IEC 61784-3-8

Edition 3.0 2021-05

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Industrial communication networks – Profiles – Part 3-8: Functional safety fieldbuses – Additional specifications for CPF 8

Réseaux de communication industriels – Profils – Partie 3-8: Bus de terrain de sécurité fonctionnelle – Spécifications supplémentaires pour CPF 8

IEC 61784-3-8:2021-05(en-fr)

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
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 corrigendum or an amendment might have been published.

IEC publications search - webstore.iec.ch/advsearchform
The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee, …). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

IEC Customer Service Centre - webstore.iec.ch/csc
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

IEC online collection - oc.iec.ch
Discover our powerful search engine and read freely all the publications previews. With a subscription you will always have access to up to date content tailored to your needs.

Electropedia - www.electropedia.org
The world's leading online dictionary on electrotechnology, containing more than 22 000 terminological entries in English and French, with equivalent terms in 18 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

A propos de l'IEC
La Commission Electrotechnique Internationale (IEC) 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 IEC
Le contenu technique des publications IEC est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Recherche de publications IEC - webstore.iec.ch/advsearchform
La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études, …). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

IEC Just Published - webstore.iec.ch/justpublished
Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et une fois par mois par email.

Service Clients - webstore.iec.ch/csc
Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: sales@iec.ch.

IEC online collection - oc.iec.ch
Découvrez notre puissant moteur de recherche et consultez gratuitement tous les aperçus des publications. Avec un abonnement, vous aurez toujours accès à un contenu à jour adapté à vos besoins.

Electropedia - www.electropedia.org
Le premier dictionnaire d'électrotechnologie en ligne au monde, avec plus de 22 000 articles terminologiques en anglais et en français, ainsi que les termes équivalents dans 16 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

IEC 61784-3-8

Edition 3.0 2021-05

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Industrial communication networks – Profiles – Part 3-8: Functional safety fieldbuses – Additional specifications for CPF 8

Réseaux de communication industriels – Profils – Partie 3-8: Bus de terrain de sécurité fonctionnelle – Spécifications supplémentaires pour CPF 8

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

ICS 25.040.40; 35.100.05

ISBN 978-2-8322-9751-3

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES –

Part 3-8: Functional safety fieldbuses – Additional specifications for CPF 8

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.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

IEC 61784-3-8 has been prepared by subcommittee 65C: Industrial networks, of IEC technical committee 65: Industrial-process measurement, control and automation. It is an International Standard.

This third edition cancels and replaces the second edition published in 2016. This edition constitutes a technical revision.

This edition includes the following significant technical changes with respect to the previous edition:

- structured for compliance with IEC 61784-3 Ed.4;
- general editorial changes and clarifications;
- safety measures (11.5.3);

- safety application service elements (11.6.2);
- safety PDU format (11.7.1);
- constraints for calculations of system characteristics (11.9.5);
- safety measures (12.5.3);
- safety PDU format (12.7.1);
- behaviour (12.7.2);
- constraints for calculations of system characteristics (12.9.5);
- hash function calculations (Annex A).

The text of this International Standard is based on the following documents:

FDIS	Report on voting
65C/1083/FDIS	65C/1087/RVD

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

The language used for the development of this International Standard is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/standardsdev/publications.

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 document will remain unchanged until the stability date indicated on the IEC website under "http://webstore.iec.ch" in the data related to the specific document. At this date, the document 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.

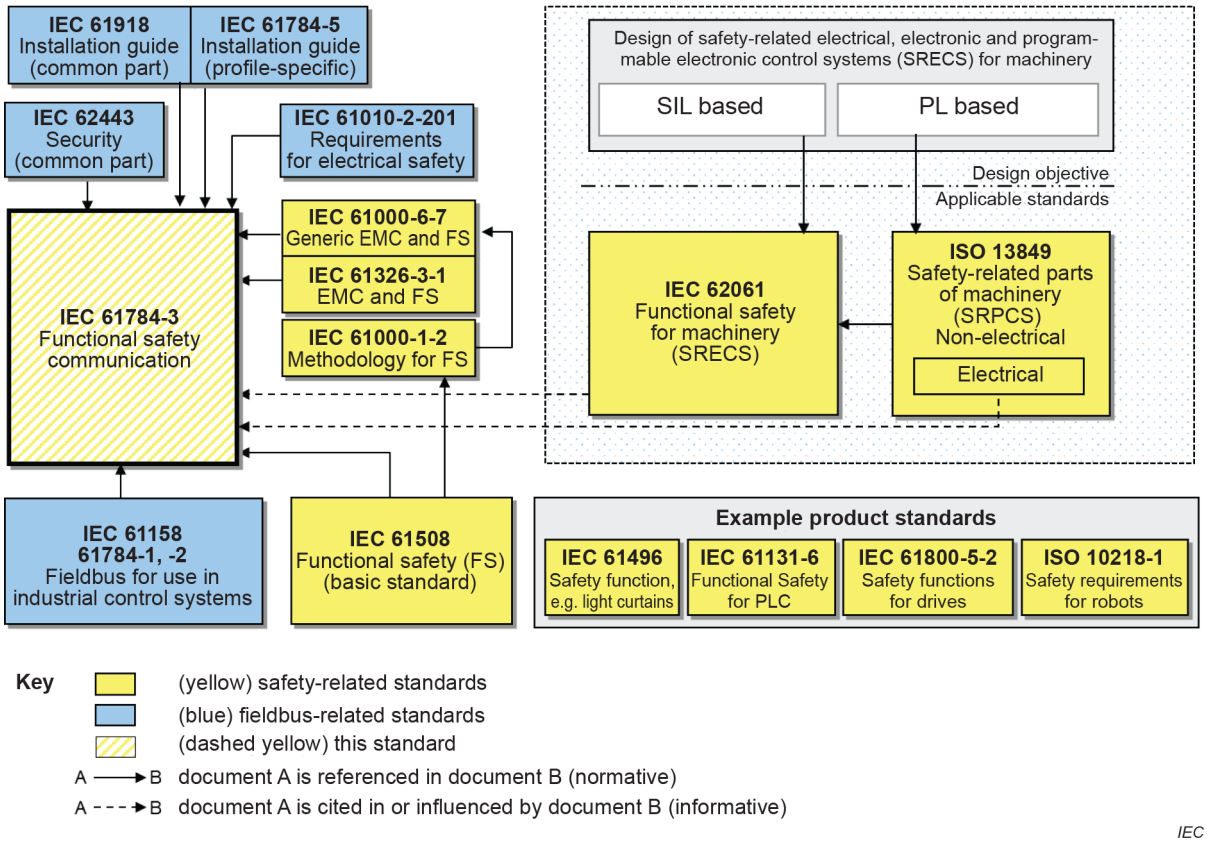
0 Introduction

0.1 General

The IEC 61158 (all parts) 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 fieldbus enhancements continue to emerge, addressing applications for areas such as real time and safety-related applications.

IEC 61784-3 (all parts) explains the relevant principles for functional safety communications with reference to IEC 61508 (all parts) 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 IEC 61158 (all parts). It does not cover electrical safety and intrinsic safety aspects. It also does not cover security aspects, nor does it provide any requirements for security.

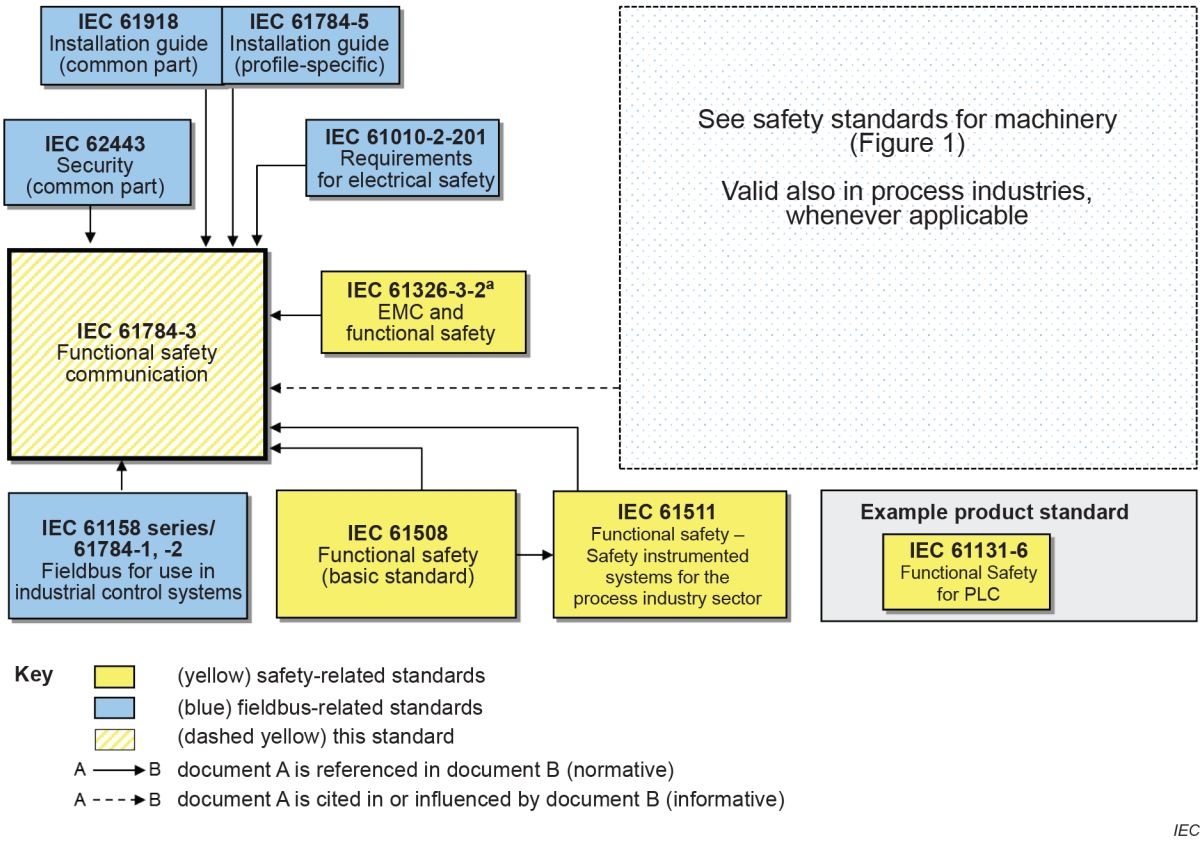
Figure 1 shows the relationships between IEC 61784-3 (all parts) and relevant safety and fieldbus standards in a machinery environment.



NOTE IEC 62061 specifies the relationship between PL (Category) and SIL.

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

Figure 2 shows the relationships between IEC 61784-3 (all parts) and relevant safety and fieldbus standards in a process environment.



[a] For specified electromagnetic environments; otherwise IEC 61326-3-1 or IEC 61000-6-7.

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 (all parts) 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 IEC 61784-3 (all parts) 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 (FSCP) within this system – implementation of a functional safety communication profile in a standard device is not sufficient to qualify it as a safety device.

IEC 61784-3 (all parts) describes:

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

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 a patent concerning the functional safety communication profiles for family 8. IEC takes no position concerning the evidence, validity, and scope of this patent right.

The holder of this patent right has assured IEC that s/he is willing to negotiate licences under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statement of the holder of this patent right is registered with IEC. Information may be obtained from the patent database available at http://patents.iec.ch.

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

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES –

Part 3-8: Functional safety fieldbuses – Additional specifications for CPF 8

1 Scope

This part of IEC 61784-3 (all parts) specifies a safety communication layer (services and protocol) based on CPF 8 of IEC 61784-1, IEC 61784-2 and IEC 61158 Type 18 and Type 23. It identifies the principles for functional safety communications defined in IEC 61784-3 that are relevant for this safety communication layer. This safety communication layer is intended for implementation in safety devices only.

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 document 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 (all parts)[1] for functional safety. These mechanisms may be used in various industrial applications such as process control, manufacturing automation and machinery.

This document 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 document in a standard device is not sufficient to qualify it as a safety device.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 61131-2, *Industrial-process measurement and control – Programmable controllers – Part 2: Equipment requirements and tests*

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 61158-3-18, *Industrial communication networks – Fieldbus specifications – Part 3-18: Data-link layer service definition – Type 18 elements*

IEC 61158-4-18, *Industrial communication networks – Fieldbus specifications – Part 4-18: Data-link layer protocol specification – Type 18 elements*

---

1 In the following pages of this document, "IEC 61508" will be used for "IEC 61508 (all parts)".

IEC 61158-5-18, *Industrial communication networks – Fieldbus specifications – Part 5-18: Application layer service definition – Type 18 elements*

IEC 61158-5-23, *Industrial communication networks – Fieldbus specifications – Part 5-23: Application layer service definition – Type 23 elements*

IEC 61158-6-18, *Industrial communication networks – Fieldbus specifications – Part 6-18: Application layer protocol specification – Type 18 elements*

IEC 61158-6-23, *Industrial communication networks – Fieldbus specifications – Part 6-23: Application layer protocol specification – Type 23 elements*

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*

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*

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/IEEE 8802-3*

IEC 61784-3:2021, *Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions*

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

ISO/IEC/IEEE 8802-3, *Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 3: Standard for Ethernet*

3 Terms, definitions, symbols, abbreviated terms and conventions

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC 61784-3 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp

NOTE Italics are used in the definitions to highlight terms which are themselves defined in 3.1.

3.1.1 Common terms and definitions

NOTE These common terms and definitions are inherited from IEC 61784-3:2021.

3.1.1.1
absolute time stamp
time stamp referenced to a global time which is common for a group of devices using a *fieldbus*

[SOURCE: IEC 62280:2014, 3.1.1, modified – use of "devices" and "fieldbus" instead of "entities" and "transmission system"]

3.1.1.2
active network element
network element containing electrically and/or optically active components that allows extension of the network

Note 1 to entry: Examples of active network elements are repeaters and switches.

[SOURCE: IEC 61918:2018, 3.1.2]

3.1.1.3
bit error probability
Pe
probability for a given bit to be received with the incorrect value

3.1.1.4
black channel
defined communication system containing one or more elements without evidence of design or validation according to IEC 61508

Note 1 to entry: This definition expands the usual meaning of channel to include the system that contains the channel.

3.1.1.5
bridge
abstract device that connects multiple network segments along the data link layer

3.1.1.6
closed communication system
fixed number or fixed maximum number of participants linked by a *communication system* with well-known and fixed properties, and where the *risk* of unauthorized access is considered negligible

[SOURCE: IEC 62280:2014, 3.1.6, modified – transmission replaced by communication]

3.1.1.7
communication channel
logical *connection* between two end-points within a *communication system*

3.1.1.8
communication system
arrangement of hardware, software and propagation media to allow the transfer of *messages* (ISO/IEC 7498-1 application layer) from one application to another

3.1.1.9
connection
logical binding between two application objects within the same or different devices

3.1.1.10
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 to entry: Terms "CRC code" and "CRC signature", and labels such as CRC1, CRC2, may also be used in this document to refer to the redundant data.

Note 2 to entry: See also [26], [27][2].

3.1.1.11
defined communication system
defined channel
fixed number or fixed maximum number of participants linked by a *fieldbus* based *communication system* with well-known and fixed properties, such as installation conditions, electromagnetic immunity, industrial *(active) network elements*, and where the *risk* of unauthorized access is reduced to a tolerated level according to the lifecycle model of IEC 62443 (all parts), using for example zones and conduits

3.1.1.12
diversity
different means of performing a required function

Note 1 to entry: Diversity may be achieved by different physical methods or different design approaches.

[SOURCE: IEC 61508-4:2010, 3.3.7]

3.1.1.13
DLPDU
DEPRECATED: frame
Data Link Protocol Data Unit

3.1.1.14
error
discrepancy between a computed, observed or measured value or condition and the true, specified or theoretically correct value or condition

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

Note 2 to entry: Errors do not necessarily result in a *failure* or a *fault*.

[SOURCE: IEC 61508-4:2010, 3.6.11, modified – notes added]

3.1.1.15
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 to entry: Failure may be due to an *error* (for example, problem with hardware/software design or *message* disruption).

[SOURCE: IEC 61508-4:2010, 3.6.4, modified – notes and figures replaced]

---

2 Figures in square brackets refer to the bibliography.

3.1.1.16
fault
abnormal condition that may cause a reduction in, or loss of, the capability of a functional unit to perform a required function

Note 1 to entry: IEC 60050-191:1990, 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.

[SOURCE: IEC 61508-4:2010, 3.6.1, modified – figure reference deleted]

3.1.1.17
fieldbus
communication system based on serial data transfer and used in industrial automation or process control applications

3.1.1.18
fieldbus system
system using a *fieldbus* with connected devices

3.1.1.19
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 to entry: An FCS can be derived using for example a CRC or other *hash function*.

Note 2 to entry: See also [26], [27].

3.1.1.20
hash function
(mathematical) function that maps values from a (possibly very) large set of values into a (usually) smaller range of values

Note 1 to entry: Hash functions can be used to detect data corruption.

Note 2 to entry: Common hash functions include parity, checksum or CRC.

3.1.1.21
hazard
potential source of harm

Note 1 to entry: The term includes danger to persons arising within a short time scale (for example, fire and explosion) and also those that have a long-term effect on a person's health (for example, release of a toxic substance).

[SOURCE: IEC 61508-4:2010, 3.1.2 and ISO/IEC Guide 51:2014, definition 3.2]

3.1.1.22
master
communication entity able to initiate and schedule communication activities by other stations which may be masters or *slaves*

3.1.1.23
message
<information theory and communication theory> ordered sequence of characters (usually octets) intended to convey information

[SOURCE: ISO/IEC 2382:2015, 2123205, modified – insertion of "(usually octets)", deletion of notes and source]

3.1.1.24
message sink
information sink
part of a *communication system* in which *messages* are considered to be received

[SOURCE: ISO/IEC 2382:2015, 2123207, modified – deletion of notes and source]

3.1.1.25
message source
information source
part of a *communication system* from which *messages* are considered to originate

[SOURCE: ISO/IEC 2382:2015, 2123206, modified – deletion of notes and source]

3.1.1.26
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

[SOURCE: ISO 13849-1:2015, 3.1.23]

3.1.1.27
redundancy
existence of more than one means for performing a required function or for representing information

[SOURCE: IEC 61508-4:2010, 3.4.6, modified – example and notes deleted]

3.1.1.28
relative time stamp
time stamp referenced to the local clock of an entity

Note 1 to entry: In general, there is no relationship to clocks of other entities.

[SOURCE: IEC 62280:2014, 3.1.43, modified – format adjusted]

3.1.1.29
residual error probability
RP
probability of an *error* undetected by the SCL *safety measures*

3.1.1.30
residual error rate
statistical rate at which the SCL *safety measures* fail to detect *errors*

3.1.1.31
risk
combination of the probability of occurrence of harm and the severity of that harm

Note 1 to entry: For more discussion on this concept see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6, and ISO/IEC Guide 51:2014, definition 3.9, modified – different note]

3.1.1.32
safety communication channel
communication channel starting at the top of the SCL of the source and ending at the top of the SCL of the sink

Note 1 to entry: It can be modelled as two SCLs connected by a *black channel* or a *defined communication system*, or a *defined channel*.

3.1.1.33
safety communication layer
SCL
communication layer above the FAL that includes all necessary additional measures to ensure safe transmission of data in accordance with the requirements of IEC 61508

3.1.1.34
safety connection
connection that utilizes the safety protocol for communications transactions

3.1.1.35
safety data
data transmitted across a safety network using a safety protocol

Note 1 to entry: The *Safety Communication Layer* does not ensure safety of the data itself, only that the data is transmitted safely.

3.1.1.36
safety device
device designed in accordance with IEC 61508 and which implements the functional safety communication profile

3.1.1.37
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

[SOURCE: IEC 61508-4:2010, 3.5.1, modified – references and example deleted]

3.1.1.38
safety function response time
worst case elapsed time following an actuation of a safety sensor connected to a *fieldbus*, until the corresponding safe state of its safety actuator(s) is achieved in the presence of *errors* or *failures* in the *safety function*

Note 1 to entry: This concept is introduced in IEC 61784-3:2021, 5.2.4 and addressed by the functional safety communication profiles defined in this document.

3.1.1.39
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 to entry: 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.

Note 2 to entry: 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 to entry: 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.

[SOURCE: IEC 61508-4:2010, 3.5.8]

3.1.1.40
safety measure
measure to control possible communication *errors* that is designed and implemented in compliance with the requirements of IEC 61508

Note 1 to entry: In practice, several safety measures are combined to achieve the required *safety integrity level*.

Note 2 to entry: Communication *errors* and related safety measures are detailed in IEC 61784-3:2021, 5.3 and 5.4.

3.1.1.41
safety PDU
SPDU
PDU transferred through the *safety communication channel*

Note 1 to entry: The SPDU may include more than one copy of the *safety data* using differing coding structures and *hash functions* together with explicit parts of additional protections such as a key, a sequence count, or a *time stamp* mechanism.

Note 2 to entry: Redundant SCLs may provide two different versions of the SPDU for insertion into separate fields of the *fieldbus frame*.

3.1.1.42
safety-related application
programs designed in accordance with IEC 61508 to meet the SIL requirements of the application

3.1.1.43
safety-related system
system performing *safety functions* according to IEC 61508

3.1.1.44
slave
communication entity able to receive *messages* and send them in response to another communication entity which may be a *master* or a slave, but not to initiate communication activities

3.1.1.45
spurious trip
trip caused by the safety system without a process demand

3.1.1.46
timeliness code
time information included in a *message*

3.1.1.47
uniform distribution
probability distribution where all values from a finite set are equally likely to occur

Note 1 to entry: For a field of bit length i the probability of occurrence of a particular field value is 2^{-i} since the sum of all probabilities of occurrence is equal to 1.

3.1.1.48
white channel
defined communication system in which all relevant hardware and software elements are designed, implemented and validated according to IEC 61508

Note 1 to entry: This definition expands the usual meaning of channel to include the system that contains the channel.

3.1.2 CPF 8: Additional terms and definitions

3.1.2.1
cycle
interval at which an activity is repetitively and continuously executed

3.1.2.2
safety application relationship
SAR
application relationship between two or more safety related application relationship endpoints

3.1.2.3
safety application service element
SASE
safety related application service element

3.1.2.4
safety clock
clock (counter) for recording the time of occurrence of events such as the transmission and reception of safety communication related messages

3.1.2.5
safety data monitor timer
timer used by the time expectation function for safety data transmission

3.1.2.6
safety monitor timer
timer used by the time expectation function for safety connection management

3.1.2.7
safety refresh
periodic transmission and reception of safety data between master and slave stations

3.1.2.8
slot
one quantum (granularity) of the position dependent mapping of the cyclic data fields

3.1.2.9
station
device and its corresponding SAREP associated with the transmission and reception of safety data

Note 1 to entry: The station number is used in the position dependent mapping of the cyclic data fields (a station occupies one or more slots).

3.1.2.10
safety protocol transmission information
information distinguishing safety relevant messages

3.2 Symbols and abbreviated terms

3.2.1 Common symbols and abbreviated terms

A-code	Authentication code	
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	
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 (all parts)]
FS	Functional Safety	
FSCP	Functional Safety Communication Profile	
FSPM	FAL Service Protocol Machine	[IEC 61158-1]
MTBF	Mean Time Between Failures	
MTTF	Mean Time To Failure	
PDU	Protocol Data Unit	[ISO/IEC 7498-1]
Pe	Bit error probability	
PhL	Physical Layer	[ISO/IEC 7498-1]
PL	Performance Level	[ISO 13849-1]
PLC	Programmable Logic Controller	
SCL	Safety Communication Layer	
SIL	Safety Integrity Level	[IEC 61508-4:2010]
SPDU	Safety PDU	
T-code	Timeliness code	

3.2.2 CPF 8: Additional symbols and abbreviated terms

AR	Application Relationship
ASE	Application Service Element
CC	Carry Counter
CID	Connection Identifier
CMD	Command Data
LED	Light Emitting Diode
LID	Link Identifier
OBL	Offset Baseline
RNO	Running Number
SAR	Safety Application Relationship
SAREP	Safety Application Relationship Endpoint
SARPM	Safety Application Relationship Protocol State Machine
SASE	Safety Application Service Element
SFSPM	Safety FSPM (appended with -S Slave or -M Mater)
SRC	Safety Relevant Controller
SRP	Safety Relevant Peripheral
TPI	Safety Transmission Packet Information
TPI-T	Safety Transmission Packet Information from master
TPI-R	Safety Transmission Packet Information from slave
TS	Time Stamp

3.3 Conventions

Conventions used in this document are defined in IEC 61158 Type 18 and Type 23, IEC 61784-1 CPF 8 and IEC 61784-2 CPF 8.

In order to assist the reader familiar with the standard clause numbering and for the purpose of consistency and alignment with IEC 61784-3, Clauses 4 to 10 reference Clauses 11 to 17 for FSCP 8/1 and Clauses 18 to 24 for FSCP 8/2.

4 Overview

For overview information pertaining to FSCP 8/1, see 11.4. For overview information pertaining to FSCP 8/2, see 12.4.

5 General

For general information pertaining to FSCP 8/1, see 11.5. For general information pertaining to FSCP 8/2, see 12.5.

6 Safety communication layer services

For safety communication layer services information pertaining to FSCP 8/1, see 11.6. For safety communication layer services information pertaining to FSCP 8/2, see 12.6.

7 Safety communication layer protocol

For safety communication layer protocol information pertaining to FSCP 8/1, see 11.7. For safety communication layer protocol information pertaining to FSCP 8/2, see 12.7.

8 Safety communication layer management

For safety communication layer management information pertaining to FSCP 8/1, see 11.8. For safety communication layer management information pertaining to FSCP 8/2, see 12.8.

9 System requirements

For system requirements information pertaining to FSCP 8/1, see 11.9. For system requirements information pertaining to FSCP 8/2, see 12.9.

10 Assessment

For assessment information pertaining to FSCP 8/1, see 11.10. For assessment information pertaining to FSCP 8/2, see 12.10.

11 FSCP 8/1

11.1 Scope – FSCP 8/1

See Clause 1.

11.2 Normative references – FSCP 8/1

See Clause 2.

11.3 Terms, definitions, symbols, abbreviated terms and conventions – FSCP 8/1

See Clause 3.

11.4 Overview of FSCP 8/1 (CC-Link Safety™)

Communication Profile Family 8 (commonly known as CC-Link™ [3]) defines communication profiles based on IEC 61158-2 Type 18, IEC 61158-3-18, IEC 61158-4-18, IEC 61158-5-18, and IEC 61158-6-18.

The basic profiles CP 8/1, CP 8/2, and CP 8/3 are defined in IEC 61784-1. The CPF 8 functional safety communication profile FSCP 8/1 (CC-Link Safety™ [3]) is based on the CPF 8 basic profiles in IEC 61784-1 and the safety communication layer specifications defined in this document.

---

[3] CC-Link™ and CC-Link Safety™ are trade names of the non-profit organization CC-Link Partner Association. This information is given for the convenience of users of this document and does not constitute an endorsement by IEC of the trade name holder or any of its products. Compliance to this document does not require use of the trade names CC-Link™ or CC-Link Safety™. Use of the trade names CC-Link™ or CC-Link Safety™ requires permission of CC-Link Partner Association and compliance with conditions for their use (such as testing and validation).

FSCP 8/1 is a protocol for communicating safety-relevant data such as emergency stop signals among participants within a distributed network using fieldbus technology in accordance with the requirements of IEC 61508 for functional safety. This protocol is used in various applications such as process control, manufacturing automation and machinery.

The FSCP 8/1 protocol is designed to support Safety Integrity Level SIL3 (IEC 61508) using CPF 8 by additionally specifying mechanisms for the implementation of sequence number, time expectation, connection authentication, feedback message, data integrity assurance and different data integrity assurance safety measures.

SCL capabilities for FSCP 8/1 are provided with the introduction of safety application service elements (SASE). These SASEs are used in place of their corresponding ASEs as specified in this document. However, since inheriting directly from the parent classes defined for CPF 8, these SASEs specify required additions to CPF 8 for functional safety using a black channel approach.

11.5 General – FSCP 8/1

11.5.1 External documents providing specifications for the profile

Manufacturers of FSCP 8/1 safety devices are encouraged to check documents [30], [31] and [32] which provide additional specifications relevant for implementation of the SCL defined in this document.

11.5.2 Safety functional requirements

This document specifies the services and protocols for a functional safety communication system based on IEC 61158 Type 18. The communication technologies specified in this document shall only be implemented in devices designed in accordance with the requirements of IEC 61508.

The following requirements shall apply to the development of devices that implement FSCP 8/1 protocols. The same requirements were used in the development of FSCP 8/1.

- The FSCP 8/1 protocols are designed to support Safety Integrity Level SIL3 (refer to IEC 61508).
- Implementations of FSCP 8/1 shall comply with IEC 61508.
- The basic requirements for the development of the FSCP 8/1 protocol are specified in IEC 61784-3.
- The safety state for discrete data is the de-energized state (0). For analog values the de-energized state shall be defined by the safety-related application.
- Environmental conditions shall be according to IEC 61131-2 for the basic levels and IEC 61326-3-1, IEC 61326-3-2 for the safety margin tests, unless there are specific product standards.
- Unless specified in this document, the CPF 8 requirements shall be unchanged for safety.

11.5.3 Safety measures

11.5.3.1 General

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

– sequence number;

– time expectation;

– connection authentication;

– feedback message;

- data integrity assurance;
- redundancy with cross-checking;
- different data integrity assurance systems.

The selection of the various measures for possible errors is shown in Table 1.

Table 1 – 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	X	
Unintended repetition	X							
Incorrect sequence	X							
Loss	X							
Unacceptable delay			X					
Insertion	X			X	X			
Masquerade				X	X		X	X
Addressing				X				
NOTE Table adapted from IEC 62280:2014								

11.5.3.2 Sequence number

Safety messages contain a sequence number (RNO) with a width of 24 bits and a specified sequence (see 11.7.1 and 11.7.2). This RNO is a combination of RNO-1 (4 bits) RNO-2 (4 bits) and RNO-3 (16 bits). If the sequence is not followed, all safety related output signals shall be set to their safe states.

11.5.3.3 Time expectation

An integrated watchdog timer providing the time expectation of each output channel on each safety output slave ensures a safety function response 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 11.9.3.

The safety function response 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 safety function response 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.

11.5.3.4 Connection authentication

The connection authentication is implemented by a set of a safety connection ID (Link ID) and a station number. Each safety slave uses a 3 bit Link ID which specifies its safety network system. This provides the SRC with up to 8 safety network systems. The assignment of Link ID values shall be unique within a functional safety communication system. The safety messages always contain the Link ID.

11.5.3.5 Feedback message

A feedback message is provided from each slave that confirms receipt of messages from the master. The feedback message contains error status information from the slave as well as acknowledgment of the RNO, link ID, and command ID.

11.5.3.6 Data integrity assurance

Data integrity is assured using the CRCs included in the safety PDU. The transmitting node sends the safety PDU including its calculated CRCs. The receiving node compares the CRCs included in the received safety PDU with the CRCs calculated from the received safety PDU, and determines if corruption occurred.

11.5.3.7 Redundancy with cross checking

The receiving node cross checks the redundant portions of the received safety PDU to verify that these portions match each other bit-for-bit.

11.5.3.8 Different data integrity assurance system

Distinction between safety relevant messages and non-safety relevant messages: Safety messages contain a CRC checksum (32 bits). The IEC 61158 Type 18 protocol uses a different CRC algorithm (16-bit CRC). Additionally, each telegram contains an 8-bit command ID, a 3-bit link ID and a 24-bit RNO and each of these components shall conform to the restrictions as defined for these fields.

11.5.4 Safety communication layer structure

SCL capabilities for FSCP 8/1 are provided with the introduction of safety application service elements (SASE). These SASEs are used in place of their corresponding application service elements (ASEs) as specified herein. Since they inherit directly from the parent classes defined for CPF 8, these SASEs specify additions to CPF 8. The SASEs are implemented based on the following:

– Device manager – ASE class specifications for M1 and S1 type device manager;
– Connection manager – AR class definition for M1 and S1 type connection manager;
– Cyclic transmission – Process data AR ASE class specification for M1 and S1 type cyclic transmission.

The SCL augments these ASE definitions with:

– M1 and S1 type safety device manager;
– M1 and S1 type safety connection manager;
– M1 and S1 type safety cyclic transmission.

All management, behaviors and functions of the SCL are handled with these safety application service elements.

11.5.5 Relationships with FAL (and DLL, PhL)

11.5.5.1 Overview

Figure 3 shows the relationship between the SCL and the other layers of the IEC 61158 Type 18 communication stack.

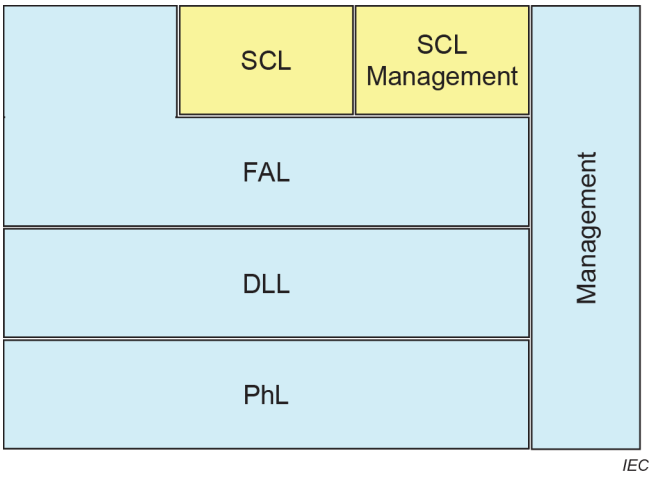


Figure 3 – Relationship between SCL and the other layers of IEC 61158 Type 18

11.5.5.2 Data types

Data types of safety data are specified in IEC 61158-5-18.

11.6 Safety communication layer services for FSCP 8/1

11.6.1 General

The FSCP 8/1 SAR uses buffered transport for process data inputs and outputs. Transmission triggering type services are required depending upon the configuration of the instantiated objects. Connection management is handled by the safety connection manager class. Safety-related applications use safety application service elements to communicate via the safety communication layer. The formal model of these service elements is defined in 11.6.

11.6.2 SASEs

11.6.2.1 M1 safety device manager class specification

The M1 safety device manager class supports a master type SCL user on a polled type DL implementation.

SCL ASE:			Management SASE
CLASS:			M1 safety device manager
CLASS ID:			not used
PARENT CLASS:			M1 device manager
ATTRIBUTES:			
1	(m)	Attribute:	Management information
1.1	(m)	Attribute:	Link id
1.2	(o)	Attribute:	Software/protocol version
2	(m)	Attribute:	Connected slaves management information
2.1	(m)	Attribute:	Software/protocol version 1
…	…	…	…
2.n	(m)	Attribute:	Software/protocol version n

...	...	...	...
2.64	(m)	Attribute:	Software/protocol version 64

11.6.2.2 S1 safety device manager class specification

The S1 safety device manager class supports a slave type SCL user on a polled type DL implementation.

SCL ASE:			Management SASE
CLASS:			S1 safety device manager
CLASS ID:			not used
PARENT CLASS:			S1 device manager
ATTRIBUTES:			
1	(m)	Attribute:	Management information
1.1	(m)	Attribute:	Link id
1.2	(m)	Attribute:	Software/protocol version

11.6.3 SARs

11.6.3.1 M1 safety connection manager class

The M1 safety connection manager class supports a master type SCL user on a polled type DL implementation.

SCL ASE:			Management SASE
CLASS:			M1 safety connection manager
CLASS ID:			not used
PARENT CLASS:			M1 connection manager
ATTRIBUTES:			
1	(m)	Attribute:	Parameter information
1.1	(m)	Attribute:	Safety monitor timer value
1.2	(m)	Attribute	Safety data monitor timer value
1.3	(m)	Attribute:	Safety slave specification
1.4	(m)	Attribute:	Safety slave specification source
1.5	(m)	Attribute:	Safety slave product information
2	(m)	Attribute:	Safety slave parameter data
3	(m)	Attribute	Safety slave link status

11.6.3.2 S1 safety connection manager class

The S1 safety connection manager class supports a slave type SCL user on a polled type DL implementation.

SCL ASE:			Management SASE
CLASS:			S1 safety connection manager
CLASS ID:			not used
PARENT CLASS:			S1 connection manager
ATTRIBUTES:			
1	(m)	Attribute:	Safety product information
2	(m)	Attribute:	Safety slave parameter data

11.6.4 Process data SAR ASEs

11.6.4.1 M1 safety cyclic transmission class specification

The M1 safety cyclic transmission class supports a master type SCL user in association with an M1 safety connection manager.

SCL ASE:			Process Data SAR ASE
CLASS:			M1 safety cyclic transmission
CLASS ID:			not used
PARENT CLASS:			M1 cyclic transmission
ATTRIBUTES:			
1.	(m)	Attribute:	Data out
1.1.	(m)	Attribute:	Safety RY data
1.2.	(m)	Attribute:	RWw data
1.2.1.	(m)	Attribute:	Safety RWw data
1.2.2.	(m)	Attribute:	Safety TPI-T
1.3.	(m)	Attribute:	Safety RY-r data
1.4.	(m)	Attribute:	RWw-r data
1.4.1.	(m)	Attribute:	Safety RWw-r data
1.4.2.	(m)	Attribute:	Safety TPI-T-r
2.	(m)	Attribute:	Data in
2.1.	(m)	Attribute:	Safety data in 1
2.1.1.	(m)	Attribute:	Safety RX data 1
2.1.2.	(m)	Attribute:	RWr data 1
2.1.2.1	(m)	Attribute:	Safety RWr data 1
2.1.2.2	(m)	Attribute:	Safety TPI-R 1
2.1.3.	(m)	Attribute:	Safety RX-r data 1
2.1.4.	(m)	Attribute:	RWr-r data 1
2.1.4.1	(m)	Attribute:	Safety RWr-r data 1
2.1.4.2	(m)	Attribute:	Safety TPI-R-r 1
…	…	…	…
2.n.	(m)	Attribute:	Safety data in n
…	…	…	…
2.64.	(m)	Attribute:	Safety data in 64

11.6.4.2 S1 safety cyclic transmission class specification

The S1 safety cyclic transmission class supports a slave type SCL user in association with an S1 safety connection manager.

SCL ASE:			Process Data SAR ASE
CLASS:			S1 safety cyclic transmission
CLASS ID:			not used
PARENT CLASS:			S1 cyclic transmission
ATTRIBUTES:			
1.	(m)	Attribute:	Data out
1.1	(m)	Attribute:	Safety RY data
1.2	(m)	Attribute:	RWw data
1.2.1.	(m)	Attribute:	Safety RWw data
1.2.2.	(m)	Attribute:	Safety TPI-T
1.3	(m)	Attribute:	Safety RY-r data
1.4	(m)	Attribute:	RWw-r data
1.4.1.	(m)	Attribute:	Safety RWw-r data
1.4.2.	(m)	Attribute:	Safety TPI-T-r
2.	(m)	Attribute:	Data in
2.1	(m)	Attribute:	Safety RX data
2.2	(m)	Attribute:	RWr data
2.2.1	(m)	Attribute:	Safety RWr data
2.2.2	(m)	Attribute:	Safety TPI-R
2.3	(m)	Attribute:	Safety RX-r data
2.4	(m)	Attribute:	RWr-r data
2.4.1	(m)	Attribute:	Safety RWr-r data
2.4.2	(m)	Attribute:	Safety TPI-R-r

11.7 Safety communication layer protocol for FSCP 8/1

11.7.1 Safety PDU format

11.7.1.1 General

The safety PDU syntax and encoding is described as in IEC 61158-6-18 in terms of abstract syntax and transfer syntax.

11.7.1.2 Abstract syntax

11.7.1.2.1 M1 safety device manager PDU abstract syntax

The abstract syntax for attributes belonging to this class is described in Table 2.

Table 2 – M1 safety device manager attribute format

Attribute	Format	Size (bits)
Management information	Structure of 2 elements:	11
Link id	Unsigned3	3
Software/protocol version	1 octet, bit mapped	8
Connected slave management information	Array of 64 members:	64 octets
Software/protocol version	1 octet, bit mapped	8

11.7.1.2.2 S1 safety device manager PDU abstract syntax

The abstract syntax for attributes belonging to this class is described in Table 3.

Table 3 – S1 safety device manager attribute format

Attribute	Format	Size (bits)
Management information	Structure of 3 elements:	11
Link id	Unsigned3	3
Software/protocol version	1 octet, bit mapped	8

11.7.1.2.3 M1 safety connection manager PDU abstract syntax

The abstract syntax for attributes belonging to this class is described in Table 4.

Table 4 – M1 safety connection manager attribute format

Attribute	Format	Size (bits)
Parameter information	Structure of 5 elements:	2 004 octets
Safety monitor timer value	Unsigned16	16
Safety data monitor timer value	Unsigned16	16
Safety slave specification	8 octets, bit mapped	64
Safety slave specification source	8 octets, bit mapped	64
Safety slave product information	Array of 64 members:	1 984 octets
Safety product information 1 – 64	Word oriented data structure	31 octets
Safety slave parameter data	16 – 52 224 octets	16 – 52 224 octets
Safety slave link status	8 octets, bit mapped	64

11.7.1.2.4 S1 safety connection manager PDU abstract syntax

The abstract syntax for attributes belonging to this class is described in Table 5.

Table 5 – S1 safety connection manager attribute format

Attribute	Format	Size (bits)
Safety product information 1 – 64	Word oriented data structure	31 octets
Safety slave parameter data	16 – 816 octets	16 – 816 octets

11.7.1.2.5 M1 safety cyclic transmission PDU abstract syntax

The abstract syntax for attributes belonging to this class is described in Table 6.

Table 6 – M1 safety cyclic transmission attribute format

Attribute	Format	Size (bits)
Data out	Structure of 2 elements:	192 × n
Safety RY data	Bit-oriented data structure	32 × n
RWw data	Word-oriented data structure	64 × n
Safety RWw data	Word-oriented data	64 × (n – m)
Safety TPI-T	Safety transmission packet information	64 × m
Safety RY-r data	Bit-oriented data structure	32 × n
RWw-r data	Word-oriented data structure	64 × n
Safety RWw-r data	Word-oriented data	64 × (n – m)
Safety TPI-T-r	Safety transmission packet information	64 × m
Data in	Structure of n elements	192 × n
Safety data in 1	Structure of 2 elements	192
Safety RX data	Bit-oriented data structure	64
RWr data	Word-oriented data structure	128
Safety RWr data	Word-oriented data	64
Safety TPI-R	Safety transmission packet information	64
Safety RX-r data	Bit-oriented data structure	32
RWr-r data	Word-oriented data structure	64
Safety RWr-r data	Word-oriented data	64
Safety TPI-R-r	Safety transmission packet information	64
…	…	…
Safety data in n	Structure of 2 elements	192
NOTE The values of n and m are dependent upon the values of the corresponding configuration settings in the master status.		

11.7.1.2.6 S1 safety cyclic transmission PDU abstract syntax

The abstract syntax for attributes belonging to this class is described in Table 7.

Table 7 – S1 safety cyclic transmission attribute format

Attribute	Format	Size (bits)
Data out	Structure of 2 elements:	192
Safety RY data	Bit-oriented data structure	32
RWw data	Word-oriented data structure	64
Safety RWw data	Word-oriented data	64
Safety TPI-T	Safety transmission packet information	64
Safety RY-r data	Bit-oriented data structure	32
RWw-r data	Word-oriented data structure	64
Safety RWw-r data	Word-oriented data	64
Safety TPI-T-r	Safety transmission packet information	64
Data in	Structure of 2 elements:	192
Safety RX data	Bit-oriented data structure	64
RWr data	Word-oriented data structure	128
Safety RWr data	Word-oriented data	64
Safety TPI-R	Safety transmission packet information	64
Safety RX-r data	Bit-oriented data structure	64
RWr-r data	Word-oriented data structure	128
Safety RWr-r data	Word-oriented data	64
Safety TPI-R-r	Safety transmission packet information	64

11.7.1.3 Transfer syntax

11.7.1.3.1 M1 safety device manager PDU encoding

The specific PDU encoding for attributes belonging to this class is described in Table 8.

Table 8 – M1 safety device manager attribute encoding

Attribute	Encoding		
Management information	Specifies the configuration of the master device		
Link id	0 – 7 = allowable range		
Software/protocol version	**Bit**	**Description**	**Value**
	5 – 0	Software version	1 – 63 = allowable range
	7 – 6	Protocol version	0 = Version 1 1 = Version 2 2 = Version 3 3 = Version 4
Connected slave management information	Specifies the configuration of the connected slaves		
Slave information 1 – 64	Array of 64 elements, each encoded as:		
Software/protocol version	**Bit**	**Description**	**Value**
	5 – 0	Software version	1 – 63 = allowable range
	7 – 6	Protocol version	0 = Version 1 1 = Version 2 2 = Version 3 3 = Version 4

11.7.1.3.2 S1 safety device manager PDU encoding

The specific PDU encoding for attributes belonging to this class is described in Table 9.

Table 9 – S1 safety device manager attribute encoding

Attribute	Encoding		
Management information	Specifies the configuration of the master device		
Link id	0 – 7 = allowable range		
Software/protocol version	**Bit**	**Description**	**Value**
	5 – 0	Software version	1 – 63 = allowable range
	7 – 6	Protocol version	0 = Version 1 1 = Version 2 2 = Version 3 3 = Version 4

11.7.1.3.3 M1 safety connection manager PDU encoding

The specific PDU encoding for attributes belonging to this class is described in Table 10.

Table 10 – M1 safety connection manager attribute encoding

Attribute	Encoding
Parameter information	Specifies the connection configuration
Safety monitor timer value	1 – 65 535 = ms
Safety data monitor timer value	1 – 65 535 = ms
Safety slave specification	Bit 0 – 63 correspond to slot 1 – 64, where: 0 = SCL not supported 1 = SCL supported
Safety slave specification source	Bit 0 – 63 correspond to slot 1 – 64, where: 0 = SCL-user specification not supported 1 = SCL-user specification supported
Safety slave product information 1 – 64	Array of 64 elements, each encoded as:
Safety product information	31 octets of data for safety product information
Safety parameter data	0 – 52 224 octets of data for slave memory access
Safety slave link status	Bit 0 – 63 correspond to slot 1 – 64, where: 0 = Safety slave station not running 1 = Safety slave station running

11.7.1.3.4 S1 safety connection manager PDU encoding

The specific PDU encoding for attributes belonging to this class is described in Table 11.

Table 11 – S1 safety connection manager attribute encoding

Attribute	Encoding
Safety product information	31 octets of data for safety product information
Safety parameter data	0 – 816 octets of data for slave memory access

11.7.1.3.5 M1 safety cyclic transmission PDU encoding

The specific PDU encoding for attributes belonging to this class is described in Table 12.

Table 12 – M1 safety cyclic transmission attribute encoding

Attribute	Encoding			
Data out	Process data registers set by the master for slave device output			
Safety RY data	A position mapped field of bit-oriented output data for all connected slave devices ordered by slot with 32 bits			
RWw data	A position mapped field into which is mapped: word-oriented output data for all connected safety slave devices and the safety transmission packet information for transmission to the safety slave devices			
Safety RWw data	A position mapped field of word-oriented output data for all connected slave devices. Contains 4 words per slot beginning with the second slot. This is because the following field occupies the space allocated for the first slot in a non-safety slave			
Safety TPI-T	**Octet**	**Bit**	**Description**	**Values**
	0 – 1	–	RNO-3	0 – 65 535
	2 – 3	0 – 3	RNO-1	0 – 15
		4 – 6	Link id	0 – 7
		7	reserved	0
		8 – 11	Transmission data type	0 – 15
		12	Busy flag	0 = busy 1 = not busy
		13	reserved	0
		14	Read request	0 = no request 1 = request
		15	SCL-user application mode	0 = test mode 1 = safety mode
	4 – 7	–	CRC32-A	CRC32-A
Safety RY-r data	same as RY			
RWw-r data	same as RWw			
Safety RWw-r data	same as Safety RWw			
Safety TPI-T-r	**Octet**	**Bit**	**Description**	**Values**
	0 – 1	–	Tx/Rx (A-code)	255 / 1 – 64
	2 – 3	0 – 3	RNO-2	0 – 15
		4 – 15	same as Safety TPI-T	
	4 – 7	–	CRC32-B	CRC32-B
Data in	Process data registers read by the master representing slave device inputs			
Safety data in	Process data registers read by the master representing safety slave device inputs			
Safety RX data	A field containing the bit-oriented input data from slave device n ordered by slot with 32 bits			
RWr data	A field containing the word-oriented input data from slave device n ordered by slot with 4 words			

<table>
<tr><th>Attribute</th><th colspan="3">Encoding</th></tr>
<tr><td>Safety RWr data</td><td colspan="3">A position mapped field of word-oriented input data from slave device n. Contains 4 words per slot beginning with the second slot. This is because the following field occupies the space allocated for the first slot in a non-safety slave</td></tr>
<tr><td rowspan="11">Safety TPI-R</td><td>Bit</td><td>Description</td><td>Values</td></tr>
<tr><td>0 – 15</td><td>RNO-3</td><td>0 – 65 535</td></tr>
<tr><td>16 – 19</td><td>RNO-1</td><td>0 – 15</td></tr>
<tr><td>20 – 22</td><td>Link id</td><td>0 – 7</td></tr>
<tr><td>23</td><td>reserved</td><td>0</td></tr>
<tr><td>24 – 27</td><td>Transmission data type</td><td>0 – 15</td></tr>
<tr><td>28</td><td>Busy flag</td><td>0 = busy
1 = not busy</td></tr>
<tr><td>29</td><td>Error notification</td><td>0 = no error
1 = error</td></tr>
<tr><td>30</td><td>reserved</td><td>0</td></tr>
<tr><td>31</td><td>SCL-user application mode</td><td>0 = test mode
1 = safety mode</td></tr>
<tr><td>32 – 63</td><td>CRC32-A</td><td>CRC32-A</td></tr>
<tr><td>Safety RX-r data</td><td colspan="3">same as Safety RX</td></tr>
<tr><td>RWr-r data</td><td colspan="3">same as RWr</td></tr>
<tr><td>Safety RWr-r data</td><td colspan="3">same as Safety RWr</td></tr>
<tr><td rowspan="5">Safety TPI-R-r</td><td>Bit</td><td>Description</td><td>Values</td></tr>
<tr><td>0 – 15</td><td>Tx/Rx (A-code)</td><td>255 / 1 – 64</td></tr>
<tr><td>16 – 19</td><td>RNO-2</td><td>0 – 15</td></tr>
<tr><td>20 – 31</td><td>same as Safety TPI-R</td><td></td></tr>
<tr><td>32 – 63</td><td>CRC32-B</td><td>CRC32-B</td></tr>
<tr><td colspan="4">NOTE The value of RNO is derived by combining the RNO subparts as follows:
RNO-1 = RNO bits 0-3
RNO-2 = RNO bits 4-7
RNO-3 = RNO bits 8-23</td></tr>
</table>

11.7.1.3.6 S1 safety cyclic transmission PDU encoding

The specific PDU encoding for attributes belonging to this class is described in Table 13.

