qu'un système automatisé exécute une fonction requise dans les conditions données décroît.

NOTE 4 La fiabilité est différente de la disponibilité.

[CEI 62059-11, modifiée]

3.1.1.21
risque
combinaison de la probabilité d'occurrence d'un dommage ou préjudice et de la gravité de ce dernier

NOTE Pour plus d'informations sur ce concept, se reporter à l'Annexe A de la CEI 61508-5:2010[9].

[CEI 61508-4:2010], [ISO/CEI Guide 51:1999, définition 3.2]

---

8 PL = *Performance Level*

9 A publier.

3.1.1.22
couche de communication de sécurité (SCL[10])
couche de communication qui comprend toutes les mesures nécessaires permettant d'assurer la transmission de données en toute sécurité conformément aux exigences de la CEI 61508

3.1.1.23
connexion de sécurité
connexion qui utilise le protocole de sécurité pour des transactions de communications

3.1.1.24
données de sécurité
données transmises par un réseau de sécurité utilisant un protocole de sécurité

NOTE La couche de communication de sécurité ne garantit pas la sécurité des données proprement dites, mais uniquement la transmission en toute sécurité de ces dernières.

3.1.1.25
dispositif de sécurité
dispositif conçu conformément à la CEI 61508 et qui met en œuvre le profil de communication de sécurité fonctionnelle

3.1.1.26
très basse tension de sécurité (TBTS)
circuit électrique dans lequel la tension ne peut pas dépasser 30 V eff. en c.a., 42,4 V crête ou 60 V en c.c. dans des conditions normales de premier défaut, y compris les défauts à la terre dans les autres circuits

NOTE Un circuit TBTS n'est pas relié à la terre de protection.

[CEI 61131-2]

3.1.1.27
fonction de sécurité
fonction qu'un système E/E/PE relatif à la sécurité ou d'autres mesures de réduction du risque doivent mettre en œuvre et qui est destinée à atteindre ou à maintenir un état de sécurité de l'équipement commandé, compte tenu d'un événement dangereux spécifique

NOTE La définition de la CEI 61508-4 est identique, avec un exemple et des références supplémentaires.

[CEI 61508-4:2010, modifiée]

3.1.1.28
temps de réponse de la fonction de sécurité
temps écoulé du cas le plus défavorable suite à l'activation d'un capteur de sécurité relié à un bus de terrain, avant que ne soit atteint l'état de sécurité correspondant de son (ses) actionneur(s) de sécurité, du fait d'erreurs ou de défaillances avérées dans le canal de fonction de sécurité

NOTE Ce concept, introduit dans la CEI 61784-3:2010[11], 5.2.4, est traité par les profils de communication de sécurité fonctionnelle définis dans la présente partie.

3.1.1.29
niveau d'intégrité de sécurité (SIL[12])
niveau discret (un sur quatre niveaux possibles), correspondant à une plage de valeurs d'intégrité de sécurité, où le niveau d'intégrité de sécurité 4 est le niveau le plus élevé et le niveau d'intégrité de sécurité 1 est le niveau le plus faible

---

10 SCL = *Safety Communication Layer*

11 En cours d'élaboration.

12 SIL = *Safety Integrity Level*

NOTE 1 Les mesures de défaillance cible (voir la CEI 61508-4:2010, 3.5.17) applicables aux quatre niveaux d'intégrité de sécurité sont spécifiées dans les Tableaux 2 et 3 de la CEI 61508-1:2010[13].

NOTE 2 Les niveaux d'intégrité de sécurité sont utilisés pour spécifier les exigences d'intégrité de sécurité des fonctions équivalentes à attribuer aux systèmes E/E/PE relatifs à la sécurité.

NOTE 3 Le niveau d'intégrité de sécurité (SIL) n'est pas une propriété d'un système, sous-système, élément ou composant. L'interprétation correcte de l'expression « système relatif à la sécurité avec SILn » (où n est égal à 1, 2, 3 ou 4) signifie que le système est potentiellement capable de prendre en charge des fonctions de sécurité avec un niveau d'intégrité de sécurité jusqu'à n.

[CEI 61508-4:2010]

3.1.1.30
mesure de sécurité
<la présente norme> mesure permettant de contrôler les *erreurs* de communication éventuelles, qui est conçue et mise en œuvre conformément aux exigences de la CEI 61508

NOTE 1 Dans la pratique, plusieurs mesures de sécurité sont combinées pour atteindre le niveau d'intégrité de sécurité requis.

NOTE 2 Les *erreurs* de communication et les mesures de sécurité associées sont détaillées dans la CEI 61784-3:2010, 5.3 et 5.4.

3.1.1.31
application relative à la sécurité
programmes conçus conformément à la CEI 61508 pour satisfaire aux exigences SIL de l'application

3.1.1.32
système relatif à la sécurité
système qui exécute les *fonctions de sécurité* conformément à la CEI 61508

3.1.1.33
limite de revendication du SIL (SIL CL[14])
SIL maximal qui peut être revendiqué pour un *système relatif à la sécurité* en relation avec les contraintes architecturales et l'intégrité de sécurité systématique

[CEI 62061, modifiée]

3.1.1.34
esclave
entité de communication passive capable de recevoir des messages et de les envoyer en réponse à une autre entité de communication qui peut être maître ou esclave

3.1.1.35
datation (horodatage)
information temporelle incluse dans un *message*

3.1.2 CPF 6: Termes et définitions supplémentaires

3.1.2.1
cycle
intervalle d'exécution d'une activité de manière répétitive et continue

3.1.2.2
temps d'arrêt paramétré
temps de réponse de la fonction de sécurité (dans le cas le moins favorable pour chacune d'elles) sans t1 et t2

---

13 A publier.

14 SIL CL = *SIL Claim Limit*

NOTE Voir la CEI 61784-3:2010, 5.2.4, Figure 4.

3.1.2.3
PDU de sécurité
synonyme de DLPDU relatif à la sécurité

3.1.2.4
données (entrée/sortie) de sécurité
données entrées ou sorties de manière sécurisée au niveau des interfaces externes (blocs d'extrémité) des blocs de fonctions

3.2 Symboles et abréviations

3.2.1 Symboles et abréviations communs

CP	Profil de communication (*Communication Profile*)	[CEI 61784-1]
CPF	Famille de profils de communication (*Communication Profile Family)*	[CEI 61784-1]
CRC	Contrôle de redondance cyclique (*Cyclic Redundancy Check)*	
DLL	Couche de liaison de données (*Data Link Layer*)	[ISO/CEI 7498-1]
DLPDU	Ensemble (unité) de données de protocole de liaison de données (*Data Link Protocol Data Unit)*	
CEM	Compatibilité électromagnétique	
EMI	Perturbation électromagnétique (*Electromagnetic Interference*)	
EUC	Equipement commandé (*Equipment Under Control)*	[CEI 61508-4:2010]
E/E/PE	Electrique/électronique/électronique programmable (*Electrical/Electronic/Programmable Electronic*)	[CEI 61508-4:2010]
FAL	Couche Application de bus de terrain (*Fieldbus Application Layer*)	[CEI 61158-5]
FCS	Séquence de contrôle de trame (*Frame Check Sequence)*	
FS	Sécurité fonctionnelle (*Functional Safety)*	
FSCP	Profil de communication de sécurité fonctionnelle (*Functional Safety Communication Profile)*	
MTBF	Moyenne des temps de bon fonctionnement entre défaillances (*Mean Time Between Failures*)	
MTTF	Durée moyenne de fonctionnement avant défaillance (*Mean Time To Failure*)	
PDU	Ensemble (Unité) de données de protocole (*Protocol Data Unit*)	[ISO/CEI 7498-1]
TBTP	Très basse tension de protection	
PES	Système électronique programmable (*Programmable Electronic System*)	[CEI 61508-4:2010]
PFH	Fréquence moyenne de défaillance dangereuse [h^{-1}] par heure	[CEI 61508-6:2010[15]]
PhL	Couche physique (*Physical Layer*)	[ISO/CEI 7498-1]
PL	Niveau de performance (*Performance Level*)	[ISO 13849-1]
PLC	Automate programmable (*Programmable Logic Controller*)	
SCL	Couche de communication de sécurité (*Safety Communication Layer*)	
TBTS	Très basse tension de sécurité	
SIL	Niveau d'intégrité de sécurité (*Safety Integrity Level*)	[CEI 61508-4:2010]
SIL CL	Limite de revendication du SIL (SIL Claim Limit)	[CEI 62061]

3.2.2 CPF 6: Symboles et abréviations supplémentaires

3.2.2.1 Abréviations supplémentaires

SCLM	Maître de la couche de communication de sécurité (*Safety Communication Layer Master*)

15 A publier.

SCLS Esclave de la couche de communication de sécurité (*Safety Communication Layer Slave*)

SRC Contrôleur de sécurité (Safety Relevant Controller)

SRP Périphérique de sécurité (Safety Relevant Peripheral)

S_CON_ID ID de connexion de sécurité (Safety Connection ID)

3.2.2.2 Symboles supplémentaires

Symbole	Définition	Unité
a	Nombre d'esclaves	—
AF	Facteur de disponibilité	—
I_s	Nombre d'esclaves de sécurité	
M	Facteur de mise en œuvre du maître de Type 8	—
n	Nombre d'octets de données	octet
n_{as}	Nombre d'esclaves de sécurité	—
n_{FBS}	Nombre de blocs de fonctions utilisés (dans le logiciel d'application relatif à la sécurité)	—
P_e	Probabilité d'erreurs sur les bits	—
$R_{SL}(P_e)$	Probabilité d'erreurs résiduelles d'un message de sécurité	—
t_A	Temps de réponse de l'actionneur	ms
t_{CTSCS}	Durée de cycle du système de communication de sécurité fonctionnelle	ms
t_G	Temps d'arrêt garanti	ms
T_{bit}	Durée nominale en bit	ms
t_{IB}	Durée de cycle du système de communication de Type 8 de la CEI 61158	ms
t_{IN}	Temps de traitement de l'entrée de sécurité	ms
t_{FBS}	Temps de traitement moyen du bloc de fonctions (dans le logiciel d'application relatif à la sécurité)	ms
t_{OD}	Temps de traitement du dispositif de sortie de sécurité	ms
t_{PST}	Temps d'arrêt paramétré d'une sortie de sécurité	ms
t_S	Temps de réponse du capteur	ms
t_{SF}	Temps de réponse de la fonction de sécurité	ms
t_{SRC}	Temps de réponse du SRC	ms
t_{Stop}	Temps d'arrêt de la machine	ms
t_{SW}	Temps de traitement logiciel du maître (spécifique à l'application)	ms
$\Lambda_{SL}(P_e)$	Taux d'erreurs résiduelles par heure de la couche de communication de sécurité eu égard à la probabilité d'erreurs sur les bits	—
ν	Nombre maximal de messages de sécurité par heure	—

3.3 Conventions

Les conventions de définitions de service de la CEI 61158-5-8:2007, 3.8.4, sont utilisées.

4 Présentation de FSCP 6/7 (INTERBUS™ Safety)

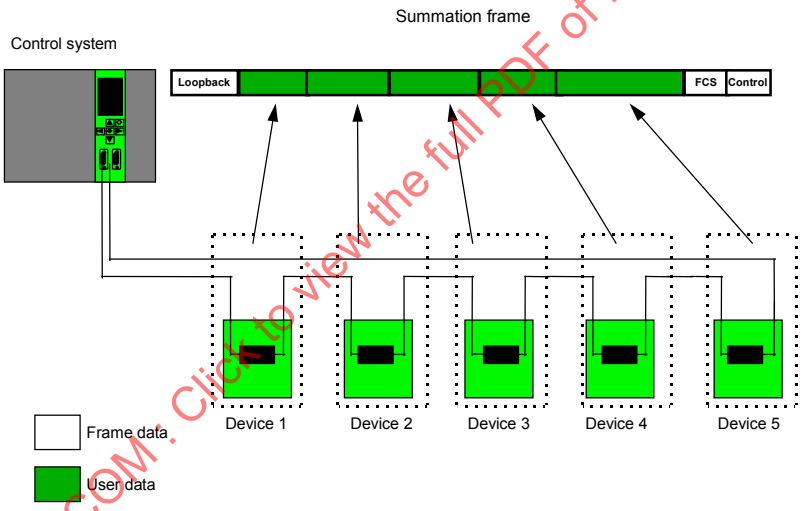
4.1 Généralités

La famille de profils de communication 6 (communément appelée INTERBUS®[16]) définit des profils de communication sur la base du Type 8 de la CEI 61158-2, de la CEI 61158-3-8, la CEI 61158-4-8, la CEI 61158-5-8 et la CEI 61158-6-8.

Les profils de base CP 6/1, CP 6/2, CP 6/3 sont définis dans la CEI 61784-1. Le profil de communication de sécurité fonctionnelle CPF 6 FSCP 6/7 (INTERBUS Safety™ [10]) est fondé sur les profils de base CPF 6 définis dans la CEI 61784-1, ainsi que les spécifications de la couche de communication de sécurité définies dans la présente partie.

4.2 Présentation générale d'ordre technique

Le FSCP 6/7 utilise la voie de transport existante pour la transmission cyclique des données (pour les données de processus). Il s'agit, en principe, d'un concept maître-esclave avec une topologie en anneau physique et l'existence de relations logiques un-un entre un maître et chacun de ses esclaves (Figure 3). La transmission des données s'effectue via un PDU – communément appelé cadre de sommation – à partir duquel chaque esclave extrait ses données de sortie et insère ses données d'entrée.



Légende

Anglais	Français
Control system	Système de commande
Loopback	Retour de boucle
Summation frame	Cadre de sommation
Device 1	Dispositif 1
Frame data	Données de trame
User data	Données utilisateur

Figure 3 – Conditions préalables de communication FSCP 6/7

16 INTERBUS® et INTERBUS Safety™ désignent les appellations commerciales de Phoenix Contact GmbH & Co. KG. Le contrôle de l'emploi des appellations commerciales est confié à l'organisme sans but lucratif INTERBUS Club. Cette information est donnée à l'intention des utilisateurs de la présente Norme internationale et ne signifie nullement que la CEI approuve ou recommande le détenteur de la marque ou de l'un quelconque de ses produits. La conformité à la présente partie n'exige pas l'emploi des appellations INTERBUS® ou INTERBUS Safety™. L'emploi des appellations INTERBUS® ou INTERBUS Safety™ exige l'autorisation de INTERBUS Club.

La couche de communication de sécurité du FSCP 6/7 fournit les mesures de sécurité suivantes pour sa réalisation:

— numéro de séquence;

— datation (horodatage);

— authentification de connexion;

— contrôle de redondance cyclique pour l'intégrité des données de sécurité.

La numérotation de séquence utilise la plage comprise entre 001 et 111 sans 000. L'authentification de connexion (informations émetteur/récepteur) consiste en 7 bits, de sorte qu'il est possible d'intégrer un nombre maximal de 126 esclaves dans le bus de terrain de sécurité. Le transfert des données de sécurité peut s'effectuer entre le maître de sécurité et chaque esclave de sécurité correspondant, et entre chaque esclave de sécurité et le maître de sécurité correspondant dans le cadre d'un cycle de données unique. Un temporisateur séparé placé sur chaque esclave de sortie de sécurité garantit un temps de réponse pour chaque fonction de sécurité, et peut faire l'objet d'un paramétrage sur une échelle à grandes valeurs. Le temporisateur peut être adapté pour chaque canal de sortie de sécurité d'un esclave de sortie correspondant.

La couche de communication de sécurité de FSCP 6/7 peut être utilisée pour des fonctions de sécurité jusqu'au niveau SIL 3. Par conséquent, le bus de terrain de sécurité consomme au maximum 1 % de la PFH globale. On obtient $\Lambda < 10^{-7}$ dans le bus de terrain de sécurité. Un temporisateur intégré fournissant le délai de chaque canal de sortie de chaque esclave de sortie de sécurité correspondant, garantit un temps de réponse de sécurité fonctionnelle. Le temps de réponse de sécurité fonctionnelle comprend le temps de transmission de bus de terrain entre un esclave d'entrée de sécurité et le maître, et entre le maître et l'esclave de sortie de sécurité, y compris également les répétitions éventuelles du PDU de sécurité en raison des erreurs de transmission, le temps de traitement de chaque esclave de sécurité (entrée et sortie) et le temps de traitement du système PES (généralement sous la forme d'un PLC de sécurité avec un maître intégré) et le temps d'arrêt d'une machine. En cas de dépassement du temps configuré du temporisateur intégré d'un canal de sortie spécifique d'un esclave de sortie de sécurité, le canal de sortie correspondant est réglé sur son état de sécurité, qui est habituellement l'état d'impuissance.

La structure du PDU de sécurité comprend les mesures de sécurité (numéro de séquence, datation, authentification de connexion, CRC) et les données de sécurité. Les données et les mesures de sécurité pour chaque esclave de sécurité sont intégrées dans le cadre de sommation.

4.3 Profil de communication de sécurité fonctionnelle 6/7

Le profil de communication de sécurité fonctionnelle CPF 6 FSCP 6/7 repose sur les profils CPF 6 CP 6/1, CP 6/2 et CP 6/3 spécifiés dans la CEI 61784-1. Ces profils contiennent des services facultatifs, spécifiés par les identifiants de profil. Les identifiants de profil appropriés pour le protocole CP 6/7 sont présentés dans le Tableau 1.

Tableau 1 – Présentation générale de l'identifiant de profil applicable au protocole FSCP 6/7

Profil	Maître		Esclave		
	Cyclique	Cyclique et non cyclique	Cyclique	Non cyclique	Cyclique et non cyclique
Profil 6/1	618	619	611	—	613
Profil 6/2	—	629	—	—	623
Profil 6/3	—	639	—	—	633

La spécification de la couche de communication de sécurité donnée dans la présente partie s'applique dans son intégralité.

5 Généralités

5.1 Documents externes de spécifications applicables au profil

Il est recommandé aux fabricants d'un dispositif de sécurité de consulter les documents [31] et [44] à [50] donnant des spécifications supplémentaires susceptibles d'être utiles à la mise en œuvre de la SCL définie dans la présente partie.

5.2 Exigences fonctionnelles de sécurité

Les exigences de conception des dispositifs de sécurité (le maître et les esclaves de sécurité, par exemple) n'entrent pas dans le domaine d'application de la présente partie. Le concepteur de ces dispositifs doit tenir compte des exigences de la CEI 61508.

Certaines exigences relatives aux blocs de fonctions qui doivent être mis en œuvre sur des dispositifs de sécurité sont spécifiées en 6.3. Les exigences relatives aux blocs de fonctions utilisés dans la présente partie pour spécifier les services et protocoles sont indiquées en 5.4.

Les spécifications des sous-systèmes ou éléments conformes à la CEI 61508 sont spécifiques à la mise en œuvre et, à ce titre, n'entrent pas dans le domaine d'application de la présente partie. La présente partie spécifie uniquement les services et protocoles d'un système de communication de sécurité fonctionnelle reposant sur le Type 8 de la série CEI 61158.

La description des états de sécurité est donnée en 5.4.6.

5.3 Mesures de sécurité

5.3.1 Généralités

La couche de communication de sécurité décrite dans la présente partie fournit les mesures correctives déterministes suivantes pour sa mise en œuvre:

— numéro de séquence;
— datation (horodatage);
— authentification de connexion;
— contrôle de redondance cyclique pour l'intégrité des données de sécurité (CRC 24);
— différents systèmes d'assurance d'intégrité des données.

La sélection des différentes mesures correspondant aux erreurs possibles est présentée dans le Tableau 2.

Tableau 2 – Sélection des différentes mesures correspondant aux erreurs possibles

Erreurs de communication	Mesures correctives déterministes							
	Numéro de séquence	Datation	Délai	Authentification de connexion	Message de réaction	Assurance d'intégrité des données	Redondance avec contre-vérification	Différents systèmes d'assurance d'intégrité des données
Corruption						X		
Répétition non prévue	X							
Séquence incorrecte	X							
Perte	X							
Retard inacceptable		X [c]	X [b]					
Insertion	X			X [a]				
Déguisement				X				X
Adressage				X				

NOTE Tableau adapté de la CEI 62280-2 [18] et de l'EN 954-1 [27].

[a] Uniquement pour l'identification de l'émetteur. Détecte uniquement l'insertion d'une source invalide.

[b] Requis dans tous les cas.

[c] La datation (horodatage) est créée en local du côté SLCS. La détection de la répétition non prévue et de la séquence incorrecte ne peut pas être réalisée avec elle. Spécifique au Type 8 de la série CEI 61158.

5.3.2 Numéro de séquence

Les messages de sécurité contiennent un numéro de séquence d'une largeur de 3 bits et une séquence spécifiée (voir 7.1 et 7.2). Si la séquence n'est pas respectée, tous les signaux de sortie relatifs à la sécurité doivent être définis sur leur état de sécurité (Figures 47 et 48). Tous les esclaves de sécurité doivent définitivement porter le même numéro de séquence (voir 7.1 et 7.2).

5.3.3 Datation

Le numéro de séquence et une horloge locale peuvent être utilisés pour générer une datation relative locale pour chaque SCLS. Cette datation relative concerne toutes les données d'entrée et de sortie de sécurité du système.

5.3.4 Délai

Le SCLS peut utiliser une datation pour déterminer si les données d'entrée de sécurité utilisées pour lier les données de sortie de sécurité ne sont pas trop anciennes.

5.3.5 Acquittement

Un acquittement est assuré lorsque le numéro de séquence est correctement mis à jour.

5.3.6 Authentification de connexion

L'authentification de connexion est mise en œuvre par un ID de connexion de sécurité (S_CON_ID) composé de 7 bits, de manière à pouvoir intégrer jusqu'à 126 esclaves dans le

système de communication de sécurité fonctionnelle. L'attribution des ID de connexion de sécurité doit être unique dans un système de communication de sécurité fonctionnelle.

Les messages de sécurité contiennent toujours l'ID de connexion de sécurité.

5.3.7 Distinction entre les messages relatifs et non relatifs à la sécurité – différents systèmes d'assurance d'intégrité des données

Les messages de sécurité (48 bits) contiennent une somme de contrôle CRC (24 bits). Le protocole de Type 8 de la CEI 61158 utilise un autre algorithme CRC (CRC 16 bits). De plus, chaque message contient un ID de connexion de sécurité de 7 bits.

5.3.8 Temps d'arrêt paramétré

Un temporisateur intégré indiquant le délai de chaque canal de sortie de chaque esclave de sortie de sécurité assure un temps d'arrêt paramétré, qui est le temps qui s'écoule entre la détection d'un événement au niveau de l'esclave d'entrée de sécurité et la réponse apportée par le canal de sortie correspondant de l'esclave de sortie de sécurité, hors temps de traitement de l'entrée de sécurité. Pour plus de détails, voir également 9.3.2.2.

Le temps d'arrêt paramétré est le temps de transmission de bus de terrain entre un esclave d'entrée de sécurité et le maître et entre le maître de sécurité et l'esclave de sortie de sécurité, en y intégrant les éventuelles répétitions du PDU de sécurité dues aux erreurs de transmission, le temps de traitement de l'esclave de sortie de sécurité et le temps de traitement du SRC.

En cas de dépassement du temps d'arrêt paramétré d'un canal de sortie spécifique d'un esclave de sortie de sécurité, le canal de sortie correspondant est réglé sur son état de sécurité, qui est en général l'état Inactif. Cette règle doit être respectée par la couche d'application du SRP.

5.4 Structure de la couche de communication de sécurité

5.4.1 Processus de décomposition

Le système de Type 8 de la CEI 61158 a été conçu pour assurer des courts temps de réponse et des temps de transmission prévisibles. Ces deux qualités sont indispensables aux applications relatives à la sécurité.

EXEMPLE 1 Un mouvement dangereux doit être interrompu aussi rapidement que possible. Pour ce faire, un système de communication de sécurité offrant des temps de transmission courts est requis.

EXEMPLE 2 Des dispositifs de protection doivent être installés à une certaine distance de sécurité afin que personne ne puisse accéder à la machine avant qu'elle ne soit arrêtée. Pour calculer cette distance de sécurité, une définition du temps de réponse le moins favorable est requise.

Pour exécuter des fonctions de sécurité, des dispositifs sont en général utilisés, qui n'intègrent aucun composant électronique complexe ni composant électronique programmable. Les modes de défaillance de ces dispositifs sont parfaitement définis. Les technologies conventionnelles sont limitées si les exigences de l'application augmentent en matière de souplesse, de fonctionnalité et de diagnostic. Le développement d'un système de communication de sécurité reposant sur le Type 8 de la CEI 61158 a pour objet de faire bénéficier la technologie de sécurité des avantages qu'offre un système de bus de terrain standard.

La conception de la couche de communication de sécurité respecte les principes de la CEI 61508, de la CEI 62061 et de l'ISO 13849-1.

NOTE 1 Le respect des principes de la CEI 62061 ne signifie pas que seules les machines sont concernées.

L'étape qui suit immédiatement la détermination des limites d'une machine et la définition d'un concept adapté aux machines consiste généralement à lancer un processus de réduction des risques conformément à l'ISO 12100-1. Les fonctions de sécurité nécessaires au niveau requis de sécurité fonctionnelle pour chaque danger déterminé sont indiquées plus loin.

EXEMPLE 3 Une fonction de sécurité peut indiquer que « si le dispositif de sécurité est ouvert, la vitesse de rotation de l'axe est nulle pendant une durée spécifiée ».

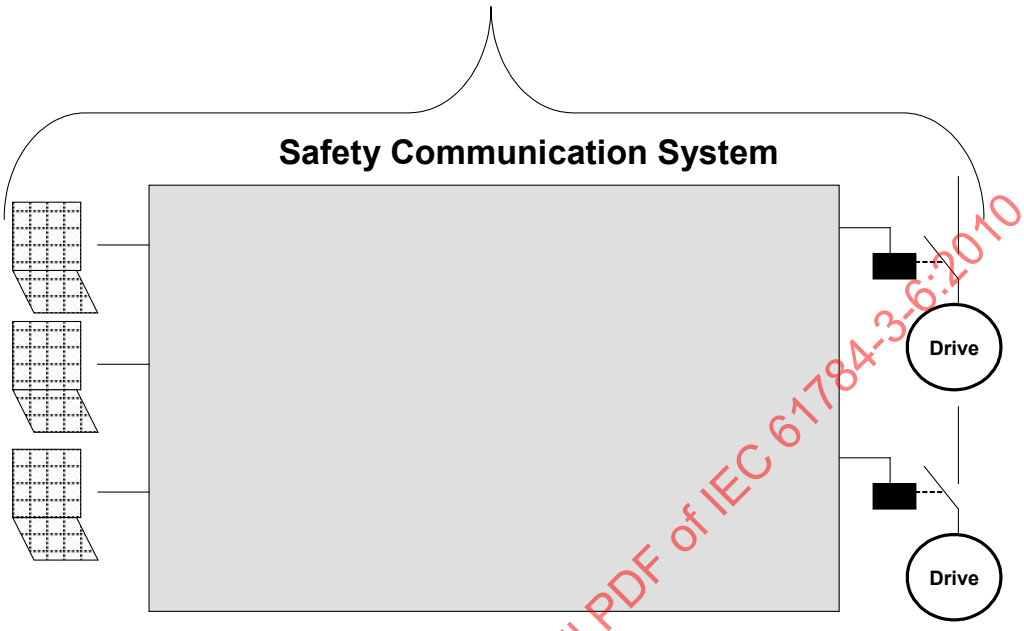
Le processus de décomposition de l'ensemble de la fonction de sécurité spécifique à l'application vers le système de bus de terrain est présenté ci-dessous. Ce processus se traduit par une spécification des blocs de fonctions et des interfaces qui les unissent.

NOTE 2 Le terme « bloc de fonctions de sécurité » est utilisé de la même manière que dans la CEI 62061, mais ne limite pas le domaine d'application de la présente partie au seul secteur des machines.