Table 13 – S1 safety cyclic transmission attribute encoding

Attribute	Encoding		
Data out	The process data received from the master		
Safety RY data	A field containing the bit-oriented input data ordered by slot with 32 bits		
RWw data	A position mapped field into which is mapped: word-oriented output data (optionally) and the safety transmission packet information as received from the master		
Safety RWw data	A position mapped field of word-oriented output data for the slave device. Contains 4 words per slot beginning with the second slot. This is because the following field occupies the space allocated for the first slot in a non-safety slave		
Safety TPI-T	**Bit**	**Description**	**Values**
	0 – 15	RNO-3	0 – 65 535
	16 – 19	RNO-1	0 – 15
	20 – 22	Link id	0 – 7
	23	reserved	0
	24 – 27	Transmission data type	0 – 15
	28	Busy flag	0 = busy 1 = not busy
	29	reserved	0
	30	Read request	0 = no request 1 = request
	31	SCL-user application mode	0 = test mode 1 = safety mode
	32 – 63	CRC32-A	CRC32-A
Safety RY-r data	same as Safety RY		
RWw-r data	same as RWw		
Safety RWw-r data	same as Safety RWw		
Safety TPI-T-r	**Bit**	**Description**	**Values**
	0 – 15	Tx/Rx (A-code)	1 – 64 / 255
	16 – 19	RNO-2	0 – 15
	20 – 31	same as Safety TPI-T	
	32 – 63	CRC32-B	CRC32-B
Data in	The process data transmitted to the master		
Safety RX data	A field containing the bit-oriented input data ordered by slot with 32 bits		
RWr data	A field containing the word-oriented input data from the master.		
Safety RWr data	A position mapped field of word-oriented input data for the slave device. Contains 4 words per slot beginning with the second slot. This is because the following field occupies the space allocated for the first slot in a non-safety slave		

Attribute	Encoding		
Safety TPI-R	**Bit**	**Description**	**Values**
	0 – 15	RNO-3	0 – 65 535
	16 – 19	RNO-1	0 – 15
	20 – 22	Link id	0 – 7
	23	reserved	0
	24 – 27	Transmission data type	0 – 15
	28	Busy flag	0 = busy 1 = not busy
	29	Error notification	0 = no error 1 = error
	30	reserved	0
	31	SCL-user application mode	0 = test mode 1 = safety mode
	32 – 63	CRC32-A	CRC32-A
Safety RX-r data	same as Safety RX		
RWr-r data	same as RWr		
Safety RWr-r data	same as Safety RWr		
Safety TPI-R-r	**Bit**	**Description**	**Values**
	0 – 15	Tx/Rx (A-code)	1 – 64 / 255
	16 – 19	RNO-2	0 – 15
	20 – 31	same as Safety TPI-R	
	32 – 63	CRC32-B	CRC32-B
NOTE The value of RNO is derived by combining the RNO subparts as follows: RNO-1 = RNO bits 0-3 RNO-2 = RNO bits 4-7 RNO-3 = RNO bits 8-23			

11.7.2 State description

11.7.2.1 Overview

The SCL state model is extended from IEC 61158 Type 18 with a safe state, shown in Figure 4 as Fail safe state. The safe state is entered upon error conditions and is configured to ensure all outputs are maintained in safe states: digital outputs are low, zero, or off, and analog outputs are held at a safe level previously configured by the SCL user. The M1 safety master device manages the states of each safety slave device individually.

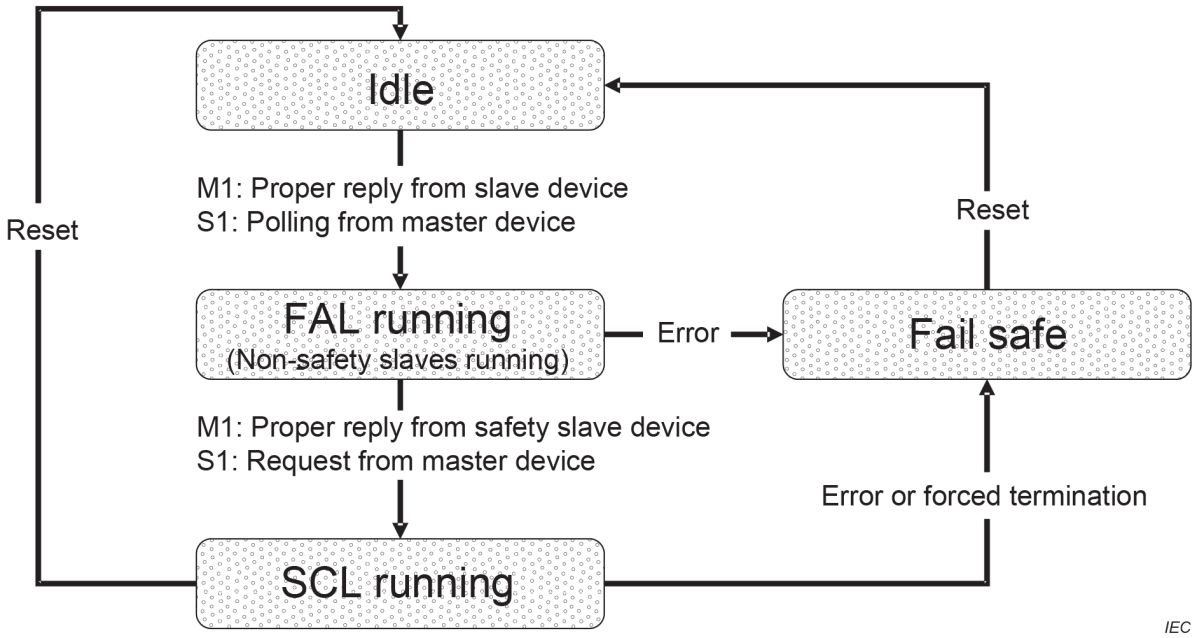


Figure 4 – State diagram

The general method of connection establishment, slave verification, and data refresh is also extended beyond that of IEC 61158 Type 18 and includes safety parameter transmission and processing (see SCL management in 11.8) and safety data transmission and confirmation monitoring.

11.7.2.2 Idle

11.7.2.2.1 Overview

The idle state exists prior to any FAL communications among devices.

11.7.2.2.2 Transition

Upon an appropriate request from the FAL user to the M1 safety master device, receipt of a proper reply from the S1 safety slave device yields a transition from the idle state to the FAL running state.

Upon the receipt of polling communications from the M1 safety master, the S1 safety slave device transitions to the FAL running state.

11.7.2.3 FAL running

11.7.2.3.1 Overview

In the FAL running state, the M1 safety master devices and S1 safety slave devices have established non-safety communications.

11.7.2.3.2 Transition

Upon receipt of request from the M1 safety master, the S1 safety slave transitions to the SCL running state.

Upon receipt of appropriate responses from the S1 safety slave devices, the M1 safety master transitions to the SCL running state.

Any condition of error or fault while in the FAL running state or failed attempt to transition to the SCL running state causes a FSCP 8/1 device to transition to the fail safe state.

11.7.2.4 SCL running

11.7.2.4.1 Overview

The details of the SCL running state are explained in 11.8.

11.7.2.4.2 Transition

As explained in 11.7.2.6, a FSCP 8/1 device transitions to the fail safe state upon detection of an error by any of the following safety measures:

– sequence number;
– time expectation;
– connection authentication;
– feedback message;
– data integrity assurance;
– redundancy with cross checking;
– different data integrity assurance systems.

As explained in 11.7.2.7, a FSCP 8/1 device transitions to the fail safe state upon receipt of a forced termination request.

11.7.2.5 Fail safe

11.7.2.5.1 Overview

The fail safe state is one where all outputs are held in their safe state. For digital outputs, unless otherwise specified, this is the off (or zero or low) state, and for analog outputs, unless otherwise specified, this is the zero output (i.e., no voltage and/or no current) state. Typically, analog outputs will be configured with a safe value that is imposed on the output when in the fail safe state.

11.7.2.5.2 Transition

Exit from the fail safe state is only possible via slave reset.

11.7.2.6 Safety data transmission and processing

11.7.2.6.1 Overview

The SCL of FSCP 8/1 provides the following safety measures:

– sequence number;
– time expectation;
– connection authentication;
– feedback message;
– data integrity assurance;
– redundancy with cross checking;
– different data integrity assurance systems.

The safety master and each safety slave manages and analyzes safety transmissions in order to verify their integrity.

11.7.2.6.2 Sequence number

Safety messages contain a sequence number (RNO) with a width of 24 bits and a specified sequence. The RNO is incremented and transmitted by the safety master. The safety slave echoes the received RNO. If an out of sequence RNO is received, the safety slave is transitioned to the safe state.

11.7.2.6.3 Time expectation

The SCL uses a safety monitor timer and safety data monitor timers to ensure reliable and continuous communications. SLC management configures the timer with a value in the range of 1 ms to 65 535 ms.

The safety monitor timer is used for confirming that safety cyclic communication is being performed normally, and the safety data monitor timers are used for confirming that successive safety cyclic communications are being performed normally. Safety stations monitor the reception interval of the cyclic data that is protected by the normal safety data protection information by this safety monitor timer. Additionally, safety slave stations monitor the reception intervals of the cyclic data that are protected by the normal safety data protection information by the safety data monitor timers.

Table 14, Table 15, and Table 16 describe the operation of the safety monitor timer for both safety master and safety slave devices.

Table 14 – Safety master monitor timer operation

Startup	Termination	Error termination
Sending of safety data (RNO ≠ 0)	Reception of slave response (refresh) data (of the same RNO as send RNO) to which safety data protection information has been properly added	(1) At occurrence of a monitoring timeout (2) At detection of an RNO error

Table 15 – Safety slave monitor timer operation

Startup	Reset	Termination
Reception of safety data (CMD ID=01h)	Reception of master station polling and refresh data (previously RNO+1) to which safety data protection information has been properly added	(1) At occurrence of a monitoring timeout (2) At detection of an RNO error (3) At reception of a forced termination request

Table 16 – Safety data monitor timer operation

Startup	Reset	Termination
Reception of safety cyclic I/O data (CMD ID = 0Fh)	Reception of master station polling and refresh data (previously RNO+2) to which safety data protection information has been properly added	(1) At occurrence of a monitoring timeout (2) At detection of an RNO error (3) At reception of a forced termination request
NOTE Safety slave stations have two safety data monitor timers. A safety data monitor timer starts up upon reception of safety cyclic I/O data (CMS ID=0Fh and RNO=n), and reception of two successive data (RNO=n+2) resets it. The other safety data monitor timer starts up upon reception of safety cyclic I/O data (CMD ID=0Fh and RNO=n+1), and reception of two successive data (RNO=n+3) reset it.		

The behavior of a safety master upon expiration of the safety monitor timer is specified as:

1) Failsafe processing such as the clearing of S-RX delivered to the SCL user to zero.
2) Error notification to SCL user.
3) Transition to the idle state.

The behavior of a safety slave upon expiration of the safety monitor timer is specified as:

1) Failsafe processing such as the termination of output to external devices.
2) Error notification to SCL user.
3) Transition to the safe state.

11.7.2.6.4 Connection authentication

Connection authentication is implemented by a set of a safety connection ID (Link ID) and a station number. Each safety slave uses a 3 bit Link ID which specifies its safety network system. This provides the SRC with up to 8 safety network systems. The assignment of Link ID values shall be unique within a functional safety communication system. The safety messages always contain the Link ID.

Additionally, the transmitted 16-bit logical connection ID is appended to the SPDU for validation. This field, which is comprised of Tx (8-bit source ID) and Rx (8-bit destination ID), is checked for correctness and also included in the data integrity measures.

11.7.2.6.5 Feedback message

A feedback message is provided from each slave that confirms receipt of messages from the master. The feedback message contains error status information from the slave as well as acknowledgment of the RNO, link ID, and command ID.

11.7.2.6.6 Data integrity

The CRC32 for FSCP 8/1 is calculated as described in Annex A. The residual error rate for FSCP 8/1 is calculated in accordance with IEC 61784-3.

11.7.2.6.7 Redundancy with cross checking

The redundant data fields are compared bit-for-bit to their counterparts.

11.7.2.6.8 Different data integrity assurance system

The distinction between safety relevant and non-safety relevant messages is ensured by validating the uniqueness of safety messages to contain a properly formatted CRC checksum (32 bits), an 8-bit command ID, a 3-bit link ID and a 24-bit RNO.

The IEC 61158 Type 18 protocol uses a different CRC algorithm (16-bit CRC) and no inclusion of command ID, link ID or RNO.

11.7.2.7 Forced termination

Forced termination processing is used when the safety master requests a safety slave to terminate communication. The safety slave that receives the forced termination request transitions to the fail safe state (stopping external output) and then immediately terminates communication.

11.8 Safety communication layer management for FSCP 8/1

11.8.1 General

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

– establish connection;
– verify slave configuration;
– safety slave parameter transmission.

11.8.2 Connection establishment and confirmation processing

Upon connection establishment, initial configuration is confirmed by validating that the SAREPs reside in safety devices and that safety cyclic transmission is supported. This process is described in Table 17.

Table 17 – Details of connection establishment and confirmation processing

SAREP type	Details of processing
Safety master	(1) Confirm that the slave is a safety slave device. (This is confirmed by communicating the safety cyclic data.) (2) Confirm that the safety slave has received the establish connection command. (This is confirmed by checking that the CMD of the response data are identical with the send data.) (3) Transmit the safety monitor timer value.
Safety slave	(1) Confirm that the master is a safety master device. (This is confirmed by communicating the safety cyclic data.) (2) Receive the safety monitor timer value and registers the value internally.

The safety master station transmits RNO = 0 when sending the establish connection command.

11.8.3 Safety slave verification

11.8.3.1 General

Product information verification processing confirms that the connected safety slave stations match the safety slave stations currently set to the network parameters of the safety master station to detect misconnections and misconfiguration. A replacement slave device that is not a safety slave, is detected and disabled at start-up.

11.8.3.2 Safety slave information verification process

The safety slave information verification process is described in Table 18.

Table 18 – Details of slave information verification processing

SAREP type	Details of processing
Safety master	(1) Read the product information from safety slaves, and verify that information against product information set to network parameters. (2) After verification, send the product information to safety slave stations.
Safety slave	(1) Verify the product information of the slave against the product information received from the safety master.

Slave information verification processing verifies safety slave product information.

11.8.3.3 Safety slave parameter transmission

Safety slave configuration parameters are transmitted from the safety master to each safety slave. This process is described in Table 19.

Table 19 – Details of safety slave parameter transmission processing

SAREP type	Details of processing
Safety master	(1) Read the CRC32 of the ROM storage parameters from the safety slave stations, and verify this CRC32 with the CRC32 of the ROM storage parameters registered from the SCL user. (2) Send the safety slave parameters to the safety slave.
Safety slave	(1) Receive the safety slave parameters from the safety master, confirm the setting values, and perform internal registration processing.

11.9 System requirements for FSCP 8/1

11.9.1 Indicators and switches

11.9.1.1 Switches

Each safety device shall provide physical means for setting the following:

- Online – Set this mode to establish a data link.
- Station number – 0: Safety master, 1 to 64: Safety slave – required for safety slave only.
- Link ID – 0 to 7
- Baud rate – 156 kbit/s, 625 kbit/s, 2,5 Mbit/s, 5 Mbit/s, 10 Mbit/s – required for safety master only.
- Reset – required for safety slave only

and optionally provides physical means for setting the following:

- Number of occupied slots – Station slots (1 or 2) occupied by one safety slave station.
- Line test 1 – Verifies that the master is able to connect to all slave stations.
- Line test 2 – Verifies that the master is able to connect to a specific slave station.
- Parameter check test – Verifies the parameter content.
- Hardware test – Verifies each individual module for normal operation.

11.9.1.2 Indicators

Indicator requirements are specified in Table 20 with the following interpretation:

M = mandatory

O = optional

Indicator type, color and shape are not specified. Also, where computers or other devices with screens are used, indication may be supported via indication on the screen.

Table 20 – Monitor LEDs

No.	LED Name	Description	Safety master station	Safety remote device station	Safety remote I/O station
1	RUN	Lit: Module normal Out: Watchdog timer error	M	O	O
2	ERR	Lit: Communication with all stations error This LED lights when one of the following occurs: ・Switch setting error ・Master station duplicated on same line ・Parameter content error ・Data link monitor timer activated ・Cable wire break Or cable influenced by noise on the transmission path Flashing: Communication error	M	O	O
3	L RUN	Lit: Data link execution in progress	M	O	O
4	L ERR.	Lit: Communication error (self station) Flashing: Switch type setting was changed with power ON	M	O	O

11.9.2 Installation guidelines

This document specifies protocol and services for a safety communication system based on IEC 61158 Type 18. Usage of safety devices with the safety protocol specified in this document requires proper installation.

Additional installation information is also given in [30] and [31] in the Bibliography.

11.9.3 Safety function response time

11.9.3.1 General

As mentioned in 11.5.3, an integrated watchdog timer is used which provides the time expectation of each output channel on each safety output slave. It ensures a safety function response time.

If the safety function response 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.

11.9.3.2 Time calculation

An integrated watchdog timer providing the time expectation of each output channel on each safety output slave ensures a safety function response 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.

The safety function response 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 SRC.

The safety function response time is calculated as the sum of (a) through (f) from Table 21 with the terms as defined in Table 22.

NOTE 1 The safety master calculates the timeout based on: the safety refresh monitoring time – ((WDT × n) × 2).

NOTE 2 (WDT × n) × 2 is the time required for the safety master to send communication data.

Table 21 – Safety function response time calculation

Item	Maximum
(a) Input device response time	DT1
(b) Safety slave input processing time	Time of noise removal filter + Processing time of remote input station
(c) Monitoring time from safety input to safety output	Safety data monitor time
(d) Safety slave output processing time	Processing time of remote output station
(e) Output device response time	DT2
Total	(a)+(b)+(c)+(d)+(e)

Table 22 – Safety function response time definition of terms

Item	Definition
LS	Link Scan Time as specified by the manufacturer
n	Value after the decimal point of LS/WDT (rounded up)
SRRP	Safety refresh response processing time. As specified by the manufacturer
m	Value after the decimal point of SRRP/(WDT × n) (rounded up)
Time of noise removal filter	Configured in safety remote station settings (Setting value: 1 ms to 50 ms)
DT1, DT2	Response time of sensor or output destination controlling device. As specified by the manufacturer.
Safety data monitor time	Time set in network parameter. Use the value derived from the following formula as the measure: Safety refresh monitor time × 2 – ((WDT × n) × m) – 10 [ms]
Safety refresh monitor time	Time set in network parameter. Use the value gained by the following calculation formula as the measure. In triggered mode: (WDT × n) × 3 + (WDT × n) × m × 2 + (WDT × α) [ms] In free-running mode: (WDT × n) × 3 + LS + (WDT × n) × m × 2 + (WDT × α) [ms] where: α = 0, for LS ≤ 1,5 ms α = 1, for LS > 1,5 ms
WDT (Watchdog timer)	Time set in configuration parameter.
Triggered mode	Mode which performs data link when sequence scan is synchronized with link scan. In the triggered mode, sequence scan and link scan start simultaneously
Free-running mode	Mode which performs data link without synchronizing sequence program

11.9.4 Duration of demands

The duration of demand by the safety-related application to the safety communication layer shall be sufficient in duration such that demand is detected within the longest safety function response time by the application.

11.9.5 Constraints for calculation of system characteristics

An FSCP 8/1 safety system shall comply with the following constraints:

- IEC 61158 Type 18: No restrictions
- Maximum number of safety slots: 64
- Minimum scan cycle time: 10 ms
- Maximum number of safety relevant I/O bits per safety PDU – slave to master: 208
- Maximum number of safety relevant I/O bits per safety PDU – master to slave: 7 168

11.9.6 Maintenance

There are no SCL specific requirements for maintenance.

Specifications for system behavior in case of device repair and replacement are outside the scope of this document. 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.

For information on programming the SRP and setting the parameters of safety devices, it is strongly recommended to contact the device or system supplier. Also, it is recommended to take into account the documents [30] and [31]. In these documents additional information, e.g. checklists, is given for the user of a CC-LINK-Safety system.

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

11.9.7 Safety manual

The supplier of safety slaves that incorporate the SCL according to the SCL specifications given in this document shall prepare an appropriate safety manual according to IEC 61508. This safety manual shall also include the installation requirements as specified in 11.9.2 as well as guidelines for the configuration of device switches. In addition to switches common with IEC 61158 Type 18, these guidelines shall include the statement that all safety devices on the same network shall be configured with the same Link ID. See 11.9.1.1.

According to the safety communication system based on IEC 61158 Type 18, it is strongly recommended to take into account the specifications [30], [31] and [32].

NOTE Before starting the implementation of a safety device it is good engineering practice to contact the CLPA to determine if there are amendments to implementation guidelines and/or implementation requirements.

11.10 Assessment for FSCP 8/1

It is the manufacturer's responsibility to develop the device 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). Additional information is provided in Annex B.

12 FSCP 8/2

12.1 Scope – FSCP 8/2

See Clause 1.

12.2 Normative references – FSCP 8/2

See Clause 2.

12.3 Terms, definitions, symbols, abbreviated terms and conventions – FSCP 8/2

See Clause 3.

12.4 Overview of FSCP 8/2 (CC-Link IE™ Safety communication function)

Communication Profile 8/4 and 8/5 (commonly known as CC-Link IE™ [4]) defines communication profiles based on ISO/IEC/IEEE 8802-3, IEC 61158-5-23, and IEC 61158-6-23.

The basic profiles CP 8/4, and CP 8/5 are defined in IEC 61784-2. The CPF 8 functional safety communication profile FSCP 8/2 (CC-Link IE™ Safety communication function[3]) is based on the CP 8/4 and CP 8/5 basic profiles in IEC 61784-2 and the safety communication layer specifications defined in this document.

FSCP 8/2 is a protocol for communicating safety-relevant data such as emergency stop signals among participants within a distributed network using fieldbus technology in accordance with the requirements of IEC 61508 for functional safety. This protocol is used in various applications such as process control, manufacturing automation and machinery.

The FSCP 8/2 protocol is designed to support Safety Integrity Level SIL3 (IEC 61508) using CP 8/4 and CP 8/5 by additionally specifying mechanisms for the implementation of time stamp, time expectation, connection authentication, feedback message, data integrity assurance and different data integrity assurance safety measures.

SCL capabilities for FSCP 8/2 are provided with the introduction of safety application service elements (SASE). These SASEs are used in place of their corresponding ASEs as specified in this document. However, since inheriting directly from the parent classes defined for CP 8/4 and CP 8/5, these SASEs specify required additions to CP 8/4 and CP 8/5 for functional safety using a black channel approach.

The master and slave construct yields two SASEs, the SASE-M and SASE-S respectively. Each are managed by an safety FAL service protocol machine, the SFSPM-M and the SFSPM-S respectively.

12.5 General – FSCP 8/2

12.5.1 External documents providing specifications for the profile

Manufacturers of FSCP 8/2 safety devices are encouraged to review CC-Link Safety Specifications which provide additional specifications relevant for implementation of the SCL defined in this document.

NOTE Documents [30] and [31] contain important information related to FSCP 8/2.

---

[4] CC-Link IE™ is a trade name of the non-profit organization CC-Link Partner Association. This information is given for the convenience of users of this document and does not constitute an endorsement by IEC of the trade name holder or any of its products. Compliance to this document does not require use of the trade name CC-Link IE™. Use of the trade name CC-Link IE™ requires permission of CC-Link Partner Association and compliance with conditions for their use (such as testing and validation).

12.5.2 Safety functional requirements

This document specifies the services and protocols for a functional safety communication system based on IEC 61158 Type 23. The communication technologies specified in this document shall only be implemented in devices designed in accordance with the requirements of IEC 61508.

The following requirements shall apply to the development of devices that implement FSCP 8/2 protocols. The same requirements were used in the development of FSCP 8/2.

– The FSCP 8/2 protocols are designed to support Safety Integrity Level SIL3 (refer to IEC 61508).
– Implementations of FSCP 8/2 shall comply with IEC 61508.
– The basic requirements for the development of the FSCP 8/2 protocol are in IEC 61784-3.
– The safety state for discrete data is the de-energized state (0). For analog values the de-energized state shall be defined by the safety-related application.
– Environmental conditions shall be according to IEC 61131-2 for the basic levels and IEC 61326-3-1, IEC 61326-3-2 for the safety margin tests, unless there are specific product standards.
– Unless specified in this document, the CPF 8 requirements shall be unchanged for safety.

12.5.3 Safety measures

12.5.3.1 General

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

- time stamp;
- time expectation;
- connection authentication;
- feedback message;
- data integrity assurance;
- redundancy with cross-checking;
- different data integrity assurance systems.

The selection of the various measures for possible errors is shown in Table 23.

Table 23 – 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	X [c]	
Unintended repetition		X						
Incorrect sequence		X						
Loss		X [a,c]			X [b]			
Unacceptable delay		X [c]	X					
Insertion				X				
Masquerade							X [c]	X
Addressing				X				

[a] Assessed by received time stamp.

[b] Used in request/response model.

[c] Not used in request/response model.

12.5.3.2 Corruption

Corruption is detected using the CRCs included in the safety PDU. The transmitting node sends the safety PDU including its calculated CRCs. The receiving node compares the CRCs included in the received safety PDU with the CRCs calculated from the received safety PDU, and determines if corruption occurred. Additionally, the receiving node cross checks the redundant portions of the received safety PDU to verify that these portions match each other bit-for-bit. If the comparison of CRCs or cross check result indicates not a match, the receiving node deems that corruption has occurred and shall discard the received safety PDU. When the received safety PDU is discarded, the timer delay_detection_timer used for unacceptable delays shall not be reset.

12.5.3.3 Unintended repetition

Unintended repetition is the repeated receipt of a safety PDU that is not the latest safety PDU at appropriate timing, due to an error, fault, or interference. The identity of the safety PDU is detected using the T-code (TS combined with CC to form a single timeliness code) included in the safety PDU. The transmitting node sends safety PDUs that includes a T-code.

The receiving node receives the safety PDU and holds the T-code of the received safety PDU in order to detect unintended repetition of the safety PDU at the time of the next reception. Upon receipt of the safety PDU, the receiving node compares the T-code included in the safety PDU with the held T-code of the safety PDU previously received. If the T-code of the received safety PDU is the same as the T-code of the previously received PDU, the receiving node deems that unintended repetition has occurred, and shall discard the received safety PDU. When a safety PDU having the same T-code value is received, the timer delay_detection_timer used to detect unacceptable delays shall not be reset.

Figure 5 shows the sequence in a case where safety PDUs are sent from SASE-M to SASE-S, and unintended repetition is detected in SASE-S. Similarly, when a safety PDU is sent from SASE-S to SASE-M, unintended repetition is detected by SASE-M on the receiving node.

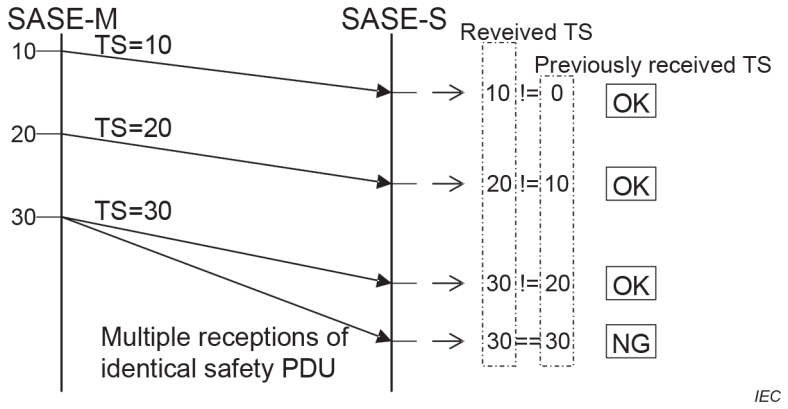


Figure 5 – Detection of unintended repetition

12.5.3.4 Incorrect sequence

Incorrect sequence is the receiving node's receipt of safety PDUs in an order that differs from the order in which the safety PDUs were sent from the transmitting node. TS and CC are combined to form a single T-code. The order is detected using the T-code included in the safety PDUs. The transmitting node sends safety PDUs that include a T-code.

The receiving node receives a safety PDU and holds the T-code of the received safety PDU. Upon receipt of the next safety PDU, the receiving node compares the T-code included in the safety PDU with the held T-code of the safety PDU previously received. If the T-code of the received PDU is less than the T-code of the previously received PDU, the receiving node deems that the order is incorrect, and shall terminate the safety connection.

Figure 6 shows the sequence in a case where safety PDUs are sent from SASE-M to SASE-S, and incorrect order is detected in SASE-S. Similarly, when a safety PDU is sent from SASE-S to SASE-M, incorrect order is detected by SASE-M on the receiving node.

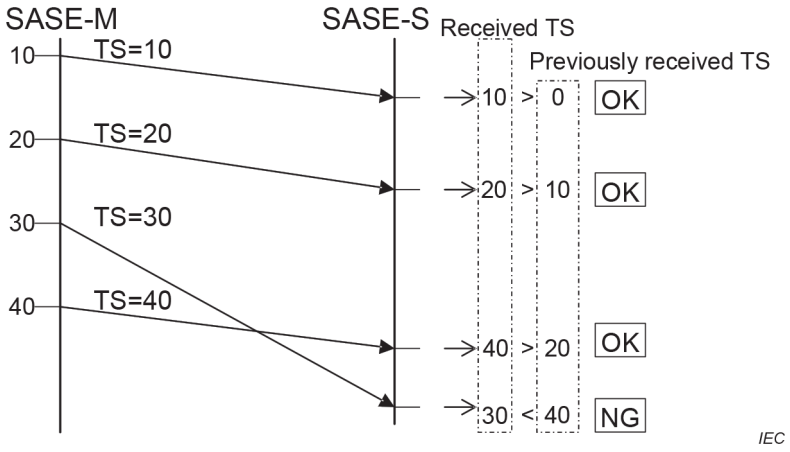


Figure 6 – Detection of incorrect sequence

12.5.3.5 Loss

Loss is detected using T-code.

SASE-M periodically sends safety PDUs to SASE-S based on the SASE-M transmission interval (transmission_interval). The T-code included in the safety PDU sent by SASE-M is the value of the safety clock during safety PDU transmission. SASE-S periodically sends safety PDUs to SASE-M based on the SASE-S transmission interval (transmission_interval). The T-code included in the safety PDU sent by SASE-S is a value calculated based on the safety clock value during safety PDU transmission and the offset ts_offset with SASE-M.

The receiving node receives a safety PDU, verifies that the T-code of the received safety PDU is not larger than the sum of the transmission_interval of the transmitting node added to the T-code of the safety PDU previously received, and deems that loss has occurred if the value is larger. If loss is detected, the receiving node shall terminate the safety connection.

Figure 7 shows the sequence in a case where safety PDUs are sent from SASE-M to SASE-S and loss is detected in SASE-S. Similarly, when a safety PDU is sent from SASE-S to SASE-M, loss is detected in SASE-M on the receiving node.

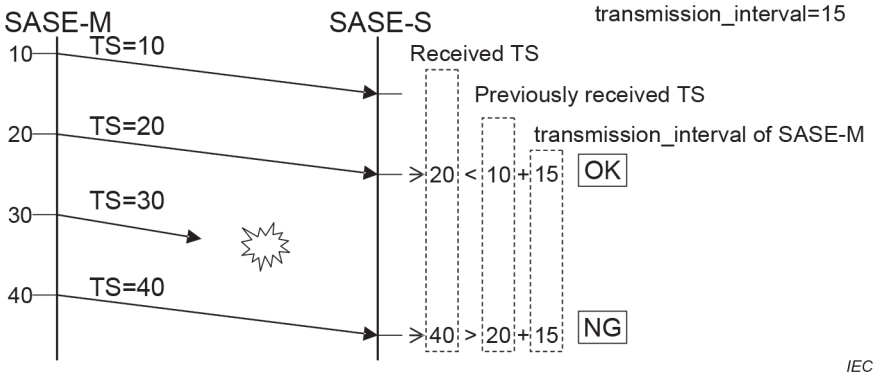


Figure 7 – Detection of loss

12.5.3.6 Unacceptable delay

An unacceptable delay is detected using timers and T-code.

SASE-M periodically sends safety PDUs to SASE-S based on the SASE-M transmission interval (transmission_interval). The T-code included in the safety PDU sent by SASE-M is the value of the safety clock during safety PDU transmission. SASE-S periodically sends safety PDUs to SASE-M based on the SASE-S transmission interval (transmission_interval). The T-code included in the safety PDU sent by SASE-S is the sum of the safety clock value during safety PDU transmission and the offset ts_offset with SASE-M.

SASE-S on the receiving node receives a safety PDU from SASE-M, records the safety clock value at the time of safety PDU reception, and starts or resets the timer delay_detection_timer. SASE-S calculates the difference between the sum of the recorded safety clock value and the offset ts_offset and the received T-code, and calculates the delay value from SASE-M to SASE-S. If the calculated value does not satisfy the following condition that takes into consideration offset dispersion (offset_dispersion), the receiving node deems that an unacceptable delay has occurred.

offset_dispersion < Calculated value < allowable_delay + offset_dispersion

If a valid safety PDU is not received before the timer delay_detection_timer expires, which occurs at the allowable_refresh_interval, the receiving node deems that an unacceptable delay has occurred. If this happens, SASE-S shall terminate the safety connection.

SASE-M on the receiving node receives a safety PDU from SASE-S, records the safety clock value at the time of safety PDU reception, and starts or resets the timer delay_detection_timer. SASE-M calculates the difference between the recorded safety clock value and the received T-code, and calculates the delay value from SASE-S to SASE-M. If the calculated value does not satisfy the above-described SASE-S assessment formula, the receiving node deems that an unacceptable delay has occurred. In addition, if a valid safety PDU cannot be received before delay_detection_timer expires, the receiving node deems that an unacceptable delay has occurred. When this happens, SASE-M shall terminate the safety connection.

Figure 8 shows the sequence in a case where safety PDUs are sent from SASE-M to SASE-S and an unacceptable delay is detected by time stamps in SASE-S. Figure 9 shows a case where an unacceptable delay is detected by a timer in SASE-S. Similarly, when a safety PDU is sent from SASE-S to SASE-M, an unacceptable delay is detected in SASE-M on the receiving node.

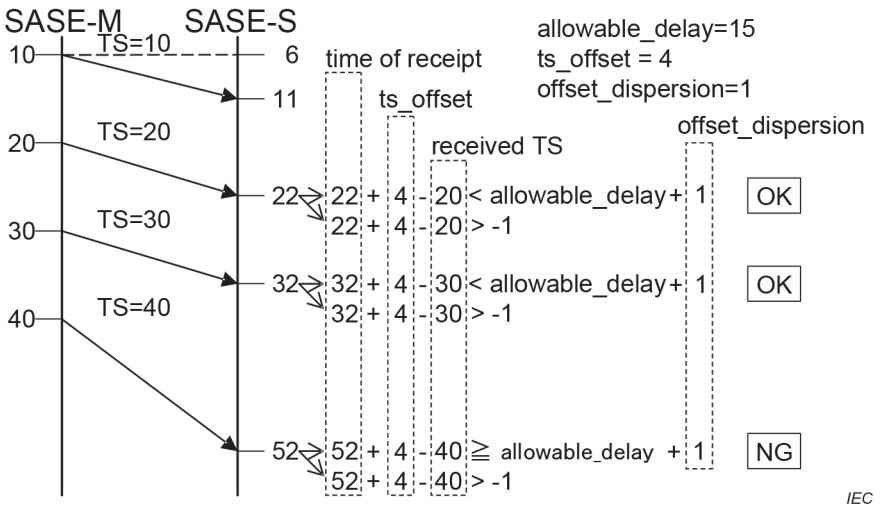


Figure 8 – Detection of unacceptable delay by time stamps

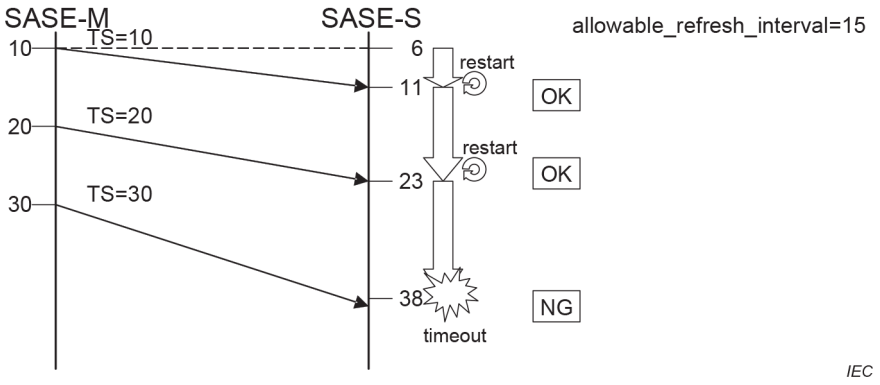


Figure 9 – Detection of unacceptable delay by timer

12.5.3.7 Insertion

Insertion is the insertion of a message from an unexpected or unknown transmission source. Insertion is detected using the safety connection identifier connection_id (CID) included in the safety PDU. The transmitting node sends a safety PDU that stores the connection_id in CID.

The receiving node compares the CID included in the safety PDU with the connection_id agreed upon at the time of connection establishment, and determines if the two match. If the two do not match, the receiving node shall discard the received safety PDU. If the received safety PDU is discarded, the timer delay_detection_timer used to detect unacceptable delays shall not be reset.

12.5.3.8 Masquerade

Masquerade is the reception of a non-safety message by a safety station and insertion of the message from what appears to be a valid transmission source as a result of a fault or interference. Masquerade is detected using CRCs generated by a generator polynomial that differs from that for non-safety communication in addition to the validation of SCL protocol specific data constraints within the received PDU.

The transmitting node sends a safety PDU that includes its calculated CRCs. The receiving node compares the CRCs included in the safety PDU with the CRCs calculated from the received safety PDU. Additionally, the receiving node cross checks the redundant portions of the received safety PDU to verify that these portions match each other bit-for-bit. If the two do not match, or if other expected data are outside the constraints of a properly defined safety PDU, the receiving node shall discard the received safety PDU. If the received safety PDU is discarded, the timer delay_detection_timer used to detect unacceptable delays shall not be reset.

12.5.3.9 Addressing

Addressing, or authentication, is the transmission of a safety message to the wrong safety station and treatment of the message as a correct message due to a fault or interference. Addressing is detected using the safety connection identifier connect_id included in the safety PDU.

The transmitting node sends a safety PDU that stores the connection_id in CID. The receiving node compares the CID included in the safety PDU with the connection_id agreed upon at the time of connection establishment, and determines if the two match. If the two do not match, the receiving node shall discard the received safety PDU. If the received safety PDU is discarded, the timer delay_detection_timer used to detect unacceptable delays shall not be reset.

12.5.4 Safety communication layer structure

The protocol hierarchy of the safety station is comprised of the protocol hierarchy of CP 8/4 and CP 8/5 (ISO/IEC/IEEE 8802-3 and FAL Type 23) which serves as the foundation, the safety communication layer FSCP 8/2 which implements safety communication, and safety related applications. This hierarchy is shown (for CP 8/5) in Figure 10.

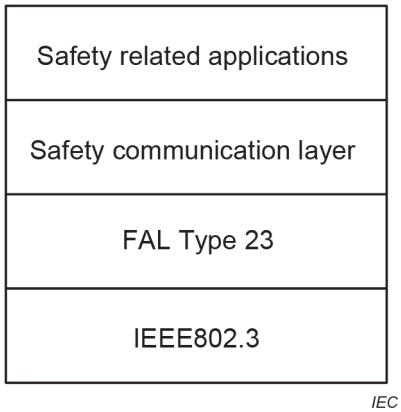


Figure 10 – Protocol Hierarchy

12.5.5 Relationships with FAL (and DLL, PhL)

12.5.5.1 General

There are no FAL requirements other than those stated in this document.

FSCP 8/2 uses the services of the CP 8/4, CP 8/5 FAL. Safety data delivery uses the transient transmission service. The CP 8/4 uses the "Read memory" and "Write memory" services, and the CP 8/5 uses the "AC Send ND" service. Both are described in FAL Type 23.

12.5.5.2 Data types

Data types of safety data are specified in IEC 61158-5-23.

12.6 Safety communication layer services for FSCP 8/2

12.6.1 General

The FSCP 8/2 is structured around two state machines, the SFSPM-M in the safety master, and the SFSPM-S in the safety slave, with state transitions effected via services as described in 12.6. Safety-related applications use safety application services to communicate via the safety communication layer.

12.6.2 Connection reestablishment services

12.6.2.1 SS-Start

SS-Start is a service used for requesting the start of safety communication. Table 24 shows the SS-Start parameters.

Table 24 – SS-Start

Parameter Name	Req	Ind	Rsp	Cnf
Argument	M	M(=)		
ConnectionID	M	M(=)		

ConnectionID
Specifies the ID of the safety connection that is to start safety communication. The size is 32 bits.

12.6.2.2 SS-Restart

SS-Restart is a service used for requesting the restart of safety communication. Table 25 shows the SS-Restart parameters.

Table 25 – SS-Restart

Parameter Name	Req	Ind	Rsp	Cnf
Argument	M	M(=)		
ConnectionID	M	M(=)		

ConnectionID
Specifies the ID of the safety connection that is to restart safety communication. The size is 32 bits.

12.6.2.3 SS-InvokeFunc

SS-InvokeFunc is a service used for requesting the execution of a safety application command. Table 26 shows the SS-InvokeFunc parameters.

Table 26 – SS-InvokeFunc

Parameter Name	Req	Ind	Rsp	Cnf
Argument	M	M(=)		
ConnectionID	M	M(=)		
Command	M	M(=)		
Data	C	C(=)		
Result			C	C(=)
R Data			C	C(=)

ConnectionID
Specifies the ID of the target safety connection. The size is 32 bits.

Command
Specifies the command to be executed.

Data
Specifies the information related to the command to be executed.

R Data
Contains the information returned from the executed service.

12.6.3 Data transmission services

12.6.3.1 SS-Read

This service is used to read safety data of a specified size from safety cyclic memory. Table 27 shows the parameters of this service.

Table 27 – SS-Read

Parameter Name	Req	Ind	Rsp	Cnf
Argument	M	M(=)		
Address	M	M(=)		
Size	M	M(=)		
Result			M	M(=)
R Data			M	M(=)

Address
Specifies the target memory head address.

Size
Specifies the target memory size (bit units).

Data
Contains the contents of the read memory.

12.6.3.2 SS-Write

This service is used to write safety data of a specified size to safety cyclic memory. Table 28 shows the parameters of this service.

Table 28 – SS-Write

Parameter Name	Req	Ind	Rsp	Cnf
Argument	M	M(=)		
Address	M	M(=)		
Size	M	M(=)		
Data	M	M(=)		

Address
Specifies the target memory head address.

Size
Specifies the target memory size (bit units).

Data
Specifies the safety data to be written to the target memory.

12.6.4 Connection termination notification services

12.6.4.1 SS-Terminate

This service is used to issue a notification of termination of the safety connection. Table 29 shows the parameters of this service.

Table 29 – SS-Terminate

Parameter Name	Req	Ind	Rsp	Cnf
Argument		M		
CID		M		

CID
Specifies the CID of the terminated safety connection.

12.7 Safety communication layer protocol for FSCP 8/2

12.7.1 Safety PDU format

12.7.1.1 Safety PDU structure

Figure 11 shows the structure of the safety PDU used by the FSCP 8/2 safety communication function. S-Data indicates the safety data area and stores safety input data or safety output data. The maximum size of S-Data is 800 bits.

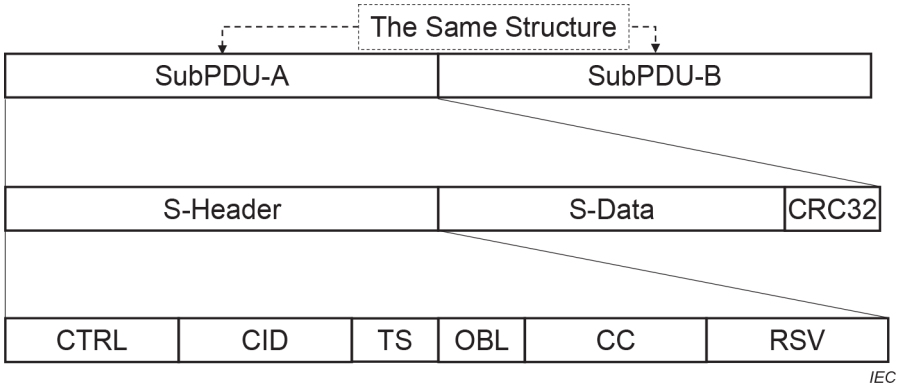


Figure 11 – Safety PDU Structure

Table 30 shows the names, sizes, and contents of the elements that make up the safety PDU. Only one instance of a SubPDU is shown, although the SubPDU is repeated twice, shown as SubPDU-A and SubPDU-B respectively.

Table 30 – Safety PDU elements

Attribute	Description	Size (bits)
S-Header	Structure of 6 elements:	160
CTRL	Command type, status	32
CID	Safety connection identifier	32
TS	Time stamp	16
OBL	Offset generation information	16
CC	Upper 32 bits of safety clock	32
RSV	Reserved for future use	32
S-Data	Safety data (size is in units of 4 octets)	32 min 800 max
CRC32	Cyclic Redundancy Check	32

12.7.1.2 CTRL

Figure 12 shows the configuration of CTRL. Table 31 describes the contents of the elements that make up CTRL.

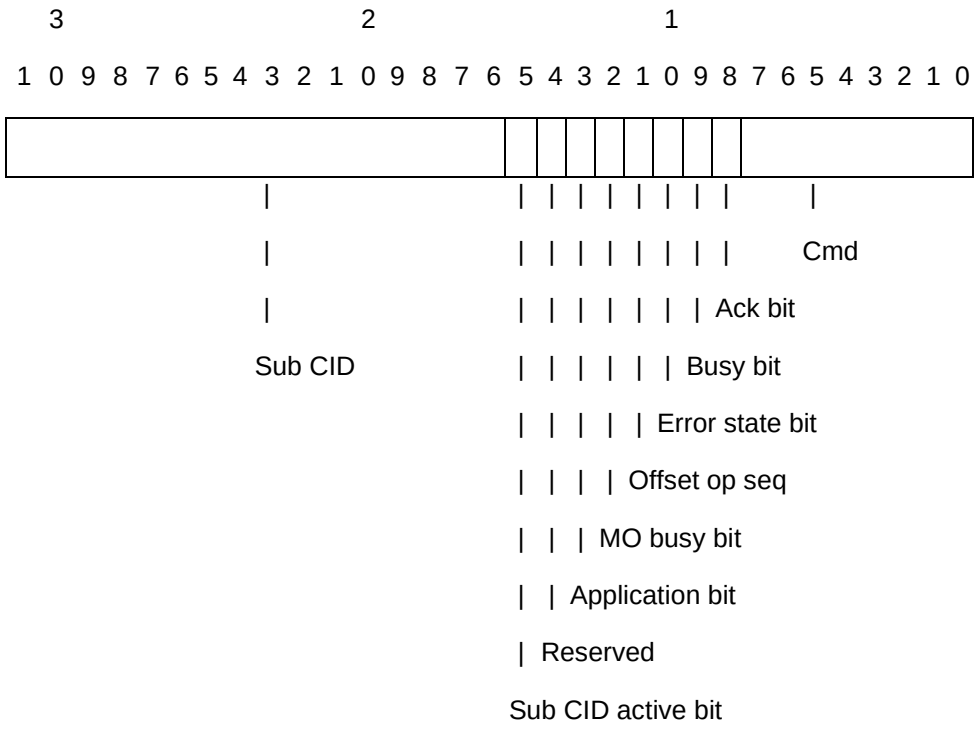


Figure 12 – CTRL Configuration

Table 31 – CTRL Elements

Item		Value	Description
Cmd	S-Connect	0x00	Establish safety connection
	S-InitConfirmNetPrm	0x01	Confirm safety network parameters
	S-InitVerifyStnPrm	0x02	Verify safety station parameters
	S-InvokeFunc	0x03	Safety application command
	Reserved	0x04 – 0xF8	For future expansion
	S-Disconnect	0xF9	Termination of safety connection
	S-ReadErrorInfo	0xFA	Read error information
	S-WriteErrorInfo	0xFB	Issue error notification
	S-RefreshReady	0xFC	Issue safety refresh ready notification and measure offset
	S-RefreshMO	0xFD	Safety refresh; measure offset
	S-RefreshGO	0xFE	Safety refresh; generate offset
	S-Refresh	0xFF	Safety refresh
Ack bit		0x00	Request
		0x01	Response
Busy bit		0x00	Processing complete
		0x01	Processing not complete
Error state bit		0x00	No error
		0x01	Error
Offset op seq		0x00, 0x01	Offset measurement/generation sequence number
MO busy bit		0x00	Processing complete
		0x01	Processing not complete
Application bit		0x00, 0x01	Application bit

Item	Value	Description
Reserved	—	For future expansion
Sub CID active bit	0x00	Sub CID inactive
	0x01	Sub CID in use
Sub CID	0x0000 – 0xFFFF	Safety connection sub identification

Cmd
Indicates the safety PDU type.

Ack bit
Indicates whether Cmd is a request or a response. 0 indicates request and 1 indicates response.

Busy bit
Indicates whether or not the processing on the Cmd by the transmitting node has been completed at a time other than safety refresh. 0 indicates that the request process is completed, and 1 indicates that the request process is not complete. The Busy bit shall be 0 during safety refresh.

When Cmd is sent with the Busy bit set to 1, SASE-M shall send the same Cmd with the Busy bit set to 0 after the processing that caused the Busy bit is completed. Upon receipt of a safety PDU with the Busy bit set to 1, SASE-M discards the received safety PDU, restarts roundtrip_time, and then resends the same Cmd. Upon receipt of a safety PDU with the Busy bit set to 1, SASE-S discards the received safety PDU, restarts roundtrip_timer, and sends a response with the Busy bit set to 0.

Error state bit
Indicates the error state. 0 indicates no error, and 1 indicates error. The Error state bit is 1 from the moment an error occurs to the moment it is cleared.

Offset op seq
Used to associate requests sent by SASE-M with responses sent by SASE-S at the time of offset measurement and offset generation. Offset op seq is used when Cmd is:

S-RefreshReady,

S-RefreshMO, or

S-RefreshGO.

Its initial value is 0. SASE-M alternately specifies 0 and 1 at each offset measurement. With offset generation implemented following offset measurement, the value used with offset measurement is used as Offset op seq. SASE-S uses the Offset op seq value received in a request from SASE-M as the response Offset op seq.

NOTE 1 During offset measurement and offset generation which follows offset measurement, offset measurement and offset generation are associated by using the same value as Offset op seq.

MO Busy bit
Indicates whether or not the transmitting node processing is completed for offset measurement during safety refresh. 0 indicates that the processing is completed, and 1 indicates that it is not. When a safety PDU with the MO Busy bit set to 1 is received, restart shall be performed if roundtrip_timer has been started. When a safety PDU with the MO busy bit set to 1 is transmitted, the transmitting node does not start roundtrip_timer.

NOTE 2 The MO Busy bit is used for restarting the roundtrip_timer only. It does not extend the interval of clock offset interpolation.

Application bit
Used to indicate device-specific application identity.

Sub CID active bit
Indicates the validity of the Sub CID. 0 indicates the Sub CID is inactive and therefore an invalid field. 1 indicates the Sub CID is in use and therefore valid.

Sub CID
Indicates the identity of a sub-connection within a given CID. Only used if the Sub CID active bit is set to 1.

12.7.1.3 CID

CID is a safety connection identifier that indicates the relationship between a transmission source and a transmission destination. CID is generated so as to include the SASE-M address and SASE-S address.

There is a maximum of two connections per set of safety stations. Given n1 as the network number of station A, n2 as the station number, n3 as the network number of station B, and n4 as the station number, the CIDs are as follows:

CID

$CID_1 = ((n1 \times 256 + n2) \times 65536) + (n3 \times 256 + n4)$

$CID_2 = ((n3 \times 256 + n4) \times 65536) + (n1 \times 256 + n2)$

where

CID_1 is the CID for safety connection 1

CID_2 is the CID for safety connection 2

12.7.1.4 TS and CC

TS is a time stamp that indicates the lower 16 bits of a 48-bit safety clock. Its unit is 128 microseconds. TS uses the safety clock of SASE-M as its standard.

NOTE The time period handled by the 48-bit safety clock (unit: 128 microseconds) is approximately 1140 years.

When SASE-M executes a Cmd request, the value of the lower 16 bits of the safety clock during the Cmd request shall be stored in TS.

When SASE-S executes a Cmd request, the value calculated by the formula below shall be stored in TS. sending_time is the lower 16-bit value of the SASE-S safety clock, and ts_offset is the offset of the SASE-M safety clock.

Time stamp

$TS = (sending\_time + ts\_offset) \bmod 2^{16}$

Figure 13 indicates the relationship between the SASE-M and SASE-S safety clocks and the TS during a Cmd request.

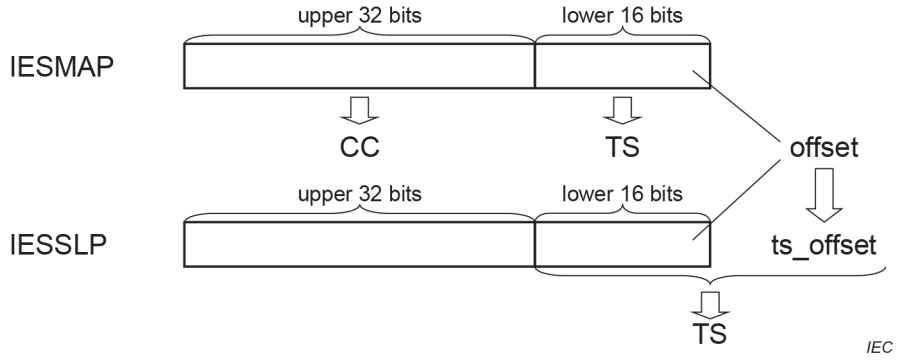


Figure 13 – SASE-M and SASE-S TS

When a response is sent to the Cmd request, TS shall be the same value as the TS used by the Cmd requesting node.

CC is the upper 32 bits of the 48-bit safety clock. TS and CC combine to form a single T-code.

12.7.1.5 OBL

OBL is information used to generate the offset ts_offset of the safety clock. OBL is used in the request S-RefreshGO-req sent by SASE-M and in the response S-RefreshGO-rsp sent by SASE-S.

The information stored in OBL of S-RefreshGO-req is offset_baseline described in 12.7.2.5. The information stored in OBL of S-RefreshGO-rsp is the value of the difference between the calculated ts_offset and the used ts_offset, also described in 12.7.2.5.

12.7.1.6 S-Data

12.7.1.6.1 Structure

S-Data is an area that stores safety data. During safety refresh, S-Data uses the format shown in Figure 14, where safety_data is safety refresh data. The minimum size is 32 bits and the maximum size is 800 bits. The length of S-Data is variable in units of 4 octets (32-bit increments).

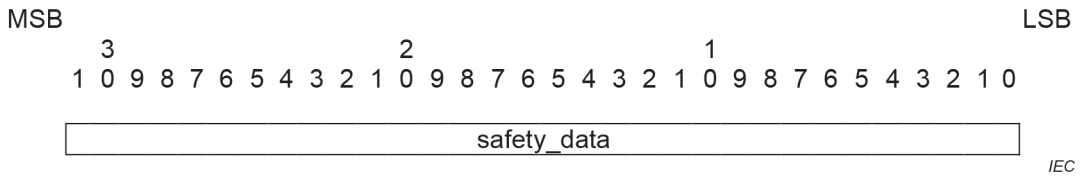


Figure 14 – S-Data during safety refresh

Figure 15 and Figure 16 show the S-Data formats used at times other than during safety refresh.

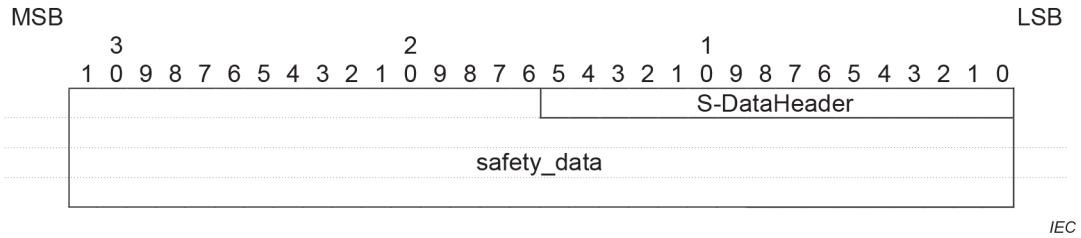


Figure 15 – S-Data not during safety refresh

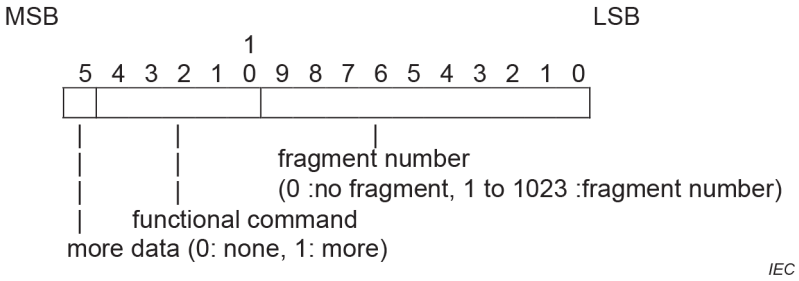


Figure 16 – S-Data header configuration

S-DataHeader
The header used when safety data is transmitted in fragments or when a functional command is executed.

Fragment number
Indicates the number of fragments. 0 indicates no fragments, and 1 to 1023 indicates the number of fragments.

Functional command
Indicates the functional command.

More data
Indicates whether or not there is more data when the safety data is transmitted in fragments. 0 indicates that there is no more data, and 1 indicates that there is more data.

12.7.1.6.2 Fragmentation

When safety data is transmitted in fragments, SASE-M sets the fragment number of the first S-DataHeader of the fragmented safety data to 1 and more data to 1. In the second and subsequent S-DataHeaders, SASE-M sequentially sets the fragment number to a value incremented by 1. SASE-M sets more data to 0 only when the fragment is the last fragment, and to 1 at any other time.

When requesting SASE-S to transmit safety data, SASE-M sends a request with the fragment number of the S-DataHeader set to 1 and more data set to 0. When SASE-S transmits the safety data in fragments, SASE-S sets the fragment number to 1 and more data to 1 in the S-DataHeader of the first fragmented safety data. When SASE-M receives the first fragmented safety data from SASE-S, it sends a request with the fragment number of the S-DataHeader set to 2 (equivalent to the value at the time of the previous request transmission incremented by 1) and more data set to 0. SASE-S then enters a value incremented by 1 as the fragment value in the second and subsequent S-DataHeaders.

SASE-S enters 0 for the last more data only, and 1 for all other more data values. SASE-M always enters a value equivalent to the previous value incremented by 1 for the fragment data of S-DataHeader, and 0 for more data.

12.7.1.7 CRC32

CRC32 is a 32-bit CRC for safety communication. The following formula shall be used as the CRC generator polynomial with the FSCP 8/2 safety communication function.

CRC generator polynomial (0x1F1922815)

$$G(x) = x^{32} + x^{31} + x^{30} + x^{29} + x^{28} + x^{24} + x^{23} + x^{20} + x^{17} + x^{13} + x^{11} + x^4 + x^2 + 1$$

NOTE This CRC generator polynomial is described in [32]. It exhibits properness when the block length (n), which is the sum of the message length and CRC length, is less than 2 046. In the range of 99 ≤ n ≤ 1 024, the minimum hamming distance of this CRC generator polynomial is 8.

CRC32 shall be calculated using CRTL, CID, TS, OBL, CC, RSV, and S-Data included in the safety PDU as shown in Figure 17.

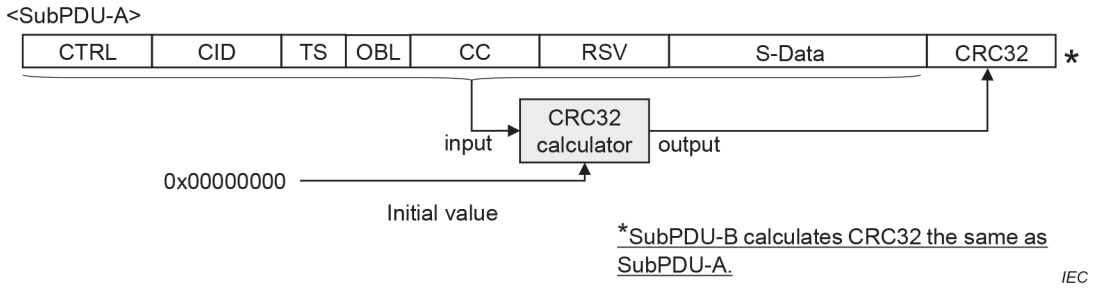


Figure 17 – CRC calculation

12.7.2 Safety FAL service protocol machine (SFSPM)

12.7.2.1 Overview

The behaviour of the safety communication layer of FSCP 8/2 is defined by the state machines, SFSPM-M and SFSPM-S, each time a safety connection is made. SFSPM-M and SFSPM-S communication uses the models shown in Figure 18 when performing safety refresh operations configured to transmit and receive safety input and output, and when performing operations other than safety refresh.

When operations other than safety refresh are performed, SFSPM-M sends a request to SFSPM-S, and SFSPM-S sends a response to SFSPM-M. When safety refresh operations are performed, SFSPM-M and SFSPM-S independently send requests to one another.

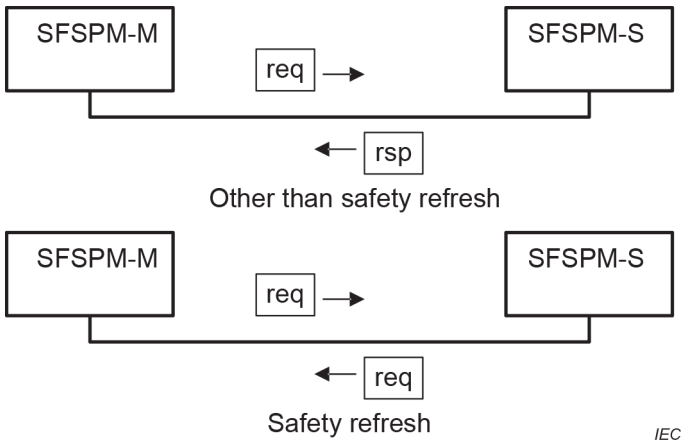


Figure 18 – Communication models

Figure 19 provides an overview of the state transitions of the safety communication layer.

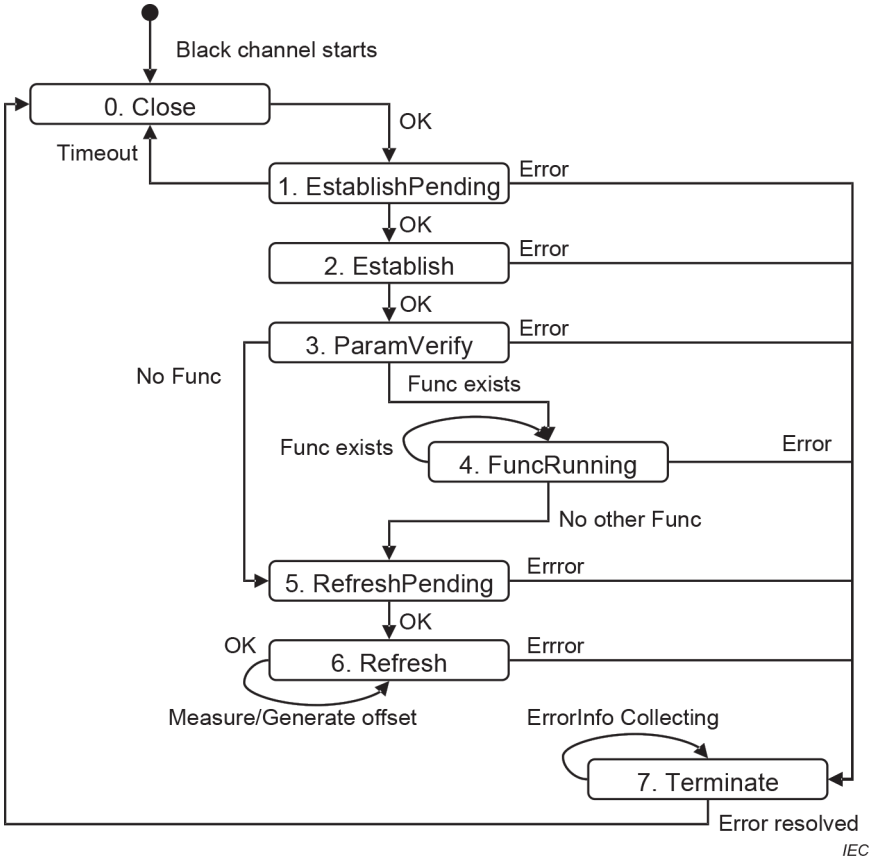


Figure 19 – SFSPM state transition diagram

Table 32 describes the states shown in Figure 19.

Table 32 – State list

No.	State Name	State	Description
0	Close	Safety connection not established	A safety connection is not established between SFSPM-M and SFSPM-S.
1	EstablishPending	Safety connection establishment pending	The establishment of a safety connection between SFSPM-M and SFSPM-S is pending.
2	Establish	Safety connection established	A safety connection is established between SFSPM-M and SFSPM-S.
3	ParamVerify	Parameter verification	The parameters held by SFSPM-M and SFSPM-S are being verified.
4	FuncRunning	Function running	Support functions of SFSPM-M and SFSPM-S are running. For executable support function, see Table 35, bits 2 to 31. This state is for future expansion. State transitions to this state do not occur.
5	RefreshPending	Safety refresh pending	Verification of the safety refresh ready status of SFSPM-M and SFSPM-S and measurement of the safety clock offset are currently in progress.
6	Refresh	Safety refresh in progress	Safety input/output information is currently being exchanged between SFSPM-M and SFSPM-S. At the same time, periodic safety clock offset measurement and generation are also being performed.
7	Terminate	Safety connection terminated	An error occurred on SFSPM-M and/or SFSPM-S, and the safety connection was terminated.

12.7.2.2 Behaviour

12.7.2.2.1 Safety initialization

The safety communication layer establishes a safety connection prior to communication as shown in Figure 20. The safety connection is established between SFSPM-M and SFSPM-S following the sequence below:

1) SFSPM-M starts a process to establish a safety connection. SFSPM-M sends a request to establish a safety connection in accordance with safety connection parameters given in advance.
2) SFSPM-S confirms that the received protocol version and the received S-Data size are correct.
3) SFSPM-S sends a request to establish a safety connection.
4) SFSPM-M confirms that the received protocol version and the received S-Data size are correct.
5) SFSPM-M sends a request to invoke the supported functions based on the supported functions information, which was agreed when the safety connection was established. SFSPM-M sends a request to confirm the network parameter, which is the supported function.
6) SFSPM-S keeps the network parameter contained in the request and sends a response to the network parameter confirmation.
7) SFSPM-M keeps the network parameter contained in the response.
8) SFSPM-M sends a request to verify safety station parameter.
9) SFSPM-S sends a response containing safety station parameter given in advance.
10) SFSPM-M identifies the SFSPM-S as the correct target by validating the received information with safety parameters given in advance.
11) SFSPM-M sends another supported function request unless all supported functions are requested.
12) SFSPM-S sends the response to the request unless supported functions requests are received.
13) SFSPM-M sends a refresh ready and offset measurement request.
14) SFSPM-S sends a refresh ready and offset measurement response.
15) SFSPM-M generates information to calculate offset and sends a safety refresh and offset generation request.
16) SFSPM-S generates offset based on the received information included in the request and sends a response.
17) SFSPM-M starts safety refresh by sending a safety refresh and offset generation request, and sends a safety refresh request at specified intervals.
18) SFSPM-S starts safety refresh by sending a safety refresh and offset generation request, and sends a safety refresh request at specified intervals.

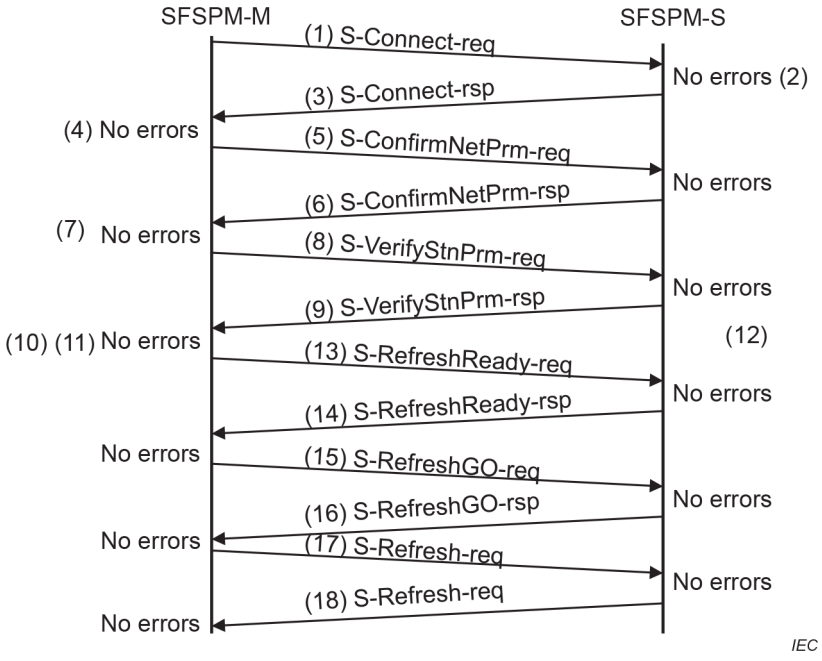


Figure 20 – Connection establishment sequence

During a safety connection establishment, an optional sequence can be executed after the safety parameters are verified. After executing the optional sequence, SFSPM-M sends a refresh ready and offset measurement request to the SFSPM-S.

The optional sequence is executed for the supported functions which are agreed between SFSPM-M and SFSPM-S during safety connection establishment.

The optional sequence diagram for station specific ID information verification, station specific configuration information check code verification, station specific configuration information write, and S-Data format negotiation is shown in Figure 21.

19) SFSPM-M sends a station specific ID information verification request if station specific ID information verification is agreed when safety connection is established.
20) SFSPM-S sends a response containing its station specific ID information given in advance.
21) SFSPM-M verifies the received station specific ID information.
22) If station specific configuration information check code verification is agreed when safety connection is established, the SFSPM-M sends a station specific configuration information check code verification request.
23) SFSPM-S sends a response containing its station specific configuration information check codes given in advance.
24) SFSPM-M verifies the received station specific configuration information check codes and the stored station specific configuration information check codes.
25) SFSPM-M sends a station specific configuration information write request if station specific configuration information write is agreed when safety connection is established.
26) SFSPM-S keeps the configuration contained in the request and sends a response.
27) If S-Data format negotiation is agreed when safety connection is established, the SFSPM-M sends an S-Data format negotiation request.
28) SFSPM-S sends an S-Data format negotiation response containing the S-Data format information given in advance.
29) SFSPM-M verifies the S-Data format information.

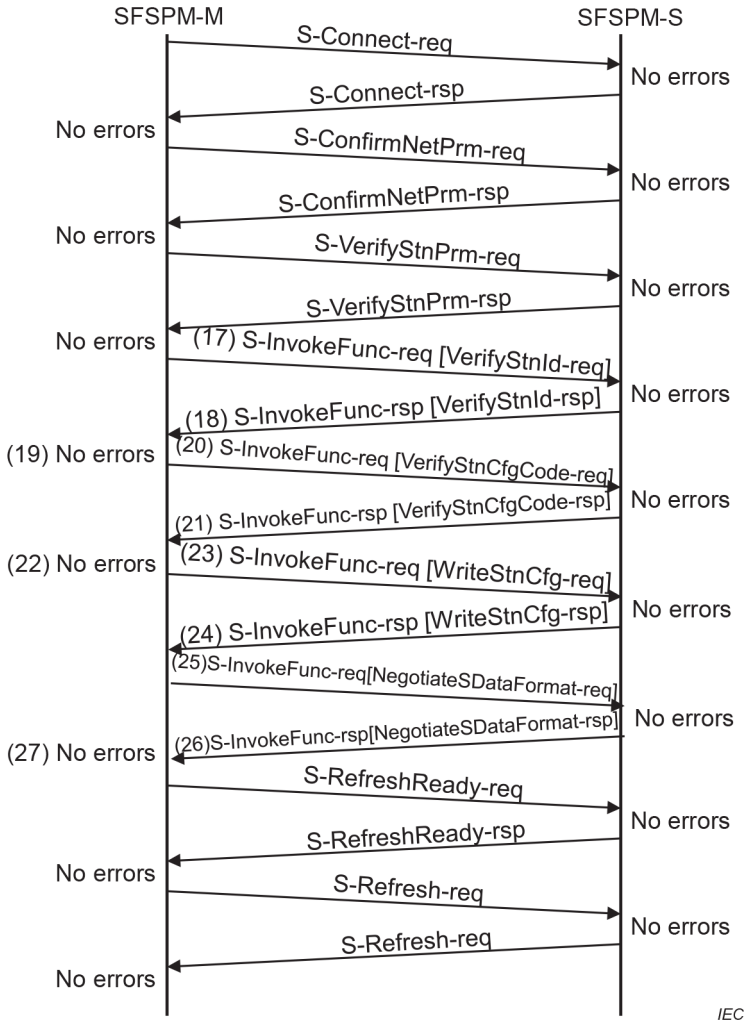


Figure 21 – Optional sequence during connection establishment sequence

12.7.2.2.2 Safety refresh

Figure 22 shows the normal communication sequence from SFSPM-M to SFSPM-S during the safety refresh communication that executes safety input/output transmission and reception.

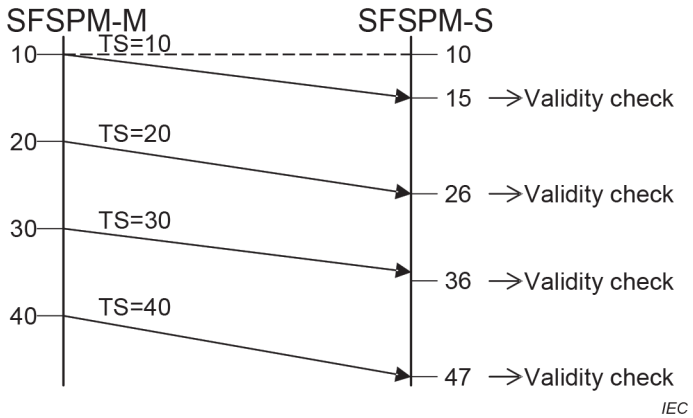


Figure 22 – Communication sequence during safety refresh communication

SFSPM-M periodically sends safety PDUs to SFSPM-S based on the SFSPM-M transmission interval (transmission_interval). SFSPM-S verifies the received safety PDUs.

SFSPM-S periodically sends safety PDUs to SFSPM-M based on the SFSPM-S transmission interval (transmission_interval). SFSPM-M verifies the received safety PDUs.

SFSPM-M and SFSPM-S shall conduct safety connection identifier verification, CRC verification, and time stamp verification of the received safety PDUs. SFSPM-M and SFSPM-S shall mutually monitor the periodic transmission of safety PDUs.

SFSPM-M and SFSPM-S shall deliver the received safety data to upper layers when the verification results of a received safety PDU indicate that the PDU is normal.

During safety refresh communication, SFSPM-M and SFSPM-S periodically execute offset measurement and generation. Figure 23 shows the sequence at the time of offset measurement and generation between SFSPM-M and SFSPM-S.

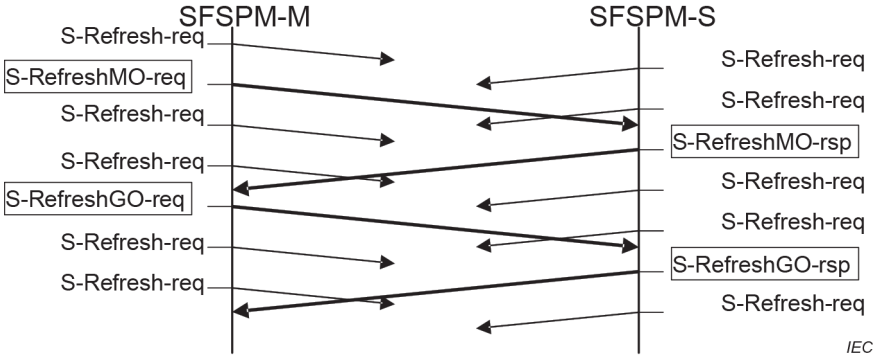


Figure 23 – Offset measurement and generation sequence during safety refresh communication

12.7.2.2.3 Safety connection termination

When a communication error is detected during safety initialization or safety refresh, SFSPM-M and SFSPM-S stop safety refresh (if the error occurred during safety refresh) and terminate the safety connection.

SFSPM-M or SFSPM-S shall terminate the safety connection following the procedure below.

1) SFSPM-M or SFSPM-S detects an error requiring safety connection termination.
2) SFSPM-M or SFSPM-S issues a notification to the safety user layer indicating that an error occurred requiring termination of the safety connection and the safety connection is subject to termination.
3) The safety user layer application switches the state and information related to the safety connection where the error occurred to a safe state.
4) SFSPM-M or SFSPM-S terminates the safety connection where the error occurred.
5) SFSPM-M re-establishes the safety connection once the error is cleared.

12.7.2.3 SFSPM-M

12.7.2.3.1 State transitions

Figure 24 shows an SFSPM-M state transition diagram.

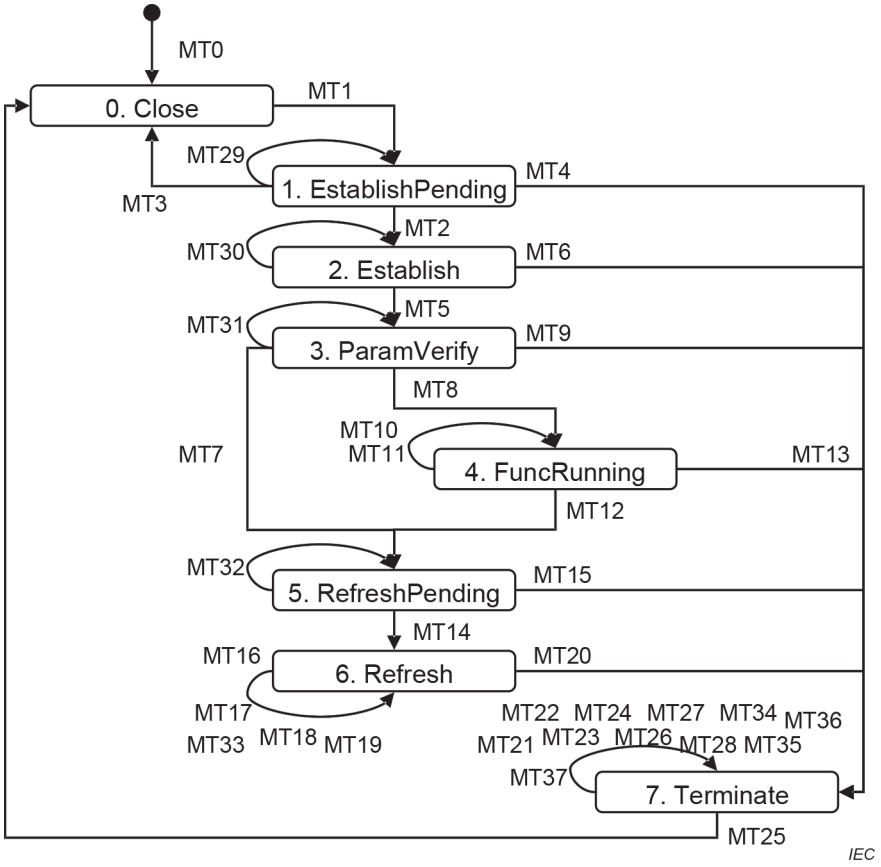


Figure 24 – SFSPM-M state transition diagram

Table 33 describes the timers used by SFSPM-M.

Table 33 – SFSPM-M timers

Name	Description
roundtrip_timer	Used to detect unallowable delays other than during safety refresh. It expires after the allowable_roundtrip_delay has elapsed.
delay_detection_timer	Used to detect unallowable delays. It expires after the allowable_refresh_interval has elapsed.

Table 34 shows the SFSPM-M state transition table.

Table 34 – SFSPM-M state transition table

Trans	State	Condition	Action	Next State
MT0	—	Black channel ready	—	0.Close
MT1	0.Close	—	Send S-Connect-req && Start roundtrip_timer	1.EstablishPending
MT2	1.EstablishPending	Receive S-Connect-rsp [NoError]	Stop roundtrip_timer && Send S-InitConfirmNetPrm-req && Start roundtrip_timer	2.Establish
MT29	1.EstablishPending	Receive S-Connect-rsp [Busy]	Stop roundtrip_timer && Send previously sent S-Connect-req && Start roundtrip_timer	1.EstablishPending
MT3	1.EstablishPending	roundtrip_timer timeout	—	0.Close
MT4	1.EstablishPending	Receive S-Connect-rsp [Error]	Stop roundtrip_timer	7.Terminate
MT5	2.Establish	Receive S-InitConfirmNetPrm-rsp [NoError]	Stop roundtrip_timer && Send S-InitVerifyStnPrm-req && Start roundtrip_timer	3.ParamVerify
MT30	2.Establish	Receive S-InitConfirmNetPrm-rsp [Busy]	Stop roundtrip_timer && Send previously sent S-InitConfirmNetPrm-req && Start roundtrip_timer	2.Establish
MT6	2.Establish	roundtrip_timer timeout	—	7.Terminate
MT6	2.Establish	Receive S-InitConfirmNetPrm-rsp [Error]	Stop roundtrip_timer	7.Terminate
MT7	3.ParamVerify	Receive S-InitVerifyStnPrm-rsp [NoError] && OptFuncs not exist	Stop roundtrip_timer && Send S-RefreshReady-req && Start roundtrip_timer	6.RefreshPending
MT8	3.ParamVerify	Receive S-InitVerifyStnPrm-rsp [NoError] && OptFuncs exist	Stop roundtrip_timer && Send S-InvokeFunc-req && Start roundtrip_timer	4.FuncRunning
MT31	3.ParamVerify	Receive S-InitVerifyStnPrm-rsp [Busy]	Stop roundtrip_timer && Send previously sent S-InitVerifyStnPrm-req && Start roundtrip_timer	3.ParamVerify
MT9	3.ParamVerify	roundtrip_timer timeout	—	7.Terminate
MT9	3.ParamVerify	Receive S-InitVerifyStnPrm-rsp [Error]	Stop roundtrip_timer	7.Terminate
MT10	4.FuncRunning	Receive S-InvokeFunc-rsp [NoError] && Another OptFunc exists	Stop roundtrip_timer && Send S-InvokeFunc-req && Start roundtrip_timer	4.FuncRunning

Trans	State	Condition	Action	Next State
MT11	4.FuncRunning	Receive S-InvokeFunc-rsp [Busy]	Stop roundtrip_timer && Send previously sent S-InvokeFunc-req && Start roundtrip_timer	4.FuncRunning
MT12	4.FuncRunning	Receive S-InvokeFunc-rsp [NoError] && No other OptFunc exists	Stop roundtrip_timer && Send S-RefreshReady-req && Start roundtrip_timer	6.RefreshPending
MT13	4.FuncRunning	roundtrip_timer timeout	—	7.Terminate
MT13	4.FuncRunning	Receive S-InvokeFunc-rsp [Error]	Stop roundtrip_timer	7.Terminate
MT14	5.RefreshPending	ReceiveS-RefreshReady-rsp [NoError]	Stop roundtrip_timer && Send S-RefreshGO-req && Start roundtrip_timer	6.Refresh
MT32	5.RefreshPending	ReceiveS-RefreshReady-rsp [Busy]	Stop roundtrip_timer && Send previously sent S-RefreshReady-req && Start roundtrip_timer	6.RefreshPending
MT15	5.RefreshPending	roundtrip_timer timeout	—	7.Terminate
MT15	5.RefreshPending	ReceiveS-RefreshReady-rsp [Error]	Stop roundtrip_timer	7.Terminate
MT16	6.Refresh	Time to send [NoError]	Send S-Refresh-req	6.Refresh
MT17	6.Refresh	Time to measure offset	Send S-RefreshMO-req && Start roundtrip_timer	6.Refresh
MT18	6.Refresh	ReceiveS-RefreshMO-rsp [NoError]	Stop roundtrip_timer	6.Refresh
MT18	6.Refresh	Time to send [at first after S-RefreshMO-rsp with NoMOBusy received]	Send S-RefreshGO-req && Start roundtrip_timer	6.Refresh
MT33	6.Refresh	ReceiveS-RefreshMO-rsp [MOBusy]	Stop roundtrip_timer && Start roundtrip_timer	6.Refresh
MT19	6.Refresh	ReceiveS-RefreshGO-rsp [NoError]	Stop roundtrip_timer	6.Refresh
MT20	6.Refresh	Receive S-Refresh-req [Error]	—	7.Terminate
MT20	6.Refresh	roundtrip_timer timeout	—	7.Terminate
MT20	6.Refresh	ReceiveS-RefreshMO-rsp [Error]	Stop roundtrip_timer	7.Terminate
MT20	6.Refresh	ReceiveS-RefershGO-rsp [Error]	Stop roundtrip_timer	7.Terminate
MT21	7.Terminate	Need to collect error information	Send S-ReadErrorInfo-req && Start roundtrip_timer	7.Terminate
MT22	7.Terminate	Receive S-ReadErrorInfo-rsp [No more data]	Stop roundtrip_timer	7.Terminate
MT34	7.Terminate	Receive S-ReadErrorInfo-rsp [More data]	Stop roundtrip_timer && S-ReadErrorInfo-req && Start roundtrip_timer	7.Terminate

Trans	State	Condition	Action	Next State
MT35	7.Terminate	ReceiveS-ReadErrorInfo-rsp [Busy]	Stop roundtrip_timer && Send previously sent S-ReadErrorInfo-req && Start roundtrip_timer	7.Terminate
MT23	7.Terminate	Need to send error information	Send S-WriteErrorInfo-req && Start roundtrip_timer	7.Terminate
MT24	7.Terminate	Receive S-WriteErrorInfo-rsp [No more data]	Stop roundtrip_timer	7.Terminate
MT36	7.Terminate	Receive S-WriteErrorInfo-rsp [More data]	Stop roundtrip_timer && S-WriteErrorInfo-req && Start roundtrip_timer	7.Terminate
MT37	7.Terminate	ReceiveS-WriteErrorInfo-rsp [Busy]	Stop roundtrip_timer && Send previously sent S-WriteErrorInfo-req && Start roundtrip_timer	7.Terminate
MT25	7.Terminate	Error resolved	—	0.Close
MT26	7.Terminate	Need to invoke Function	Send S-InvokeFunc-req && Start roundtrip_timer	7.Terminate
MT27	7.Terminate	Receive S-InvokeFunc-rsp	Stop roundtrip_timer	7.Terminate
MT28	7.Terminate	Receive S-InvokeFunc-rsp [Busy]	Send previously sent S-InvokeFunc-req	7.Terminate
MT4, MT6, MT9, MT13, and MT15 errors: Abnormal CTRL, Error state bit = 1, Abnormal S-Data MT20 error: Incorrect order, Loss, Unallowable delay, Abnormal CTRL, Error state bit = 1				

12.7.2.3.2 Operation other than during safety refresh

SFSPM-M starts the timer roundtrip_timer at the same time as it sends a request. SFSPM-M receives a response to the request from SFSPM-S, and stops the timer roundtrip_timer. The timer roundtrip_timer expires at the allowable_roundtrip_delay. If SFSPM-M does not receive a response to the request before the timer roundtrip_timer expires, an unallowable delay occurs. Figure 25 shows the sequence for states other than safety refresh.

When sending a request, SFSPM-M inserts the lower 16 bits of the safety clock value into the TS of the safety PDU and sends the request. When sending a response, SFSPM-S inserts the value of the TS included in the safety PDU of the corresponding request into the TS of the safety PDU that is to serve as the response. SFSPM-M verifies that the response corresponds to the request by comparing the value of the TS included in the response with the value of the TS sent. If the two values do not match, SFSPM-M shall discard the received safety PDU.

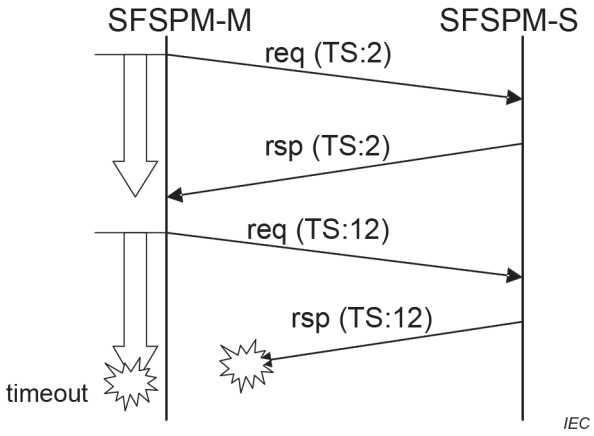


Figure 25 – Sequence other than during safety refresh

12.7.2.3.3 S-Data syntax

12.7.2.3.3.1 S-Connect-req

S-Connect-req uses the S-Data format shown in Figure 15. The safety_data area stores the data described in Figure 26.

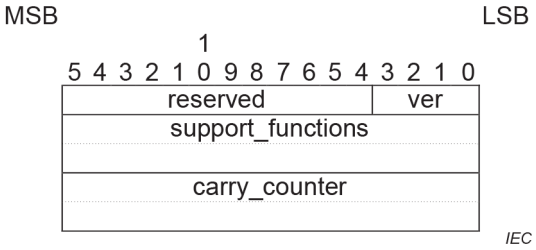


Figure 26 – S-Connect-req

ver
Indicates the protocol version of FSCP 8/2 supported by SFSPM-M. The protocol version is 0000b.

reserved
Reserved for future expansion.

support_functions
Table 35 describes the details of the support functions of S-Connect-req. Each bit indicates whether or not the function indicated in the table is supported. 1 indicates that the function is supported, and 0 indicates that the function is not supported.

Table 35 – support_functions

Bit	Function	Description
0	Safety network parameter verification	Verifies the network safety parameters held by SFSPM-M and SFSPM-S.
1	Safety station parameter verification	Verifies the safety station parameters held by SFSPM-M and SFSPM-S.
2 – 31	For future expansion	For future expansion

carry_counter
The initial value of the carry_counter used by SFSPM-M and SFSPM-S after S-Connect transmission/reception.

If S-Data of the safety PDU is S-connect-req, the value of the carry_counter used in the generation of CRC32 as initial value is 0.

12.7.2.3.3.2 S-InitConfirmNetPrm-req

S-InitConfirmNetPrm-req uses the S-Data format shown in Figure 15. The safety_data area stores the data described in Figure 27.

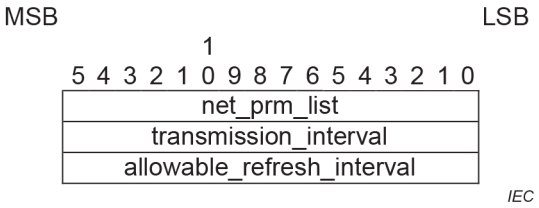


Figure 27 – S-InitConfirmNetPrm-req

net_prm_list
A list of the safety network parameters to be confirmed. Figure 28 shows the configuration of net_prm_list. 1 indicates that the parameter is to be confirmed, and 0 indicates that it is not. The bits of transmission_interval and allowable_refresh_interval are set to 1.

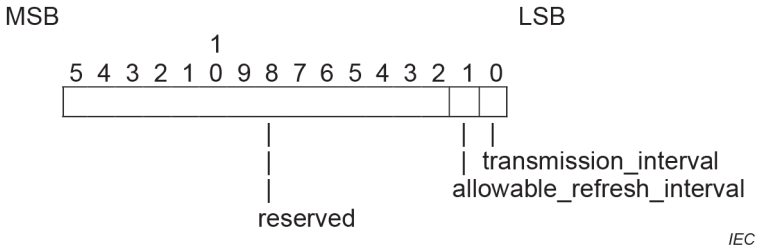


Figure 28 – net_prm_list

transmission_interval
The transmission interval of the safety PDUs of SFSPM-M during safety refresh. The unit is 128 µs.

allowable_refresh_interval
The allowable reception interval used by SFSPM-M and SFSPM-S during safety refresh. The unit is 128 µs.

12.7.2.3.3.3 S-InitVerifyStnPrm-req

S-InitVerifyStnPrm-req uses the S-Data format shown in Figure 15. The safety_data area stores the data described in Figure 29.

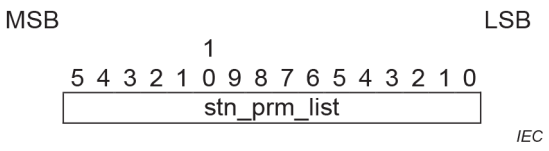


Figure 29 – S-InitVerifyStnPrm-req

stn_prm_list
A list of safety station parameters to be verified. Figure 30 shows the configuration of stn_prm_list. 1 indicates that the parameter is to be verified, and 0 indicates that it is not.

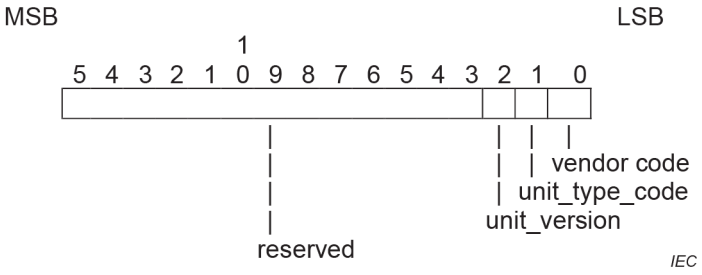


Figure 30 – stn_prm_list

12.7.2.3.3.4 S-InvokeFunc-req

S-InvokeFunc-req uses the S-Data format shown in Figure 15. The safety_data areas stores the data described in Figure 31.

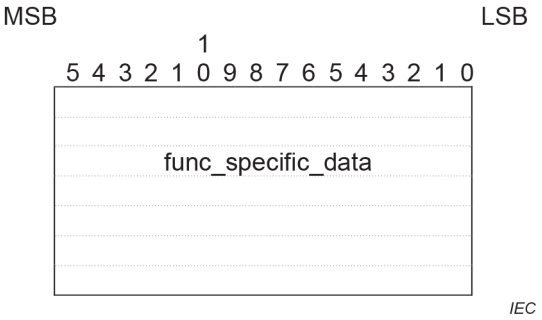


Figure 31 – S-InvokeFunc-req

func_specific_data
Data related to the function specified by the functional command of S-DataHeader. funcspecific_data is determined for each functional command.

12.7.2.3.3.5 S-RefreshReady-req

S-RefreshReady-req uses the S-Data format shown in Figure 15. The safety_data area does not store any information.

12.7.2.3.3.6 S-ReadErrorInfo-req

S-ReadErrorInfo-req uses the S-Data format shown in Figure 15. The safety_data area does not store any information.

12.7.2.3.3.7 S-WriteErrorInfo-req

S-WriteErrorInfo-req uses the S-Data format shown in Figure 15. The safety_data area stores the data described in Figure 32.

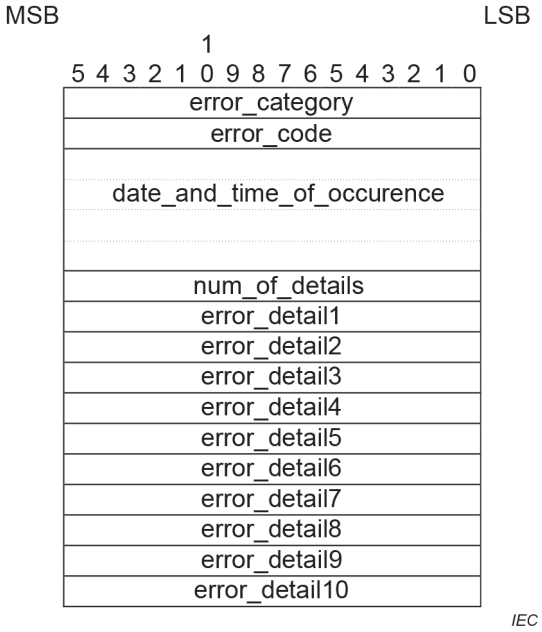


Figure 32 – S-WriteErrorInfo-req

error_category
Indicates the category of an error, and uses the values indicated in Table 36 and Table 37.

Table 36 – error_category

Value	Meaning
0 – 299	For future expansion
300 – 349	Application layer common error (see Table 37)
350	Application layer vendor definition error
351 – 399	For future expansion (application layer error)
400~449	For future expansion (service user layer common error)
450	Service user layer vendor definition error
451 – 449	For future expansion (service user layer error)
500 – 66535	For future expansion

Table 37 – error_category for AL errors

Value	Meaning
300 – 309	For future expansion
310 – 314	Application layer error

error_code
Indicates the error number. The numbers used are shown in Table 38.

Table 38 – error_code

error_category	error_code	Meaning
310	0	CRC error detection
	1	TS error
	2	CID error
311	0	delay_detection_timer timeout
	1	roundtrip_timer time-out
312	0	Fragment number error
313	0	Safety network parameter error
314	0	Safety station parameter error

date_and_time_of_occurence
Indicates the date and time of error occurrence. The format used is that shown in Figure 33. The year_upper (upper two digits of year), year_lower (lower two digits of year), month, day, hour, minute, second, and day_of_week, all expressed in BCD code.

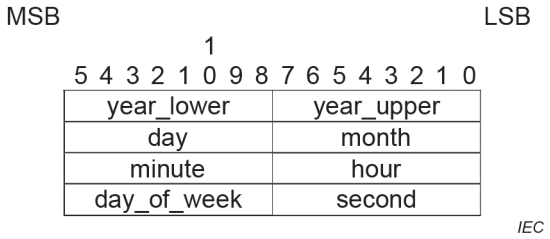


Figure 33 – date_and_time_of_occurence

num_of_details
Indicates the number of error details expressed by error_detail1 to error_detail10.

error_detail
Indicates the error details (1 – 10).

reserved
Reserved for future expansion.

12.7.2.3.3.8 S-RefreshMO-req

S-RefreshMO-req uses the S-Data format shown in Figure 14. The safety_data is safety refresh data.

12.7.2.3.3.9 S-RefreshGO-req

S-RefreshGO-req uses the S-Data format shown in Figure 14. The safety_data is safety refresh data.

12.7.2.3.3.10 S-Refresh-req

S-Refresh-req uses the S-Data format shown in Figure 14. The safety_data is safety refresh data.