5.4.2 Définition de la fonction de sécurité du système de communication de sécurité

Un système de bus de terrain n'exécute de lui-même que certaines fonctions de sécurité spécifiées d'un système de commande relatif à la sécurité. Pour ce faire, des capteurs, des actionneurs (un commutateur de dispositif de protection, un contacteur, par exemple) et en général un logiciel d'application sont également nécessaires.

La fonction de sécurité d'un système de communication de sécurité est chargée de transmettre des données de sécurité d'une entrée vers une sortie en un temps imparti. La Figure 4 donne un exemple de fonction de sécurité dans une machine. La boîte noire au milieu peut être représentée par un dispositif conventionnel de sécurité (un relais de sécurité, par exemple) ou un système de communication de sécurité. Les capteurs et actionneurs sont connectés aux interfaces à l'extérieur du système de communication de sécurité.



Légende

Anglais	Français
Safety function (e.g., if the guard door is open, the speed of shaft rotation is set to zero within a specified maximum time)	Fonction de sécurité (par exemple, si le dispositif de sécurité est ouvert, la vitesse de rotation de l'axe est nulle pendant une durée spécifiée
Safety communication system	Système de communication de sécurité
Drive	Unité

Figure 4 – Exemple de fonction de sécurité

5.4.3 Décomposition de la fonction de sécurité d'un système de communication de sécurité en blocs de fonctions

5.4.3.1 Présentation du processus de décomposition de fonction de sécurité

La fonction de sécurité exécutée par le système de communication de sécurité peut être décomposée en blocs de fonctions suivants (Figure 5):

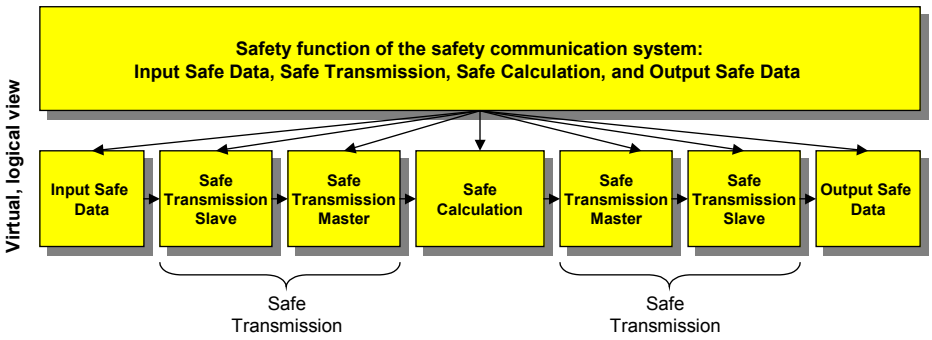
— Données d'entrée sécurisées;

— Transmission sécurisée (reposant sur le protocole de Type 8 de la CEI 61158);

— Calcul sécurisé;

— Données de sortie sécurisées.

NOTE En règle générale, la mise en œuvre d'un bloc de fonctions implique une spécification détaillée des exigences de sécurité. De même, une spécification des exigences de sécurité des sous-systèmes exécutant les blocs de fonctions est nécessaire. Ces spécifications n'entrent pas dans le domaine d'application de la présente partie.



Légende

Anglais	Français
Safety function of the safety communication system: Input Safe Data, Safe Transmission, Safe Calculation, and Output Safe Data	Fonction de sécurité du système de communication de sécurité: Données d'entrée sécurisées, Transmission sécurisée, Calcul sécurisé et Données de sortie sécurisées
Input Safe Data	Données d'entrée sécurisées
Safe Transmission Slave	Esclave de transmission sécurisée
Safe Transmission Master	Maître de transmission sécurisée
Safe Calculation	Calcul sécurisé
Output Safe Data	Données de sortie sécurisées
Safe Transmission	Transmission sécurisée
Virtual, logical view	Vue virtuelle et logique

Figure 5 – Décomposition de la fonction de sécurité en blocs de fonctions

5.4.3.2 Bloc de fonctions Données d'entrée sécurisées

Le bloc de fonctions Données d'entrée sécurisées permet de lire les signaux d'entrée physiques provenant de différents capteurs qui peuvent être connectés au bloc d'extrémité d'entrée d'un esclave de sécurité. Il prépare les données qui vont être transmises par le bloc de fonctions Transmission sécurisée.

Ce bloc de fonctions est spécifique à l'application et n'entre pas dans le domaine d'application de la présente partie.

5.4.3.3 Blocs de fonctions Transmission sécurisée

5.4.3.3.1 Présentation de la transmission sécurisée

Deux blocs de fonctions Transmission sécurisée assure la sécurité de transmission des données de sécurité entre une source et un collecteur (d'un émetteur vers un récepteur, par exemple):

— Bloc de fonctions Maître de transmission sécurisée

— Bloc de fonctions Esclave de transmission sécurisée

NOTE Conformément à la CEI 62061, un bloc de fonctions est exécuté par un seul sous-système (le dispositif, par exemple). Chaque bloc de fonctions est attribué à un sous-système dans l'architecture de la fonction de sécurité. Plusieurs blocs de fonctions peuvent être attribués à un seul sous-système. Un bloc de fonctions est uniquement exécuté par un seul sous-système.

5.4.3.3.2 Bloc de fonctions Esclave de transmission sécurisée

Le bloc de fonctions Esclave de transmission sécurisée offre des services spécifiques à l'esclave d'un dispositif d'entrée ou de sortie au sein du système de communication de sécurité et du profil de sécurité supplémentaire de la présente partie.

5.4.3.3.3 Bloc de fonctions Maître de transmission sécurisée

Le bloc de fonctions Maître de transmission sécurisée offre des services spécifiques au maître d'un dispositif de contrôle de sécurité au sein du système de communication de sécurité fonctionnelle de la présente partie.

5.4.3.4 Bloc de fonctions Calcul sécurisé

Le bloc de fonctions Calcul sécurisé procède à la résolution logique des signaux d'entrée reçus et génère de nouvelles données de sortie de sécurité en fonction du logiciel d'application relatif à la sécurité. Le début d'un nouveau cycle de bus doit être synchronisé avec ce bloc de fonctions (voir également 6.2). La spécification de ce bloc de fonctions n'entre pas dans le domaine d'application de la présente partie. Le cas échéant, la présente partie spécifie les exigences relatives à la structure du bloc de fonctions Calcul sécurisé.

5.4.3.5 Bloc de fonctions Données de sortie sécurisées

Le bloc de fonctions Données de sortie sécurisées lit les signaux de sortie reçus provenant du bloc de fonctions Esclave de transmission sécurisée, les transforme en signaux de sortie physiques et les met à disposition dans le bloc d'extrémité d'un esclave de sécurité.

Ce bloc de fonctions est spécifique à l'application et n'entre pas dans le domaine d'application de la présente partie.

5.4.4 Attribution des blocs de fonctions aux sous-systèmes

5.4.4.1 Présentation

Le Tableau 3 présente les blocs de fonctions et les sous-systèmes correspondants.

Tableau 3 – Liste des blocs de fonctions et des sous-systèmes

Bloc de fonctions	Sous-système
Données d'entrée sécurisées	Safety Relevant Peripheral (SRP)
Maître de transmission sécurisée	Maître de la couche de communication de sécurité (SCLM[17])
Esclave de transmission sécurisée	Esclave de la couche de communication de sécurité (SCLS[18])
Calcul sécurisé	Safety Relevant Controller (SRC)
Transmission sécurisée	Couche de Communication de Sécurité (SCL[19]) Profil de transmission de sécurité
Données de sortie sécurisées	Safety Relevant Peripheral (SRP)

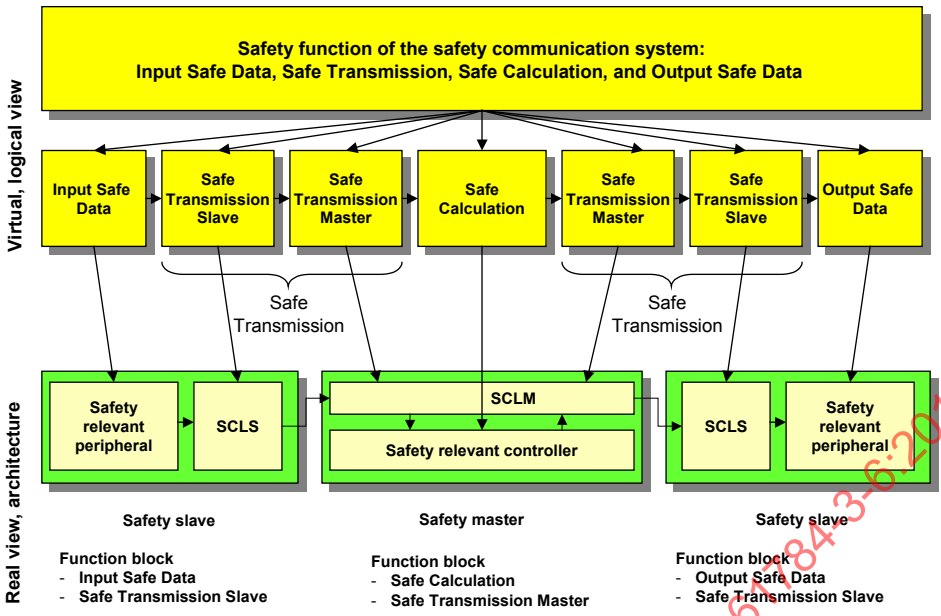
La Figure 6 présente les résultats du processus de décomposition par rapport aux fonctions de sécurité exécutées par un système de communication de sécurité.

---

17 SCLM = *Safety Communication Layer Master*

18 SCLS = *Safety Communication Layer Slave*

19 SCL = *Safety Communication Layer*



Légende

Anglais	Français
Safety function of the safety communication system:	Fonction de sécurité du système de communication de sécurité:
Input Safe Data, Transmission, Safe Calculation and Output Safe Data	Données d'entrée sécurisées, Transmission, Calcul sécurisé et Données de sortie sécurisées
Input Safe Data	Données d'entrée sécurisées
Safe Transmission Slave	Esclave de transmission sécurisée
Safe Transmission Master	Maître de transmission sécurisée
Safe Calculation	Calcul sécurisé
Safe Transmission	Transmission sécurisée
Safety relevant peripheral	SRP
Safety relevant controller	SRC
Safety slave	Esclave de sécurité
Safety master	Maître de sécurité
Function block	Bloc de fonctions
Output Safe Data	Données de sortie sécurisées

Figure 6 – Présentation des résultats du processus de décomposition

Le système de communication de sécurité repose sur les deux principaux sous-systèmes (dispositifs) ci-dessous:

— Esclave de sécurité (entrée, sortie, entrée et sortie);

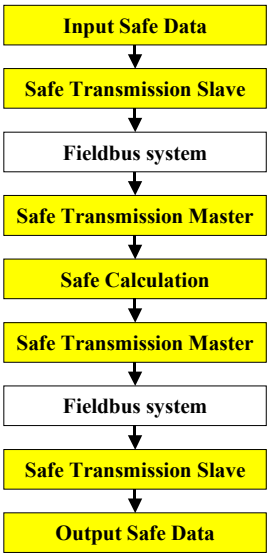
— Maître de sécurité (avec SRC).

Chacun d'eux exécute un ou plusieurs blocs de fonctions.

5.4.4.2 Description des interfaces entre les blocs de fonctions définis

5.4.4.2.1 Description du flux de signal

La Figure 7 présente le flux de signal entre les blocs de fonctions définis.



Légende

Anglais	Français
Input Safe Data	Données d'entrée sécurisées
Safe Transmission Slave	Esclave de transmission sécurisée
Fieldbus system	Système de bus de terrain
Safe Transmission Master	Maître de transmission sécurisée
Safety Calculation	Calcul sécurisé
Output Safe Data	Données de sortie sécurisées

Figure 7 – Flux de signal entre les blocs de fonctions

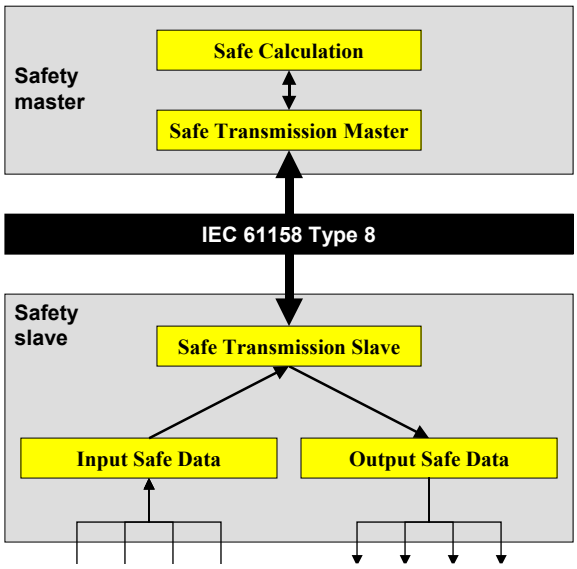
Le Tableau 4 présente le flux de signal entre les blocs de fonctions.