12.7.2.4 SFSPM-S

12.7.2.4.1 State transistions

Figure 34 shows an SFSPM-S state transition diagram.

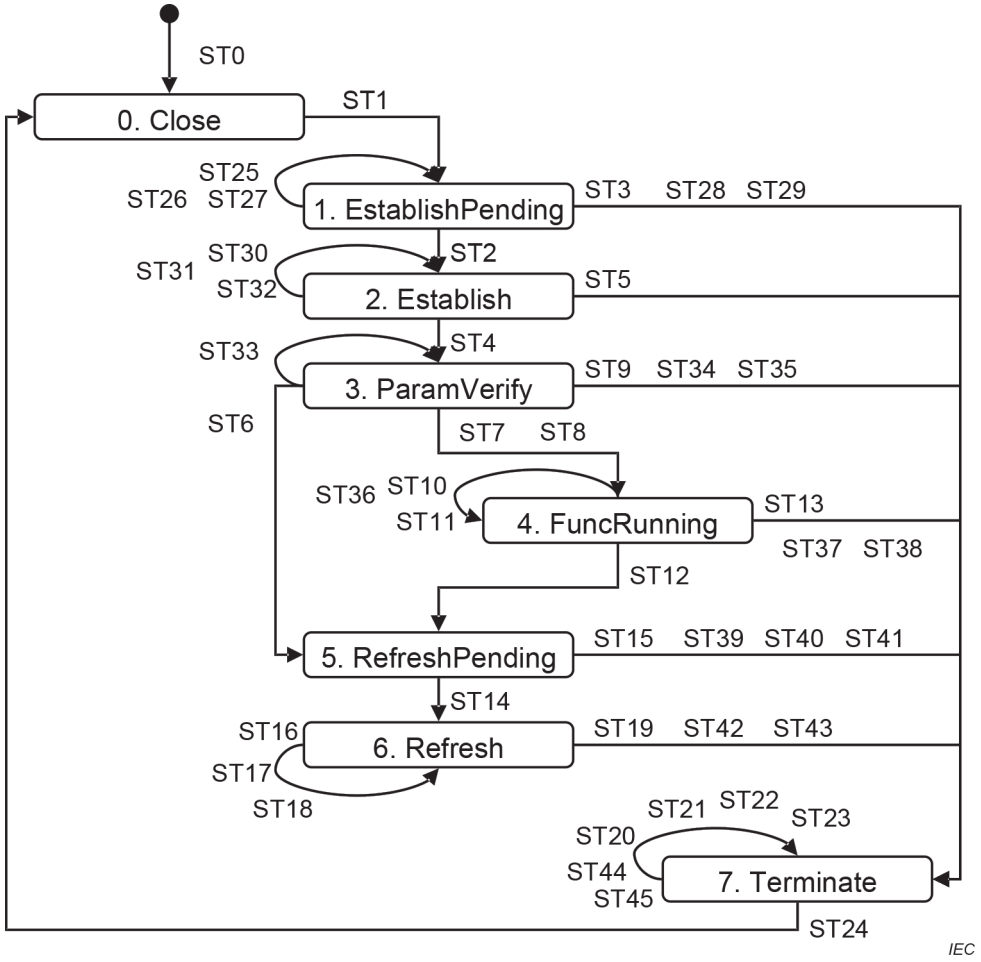


Figure 34 – SFSPM-S state transition diagram

Table 39 describes the timers used by SFSPM-S.

Table 39 – SFSPM-S timers

Name	Description
roundtrip_timer	Used to detect unallowable delays other than during safety refresh. It expires after the allowable_roundtrip_delay has elapsed.
delay_detection_timer	Used to detect unallowable delays. It expires after the allowable_refresh_interval has elapsed.

Table 40 shows the SFSPM-S state transition table.

Table 40 – SFSPM-S state transition table

Transition	State	Condition	Action	Next State
ST0	—	Black channel ready	—	0.Close
ST1	0.Close	Receive S-Connect-req [NoError]	Send S-Connect-rsp && Start roundtrip_timer	1.EstablishPending
ST2	1.EstablishPending	Receive S-InitConfirmNetPrm-req [NoError]	Stop roundtrip_timer && Send S-InitConfirmNetPrm-rsp && Start roundtrip_timer	2.Establish
ST25	1.EstablishPending	Receive S-Connect-req [NoError]	Stop roundtrip_timer && Send S-Connect-rsp && Start roundtrip_timer	1.EstablishPending
ST26	1.EstablishPending	Receive S-InitConfirmNetPrm-req [Busy]	Stop roundtrip_timer && Send S-InitConfirmNetPrm-rsp && Start roundtrip_timer	1.EstablishPending
ST27	1.EstablishPending	roundtrip_timer timeout	—	7.Terminate
ST3	1.EstablishPending	Receive S-InitConfirmNetPrm-req [Error]	Stop roundtrip_timer && Send S-InitConfirmNetPrm-rsp	7.Terminate
ST28	1.EstablishPending	Receive S-WriteErrorInfo-req [No more data]	Stop roundtrip_timer && Send S-WriteErrorInfo-rsp	7.Terminate
ST29	1.EstablishPending	Receive S-WriteErrorInfo-req [More data]	Stop roundtrip_timer && Send S-WriteErrorInfo-rsp && Start roundtrip_timer	7.Terminate
ST4	2.Establish	Receive S-InitVerifyStnPrm-req [NoError]	Stop roundtrip_timer && Send S-InitVerifyStnPrm-rsp && Start roundtrip_timer	3.ParamVerify
ST30	2.Establish	Receive S-InitVerifyStnPrm-req [Busy]	Stop roundtrip_timer && Send S-InitVerifyStnPrm-rsp && Start roundtrip_timer	2.Establish
ST31	2.Establish	Receive S-WriteErrorInfo-req [No more data]	Stop roundtrip_timer && Send S-WriteErrorInfo-rsp	7.Terminate
ST32	2.Establish	Receive S-WriteErrorInfo-req [More data]	Stop roundtrip_timer && Send S-WriteErrorInfo-rsp && Start roundtrip_timer	7.Terminate
ST5	2.Establish	roundtrip_timer timeout	—	7.Terminate
ST5	2.Establish	Receive S-InitVerifyStnPrm-req [Error]	Stop roundtrip_timer && Send S-InitVerifyStnPrm-rsp	7.Terminate
ST6	3.ParamVerify	Receive S-RefreshReady-req [NoError]	Stop roundtrip_timer && Send S-RefreshReady-rsp && Start roundtrip_timer	5.RefreshPending

Transition	State	Condition	Action	Next State
ST33	3.ParamVerify	Receive S-RefreshReady-req [Busy]	Stop roundtrip_timer && Send S-RefreshReady-rsp && Start roundtrip_timer	3.ParamVerify
ST7	3.ParamVerify	Receive S-InvokeFunc-req [NoError] && Processing complete	Stop roundtrip_timer && Send S-InvokeFunc-rsp [NoBusy] && Start roundtrip_timer	4.FuncRunning
ST8	3.ParamVerify	Receive S-InvokeFunc-req [NoError] && Function in progress	Stop roundtrip_timer && Send S-InvokeFunc-rsp [Busy] && Start roundtrip_timer	4.FuncRunning
ST34	3.ParamVerify	Receive S-WriteErrorInfo-req [No more data]	Stop roundtrip_timer && Send S-WriteErrorInfo-rsp	7.Terminate
ST35	3.ParamVerify	Receive S-WriteErrorInfo-req [More data]	Stop roundtrip_timer && Send S-WriteErrorInfo-rspStart roundtrip_timer	7.Terminate
ST9	3.ParamVerify	roundtrip_timer timeout	—	7.Terminate
ST9	3.ParamVerify	Receive S-InvokeFunc-req [Error]	Stop roundtrip_timer	7.Terminate
ST9	3.ParamVerify	Receive S-RefreshReady-req [Error]	Stop roundtrip_timer && Send S-RefreshReady-rsp	7.Terminate
ST10	4.FuncRunning	Receive S-InvokeFunc-req [NoError] && Processing complete	Stop roundtrip_timer && Send S-InvokeFunc-rsp [NoBusy] && Start roundtrip_timer	4.FuncRunning
ST11	4.FuncRunning	Receive S-InvokeFunc-req [NoError] && Function in progress	Stop roundtrip_timer && Send S-InvokeFunc-rsp [Busy] && Start roundtrip_timer	4.FuncRunning
ST12	4.FuncRunning	Receive S-RefreshReady-req [NoError]	Stop roundtrip_timer && Send S-RefreshReady-rsp && Start roundtrip_timer	5.RefreshPending
ST36	4.FuncRunning	Receive S-InvokeFunc-req [Busy]	Stop roundtrip_timer && Send S-InvokeFunc-rsp && Start roundtrip_timer	4.FuncRunning
ST37	4.FuncRunning	Receive S-WriteErrorInfo-req [No more data]	Stop roundtrip_timer && Send S-WriteErrorInfo-rsp	7.Terminate
ST38	4.FuncRunning	Receive S-WriteErrorInfo-req [More data]	Stop roundtrip_timer && Send S-WriteErrorInfo-rsp && Start roundtrip_timer	7.Terminate
ST13	4.FuncRunning	roundtrip_timer timeout	—	7.Terminate

Transition	State	Condition	Action	Next State
ST13	4.FuncRunning	Receive S-InvokeFunc-req [Error]	Stop roundtrip_timer && Send S-InvokeFunc-rsp	7.Terminate
ST13	4.FuncRunning	Receive S-RefreshReady-req [Error]	Stop roundtrip_timer && Send S-RefreshReady-rsp	7.Terminate
ST14	5.RefreshPending	ReceiveS-RefreshGO-req [NoError]	Stop roundtrip_timer && Send S-RefreshGO-rsp	6.Refresh
ST39	5.RefreshPending	Receive S-WriteErrorInfo-req [No more data]	Stop roundtrip_timer && Send S-WriteErrorInfo-rsp	7.Terminate
ST40	5.RefreshPending	Receive S-WriteErrorInfo-req [More data]	Stop roundtrip_timer && Send S-WriteErrorInfo-rsp && Start roundtrip_timer	7.Terminate
ST15	5.RefreshPending	roundtrip_timer timeout	—	7.Terminate
ST15	5.RefreshPending	ReceiveS-RefreshGO-req [ErrorA]	Stop roundtrip_timer	7.Terminate
ST15	5.RefreshPending	ReceiveS-RefreshGO-req [ErrorB]	Stop roundtrip_timer && Send S-RefreshGO-rsp && Start roundtrip_timer	7.Terminate
ST16	6.Refresh	Time to send [NoError]	Send S-Refresh-req	6.Refresh
ST17	6.Refresh	Receive S-RefreshMO-req [NoError]	Stop roundtrip_timer	6.Refresh
ST17	6.Refresh	Time to send [at first after S-RefreshMO-req with NoError received]	Send S-RefreshMO-rsp && Start roundtrip_timer	6.Refresh
ST18	6.Refresh	Receive S-RefreshGO-req [NoError]	—	6.Refresh
ST18	6.Refresh	Time to send [at first after S-RefreshGO-req with NoError received]	Send S-RefreshGO-rsp	6.Refresh
ST41	6.Refresh	Receive S-WriteErrorInfo-req [No more data]	Stop roundtrip_timer && Send S-WriteErrorInfo-rsp	7.Terminate
ST42	6.Refresh	Receive S-WriteErrorInfo-req [More data]	Stop roundtrip_timer && Send S-WriteErrorInfo-rsp && Start roundtrip_timer	7.Terminate
ST19	6.Refresh	Receive S-Refresh-req [Error]	—	7.Terminate
ST19	6.Refresh	Time to send [at first after S-Refresh-req with ErrorA received]	Send S-Refresh-req && Start roundtrip_timer	7.Terminate
ST19	6.Refresh	Receive S-RefreshMO-req [Error]	—	7.Terminate
ST19	6.Refresh	Time to send [at first after S-RefreshMO-req with ErrorA received]	Send S-RefreshMO-rsp && Startroundtrip_timer	7.Terminate
ST19	6.Refresh	Receive S-RefreshGO-req [Error]	Stop roundtrip_timer	7.Terminate
ST19	6.Refresh	Time to send [at first after S-RefreshGO-req with ErrorA received]	Send S-RefreshGO-rsp && Startroundtrip_timer	7.Terminate
ST19	6.Refresh	roundtrip_timer timeout	—	7.Terminate

Transition	State	Condition	Action	Next State
ST20	7.Terminate	Receive S-ReadErrorInfo-req [No more data]	Send S-ReadErrorInfo-rsp	7.Terminate
ST43	7.Terminate	Receive S-ReadErrorInfo-req [More data]	Stop roundtrip_timer && Send S-ReadErrorInfo-rsp && Startp roundtrip_timer	7.Terminate
ST21	7.Terminate	Receive S-WriteErrorInfo-req [No more data]	Send S-WriteErrorInfo-rsp	7.Terminate
ST44	7.Terminate	Receive S-WriteErrorInfo-req [More data]	Stop roundtrip_timer && Send S-WriteErrorInfo-rsp && Start roundtrip_timer	7.Terminate
ST22	7.Terminate	Receive S-InvokeFunc-req [NoError] && Processing complete	Send S-InvokeFunc-rsp [NoBusy]	7.Terminate
ST23	7.Terminate	Receive S-InvokeFunc-req [NoError] && Function in progress	Send S-InvokeFunc-rsp [Busy]	7.Terminate
ST24	7.Terminate	Error resolved	—	0.Close
ST3, ST5, ST9, and ST13 errors: Abnormal CTRL, Error state bit = 1, Abnormal S-Data ST15 Error A: Unallowable delay ST15 Error B: Incorrect order, Abnormal CTRL, Error state bit = 1 ST19 Error: Incorrect order, Loss, Unallowable delay, Abnormal CTRL, Error state bit = 1 ST19 Error A: Incorrect order, Abnormal CTRL, Error state bit = 1				

12.7.2.4.2 Operation other than during safety refresh

SFSPM-S starts the timer roundtrip_timer at the same time as it sends a response. SFSPM-S receives the next request in reply to its response from SFSPM-M, and stops the timer roundtrip_timer. The timer roundtrip_timer expires at the allowable_roundtrip_delay. If SFSPM-S does not receive the next request in reply to its response before the timer roundtrip_timer expires, an unallowable delay occurs. Figure 35 shows the sequence for states other than safety refresh.

When sending a response, SFSPM-S inserts the value of TS included in the safety PDU of the corresponding request into the TS of the safety PDU.

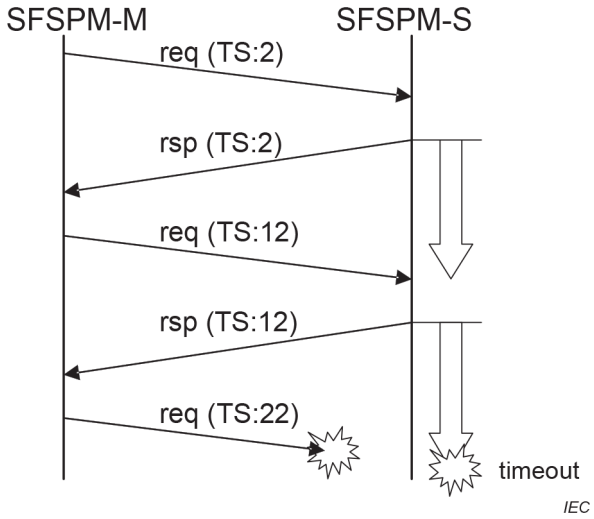


Figure 35 – Sequence other than during safety refresh

12.7.2.4.3 S-Data syntax

12.7.2.4.3.1 S-Connect-rsp

S-Connect-rsp uses the S-Data format shown in Figure 15. The safety_data area stores the data described in Figure 36.

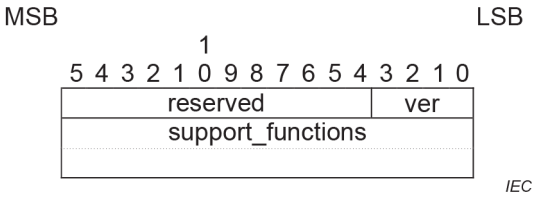


Figure 36 – S-Connect-rsp

Ver
Indicates the protocol version of the FSCP 8/2 safety communication function supported by SFSPM-S. The protocol version is 0000b.

reserved
Reserved for future expansion.

support_functions
Indicate the functions supported by SFSPM-S out of the support_functions that SFSPM-M reported to SFSPM-S. Table 35 describes the specifiable details. Each bit indicates whether or not the function indicated in the table is supported. 1 indicates that the function is supported, and 0 indicates that the function is not supported. SFSPM-S regards the value of the logical product of the support_functions notified by SFSPM-M and the functions supported by SFSPM-S as support_functions.

12.7.2.4.3.2 S-InitConfirmNetPrm-rsp

S-InitConfirmNetPrm-rsp uses the S-Data format shown in Figure 15. The safety_data area stores the data described in Table 37.

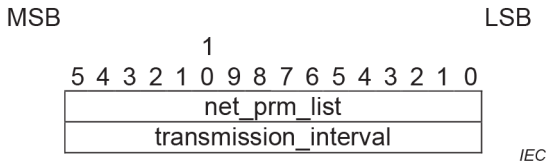


Figure 37 – S-InitConfirmNetPrm-rsp

net_prm_list
A list of safety network parameters to be confirmed. 1 indicates that the parameter is to be confirmed and 0 indicates that it is not. For the configuration of net_prm_list, see Figure 28. The bit of transmission_interval is set to 1.

transmission_interval
The transmission interval of the safety PDUs of SFSPM-S during safety refresh. The unit is 128 µs.

12.7.2.4.3.3 S-InitVerifyStnPrm-rsp

S-InitVerifyStnPrm-rsp uses the S-Data format shown in Figure 15. The safety_data area stores the data described in Figure 38.

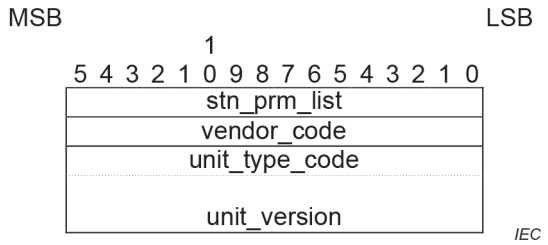


Figure 38 – S-InitVerifyStnPrm-rsp

stn_prm_list
A list of safety station parameters to be verified. For details, see 12.7.2.3.3.3.

vendor_code
A unique code assigned to a vendor to identify the vendor.

unit_type_code
A unique code assigned to each product model managed by the vendor.

unit_version
The version of the operation specifications of the product managed by the vendor.

12.7.2.4.3.4 S-InvokeFunc-rsp

S-InvokeFunc-rsp uses the S-Data format shown in Figure 15. The safety_data area stores the data described in Figure 39.

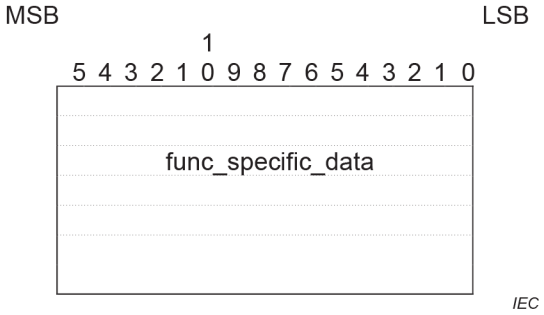


Figure 39 – S-InvokeFunc-rsp

func_specific_data
Data related to the function specified by the functional command of S-DataHeader. funcspecific_data is determined for each functional command.

12.7.2.4.3.5 S-RefreshReady-rsp

S-RefreshReady-rsp uses the S-Data format shown in Figure 15. The safety_data area does not store any information.

12.7.2.4.3.6 S-ReadErrorInfo-rsp

S-ReadErrorInfo-req uses the S-Data format shown in Figure 15. The safety_data area stores the data shown in Figure 32. For safety_data details, see 12.7.1.6.

12.7.2.4.3.7 S-WriteErrorInfo-rsp

S-WriteErrorInfo-rsp uses the S-Data format shown in Figure 15. The safety_data area does not store any information.

12.7.2.4.3.8 S-RefreshMO-rsp

S-RefreshMO-rsp uses the S-Data format shown in Figure 14. The safety_data is safety refresh data.

12.7.2.4.3.9 S-RefreshGO-rsp

S-RefreshGO-rsp uses the S-Data format shown in Figure 14. The safety_data is safety refresh data.

12.7.2.4.3.10 S-Refresh-req

S-Refresh-req uses the S-Data format shown in Figure 14. The safety_data is safety refresh data.

12.7.2.5 Correcting the clock offset

The difference between the safety clocks of SFSPM-M and SFSPM-S is the offset ts_offset.

SFSPM-M shall use the value of the lower 16 bits of the safety clock of its own node to generate time stamps.

SFSPM-S shall use the value current_time of the lower 16 bits of the safety clock of its own node and the offset ts_offset to generate time stamps. SFSPM-S shall use Formula (1) for this calculation.

$$TS = (current\_time + ts\_offest) \bmod 2^{16} \quad (1)$$

Figure 40 shows the offset calculation procedure of the safety clock.

NOTE 1 This calculation is a modified version of the widely-known Cristian's algorithm.

NOTE 2 FSCP 8/2 uses deterministic media access control based on token passing. Since transmission is performed only by the node holding the token, there is no conflict or queuing of multiple frames in intermediate nodes. In addition, only a single logical path is established between two nodes.

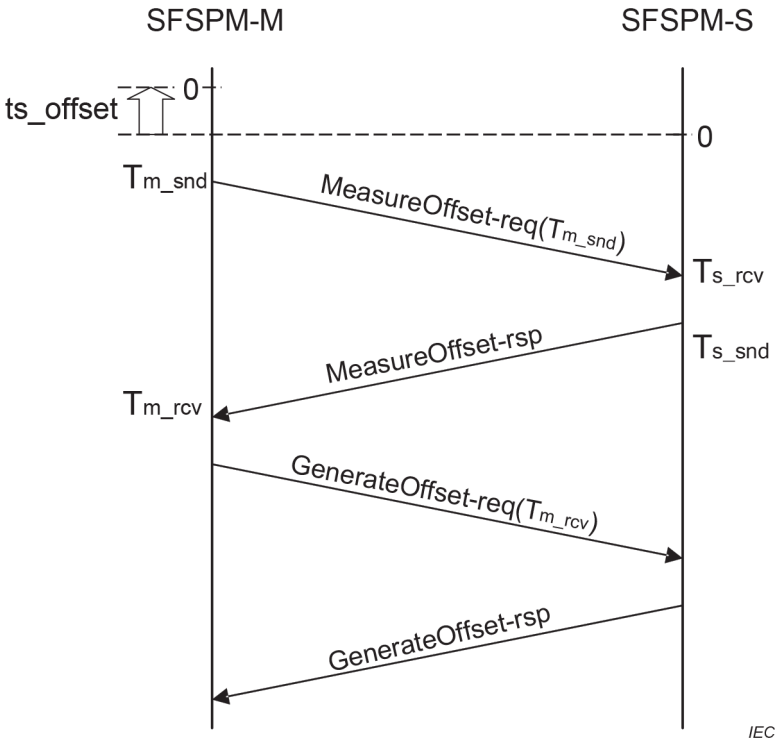


Figure 40 – Offset calculation procedure of safety clock

SFSPM-M generates MeasureOffset-req, and sends MeasureOffset-req, which includes the safety clock value at the time of MeasureOffset-req transmission, to SFSPM-S.

SFSPM-S receives MeasureOffset-req and records the safety clock value at the time of reception and the safety clock value included in MeasureOffset-req. SFSPM-S then generates MeasureOffset-rsp, records the safety clock value at the time of MeasureOffset-rsp transmission, and sends the generated MeasureOffset-rsp to SFSPM-M.

SFSPM-M receives MeasureOffset-rsp and records the safety clock value at the time of reception. SFSPM-M, which received MeasureOffset-rsp, then generates GenerateOffset-req with offset calculation information, which is the safety clock value at the time of MeasureOffset-rsp reception, and sends GenerateOffset-req to SFSPM-S.

SFSPM-S receives GenerateOffset-req, calculates and stores the offset ts_offset based on the recorded safety clock value and the offset calculation information in GenerateOffset-req. SFSPM-S then generates GenerateOffset-rsp, which stores the difference between the used ts_offset and the calculated ts_offset in OBL, and sends GenerateOffset-rsp to SFSPM-M.

SFSPM-S verifies that the round-trip transmission delay at the time of offset calculation is within range prior to ts_offset calculation using Formula (2). If the value is out of range, SFSPM-S shall not use the collected information in offset calculation.

$$0 < \left(T_{m\_rcv} - T_{m\_snd}\right) - \left(T_{s\_snd} - T_{s\_rcv}\right) \leq 2 \times link\_transmission\_delay \quad (2)$$

link_transmission_delay is the transmission delay of the FSCP 8/2 network, which is calculated from the following three parameters: the allowable_refresh_interval, SFSPM-M transmission_interval, and SFSPM-S transmission_interval (which are described in 12.7.2). D_{lt} is calculated using Formula (3).

$$D_{lt} = I_{ar} - I_{mt} - I_{st} \quad (3)$$

where

D_{lt} is the link transmission delay;

I_{ar} is the allowable refresh interval;

I_{mt} is the SFSPM-M transmission interval;

I_{st} is the SFSPM-S transmission interval.

Formula (4) shall be used to calculate the offset *ts_offset*:

$$ts\_offset = 0{,}5 \times \left(\left(T_{m\_rcv} + T_{m\_snd}\right) - \left(T_{s\_snd} + T_{s\_rcv}\right)\right) \quad (4)$$

The calculated dispersion *offset_dispersion* of Formula (5) is included in the calculated offset *ts_offset*.

$$offset\_dispersion = 0{,}5 \times \left(\left(T_{m\_rcv} - T_{m\_snd}\right) + \left(T_{s\_rcv} - T_{s\_snd}\right)\right) \quad (5)$$

The maximum value of the calculation deviation *offset_dispersion* is *link_transmission_delay*.

SFSPM-M confirms that SFSPM-S calculated the offset with the reception of GenerateOffset-rsp. SFSPM-M receives GenerateOffset-rsp and uses an adjusted TS in place of the TS included in GenerateOffset-rsp to detect incorrect order and loss of the received GenerateOffset-rsp and determine the transmission interval described in 12.7.2. The adjusted TS is a value obtained by subtracting the value stored in OBL of GenerateOffset-rsp received by SFSPM-M, that is, the difference between the ts_offset calculated by SFSPM-S and ts_offset used by SFSPM-S, from the value stored in TS of the received GenerateOffset-rsp.

NOTE When SFSPM-S changes ts_offset as a result of an offset calculation performed during safety refresh, the actual transmission interval of SFSPM-S differs from the value that is calculated by subtracting the TS of the previously received PDU subtracted from the TS of GenerateOffset-rsp. Implementing this procedure yields two matching values.

Offset calculation is performed at the time of safety connection establishment and periodically during safety refresh. At the time of safety connection establishment, S-RefreshReady is used as MeasureOffset, and S-RefreshGO is used as GenerateOffset. T_{m_snd} and T_{m_rcv} are delivered from SFSPM-M to SFSPM-S as the TS for S-RefreshReady and the OBL of S-RefreshGO, respectively. During safety refresh, S-RefreshMO is used as MeasureOffset, and S-RefreshGO is used as GenerateOffset. T_{m_snd} and T_{m_rcv} are delivered from SFSPM-M to SFSPM-S as the TS for S-RefreshMO and the OBL for S-RefreshGO, respectively.

During safety refresh, SFSPM-M shall correct the clock offset at the interval defined below. The resolution_factor shall be determined so that the error caused by clock drift is kept below 128 microseconds, which is the safety clock unit of measurement as shown by Formula (6).

$$interval = transmission\_interval \times resolution\_factor \tag{6}$$

If the safety clock accuracy is 100 ppm, the error is ± 100 µs per second, maximum. When the errors of the SFSPM-M and SFSPM-S safety clocks are opposite in direction, the difference caused by clock drift is 200 µs per second, maximum. At this time, the clock offset may be corrected at an interval of 640 ms or less to keep the error less than 128 µs. The *resolution_factor* is calculated using Formula (7).

$$resolution\_factor < \frac{640}{transmission\_interval} \tag{7}$$

12.7.2.6 Calculating the reception time

SFSPM-M shall use the value of the lower 16 bits of the safety clock at the time of reception.

SFSPM-S shall use the value calculated using Formula (8), based on the *receipt_time*, which is the value of the lower 16 bits of the safety clock at the time of reception, and the offset *ts_offset*.

$$time = (receipt\_time + ts\_offset) \bmod 2^{16} \tag{8}$$

12.7.2.7 Operating carry_counter

SFSPM-S calculates *SFSPM_M_current_time* using Formula (9) from the *current_time*, which is the lower 16 bits of the safety clock of SFSPM-S, and the offset *ts_offset*, each time a safety PDU is sent and received.

$$SFSPM\_M\_current\_time = (current\_time + ts\_offset) \bmod 2^{16} \tag{9}$$

If Formula (10) is satisfied, the carry_counter is incremented by 1.

$$prev\_SFSPM\_M\_current\_time > SFSPM\_M\_current\_time \tag{10}$$

Here, *prev_SFSPM_M_current_time* is the previously calculated *SFSPM_M_current_time*.

The transmission interval transmission_interval and current_time unit of measurement and size are the same. Thus, the current_time overflow count is 1 (maximum, as long as transmission is within the transmission_interval). As a result, the carry_counter increment is 1.

12.8 Safety communication layer management for FSCP 8/2

12.8.1 Parameter Definitions

12.8.1.1 Parameter list

Table 41 lists the parameters used by FSCP 8/2.

Table 41 – Parameters used by safety communication layer

Parameter Name	Contents	Configurable/Generated
connection_id	Safety connection identifier	Configurable
transmission_interval	Transmission interval	Configurable
allowable_refresh_interval	Allowable refresh interval	Configurable
allowable_delay	Maximum allowable delay	Generated by safety communication layer
allowable_roundtrip_delay	Allowable roundtrip delay	Generated by safety communication layer

12.8.1.2 connection_id

Connection_id is a configurable parameter that indicates the identifier of the relationship between the transmission source and transmission destination. The size is 32 bits. connection_id shall be assigned a unique value within the network. To ensure uniqueness, connection_id shall be a value derived from the transmission source address and transmission destination address (16 bits each). The transmission source address and transmission destination address are generated from the network number and station number (8 bits each).

12.8.1.3 transmission_interval

The *transmission_interval* is a configurable parameter that specifies the maximum interval for transmitting safety PDUs during safety refresh. The size is 16 bits, and the unit is 128 µs. The minimum value is 2.

The transmission interval of safety PDUs sometimes fluctuates. The *actual_transmission_interval* shall be within the range given by Formula (11).

$$\frac{transmission\_interval}{2} < actual\_transmission\_interval \leq transmission\_interval \quad (11)$$

To normally receive safety PDUs sent at the maximum transmission interval (transmission_interval), the upper limit of the actual transmission interval shall be less than or equal to the maximum transmission interval. On the other hand, the actual transmission interval requires a lower limit to detect the loss of a middle safety PDU between three safety PDUs sent continuously at the minimum transmission interval. Figure 41 shows the sequence for such a case. The loss of the second safety PDU can be detected if the value is less than twice the minimum transmission interval.

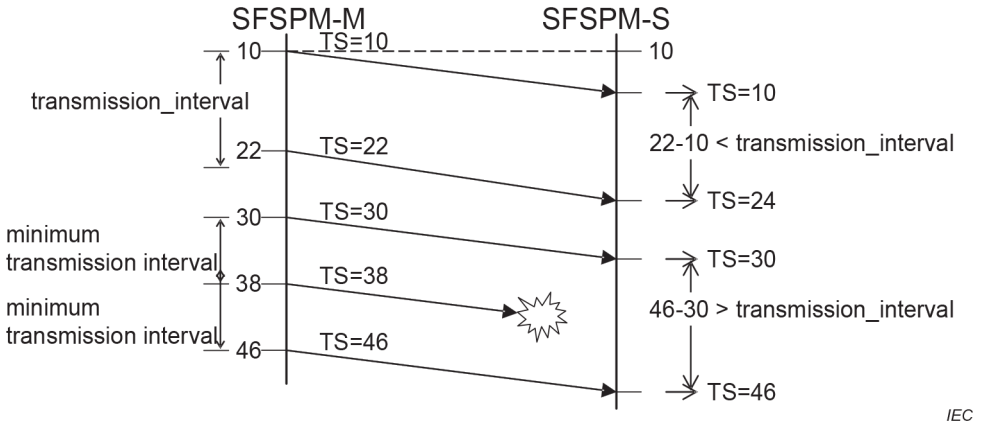


Figure 41 – Relationship between transmission interval fluctuation and transmission_interval

12.8.1.4 allowable_refresh_interval

allowable_refresh_interval is a configurable parameter that specifies the allowable refresh interval by the receiving node. The size is 16 bits, and the unit is 128 µs.

The following formula is used to calculate allowable_refresh_interval in SFSPM-S when safety PDUs are sent from SFSPM-M to SFSPM-S:

SFSPM-S allowable refresh interval, I_{sar} is calculated using Formula (12).

$$I_{sar} = I_t + D_{lt} + T_{spc} \tag{12}$$

where

I_{sar} is the SFSPM-S allowable refresh interval;

I_t SFSPM-M transmission interval;

D_{lt} link transmission delay of the FAL Type 23 network;

T_{spc} SFSPM-S processing cycle time.

When SFSPM-S is a safety logic device, the SFSPM-S processing cycletime depends on the processed contents. When SFSPM-S is a safety input/output device, the SFSPM-S processing cycletime depends on implementation.

Figure 42 illustrates the concept of determining the allowable_refresh_interval of SFSPM-S and SFSPM-M.

When the maximum delay time (TS3 – TS4) follows the shortest delay time (TS1 – TS2) during communication from SFSPM-M to SFSPM-S, the reception interval is calculated as shown below, where transmission_interval (SFSPM-M) indicates the transmission_interval of SFSPM-M.

SFSPM-S reception interval, I_{sr} is calculated using Formula (13) and Formula (14).

$$I_{sr} = I_t + D_t + T_{soc} \tag{13}$$

$$I_{sr} = I_{tm} + D_{lt} + T_{spc} \tag{14}$$

where

I_{sr} is the SFSPM-S reception interval (TS4 – TS2);
I_t is the transmission interval (TS3 – TS1);
D_t is the type 23 network transmission delay;
T_{soc} is the SFSPM-S operation cycle time;
I_{tm} is the SFSPM-M transmission interval;
D_{lt} is the link transmission delay;
T_{spc} is the SFSPM-S processing cycle time.

The same concept applies to SFSPM-S. transmission_interval (SFSPM-S) indicates the transmission_interval of SFSPM-S.

SFSPM-S allowable refresh interval, I_{sar} is calculated using Formula (15).

$$I_{sar} = I_t + D_{lt} + T_{mpc} \tag{15}$$

where

I_{sar} is the SFSPM-S allowable refresh interval;
I_t is the transmission interval;
D_{lt} is the link transmission delay;
T_{mpc} is the SFSPM-M processing cycle time.

Given that the transmission_interval is the same as the operation cycle time, the calculation formula becomes the same for both SFSPM-M and SFSPM-S. Allowable refresh interval, I_{ar} is calculated using Formula (16).

$$I_{ar} = D_{lt} + T_{mpc} + T_{spc} \tag{16}$$

where

I_{ar} is the allowable refresh interval;
D_{lt} is the link transmission delay;
T_{mpc} is the SFSPM-M processing cycle time;
T_{spc} is the SFSPM-S processing cycle time.

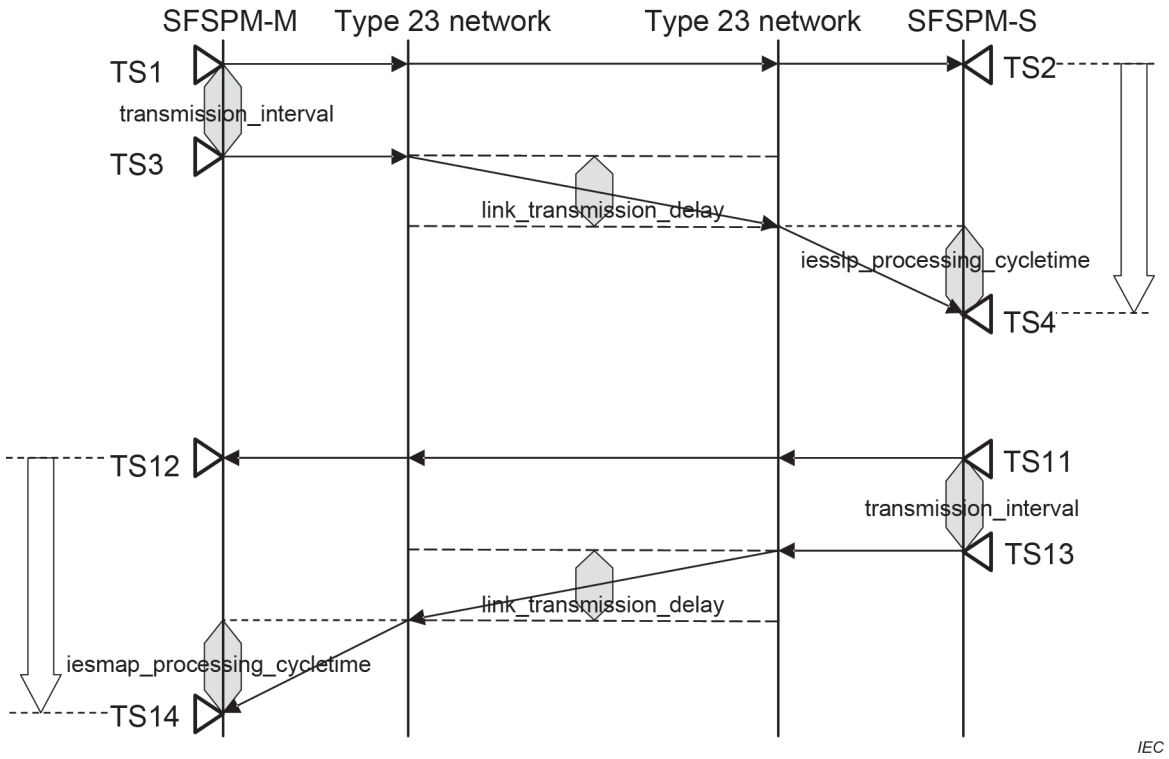


Figure 42 – Calculation of allowable_refresh_interval

12.8.1.5 allowable_delay

allowable_delay is the maximum allowable delay, and is a parameter used to detect the occurrence of unallowable delays. The size is 16 bits, and the unit is 128 µs.

The formula used to calculate allowable_delay is shown below. Transmission_interval (SFSPM-M) and transmission_interval (SFSPM-S) indicate the transmission intervals of SFSPM-M and SFSPM-S, respectively. Similar to allowable_refresh_interval, the transmission_interval is assumed to be the same as the operation cycle time.

Allowable delay for SFSPM-M, D_{ma} is calculated using Formula (17) and Formula (18).

$$D_{ma} = D_{lt} + T_{mpc} \tag{17}$$

$$D_{ma} = I_{ar} - I_{st} \tag{18}$$

Allowable delay for SFSPM-S, D_{sa} is calculated using Formula (19) and Formula (20).

$$D_{sa} = D_{lt} + T_{spc} \tag{19}$$

$$D_{sa} = I_{ar} - I_{mt} \tag{20}$$

where

D_{ma} is the SFSPM-M allowable delay;

D_{ms} is the SFSPM-S allowable delay;

D_{lt} is the link transmission delay;

T_{mpc} is the SFSPM-M processing cycle time;

T_{spc} is the SFSPM-S processing cycle time;

I_{ar} is the allowable refresh interval;

I_{mt} is the SFSPM-M transmission interval;

I_{st} is the SFSPM-S transmission interval.

Figure 43 illustrates the concept of determining the allowable_delay for transmission from SFSPM-M to SFSPM-S, and for transmission from SFSPM-S to SFSPM-M.

The period from the moment that SFSPM-M sends a safety PDU at TS1, to the moment that SFSPM-S receives the safety PDU at TS2, is the sum of the FSCP 8/2 network transmission delay and the operation cycle time of SFSPM-S on the reception side. Conversely, the period from the moment that SFSPM-S sends a safety PDU at TS3, to the moment that SFSPM-M receives the safety PDU at TS4, is the sum of the transmission delay and the operation cycle time of SFSPM-M on the reception side.

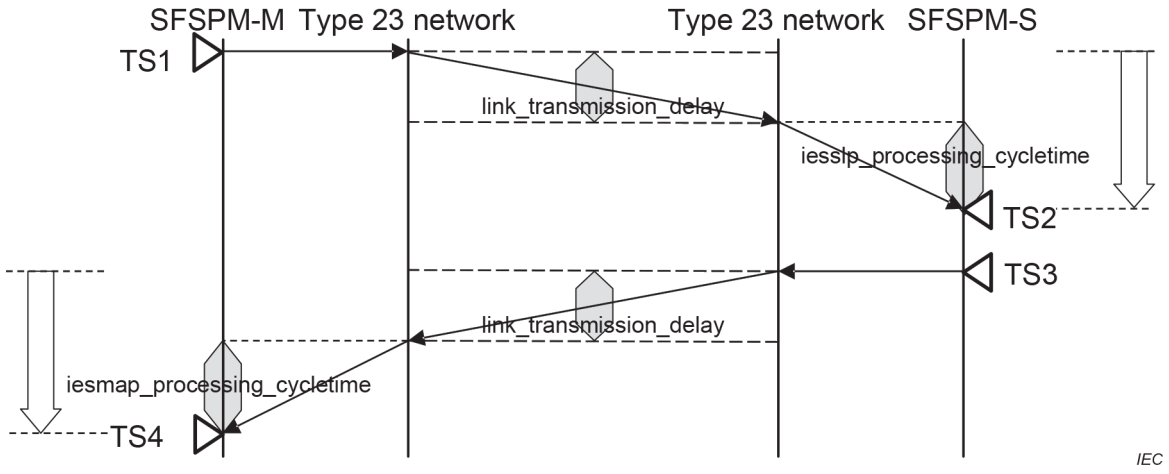


Figure 43 – Calculation of allowable_delay

12.8.1.6 allowable_roundtrip_delay

allowable_roundtrip_delay is a parameter that SFSPM-M uses in operations other than safety refresh. The unit is 128 µs, and is equivalent to three times the allowable_refresh_interval. SFSPM-S uses a value determined in advance until it is notified of the allowable_refresh_interval by SFSPM-M.

12.8.2 Parameter Setup

The parameters shown in Table 41 are set up in the safety communication layer using the services described in 12.6.

12.8.3 Management Services

12.8.3.1 SM-SetSafetyStationInfo

SM-SetSafetyStationInfo is a service used to set up safety station information. Table 42 shows the parameters of SM-SetSafetyStationInfo.

Table 42 – SM-SetSafetyStationInfo

Parameter Name	Req	Ind	Rsp	Cnf
Argument	M	M(=)		
Parameter	M	M(=)		
Result			U	U(=)
R Data			U	U(=)

Parameter
Specifies the set parameters of safety station information. See Table 43.

R Data
Contains the result of parameter setup. The value is any value.

Table 43 – Safety station information setting parameters of SM-SetSafetyStationInfo

No	Item	Size (Octets)	Range	Remarks
1	Network number	1	0 – 255	0 and 240-255: Reserved
2	Station number	1	0 – 255	121-255: Reserved
3	Safety station type	2	0x0000 – 0xFFFF	0x0: Safety PLC 0x1-0x3: Reserved 0x4: Safety remote device 0x5: Safety remote I/O 0x6-0xFFFF: Reserved
4	Vendor code	2	0x0000 – 0xFFFF	Code assigned to each vendor
5	Vendor model code	4	0x00000000 – 0xFFFFFFFF	Unique code assigned to each product model managed by vendor
6	Operation specification version	2	0x0000 – 0xFFFF	Version of operation specifications of product managed by vendor
7	Safety protocol version	2	0x00 – 0xFF	This version: 00

12.8.3.2 SM-SetSafetyNetworkParameter

SM-SetSafetyNetworkParameter is a service used to set up safety network parameters. Table 44 shows the parameters of SM-SetSafetyNetworkParameter.

Table 44 – SM-SetSafetyNetworkParameter

Parameter Name	Req	Ind	Rsp	Cnf
Argument	M	M(=)		
Parameter	M	M(=)		
Result			U	U(=)
R Data			U	U(=)

Parameter
Specifies the safety network parameters. See Table 45.

R Data
Contains the result of parameter setup. The value is any value.

Table 45 – Safety network parameters of SM-SetSafetyNetworkParameter

No	Item	Size (Octets)	Range	Remarks
1	Network number	1	0 – 255	0 and 240-255: Reserved
2	Station number	1	0 – 255	121-255: Reserved
3	Safety connection identifier	4	0x00000000 – 0xFFFFFFFF	
4	Safety connection end type	1	0x0 – 0x1	0x0:SFSPM-M 0x1:SFSPM-S
5	Maximum transmission interval	2	2 – 65535	
6	Allowable refresh interval	2	1 – 65535	
7	Safety data size	1	0-16	Unit: Octets

12.8.3.3 SM-GetSafetyStationInfo

SM-GetSafetyStationInfo is a service used to read safety station information. Table 46 shows the parameters of SM-GetSafetyStationInfo.

Table 46 – SM-GetSafetyStationInfo

Parameter Name	Req	Ind	Rsp	Cnf
Argument	M	M(=)		
Parameter	M	M(=)		
Result			M	M(=)
R Data			M	M(=)

Parameter
Specifies the acquisition destination. See Table 47.

R Data
Contains the acquisition result. See Table 48.

Table 47 – Safety station information parameters of SM-GetSafetyStationInfo (Request)

No	Item	Size (Octets)	Range	Remarks
1	Network number	1	0 – 255	0 and 240-255: Reserved
2	Station number	1	0 – 255	121-255: Reserved

Table 48 – Safety station information parameters of SM-GetSafetyStationInfo (Response)

No	Item	Size (Octets)	Range	Remarks
1	Safety station type	2	0x0000 – 0xFFFF	0x0: Safety PLC 0x1-0x3: Reserved 0x4: Safety remote device 0x5: Safety remote I/O 0x6-0xFFFF: Reserved
2	Vendor code	2	0x0000 – 0xFFFF	Code assigned to each vendor to indicate the vendor.
3	Vendor model code	4	0x00000000 – 0xFFFFFFFF	Unique code assigned to each product model managed by vendors.
4	Operation specification version	2	0x0000 – 0xFFFF	Version of operation specifications of product managed by vendor.
5	Safety protocol version	2	0x00 – 0xFF	This version: 00

12.8.3.4 SM-GetSafetyNetworkParameter

SM-GetSafetyNetworkParameter is a service used to read safety network parameters. Table 49 shows the parameters of SM-GetSafetyNetworkParameter.

Table 49 – SM-GetSafetyNetworkParameter

Parameter Name	Req	Ind	Rsp	Cnf
Argument	M	M(=)		
Parameter	M	M(=)		
Result			M	M(=)
R Data			M	M(=)

Parameter
Specifies the acquisition destination. See Table 50.

R Data
Contains the acquisition result. See Table 51.

Table 50 – Parameters of SM-GetSafetyNetworkParameter request

No	Item	Size (Octets)	Range	Remarks
1	Network number	1	0 – 255	0 and 240-255: Reserved
2	Station number	1	0 – 255	121-255: Reserved
3	Safety connection identifier	4	0x00000000 – 0xFFFFFFFF	

Table 51 – Parameters of SM-GetSafetyNetworkParameter response

No	Item	Size (Octets)	Range	Remarks
1	Safety connection end type	1	0x0 – 0x1	0x0:SFSPM-M 0x1:SFSPM-S
2	Maximum transmission interval	2	1 – 65535	
3	Allowable refresh interval	2	1 – 65535	
4	Safety data size	1	0 – 16	Unit: Octets

12.9 System requirements for FSCP 8/2

12.9.1 Indicators and switches

12.9.1.1 Switches

No switches are specified for FSCP 8/2.

12.9.1.2 Indicators

Indicator requirements are specified in Table 20, Table 52 and Table 53 with the following interpretation:

M = mandatory

O = optional

R = recommended

Indicator type, color and shape are not specified. Also, where computers or other devices with screens are used, indication may be supported via indication on the screen. For communication port monitoring, provision of displays that enable identification of the number of each communication port on both the safety master station and the safety slave station is recommended.

Table 52 – Monitor LEDs

No.	LED Name	Description	Safety master station	Safety slave local station	Safety slave intelligent device station	Safety slave remote device station	Safety slave remote I/O station
1	PW	Lit: Power is on Out: Power is off	R	R	R	R	R
2	RUN	Lit: Operation is normal Out: Error has occurred at station	M	R	R	O	O
3	ERR	Lit: Error Safety master: ▪ Station number conflict ▪ Inconsistency in sampled network information ▪ Error occurred at station Safety slave: ▪ Error occurred at station Flashing: Data link error Safety master: ▪ A station exists with a data link error Out: Operation is normal	M	R	R	O	O
4	MST	Lit: Station is operating as the master station Out: Station is not operating as the master station	O	—	—	—	—
5	D LINK	Lit: Cyclic transmission is being performed Out: Disconnection	M	R	R	O	O
6	L.ERR	Lit: Received data error Out: Received data are normal	M	R	R	R	R
7	SD	Lit: Data are being transmitted Out: Data are not being transmitted	R	R	R	R	R
8	RD	Lit: Data are being received Out: Data are not being received	R	R	R	R	R

Table 53 – Communication port monitor LEDs

No.	LED Name	Description	Safety master station	Safety slave local station	Safety slave intelligent device station	Safety slave remote device station	Safety slave remote I/O station
1	LINK	Lit: Link is operational Out: Link is not operational	O	O	O	O	O
2	L.ER	Lit: Received data error Out: Received data are normal	O	O	O	O	O

12.9.2 Installation guidelines

This document specifies protocol and services for a safety communication system based on IEC 61158 Type 23. However, usage of safety devices with the safety protocol specified in this document requires proper installation. All devices connected to a safety communication system defined in this document shall follow the recommendations and comply with the specifications given in IEC 61784-5-8.