Tableau 4 – Flux de signal entre les blocs de fonctions

Bloc de fonctions (source)	Bloc de fonctions (collecteur)	Action requise
Données d'entrée sécurisées	Esclave de transmission sécurisée	Le bloc de fonctions source transfère au bloc de fonctions du collecteur les données enregistrées au niveau du bloc d'extrémité de l'esclave de sécurité qui exécute le bloc de fonctions
Esclave de transmission sécurisée	Maître de transmission sécurisée	Le bloc de fonctions source transfère au bloc de fonctions Maître de transmission sécurisée les données enregistrées provenant du bloc de fonctions Données d'entrée sécurisées. Le protocole de Type 8 de la CEI 61158 fait office de protocole de transmission. Le bloc de fonctions Transmission sécurisée ajoute des mesures de sécurité supplémentaires (mesures correctives déterministes) aux données de sécurité transmises
Maître de transmission sécurisée	Calcul sécurisé	Le bloc de fonctions source extrait les données de sécurité reçues en supprimant les mesures de sécurité supplémentaires (mesures correctives déterministes) et les transfère vers le bloc de fonctions Calcul sécurisé
Calcul sécurisé	Maître de transmission sécurisée	A l'issue du traitement des données sécurisées, le bloc de fonctions Calcul sécurisé génère de nouvelles données de sortie de sécurité et les transfère vers le bloc de fonctions Maître de transmission sécurisée qui suit
Maître de transmission sécurisée	Esclave de transmission sécurisée	Le bloc de fonctions Maître de transmission sécurisée extrait toutes les données de sécurité du bloc de fonctions Calcul sécurisé et les transfère vers le bloc de fonctions Esclave de transmission sécurisée qui suit. Le protocole de Type 8 de la CEI 61158 fait office de protocole de transmission. Le bloc de fonctions ajoute des mesures de sécurité supplémentaires (mesures correctives déterministes) aux données de sécurité
Esclave de transmission sécurisée	Données de sortie sécurisées	Le bloc de fonctions Esclave de transmission sécurisée extrait les données des messages reçus et les transfère vers le bloc de fonctions Données de sortie sécurisées

5.4.4.2.2 Interfaces entre les blocs de fonctions et les dispositifs

La Figure 8 illustre les interfaces entre les blocs de fonctions et les dispositifs.



Légende

Anglais	Français
Input Safe Data	Données d'entrée sécurisées
Safe Transmission Slave	Esclave de transmission sécurisée
Safety master	Maître de sécurité
Safe Transmission Master	Maître de transmission sécurisée
Safety Calculation	Calcul sécurisé
Output Safe Data	Données de sortie sécurisées
Safety slave	Esclave de sécurité
IEC 61158 Type 8	Type 8 de la CEI 61158

Figure 8 – Interfaces entre les dispositifs de sécurité au sein du système de communication de sécurité

Le SRC est paramétré et programmé à l'aide d'un logiciel de langage de programmation à variabilité limitée (système de programmation Windows compatible avec la CEI 61131-3). Tous les blocs de fonctions, sous-systèmes et dispositifs peuvent être programmés, paramétrés et configurés à l'aide de ce logiciel. Ce logiciel n'entre pas dans le domaine d'application de la présente partie.

Lors de l'exécution d'une fonction de sécurité, tous les blocs de fonctions et toutes leurs interfaces sont activés.

Le cas échéant, la présente partie spécifie les exigences relatives à la conception de l'interface de programmation.

5.4.5 Exigences de sécurité et exigences d'intégrité de sécurité

Les exigences de sécurité et les exigences d'intégrité de sécurité d'une fonction de sécurité sont en général déduites d'un processus de réduction des risques (voir l'ISO 12100-1 et d'autres normes appropriées). Ce sujet n'entre pas dans le domaine d'application de la présente partie.

La couche de communication de sécurité est conçue pour le mode de fonctionnement à sollicitation élevée et jusqu'à une limite de revendication du SIL de 3. Par conséquent, le système de communication de sécurité utilise 1 % au maximum de la PFH globale. On obtient $\Lambda < 10^{-7}$ dans le système de communication de sécurité.

NOTE 1 La spécification des exigences de sécurité, y compris les exigences de sécurité et les exigences d'intégrité de sécurité, n'entre pas dans le domaine d'application de la présente norme.

NOTE 2 La spécification de ce profil est adaptée à une limite de revendication du SIL de 3. La limite de revendication du SIL obtenue d'un sous-système qui intègre la couche de communication de sécurité dépend des paramètres relatifs à la sécurité du sous-système en cours. Ce sujet n'entre pas dans le domaine d'application de la présente partie.

5.4.6 Spécification de l'état de sécurité

5.4.6.1 Généralités

Si une anomalie dangereuse est détectée dans le système de Type 8 de la CEI 61158 ou dans les blocs de fonctions, la fonction de sécurité et tous les blocs de fonctions connexes doivent être définis sur leurs états de sécurité.

Dans ce contexte, en cas d'anomalie, l'état de sécurité est une valeur qu'un bloc de fonctions doit transférer vers le bloc de fonctions qui suit. Un bloc de fonctions doit être en mesure de détecter des anomalies dans le bloc de fonctions qui le précède. Un bloc de fonctions doit comporter des mesures de diagnostic afin de détecter les anomalies dont il fait l'objet. Si un bloc de fonctions d'un dispositif est doté d'une interface directe vers un autre dispositif, des mesures doivent permettre de détecter les anomalies du dispositif précédent.

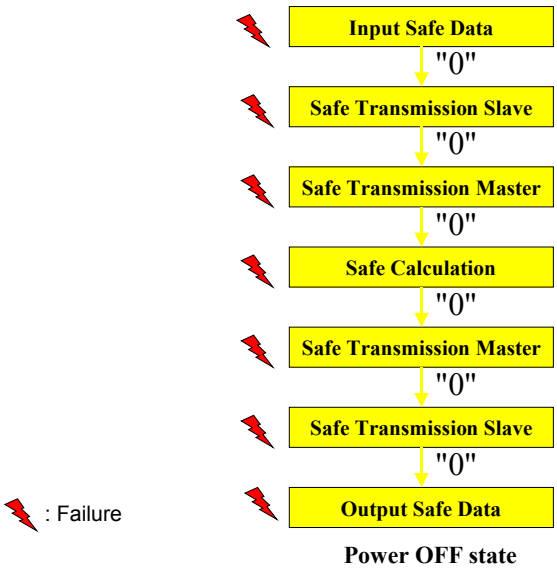
Une défaillance d'un sous-système peut entraîner l'impossibilité du bloc de fonctions à diagnostiquer sa propre anomalie ou transférer l'état de sécurité vers le bloc de fonctions qui suit. En cas d'anomalie d'un bloc de fonctions, celui du dispositif qui suit doit pouvoir la diagnostiquer. Le bloc de fonctions qui a détecté cette anomalie doit transférer son état de sécurité vers le bloc de fonctions qui suit.

Seule la valeur zéro (qui représente l'état de sécurité) doit être transmise vers les blocs de fonctions qui suivent. Les blocs de fonctions qui suivent ne sont pas en mesure de déterminer si l'état de sécurité est lié à la génération d'un état de sécurité dû à une anomalie ou au résultat d'une demande. Le bloc de fonctions doit toujours être défini sur son état de sécurité.

Il convient que le diagnostic informe l'utilisateur du système de la détection d'une demande ou d'une anomalie. Il convient que ces diagnostics soient générés par le bloc de fonctions concerné ou le bloc de fonctions suivant.

La section ci-dessous donne des informations relatives au flux de signal et à toutes les anomalies possibles.

La Figure 9 présente le flux de signal et les états de sécurité des blocs de fonctions concernés.



Légende

Anglais	Français
Input Safe Data	Données d'entrée sécurisées
Safe Transmission Slave	Esclave de transmission sécurisée
Safe Transmission Master	Maître de transmission sécurisée
Safety Calculation	Calcul sécurisé
Output Safe Data	Données de sortie sécurisées
Power OFF state	Etat inactif
Failure	Anomalie

Figure 9 – Flux de signal et états de sécurité

5.4.6.2 État de sécurité du bloc de fonctions Données d'entrée sécurisées

L'état de sécurité du bloc de fonctions consiste à transférer la valeur zéro pour toutes les valeurs du capteur.

5.4.6.3 État de sécurité du bloc de fonctions Transmission sécurisée

L'état de sécurité de ce bloc de fonctions dépend du type d'erreur. L'état de sécurité est défini comme suit:

— Transfert de la valeur zéro vers les blocs de fonctions suivants

— Pas d'activation du chien de garde qui représente le temps d'arrêt paramétré

Ces mesures s'appliquent au bloc de fonctions Transmission sécurisée. Elles sont intégrées au bloc de fonctions Transmission sécurisée et aux blocs de fonctions suivants:

— Esclave de transmission sécurisée

— Maître de transmission sécurisée

5.4.6.4 État de sécurité du bloc de fonctions Calcul sécurisé

L'état de sécurité du bloc de fonctions Calcul sécurisé consiste à transférer la valeur zéro pour toutes les valeurs de sortie.

NOTE Les valeurs de sortie sont transmises à tous les dispositifs de sortie lors du cycle de données suivant.

5.4.6.5 État de sécurité du bloc de fonctions Données de sortie sécurisées

L'état de sécurité du bloc de fonctions Données de sortie sécurisées consiste à transférer la valeur zéro pour toutes les valeurs de l'actionneur.

5.4.7 Réponse à une anomalie

5.4.7.1 Bloc de fonctions Données d'entrée sécurisées

En cas d'anomalie dans l'interface d'entrée du bloc de fonctions Données d'entrée sécurisées, ce dernier transfère la valeur zéro de chaque entrée faisant l'objet de l'anomalie en tant qu'entrée du bloc de fonctions Esclave de transmission sécurisée qui suit.

Le bloc de fonctions Données d'entrée sécurisées transfère la valeur zéro de toutes les entrées vers le bloc de fonctions Esclave de transmission sécurisée en cas d'anomalie détectée par le bloc de fonctions Données d'entrée sécurisées lui-même.

5.4.7.2 Bloc de fonctions Esclave de transmission sécurisée

Si ce bloc de fonctions détecte une anomalie dans le bloc de fonctions Données d'entrée sécurisées qui précède, il transfère la valeur zéro de toutes les entrées vers le bloc de fonctions Maître de transmission sécurisée.

Si ce bloc de fonctions détecte une anomalie dans le bloc de fonctions Maître de transmission sécurisée qui précède, il transfère la valeur zéro de toutes les sorties vers le bloc de fonctions Données de sortie sécurisées qui suit.

Si ce bloc de fonctions détecte une anomalie dans les messages reçus du bloc de fonctions Maître de transmission sécurisée qui précède, ce qui indique que ce bloc de fonctions a détecté une anomalie, il transfère la valeur zéro de toutes les sorties vers le bloc de fonctions Données de sortie sécurisées qui suit.

Si ce bloc de fonctions détecte une anomalie dans le système de Type 8 de la CEI 61158, il transfère la valeur zéro de toutes les sorties vers le bloc de fonctions Données de sortie sécurisées qui suit.

Si ce bloc de fonctions détecte une anomalie dans le dispositif précédent (SRC), il transfère la valeur zéro de toutes les sorties vers le bloc de fonctions Données de sortie sécurisées qui suit.

5.4.7.3 Bloc de fonctions Maître de transmission sécurisée

Si ce bloc de fonctions détecte une anomalie dans le bloc de fonctions Esclave de transmission sécurisée qui précède, il transfère la valeur zéro de toutes les entrées du bloc de fonctions Esclave de transmission sécurisée vers le bloc de fonctions Calcul sécurisé qui suit.

Si ce bloc de fonctions détecte une anomalie dans les messages reçus du bloc de fonctions Esclave de transmission sécurisée qui précède, ce qui indique que ce bloc de fonctions a détecté une anomalie, il transfère la valeur zéro de toutes les sorties du bloc de fonctions Esclave de transmission sécurisée associé vers le bloc de fonctions Calcul sécurisé qui suit.

Si ce bloc de fonctions détecte une anomalie dans le bloc de fonctions Calcul sécurisé qui précède, il transfère la valeur zéro de toutes les sorties vers le bloc de fonctions Esclave de transmission sécurisée qui suit.

Si ce bloc de fonctions détecte une anomalie dans le système de Type 8 de la CEI 61158, il transfère la valeur zéro de toutes les entrées du dispositif associé vers le bloc de fonctions Calcul sécurisé qui suit.

Si ce bloc de fonctions détecte une anomalie dans l'esclave d'entrée de sécurité qui précède, il transfère la valeur zéro de toutes les entrées associées de cet esclave vers le bloc de fonctions Calcul sécurisé qui suit.

5.4.7.4 Bloc de fonctions Calcul sécurisé

Si ce bloc de fonctions détecte une anomalie dans le bloc de fonctions Maître de transmission sécurisée qui précède, il définit le SRC à son état de sécurité.

5.4.7.5 Bloc de fonctions Données de sortie sécurisées

Si ce bloc de fonctions détecte une anomalie dans le bloc de fonctions Esclave de transmission sécurisée qui précède, il définit toutes les sorties à l'état OFF (inactif).

Si ce bloc de fonctions détecte une anomalie au niveau d'une ou de plusieurs sorties sur le dispositif qui l'exécute, il définit les sorties qui font l'objet de l'anomalie à leur état OFF (inactif).

5.4.8 Catégorie d'arrêt

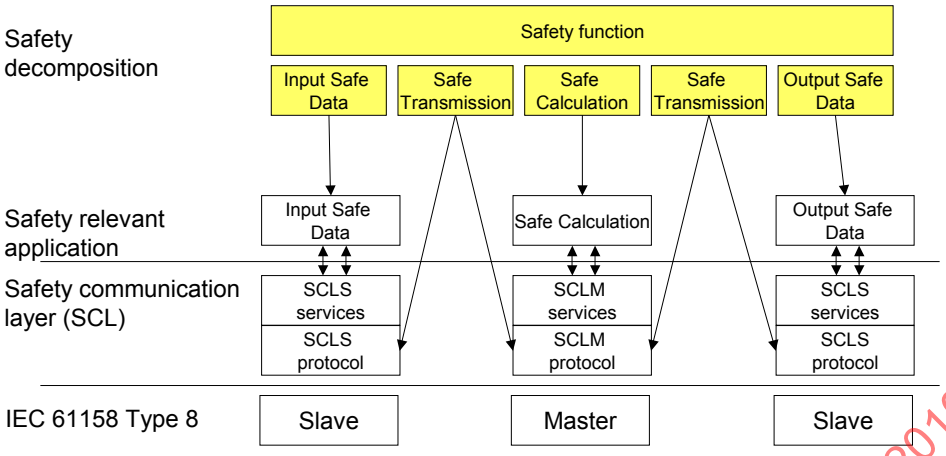
La spécification de la couche de communication de sécurité de la présente partie prend en charge la catégorie d'arrêt 0 conformément à la CEI 60204-1. En cas d'anomalie, le profil de communication de sécurité fonctionnelle définit toutes les sorties (ou les sorties associées uniquement) sur zéro. Les interfaces de sortie des esclaves de sécurité sont définies sur leur état d'alimentation OFF.