12.9.3 Safety function response time

Figure 44 illustrates the concept of the response time during safety communication between FSCP 8/2 safety stations. Calculations are explained between two safety PLCs as an example.

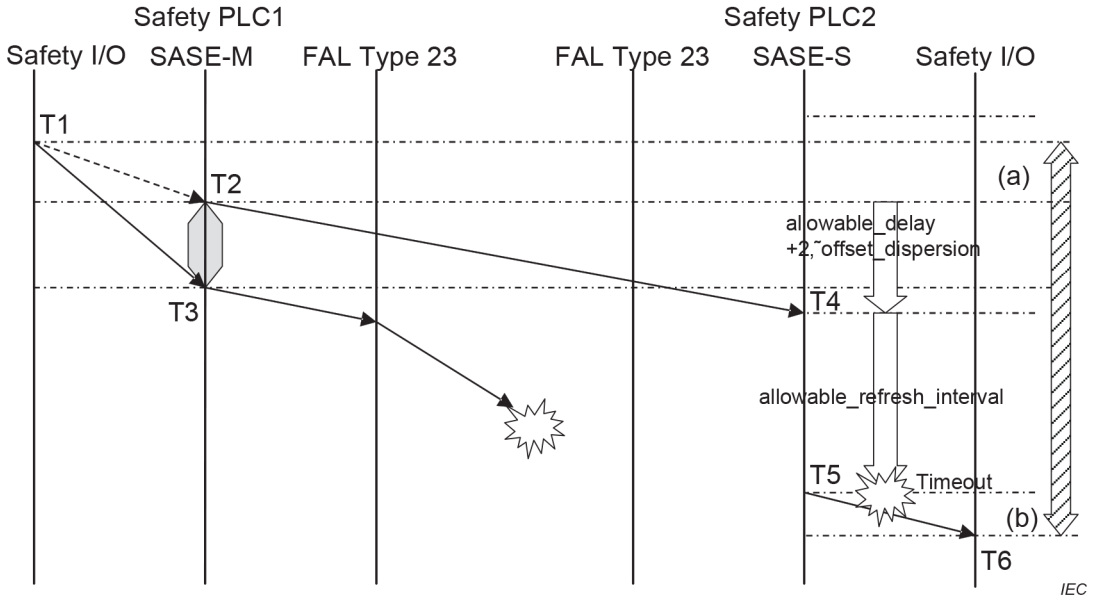


Figure 44 – Calculation of response time between safety PLCs

The response time of safety communication from safety PLC1 to safety PLC2 in Figure 44 is the period from T1 to T6. The period from T1 to T2 is the input device response time. When transmission is performed immediately before T2, transmission is performed at the next transmission interval, resulting in a wait time equal to the transmission_interval (SASE-M and SFSPM-M).

The worst case value is a case where the safety PDU sent at T3 is lost. At T5, it is determined that the safety PDU sent at T3 has not arrived within the specified time. The period from T5 to T6 is the output device response time. At this time, the worst case response time, *TR* is calculated using Formula (21), Formula (22) and Formula (23).

$$TR = a + D_a + (2 \times O_d) + I_{ar} + b \tag{21}$$

$$TR = a + D_{lt} + T_{mpc} + (2 \times D_{lt}) + I_t + D_{lt} + T_{spc} + b \tag{22}$$

$$TR = a + b + T_{mpc} + (4 \times D_{lt}) + (2 \times T_{spc}) \tag{23}$$

where

TR	is the response time;
a	is the input device response time;
D_a	is the allowable delay;
O_d	is the offset dispersion;
I_{ar}	is the allowable refresh interval;
b	is the output device response time;
D_{lt}	is the FSCP 8/2 network link transmission delay;
T_{spc}	is the SASE-S processing cycle time;
T_{mpc}	is the SASE-M processing cycle time;
I_t	is the transmission interval (SFSPM-M).

NOTE Details of the addition of 2 × offset dispersion are provided in Annex A.

12.9.4 Duration of demands

The duration of demand by the safety-related application to the safety communication layer shall be sufficient in duration such that demand is detected within the longest safety function response time by the application.

12.9.5 Constraints for calculation of system characteristics

FSCP 8/2 is an SIL 3 functional safety communication protocol, as such the residual error rate per hour of the SCL (λ_{SCL}) < 10^{-9}.

The only restriction on IEC 61158 Type 23 when implementing an FSCP 8/2 safety system is the maximum number of message storage elements (N_{SE}) such as switches and routers. This is constrained by a relationship to the maximum number logical connections permitted in a single safety function (m) and the transmission interval (I_t).

An FSCP 8/2 safety system shall comply with a constraint on N_{SE}, as a function of m and I_t as given by Formula (24).

$$N_{SE}\,(I_T, m) < \frac{3{,}602 \times 10^7}{I_t \times m} - \frac{3{,}515 \times 10^3}{{I_t}^2} \tag{24}$$

where

N_{SE}	is the number of storage elements in black channel such as switches and routers;
I_t	is the transmission interval (ms) range is 1 to 2,000;
m	is the maximum number of logical connections that is permitted in a single safety function.

Figure 45 shows the relationship between N_{SE} and m for various values of I_t (see chart colour key) using Formula (24).

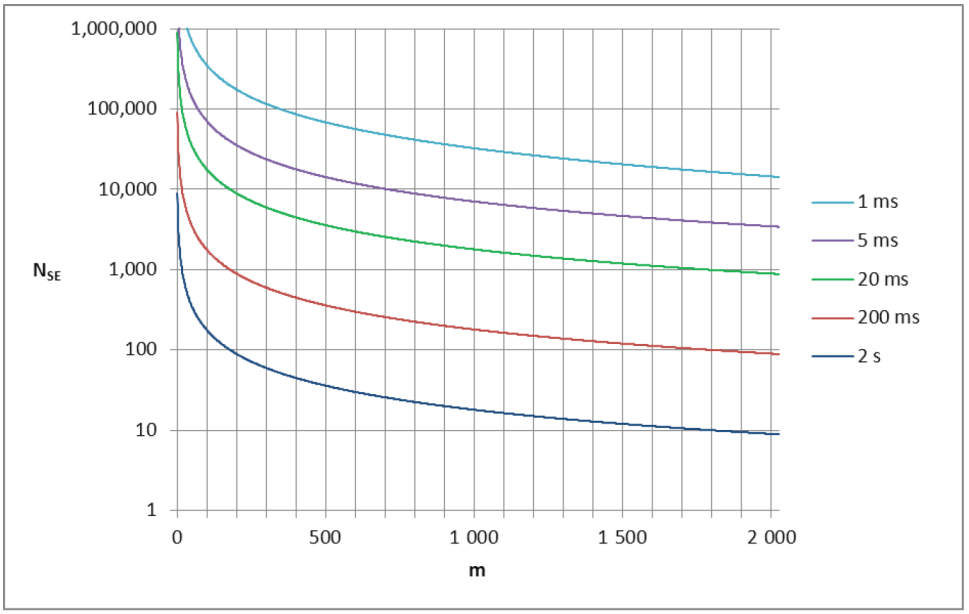


Figure 45 – Constraints on N_{SE} and m

It can be seen in Figure 45 that for practical limits of m < 100 and N_{SE} < 100 there are no concerns regarding transmission interval when implementing FSCP 8/2. However, for very complex safety functions (m > 500) or vast black channel installations (N_{SE} > 500), the constraints on safety networks using slow safety transmission interval become a concern and Formula (24) shall be used to calculate these limits.

12.9.6 Maintenance

There are no SCL specific requirements for maintenance for FSCP 8/2.

Specifications for system behavior in case of device repair and replacement are outside the scope of this document. 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 shall be considered. It is recommended to contact the device or system supplier also.

For information on programming the SRP and setting the parameters of safety devices, it is strongly recommended to contact the device or system supplier. Additionally, it is recommended to take into account CC-Link Safety Specifications. These documents contain additional information for the user of a FSCP 8/2 system.

NOTE 3 Documents [30] and [31] contain important information related to maintenance.

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

12.9.7 Safety manual

The supplier of safety slaves that incorporate the SCL according to FSCP 8/2 shall prepare an appropriate safety manual according to IEC 61508. This safety manual shall also include the installation requirements as specified in 11.9.2 as well as guidelines for the configuration of device switches where used.

A complete safety communication system based on IEC 61158 Type 23 shall consider the CC-Link Safety Specifications.

NOTE 1 Documents [30] and [31] contain important information related to safety manual.

NOTE 2 Before starting the implementation of a safety device it is good engineering practice to contact the CLPA to determine if there are amendments to implementation guidelines and/or implementation requirements.

12.10 Assessment for FSCP 8/2

It is the manufacturer's responsibility to develop the device 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). Additional information is provided in Annex B.

Annex A
(informative)

Additional information for functional safety communication profiles of CPF 8

A.1 Hash function calculation for FSCP 8/1

The CRC32 for FSCP 8/1 is calculated using the following algorithm:

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

This is the algorithm defined as 0x104C11DB7 given by ISO/IEC/IEEE 8802-3.

Code length is 96 bits.

The plot of residual error probability as a function of bit error rate (BER) demonstrates proper behavior. Representative values are shown in Table A.1.

Table A.1 – Residual error probability for FSCP 8/1 CRC

n (bits)	BER = 2/n	BER = 4/n	BER = 0,01	BER = 0,001	BER = 0,0001
96	8.5046432E-14	6.0272142E-12	4.3703467E-16	6.7137731E-24	6.9713053E-32

A.2 Hash function calculation for FSCP 8/2

The CRC32 for FSCP 8/2 is calculated using the following algorithm:

$$G(x) = x^{32} + x^{31} + x^{30} + x^{29} + x^{28} + x^{24} + x^{23} + x^{20} + x^{17} + x^{13} + x^{11} + x^4 + x^2 + 1$$

This is the algorithm defined as 0x1F1922815 given in [32].

Code length ranges from 224 to 992 bits in 32-bit increments.

The plots of residual error probability as a function of bit error rate (BER) demonstrates proper behavior. Representative values are shown in Table A.2.

Table A.2 – Residual error probability for FSCP 8/2 CRC

n (bits)	BER = 2/n	BER = 4/n	BER = 0,01	BER = 0,001	BER = 0,0001
224	4.0322236E-13	1.6638772E-11	7.9879086E-13	5.3605698E-20	6.5083171E-28
256	4.0958621E-13	1.6802011E-11	1.7536098E-12	1.5470990E-19	1.9329636E-27
288	4.1226780E-13	1.6845400E-11	3.3658478E-12	3.8931551E-19	5.0054622E-27
320	4.1234883E-13	1.6806216E-11	5.8216501E-12	8.8020027E-19	1.1645257E-26
352	4.1362666E-13	1.6817799E-11	9.3328421E-12	1.8403714E-18	2.5054735E-26
384	4.1494272E-13	1.6836188E-11	1.4028534E-11	3.5989796E-18	5.0416342E-26
416	4.1583997E-13	1.6843934E-11	1.9967756E-11	6.6464215E-18	9.5802640E-26
448	4.1662508E-13	1.6851175E-11	2.7160147E-11	1.1697734E-17	1.7349197E-25
480	4.1738988E-13	1.6860416E-11	3.5547838E-11	1.9756122E-17	3.0147964E-25
512	4.1818700E-13	1.6873006E-11	4.5015881E-11	3.2193220E-17	5.0546386E-25
544	4.1892070E-13	1.6885164E-11	5.5390975E-11	5.0825605E-17	8.2104736E-25
576	4.1948634E-13	1.6892887E-11	6.6460435E-11	7.8003437E-17	1.2964312E-24
608	4.1998645E-13	1.6899575E-11	7.8014686E-11	1.1675705E-16	1.9964542E-24
640	4.2043580E-13	1.6905565E-11	8.9834198E-11	1.7089060E-16	3.0062514E-24
672	4.2083214E-13	1.6910621E-11	1.0170590E-10	2.4511218E-16	4.4360174E-24
704	4.2120519E-13	1.6915658E-11	1.1343936E-10	3.4519998E-16	6.4270369E-24
736	4.2154801E-13	1.6920328E-11	1.2486316E-10	4.7811770E-16	9.1575007E-24
768	4.2186554E-13	1.6924719E-11	1.3583561E-10	6.5219642E-16	1.2850293E-23
800	4.2217609E-13	1.6929400E-11	1.4624685E-10	8.7732699E-16	1.7781940E-23
832	4.2247640E-13	1.6934195E-11	1.5601264E-10	1.1650838E-15	2.4291166E-23
864	4.2275033E-13	1.6938486E-11	1.6507409E-10	1.5288711E-15	3.2788831E-23
896	4.2300762E-13	1.6942569E-11	1.7340149E-10	1.9842178E-15	4.3772232E-23
928	4.2324940E-13	1.6946446E-11	1.8098527E-10	2.5488862E-15	5.7836829E-23
960	4.2347661E-13	1.6950117E-11	1.8783384E-10	3.2430792E-15	7.5691417E-23
992	4.2369108E-13	1.6953615E-11	1.9397014E-10	4.0896408E-15	9.8174726E-23

A.3 Meaning of response time calculation formula for FSCP 8/2

The period from the time T2 of SFSPM-M transmission to the time T4 of SFSPM-S reception in Figure 44 is the maximum allowable delay. In the response time calculation formula, the period from T2 to T4 is the allowable_delay + 2 × offset_dispersion. Figure A.1 illustrates the meaning of the addition of 2 × offset_dispersion.

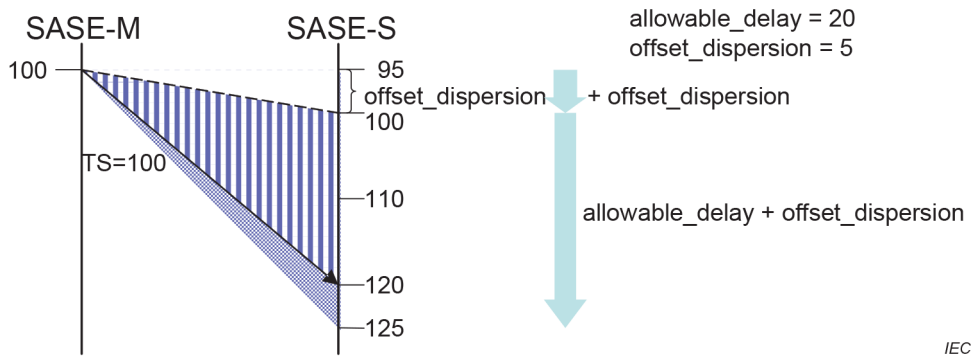


Figure A.1 – Allowable_delay and offset calculation deviation

Due to the possibility that the calculation deviation offset_dispersion will occur in the offset calculation, a formula that takes into consideration the calculation deviation offset_dispersion in the allowable delay allowable_delay is used in determining the allowable delay described in 12.7.2. Furthermore, a maximum difference of offset_dispersion occurs between the SFSPM-M and SFSPM-S safety clocks. As a result, the addition of 2 × offset_dispersion (the combined value) is required.

Annex B
(informative)

Information for assessment of the functional safety communication profiles of CPF 8

According to IEC rules, this document does not make a statement on how to validate conformance. However, test and validation of compliance of FSCP 8/1 and FSCP 8/2 devices with IEC 61784-3-8 may be required by law.

Corresponding information relative to the test and compliance with this document can be retrieved from the local National Committees of the IEC or from the relevant fieldbus organization.

NOTE For IEC 61784-3-8, the relevant fieldbus organization is CC-Link Partner Association, see www.cc-link.org.

Bibliography

[1] IEC 60050 (all parts), *International Electrotechnical Vocabulary (IEV)* (available at <http://www.electropedia.org/)

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

[2] IEC 60050-191:1990 [5] , *International Electrotechnical Vocabulary – Chapter 191: Dependability and quality of service*

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

[4] IEC 61000-6-7, *Electromagnetic compatibility (EMC) – Part 6-7: Generic standards – Immunity requirements for equipment intended to perform functions in a safety-related system (functional safety) in industrial locations*

[5] IEC 61010-2-201, *Safety requirements for electrical equipment for measurement, control and laboratory use – Part 2-201: Particular requirements for control equipment*

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

[7] IEC 61158-1, *Industrial communication networks – Fieldbus specifications – Part 1: Overview and guidance for the IEC 61158 and IEC 61784 series*

[8] IEC 61158-5 (all parts), *Industrial communication networks – Fieldbus specifications – Part 5: Application layer service definition*

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

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

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

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

[13] IEC 61784-3 (all parts), *Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses*

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

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

[16] IEC 61918:2018, *Industrial communication networks – Installation of communication networks in industrial premises*

---

5 Withdrawn.

[17] IEC 62280:2014, *Railway applications – Communication, signalling and processing systems – Safety related communication in transmission systems*

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

[19] ISO/IEC Guide 51:2014, *Safety aspects – Guidelines for their inclusion in standards*

[20] ISO/IEC 2382:2015, *Information technology – Vocabulary*

[21] ISO/IEC 7498-1, *Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model*

[22] ISO 10218-1, *Robots and robotic devices – Safety requirements for industrial robots – Part 1: Robots*

[23] ISO 13849 (all parts), *Safety of machinery – Safety-related parts of control systems*

[24] ISO 13849-1:2015, *Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design*

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

[26] ANDREW S. TANENBAUM, DAVID J. WETHERALL, *Computer Networks*, 5th Edition, Prentice Hall, N.J., ISBN-10: 0132126958, ISBN-13: 978-0132126953

[27] W. WESLEY PETERSON, EDWARD J. WELDON, *Error-Correcting Codes*, 2nd Edition 1972, MIT-Press, ISBN 0-262-16-039-0

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

[29] 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

[30] CC-Link Safety Specifications, *Overview/Protocol, BAP-C1603-001, CLPA*

[31] CC-Link Safety Specifications, *Implementation, BAP-C1603-002, CLPA*

[32] CC-Link Safety Specifications, *Profiles, BAP-C1603-003, CLPA*

[33] CC-Link IE Safety Specifications, *Overview, BAP-C1606-001, CLPA*

[34] CC-Link IE Safety Specifications, *Application Layer Service and Protocol Communication profile, BAP-C1606-002, CLPA*

_____

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

RÉSEAUX DE COMMUNICATION INDUSTRIELS – PROFILS –

Partie 3-8: Bus de terrain de sécurité fonctionnelle – Spécifications supplémentaires pour CPF 8

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC 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, l'IEC – 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 l'IEC"). 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 l'IEC, participent également aux travaux. L'IEC 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 l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC 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 l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) L'IEC 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 l'IEC. L'IEC 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 l'IEC, 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 l'IEC, 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 l'IEC ou de toute autre Publication de l'IEC, 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.
9) L'attention est attirée sur le fait que certains des éléments du présent document de l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets.

L'IEC 61784-3-8 a été établie par le sous-comité 65C: Réseaux industriels, du comité d'études 65 de l'IEC: Mesure, commande et automation dans les processus industriels. Il s'agit d'une Norme internationale.

Cette troisième édition annule et remplace la deuxième édition parue en 2016. Cette édition constitue une révision technique.

Cette édition inclut les modifications techniques majeures suivantes par rapport à l'édition précédente:

- structuration à des fins de conformité à l'IEC 61784-3 Ed.4;
- modifications et clarifications rédactionnelles d'ordre général;

- mesures de sécurité (11.5.3);
- élément de service d'application de sécurité (11.6.2);
- format PDU de sécurité (11.7.1);
- contraintes liées au calcul des caractéristiques du système (11.9.5);
- mesures de sécurité (12.5.3);
- format PDU de sécurité (12.7.1);
- comportement (12.7.2);
- contraintes liées au calcul des caractéristiques du système (12.9.5);
- calcul de la fonction de hachage (Annexe A).

Le texte de cette Norme internationale est issu des documents suivants:

FDIS	Rapport de vote
65C/1083/FDIS	65C/1087/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à son approbation.

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

La langue employée pour l'élaboration de cette Norme internationale est l'anglais.

Le présent document a été rédigé selon les Directives ISO/IEC, Partie 2, il a été développé selon les Directives ISO/IEC, Partie 1 et les Directives ISO/IEC, Supplément IEC, disponibles sous www.iec.ch/members_experts/refdocs. Les principaux types de documents développés par l'IEC sont décrits plus en détail sous www.iec.ch/standardsdev/publications.

Une liste de toutes les parties de la série IEC 61784-3, publiées sous le titre général *Réseaux de communication industriels – Profils – Bus de terrain de sécurité fonctionnelle*, se trouve sur le site web de l'IEC.

Le comité a décidé que le contenu du présent document ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous webstore.iec.ch dans les données relatives au document recherché. A cette date, le document sera

- reconduit,
- supprimé,
- remplacé par une édition révisée, ou
- amendé.

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.

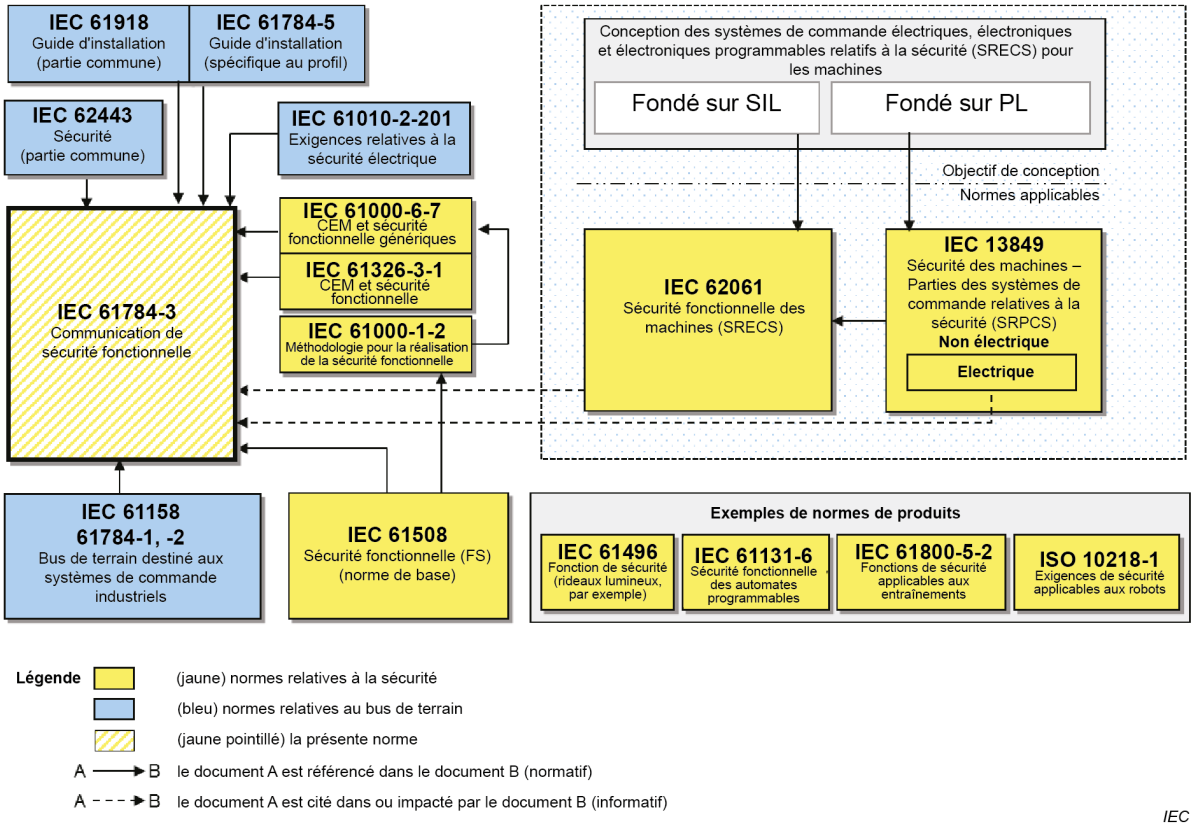
0 Introduction

0.1 Généralités

L'IEC 61158 (toutes les parties), relative aux bus de terrain, ainsi que ses normes associées IEC 61784-1 et IEC 61784-2, définissent 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. Les améliorations des bus de terrain se poursuivent; elles couvrent des applications pour des domaines comme les applications en temps réel relatives à la sécurité.

La série IEC 61784-3 (toutes les parties) explique les principes pertinents pour les communications de sécurité fonctionnelle en référence à l'IEC 61508 (toutes les parties) et spécifie plusieurs couches de communication de sécurité (profils et protocoles correspondants) qui reposent sur les profils de communication et les couches de protocole de l'IEC 61784-1, l'IEC 61784-2 et l'IEC 61158 (toutes les parties). Elle ne couvre pas les aspects relatifs à la sécurité électrique et à la sécurité intrinsèque. Elle ne couvre pas non plus les aspects relatifs à la sûreté et ne prévoit aucune exigence en matière de sûreté.

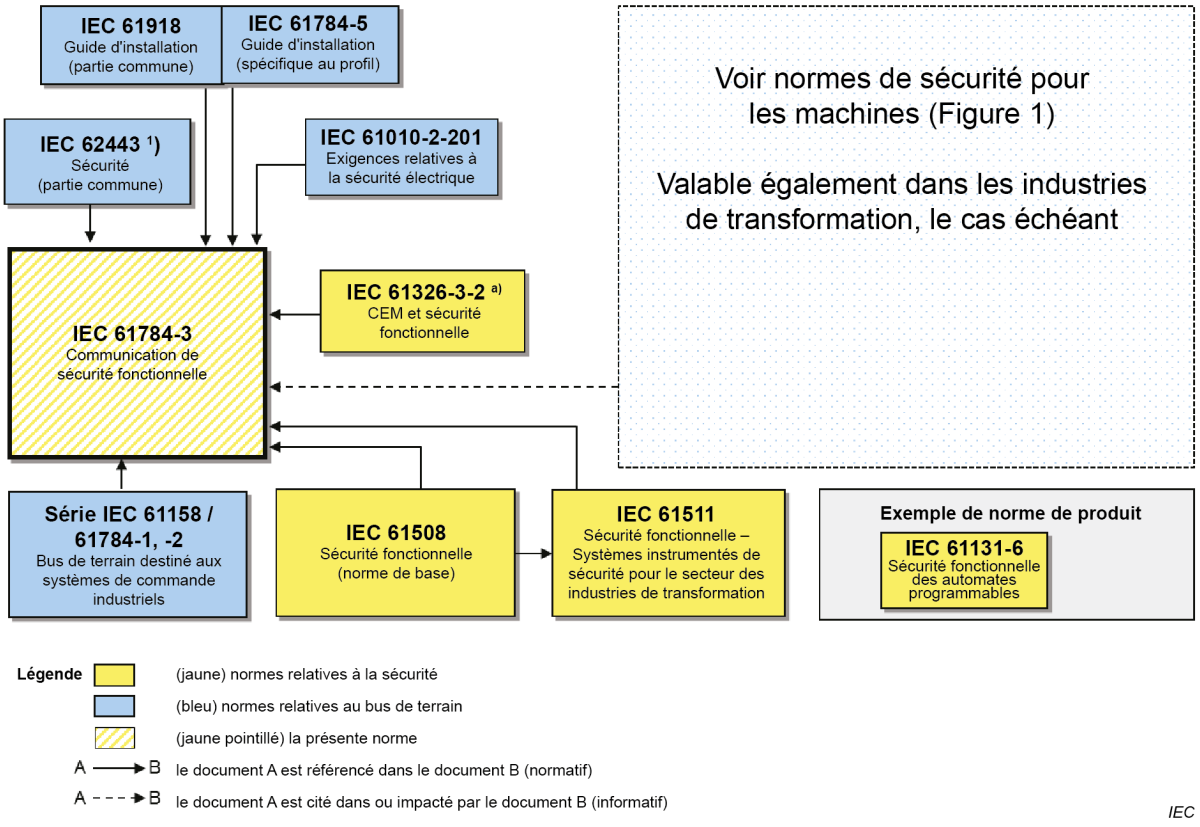
La Figure 1 représente les relations entre l'IEC 61784-3 (toutes les parties) et les normes pertinentes relatives à la sécurité et aux bus de terrain dans un environnement de machines.



NOTE L'IEC 62061 spécifie la relation entre PL (Catégorie) et SIL.

Figure 1 – Relations entre l'IEC 61784-3 et d'autres normes (machines)

La Figure 2 représente les relations entre l'IEC 61784-3 (toutes les parties) et les normes pertinentes relatives à la sécurité et aux bus de terrain dans un environnement de processus.



[a] Pour les environnements électromagnétiques spécifiés; sinon, l'IEC 61326-3-1 ou l'IEC 61000-6-7 s'applique.

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

Les couches de communication de sécurité mises en œuvre dans le cadre de systèmes relatifs à la sécurité conformément à l'IEC 61508 (toutes les parties) assurent la confiance nécessaire à accorder à la transmission de messages (informations) entre plusieurs participants 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 l'IEC 61784-3 (toutes les parties) permettent de s'assurer qu'un bus de terrain peut être utilisé dans des applications qui nécessitent 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 (FSCP) retenu au sein du système (la mise en œuvre du profil de communication de sécurité fonctionnelle dans un appareil normal ne suffit pas à le qualifier d'appareil de sécurité).

L'IEC 61784-3 (toutes les parties) décrit:

- les principes de base de la mise en œuvre des exigences de l'IEC 61508 (toutes les parties) pour les communications de données relatives à la sécurité, y compris les anomalies de transmission potentielles, les mesures correctives et des considérations relatives à l'intégrité des données;
- les profils de communication de sécurité fonctionnelle pour plusieurs familles de profils de communication dans l'IEC 61784-1 et l'IEC 61784-2, y compris les extensions de la couche de sécurité aux sections relatives au service et aux protocoles de communication de l'IEC 61158 (toutes les parties).

0.2 Déclaration de brevets

La Commission Electrotechnique Internationale (IEC) attire l'attention sur le fait qu'il est déclaré que la conformité avec les dispositions du présent document peut impliquer l'utilisation de brevets intéressant les profils de communication de sécurité fonctionnelle pour la famille 8. L'IEC ne prend pas position quant à la preuve, à la validité et à la portée de ces droits de propriété.

Le détenteur de ces droits de propriété a donné l'assurance à l'IEC qu'il consent à négocier des licences avec des demandeurs du monde entier à des termes et conditions raisonnables et non discriminatoires. A ce propos, la déclaration du détenteur des droits de propriété est enregistrée à l'IEC. Des informations peuvent être obtenues dans la base de données des droits de propriété, disponible à l'adresse suivante: http://patents.iec.ch.

L'attention est d'autre part attirée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété autres que ceux qui ont été enregistrés dans la base de données des droits de propriété. L'IEC ne saurait être tenue pour responsable de l'identification de ces droits de propriété en tout ou partie.

RÉSEAUX DE COMMUNICATION INDUSTRIELS – PROFILS –

Partie 3-8: Bus de terrain de sécurité fonctionnelle – Spécifications supplémentaires pour CPF 8

1 Domaine d'application

La présente partie de l'IEC 61784-3 (toutes les parties) spécifie une couche de communication de sécurité (services et protocole) qui repose sur la CPF 8 de l'IEC 61784-1, de l'IEC 61784-2 et de l'IEC 61158 Type 18 et Type 23. Elle identifie les principes applicables aux communications de sécurité fonctionnelle définies dans l'IEC 61784-3, qui correspondent à cette couche de communication de sécurité. Cette couche de communication de sécurité est destinée à être mise en œuvre uniquement sur les appareils 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.

Le présent document définit les mécanismes de transmission des messages relatifs à la sécurité entre les participants d'un réseau réparti, en utilisant la technologie de bus de terrain conformément aux exigences de la série IEC 61508 (toutes les parties)[1] concernant la sécurité fonctionnelle. Ces mécanismes peuvent être utilisés dans différentes applications industrielles, par exemple la commande de processus, l'usinage automatique et les machines.

Le présent document fournit des lignes directrices aux développeurs, ainsi qu'aux évaluateurs d'appareils et de 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 d'un profil de communication de sécurité fonctionnelle conforme au présent document dans un appareil normal ne suffit pas à le qualifier d'appareil de sécurité).

2 Références normatives

Les documents suivants sont cités dans le texte de sorte qu'ils constituent, pour tout ou partie de leur contenu, des exigences 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).

IEC 61131-2, *Mesurage et contrôle des processus industriels – Automates programmables – Partie 2: Exigences et essais des équipements*

IEC 61158 (toutes les parties), *Réseaux de communication industriels – Spécifications des bus de terrain*

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

IEC 61158-3-18, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 3-18: Définition des services de couche liaison de données – Eléments de type 18*

---

[1] Dans les pages suivantes du présent document, "IEC 61508" remplace "IEC 61508 (toutes les parties)".

IEC 61158-4-18, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 4-18: Spécification du protocole de la couche de liaison de données – Eléments de type 18*

IEC 61158-5-18, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 5-18: Définition des services des couches d'application – Eléments de type 18*

IEC 61158-5-23, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 5-23: Définition des services des couches d'application – Eléments de type 23*

IEC 61158-6-18, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 6-18: Spécification de protocole de la couche application – Eléments de type 18*

IEC 61158-6-23, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 6-23: Spécification de protocole de la couche application – Eléments de type 23*

IEC 61326-3-1, *Matériel électrique de mesure, de commande et de laboratoire – Exigences relatives à la CEM – Partie 3-1: Exigences d'immunité pour les systèmes relatifs à la sécurité et pour les matériels destinés à réaliser des fonctions relatives à la sécurité (sécurité fonctionnelle) – Applications industrielles générales*

IEC 61326-3-2, *Matériel électrique de mesure, de commande et de laboratoire – Exigences relatives à la CEM – Partie 3-2: Exigences d'immunité pour les systèmes relatifs à la sécurité et pour les matériels destinés à réaliser des fonctions relatives à la sécurité (sécurité fonctionnelle) – Applications industrielles dont l'environnement électromagnétique est spécifié*

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

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

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

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

IEC 61784-3:2021, *Réseaux de communication industriels – Profils – Partie 3: Bus de terrain de sécurité fonctionnelle – Règles générales et définitions de profils*

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

ISO/IEC/IEEE 8802-3, *Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 3: Standard for Ethernet* (disponible en anglais seulement)

3 Termes, définitions, symboles, abréviations et conventions

3.1 Termes et définitions

Pour les besoins du présent document, les termes et définitions de l'IEC 61784-3 ainsi que les suivants s'appliquent.

L'ISO et l'IEC tiennent à jour des bases de données terminologiques destinées à être utilisées en normalisation, consultables aux adresses suivantes:

- IEC Electropedia: disponible à l'adresse http://www.electropedia.org/
- ISO Online browsing platform: disponible à l'adresse http://www.iso.org/obp

NOTE L'italique est utilisé dans les définitions pour mettre en évidence les termes définis en 3.1.

3.1.1 Termes et définitions communs

NOTE Ces termes et définitions communs sont issus de l'IEC 61784-3:2021.

3.1.1.1
date absolue
date référencée par rapport à un temps global, commun à un groupe d'appareils utilisant un *bus de terrain*

[SOURCE: IEC 62280:2014, 3.1.1, modifié – utilisation d'"appareils" et de "bus de terrain" à la place d'"entité" et de "réseau de transmission"]

3.1.1.2
élément de réseau actif
élément de réseau contenant des composants actifs du point de vue électrique et/ou optique et permettant d'étendre le réseau

Note 1 à l'article: Les répéteurs et les commutateurs sont des exemples d'éléments de réseau actif.

[SOURCE: IEC 61918:2018, 3.1.2]

3.1.1.3
probabilité d'erreurs sur les éléments binaires
Pe
probabilité de réception d'un bit donné avec la valeur incorrecte

3.1.1.4
canal noir
système de communication défini qui contient un ou plusieurs éléments sans preuve de conception ou de validation conformément à l'IEC 61508

Note 1 à l'article: Cette définition étend la signification habituelle du canal pour inclure le système qui contient le canal.

3.1.1.5
pont
appareil abstrait qui relie plusieurs segments de réseau le long de la couche de liaison de données

3.1.1.6
système de communication fermé
nombre fixe ou nombre maximal fixe d'éléments reliés par un *système de communication* dont les propriétés sont connues et fixées et où le *risque* d'accès non autorisé est interprété comme négligeable

[SOURCE: IEC 62280:2014, 3.1.6, modifié – "transmission" remplacé par "communication"]

3.1.1.7
canal de communication
connexion logique entre deux points limites d'un *système de communication*

3.1.1.8
système de communication
ensemble de matériels, de logiciels et de supports de propagation qui permet la transmission de *messages* (ISO/IEC 7498-1, couche d'application) d'une application à une autre

3.1.1.9
connexion
liaison logique entre deux objets d'application au sein du même appareil ou d'appareils différents

3.1.1.10
contrôle de redondance cyclique
CRC
<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 à l'article: Les termes "code CRC" et "signature CRC", ainsi que les étiquettes comme CRC1, CRC2, peuvent également être utilisés dans le présent document pour se référer aux données redondantes.

Note 2 à l'article: Voir également [26], [27][2].

3.1.1.11
système de communication défini
canal défini
nombre fixe ou nombre maximal fixe d'éléments reliés par un *système de communication* à *bus de terrain*, dont les propriétés sont connues et fixées, par exemple les conditions d'installation, l'immunité électromagnétique, les *éléments (actifs) de réseau* industriel, et où le *risque* d'accès non autorisé est réduit à un niveau toléré conformément au modèle de cycle de vie de l'IEC 62443 (toutes les parties), en utilisant par exemple des zones et des conduits

3.1.1.12
diversité
moyens différents pour réaliser une fonction requise

Note 1 à l'article: La diversité peut être réalisée en utilisant des méthodes physiques ou des approches conceptuelles différentes.

[SOURCE: IEC 61508-4:2010, 3.3.7]

3.1.1.13
DLPDU
DÉCONSEILLÉ: trame
unité de données de protocole de liaison de données

Note 1 à l'article: L'abréviation "DLPDU" est dérivée du terme anglais développé correspondant "Data Link Protocol Data Unit".

[2] Les chiffres entre crochets renvoient à la bibliographie.

3.1.1.14
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

Note 1 à l'article: Les erreurs peuvent être causées par des erreurs de conception du matériel/logiciel et/ou des informations altérées du fait d'un brouillage électromagnétique et/ou autres effets.

Note 2 à l'article: Les erreurs ne produisent pas nécessairement une *défaillance* ou une *anomalie*.

[SOURCE: IEC 61508-4:2010, 3.6.11, modifié – notes ajoutées]

3.1.1.15
défaillance
cessation de l'aptitude d'une unité fonctionnelle à accomplir une fonction requise ou à fonctionner comme prévu

Note 1 à l'article: Une défaillance peut être causée par une *erreur* (problème de conception matérielle/logicielle ou rupture de *message*, par exemple).

[SOURCE: IEC 61508-4:2010, 3.6.4, modifié – notes et figures remplacées]

3.1.1.16
anomalie
condition anormale qui peut entraîner une réduction ou la perte de capacité d'une unité fonctionnelle à accomplir une fonction requise

Note 1 à l'article: L'IEC 60050-191:1990, 191-05-01, définit le terme "fault" (en français "panne") comme un état d'inaptitude à accomplir une fonction requise, en excluant l'inaptitude due à la maintenance préventive, à d'autres actions programmées ou à un manque de ressources extérieures.

[SOURCE: IEC 61508-4:2010, 3.6.1, modifié – référence à la figure supprimée]

3.1.1.17
bus de terrain
système de communication fondé sur le transfert de données en série et utilisé dans des applications d'automatisation industrielle ou de commande de processus

3.1.1.18
système de bus de terrain
système qui utilise un *bus de terrain* avec des appareils reliés

3.1.1.19
séquence de contrôle de trame
FCS
données redondantes issues d'un bloc de données d'une DLPDU (*trame*), qui utilisent une *fonction de hachage* et enregistrées ou transmises avec le bloc de données, afin de déterminer l'altération des données

Note 1 à l'article: Une FCS peut être calculée à l'aide d'un CRC ou d'une autre *fonction de hachage*.

Note 2 à l'article: Voir également [26], [27].

Note 3 à l'article: L'abréviation "FCS" est dérivée du terme anglais développé correspondant "frame check sequence".

3.1.1.20
fonction de hachage
fonction (mathématique) de mapping des valeurs d'un ensemble (éventuellement) très grand de valeurs en une plage de valeurs (habituellement) plus petite

Note 1 à l'article: Les fonctions de hachage peuvent être utilisées pour déterminer l'altération des données.

Note 2 à l'article: Les fonctions de hachage communes incluent la parité, la somme de contrôle ou le CRC.

3.1.1.21
danger
source potentielle de dommage

Note 1 à l'article: Ce terme comprend le danger sur des personnes survenant dans un laps de temps très court (par exemple, feu et explosion), mais aussi le danger à long terme sur la santé d'une personne (par exemple, dégagement d'une substance toxique).

[SOURCE: IEC 61508-4:2010, 3.1.2, et Guide ISO/IEC 51:2014, définition 3.2]

3.1.1.22
maître
entité de communication capable d'initier et de programmer des activités de communication effectuées par d'autres stations qui peuvent être des maîtres ou des *esclaves*

3.1.1.23
message
<théorie de l'information et théorie des communications> suite ordonnée de caractères (généralement des octets) destinée à communiquer des informations

[SOURCE: ISO/IEC 2382:2015, 2123205, modifié – insertion de "(généralement des octets)", suppression des notes et de la source]

3.1.1.24
collecteur de messages
collecteur d'informations
partie d'un *système de communication* où l'on considère que sont reçus les *messages*

[SOURCE: ISO/IEC 2382:2015, 2123207, modifié – notes et source supprimées]

3.1.1.25
source de messages
source d'informations
partie d'un *système de communication* d'où l'on considère que sont issus les *messages*

[SOURCE: ISO/IEC 2382:2015, 2123206, modifié – notes et source supprimées]

3.1.1.26
niveau de performance
PL
niveau discret d'aptitude de parties relatives à la sécurité à réaliser une fonction de sécurité dans des conditions prévisibles

Note 1 à l'article: L'abréviation "PL" est dérivée du terme anglais développé correspondant "performance level".

[SOURCE: ISO 13849-1:2015, 3.1.23]

3.1.1.27
redondance
existence de plusieurs moyens pour accomplir une fonction requise ou pour représenter des informations

[SOURCE: IEC 61508-4:2010, 3.4.6, modifié – exemple et notes supprimés]

3.1.1.28
date relative
date référencée par rapport à l'horloge locale d'une entité

Note 1 à l'article: En général, il n'y a pas de relation avec les horloges des autres entités.

[SOURCE: IEC 62280:2014, 3.1.43, modifié – format ajusté]

3.1.1.29
probabilité d'erreurs résiduelles
RP
probabilité de non-détection d'une *erreur* par les *mesures de sécurité* SCL

Note 1 à l'article: L'abréviation "RP" est dérivée du terme anglais développé correspondant "residual error probability".

3.1.1.30
taux d'erreurs résiduelles
taux statistique de défaut de détection d'*erreurs* par les *mesures de sécurité* SCL

3.1.1.31
risque
combinaison de la probabilité d'un dommage et de sa gravité

Note 1 à l'article: Pour plus d'informations sur ce concept, voir Annexe A de l'IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6, et Guide ISO/IEC 51:2014, définition 3.9, modifiée – note différente]

3.1.1.32
canal de communication de sécurité
canal de communication qui commence au sommet de la SCL de la source et qui se termine au sommet de la SCL du collecteur

Note 1 à l'article: Le canal peut être modélisé sous la forme de deux SCL reliées par un *canal noir*, un *système de communication défini* ou un *canal défini*.

3.1.1.33
couche de communication de sécurité
SCL
couche de communication située au-dessus de la FAL qui comprend toutes les mesures supplémentaires nécessaires qui permettent d'assurer la transmission de données en toute sécurité conformément aux exigences de l'IEC 61508

3.1.1.34
connexion de sécurité
connexion qui utilise le protocole de sécurité pour des transactions de communications

3.1.1.35
données de sécurité
données transmises par un réseau de sécurité qui utilise un protocole de sécurité

Note 1 à l'article: La *couche de communication de sécurité* n'assure pas la sécurité des données proprement dites, mais uniquement la transmission en toute sécurité de ces dernières.

3.1.1.36
appareil de sécurité
appareil conçu conformément à l'IEC 61508 et qui met en œuvre le profil de communication de sécurité fonctionnelle

3.1.1.37
fonction de sécurité
fonction à réaliser par un *système* E/E/PE *relatif à la sécurité* ou par un dispositif externe de réduction de *risque*, prévue pour assurer ou maintenir un état de sécurité de l'EUC par rapport à un événement dangereux spécifique

[SOURCE: IEC 61508-4:2010, 3.5.1, modifié – références et exemples supprimés]

3.1.1.38
temps de réponse de la fonction de sécurité
temps écoulé dans le cas le plus défavorable à la suite de l'activation d'un capteur de sécurité relié à un *bus de terrain*, avant d'atteindre l'état de sécurité correspondant de ses actionneurs de sécurité, du fait d'*erreurs* ou de *défaillances* dans la *fonction de sécurité*

Note 1 à l'article: Ce concept, introduit dans l'IEC 61784-3:2021, 5.2.4, est traité par les profils de communication de sécurité fonctionnelle définis dans le présent document.

3.1.1.39
niveau d'intégrité de sécurité
SIL
niveau discret (parmi quatre possibles) correspondant à une gamme de valeurs d'intégrité de sécurité où le niveau 4 d'intégrité de sécurité possède le plus haut degré d'intégrité et le niveau 1 possède le plus bas

Note 1 à l'article: Les objectifs chiffrés de *défaillance* (voir l'IEC 61508-4:2010, 3.5.17) pour les quatre niveaux d'intégrité de sécurité sont indiqués dans les Tableaux 2 et 3 de l'IEC 61508-1:2010.

Note 2 à l'article: Les niveaux d'intégrité de sécurité sont utilisés pour spécifier les exigences concernant l'intégrité de sécurité des *fonctions de sécurité* à allouer aux *systèmes* E/E/PE *relatifs à la sécurité*.

Note 3 à l'article: Un niveau d'intégrité de sécurité (SIL) ne constitue pas une propriété d'un système, sous-système, élément ou composant. L'interprétation correcte de l'expression "*système relatif à la sécurité* à SILn" (où n est 1, 2, 3 ou 4) signifie que le système est potentiellement capable de prendre en charge les *fonctions de sécurité* avec un niveau d'intégrité de sécurité jusqu'à n.

Note 4 à l'article: L'abréviation "SIL" est dérivée du terme anglais développé correspondant "safety integrity level".

[SOURCE: IEC 61508-4:2010, 3.5.8]

3.1.1.40
mesure de sécurité
mesure qui permet de contrôler les *erreurs* de communication éventuelles, qui est conçue et mise en œuvre conformément aux exigences de l'IEC 61508

Note 1 à l'article: Dans la pratique, plusieurs mesures de sécurité sont combinées pour atteindre le *niveau d'intégrité de sécurité* exigé.

Note 2 à l'article: Les *erreurs* de communication et les mesures de sécurité associées sont décrites dans l'IEC 61784-3:2021, 5.3 et 5.4.

3.1.1.41
PDU de sécurité
SPDU
PDU transféré par le *canal de communication de sécurité*

Note 1 à l'article: Le SPDU peut comporter plusieurs exemplaires des *données de sécurité* qui utilisent des structures de codage et des *fonctions de hachage* différentes, associées à des parties explicites de protections supplémentaires, par exemple une clé, un nombre de séquences ou un mécanisme de *datation*.

Note 2 à l'article: Les SCL redondantes peuvent fournir deux versions différentes du SPDU en vue de son insertion dans des champs séparés de la *trame de bus de terrain*.

Note 3 à l'article: L'abréviation "SPDU" est dérivée du terme anglais développé correspondant "safety PDU".

3.1.1.42
application relative à la sécurité
programmes conçus conformément à l'IEC 61508 pour satisfaire aux exigences SIL de l'application

3.1.1.43
système relatif à la sécurité
système qui exécute les *fonctions de sécurité* conformément à l'IEC 61508

3.1.1.44
esclave
entité de communication capable de recevoir des *messages* et de les envoyer en réponse à une autre entité de communication qui peut être *maître* ou esclave, mais pas d'initier des activités de communication

3.1.1.45
déclenchement parasite
déclenchement provoqué par le système de sécurité sans injonction du processus

3.1.1.46
code d'opportunité
information temporelle incluse dans un *message*

3.1.1.47
répartition uniforme
loi de probabilité où toutes les valeurs d'un ensemble fini sont également susceptibles de se produire

Note 1 à l'article: Pour un champ de longueur de bit i, la probabilité d'occurrence d'une valeur de champ particulier est égale à 2^{-i} étant donné que la somme de toutes les probabilités d'occurrence est égale à 1.

3.1.1.48
canal blanc
système de communication défini dans lequel tous les éléments pertinents du matériel et des logiciels sont conçus, mis en œuvre et validés conformément à l'IEC 61508

Note 1 à l'article: Cette définition étend la signification habituelle du canal pour inclure le système qui contient le canal.

3.1.2 CPF 8: Termes et définitions supplémentaires

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

3.1.2.2
relation d'application de sécurité
SAR
relation d'application entre deux extrémités ou plus de relation d'application relative à la sécurité

3.1.2.3
élément de service d'application de sécurité
SASE
élément de service d'application relative à la sécurité

Note 1 à l'article: L'abréviation "SASE" est dérivée du terme anglais développé correspondant "safety application service element".

3.1.2.4
horloge de sécurité
horloge (compteur) qui permet d'enregistrer l'heure de l'occurrence d'événements tels que la transmission et la réception des messages relatifs à la communication de sécurité

3.1.2.5
temporisateur de contrôle des données de sécurité
temporisateur utilisé par la fonction de temporisation pour la transmission des données de sécurité

3.1.2.6
temporisateur de contrôle de sécurité
temporisateur utilisé par la fonction de temporisation pour la gestion des connexions de sécurité

3.1.2.7
rafraîchissement de sécurité
transmission et réception périodiques des données de sécurité entre le poste maître et le poste esclave

3.1.2.8
créneau
quantum (granularité) du mapping dépendant de la position des champs de données cycliques

3.1.2.9
poste
appareil et sa SAREP correspondante associés à la transmission et à la réception des données de sécurité

Note 1 à l'article: Le numéro de poste est utilisé dans le mapping dépendant de la position des champs de données cycliques (un poste occupe un ou plusieurs créneaux).