La catégorie d'arrêt 1 ou 2 peut être mise en œuvre (dans un logiciel d'application approprié et les esclaves de sécurité, par exemple). C'est la raison pour laquelle des exigences correspondantes doivent être indiquées dans la spécification des exigences de sécurité des dispositifs. Ce sujet n'entre pas dans le domaine d'application de la présente partie.

5.4.9 Transmission sécurisée

Des mesures correctives déterministes reposent sur le protocole de Type 8 de la CEI 61158 et sont mises en œuvre sur le maître de sécurité et sur les esclaves de sécurité, en tant que maître de la couche de communication de sécurité (SCLM) et qu'esclave de la couche de communication de sécurité (SCLS) respectivement (Figure 10).

Le maître de la couche de communication de sécurité (SCLM) et l'esclave de la couche de communication de sécurité (SCLS) sont indiqués dans la spécification de la couche de communication de sécurité.



Légende

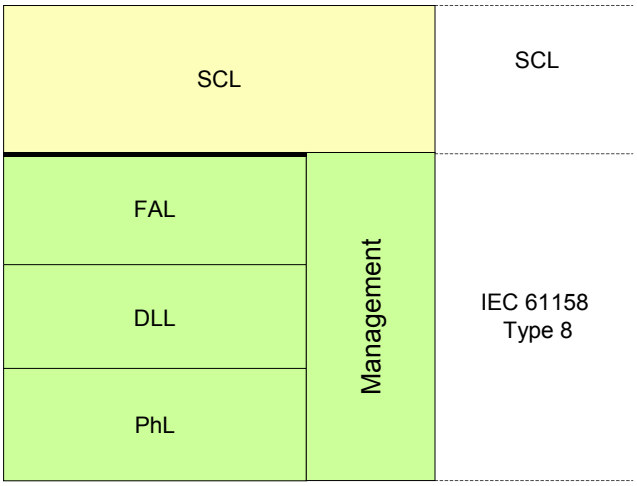
Anglais	Français
Safety decomposition	Décomposition de sécurité
Safety function	Fonction de sécurité
Input Safe Data	Données d'entrée sécurisées
Safe Transmission	Transmission sécurisée
Safe Calculation	Calcul sécurisé
Output Safe Data	Données de sortie sécurisées
Safety relevant application	Application relative à la sécurité
Safety communication layer (SCL)	Couche de communication de sécurité (SCL)
SCLS services	Services SCLS
SCLM services	Services SCLM
SCLS protocol	Protocole SCLS
SCLM protocol	Protocole SCLM
Slave	Esclave
Master	Maître
IEC 61158 Type 8	Type 8 de la CEI 61158

Figure 10 – Mise en correspondance du bloc de fonctions Transmission sécurisée

5.5 Relations avec la FAL (et DLL, PhL)

5.5.1 Présentation

Le paragraphe 5.5 explique comment la couche de communication de sécurité (SCL) utilise la couche d'application de bus de terrain (FAL). La Figure 11 illustre la relation entre la SCL et les autres couches de la pile de communication du Type 8 de la CEI 61158.



Légende

Anglais	Français
IEC 61158 Type 8	Type 8 de la CEI 61158
Management	Gestion

Figure 11 – Relation entre la SCL et les autres couches du Type 8 de la CEI 61158

La SCL définie dans la présente partie utilise le service AR-US (AR-Unconfirmed Send) de la CEI 61158-5-8 pour transférer les SPDU entre les entités SCL.

Pour transmettre les messages de sécurité, le maître de la couche de communication de sécurité (SCLM) doit utiliser le service de démarrage du Type 8 de la CEI 61158 conformément aux organigrammes séquentiels de l'Article 7. Les organigrammes séquentiels de l'Article 7 illustrent la transmission des messages de sécurité.

NOTE La SCL est accessible par le SRP (SCL: SCLS) ou le SRC (SCL: SCLM). Cet accès est spécifique à la mise en œuvre. Il est possible, par exemple, conformément au modèle D (Annexe A de la CEI 61784-3:2010).

5.5.2 Utilisation du service AR-US pour le démarrage et le paramétrage

La Figure 12 illustre l'utilisation du service AR-US avec les services SCL suivants:

— Initiate (Lancement);
— Send Application Parameter (Envoi du paramètre d'application);
— Send Application Parameter ID (Envoi de l'ID du paramètre d'application);
— Parameterize Device (Paramétrage du dispositif).

Ces services comportent plusieurs demandes AR-US et des primitives de service d'indication AR-US. Les séquences exactes sont présentées dans l'Article 7.

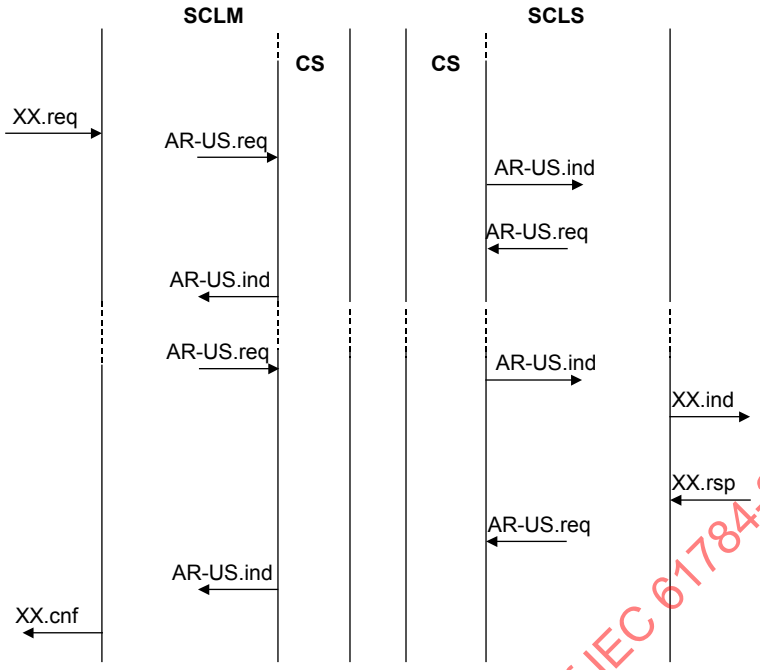


Figure 12 – Utilisation du service AR-US pour le démarrage et le paramétrage

La Figure 13 illustre l'utilisation du service AR-US par le service TDS (Transmit-Safety-Data – Transmission de données de sécurité).

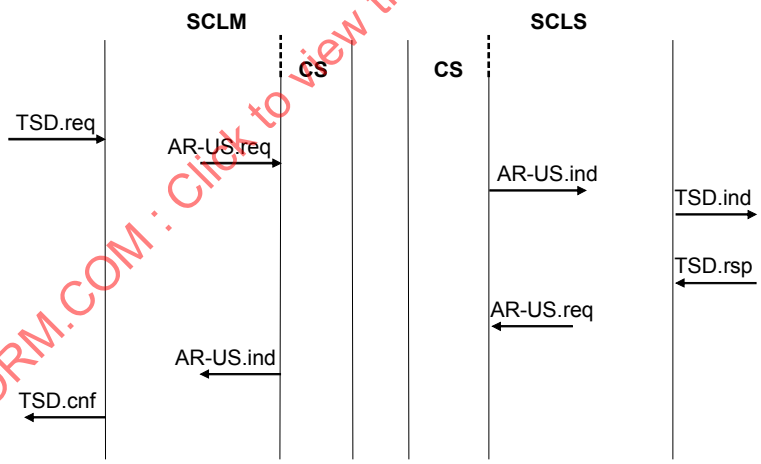


Figure 13 – Utilisation du service AR-US pour la transmission des données de sécurité

5.5.3 Utilisation du service AR-US pour la transmission des données de sécurité

La Figure 14 montre comment la couche de communication de sécurité utilise le service AR-US pour abandonner.

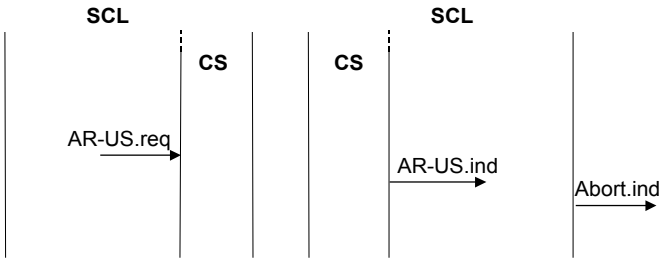


Figure 14 – Utilisation du service AR-US pour l'abandon

5.5.4 Utilisation du service AR-US pour l'abandon

La Figure 15 illustre l'utilisation du service AR-US par le service Abort (abandon).

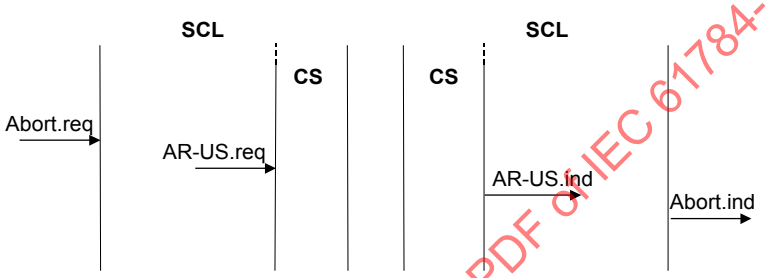


Figure 15 – Utilisation du service AR-US pour l'abandon

5.5.5 Types de données

Les types de données de sécurité sont spécifiés dans la CEI 61158-5-8:2007, Article 5.

NOTE Seuls les types de données dont la longueur de bit est inférieure au champ de données de sécurité peuvent être appliqués. Les types de données utilisés sont spécifiques au dispositif.

6 Services de la couche de communication de sécurité

6.1 Généralités

Les applications relatives à la sécurité utilisent les services suivants pour communiquer par l'intermédiaire de la couche de communication de sécurité:

- Initiate (Lancement);
- Abort (Abandon);
- Send Application Parameter (Envoi du paramètre d'application);
- Send Application Parameter ID (Envoi de l'ID du paramètre d'application);
- Parameterize Device (Paramétrage du dispositif);
- Transmit-Safety-Data (Transmission de données de sécurité);
- Set-Diagnostic-Data (Définition des données de diagnostic);
- Set-Acknowledgement-Data (Définition des données d'acquittement).

6.2 Principe de transmission des messages de sécurité entre le SCLM et le SCLS

Pour transmettre tous les messages de sécurité destinés aux SRP individuels des esclaves connectés et calculés par le SRC, le SCLM les met à la disposition du maître de Type 8 de la

CEI 61158. Ensuite, le SRC demande au maître de Type 8 de la CEI 61158 de lancer un cycle de données.

Le maître attribue les données à transmettre aux esclaves de sécurité connectés et aux esclaves standards, puis lance un nouveau cycle de données. Les données sont transmises aux esclaves qui, au même moment, renvoient leurs données au maître.

A l'issue du cycle de données, les esclaves transmettent les données reçues à leurs couches d'application (Latch-OUT). Au même instant, le maître fournit au SRC les données reçues des esclaves dans ce cycle de données et indique la fin du cycle. Les nouvelles données sont alors transférées à l'équipement de communication des esclaves pour la transmission dans le cycle de données suivant (Latch-IN). Les esclaves de sécurité entrent les données calculées provenant du cycle de données précédent dans l'équipement de communication.

A la réception du signal Latch-OUT, le SCLS est informé de la disponibilité des nouvelles données. Le SCLS interprète le message reçu comme un message de sécurité et le traite comme tel. Le SCLS a donc reçu les messages de sécurité.

Après avoir indiqué la fin du cycle de données, le SCLM lit les messages reçus. Il les interprète comme des messages de sécurité. Le SCLM a donc reçu les messages de sécurité. Toutefois, les messages antérieurs au signal Latch-IN ont été détectés.

Lorsque le SCLS a reçu les messages de sécurité de la part du SCLM, il en crée un et le met à la disposition pour une transmission à suivre. Les nouveaux messages ne sont pas entrés dans l'équipement de communication des esclaves de sécurité avant le début du cycle de données suivant. Par conséquent, le SCLM ne reçoit que la réponse au message de sécurité envoyé dans le seul cycle de données suivant.

6.3 Exigences relatives au bloc de fonctions

6.3.1 Bloc de fonctions Données d'entrée sécurisées

Après avoir reçu un service Transmit-Safety-Data.ind (voir 6.6.1), les informations d'entrée physique courantes relatives à la sécurité doivent être lues. Ces données doivent être envoyées avec le service Transmit-Safety-Data.res (voir 6.6.1) à l'aide du paramètre Safety_In_Data (voir 6.6.1). Cette opération doit avoir lieu avant la réception du service Transmit-Safety-Data.ind suivant.

Entre deux services Transmit-Safety-Data.ind, chaque sollicitation d'une fonction de sécurité doit être transmise avec le service Transmit-Safety-Data.res suivant.

6.3.2 Bloc de fonctions Données de sortie sécurisées

La fonction de sécurité reçue avec un service Transmit-Safety-Data.ind (voir 6.6.1) doit être sollicitée immédiatement. Si un service Transmit-Safety-Data.ind (voir 6.6.1) n'est pas reçu dans le temps d'arrêt paramétré, le bloc de fonctions doit être placé à l'état de sécurité. Pour cela, le paramètre Safety_In_Data_Time_Stamp du service Transmit-Safety-Data (6.6.1) doit être utilisé. Le temps d'arrêt paramétré peut être transmis avec l'enregistrement de paramètre d'application ou défini dans le bloc de fonctions.

6.3.3 Bloc de fonctions Calcul sécurisé

Pour activer l'opération en mode de données de processus, les connexions doivent être établies avec les esclaves de sécurité et les paramètres d'application doivent être transmis.

En mode de données de processus, tous les esclaves de sécurité sont traités de manière cyclique avec le service Transmit-Safety-Data.req (voir 6.6.1). Les données de sortie de sécurité transmises doivent être calculées en fonction des données d'entrée de sécurité du service Transmit-Safety-Data.con (voir 6.6.1) déjà reçu.