3.1.2.10
informations de transmission des protocoles de sécurité
informations qui différencient les messages relatifs à la sécurité

3.2 Symboles et abréviations

3.2.1 Symboles et abréviations communs

Code A	Code d'authentification	
CP	Communication Profile (Profil de communication)	[IEC 61784-1]
CPF	Communication Profile Family (Famille de profils de communication)	[IEC 61784-1]
CRC	Contrôle de redondance cyclique	
DLL	Data Link Layer (Couche de liaison de données)	[ISO/IEC 7498-1]
DLPDU	Data Link Protocol Data Unit (Unité de données de protocole de liaison de données)	
CEM	Compatibilité électromagnétique	
EUC	Equipment Under Control (Equipement commandé)	[IEC 61508-4:2010]
E/E/PE	Electrical/Electronic/Programmable Electronic (Electrique/électronique/électronique programmable)	[IEC 61508-4:2010]
FAL	Fieldbus Application Layer (Couche application de bus de terrain)	[IEC 61158-5 (toutes les parties)]
FS	Functional Safety (Sécurité fonctionnelle)	
FSCP	Functional Safety Communication Profile (Profil de communication de sécurité fonctionnelle)	
FSPM	FAL Service Protocol Machine (Machine de protocole de service FAL)	[IEC 61158-1]
MTBF	Mean Time Between Failures (Durée moyenne de bon fonctionnement)	
MTTF	Mean Time To Failure (Durée moyenne de fonctionnement avant défaillance)	
PDU	Protocol Data Unit (Unité de données de protocole)	[ISO/IEC 7498-1]
Pe	Probabilité d'erreurs sur les éléments binaires	
PhL	Physical Layer (Couche physique)	[ISO/IEC 7498-1]
PL	Performance Level (Niveau de performance)	[ISO 13849-1]
PLC	Programmable Logic Controller (Automate programmable)	
SCL	Safety Communication Layer (Couche de communication de sécurité)	
SIL	Safety Integrity Level (Niveau d'intégrité de sécurité)	[IEC 61508-4:2010]
SPDU	Safety PDU (PDU de sécurité)	
Code T	Timeliness code (Code d'opportunité)	

3.2.2 CPF 8: Symboles et abréviations supplémentaires

AR	Application Relationship (Relation d'application)
ASE	Application Service Element (Elément de service d'application)
CC	Carry Counter (Compteur de transport)
CID	Connection Identifier (Identifiant de connexion)
CMD	Command Data (Données de commande)
LED	Light Emitting Diode (Diode électroluminescente)
LID	Link Identifier (Identifiant de liaison)
OBL	Offset Baseline (Ligne de base décalée)
RNO	Running Number (Numéro d'exécution)
SAR	Safety Application Relationship (Relation d'application de sécurité)
SAREP	Safety Application Relationship Endpoint (Extrémité de relation d'application de sécurité)
SARPM	Safety Application Relationship Protocol State Machine (Diagramme d'états de protocole de relation d'application de sécurité)
SASE	Safety Application Service Element (Elément de service d'application de sécurité)
SFSPM	Safety FSPM (FSPM de sécurité) (suivi d'un -S pour Esclave (Slave) ou -M pour Maître)
SRC	Safety Relevant Controller (Contrôleur de sécurité)
SRP	Safety Relevant Peripheral (Périphérique de sécurité)
TPI	Safety Transmission Packet Information (Informations de paquets de transmission de sécurité)
TPI-T	Informations de paquets de transmission de sécurité fournies par le maître
TPI-R	Informations de paquets de transmission de sécurité fournies par l'esclave
TS	Time Stamp (Datation)

3.3 Conventions

Les conventions utilisées dans le présent document sont définies dans l'IEC 61158 Type 18 et Type 23, l'IEC 61784-1 CPF 8 et l'IEC 61784-2 CPF 8.

Pour aider le lecteur familiarisé avec la numérotation des articles de norme et pour assurer la cohérence et l'alignement sur l'IEC 61784-3, les Articles 4 à 10 renvoient aux Articles 11 à 17 de FSCP 8/1 et aux Articles 18 à 24 de FSCP 8/2.

4 Présentation générale

Pour une présentation générale de PCSF 8/1, voir 11.4. Pour une présentation générale de PCSF 8/2, voir 12.4.

5 Généralités

Pour des informations générales concernant PCSF 8/1, voir 11.5. Pour des informations générales concernant PCSF 8/2, voir 12.5.

6 Services de la couche de communication de sécurité

Pour plus d'informations sur les services de la couche de communication de sécurité relatifs à FSCP 8/1, voir 11.6. Pour plus d'informations sur les services de la couche de communication de sécurité relatifs à FSCP 8/2, voir 12.6.

7 Protocole de couche de communication de sécurité

Pour plus d'informations sur le protocole de couche de communication de sécurité relatif à FSCP 8/1, voir 11.7. Pour plus d'informations sur le protocole de couche de communication de sécurité relatif à FSCP 8/2, voir 12.7.

8 Gestion de la couche de communication de sécurité

Pour plus d'informations sur la gestion de la couche de communication de sécurité relative à FSCP 8/1, voir 11.8. Pour plus d'informations sur la gestion de la couche de communication de sécurité relative à FSCP 8/2, voir 12.8.

9 Exigences système

Pour plus d'informations sur les exigences système concernant FSCP 8/1, voir 11.9. Pour plus d'informations sur les exigences système concernant FSCP 8/2, voir 12.9.

10 Evaluation

Pour plus d'informations sur l'évaluation relative à FSCP 8/1, voir 11.10. Pour plus d'informations sur l'évaluation relative à FSCP 8/2, voir 12.10.

11 FSCP 8/1

11.1 Domaine d'application – FSCP 8/1

Voir Article 1.

11.2 Références normatives – FSCP 8/1

Voir Article 2.

11.3 Termes, définitions, symboles, abréviations et conventions – FSCP 8/1

Voir Article 3.

11.4 Aperçu de FSCP 8/1 (CC-Link Safety™)

La famille de profils de communication 8 (souvent appelée CC-Link™ [3]) définit les profils de communication qui reposent sur l'IEC 61158-2 Type 18, l'IEC 61158-3-18, l'IEC 61158-4-18, l'IEC 61158-5-18 et l'IEC 61158-6-18.

Les profils de base CP 8/1, CP 8/2 et CP 8/3 sont définis dans l'IEC 61784-1. Le profil de communication de sécurité fonctionnelle CPF 8 FSCP 8/1 (CC-Link Safety™ [3]) repose sur les profils de base CPF 8 de l'IEC 61784-1 et sur les spécifications de couche de communication de sécurité définies dans le présent document.

---

[3] CC-Link™ et CC-Link Safety™ sont des appellations commerciales de l'organisme à but non lucratif CC-Link Partner Association. Cette information est donnée à l'intention des utilisateurs du présent document et ne signifie nullement que l'IEC approuve ou recommande le détenteur de la marque ou de l'un de ses produits. La conformité au présent document n'exige pas l'emploi des appellations commerciales CC-Link™ ou CC-Link Safety™. L'emploi des appellations commerciales CC-Link™ ou CC-Link Safety™ exige l'autorisation de CC-Link Partner Association et la conformité aux conditions d'utilisation (essais et validation).

Le FSCP 8/1 est un protocole de communication des données relatives à la sécurité telles que les signaux d'arrêt d'urgence entre les participants d'un réseau réparti, en utilisant la technologie de bus de terrain conformément aux exigences de l'IEC 61508 concernant la sécurité fonctionnelle. Ce protocole est utilisé dans différentes applications telles que la commande de processus, l'usinage automatique et les machines.

Le protocole FSCP 8/1 est conçu de manière à prendre en charge le niveau d'intégrité de sécurité SIL 3 (IEC 61508) qui utilise CPF 8, en spécifiant par ailleurs des mécanismes de mise en œuvre des numéros de séquence, délai, authentification de connexion, message de réaction, assurance d'intégrité des données et différentes mesures de sécurité dédiées à ladite assurance.

Les capacités SCL de FSCP 8/1 sont fournies avec l'introduction d'éléments de service d'application de sécurité (SASE). Ces SASE sont utilisés à la place de leurs ASE correspondants, comme spécifié dans le présent document. Cependant, dans la mesure où ces SASE proviennent directement des classes de parent définies pour la CPF 8, ils spécifient les ajouts exigés par cette dernière en vue de la sécurité fonctionnelle, en appliquant la méthode du canal noir.

11.5 Généralités – FSCP 8/1

11.5.1 Documents externes de spécifications applicables au profil

Les fabricants d'appareils de sécurité FSCP 8/1 sont encouragés à consulter les documents [30], [31] et [32] qui donnent des spécifications supplémentaires relatives à la mise en œuvre de la SCL définie dans le présent document.

11.5.2 Exigences fonctionnelles de sécurité

Le présent document spécifie les services et protocoles d'un système de communication de sécurité fonctionnelle qui repose sur le Type 18 de l'IEC 61158. Les technologies de communication spécifiées dans le présent document doivent être mises en œuvre uniquement dans les appareils conçus conformément aux exigences de l'IEC 61508.

Les exigences suivantes doivent s'appliquer au développement des appareils qui mettent en œuvre les protocoles FSCP 8/1. Les mêmes exigences ont été utilisées dans le développement de FSCP 8/1.

- Les protocoles FSCP 8/1 sont conçus de manière à prendre en charge le niveau d'intégrité de sécurité 3 (SIL 3) (se reporter à l'IEC 61508).
- Les mises en œuvre des protocoles FSCP 8/1 doivent être conformes à l'IEC 61508.
- Les exigences de base qui s'appliquent au développement du protocole FSCP 8/1 sont spécifiées dans l'IEC 61784-3.
- L'état de sécurité des données discrètes est l'état hors tension (0). Pour les valeurs analogiques, l'état hors tension doit être défini par l'application relative à la sécurité.
- Les conditions environnementales doivent être conformes à l'IEC 61131-2 pour les niveaux de base et aux IEC 61326-3-1 et IEC 61326-3-2 pour les essais de marge de sécurité, à moins que des normes de produits spécifiques existent.
- Sauf spécification explicite dans le présent document, les exigences CPF 8 ne doivent pas être modifiées pour la sécurité.

11.5.3 Mesures de sécurité

11.5.3.1 Généralités

La couche de communication de sécurité décrite dans le présent document fournit les mesures correctives déterministes suivantes pour sa mise en œuvre:

– numéro de séquence;

– délai;
– authentification de connexion;
– message de réaction;
– assurance d'intégrité des données;
– redondance avec contre-vérification;
– différents systèmes d'assurance d'intégrité des données.

Le choix des différentes mesures qui correspondent aux erreurs possibles est présenté dans le Tableau 1.

Tableau 1 – Choix des différentes mesures qui correspondent aux erreurs possibles

Erreurs de communication	Mesures correctives déterministes							
	Numéro de séquence	Datation (horodatage)	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	X	
Répétition non prévue	X							
Séquence incorrecte	X							
Perte	X							
Retard inacceptable			X					
Insertion	X			X	X			
Déguisement				X	X		X	X
Adressage				X				
NOTE Tableau adapté de l'IEC 62280:2014.								

11.5.3.2 Numéro de séquence

Les messages de sécurité contiennent un numéro de séquence (RNO) d'une largeur de 24 bits et une séquence spécifiée (voir 11.7.1 et 11.7.2). Ce RNO est une combinaison de RNO-1 (4 bits), RNO-2 (4 bits) et RNO-3 (16 bits). Si la séquence n'est pas respectée, tous les signaux de sortie relatifs à la sécurité doivent être définis sur leurs états de sécurité.

11.5.3.3 Délai

Un temporisateur de chien de garde intégré qui indique le délai de chaque canal de sortie de chaque esclave de sortie de sécurité assure un temps de réponse de la fonction de sécurité, 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 ou les canaux de sortie correspondants de l'esclave ou des esclaves de sortie de sécurité, hors temps de traitement de l'entrée de sécurité. Pour plus d'informations, voir également 11.9.3.

Le temps de réponse de la fonction de sécurité 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 contrôleur de sécurité (SRC).

En cas de dépassement du temps de réponse de la fonction de sécurité 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 OFF (Inactif). Cette règle doit être respectée par la couche d'application du SRP.

11.5.3.4 Authentification de connexion

Elle est mise en œuvre par un ensemble d'identifiants de connexion de sécurité (ID de liaison) et de numéro de poste. Chaque esclave de sécurité utilise un ID de liaison à 3 bits qui spécifie son système de réseau de sécurité. Ceci fournit au SRC un nombre maximal de 8 systèmes de réseaux de sécurité. L'attribution des valeurs d'identifiant de liaison doit être unique dans un système de communication de sécurité fonctionnelle. Les messages de sécurité contiennent toujours l'ID de liaison.

11.5.3.5 Message de réaction

Il est fourni par chaque esclave qui confirme la réception de messages en provenance du maître. Le message de réaction contient des informations relatives à l'état d'erreur fournies par l'esclave, ainsi que l'acquittement du RNO, de l'ID de liaison et de l'ID de commande.

11.5.3.6 Assurance d'intégrité des données

L'intégrité des données est assurée à l'aide du CRC inclus dans le PDU de sécurité. Le nœud de transmission envoie le PDU de sécurité en incluant les CRC calculés. Le nœud de réception compare les CRC inclus dans le PDU de sécurité reçu aux CRC calculés à partir de ce même PDU, puis détermine si une corruption s'est produite.

11.5.3.7 Redondance avec contre-vérification

Le nœud récepteur vérifie les parties redondantes du PDU de sécurité reçu afin de vérifier que ces portions correspondent les unes aux autres bit par bit.

11.5.3.8 Différents systèmes d'assurance d'intégrité des données

Distinction entre les messages de sécurité et les messages de non-sécurité: les messages de sécurité contiennent une somme de contrôle CRC (32 bits). Le protocole de Type 18 de l'IEC 61158 utilise un autre algorithme CRC (CRC 16 bits). De plus, chaque télégramme contient un ID de commande de 8 bits, un ID de liaison de 3 bits et un RNO de 24 bits, et chacun de ces composants doit se conformer aux restrictions définies pour ces champs.

11.5.4 Structure de la couche de communication de sécurité

Les capacités SCL de FSCP 8/1 sont fournies avec l'introduction d'éléments de service d'application de sécurité (SASE). Ces SASE sont utilisés à la place de leurs éléments de service d'application (SASE) correspondants comme spécifié ici. Dans la mesure où ces SASE proviennent directement des classes de parent définies pour la CPF 8, ils spécifient des ajouts à cette dernière. Les SASE sont mis en œuvre sur la base des éléments suivants:

- gestionnaire d'appareil – Spécification de classe ASE pour le gestionnaire d'appareil de types M1 et S1;
- gestionnaire de connexion – Définition de classe AR pour le gestionnaire de connexion de types M1 et S1;
- transmission cyclique – Spécification de classe ASE AR de données de processus pour la transmission cyclique de types M1 et S1.

La SCL enrichit ces définitions ASE par les ajouts suivants:

- gestionnaire d'appareil de sécurité de types M1 et S1;
- gestionnaire de connexion de sécurité de types M1 et S1;

– transmission cyclique de sécurité de types M1 et S1;

L'ensemble des gestions, comportements et fonctions de la SCL sont traités avec ces éléments de service d'application de sécurité.

11.5.5 Relations avec la FAL (et DLL PhL)

11.5.5.1 Présentation générale

Figure 3 représente la relation entre la SCL et les autres couches de la pile de communication du Type 18 de l'IEC 61158.

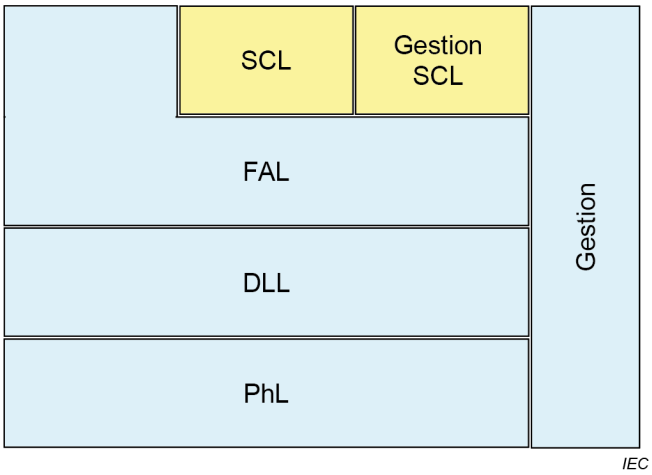


Figure 3 – Relation entre la SCL et les autres couches du Type 18 de l'IEC 61158

11.5.5.2 Types de données

Les types de données de sécurité sont spécifiés dans l'IEC 61158-5-18.

11.6 Services de la couche de communication de sécurité pour FSCP 8/1

11.6.1 Généralités

La SAR FSCP 8/1 utilise le transport tamponné pour les entrées et les sorties de données de processus. Les services de type de déclenchement de transmission sont nécessaires selon la configuration des objets instanciés. La classe de gestionnaire de connexion de sécurité prend en charge la gestion de connexion. Les applications relatives à la sécurité utilisent les éléments de service d'application de sécurité pour communiquer par l'intermédiaire de la couche de communication de sécurité. Les modèles formels de ces éléments de service sont définis en 11.6.

11.6.2 SASE

11.6.2.1 Spécification de classe de gestionnaire d'appareil de sécurité M1

La classe de gestionnaire d'appareil de sécurité M1 prend en charge un utilisateur SCL de type maître avec une mise en œuvre DL de type interrogation.

ASE SCL:			SASE de gestion
CLASSE:			Gestionnaire d'appareil de sécurité M1
ID DE CLASSE:			non utilisé
CLASSE PARENTE:			Gestionnaire d'appareil M1
ATTRIBUTS:			
1	(m)	Attribut:	Informations de gestion
1.1	(m)	Attribut:	ID de liaison
1.2	(o)	Attribut:	Version de logiciel/protocole
2	(m)	Attribut:	Informations de gestion des esclaves connectés
2.1	(m)	Attribut:	Version de logiciel/protocole 1
...	...	...	...
2.n	(m)	Attribut:	Version de logiciel/protocole n
...	...	...	...
2.64	(m)	Attribut:	Version de logiciel/protocole 64

11.6.2.2 Spécification de classe de gestionnaire d'appareil de sécurité S1

La classe de gestionnaire d'appareil de sécurité S1 prend en charge un utilisateur SCL de type esclave avec une mise en œuvre DL de type interrogation.

ASE SCL:			SASE de gestion
CLASSE:			Gestionnaire d'appareil de sécurité S1
ID DE CLASSE:			non utilisé
CLASSE PARENTE:			Gestionnaire d'appareil S1
ATTRIBUTS:			
1	(m)	Attribut:	Informations de gestion
1.1	(m)	Attribut:	ID de liaison
1.2	(m)	Attribut:	Version de logiciel/protocole

11.6.3 SAR

11.6.3.1 Classe de gestionnaire de connexion de sécurité M1

La classe de gestionnaire de connexion de sécurité M1 prend en charge un utilisateur SCL de type maître avec une mise en œuvre DL de type interrogation.

ASE SCL:			SASE de gestion
CLASSE:			Gestionnaire de connexion de sécurité M1
ID DE CLASSE:			non utilisé
CLASSE PARENTE:			Gestionnaire de connexion M1
ATTRIBUTS:			
1	(m)	Attribut:	Informations concernant les paramètres
1.1	(m)	Attribut:	Valeur du temporisateur de contrôle de sécurité
1.2	(m)	Attribut	Valeur du temporisateur de contrôle des données de sécurité
1.3	(m)	Attribut:	Spécification relative aux esclaves de sécurité
1.4	(m)	Attribut:	Source de spécification relative aux esclaves de sécurité
1.5	(m)	Attribut:	Informations sur les produits concernant les esclaves de sécurité
2	(m)	Attribut:	Données de paramètres relatives aux esclaves de sécurité
3	(m)	Attribut	Etat de liaison des esclaves de sécurité

11.6.3.2 Classe de gestionnaire de connexion de sécurité S1

La classe de gestionnaire de connexion de sécurité S1 prend en charge un utilisateur SCL de type esclave avec une mise en œuvre DL de type interrogation.

ASE SCL:			SASE de gestion
CLASSE:			Gestionnaire de connexion de sécurité S1
ID DE CLASSE:			non utilisé
CLASSE PARENTE:			Gestionnaire de connexion S1
ATTRIBUTS:			
1	(m)	Attribut:	Informations sur les produits de sécurité
2	(m)	Attribut:	Données de paramètres relatives aux esclaves de sécurité

11.6.4 ASE SAR des données de processus

11.6.4.1 Spécification de classe de transmission cyclique de sécurité M1

La classe de transmission cyclique de sécurité M1 prend en charge un utilisateur SCL de type maître associé à un gestionnaire de connexion de sécurité M1.

ASE SCL:			ASE SAR des données de processus
CLASSE:			Transmission cyclique de sécurité M1
ID DE CLASSE:			non utilisé
CLASSE PARENTE:			Transmission cyclique M1
ATTRIBUTS:			
1.	(m)	Attribut:	Données de sortie
1.1.	(m)	Attribut:	Données RY de sécurité
1.2.	(m)	Attribut:	Données RWw
1.2.1.	(m)	Attribut:	Données RWw de sécurité
1.2.2.	(m)	Attribut:	TPI-T de sécurité
1.3.	(m)	Attribut:	Données RY-r de sécurité
1.4.	(m)	Attribut:	Données RWw-r
1.4.1.	(m)	Attribut:	Données RWw-r de sécurité
1.4.2.	(m)	Attribut:	TPI-T-r de sécurité
2.	(m)	Attribut:	Données d'entrée
2.1.	(m)	Attribut:	Données de sécurité en 1
2.1.1.	(m)	Attribut:	Données RX de sécurité 1
2.1.2.	(m)	Attribut:	Données RWr 1
2.1.2.1	(m)	Attribut:	Données RWr de sécurité 1
2.1.2.2	(m)	Attribut:	TPI-R de sécurité 1
2.1.3.	(m)	Attribut:	Données RX-r de sécurité 1
2.1.4.	(m)	Attribut:	Données RWr-r 1
2.1.4.1	(m)	Attribut:	Données RWr-r de sécurité 1
2.1.4.2	(m)	Attribut:	TPI-R-r de sécurité 1
…	…	…	…
2.n.	(m)	Attribut:	Données de sécurité d'entrée en n
…	…	…	…
2,64.	(m)	Attribut:	Données de sécurité en 64

11.6.4.2 Spécification de classe de transmission cyclique de sécurité S1

La classe de transmission cyclique de sécurité S1 prend en charge un utilisateur SCL de type esclave associé à un gestionnaire de connexion de sécurité S1.

ASE SCL:			ASE SAR des données de processus
CLASSE:			Transmission cyclique de sécurité S1
ID DE CLASSE:			non utilisé
CLASSE PARENTE:			Transmission cyclique S1
ATTRIBUTS:			
1.	(m)	Attribut:	Données de sortie
1.1	(m)	Attribut:	Données RY de sécurité
1.2	(m)	Attribut:	Données RWw
1.2.1.	(m)	Attribut:	Données RWw de sécurité
1.2.2.	(m)	Attribut:	TPI-T de sécurité
1.3	(m)	Attribut:	Données RY-r de sécurité
1.4	(m)	Attribut:	Données RWw-r
1.4.1.	(m)	Attribut:	Données RWw-r de sécurité
1.4.2.	(m)	Attribut:	TPI-T-r de sécurité
2.	(m)	Attribut:	Données d'entrée
2.1	(m)	Attribut:	Données RX de sécurité
2.2	(m)	Attribut:	Données RWr
2.2.1	(m)	Attribut:	Données RWr de sécurité
2.2.2	(m)	Attribut:	TPI-R de sécurité
2.3	(m)	Attribut:	Données RX-r de sécurité
2.4	(m)	Attribut:	Données RWr-r
2.4.1	(m)	Attribut:	Données RWr-r de sécurité
2.4.2	(m)	Attribut:	TPI-R-r de sécurité

11.7 Protocole de couche de communication de sécurité pour FSCP 8/1

11.7.1 Format PDU de sécurité

11.7.1.1 Généralités

La syntaxe et le codage PDU de sécurité sont décrits comme dans l'IEC 61158-6-18 (syntaxe abstraite et syntaxe de transfert).

11.7.1.2 Syntaxe abstraite

11.7.1.2.1 Syntaxe abstraite PDU de gestionnaire d'appareil de sécurité M1

La syntaxe abstraite applicable aux attributs qui appartiennent à cette classe est décrite dans le Tableau 2.

Tableau 2 – Format d'attributs de gestionnaire d'appareil de sécurité M1

Attribut	Format	Taille (bits)
Informations de gestion	Structure de 2 éléments:	11
ID de liaison	Unsigned3	3
Version de logiciel/protocole	1 octet, en mode point	8
Informations de gestion des esclaves connectés	Matrice de 64 membres	64 octets
Version de logiciel/protocole	1 octet, en mode point	8

11.7.1.2.2 Syntaxe abstraite PDU de gestionnaire d'appareil de sécurité S1

La syntaxe abstraite applicable aux attributs qui appartiennent à cette classe est décrite dans le Tableau 3.

Tableau 3 – Format d'attributs de gestionnaire d'appareil de sécurité S1

Attribut	Format	Taille (bits)
Informations de gestion	Structure de 3 éléments:	11
ID de liaison	Unsigned3	3
Version de logiciel/protocole	1 octet, en mode point	8

11.7.1.2.3 Syntaxe abstraite PDU de gestionnaire de connexion de sécurité M1

La syntaxe abstraite applicable aux attributs qui appartiennent à cette classe est décrite dans le Tableau 4.

Tableau 4 – Format d'attributs de gestionnaire de connexion de sécurité M1

Attribut	Format	Taille (bits)
Informations concernant les paramètres	Structure de 5 éléments:	2 004 octets
Valeur du temporisateur de contrôle de sécurité	Unsigned16	16
Valeur du temporisateur de contrôle des données de sécurité	Unsigned16	16
Spécification relative aux esclaves de sécurité	8 octets, en mode point	64
Source de spécification relative aux esclaves de sécurité	8 octets, en mode point	64
Informations sur les produits concernant les esclaves de sécurité	Matrice de 64 membres	1 984 octets
Informations sur les produits de sécurité 1 – 64	Structure de données par mot	31 octets
Données de paramètres relatives aux esclaves de sécurité	16 – 52 224 octets	16 – 52 224 octets
Etat de liaison des esclaves de sécurité	8 octets, en mode point	64

11.7.1.2.4 Syntaxe abstraite PDU de gestionnaire de connexion de sécurité S1

La syntaxe abstraite applicable aux attributs qui appartiennent à cette classe est décrite dans le Tableau 5.

Tableau 5 – Format d'attributs de gestionnaire de connexion de sécurité S1

Attribut	Format	Taille (bits)
Informations sur les produits de sécurité 1 – 64	Structure de données par mot	31 octets
Données de paramètres relatives aux esclaves de sécurité	16 – 816 octets	16 – 816 octets

11.7.1.2.5 Syntaxe abstraite PDU de transmission cyclique de sécurité M1

La syntaxe abstraite applicable aux attributs qui appartiennent à cette classe est décrite dans le Tableau 6.

Tableau 6 – Format d'attributs de transmission cyclique de sécurité M1

Attribut	Format	Taille (bits)
Données de sortie	Structure de 2 éléments:	192 × n
Données RY de sécurité	Structure de données orientées sur les bits	32 × n
Données RWw	Structure de données par mot	64 × n
Données RWw de sécurité	Données par mot	64 × (n – m)
TPI-T de sécurité	Informations de paquets de transmission de sécurité	64 × m
Données RY-r de sécurité	Structure de données orientées sur les bits	32 × n
Données RWw-r	Structure de données par mot	64 × n
Données RWw-r de sécurité	Données par mot	64 × (n – m)
TPI-T-r de sécurité	Informations de paquets de transmission de sécurité	64 × m
Données d'entrée	Structure de n éléments:	192 × n
Données de sécurité en 1	Structure de 2 éléments:	192
Données RX de sécurité	Structure de données orientées sur les bits	64
Données RWr	Structure de données par mot	128
Données RWr de sécurité	Données par mot	64
TPI-R de sécurité	Informations de paquets de transmission de sécurité	64
Données RX-r de sécurité	Structure de données orientées sur les bits	32
Données RWr-r	Structure de données par mot	64
Données RWr-r de sécurité	Données par mot	64
TPI-R-r de sécurité	Informations de paquets de transmission de sécurité	64
…	…	…
Données de sécurité d'entrée en n	Structure de 2 éléments:	192
NOTE Les valeurs de n et de m dépendent des valeurs des paramètres de configuration correspondants dans l'état du maître.		

11.7.1.2.6 Syntaxe abstraite PDU de transmission cyclique de sécurité S1

La syntaxe abstraite applicable aux attributs qui appartiennent à cette classe est décrite dans le Tableau 7.

Tableau 7 – Format d'attributs de transmission cyclique de sécurité S1

Attribut	Format	Taille (bits)
Données de sortie	Structure de 2 éléments:	192
Données RY de sécurité	Structure de données orientées sur les bits	32
Données RWw	Structure de données par mot	64
Données RWw de sécurité	Données par mot	64
TPI-T de sécurité	Informations de paquets de transmission de sécurité	64
Données RY-r de sécurité	Structure de données orientées sur les bits	32
Données RWw-r	Structure de données par mot	64
Données RWw-r de sécurité	Données par mot	64
TPI-T-r de sécurité	Informations de paquets de transmission de sécurité	64
Données d'entrée	Structure de 2 éléments:	192
Données RX de sécurité	Structure de données orientées sur les bits	64
Données RWr	Structure de données par mot	128
Données RWr de sécurité	Données par mot	64
TPI-R de sécurité	Informations de paquets de transmission de sécurité	64
Données RX-r de sécurité	Structure de données orientées sur les bits	64
Données RWr-r	Structure de données par mot	128
Données RWr-r de sécurité	Données par mot	64
TPI-R-r de sécurité	Informations de paquets de transmission de sécurité	64

11.7.1.3 Syntaxe de transfert

11.7.1.3.1 Codage PDU de gestionnaire d'appareil de sécurité M1

Le codage PDU spécifique applicable aux attributs qui appartiennent à cette classe est décrit dans le Tableau 8.

Tableau 8 – Codage d'attributs de gestionnaire d'appareil de sécurité M1

Attribut	Codage		
Informations de gestion	Spécifie la configuration de l'appareil maître		
ID de liaison	0 – 7 = plage admissible		
Version de logiciel/protocole	**Bit**	**Description**	**Valeur**
	5 – 0	Version de logiciel	1 – 63 = plage admissible
	7 – 6	Version de protocole	0 = Version 1 1 = Version 2 2 = Version 3 3 = Version 4
Informations de gestion des esclaves connectés	Spécifie la configuration des esclaves connectés		
Informations sur les esclaves 1 – 64	Matrice de 64 éléments, chaque élément étant codé comme suit:		
Version de logiciel/protocole	**Bit**	**Description**	**Valeur**
	5 – 0	Version de logiciel	1 – 63 = plage admissible
	7 – 6	Version de protocole	0 = Version 1 1 = Version 2 2 = Version 3 3 = Version 4

11.7.1.3.2 Codage PDU de gestionnaire d'appareil de sécurité S1

Le codage PDU spécifique applicable aux attributs qui appartiennent à cette classe est décrit dans le Tableau 9.

Tableau 9 – Codage d'attributs de gestionnaire d'appareil de sécurité S1

Attribut	Codage		
Informations de gestion	Spécifie la configuration de l'appareil maître		
ID de liaison	0 – 7 = plage admissible		
Version de logiciel/protocole	**Bit**	**Description**	**Valeur**
	5 – 0	Version de logiciel	1 – 63 = plage admissible
	7 – 6	Version de protocole	0 = Version 1 1 = Version 2 2 = Version 3 3 = Version 4

11.7.1.3.3 Codage PDU de gestionnaire de connexion de sécurité M1

Le codage PDU spécifique applicable aux attributs qui appartiennent à cette classe est décrit dans le Tableau 10.

Tableau 10 – Codage d'attributs de gestionnaire de connexion de sécurité M1

Attribut	Codage
Informations concernant les paramètres	Spécifie la configuration de connexion
Valeur du temporisateur de contrôle de sécurité	1 – 65 535 = ms
Valeur du temporisateur de contrôle des données de sécurité	1 – 65 535 = ms
Spécification relative aux esclaves de sécurité	Les bits 0 – 63 correspondent aux créneaux 1 – 64, où: 0 = SCL non prise en charge 1 = SCL prise en charge
Source de spécification relative aux esclaves de sécurité	Les bits 0 – 63 correspondent aux créneaux 1 – 64, où: 0 = spécification de l'utilisateur SCL non prise en charge 1 = spécification de l'utilisateur SCL prise en charge
Informations sur les produits d'esclaves de sécurité 1 – 64	Matrice de 64 éléments, chaque élément étant codé comme suit:
Informations sur les produits de sécurité	31 octets de données pour les informations sur les produits de sécurité
Données de paramètres de sécurité	0 – 52 224 octets de données pour l'accès à la mémoire esclave
Etat de liaison des esclaves de sécurité	Les bits 0 – 63 correspondent aux créneaux 1 – 64, où: 0 = Poste esclave de sécurité hors fonctionnement 1 = Poste esclave de sécurité en fonctionnement

11.7.1.3.4 Codage PDU de gestionnaire de connexion de sécurité S1

Le codage PDU spécifique applicable aux attributs qui appartiennent à cette classe est décrit dans le Tableau 11.

Tableau 11 – Codage d'attributs de gestionnaire de connexion de sécurité S1

Attribut	Codage
Informations sur les produits de sécurité	31 octets de données pour les informations sur les produits de sécurité
Données de paramètres de sécurité	0 – 816 octets de données pour l'accès à la mémoire esclave

11.7.1.3.5 Codage PDU de transmission cyclique de sécurité M1

Le codage PDU spécifique applicable aux attributs qui appartiennent à cette classe est décrit dans le Tableau 12.

Tableau 12 – Codage d'attributs de transmission cyclique de sécurité M1

<table>
<tr><th>Attribut</th><th colspan="4">Codage</th></tr>
<tr><td>Données de sortie</td><td colspan="4">Registres de données de processus réglés par le maître pour la sortie de l'appareil esclave</td></tr>
<tr><td>Données RY de sécurité</td><td colspan="4">Champ à mapping positionnel de données de sortie orientées sur les bits pour tous les appareils esclaves connectés ordonnés par créneau avec 32 bits</td></tr>
<tr><td>Données RWw</td><td colspan="4">Champ à mapping positionnel dans lequel sont mappées les données de sortie par mot pour tous les appareils esclaves de sécurité connectés et toutes les informations de paquets de transmission de sécurité pour une transmission aux appareils esclaves de sécurité</td></tr>
<tr><td>Données RWw de sécurité</td><td colspan="4">Champ à mapping positionnel de données de sortie par mot pour tous les appareils esclaves connectés. Contient 4 mots par créneau, en commençant par le second créneau. Ceci est dû au fait que le champ suivant occupe l'espace alloué au premier créneau dans un esclave de non-sécurité</td></tr>
<tr><td rowspan="11">TPI-T de sécurité</td><td>Octet</td><td>Bit</td><td>Description</td><td>Valeurs</td></tr>
<tr><td>0 – 1</td><td>–</td><td>RNO-3</td><td>0 – 65 535</td></tr>
<tr><td rowspan="9">2 – 3</td><td>0 – 3</td><td>RNO-1</td><td>0 – 15</td></tr>
<tr><td>4 – 6</td><td>ID de liaison</td><td>0 – 7</td></tr>
<tr><td>7</td><td>réservé</td><td>0</td></tr>
<tr><td>8 – 11</td><td>Type de données de transmission</td><td>0 – 15</td></tr>
<tr><td>12</td><td>Drapeau occupé</td><td>0 = occupé
1 = non occupé</td></tr>
<tr><td>13</td><td>réservé</td><td>0</td></tr>
<tr><td>14</td><td>Demande de lecture</td><td>0 = pas de demande
1 = demande</td></tr>
<tr><td>15</td><td>Mode d'application de l'utilisateur SCL</td><td>0 = mode d'essai
1 = mode de sécurité</td></tr>
<tr><td>4 – 7</td><td>–</td><td>CRC32-A</td><td>CRC32-A</td></tr>
<tr><td>Données RY-r de sécurité</td><td colspan="4">identique à RY</td></tr>
<tr><td>Données RWw-r</td><td colspan="4">identique à RWw</td></tr>
<tr><td>Données RWw-r de sécurité</td><td colspan="4">identique à RWw de sécurité</td></tr>
<tr><td rowspan="5">TPI-T-r de sécurité</td><td>Octet</td><td>Bit</td><td>Description</td><td>Valeurs</td></tr>
<tr><td>0 – 1</td><td>–</td><td>Tx/Rx (Code A)</td><td>255 / 1 – 64</td></tr>
<tr><td rowspan="2">2 – 3</td><td>0 – 3</td><td>RNO-2</td><td>0 – 15</td></tr>
<tr><td>4 – 15</td><td colspan="2">identique à TPI-T de sécurité</td></tr>
<tr><td>4 – 7</td><td>–</td><td>CRC32-B</td><td>CRC32-B</td></tr>
<tr><td>Données d'entrée</td><td colspan="4">Registres de données de processus lus par le maître qui représentent les entrées de l'appareil esclave</td></tr>
<tr><td>Données de sécurité d'entrée</td><td colspan="4">Registres de données de processus lus par le maître qui représentent les entrées de l'appareil esclave de sécurité</td></tr>
</table>

<table>
<tr><th>Attribut</th><th colspan="3">Codage</th></tr>
<tr><td>Données RX de sécurité</td><td colspan="3">Champ qui contient les données d'entrée orientées sur les bits envoyées par l'appareil esclave n ordonné par créneau avec 32 bits</td></tr>
<tr><td>Données RWr</td><td colspan="3">Champ qui contient les données d'entrée orientées par mot envoyées par l'appareil esclave n ordonné par créneau avec 4 mots</td></tr>
<tr><td>Données RWr de sécurité</td><td colspan="3">Champ à mapping positionnel des données d'entrée par mot envoyées par l'appareil esclave n. Contient 4 mots par créneau en commençant par le second créneau. Ceci est dû au fait que le champ suivant occupe l'espace alloué au premier créneau dans un esclave de non-sécurité</td></tr>
<tr><td>TPI-R de sécurité</td><td>Bit</td><td>Description</td><td>Valeurs</td></tr>
<tr><td></td><td>0 – 15</td><td>RNO-3</td><td>0 – 65 535</td></tr>
<tr><td></td><td>16 – 19</td><td>RNO-1</td><td>0 – 15</td></tr>
<tr><td></td><td>20 – 22</td><td>ID de liaison</td><td>0 – 7</td></tr>
<tr><td></td><td>23</td><td>réservé</td><td>0</td></tr>
<tr><td></td><td>24 – 27</td><td>Type de données de transmission</td><td>0 – 15</td></tr>
<tr><td></td><td>28</td><td>Drapeau occupé</td><td>0 = occupé
1 = non occupé</td></tr>
<tr><td></td><td>29</td><td>Notification d'erreur</td><td>0 = pas d'erreur
1 = erreur</td></tr>
<tr><td></td><td>30</td><td>réservé</td><td>0</td></tr>
<tr><td></td><td>31</td><td>Mode d'application de l'utilisateur SCL</td><td>0 = mode d'essai
1 = mode de sécurité</td></tr>
<tr><td></td><td>32 – 63</td><td>CRC32-A</td><td>CRC32-A</td></tr>
<tr><td>Données RX-r de sécurité</td><td colspan="3">identique à RX de sécurité</td></tr>
<tr><td>Données RWr-r</td><td colspan="3">identique à RWr</td></tr>
<tr><td>Données RWr-r de sécurité</td><td colspan="3">identique à RWr de sécurité</td></tr>
<tr><td>TPI-R-r de sécurité</td><td>Bit</td><td>Description</td><td>Valeurs</td></tr>
<tr><td></td><td>0 – 15</td><td>Tx/Rx (Code A)</td><td>255 / 1 – 64</td></tr>
<tr><td></td><td>16 – 19</td><td>RNO-2</td><td>0 – 15</td></tr>
<tr><td></td><td>20 – 31</td><td>identique à TPI-R de sécurité</td><td></td></tr>
<tr><td></td><td>32 – 63</td><td>CRC32-B</td><td>CRC32-B</td></tr>
<tr><td colspan="4">NOTE La valeur de RNO est obtenue en combinant les sous-parties du RNO de la manière suivante:
RNO-1 = bits 0-3 du RNO
RNO-2 = bits 4-7 du RNO
RNO-3 = bits 8-23 du RNO</td></tr>
</table>

11.7.1.3.6 Codage PDU de transmission cyclique de sécurité S1

Le codage PDU spécifique applicable aux attributs qui appartiennent à cette classe est décrit dans le Tableau 13.

Tableau 13 – Codage d'attributs de transmission cyclique de sécurité S1

Attribut	Codage		
Données de sortie	Données de processus reçues par le maître		
Données RY de sécurité	Champ qui contient les données d'entrée orientées sur les bits ordonnées par créneau avec 32 bits		
Données RWw	Champ à mapping positionnel dans lequel sont mappées les données de sortie par mot (facultativement) et les informations de paquets de transmission de sécurité reçues par le maître		
Données RWw de sécurité	Champ à mapping positionnel de données de sortie par mot pour l'appareil esclave. Contient 4 mots par créneau, en commençant par le second créneau. Ceci est dû au fait que le champ suivant occupe l'espace alloué au premier créneau dans un esclave de non-sécurité		
TPI-T de sécurité	**Bit**	**Description**	**Valeurs**
	0 – 15	RNO-3	0 – 65 535
	16 – 19	RNO-1	0 – 15
	20 – 22	ID de liaison	0 – 7
	23	réservé	0
	24 – 27	Type de données de transmission	0 – 15
	28	Drapeau occupé	0 = occupé 1 = non occupé
	29	réservé	0
	30	Demande de lecture	0 = pas de demande 1 = demande
	31	Mode d'application de l'utilisateur SCL	0 = mode d'essai 1 = mode de sécurité
	32 – 63	CRC32-A	CRC32-A
Données RY-r de sécurité	identique à RY de sécurité		
Données RWw-r	identique à RWw		
Données RWw-r de sécurité	identique à RWw de sécurité		
TPI-T-r de sécurité	**Bit**	**Description**	**Valeurs**
	0 – 15	Tx/Rx (Code A)	1 – 64 / 255
	16 – 19	RNO-2	0 – 15
	20 – 31	identique à TPI-T de sécurité	
	32 – 63	CRC32-B	CRC32-B
Données d'entrée	Données de processus transmises au maître		
Données RX de sécurité	Champ qui contient les données d'entrée orientées sur les bits ordonnées par créneau avec 32 bits		
Données RWr	Champ qui contient les données d'entrée par mot fournies par le maître.		

<table>
<tr><th>Attribut</th><th colspan="3">Codage</th></tr>
<tr><td>Données RWr de sécurité</td><td colspan="3">Champ à mapping positionnel de données d'entrée par mot pour l'appareil esclave. Contient 4 mots par créneau, en commençant par le second créneau. Ceci est dû au fait que le champ suivant occupe l'espace alloué au premier créneau dans un esclave de non-sécurité</td></tr>
<tr><td rowspan="11">TPI-R de sécurité</td><td>Bit</td><td>Description</td><td>Valeurs</td></tr>
<tr><td>0 – 15</td><td>RNO-3</td><td>0 – 65 535</td></tr>
<tr><td>16 – 19</td><td>RNO-1</td><td>0 – 15</td></tr>
<tr><td>20 – 22</td><td>ID de liaison</td><td>0 – 7</td></tr>
<tr><td>23</td><td>réservé</td><td>0</td></tr>
<tr><td>24 – 27</td><td>Type de données de transmission</td><td>0 – 15</td></tr>
<tr><td>28</td><td>Drapeau occupé</td><td>0 = occupé
1 = non occupé</td></tr>
<tr><td>29</td><td>Notification d'erreur</td><td>0 = pas d'erreur
1 = erreur</td></tr>
<tr><td>30</td><td>réservé</td><td>0</td></tr>
<tr><td>31</td><td>Mode d'application de l'utilisateur SCL</td><td>0 = mode d'essai
1 = mode de sécurité</td></tr>
<tr><td>32 – 63</td><td>CRC32-A</td><td>CRC32-A</td></tr>
<tr><td>Données RX-r de sécurité</td><td colspan="3">identique à RX de sécurité</td></tr>
<tr><td>Données RWr-r</td><td colspan="3">identique à RWr</td></tr>
<tr><td>Données RWr-r de sécurité</td><td colspan="3">identique à RWr de sécurité</td></tr>
<tr><td rowspan="5">TPI-R-r de sécurité</td><td>Bit</td><td>Description</td><td>Valeurs</td></tr>
<tr><td>0 – 15</td><td>Tx/Rx (Code A)</td><td>1 – 64 / 255</td></tr>
<tr><td>16 – 19</td><td>RNO-2</td><td>0 – 15</td></tr>
<tr><td>20 – 31</td><td>identique à TPI-R de sécurité</td><td></td></tr>
<tr><td>32 – 63</td><td>CRC32-B</td><td>CRC32-B</td></tr>
<tr><td colspan="4">NOTE La valeur de RNO est obtenue en combinant les sous-parties du RNO de la manière suivante:
RNO-1 = bits 0-3 du RNO
RNO-2 = bits 4-7 du RNO
RNO-3 = bits 8-23 du RNO</td></tr>
</table>

11.7.2 Description d'état

11.7.2.1 Présentation générale

L'extension du modèle d'état SCL s'effectue à partir du Type 18 de l'IEC 61158 avec un état de sécurité, comme représenté à la Figure 4. L'état de sécurité est actif dans des conditions d'erreur et est configuré afin de s'assurer que toutes les sorties sont maintenues dans des états de sécurité. Les sorties numériques sont les suivantes: faible, nul ou hors tension, et les sorties analogiques sont maintenues à un niveau de sécurité configuré précédemment par l'utilisateur SCL. L'appareil maître de sécurité M1 gère les états de chaque appareil esclave de sécurité de manière individuelle.

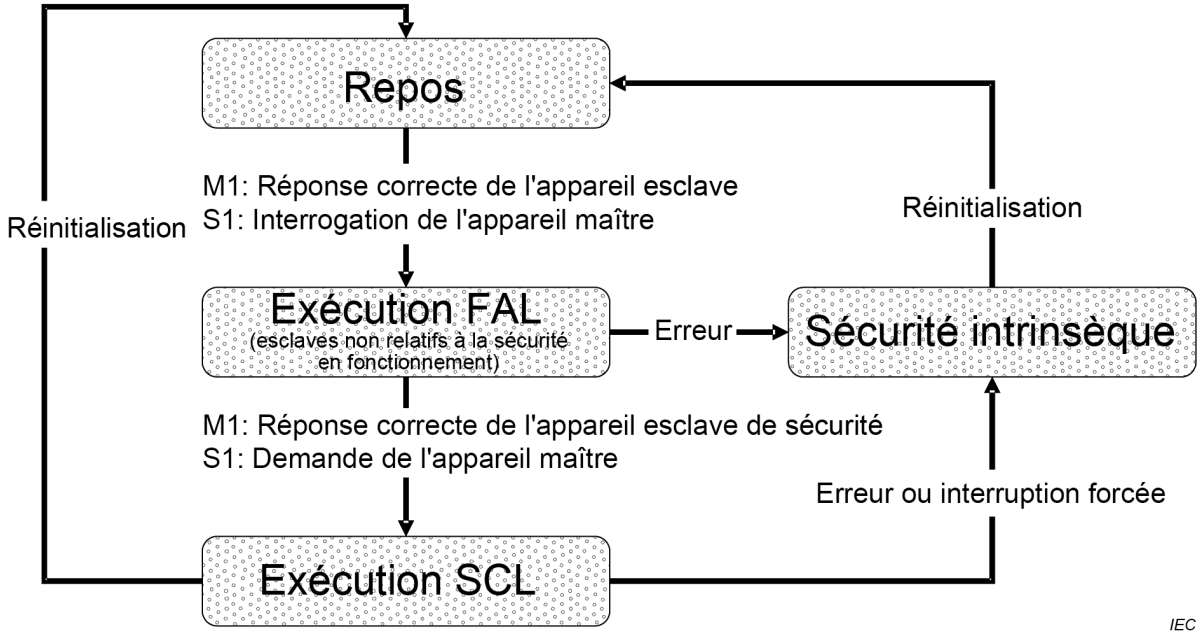


Figure 4 – Diagramme d'états

La méthode générale d'établissement de connexions, de vérification des esclaves et de rafraîchissement des données s'étend également au-delà de celle du Type 18 de l'IEC 61158, et inclut la transmission et le traitement des paramètres de sécurité (voir gestion SCL en 11.8), ainsi que la transmission des données de sécurité et le contrôle de la confirmation.

11.7.2.2 Repos

11.7.2.2.1 Présentation générale

L'état de repos existe préalablement aux communications FAL éventuelles entre les appareils.

11.7.2.2.2 Transition

Sur demande appropriée de l'utilisateur FAL à l'appareil maître de sécurité M1, la réception d'une réponse adaptée de l'appareil esclave de sécurité S1 génère une transition de l'état de repos à l'état d'exécution FAL.

A la réception de communications d'interrogation en provenance du maître de sécurité M1, l'appareil esclave de sécurité S1 passe à l'état d'exécution FAL.

11.7.2.3 Exécution FAL

11.7.2.3.1 Présentation générale

A l'état d'exécution FAL, les appareils maîtres de sécurité M1 et les appareils esclaves de sécurité S1 ont établi des communications de non-sécurité.

11.7.2.3.2 Transition

Sur réception d'une demande en provenance du maître de sécurité M1, l'appareil esclave de sécurité S1 passe à l'état d'exécution SCL.