Lorsqu'un service Transmit-Safety-Data.con est reçu avec le paramètre Safety_In_Data_Valid = FALSE, les données déjà reçues doivent être utilisées pour le calcul.

Lorsqu'un service Abort.ind (voir 6.4.2) avec service Abort_Info issu du Tableau 8 et du Tableau 20 (voir 6.4.2) est reçu, le bloc de fonctions Calcul sécurisé doit utiliser la valeur zéro à la place de Safety_In_Data tant qu'un service Transmit-Safety-Data.con (voir 6.6.1) n'a pas été reçu avec le paramètre Safety_In_Data_Valid = TRUE.

Lorsqu'un service Abort.ind (voir 6.4.2) avec Abort_Info est issu du Tableau 21 ou du Tableau 22, le bloc de fonctions Calcul sécurisé doit être placé à l'état de sécurité.

6.4 Gestion de contexte

6.4.1 Service Initiate

Le service Initiate permet d'établir une connexion point à point. Les paramètres de ce service sont spécifiés dans le Tableau 5.

Tableau 5 – Paramètres du service Initiate

Nom du paramètre	Req	Ind	Rsp	Cnf
Argument	O	O		
Physical_Position	O			
Location_ID	O	O		
Parameterization_Mode	O	O		
Result(+)				O
Serial_Number			O	O
Vendor_ID			O	
Device_Type			O	
Device_Revision			O	
User_Data			O	O
SCLS_Revision			O	O

Argument

L'argument contient les paramètres de la demande de service.

Physical_Position

Ce paramètre indique le nombre de dispositifs de sécurité avec lesquels la connexion doit être établie.

Location_ID

Ce paramètre contient l'ID d'emplacement du dispositif [1 … 126]. Il est utilisé pour l'esclave.

Parameterization_Mode

Ce paramètre contient le mode de paramétrage. Le paramétrage doit être réalisé en fonction du mode de définition (1, 2, 3). Le Tableau 6 spécifie les services qui doivent être réalisés conformément au mode de paramétrage défini.

Tableau 6 – Mode de paramétrage et services connexes

Mode de paramétrage	Service
1	Send Application Parameter (Envoi du paramètre d'application)
2	Send Application Parameter ID (Envoi de l'ID du paramètre d'application)
3	Parameterize Device (Paramétrage du dispositif)

Result(+)

Ce paramètre de type de sélection indique que la demande de service a abouti. Il confirme donc que le dispositif contacté détient les ID de dispositif et d'emplacement corrects.

Serial_Number

Ce paramètre contient le numéro de série unique du dispositif contacté.

Vendor_ID

Ce paramètre contient l'ID fournisseur du dispositif contacté.

Device_Type

Ce paramètre contient le type de dispositif contacté.

Device_Revision

Ce paramètre contient la révision du dispositif contacté.

User_Data

Ce paramètre contient les données d'application (2 octets) lues par le dispositif contacté.

SCLS_Revision

Ce paramètre contient la révision SCLS.

6.4.2 Service Abort

Le service Abort permet d'annuler une connexion point à point. Les paramètres de ce service sont spécifiés dans le Tableau 7.

Tableau 7 – Paramètres du service Abort

Nom du paramètre	Req	Ind
Argument	O	O(=)
Location_ID	O	O(=)
Abort_Info	O	O
Additional_Info	O	O

Argument

L'argument contient les paramètres de la demande de service.

Location_ID

Ce paramètre contient l'ID d'emplacement du dispositif contacté [1 … 126]. Il est utilisé pour le dispositif.

Abort_Info

En cas d'abandon, ce paramètre contient:

— La raison de l'appel du service (voir le Tableau 8), ou

— La raison de l'abandon (Tableaux 8, 20, 21 et 22)

Additional_Info

Si des valeurs particulières apparaissent dans Abort_Info, ce paramètre contient des informations supplémentaires.

Tableau 8 – Abandon d'une connexion point à point par le SRP ou le SRC

Abort_Info	Appelé par	Signification
SRP_Detected_Error_Para	SRP	L'enregistrement du paramètre n'est pas cohérent.
SRP_Detected_Error_Para_ID	SRP	L'ID d'enregistrement du paramètre n'est pas valide.
SRP_Detected_Error_Loc_ID_Not_Saved	SRP	L'ID d'emplacement n'a pas été stocké définitivement.
Abort_Connection	SRC	Abandon lancé d'une connexion point à point.

6.5 Paramétrage du bloc de fonctions

6.5.1 **Service Send Application Parameter** (Envoi du paramètre d'application)

Ce service transmet l'enregistrement du paramètre d'application des dispositifs de sécurité. Les paramètres du service Send Application Parameter sont spécifiés dans le Tableau 9.

Tableau 9 – Service Send Application Parameter

Nom du paramètre	Req	Ind	Rsp	Cnf
Argument	O	O(=)		
Location_ID	O		O(=)	
Application_Parameter_Record	O	O		
Result(+)			O	O
Location_ID_Changed			O	O

Argument

L'argument contient les paramètres de la demande de service.

Location_ID

Ce paramètre contient l'ID d'emplacement du dispositif contacté [1 … 126]. Il est utilisé pour le dispositif.

Application_Parameter_Record

Ce paramètre contient le paramètre d'application et son numéro.

Result(+)

Ce paramètre de type de sélection indique que la demande de service a abouti.

Location_ID_Changed

Ce paramètre contient la valeur TRUE ou FALSE. Si TRUE, l'ID d'emplacement était différent et le nouvel ID a été accepté. Si FALSE, l'ID d'emplacement était correct.

6.5.2 Service Send Application Parameter ID (Envoi de l'ID du paramètre d'application)

Ce service transmet l'ID d'enregistrement du paramètre d'application. Si l'enregistrement existant du paramètre d'application stocké sur le dispositif porte le même ID d'enregistrement, celui-ci est utilisé. Les paramètres du service Send Application Parameter ID sont spécifiés dans le Tableau 10.

Tableau 10 – Service Send Application Parameter ID

Nom du paramètre	Req	Ind	Rsp	Cnf
Argument	O	O(=)		
Location_ID	O		O(=)	
Application_Parameter_Record_ID	O	O		
Result(+)			O	O
Location_ID_Changed			O	O

Argument

L'argument contient les paramètres de la demande de service.

Location_ID

Ce paramètre contient l'ID d'emplacement du dispositif contacté [1 … 126]. Il est utilisé pour le dispositif.

Application_Parameter_Record_ID

Ce paramètre contient l'ID d'un enregistrement de paramètre.

Result(+)

Ce paramètre de type de sélection indique que la demande de service a abouti.

Location_ID_Changed

Ce paramètre contient la valeur TRUE ou FALSE. Si TRUE, l'ID d'emplacement était différent et le nouvel ID a été accepté. Si FALSE, l'ID d'emplacement était correct.

6.5.3 Service « Parameterize Device »

Ce service permet d'activer l'enregistrement de paramètre du SRP des dispositifs de sécurité avec l'ID d'enregistrement de paramètre d'application, si ce dernier est identique à celui reçu.

Ce service transmet le paramètre d'application et l'ID d'enregistrement de paramètre d'application. Les paramètres du service Parameterize Device sont présentés dans le Tableau 11.

Tableau 11 – Paramètres du service Parameterize Device

Nom du paramètre	Req	Ind	Rsp	Cnf
Argument	O	O(=)		
Location_ID	O		O(=)	
Application_Parameter_Record	O	O		
Application_Parameter_Record_ID	O	O		
Result(+)			O	O
Location_ID_Changed			O	O

Argument

L'argument contient les paramètres de la demande de service.

Location_ID

Ce paramètre contient l'ID d'emplacement du dispositif contacté [1 … 126]. Il est utilisé pour le dispositif.

Application_Parameter_Record

Ce paramètre contient le paramètre d'application et son numéro.

Application_Parameter_Record_ID

Ce paramètre contient l'ID d'un enregistrement de paramètre.

Result(+)

Ce paramètre de type de sélection indique que la demande de service a abouti.

Location_ID_Changed

Ce paramètre contient la valeur TRUE ou FALSE. Si TRUE, l'ID d'emplacement était différent et le nouvel ID a été accepté. Si FALSE, l'ID d'emplacement était correct.

6.6 Mode de données de processus sécurisé

6.6.1 **Transmit-Safety-Data** (Transmission de données de sécurité)

Le bloc de fonctions Transmission sécurisée utilise ce service pour transmettre des données de sortie de sécurité du SRC vers le SRP, et inversement. Le bloc de fonctions Données de sortie sécurisées utilise les datations pour déterminer l'âge des données d'entrée de sécurité utilisées pour calculer les données de sortie de sécurité. Les paramètres du service Transmit-Safety-Data sont spécifiés dans le Tableau 12.

Tableau 12 – Paramètres du service Transmit-Safety-Data

Nom du paramètre	Req	Ind	Res	Cnf
Argument	O	O(=)		
Location_ID	O			
Safety_Out_Data	F	F		
Safety_Out_Data_Valid		O		
Safety_In_Data_Time_Stamp		C		
Safety_In_Data_ACK		O		
Result			S	S
Location_ID				O(=)
Safety_In_Data			F	F
Safety_In_Data_Valid				C
Actual_Time_Stamp			C	

Argument

L'argument contient les paramètres de la demande de service.

Location_ID

Ce paramètre contient l'ID d'emplacement du dispositif contacté [1 … 126]. Il est utilisé pour le dispositif.

Safety_Out_Data

Ce paramètre contient les données de sortie de sécurité.

Safety_Out_Data_Valid

Ce paramètre indique si les données du paramètre Safety_Out_Data sont valides et peuvent être utilisées.

Safety_In_Data_Time_Stamp

Le bloc de fonctions Données de sortie sécurisées utilise ce paramètre pour lire l'heure à laquelle les données d'entrée sécurisées utilisées pour calculer ces données de sortie sécurisées ont été lues dans son SCLS. Si la datation = 0, seuls les zéros de Safety_Out_Data peuvent être transférés vers les sorties.

Safety_In_Data_ACK

Ce paramètre contient une copie de Safety_In_Data. Les bits de Safety_In_Data dont la valeur est 1 sont immédiatement copiés dans Safety_In_Data_ACK, ceux dont la valeur est 0 étant copiés dans Safety_In_Data_ACK lorsque le SRC les a reçus. Le SCLS peut être sûr que ces bits ont été reçus si le numéro de séquence a été correctement incrémenté de 3.

Result

Ce paramètre de type de sélection indique que la demande de service a abouti.

Safety_In_Data

Ce paramètre contient les données d'entrée de sécurité.

Safety_In_Data_Valid

Ce paramètre indique si les données du paramètre Safety_In_Data sont valides et peuvent être utilisées.

Actual_Time_Stamp

Ce paramètre contient l'heure d'envoi de la demande.

Le bloc de fonctions Données de sortie sécurisées utilise ce paramètre pour transmettre l'heure d'appel de la demande à son SCLS.

6.6.2 **Service Set-Diagnostic-Data** (Définition des données de diagnostic)

Le service Set-Diagnostic-Data permet de transmettre les données de diagnostic du SCLS au SCLM. Les paramètres du service Set-Diagnostic-Data sont présentés dans le Tableau 13.

Tableau 13 – Paramètres du service Set-Diagnostic-Data

Nom du paramètre	Req	Ind
Argument	O	O(=)
Location_ID		O
Diagnostic_Data	O	O(=)

Argument

L'argument contient les paramètres de la demande de service.

Location_ID

Ce paramètre contient l'ID d'emplacement du dispositif contacté [1 … 126]. Il est utilisé pour le dispositif.

Diagnostic_Data

Ce paramètre contient les données de diagnostic d'un dispositif de sécurité avec l'ID d'emplacement spécifié.

6.6.3 **Service Set-Acknowledgement-Data** (Définition des données d'acquittement)

Le service Set-Acknowledgement-Data permet de transmettre les données d'acquittement du SCLM au SCLS. Les paramètres du service Set-Acknowledgement-Data sont présentés dans le Tableau 14.

Tableau 14 – Paramètres du service Set-Acknowledgement-Data

Nom du paramètre	Req	Ind
Argument	O	O(=)
Location_ID	O	
Acknowledgement_Data	O	O(=)

Argument

L'argument contient les paramètres de la demande de service.

Location_ID

Ce paramètre contient l'ID d'emplacement du dispositif contacté [1 … 126]. Il est utilisé pour le dispositif.

Acknowledgement_Data

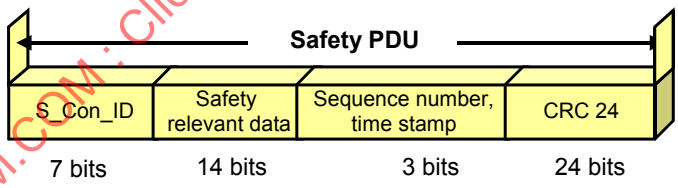
Ce paramètre contient les acquittements des données de diagnostic du dispositif de sécurité avec l'ID d'emplacement spécifié.

7 Protocole de couche de communication de sécurité

7.1 Format PDU de sécurité

7.1.1 Structure des messages de sécurité

La structure du PDU de sécurité comprenant les mesures correctives déterministes et les données de sécurité est spécifiée dans la Figure 16.



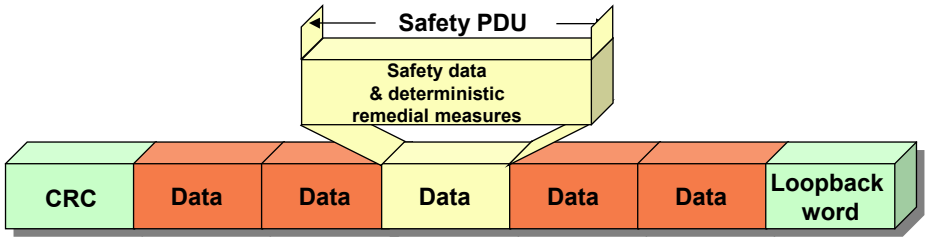
Légende

Anglais	Français
Safety PDU	PDU de sécurité
Safety relevant data	Données relatives à la sécurité
Sequence number, time stamp	Numéro de séquence, datation

Figure 16 – Structure du PDU de sécurité

Le message de sécurité est composé de 24 bits d'informations (14 bits de données de sécurité + ID de connexion de sécurité à 7 bits + numéro de séquence à 3 bits) et d'une somme de contrôle à 24 bits.