A la réception de réponses adaptées en provenance des appareils esclaves de sécurité S1, l'appareil maître de sécurité M1 passe à l'état d'exécution SCL.

Toute condition d'erreur ou d'anomalie au cours de l'état d'exécution FAL ou toute tentative avortée de passage à l'état d'exécution SCL entraîne le passage d'un appareil FSCP 8/1 à l'état de sécurité intrinsèque.

11.7.2.4 Exécution SCL

11.7.2.4.1 Présentation générale

Les détails de l'état d'exécution SCL sont expliqués en 11.8.

11.7.2.4.2 Transition

Comme expliqué en 11.7.2.6, un appareil FSCP 8/1 passe à l'état de sécurité intrinsèque lorsqu'une erreur est détectée par l'une des mesures de sécurité suivantes:

– numéro de séquence;
– délai;
– authentification de connexion;
– message de réaction;
– assurance d'intégrité des données;
– redondance avec contre-vérification;
– différents systèmes d'assurance d'intégrité des données.

Comme expliqué en 11.7.2.7, un appareil FSCP 8/1 passe à l'état de sécurité intrinsèque sur réception d'une demande d'interruption forcée.

11.7.2.5 Etat de sécurité intrinsèque

11.7.2.5.1 Présentation générale

L'état de sécurité intrinsèque est un état dont toutes les sorties sont maintenues dans leur état de sécurité. Pour les sorties numériques, et sauf spécification contraire, il s'agit de l'état hors tension (ou nul ou faible), et pour les sorties analogiques, sauf spécification contraire, il s'agit de l'état de sortie nulle (c'est-à-dire pas de tension et/ou pas de courant). Généralement, les sorties analogiques sont configurées avec une valeur de sécurité imposée sur la sortie dans l'état de sécurité intrinsèque.

11.7.2.5.2 Transition

La sortie de l'état de sécurité intrinsèque est possible uniquement par une réinitialisation des esclaves.

11.7.2.6 Transmission et traitement des données de sécurité

11.7.2.6.1 Présentation générale

La SCL du protocole FSCP 8/1 fournit les mesures de sécurité suivantes:

– numéro de séquence;
– délai;
– authentification de connexion;
– message de réaction;
– assurance d'intégrité des données;
– redondance avec contre-vérification;
– différents systèmes d'assurance d'intégrité des données.

Le maître de sécurité et chaque esclave de sécurité gèrent et analysent les transmissions de sécurité afin de vérifier leur intégrité.

11.7.2.6.2 Numéro de séquence

Les messages de sécurité contiennent un numéro de séquence (RNO) d'une largeur de 24 bits et une séquence spécifiée. Le RNO est incrémenté et transmis par le maître de sécurité. L'esclave de sécurité renvoie le RNO reçu. En cas de réception d'un RNO hors séquence, l'esclave de sécurité passe à l'état de sécurité.

11.7.2.6.3 Délai

La SCL utilise un temporisateur de contrôle de sécurité et des temporisateurs de contrôle des données de sécurité afin d'assurer des communications continues fiables. La gestion SLC configure le temporisateur à une valeur comprise entre 1 ms et 65 535 ms.

Le temporisateur de contrôle de sécurité permet de confirmer que la communication cyclique de sécurité s'effectue dans des conditions normales, et les temporisateurs de contrôle des données de sécurité permettent de confirmer que les communications cycliques de sécurité successives s'effectuent également dans des conditions normales. Les postes de sécurité contrôlent l'intervalle de réception des données cycliques qui sont protégées par les informations de protection des données de sécurité normales fournies par ce temporisateur de contrôle de sécurité. De plus, les postes esclaves de sécurité contrôlent les intervalles de réception des données cycliques qui sont protégées par les informations de protection des données de sécurité normales fournies par les temporisateurs de contrôle des données de sécurité.

Le Tableau 14, le Tableau 15 et le Tableau 16 décrivent le fonctionnement du temporisateur de contrôle de sécurité pour les appareils maîtres et esclaves de sécurité.

Tableau 14 – Fonctionnement du temporisateur de contrôle des appareils maîtres de sécurité

Démarrage	Fin	Fin d'erreur
Transmission des données de sécurité (RNO ≠ 0)	Réception des données (de rafraîchissement) de la réponse des appareils esclaves (du même RNO que le RNO transmis) auxquelles les informations de protection des données de sécurité ont été ajoutées de manière appropriée	(1) Lors d'une temporisation de contrôle (2) Lors de la détection d'une erreur RNO

Tableau 15 – Fonctionnement du temporisateur de contrôle des appareils esclaves de sécurité

Démarrage	Réinitialisation	Fin
Réception des données de sécurité (CMD ID=01h)	Réception des données d'interrogation et de rafraîchissement du poste maître (précédemment RNO+1) auxquelles les informations de protection des données de sécurité ont été ajoutées de manière appropriée	(1) Lors d'une temporisation de contrôle (2) Lors de la détection d'une erreur RNO (3) A la réception d'une demande d'interruption forcée

Tableau 16 – Fonctionnement du temporisateur de contrôle des données de sécurité

Démarrage	Réinitialisation	Fin
Réception des données E/S cycliques de sécurité (CMD ID=0Fh)	Réception des données d'interrogation et de rafraîchissement du poste maître (précédemment RNO+2) auxquelles les informations de protection des données de sécurité ont été ajoutées de manière appropriée	(1) Lors d'une temporisation de contrôle (2) Lors de la détection d'une erreur RNO (3) A la réception d'une demande d'interruption forcée
NOTE Les postes esclaves de sécurité ont deux temporisateurs de contrôle des données de sécurité. Un temporisateur de contrôle des données de sécurité se déclenche à réception des données E/S cycliques de sécurité (CMS ID=0Fh et RNO=n), la réception de deux données successives (RNO=n+2) le réinitialise. L'autre temporisateur de contrôle des données de sécurité se déclenche à réception des données E/S cycliques de sécurité (CMS ID=0Fh et RNO=n)+1, la réception de deux données successives (RNO=n+3) le réinitialise.		

Le comportement d'un maître de sécurité à l'expiration du temporisateur de contrôle de sécurité est spécifié comme suit:

1) traitement à sécurité intrinsèque tel que la mise à zéro des données S-RX fournies à l'utilisateur SCL;
2) notification d'erreur à l'utilisateur SCL;
3) passage à l'état de repos.

Le comportement d'un esclave de sécurité à l'expiration du temporisateur de contrôle de sécurité est spécifié comme suit:

1) traitement à sécurité intrinsèque tel que l'interruption de la sortie avec les appareils externes;
2) notification d'erreur à l'utilisateur SCL;
3) passage à l'état de sécurité.

11.7.2.6.4 Authentification de connexion

L'authentification de connexion est mise en œuvre par un ensemble d'identifiants de connexion de sécurité (ID de liaison) et de numéro de poste. Chaque esclave de sécurité utilise un ID de liaison à 3 bits qui spécifie son système de réseau de sécurité. Ceci fournit au SRC un nombre maximal de 8 systèmes de réseaux de sécurité. L'attribution des valeurs d'identifiant de liaison doit être unique dans un système de communication de sécurité fonctionnelle. Les messages de sécurité contiennent toujours l'ID de liaison.

De plus, l'ID de connexion logique de 16 bits transmis est annexé au SPDU pour validation. Ce champ, qui est composé de Tx (ID source de 8 bits) et Rx (ID de destination de 8 bits) est vérifié quant à l'exactitude et également inclus dans les mesures d'intégrité des données.

11.7.2.6.5 Message de réaction

Il est fourni par chaque esclave qui confirme la réception de messages en provenance du maître. Le message de réaction contient des informations relatives à l'état d'erreur fournies par l'esclave, ainsi que l'acquittement du RNO, de l'ID de liaison et de l'ID de commande.

11.7.2.6.6 Intégrité des données

Le calcul du CRC32 pour le protocole FSCP 8/1 est décrit à l'Annexe A. Le taux d'erreurs résiduelles pour le protocole FSCP 8/1 est calculé conformément à l'IEC 61784-3.

11.7.2.6.7 Redondance avec contre-vérification

Les champs de données redondants sont comparés bit par bit à leurs homologues.

11.7.2.6.8 Différents systèmes d'assurance d'intégrité des données

La distinction entre les messages importants pour la sécurité et les messages non importants pour la sécurité est assurée par la validation du caractère unique des messages de sécurité à contenir une somme de contrôle CRC à format approprié (32 bits), un ID de commande de 8 bits, un ID de liaison de 3 bits et un RNO de 24 bits.

Le protocole de Type 18 de l'IEC 61158 utilise un algorithme CRC différent (CRC de 16 bits), en excluant tout champ de données de soutien au protocole, ainsi que tout ID de commande ou de liaison ou tout RNO.

11.7.2.7 Interruption forcée

Le traitement à interruption forcée est utilisé lorsqu'un maître de sécurité demande à un esclave de sécurité d'interrompre la communication. L'esclave de sécurité qui reçoit la demande d'interruption forcée passe à l'état de sécurité intrinsèque (en interrompant toute sortie externe), puis interrompt alors immédiatement la communication.

11.8 Gestion de la couche de communication de sécurité pour FSCP 8/1

11.8.1 Généralités

Les applications relatives à la sécurité utilisent les services suivants pour configurer le système de communication de sécurité:

– établir une connexion;
– vérifier la configuration des appareils esclaves;
– transmettre des paramètres d'esclaves de sécurité.

11.8.2 Etablissement de connexion et processus de confirmation

A l'établissement de la connexion, la configuration initiale est confirmée par la validation du fait que les appareils de sécurité contiennent les SAREP et que la transmission cyclique de sécurité est prise en charge. Ce processus est décrit dans le Tableau 17.

Tableau 17 – Détails de l'établissement de connexion et du processus de confirmation

Type de SAREP	Détails du processus
Maître de sécurité	(1) Confirmer que l'esclave est un appareil esclave de sécurité (cela est confirmé par la communication des données cycliques de sécurité). (2) Confirmer que l'esclave de sécurité a reçu la commande Etablir connexion (cela est confirmé par la vérification du fait que les CMD des données de réponse sont identiques aux données transmises). (3) Transmettre la valeur du temporisateur de contrôle de sécurité.
Esclave de sécurité	(1) Confirmer que le maître est un appareil maître de sécurité (cela est confirmé par la communication des données cycliques de sécurité). (2) Recevoir la valeur du temporisateur de contrôle de sécurité et enregistrer cette dernière de manière interne.

Le poste maître de sécurité transmet RNO = 0 lors de la transmission de la commande Etablir connexion.

11.8.3 Vérification des esclaves de sécurité

11.8.3.1 Généralités

Le processus de vérification des informations sur les produits confirme que les postes esclaves de sécurité connectés sont adaptés aux postes esclaves de sécurité actuellement définis selon les paramètres de réseau du poste maître de sécurité, afin de détecter les défauts de connexion et de configuration. Un appareil esclave de substitution qui n'est pas un esclave de sécurité est détecté et désactivé au démarrage.

11.8.3.2 Processus de vérification des informations sur les esclaves de sécurité

Le processus de vérification des informations sur les esclaves de sécurité est décrit dans le Tableau 18.

Tableau 18 – Détails du processus de vérification des informations sur les esclaves

Type de SAREP	Détails du processus
Maître de sécurité	(1) Lire les informations sur les produits fournies par les esclaves de sécurité, et vérifier ces informations par rapport aux informations sur les produits définies selon les paramètres de réseau. (2) Après vérification, transmettre les informations sur les produits aux postes esclaves de sécurité.
Esclave de sécurité	(1) Vérifier les informations sur les produits de l'esclave par rapport aux informations sur les produits reçues par le maître de sécurité.

Le processus de vérification des informations sur les esclaves vérifie les informations sur les produits fournies par les esclaves de sécurité.

11.8.3.3 Transmission des paramètres d'esclaves de sécurité

Le maître de sécurité transmet les paramètres de configuration des esclaves de sécurité à chaque esclave de sécurité. Ce processus est décrit dans le Tableau 19.

Tableau 19 – Détails du processus de transmission des paramètres des esclaves de sécurité

Type de SAREP	Détails du processus
Maître de sécurité	(1) Lire le CRC32 des paramètres de la mémoire ROM issus des postes esclaves de sécurité, et vérifier ce CRC32 avec le CRC32 des paramètres de la mémoire ROM enregistrés issus de l'utilisateur SCL. (2) Transmettre les paramètres des esclaves de sécurité à l'esclave de sécurité.
Esclave de sécurité	(1) Recevoir les paramètres de l'esclave de sécurité issus du maître de sécurité, confirmer les valeurs de réglage et exécuter un processus d'enregistrement interne.

11.9 Exigences système pour FSCP 8/1

11.9.1 Voyants et commutateurs

11.9.1.1 Commutateurs

Chaque appareil de sécurité doit fournir les moyens physiques qui permettent de régler les éléments suivants:

– activé (en ligne) – régler ce mode pour établir une liaison de données;

– nombre de postes – 0: Maître de sécurité, 1 à 64: Esclave de sécurité – exigé uniquement pour l'esclave de sécurité;

– ID de liaison – 0 à 7;
– débit en baud – 156 kbit/s, 625 kbit/s, 2,5 Mbit/s, 5 Mbit/s, 10 Mbit/s – exigé uniquement pour le maître de sécurité;
– réinitialisation – exigé uniquement pour l'esclave de sécurité;

et fournit éventuellement les moyens physiques qui permettent de régler les éléments suivants:

– nombre de créneaux occupés – créneaux de postes (1 ou 2) occupés par un poste esclave de sécurité;
– essai de ligne 1 – vérifie que le maître est capable de se connecter à tous les postes esclaves;
– essai de ligne 2 – vérifie que le maître est capable de se connecter à un poste esclave spécifique;
– essai de vérification de paramètres – vérifie le contenu des paramètres;
– essai de matériel – vérifie que chaque module individuel fonctionne normalement.

11.9.1.2 Voyants

Les exigences relatives aux voyants sont spécifiées dans le Tableau 20 avec l'interprétation suivante:

M = obligatoire (mandatory);

O = facultatif (optional).

Le type, la couleur et la forme des voyants ne sont pas spécifiés. De même, lorsque des ordinateurs ou autres appareils avec écrans sont utilisés, l'indication peut être prise en charge par une indication visuelle sur l'écran.

Tableau 20 – LED du moniteur

Nº	Nom de LED	Description	Poste de maître de sécurité	Poste d'appareil distant de sécurité	Poste E/S distant de sécurité
1	RUN	Allumée: module normal Sortie: erreur de temporisateur de chien de garde	M	O	O
2	ERR	Allumée: erreur de communication avec tous les postes Cette LED s'allume lorsque l'une des situations suivantes se produit: · erreur de réglage des commutateurs · duplication du poste maître sur la même ligne · erreur de contenu des paramètres · activation du temporisateur de contrôle de liaison de données · rupture des conducteurs de câble ou câble influencé par le bruit sur le chemin de transmission Clignotement: erreur de communication	M	O	O
3	L RUN	Allumée: exécution de la liaison de données en cours	M	O	O
4	L ERR	Allumée: erreur de communication (poste automatique) Clignotement: modification du paramétrage du type de commutateur sous tension (position ON)	M	O	O

11.9.2 Lignes directrices d'installation

Le présent document spécifie le protocole et les services d'un système de communication de sécurité qui repose sur le Type 18 de l'IEC 61158. L'utilisation d'appareils de sécurité avec le protocole de sécurité spécifié dans le présent document exige une installation correcte.

Des informations supplémentaires relatives à l'installation sont également données en [30] et [31] de la Bibliographie.

11.9.3 Temps de réponse de la fonction de sécurité

11.9.3.1 Généralités

Comme indiqué en 11.5.3, un temporisateur de chien de garde intégré indique le délai de chaque canal de sortie de chaque esclave de sortie de sécurité. Il assure un temps de réponse de la fonction de sécurité.

En cas de dépassement du temps de réponse de la fonction de sécurité 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 OFF (Inactif).

11.9.3.2 Calcul du temps

Un temporisateur de chien de garde intégré qui indique le délai de chaque canal de sortie de chaque esclave de sortie de sécurité assure un temps de réponse de la fonction de sécurité, 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 ou les canaux de sortie correspondants de l'esclave ou des esclaves de sortie de sécurité, hors temps de traitement de l'entrée de sécurité.

Le temps de réponse de la fonction de sécurité 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.

Le temps de réponse de la fonction de sécurité est calculé comme la somme de (a) à (f) indiquée dans le Tableau 21 avec les termes définis dans le Tableau 22.

NOTE 1 Le maître de sécurité calcule la temporisation en se fondant sur le temps de contrôle du rafraîchissement des données de sécurité – ((WDT × n) × 2).

NOTE 2 (WDT × n) × 2 est le temps exigé par le maître de sécurité pour transmettre les données de communication.

Tableau 21 – Calcul du temps de réponse de la fonction de sécurité

Elément	Maximum
(a) Temps de réponse de l'appareil d'entrée	DT1
(b) Temps de traitement de l'entrée de l'esclave de sécurité	Temps de traitement du filtre de suppression de bruit + Temps de traitement du poste d'entrée distant
(c) Temps de contrôle entre l'entrée et la sortie de sécurité	Temps de contrôle des données de sécurité
(d) Temps de traitement de la sortie de l'esclave de sécurité	Temps de traitement du poste de sortie distant
(e) Temps de réponse de l'appareil de sortie	DT2
Total	(a)+(b)+(c)+(d)+(e)

Tableau 22 – Définitions des termes relatifs au temps de réponse de la fonction de sécurité

Elément	Définition
LS	Temps d'analyse de liaison spécifié par le fabricant
n	Valeur après la décimale de LS/WDT (arrondie à l'unité supérieure la plus proche)
SRRP	Temps de traitement de la réponse de rafraîchissement des données de sécurité. Comme spécifié par le fabricant
m	Valeur après la décimale de SRRP/(WDT × n) (arrondie à l'unité supérieure la plus proche)
Temps de traitement du filtre de suppression de bruit	Configuré selon les paramétrages du poste distant de sécurité (Valeur de réglage: 1 ms à 50 ms)
DT1, DT2	Temps de réponse du capteur ou appareil de contrôle de la destination de sortie. Comme spécifié par le fabricant.
Temps de contrôle des données de sécurité	Temps défini dans le paramètre de réseau. Utiliser la valeur issue de la formule suivante comme la mesure: Temps de contrôle de rafraîchissement des données de sécurité × 2 – ((WDT × n) × m) – 10 [ms]
Temps de contrôle de rafraîchissement des données de sécurité	Temps défini dans le paramètre de réseau. Utiliser la valeur obtenue par la formule de calcul suivante comme la mesure: En mode déclenché: (WDT × n) × 3 + (WDT × n) × m × 2 + (WDT × α) [ms] En mode libre: (WDT × n) × 3 + LS + (WDT × n) × m × 2 + (WDT × α) [ms] où: α = 0, pour LS ≤ 1,5 ms α = 1, pour LS > 1,5 ms
WDT (Temporisateur de chien de garde)	Temps défini dans le paramètre de configuration.
Mode déclenché	Mode qui exécute la liaison de données lorsque l'analyse de séquence est synchronisée avec l'analyse de liaison. En mode déclenché, l'analyse de séquence et l'analyse de liaison commencent de manière simultanée
Mode libre	Mode qui exécute la liaison de données sans synchronisation du programme de séquences

11.9.4 Durée des demandes (ou sollicitations)

La durée de la sollicitation entre l'application relative à la sécurité et la couche de communication de sécurité doit être suffisante de manière à ce que la sollicitation soit détectée par l'application dans le cadre du temps de réponse le plus long de la fonction de sécurité.

11.9.5 Contraintes liées au calcul des caractéristiques du système

Un système de sécurité FSCP 8/1 doit respecter les contraintes suivantes:

– type 18 de l'IEC 61158: Aucune restriction;
– nombre maximal de créneaux de sécurité: 64;
– durée minimale du cycle d'analyse: 10 ms;
– nombre maximal de bits E/S de sécurité par PDU de sécurité – esclave à maître: 208;
– nombre maximal de bits E/S de sécurité par PDU de sécurité – maître à esclave: 7 168.

11.9.6 Maintenance

Aucune exigence spécifique à la SCL pour la maintenance n'est exigée.

Les spécifications du comportement du système en cas de réparation et de remplacement de l'appareil n'entrent pas dans le domaine d'application du présent document. La spécification de ces activités et les responsabilités ne concernent pas la spécification des services et des protocoles. En règle générale, cela fait partie intégrante d'un plan de gestion de sécurité fonctionnelle. Toutefois, la réparation, le remplacement et la maintenance, la validation de la sécurité globale, le fonctionnement global, les modifications, les mises à niveau et le déclassement ou la mise au rebut conformément à l'IEC 61508 sont des questions importantes qui doivent être prises en compte. Il est également recommandé de prendre contact avec le fournisseur de l'appareil ou du système.

Pour obtenir des informations relatives à la programmation du SRP et à la définition des paramètres des appareils de sécurité, il est vivement recommandé de prendre contact avec le fournisseur de l'appareil ou du système. Il est également recommandé de s'appuyer sur les documents [30] et [31]. Dans ces documents, des informations supplémentaires, par exemple, des listes de contrôle, sont données à l'intention de l'utilisateur d'un système CC-LINK-Safety.

NOTE Des exigences de maintenance supplémentaires (entre autres) sont spécifiées dans l'IEC 61508, l'IEC 61511 et/ou l'IEC 62061.

11.9.7 Manuel de sécurité

Le fournisseur d'esclaves de sécurité qui intègre la SCL conformément aux spécifications correspondantes données dans le présent document doit élaborer un manuel de sécurité approprié conformément à l'IEC 61508. Ce manuel de sécurité doit également comprendre les exigences d'installation spécifiées en 11.9.2, ainsi que les lignes directrices applicables à la configuration des commutateurs d'appareil. Outre les commutateurs communs au Type 18 de l'IEC 61158, ces lignes directrices doivent inclure l'indication selon laquelle tous les appareils de sécurité présents sur le même réseau doivent être configurés avec le même ID de liaison. Voir 11.9.1.1.

Selon le système de communication de sécurité qui repose sur le Type 18 de l'IEC 61158, il est vivement recommandé de tenir compte des spécifications [30], [31] et [32].

NOTE Avant de commencer la mise en œuvre d'un appareil de sécurité, il est judicieux de prendre contact avec la CPLA pour déterminer si des modifications ont été apportées aux lignes directrices et/ou exigences de mise en œuvre.

11.10 Evaluation de FSCP 8/1

Il revient au fabricant de développer l'appareil en fonction des processus appropriés conformes aux normes de sécurité (voir l'IEC 61508, l'IEC 61511, l'IEC 62061, etc.) et aux règlements juridiques pertinents (Directive européenne relative aux machines, par exemple). Des informations complémentaires sont fournies à l'Annexe B.

12 FSCP 8/2

12.1 Domaine d'application – FSCP 8/2

Voir Article 1.

12.2 Références normatives – FSCP 8/2

Voir Article 2.

12.3 Termes, définitions, symboles, abréviations et conventions – FSCP 8/2

Voir Article 3.

12.4 Présentation de FSCP 8/2 (fonction de communication de sécurité CC-Link IE™)

Le profil de communication 8/4 et 8/5 (communément appelé CC-Link IE™[4]) définit les profils de communication qui reposent sur l'ISO/IEC/IEEE 8802-3, l'IEC 61158-5-23 et l'IEC 61158-6-23.

Les profils de base CP 8/4 et CP 8/5 sont définis dans l'IEC 61784-2. Le profil de communication de sécurité fonctionnelle CPF 8 FSCP 8/2 (fonction de communication de sécurité CC-Link IE™[3]) repose sur les profils de base CP 8/4 et CP 8/5 de l'IEC 61784-2 et sur les spécifications de couche de communication de sécurité définies dans le présent document.

Le FSCP 8/2 est un protocole de communication des données relatives à la sécurité telles que les signaux d'arrêt d'urgence entre les participants d'un réseau réparti, en utilisant la technologie de bus de terrain conformément aux exigences de l'IEC 61508 concernant la sécurité fonctionnelle. Ce protocole est utilisé dans différentes applications telles que la commande de processus, l'usinage automatique et les machines.

Le protocole FSCP 8/2 est conçu de manière à prendre en charge le niveau d'intégrité de sécurité SIL 3 (IEC 61508) qui utilise CP 8/4 et CP 8/5, en spécifiant par ailleurs des mécanismes de mise en œuvre de la datation, du délai, de l'authentification de connexion, du message de réaction, de l'assurance d'intégrité des données et de différentes mesures de sécurité dédiées à ladite assurance.

Les capacités SCL de FSCP 8/2 sont fournies avec l'introduction d'éléments de service d'application de sécurité (SASE). Ces SASE sont utilisés à la place de leurs ASE correspondants, comme spécifié dans le présent document. Toutefois, dans la mesure où ces SASE proviennent directement des classes parents définies pour CP 8/4 et CP 8/5, ils spécifient les ajouts exigés à CP 8/4 et CP 8/5 pour la sécurité fonctionnelle, en appliquant la méthode du canal noir.

La construction du maître et de l'esclave donne deux SASE: SASE-M et SASE-S respectivement. Chacun d'eux est géré par une machine de protocole de service FAL, la SFSPM-M et la SFSPM-S, respectivement.

12.5 Généralités – FSCP 8/2

12.5.1 Documents externes de spécifications applicables au profil

Les fabricants d'appareils de sécurité FSCP 8/2 sont encouragés à consulter les Spécifications de sécurité CC-Link, qui donnent des spécifications supplémentaires relatives à la mise en œuvre de la SCL définie dans le présent document.

NOTE Les documents [30] et [31] contiennent des informations importantes relatives à FSCP 8/2.

12.5.2 Exigences fonctionnelles de sécurité

Le présent document spécifie les services et protocoles d'un système de communication de sécurité fonctionnelle qui repose sur le Type 23 de l'IEC 61158. Les technologies de communication spécifiées dans le présent document doivent être mises en œuvre uniquement dans les appareils conçus conformément aux exigences de l'IEC 61508.

---

[4] CC-Link IE™ est une appellation commerciale de l'organisme à but non lucratif CC-Link Partner Association. Cette information est donnée à l'intention des utilisateurs du présent document et ne signifie nullement que l'IEC approuve ou recommande le détenteur de la marque ou de l'un de ses produits. La conformité au présent document n'exige pas l'emploi de l'appellation commerciale CC-Link IE™. L'emploi de l'appellation commerciale CC-Link IE™ exige l'autorisation de la CC-Link Partner Association et la conformité aux conditions d'utilisation (essais et validation).

Les exigences suivantes doivent s'appliquer au développement des appareils qui mettent en œuvre les protocoles FSCP 8/2. Les mêmes exigences ont été utilisées dans le développement de FSCP 8/2.

– Les protocoles FSCP 8/2 sont conçus de manière à prendre en charge le niveau d'intégrité de sécurité 3 (SIL 3) (se reporter à l'IEC 61508).
– Les mises en œuvre des protocoles FSCP 8/2 doivent être conformes à l'IEC 61508.
– Les exigences de base qui s'appliquent au développement du protocole FSCP 8/2 sont spécifiées dans l'IEC 61784-3.
– L'état de sécurité des données discrètes est l'état hors tension (0). Pour les valeurs analogiques, l'état hors tension doit être défini par l'application relative à la sécurité.
– Les conditions environnementales doivent être conformes à l'IEC 61131-2 pour les niveaux de base et aux IEC 61326-3-1 et IEC 61326-3-2 pour les essais de marge de sécurité, à moins que des normes de produits spécifiques existent.
– Sauf spécification explicite dans le présent document, les exigences CPF 8 ne doivent pas être modifiées pour la sécurité.

12.5.3 Mesures de sécurité

12.5.3.1 Généralités

La couche de communication de sécurité décrite dans le présent document fournit les mesures correctives déterministes suivantes pour sa mise en œuvre:

- 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.

Le choix des différentes mesures qui correspondent aux erreurs possibles est présenté dans le Tableau 23.

Tableau 23 – Choix des différentes mesures qui correspondent aux erreurs possibles

Erreurs de communication	Mesures correctives déterministes							
	Numéro de séquence	Datation (horodatage)	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	X [c]	
Répétition non prévue		X						
Séquence incorrecte		X						
Perte		X [a,c]			X [b]			
Retard inacceptable		X [c]	X					
Insertion				X				
Déguisement							X [c]	X
Adressage				X				

[a] Evalué par horodatage reçu.

[b] Utilisé dans le modèle de demande/réponse.

[c] Non utilisé dans le modèle de demande/réponse.

12.5.3.2 Corruption

La corruption est détectée à l'aide des CRC inclus dans le PDU de sécurité. Le nœud de transmission envoie le PDU de sécurité en incluant les CRC calculés. Le nœud de réception compare les CRC inclus dans le PDU de sécurité reçu aux CRC calculés à partir de ce même PDU, puis détermine si une corruption s'est produite. De plus, le nœud récepteur vérifie les parties redondantes du PDU de sécurité reçu afin de vérifier que ces portions correspondent les unes aux autres bit par bit. Si la comparaison des CRC ou le résultat de la contre-vérification ne révèle aucune correspondance, le nœud de réception considère qu'une corruption s'est produite et doit écarter le PDU de sécurité reçu. Si le PDU de sécurité reçu est écarté, le temporisateur delay_detection_timer utilisé pour les délais inacceptables ne doit pas être réinitialisé.

12.5.3.3 Répétition non prévue

La répétition non prévue est la réception répétée d'un PDU de sécurité qui n'est pas le dernier PDU de sécurité avec la temporisation appropriée, après une erreur, une anomalie ou une interférence. L'identité du PDU de sécurité est détectée à l'aide du code T (TS combiné à CC pour former un seul code d'opportunité) inclus dans le PDU de sécurité. Le nœud de transmission envoie des PDU de sécurité qui contiennent un code T.

Le nœud de réception reçoit le PDU de sécurité et conserve son code T afin de détecter la répétition non prévue du PDU de sécurité à la réception suivante. Lors de la réception du PDU de sécurité, le nœud de réception compare le code T inclus dans le PDU de sécurité au code T conservé du PDU de sécurité déjà reçu. Si le code T du PDU de sécurité reçu est identique au code T du PDU déjà reçu, le nœud de réception considère qu'une répétition non prévue s'est produite et doit ignorer le PDU de sécurité reçu. En cas de réception d'un PDU de sécurité qui comporte la même valeur de code T, le temporisateur delay_detection_timer utilisé pour détecter les délais inacceptables ne doit pas être réinitialisé.

La Figure 5 représente la séquence lorsque des PDU de sécurité sont envoyés de SASE-M à SASE-S, et qu'une répétition non prévue est détectée dans SASE-S. De même, lorsqu'un PDU de sécurité est envoyé de SASE-S à SASE-M, une répétition non prévue est détectée par SASE-M sur le nœud de réception.

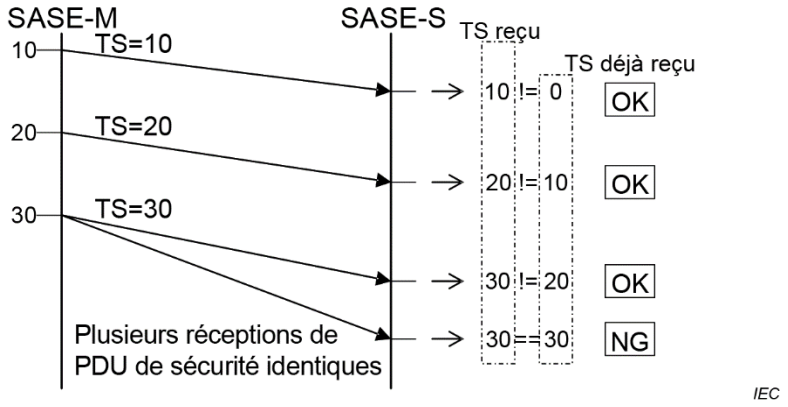


Figure 5 – Détection d'une répétition non prévue

12.5.3.4 Séquence incorrecte

Une séquence incorrecte est la réception de PDU de sécurité par le nœud de réception dans un ordre différent de celui dans lequel les PDU de sécurité ont été envoyés du nœud de transmission. Le TS et le CC sont combinés pour former un seul code T. L'ordre est détecté à l'aide du code T inclus dans les PDU de sécurité. Le nœud de transmission envoie des PDU de sécurité qui contiennent un code T.

Le nœud de réception reçoit un PDU de sécurité dont il conserve le code T. Lors de la réception du PDU de sécurité suivant, le nœud de réception compare le code T inclus dans le PDU de sécurité au code T conservé du PDU de sécurité déjà reçu. Si le code T du PDU reçu est inférieur au code T du PDU déjà reçu, le nœud de réception considère que l'ordre est incorrect, et doit interrompre la connexion de sécurité.

La Figure 6 représente la séquence lorsque des PDU de sécurité sont envoyés de SASE-M à SASE-S, et qu'un ordre incorrect est détecté dans SASE-S. De même, lorsqu'un PDU de sécurité est envoyé de SASE-S à SASE-M, un ordre incorrect est détecté par SASE-M sur le nœud de réception.

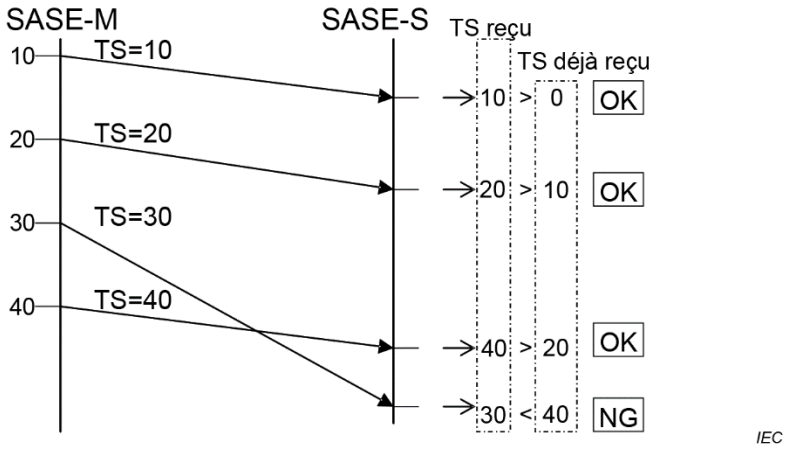


Figure 6 – Détection d'une séquence incorrecte

12.5.3.5 Perte

La perte est détectée à l'aide du code T.

SASE-M envoie régulièrement des PDU de sécurité à SASE-S en fonction de l'intervalle de transmission SASE-M (transmission_interval). Le code T inclus dans le PDU de sécurité envoyé par SASE-M est la valeur de l'horloge de sécurité lors de la transmission du PDU de sécurité. SASE-S envoie régulièrement des PDU de sécurité à SASE-M en fonction de l'intervalle de transmission SASE-S (transmission_interval). Le code T inclus dans le PDU de sécurité envoyé par SASE-S est une valeur calculée en fonction de la valeur de l'horloge de sécurité pendant la transmission du PDU de sécurité et du décalage ts_offset avec SASE-M.

Le nœud de réception reçoit un PDU de sécurité, vérifie que son code T n'est pas supérieur à la somme de transmission_interval du nœud de transmission ajouté au code T du PDU de sécurité déjà reçu, et considère qu'une perte s'est produite si tel est le cas. Si une perte est détectée, le nœud de réception doit interrompre la connexion de sécurité.

La Figure 7 représente la séquence lorsque des PDU de sécurité sont envoyés de SASE-M à SASE-S, et qu'une perte est détectée dans SASE-S. De même, lorsqu'un PDU de sécurité est envoyé de SASE-S à SASE-M, une perte est détectée dans SASE-M sur le nœud de réception.

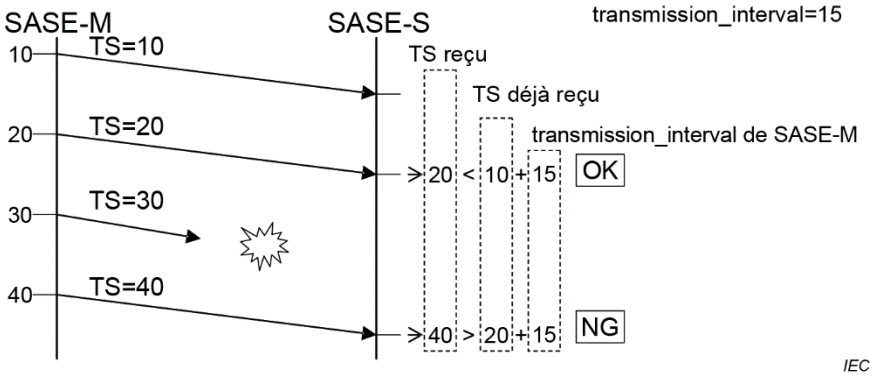


Figure 7 – Détection d'une perte

12.5.3.6 Retard inacceptable

Un retard inacceptable est détecté à l'aide des temporisateurs et du code T.

SASE-M envoie régulièrement des PDU de sécurité à SASE-S en fonction de l'intervalle de transmission SASE-M (transmission_interval). Le code T inclus dans le PDU de sécurité envoyé par SASE-M est la valeur de l'horloge de sécurité lors de la transmission du PDU de sécurité. SASE-S envoie régulièrement des PDU de sécurité à SASE-M en fonction de l'intervalle de transmission SASE-S (transmission_interval). Le code T inclus dans le PDU de sécurité envoyé par SASE-S est la somme de la valeur de l'horloge de sécurité lors de la transmission du PDU de sécurité et du décalage ts_offset avec SASE-M.

SASE-S sur le nœud de réception reçoit un PDU de sécurité de la part de SASE-M, enregistre la valeur de l'horloge de sécurité au moment de la réception du PDU de sécurité et lance ou réinitialise le temporisateur delay_detection_timer. SASE-S calcule la différence entre la somme de la valeur de l'horloge de sécurité enregistrée et le décalage ts_offset et le code T reçu, puis calcule la valeur de retard entre SASE-M et SASE-S. Si la valeur calculée ne satisfait pas la condition suivante qui tient compte de la dispersion de décalage (offset_dispersion), le nœud de réception considère qu'un retard inacceptable s'est produit.

offset_dispersion < value calculée < allowable_delay + offset_dispersion

Si aucun PDU de sécurité valide n'est reçu avant l'expiration du temporisateur delay_detection_timer, qui se produit à allowable_refresh_interval, le nœud de réception considère qu'un retard inacceptable s'est produit. Si cela se produit, SASE-S doit interrompre la connexion de sécurité.

SASE-M sur le nœud de réception reçoit un PDU de sécurité de la part de SASE-S, enregistre la valeur de l'horloge de sécurité au moment de la réception du PDU de sécurité et lance ou réinitialise le temporisateur delay_detection_timer. SASE-M calcule la différence entre la valeur de l'horloge de sécurité enregistrée et le code T reçu, puis calcule la valeur de retard entre SASE-S et SASE-M. Si la valeur calculée ne satisfait pas à la formule d'évaluation SASE-S décrite ci-dessus, le nœud de réception considère qu'un retard inacceptable s'est produit. De plus, si un PDU de sécurité valide ne peut pas être reçu avant l'expiration de delay_detection_timer, le nœud de réception considère qu'un retard inacceptable s'est produit. Si cela se produit, SASE-M doit interrompre la connexion de sécurité.

La Figure 8 représente la séquence lorsque des PDU de sécurité sont envoyés de SASE-M à SASE-S et qu'un retard inacceptable est détecté par les horodatages dans SASE-S. La Figure 9 présente un cas dans lequel un retard inacceptable est détecté par un temporisateur dans SASE-S. De même, lorsqu'un PDU de sécurité est envoyé de SASE-S à SASE-M, un retard inacceptable est détecté dans SASE-M sur le nœud de réception.

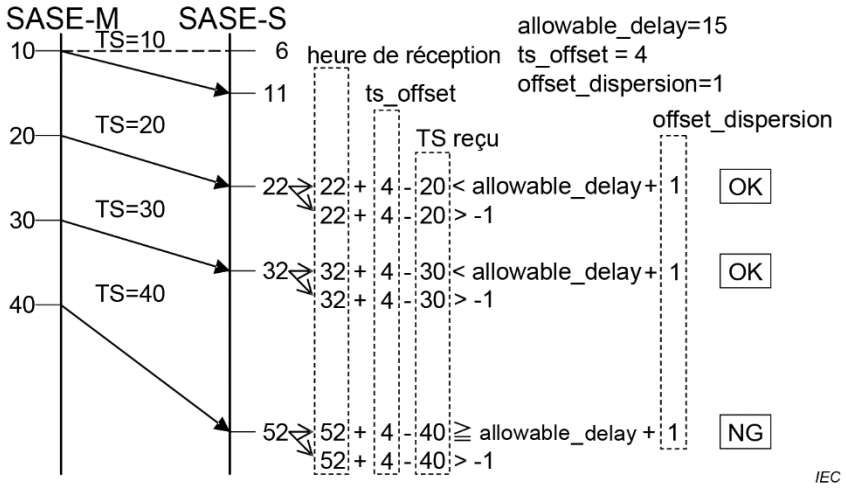


Figure 8 – Détection d'un retard inacceptable par les horodatages

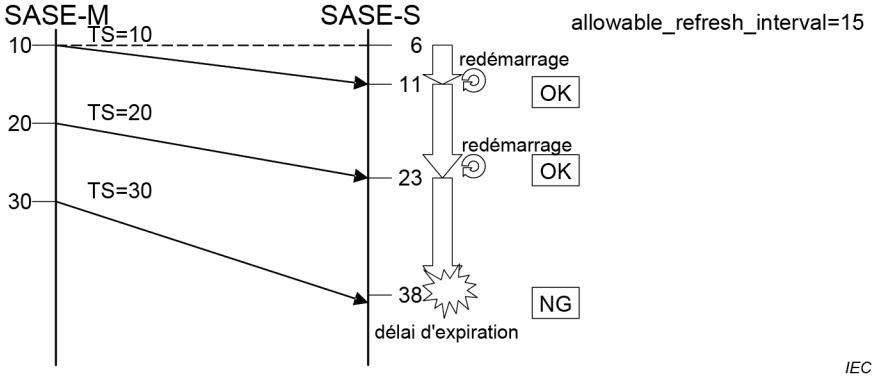


Figure 9 – Détection d'un retard inacceptable par le temporisateur

12.5.3.7 Insertion

L'insertion consiste à insérer un message en provenance d'une source de transmission imprévue ou inconnue. L'insertion est détectée à l'aide de l'identifiant de connexion de sécurité connection_id (CID) inclus dans le PDU de sécurité. Le nœud de transmission envoie un PDU de sécurité dont le CID contient le connection_id.

Le nœud de réception compare le CID inclus dans le PDU de sécurité au connection_id fixé par accord au moment de l'établissement de la connexion, puis détermine s'ils correspondent. S'ils ne correspondent pas, le nœud de réception doit ignorer le PDU de sécurité reçu. Si le PDU de sécurité reçu est ignoré, le temporisateur delay_detection_timer utilisé pour détecter les retards inacceptables ne doit pas être réinitialisé.

12.5.3.8 Déguisement

Le déguisement est la réception d'un message non relatif à la sécurité par un poste de sécurité et l'insertion du message en provenance de ce qui semble être une source de transmission valide par suite d'une anomalie ou d'une interférence. Un déguisement est détecté à l'aide des CRC générés par un polynôme générateur différent de celui d'une communication non relative à la sécurité, en plus de la validation des contraintes de données spécifiques au protocole SCL dans le PDU reçu.

Le nœud de transmission envoie un PDU de sécurité qui contient les CRC calculés. Le nœud de réception compare les CRC inclus dans le PDU de sécurité aux CRC calculés à partir du PDU de sécurité reçu. De plus, le nœud récepteur vérifie les parties redondantes du PDU de sécurité reçu afin de vérifier que ces portions correspondent les unes aux autres bit par bit. Si les deux ne correspondent pas, ou si d'autres données attendues ne sont pas conformes aux contraintes d'un PDU de sécurité correctement défini, le nœud de réception doit ignorer le PDU de sécurité reçu. Si le PDU de sécurité reçu est ignoré, le temporisateur delay_detection_timer utilisé pour détecter les retards inacceptables ne doit pas être réinitialisé.

12.5.3.9 Adressage

L'adressage, ou l'authentification, est la transmission d'un message de sécurité au mauvais poste de sécurité, et son traitement comme message incorrect après une anomalie ou une interférence. L'adressage est détecté à l'aide de l'identifiant de connexion de sécurité connect_id inclus dans le PDU de sécurité.

Le nœud de transmission envoie un PDU de sécurité dont le CID contient le connection_id. Le nœud de réception compare le CID inclus dans le PDU de sécurité au connection_id fixé par accord au moment de l'établissement de la connexion, puis détermine s'ils correspondent. S'ils ne correspondent pas, le nœud de réception doit ignorer le PDU de sécurité reçu. Si le PDU de sécurité reçu est ignoré, le temporisateur delay_detection_timer utilisé pour détecter les retards inacceptables ne doit pas être réinitialisé.

12.5.4 Structure de la couche de communication de sécurité

La hiérarchie de protocole du poste de sécurité est composée de la hiérarchie de protocole de CP 8/4 et CP 8/5 (ISO/IEC/IEEE 8802-3 et FAL Type 23) qui sert de fondement, de la couche de communication de sécurité FSCP 8/2 qui met en œuvre la communication de sécurité, et des applications relatives à la sécurité. Cette hiérarchie est représentée (pour CP 8/5) à la Figure 10.

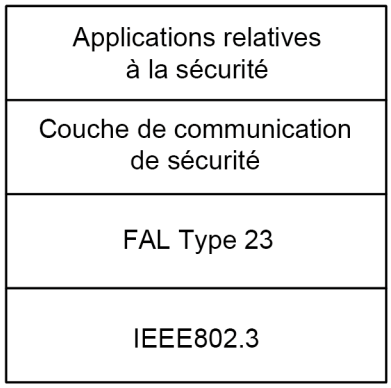


Figure 10 – Hiérarchie de protocole

12.5.5 Relations avec la FAL (et DLL PhL)

12.5.5.1 Généralités

Il n'existe aucune exigence FAL autre que celles énoncées dans le présent document.

FSCP 8/2 utilise les services de la FAL CP 8/4, CP 8/5. La livraison de données de sécurité utilise le service de transmission transitoire. Le CP 8/4 utilise les services "Read memory" et "Write memory", et le CP 8/5 utilise le service "AC Send ND". Les deux sont décrits dans la FAL Type 23.

12.5.5.2 Types de données

Les types de données de sécurité sont spécifiés dans l'IEC 61158-5-23.

12.6 Services de la couche de communication de sécurité pour FSCP 8/2

12.6.1 Généralités

Le FSCP 8/2 est structuré autour de deux diagrammes d'états: le SFSPM-M du maître de sécurité et le SFSPM-S de l'esclave de sécurité, les transitions d'état étant réalisées par l'intermédiaire des services décrits en 12.6. Les applications relatives à la sécurité utilisent les services d'application de sécurité pour communiquer par l'intermédiaire de la couche de communication de sécurité.

12.6.2 Services de rétablissement de la connexion

12.6.2.1 SS-Start

SS-Start est un service utilisé pour demander le lancement de la communication de sécurité. Le Tableau 24 présente les paramètres de SS-Start.

Tableau 24 – SS-Start

Nom de paramètre	Req	Ind	Rsp	Cnf
Argument	M	M(=)		
ConnectionID	M	M(=)		

ConnectionID
Spécifie l'ID de la connexion de sécurité qui doit lancer la communication de sécurité. Sa taille est de 32 bits.

12.6.2.2 SS-Restart

SS-Restart est un service utilisé pour demander la relance de la communication de sécurité. Le Tableau 25 présente les paramètres de SS-Restart.

Tableau 25 – SS-Restart

Nom de paramètre	Req	Ind	Rsp	Cnf
Argument	M	M(=)		
ConnectionID	M	M(=)		

ConnectionID
Spécifie l'ID de la connexion de sécurité qui doit relancer la communication de sécurité. Sa taille est de 32 bits.

12.6.2.3 SS-InvokeFunc

SS-InvokeFunc est un service utilisé pour demander l'exécution d'une commande d'application de sécurité. Le Tableau 26 présente les paramètres de SS-InvokeFunc.

Tableau 26 – SS-InvokeFunc

Nom de paramètre	Req	Ind	Rsp	Cnf
Argument	M	M(=)		
ConnectionID	M	M(=)		
Command	M	M(=)		
Data	C	C(=)		
Result			C	C(=)
R Data			C	C(=)

ConnectionID
Spécifie l'ID de la connexion de sécurité cible. Sa taille est de 32 bits.

Command
Spécifie la commande à exécuter.

Data
Spécifie les informations relatives à la commande à exécuter.

R Data
Contient les informations renvoyées par le service exécuté.

12.6.3 Services de transmission de données

12.6.3.1 SS-Read

Ce service est utilisé pour lire les données de sécurité d'une taille spécifiée dans une mémoire cyclique de sécurité. Le Tableau 27 indique les paramètres de ce service.

Tableau 27 – SS-Read

Nom de paramètre	Req	Ind	Rsp	Cnf
Argument	M	M(=)		
Address	M	M(=)		
Size	M	M(=)		
Result			M	M(=)
R Data			M	M(=)

Address
Spécifie l'adresse de tête de mémoire cible.

Size
Spécifie la taille de la mémoire cible (unités binaires).

Data
Contient le contenu de la mémoire en lecture.

12.6.3.2 SS-Write

Ce service est utilisé pour écrire les données de sécurité d'une taille spécifiée dans une mémoire cyclique de sécurité. Le Tableau 28 indique les paramètres de ce service.

Tableau 28 – SS-Write

Nom de paramètre	Req	Ind	Rsp	Cnf
Argument	M	M(=)		
Address	M	M(=)		
Size	M	M(=)		
Data	M	M(=)		

Address
Spécifie l'adresse de tête de mémoire cible.

Size
Spécifie la taille de la mémoire cible (unités binaires).

Data
Spécifie les données de sécurité à écrire dans la mémoire cible.

12.6.4 Service de notification de fin de connexion

12.6.4.1 SS-Terminate

Ce service est utilisé pour émettre une notification de fin de la connexion de sécurité. Le Tableau 29 indique les paramètres de ce service.