Le PDU de sécurité (SPDU) de chaque esclave de sécurité est intégré dans le PhPDU du Type 8 de la CEI 61158 (voir la Figure 17).



Légende

Anglais	Français
Safety data & deterministic remedial measures	Données de sécurité et des mesures correctives déterministes
Data	Données
Loopback word	Mot de boucle de retour

Figure 17 – Intégration des données de sécurité et des mesures correctives déterministes dans le cadre de sommation

7.1.2 Description du polynôme utilisé

L'Equation (1) spécifie le polynôme utilisé pour calculer le CRC.

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

La description des propriétés du code sélectionné n'entre pas dans le domaine d'application de la présente partie.

7.1.3 Structure des messages de sécurité du paramétrage sécurisé et de l'état de repos

7.1.3.1 Généralités

La transmission de tous les paramètres est relative à la sécurité. Par conséquent, il convient de placer des exigences de niveau élevé équivalent pour les messages de paramètre et les messages de transmission de données de sécurité.

Les messages suivants sont utilisés dans la phase de paramétrage:

- 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 des messages

7.1.3.2.1 Write_Parameter_Byte_Req

Si le SCLM souhaite envoyer un octet de paramètre à un SCLS, le message **Write_Parameter_Byte_Req** est utilisé (Figure 18):

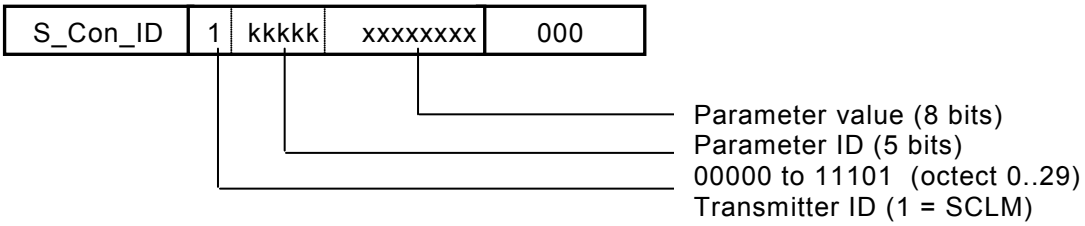


Figure 18 – Message Write_Parameter_Byte_Req

7.1.3.2.2 Read_Parameter_Byte_Req

Si le SCLM souhaite lire un octet de paramètre provenant d'un SCLS, le message **Read_Parameter_Byte_Req** est utilisé (Figure 19):

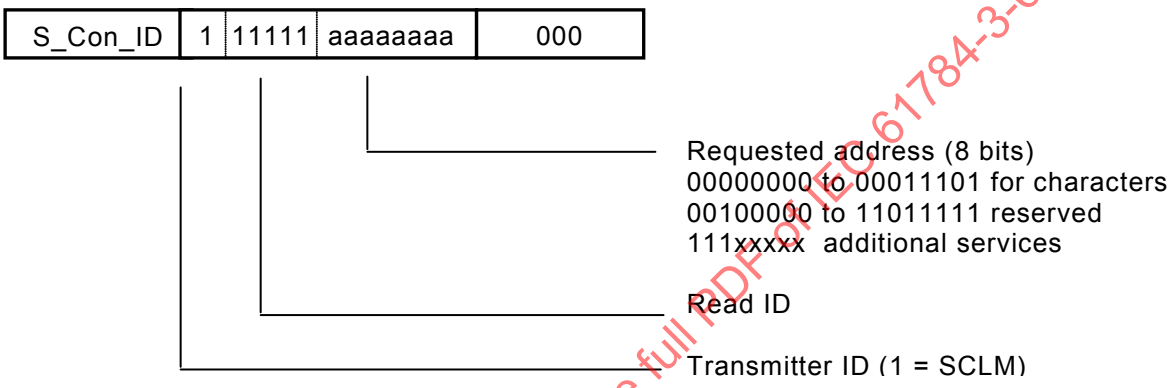


Figure 19 – Message Read_Parameter_Byte_Req

7.1.3.2.3 Parameter_Byte_Con

Dans les deux cas, le SCLS répond par un message **Parameter_Byte_Con** (Figure 20).

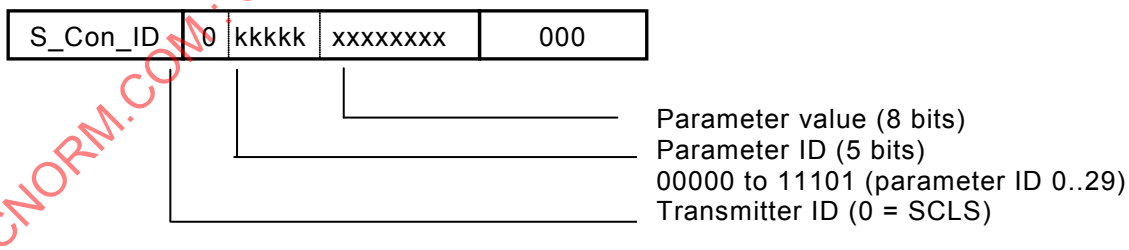


Figure 20 – Message Parameter_Byte_Con

7.1.3.2.4 Utilisation des messages de paramètre

Lorsqu'un octet avec l'ID de paramètre correspondant est écrit, une réponse est toujours envoyée par retour de la valeur écrite.

Le Tableau 15 spécifie les ID de paramètre des dispositifs de sécurité.

Tableau 15 – ID de paramètre

ID de paramètre	ID de paramètre	Signification
00000	0	Réservé à l'ID de connexion de sécurité
00001	1	SCLS_Revision
00010	2	ID d'emplacement
00011	3	Mode de paramétrage
00100	4	réservé, ne doit pas être utilisé
00101	5	réservé, ne doit pas être utilisé
00110	6	réservé, ne doit pas être utilisé
00111	7	réservé, ne doit pas être utilisé
01000	8	réservé, ne doit pas être utilisé
01001	9	ID de bloc (n)
01010	10	Données provenant du bloc n
:	:	: :
11101	29	Données provenant du bloc n
11110	30	Réservé
11111	31	Demande de lecture et messages supplémentaires avec services spéciaux

Les octets avec l'ID de paramètre 0 à 9 contiennent des paramètres requis pour la communication sécurisée.

Les octets avec l'ID de paramètre 10 à 29 sont considérés comme un bloc et sont disponibles 256 fois. Le bloc, qui peut être traité à l'aide des ID de paramètre 01010 (10 dec) à 11101 (29 dec), est spécifié par l'ID de bloc (octet 9). L'ID de bloc est donc une extension de l'ID de paramètre.

Les blocs 0 et 1 sont réservés à l'ID de dispositif et l'ID d'enregistrement de paramètre (voir le Tableaux 16 et 17). L'ID d'enregistrement de paramètre permet une identification unique des enregistrements de paramètre.

NOTE Pour les informations relatives à la génération de l'ID d'enregistrement de paramètre, il est vivement recommandé de prendre contact avec INTERBUS-Club.

Les octets dotés d'ID de paramètre réservés ne doivent pas être utilisés. Néanmoins, l'utilisateur doit être informé d'une éventuelle utilisation du champ d'octet d'un ID de paramètre et un message d'erreur doit être généré.

Tableau 16 – Bloc 0: ID de dispositif

ID de paramètre	Signification
10	Octet 1 du numéro de série
11	Octet 2 du numéro de série
12	Octet 3 du numéro de série
13	Octet 4 du numéro de série
14	Octet 5 du numéro de série
15	Octet 6 du numéro de série
16	Octet 1 de l'ID fournisseur
17	Octet 2 de l'ID fournisseur
18	Octet 3 de l'ID fournisseur

ID de paramètre	Signification
19	Octet 4 de l'ID fournisseur
20	Octet 1 de l'ID de type de dispositif
21	Octet 2 de l'ID de type de dispositif
22	Octet 3 de l'ID de type de dispositif
23	Octet 4 de l'ID de type de dispositif
24	Octet 5 de l'ID de type de dispositif
25	Octet 6 de l'ID de type de dispositif
26	Octet 7 de l'ID de type de dispositif
27	Octet 1 de la révision de dispositif
28	Octet 1 du paramètre de lecture (spécifique au dispositif)
29	Octet 2 du paramètre de lecture (spécifique au dispositif)

Tableau 17 – Bloc 1: ID d'enregistrement de paramètre

ID de paramètre	Signification
10	Octet 1 de l'ID d'enregistrement de paramètre
11	Octet 2 de l'ID d'enregistrement de paramètre
12	Octet 3 de l'ID d'enregistrement de paramètre
13	Octet 4 de l'ID d'enregistrement de paramètre
14	Octet 5 de l'ID d'enregistrement de paramètre
15	Octet 6 de l'ID d'enregistrement de paramètre
16	Octet 7 de l'ID d'enregistrement de paramètre
17	Octet 8 de l'ID d'enregistrement de paramètre
18	Octet 9 de l'ID d'enregistrement de paramètre
19	Octet 10 de l'ID d'enregistrement de paramètre
20	Octet 11 de l'ID d'enregistrement de paramètre
21	Octet 12 de l'ID d'enregistrement de paramètre
22	réservé, ne doit pas être utilisé
23	réservé, ne doit pas être utilisé
24	réservé, ne doit pas être utilisé
25	réservé, ne doit pas être utilisé
26	réservé, ne doit pas être utilisé
27	réservé, ne doit pas être utilisé
28	réservé, ne doit pas être utilisé
29	réservé, ne doit pas être utilisé

Les blocs 2 à 255 peuvent être utilisés librement pour les paramètres d'application. Pour le bloc 2, les deux premiers octets doivent contenir le nombre de paramètres subséquents (y compris tous les blocs supplémentaires). Voir le Tableau 18.

Tableau 18 – Bloc 2: Paramètre d'application

ID de paramètre	Signification
10	Nombre d'octets de paramètre subséquent (élevé)
11	Nombre d'octets de paramètre subséquent (bas)
12	Paramètre d'application
13	Paramètre d'application
:	:
:	:
29	Paramètre d'application

Par conséquent, le nombre maximal de paramètres qui peut être transmis est de:
254 × 20 – 2 = 5 078 octets.

7.1.3.2.5 Message Set_Safety_Connection_ID_Req

Le SCLM utilise le message Set_Safety_Connection_ID_Req (spécifié dans la Figure 21) pour transmettre l'ID de connexion de sécurité au SCLS des esclaves de sécurité.

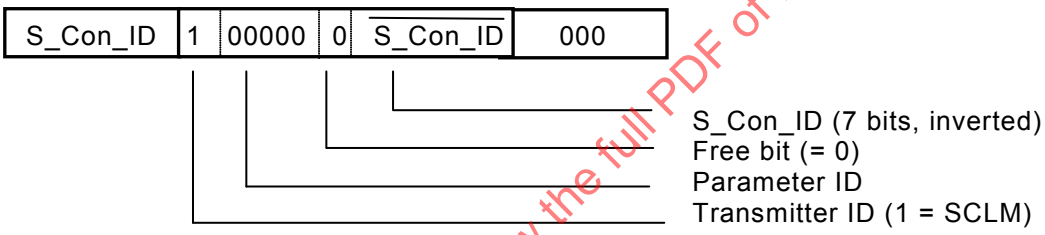


Figure 21 – Message Set_Safety_Connection_ID_Req

7.1.3.2.6 Message Set_Safety_Connection_ID_Con des esclaves de sécurité

Le SCLS utilise le message Set_Safety_Connection_ID_Con (spécifié dans la Figure 22) pour transmettre son ID de connexion de sécurité au SCLM.

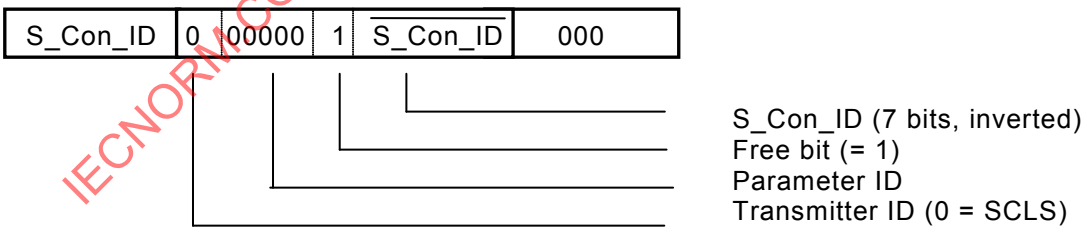


Figure 22 – Message Set_Safety_Connection_ID_Con des esclaves de sécurité

7.1.3.2.7 Parameter_Idle_Req

Une fois les paramètres transmis, le SCLM envoie les messages Parameter_Idle_Req. Le SCLS répond par le message Parameter_Idle_Con et, après vérification des paramètres, par les messages Parameter_Check_Con et Parameter_Loc_ID_Changed_Con. La structure des messages est spécifiée des Figures 23 à 26.

Le idle_count (nombre ou compte de mises en repos) à 3 bits permet de modifier le codage du message qui suit.

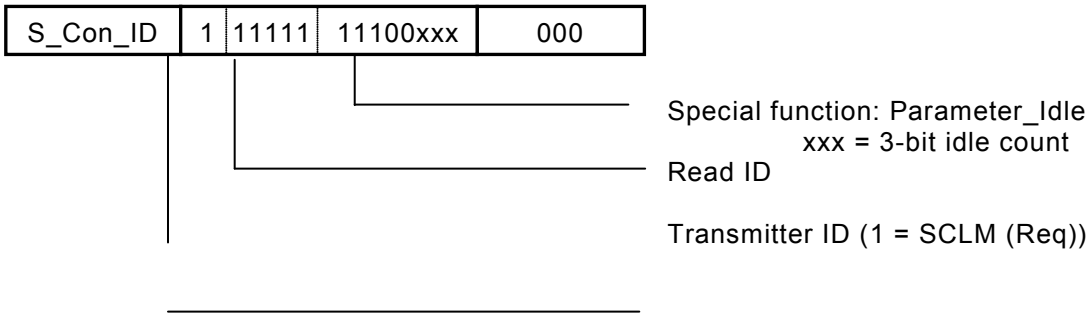


Figure 23 – Parameter_Idle_Req

7.1.3.2.8 Parameter_Idle_Con

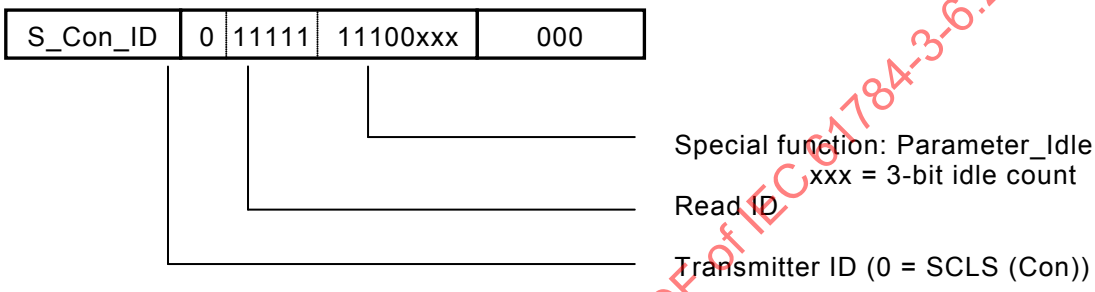


Figure 24 – Parameter_Idle_Con

7.1.3.2.9 Parameter_Check_Con

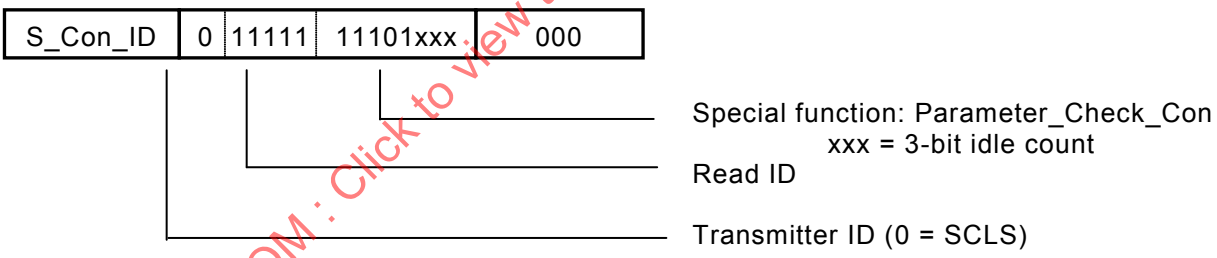


Figure 25 – Parameter_Check_Con

7.1.3.2.10 Parameter_Loc_ID_Changed_Con

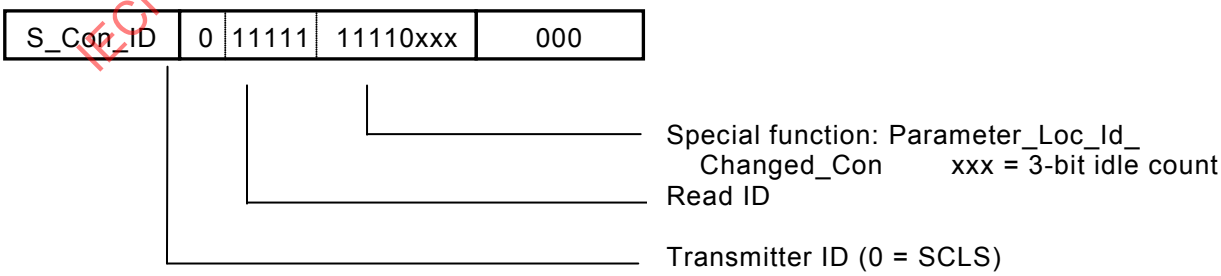


Figure 26 – Parameter_Loc_ID_Changed_Con

7.1.4 Structure des messages de sécurité pour la transmission des données de sécurité

La Figure 27 illustre la structure du message de transmission des données de sécurité.

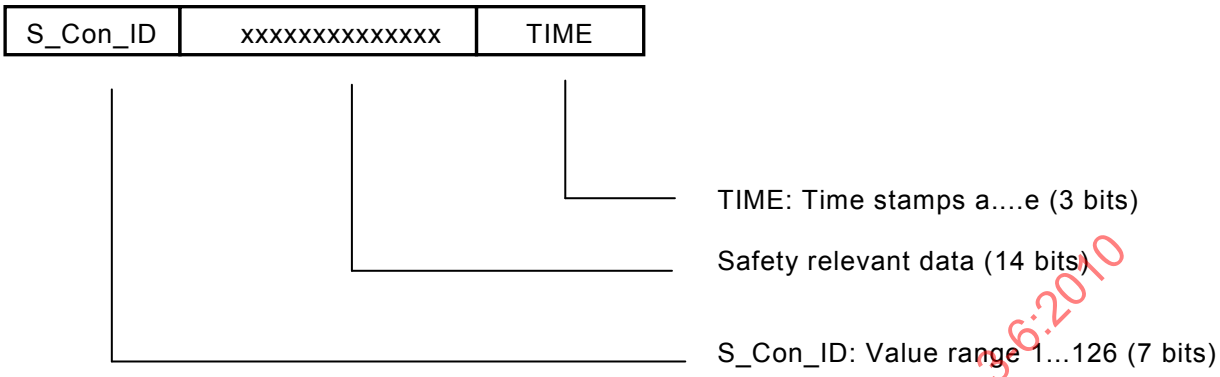


Figure 27 – Message de transmission des données de sécurité

Les messages de sécurité contiennent un numéro de séquence (TIME) codé par une valeur à 3 bits (voir le Tableau 19).

Tableau 19 – Codage TIME

Numéro de séquence	Codage TIME	Remarques
-	000	
Sync_a	001	
a	010	Transmission du numéro de séquence a et des données de processus
b	011	Transmission du numéro de séquence b et des données de processus
c	100	Transmission du numéro de séquence c et des données de processus
d	101	Transmission du numéro de séquence d et des données de processus
e	110	Transmission du numéro de séquence e et des données de processus
e	111	Transmission du numéro de séquence e et diagnostic/acquittement et données de processus inchangées

Ces messages transmettent des données de sécurité entre le SCLS et le SCLM, et entre le SCLM et le SCLS des esclaves de sécurité. L'ID de l'émetteur/récepteur est indiqué par la séquence des valeurs de TIME.

Le numéro de séquence est incrémenté de a à e. Lorsque e est atteint, le SCLM/SCLS compare les données de processus à transmettre à celles qui ont été envoyées avec le numéro de séquence d. Si les données de processus sont inchangées, le SCLM/SCLS peut envoyer des données d'acquittement/de diagnostic à la place des données de processus. Il convient de procéder à cette opération si un service Set-Acknowledgement-Data.req/Set-Diagnostic-Data.req est en attente.

7.1.5 Messages de synchronisation

7.1.5.1 Message Sync_a du SCLM

Le SCLM utilise les messages Sync_a pour synchroniser la datation de tous les esclaves de sécurité « valides » (Figure 28). Ce message est toujours envoyé à tous les esclaves de sécurité en même temps. La première synchronisation d'un esclave de sécurité fait suite au paramétrage. En recevant le message Sync_a, il passe de l'état de paramétrage sécurisé à l'état de transmission sécurisée des données de processus.

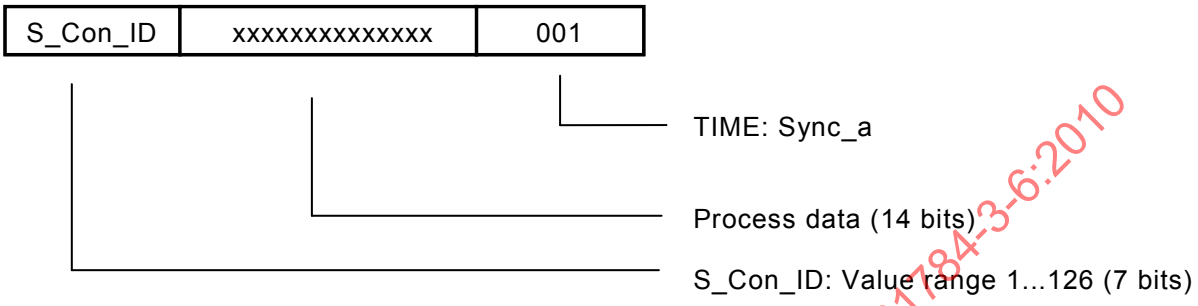


Figure 28 – Message Sync_a du SCLM

7.1.5.2 Message Req_b du SCLM

Le message Req_b du SCLM est spécifié dans la Figure 29.

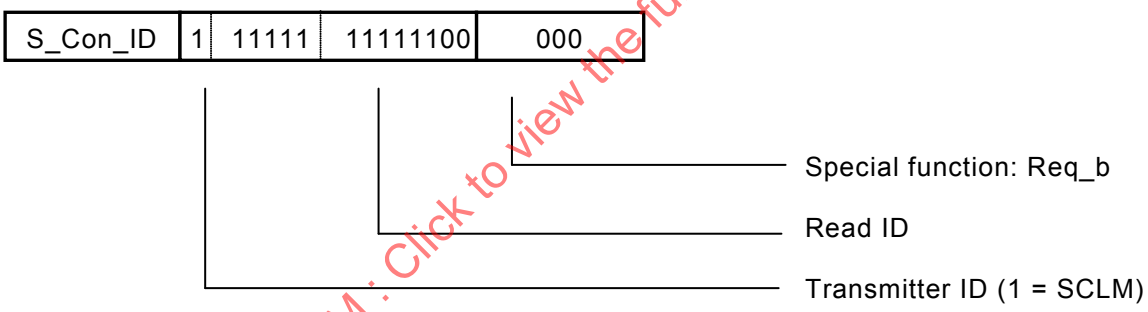


Figure 29 – Message Req_b du SCLM

7.1.5.3 Message Req_c du SCLM

Le message Req_c du SCLM est spécifié dans la Figure 30.

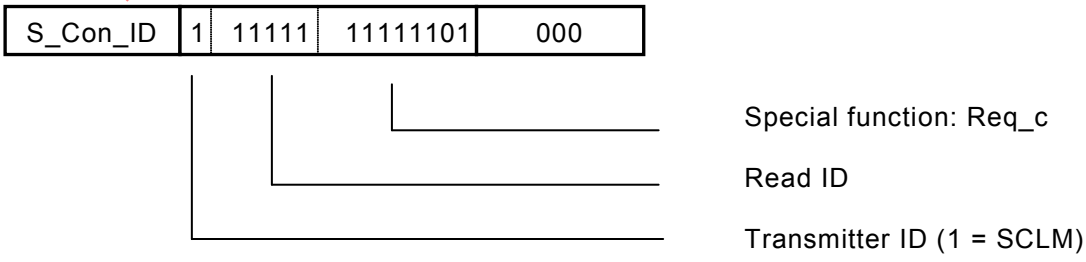


Figure 30 – Message Req_c du SCLM

7.1.5.4 Message Req_d du SCLM

Le message Req_d du SCLM est spécifié dans la Figure 31.

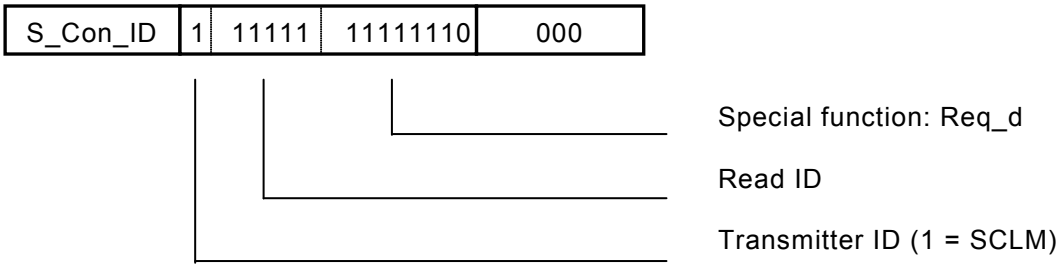


Figure 31 – Message Req_d du SCLM

Ces messages de sécurité (Figure 28 à Figure 31) sont utilisés au début et au cours de la transmission sécurisée des données de processus à partir du SCLM, afin de synchroniser la datation (TIME) dans le SCLS des esclaves de sécurité. La séquence des messages est prédéfinie. En cas d'erreur, le SCLS concerné entre en état de connexion abandonnée et répond par un message Safety_Slave_Error.

7.1.6 Structure des messages de sécurité d'abandon des connexions

7.1.6.1 Message Abort_Connection du SCLM

Ce message (Figure 32) permet d'envoyer un service Abort.ind à l'esclave de sécurité. Il transmet Abort_Info = Abort_Connection.

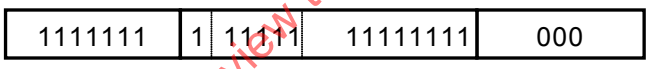
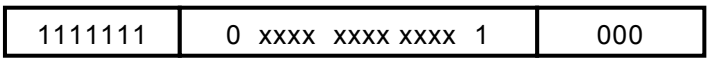


Figure 32 – Message Abort_Connection

7.1.6.2 Message Safety_Slave_Error des esclaves de sécurité

Les esclaves de sécurité envoient ce message (Figure 33) si une erreur a été détectée dans la séquence de paramétrage ou pendant leur fonctionnement, donnant lieu à un nouveau paramétrage. Le type d'erreur est également transmis.

Cet état peut uniquement être maintenu en cas de réception d'un message Set_Safety_Connection_ID de la part du SCLM.



NOTE xxxx xxxx xxxx est Abort_Info.

Figure 33 – Message Safety-Slave_Error

7.2 Description d'état

7.2.1 Diagrammes d'états du SCLM et du SCLS

La Figure 34 et la Figure 35 illustrent respectivement le diagramme d'états du SCLM et celui du SCLS.