Tableau 29 – SS-Terminate

Nom de paramètre	Req	Ind	Rsp	Cnf
Argument		M		
CID		M		

CID
Spécifie le CID de la connexion de sécurité terminée.

12.7 Protocole de couche de communication de sécurité pour FSCP 8/2

12.7.1 Format PDU de sécurité

12.7.1.1 Structure du PDU de sécurité

La Figure 11 représente la structure du PDU de sécurité utilisé par la fonction de communication de sécurité FSCP 8/2. S-Data indique la zone de données de sécurité et stocke les données d'entrée de sécurité ou les données de sortie de sécurité. La taille maximale de S-Data est de 800 bits.

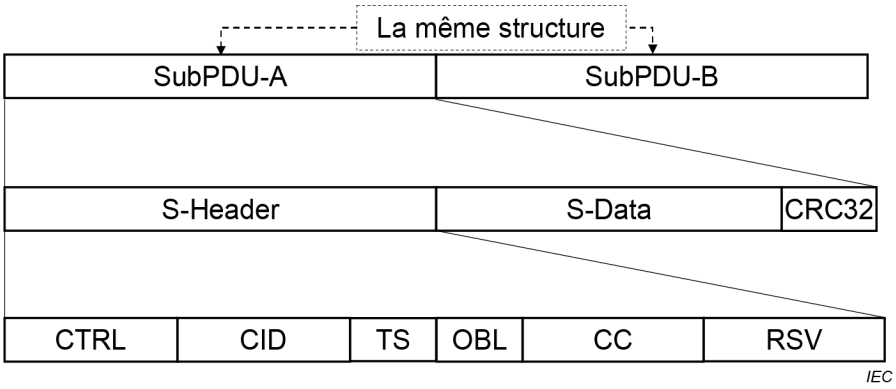


Figure 11 – Structure du PDU de sécurité

Le Tableau 30 indique les noms, tailles et contenus des éléments qui composent le PDU de sécurité. Une seule instance d'un sous-PDU est représentée, bien que le sous-PDU soit répétée deux fois, sous les formes sous-PDU A et sous-PDU B, respectivement.

Tableau 30 – Eléments du PDU de sécurité

Attribut	Description	Taille (bits)
S-Header	Structure de 6 éléments:	160
CTRL	Type de commande, état	32
CID	Identifiant de connexion de sécurité	32
TS	Datation (horodatage)	16
OBL	Informations de génération de décalage	16
CC	32 bits supérieurs de l'horloge de sécurité	32
RSV	Réservé pour une utilisation ultérieure	32
S-Data	Données de sécurité (la taille est exprimée en unités de 4 octets)	32 min 800 max
CRC32	Contrôle de redondance cyclique	32

12.7.1.2 CTRL

La Figure 12 représente la configuration de CTRL. Le Tableau 31 décrit le contenu des éléments qui composent CTRL.

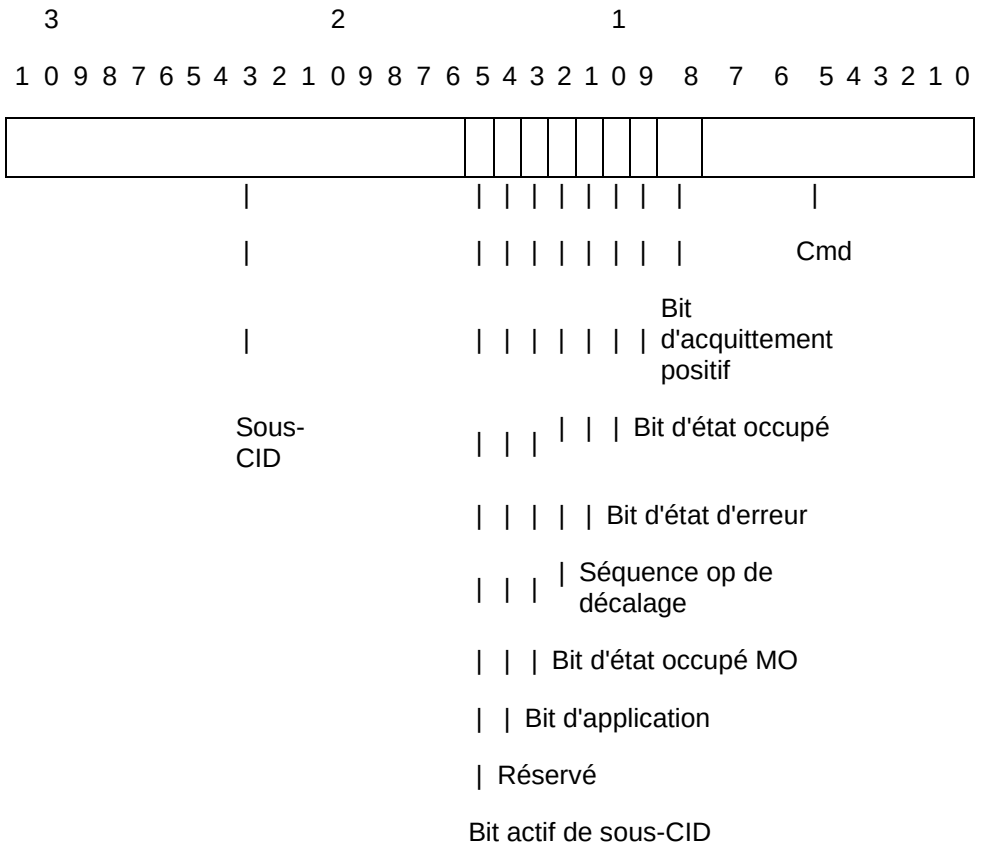


Figure 12 – Configuration CTRL

Tableau 31 – Eléments de CTRL

Elément		Valeur	Description
Cmd	S-Connect	0x00	Etablir la connexion de sécurité
	S-InitConfirmNetPrm	0x01	Confirmer les paramètres de réseau de sécurité
	S-InitVerifyStnPrm	0x02	Vérifier les paramètres du poste de sécurité
	S-InvokeFunc	0x03	Commande d'application de sécurité
	Réservé	0x04 – 0xF8	Pour une extension ultérieure
	S-Dissconnect	0xF9	Fin de la connexion de sécurité
	S-ReadErrorInfo	0xFA	Lire les informations relatives à l'erreur
	S-WriteErrorInfo	0xFB	Emettre la notification d'erreur
	S-RefreshReady	0xFC	Emettre la notification de rafraîchissement de sécurité et mesurer le décalage
	S-RefreshMO	0xFD	Rafraîchissement de sécurité; mesurer le décalage
	S-RefreshGO	0xFE	Rafraîchissement de sécurité; générer le décalage
	S-Refresh	0xFF	Rafraîchissement de sécurité
Bit d'acquittement positif		0x00	Demande
		0x01	Réponse
Bit d'état occupé		0x00	Traitement terminé
		0x01	Traitement non terminé

Elément	Valeur	Description
Bit d'état d'erreur	0x00	Pas d'erreur
	0x01	Erreur
Séquence op de décalage	0x00, 0x01	Mesurage du décalage/numéro de séquence de génération
Bit d'état occupé MO	0x00	Traitement terminé
	0x01	Traitement non terminé
Bit d'application	0x00, 0x01	Bit d'application
Réservé	—	Pour une extension ultérieure
Bit actif de sous-CID	0x00	Sous-CID inactif
	0x01	Sous-CID en cours d'utilisation
Sous-CID	0x0000 – 0xFFFF	Sous-identification de la connexion de sécurité

Cmd
Indique le type de PDU de sécurité.

Bit d'acquittement positif
Indique si Cmd est une demande ou une réponse. 0 indique une demande et 1 une réponse.

Bit d'état occupé
Indique si le traitement dont fait l'objet Cmd par le nœud de transmission s'est terminé à un moment différent du rafraîchissement de sécurité. 0 indique que le processus de demande est terminé, et 1 que le processus de demande n'est pas terminé. La valeur du Bit d'état occupé doit être 0 pendant le rafraîchissement de sécurité.

Si Cmd est envoyé et que la valeur du Bit d'état occupé est 1, SASE-M doit envoyer le même Cmd avec le Bit d'état occupé défini sur 0 à l'issue du traitement qui a généré le Bit d'état occupé. A la réception d'un PDU de sécurité dont le Bit d'état occupé est défini sur 1, SASE-M ignore le PDU de sécurité reçu, relance roundtrip_time, puis renvoie le même Cmd. A la réception d'un PDU de sécurité dont le Bit d'état occupé est défini sur 1, SASE-S ignore le PDU de sécurité reçu, relance roundtrip_timer, puis envoie une réponse avec le Bit d'état occupé défini sur 0.

Bit d'état d'erreur
Indique l'état d'erreur. 0 indique l'absence d'erreur et 1 la présence d'une erreur. Le Bit d'état d'erreur est défini sur 1 entre le moment où une erreur se produit et le moment où elle est résolue.

Séquence op de décalage
Permet d'associer les demandes envoyées par SASE-M aux réponses envoyées par SASE-S au moment du mesurage du décalage et de la génération du décalage. La Séquence op de décalage est utilisée lorsque Cmd est:

S-RefreshReady;

S-RefreshMO; ou

S-RefreshGO.

Sa valeur initiale est 0. D'autre part, SASE-M spécifie 0 et 1 à chaque mesurage du décalage. Avec la génération du décalage mise en œuvre à la suite du mesurage du décalage, la valeur utilisée avec le mesurage du décalage est utilisée comme Séquence op de décalage. SASE-S utilise la valeur de Séquence op de décalage dans une demande en provenance de SASE-M en tant que réponse de Séquence op de décalage.

NOTE 1 Lors du mesurage du décalage et de la génération du décalage qui suit, le mesurage du décalage et la génération du décalage sont associés par la même valeur que Séquence op de décalage.

Bit d'état occupé MO
Indique si le traitement du nœud de transmission est terminé ou pas pour le mesurage du décalage lors du rafraîchissement de sécurité. 0 indique que le traitement est terminé, et 1 qu'il ne l'est pas. Lors de la réception d'un PDU de sécurité avec un Bit d'état occupé MO défini sur 1, le redémarrage doit avoir lieu si roundtrip_timer a été lancé. Lors de la transmission d'un PDU de sécurité avec un bit d'état occupé MO défini sur 1, le nœud de transmission ne lance pas roundtrip_timer.

NOTE 2 Le Bit d'état occupé MO est utilisé pour relancer roundtrip_timer uniquement. Il n'étend pas l'intervalle d'interpolation de décalage d'horloge.

Bit d'application
Utilisé pour indiquer l'identité de l'application spécifique à l'appareil.

Bit actif de sous-CID
Indique la validité du sous-CID. 0 indique que le sous-CID est inactif et qu'il s'agit donc d'un champ non valide. 1 indique que le sous-CID est utilisé et donc valide.

Sous-CID
Indique l'identité d'une sous-connexion dans un CID donné. Utilisé uniquement si le bit actif de sous-CID est défini sur 1.

12.7.1.3 CID

Le CID est un identifiant de connexion de sécurité qui indique la relation entre une source de transmission et une destination de transmission. Le CID est généré de manière à inclure l'adresse du SASE-M et l'adresse du SASE-S.

Chaque ensemble de postes de sécurité comporte au maximum deux connexions. Soit n1 le numéro de réseau du poste A, n2 le numéro de poste, n3 le numéro de réseau du poste B et n4 le numéro de poste, les CID sont les suivants:

CID

$CID_1 = ((n1 \times 256 + n2) \times 65536) + (n3 \times 256 + n4)$

$CID_2 = ((n3 \times 256 + n4) \times 65536) + (n1 \times 256 + n2)$

où

CID_1 est le CID de la connexion de sécurité 1

CID_2 est le CID de la connexion de sécurité 2

12.7.1.4 TS et CC

TS est un horodatage qui indique les 16 bits inférieurs d'une horloge de sécurité de 48 bits. Son unité est 128 microsecondes. TS utilise l'horloge de sécurité de SASE-M comme étant sa norme.

NOTE La période de temps traitée par l'horloge de sécurité de 48 bits (unité: 128 microsecondes) est d'environ 1 140 ans.

Lorsque le SASE-M exécute une demande Cmd, la valeur des 16 bits inférieurs de l'horloge de sécurité pendant la demande Cmd doit être stockée dans TS.

Lorsque SASE-S exécute une demande Cmd, la valeur calculée par la formule ci-dessous doit être stockée dans TS. sending_time est la valeur des 16 bits inférieurs de l'horloge de sécurité de SASE-S, et son ts_offset est le décalage de l'horloge de sécurité SASE-M.

Datation (horodatage)

$TS = (sending\_time + ts\_offset) \bmod 2^{16}$

La Figure 13 indique la relation entre les horloges de sécurité SASE-M et SASE-S et le TS lors d'une demande Cmd.

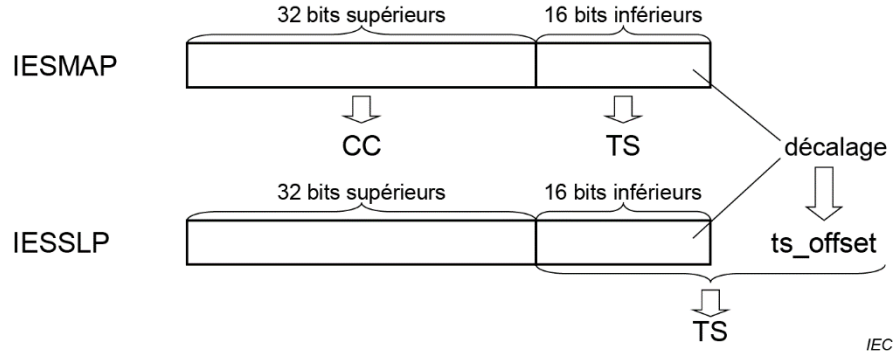


Figure 13 – TS du SASE-M et du SASE-S

Lorsqu'une réponse est envoyée à la demande Cmd, la valeur de TS doit être identique au TS utilisé par le nœud de demande Cmd.

CC représente les 32 bits supérieurs de l'horloge de sécurité de 48 bits. TS et CC se combinent pour former un seul code T.

12.7.1.5 OBL

OBL est une information utilisée pour générer le décalage ts_offset de l'horloge de sécurité. OBL est utilisé dans la demande S-RefreshGO-req envoyée par SASE-M et dans la réponse S-RefreshGO-rsp envoyée par SASE-S.

Les informations stockées dans l'OBL de S-RefreshGO-req sont offset_baseline décrites en 12.7.2.5. Les informations stockées dans l'OBL de S-RefreshGO-rsp sont la valeur de la différence entre le ts_offset calculé et le ts_offset utilisé, également décrit en 12.7.2.5.

12.7.1.6 S-Data

12.7.1.6.1 Structure

S-Data est une zone qui permet de stocker les données de sécurité. Lors du rafraîchissement de sécurité, S-Data utilise le format représenté à la Figure 14, dans lequel safety_data représente les données de rafraîchissement de sécurité. Sa taille minimale est de 32 bits et sa taille maximale est de 800 bits. La longueur de S-Data est variable en unités de 4 octets (par incréments de 32 bits).

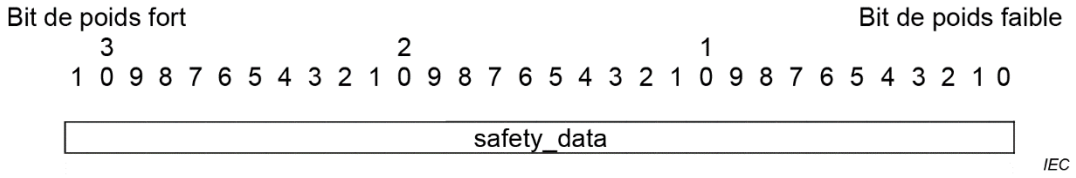


Figure 14 – S-Data lors du rafraîchissement de sécurité

La Figure 15 et la Figure 16 représentent les formats S-Data utilisés à des périodes autres que le rafraîchissement de sécurité.

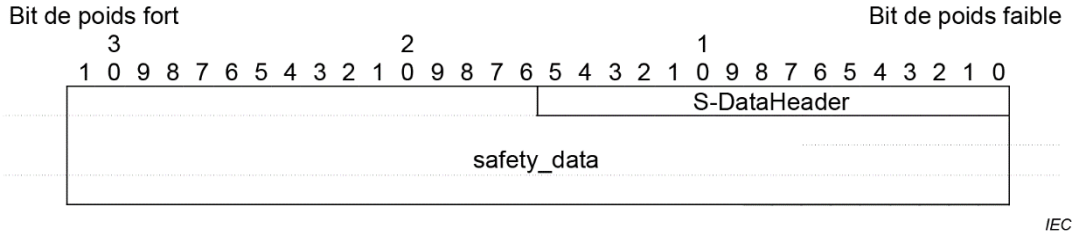


Figure 15 – S-Data hors du rafraîchissement de sécurité

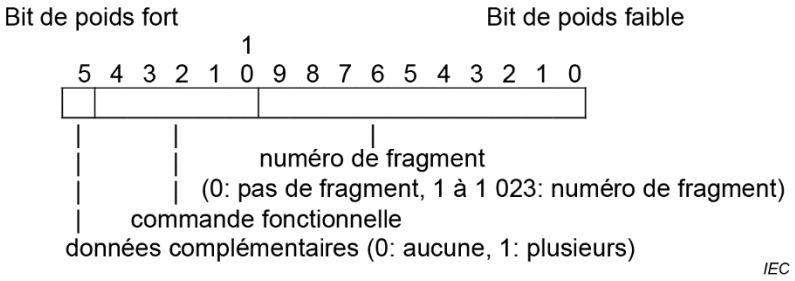


Figure 16 – Configuration d'en-tête S-Data

S-DataHeader
L'en-tête utilisé lors de la transmission des données de sécurité en fragments ou lors de l'exécution d'une commande fonctionnelle.

Numéro de fragment
Indique le numéro de fragment. 0 indique l'absence de fragment, et 1 à 1 023 indique le numéro de fragment.

Commande fonctionnelle
Indique la commande fonctionnelle.

Données complémentaires
Indique la présence ou pas de données complémentaires lorsque les données de sécurité sont transmises en fragments. 0 indique l'absence de données complémentaires et 1 la présence de données complémentaires.

12.7.1.6.2 Fragmentation

Si les données de sécurité sont transmises en fragments, SASE-M attribue la valeur 1 au numéro de fragment du premier S-DataHeader des données de sécurité fragmentées et la valeur 1 aux données complémentaires. Dans le deuxième S-DataHeaders, SASE-M attribue de manière séquentielle une valeur au numéro de fragment par incrément de 1. SASE-M attribue la valeur 0 aux données complémentaires uniquement s'il s'agit du dernier fragment, et la valeur 1 dans les autres cas.

Lorsqu'il est demandé à SASE-S de transmettre les données de sécurité, SASE-M envoie une demande qui contient le numéro de fragment de S-DataHeader défini sur 1 et les données complémentaires définies sur 0. Lorsque SASE-S transmet les données de sécurité en fragments, SASE-S attribue la valeur 1 au numéro de fragment et la valeur 1 aux données complémentaires dans le S-DataHeader des premières données de sécurité fragmentées. Lorsque SASE-M reçoit les premières données de sécurité fragmentées de la part de SASE-S, il envoie une demande en attribuant la valeur 2 au numéro de fragment de S-DataHeader (valeur au moment de la transmission de la demande précédente, augmentée de 1) et la valeur 0 aux données complémentaires. SASE-S entre alors une valeur augmentée de 1 en tant que valeur de fragment du deuxième S-DataHeaders qui suit.

SASE-S entre la valeur 0 pour les dernières données complémentaires uniquement, et 1 pour toutes les autres valeurs de données complémentaires. SASE-M entre toujours une valeur équivalente à la valeur précédente, augmentée de 1 pour les données de fragment de S-DataHeader, et 0 pour les données complémentaires.

12.7.1.7 CRC32

CRC32 est un CRC 32 bits destiné à la communication de sécurité. La formule suivante doit être utilisée comme le polynôme générateur de CRC avec la fonction de communication de sécurité FSCP 8/2.

Polynôme générateur de CRC (0x1F1922815)

$$G(x) = x^{32} + x^{31} + x^{30} + x^{29} + x^{28} + x^{24} + x^{23} + x^{20} + x^{17} + x^{13} + x^{11} + x^{4} + x^{2} + 1$$

NOTE Ce polynôme générateur de CRC est décrit en [32]. Il apparaît judicieux lorsque la longueur du bloc (n), qui est la somme de la longueur du message et de la longueur du CRC, est inférieure à 2 046. Dans la plage $99 \leq n \leq 1\,024$, la distance de Hamming minimale de ce polynôme générateur de CRC est de 8.

CRC32 doit être calculé à l'aide de CRTL, de CID, de TS, d'OBL, de CC, de RSV et de S-Data inclus dans le PDU de sécurité (voir Figure 17).

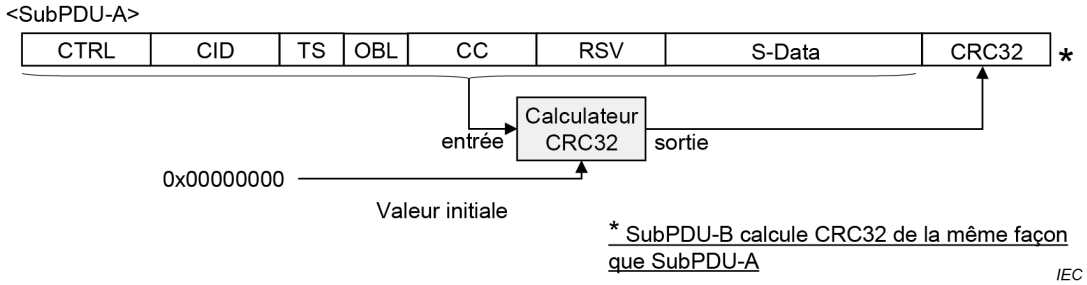


Figure 17 – Calcul de CRC

12.7.2 Machine de protocole de service FAL de sécurité (SFSPM)

12.7.2.1 Présentation générale

Le comportement de la couche de communication de sécurité de FSCP 8/2 est défini par les diagrammes d'états, SFSPM-M et SFSPM-S, à chaque connexion de sécurité. La communication SFSPM-M et SFSPM-S utilise les modèles représentés à la Figure 18 lors des opérations de rafraîchissement de sécurité configurées pour transmettre et recevoir une entrée et une sortie de sécurité, et lors des opérations autres que le rafraîchissement de sécurité.

Lorsque des opérations autres que le rafraîchissement de sécurité sont réalisées, SFSPM-M envoie une demande à SFSPM-S, et SFSPM-S envoie une réponse à SFSPM-M. Lorsque des opérations de rafraîchissement de sécurité sont réalisées, SFSPM-M et SFSPM-S s'envoient indépendamment des demandes l'un à l'autre.

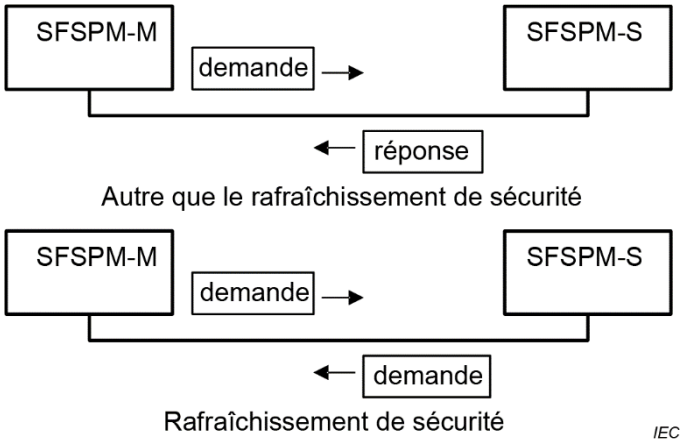


Figure 18 – Modèle de communication

La Figure 19 donne un aperçu des transitions d'état de la couche de communication de sécurité.

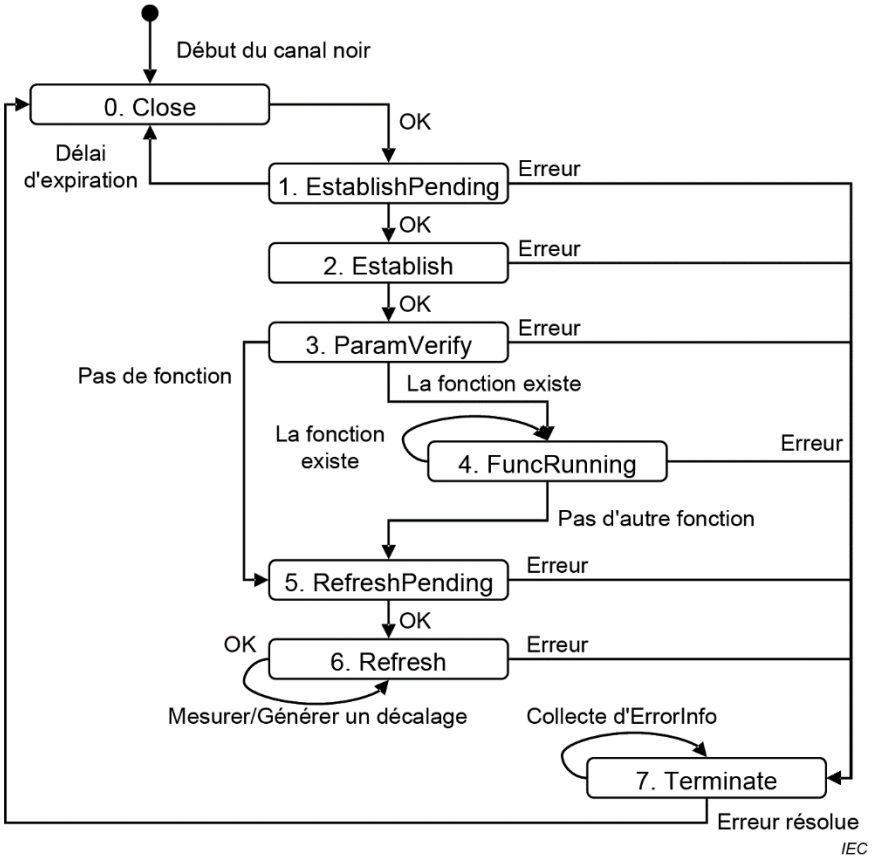


Figure 19 – Diagramme de transition d'état SFSPM

Le Tableau 32 décrit les états représentés à la Figure 19.

Tableau 32 – Liste des états

Nº	Nom de l'état	Etat	Description
0	Close	Connexion de sécurité non établie	Aucune connexion de sécurité n'est établie entre SFSPM-M et SFSPM-S.
1	EstablishPending	En attente d'établissement de la connexion de sécurité	L'établissement d'une connexion de sécurité entre SFSPM-M et SFSPM-S est en attente.
2	Establish	Connexion de sécurité établie	Une connexion de sécurité est établie entre SFSPM-M et SFSPM-S.
3	ParamVerify	Vérification de paramètre	Les paramètres de SFSPM-M et SFSPM-S sont en cours de vérification.
4	FuncRunning	Fonction en cours	Les fonctions auxiliaires de SFSPM-M et de SFSPM-S sont en cours. Pour la fonction auxiliaire exécutable, voir Tableau 35, bits 2 à 31. Cet état est pour une extension ultérieure. Les transitions vers cet état ne se produisent pas.
5	RefreshPending	Rafraîchissement de sécurité en attente	La vérification de l'état prêt du rafraîchissement de sécurité de SFSPM-M et SFSPM-S et le mesurage du décalage de l'horloge de sécurité sont en cours.
6	Refresh	Rafraîchissement de sécurité en cours	SFSPM-M et SFSPM-S échangent actuellement des informations d'entrée/de sortie de sécurité. Au même moment, le mesurage et la génération périodiques du décalage de l'horloge de sécurité sont en cours.
7	Terminate	Connexion de sécurité terminée	Une erreur s'est produite sur SFSPM-M et/ou SFSPM-S et la connexion de sécurité a été interrompue.

12.7.2.2 Comportement

12.7.2.2.1 Initialisation de sécurité

La couche de communication de sécurité établit une connexion de sécurité avant la communication (voir Figure 20). La connexion de sécurité est établie entre SFSPM-M et SFSPM-S selon la séquence suivante:

1) SFSPM-M lance un processus pour établir une connexion de sécurité. SFSPM-M envoie une demande pour établir une connexion de sécurité conformément aux paramètres de connexion de sécurité donnés à l'avance;
2) SFSPM-S confirme que la version de protocole reçue et la taille de S-Data reçue sont correctes;
3) SFSPM-S envoie une demande pour établir une connexion de sécurité;
4) SFSPM-M confirme que la version de protocole reçue et la taille de S-Data reçue sont correctes;
5) SFSPM-M envoie une demande pour appeler les fonctions prises en charge en fonction des informations sur les fonctions prises en charge, qui ont été fixées par accord lors de l'établissement de la connexion de sécurité. SFSPM-M envoie une demande de confirmation du paramètre réseau, qui correspond à la fonction prise en charge;
6) SFSPM-S conserve le paramètre réseau contenu dans la demande et envoie une réponse à la confirmation du paramètre réseau;
7) SFSPM-M conserve le paramètre réseau contenu dans la réponse;
8) SFSPM-M envoie une demande pour vérifier le paramètre du poste de sécurité;
9) SFSPM-S envoie une réponse qui contient un paramètre de poste de sécurité donné à l'avance;
10) SFSPM-M identifie le SFSPM-S comme cible correcte en validant l'information reçue avec des paramètres de sécurité donnés à l'avance;

11) SFSPM-M envoie une autre demande de fonction prise en charge à moins que toutes les fonctions prises en charge ne soient demandées;

12) SFSPM-S envoie la réponse à la demande sauf si les demandes de fonctions prises en charge sont reçues;

13) SFSPM-M envoie une demande de rafraîchissement et de mesurage du décalage;

14) SFSPM-M envoie une réponse de rafraîchissement et de mesurage du décalage;

15) SFSPM-M génère des informations pour calculer le décalage et envoie une demande de rafraîchissement de sécurité et de génération de décalage;

16) SFSPM-S génère un décalage en fonction des informations reçues incluses dans la demande et envoie une réponse;

17) SFSPM-M initie un rafraîchissement de sécurité en envoyant une demande de rafraîchissement de sécurité et de génération de décalage, et envoie une demande de rafraîchissement de sécurité à des intervalles spécifiés;

18) SFSPM-S initie un rafraîchissement de sécurité en envoyant une demande de rafraîchissement de sécurité et de génération de décalage, et envoie une demande de rafraîchissement de sécurité à des intervalles spécifiés.

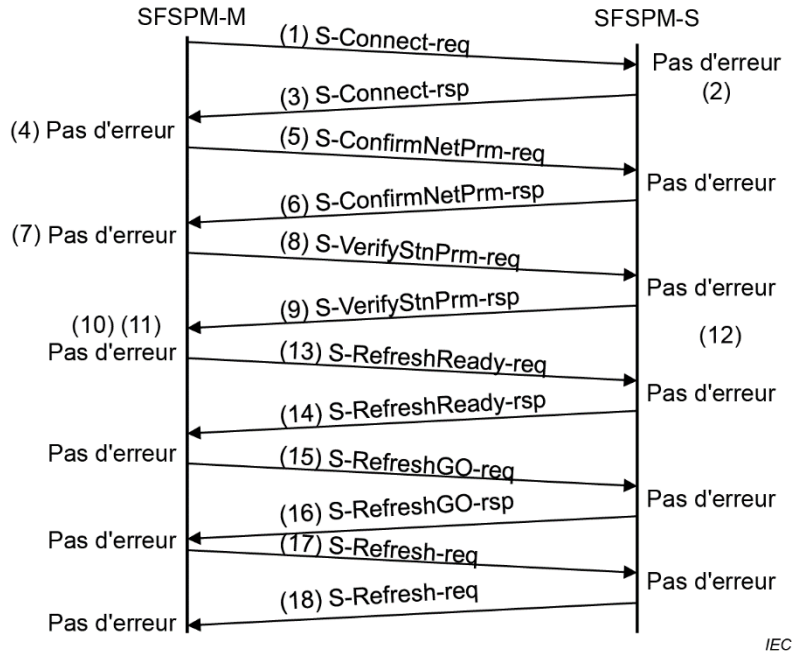


Figure 20 – Séquence d'établissement d'une connexion

Lors de l'établissement d'une connexion de sécurité, une séquence facultative peut être exécutée après vérification des paramètres de sécurité. Lorsque la séquence facultative a été exécutée, SFSPM-M envoie une demande de rafraîchissement et de mesurage du décalage au SFSPM-S.

La séquence facultative est exécutée pour les fonctions prises en charge qui sont fixées par accord entre SFSPM-M et SFSPM-S lors de l'établissement de la connexion de sécurité.

La Figure 21 représente le diagramme séquentiel facultatif pour la vérification des informations d'identification spécifiques au poste, la vérification du code de contrôle des informations de configuration spécifiques au poste, l'écriture des informations de configuration spécifiques au poste et la négociation du format S-Data.

19) SFSPM-M envoie une demande de vérification d'informations d'identification spécifiques au poste si la vérification d'informations d'identification spécifiques au poste est acceptée lors de l'établissement de la connexion de sécurité.

20) SFSPM-S envoie une réponse qui contient ses informations d'identification spécifiques au poste données à l'avance.
21) SFSPM-M vérifie les informations d'identification spécifiques au poste reçues.
22) Si la vérification du code de contrôle des informations de configuration spécifiques au poste est acceptée lors de l'établissement de la connexion de sécurité, le SFSPM-M envoie une demande de vérification du code de contrôle des informations de configuration spécifiques au poste.
23) SFSPM-S envoie une réponse qui contient ses codes de contrôle des informations d'identification spécifiques au poste donnés à l'avance.
24) SFSPM-M vérifie les codes de contrôle des informations de configuration spécifiques au poste reçus et les codes de contrôle des informations de configuration spécifiques au poste stockés.
25) SFSPM-M envoie une demande d'écriture d'informations de configuration spécifiques au poste si l'écriture d'informations de configuration spécifiques au poste est acceptée lors de l'établissement de la connexion de sécurité.
26) SFSPM-S conserve la configuration contenue dans la demande et envoie une réponse.
27) Si la négociation du format S-Data est acceptée lors de l'établissement de la connexion de sécurité, le SFSPM-M envoie une demande de négociation du format S-Data.
28) SFSPM-S envoie une réponse de négociation du format S-Data qui contient les informations de format S-Data données à l'avance.
29) SFSPM-M vérifie les informations de format S-Data.

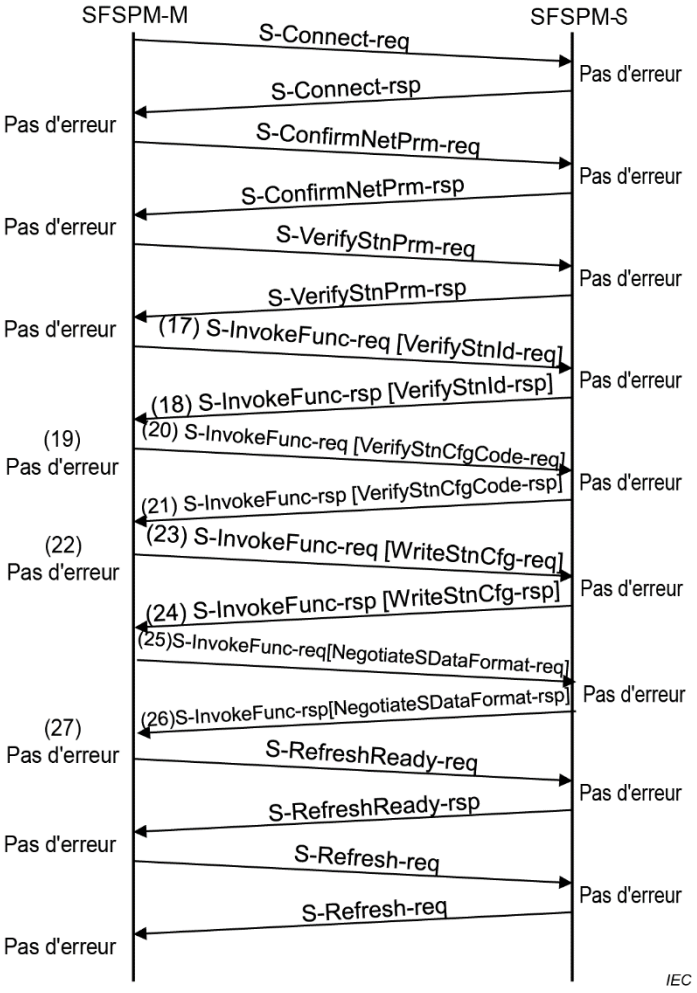


Figure 21 – Séquence facultative au cours de la séquence d'établissement de la connexion

12.7.2.2.2 Rafraîchissement de sécurité

La Figure 22 représente la séquence de communication normale entre SFSPM-M et SFSPM-S lors de la communication de rafraîchissement de sécurité qui procède à la transmission et à la réception d'entrée/de sortie.

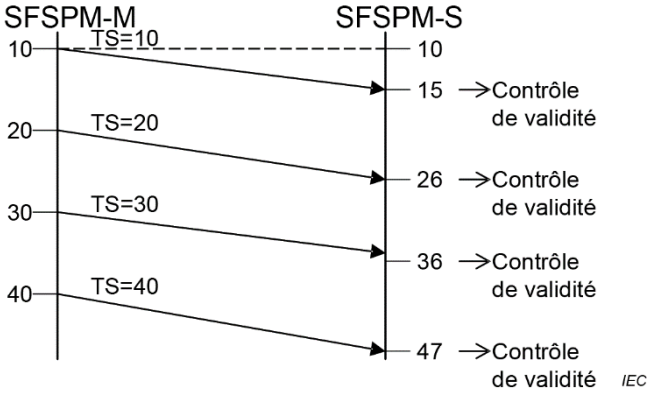


Figure 22 – Séquence de communication lors de la communication de rafraîchissement de sécurité

SFSPM-M envoie régulièrement des PDU de sécurité à SFSPM-S en fonction de l'intervalle de transmission SFSPM-M (transmission_interval). SFSPM-S vérifie les PDU de sécurité reçus.

SFSPM-S envoie régulièrement des PDU de sécurité à SFSPM-M en fonction de l'intervalle de transmission SFSPM-S (transmission_interval). SFSPM-M vérifie les PDU de sécurité reçus.

SFSPM-M et SFSPM-S doivent vérifier l'identifiant de connexion de sécurité, le CRC et l'horodatage des PDU de sécurité reçus. SFSPM-M et SFSPM-S doivent mutuellement surveiller la transmission périodique des PDU de sécurité.

SFSPM-M et SFSPM-S doivent fournir les données de sécurité reçues aux couches supérieures lorsque les résultats de la vérification d'un PDU de sécurité reçu indiquent que le PDU est normal.

Lors de la communication de rafraîchissement de sécurité, SFSPM-M et SFSPM-S procèdent régulièrement au mesurage et à la génération du décalage. La Figure 23 représente la séquence au moment du mesurage et de la génération du décalage entre SFSPM-M et SFSPM-S.

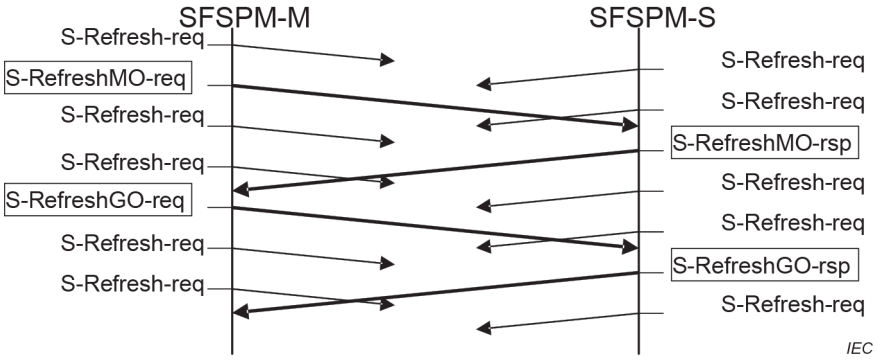


Figure 23 – Séquence de mesure et de génération du décalage lors de la communication de rafraîchissement de sécurité

12.7.2.2.3 Interruption de connexion de sécurité

Lorsqu'une erreur de communication est détectée lors de l'initialisation de sécurité ou du rafraîchissement de sécurité, SFSPM-M et SFSPM-S arrêtent le rafraîchissement de sécurité (si l'erreur s'est produite à ce moment-là) et interrompent la connexion de sécurité.

SFSPM-M ou SFSPM-S doit interrompre la connexion de sécurité selon la procédure suivante.

1) SFSPM-M ou SFSPM-S détecte une erreur qui oblige à interrompre la connexion de sécurité.
2) SFSPM-M ou SFSPM-S émet une notification adressée à la couche sécurité de l'utilisateur en indiquant qu'une erreur s'est produite, l'obligeant à interrompre la connexion de sécurité, ce qui risque de se produire.
3) L'application de couche sécurité de l'utilisateur indique l'état et les informations relatives à la connexion de sécurité si l'erreur s'est produite à l'état sûr.
4) SFSPM-M ou SFSPM-S interrompt la connexion de sécurité à l'endroit où l'erreur s'est produite.
5) SFSPM-M rétablit la connexion de sécurité après la résolution de l'erreur.

12.7.2.3 SFSPM-M

12.7.2.3.1 Transitions d'état

La Figure 24 représente un diagramme de transition d'état SFSPM-M.

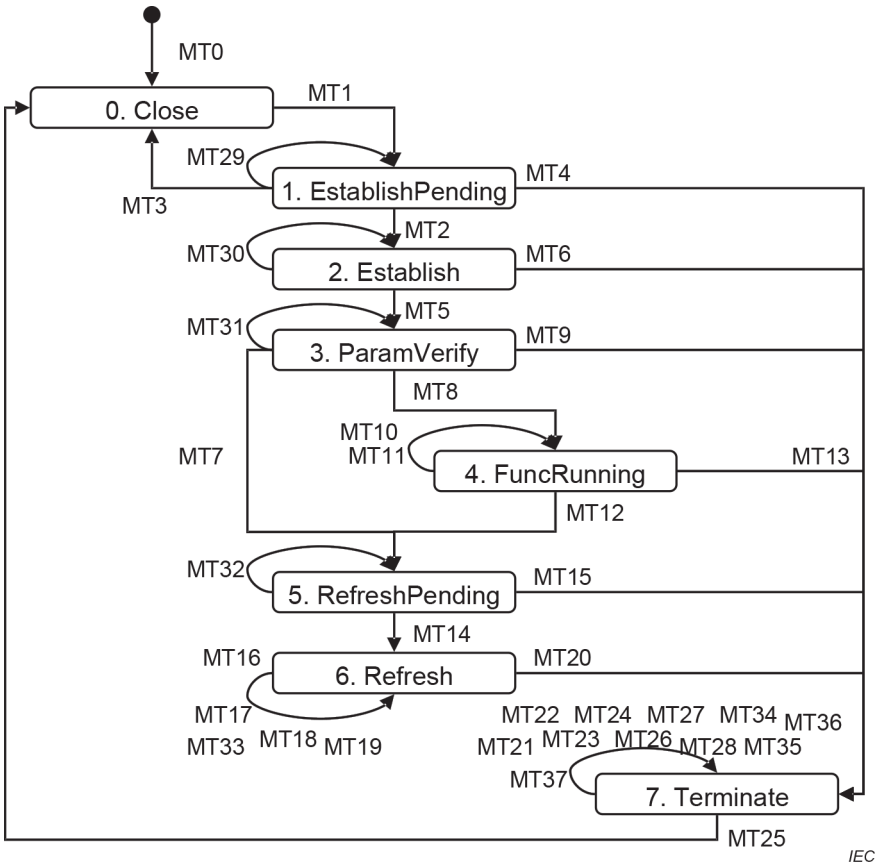


Figure 24 – Diagramme de transition d'état SFSPM-M

Le Tableau 33 décrit les temporisateurs utilisés par SFSPM-M.

Tableau 33 – Temporisateurs SFSPM-M

Nom	Description
roundtrip_timer	Utilisé pour détecter les délais inadmissibles autres que ceux qui se produisent lors du rafraîchissement de sécurité. Il expire lorsque allowable_roundtrip_delay s'est écoulé.
delay_detection_timer	Utilisé pour détecter les délais inadmissibles. Il expire lorsque allowable_refresh_interval s'est écoulé.

Le Tableau 34 présente la table des transitions d'état SFSPM-M.

Tableau 34 – Table des transitions d'état SFSPM-M

Trans	Etat	Condition	Action	Etat suivant
MT0	—	Canal noir prêt	—	0.Close
MT1	0.Close	—	Envoyer S-Connect-req && Lancer roundtrip_timer	1.EstablishPending
MT2	1.EstablishPending	Recevoir S-Connect-rsp [NoError]	Arrêter roundtrip_timer && Envoyer S-InitConfirmNetPrm-req && Lancer roundtrip_timer	2.Establish
MT29	1.EstablishPending	Recevoir S-Connect-rsp [Busy]	Arrêter roundtrip_timer && Envoyer S-Connect-req déjà envoyé && Lancer roundtrip_timer	1.EstablishPending
MT3	1.EstablishPending	Temporisation roundtrip_timer	—	0.Close
MT4	1.EstablishPending	Recevoir S-Connect-rsp [Error]	Arrêter roundtrip_timer	7.Terminate
MT5	2.Establish	Recevoir S-InitConfirmNetPrm-rsp [NoError]	Arrêter roundtrip_timer && Envoyer S-InitVerifyStnPrm-req && Lancer roundtrip_timer	3.ParamVerify
MT30	2.Establish	Recevoir S-InitConfirmNetPrm-rsp [Busy]	Arrêter roundtrip_timer && Envoyer S-InitConfirmNetPrm-req déjà envoyé && Lancer roundtrip_timer	2.Establish
MT6	2.Establish	Temporisation roundtrip_timer	—	7.Terminate
MT6	2.Establish	Recevoir S-InitConfirmNetPrm-rsp [Error]	Arrêter roundtrip_timer	7.Terminate
MT7	3.ParamVerify	Recevoir S-InitVerifyStnPrm-rsp [NoError] && OptFuncs n'existe pas	Arrêter roundtrip_timer && Envoyer S-RefreshReady-req && Lancer roundtrip_timer	6.RefreshPending

Trans	Etat	Condition	Action	Etat suivant
MT8	3.ParamVerify	Recevoir S-InitVerifyStnPrm-rsp [NoError] && OptFuncs existe	Arrêter roundtrip_timer && Envoyer S-InvokeFunc-req && Lancer roundtrip_timer	4.FuncRunning
MT31	3.ParamVerify	Recevoir S-InitVerifyStnPrm-rsp [Busy]	Arrêter roundtrip_timer && Envoyer S-InitVerifyStnPrm-req déjà envoyé && Lancer roundtrip_timer	3.ParamVerify
MT9	3.ParamVerify	Temporisation roundtrip_timer	—	7.Terminate
MT9	3.ParamVerify	Recevoir S-InitVerifyStnPrm-rsp [Error]	Arrêter roundtrip_timer	7.Terminate
MT10	4.FuncRunning	Recevoir S-InvokeFunc-rsp [NoError] && Une autre OptFunc existe	Arrêter roundtrip_timer && Envoyer S-InvokeFunc-req && Lancer roundtrip_timer	4.FuncRunning
MT11	4.FuncRunning	Recevoir S-InvokeFunc-rsp [Busy]	Arrêter roundtrip_timer && Envoyer S-InvokeFunc-req déjà envoyé && Lancer roundtrip_timer	4.FuncRunning
MT12	4.FuncRunning	Recevoir S-InvokeFunc-rsp [NoError] && Aucune autre OptFunc n'existe	Arrêter roundtrip_timer && Envoyer S-RefreshReady-req && Lancer roundtrip_timer	6.RefreshPending
MT13	4.FuncRunning	Temporisation roundtrip_timer	—	7.Terminate
MT13	4.FuncRunning	Recevoir S-InvokeFunc-rsp [Error]	Arrêter roundtrip_timer	7.Terminate
MT14	5.RefreshPending	Recevoir S-RefreshReady-rsp [NoError]	Arrêter roundtrip_timer && Envoyer S-RefreshGO-req && Lancer roundtrip_timer	6.Refresh
MT32	5.RefreshPending	Recevoir S-RefreshReady-rsp [Busy]	Arrêter roundtrip_timer && Envoyer S-RefreshReady-req déjà envoyé && Lancer roundtrip_timer	6.RefreshPending
MT15	5.RefreshPending	Temporisation roundtrip_timer	—	7.Terminate
MT15	5.RefreshPending	Recevoir S-RefreshReady-rsp [Error]	Arrêter roundtrip_timer	7.Terminate
MT16	6.Refresh	Durée d'envoi [NoError]	Envoyer S-Refresh-req	6.Refresh
MT17	6.Refresh	Durée de mesure du décalage	Envoyer S-RefreshMO-req && Lancer roundtrip_timer	6.Refresh
MT18	6.Refresh	Recevoir S-RefreshMO-rsp [NoError]	Arrêter roundtrip_timer	6.Refresh
MT18	6.Refresh	Durée d'envoi [en premier lieu après S-RefreshMO-rsp avec NoMOBusy reçu]	Envoyer S-RefreshGO-req && Lancer roundtrip_timer	6.Refresh
MT33	6.Refresh	Recevoir S-RefreshMO-rsp [MOBusy]	Arrêter roundtrip_timer && Lancer roundtrip_timer	6.Refresh

Trans	Etat	Condition	Action	Etat suivant
MT19	6.Refresh	Recevoir S-RefreshGO-rsp [NoError]	Arrêter roundtrip_timer	6.Refresh
MT20	6.Refresh	Recevoir S-Refresh-req [Error]	—	7.Terminate
MT20	6.Refresh	Temporisation roundtrip_timer	—	7.Terminate
MT20	6.Refresh	Recevoir S-RefreshMO-rsp [Error]	Arrêter roundtrip_timer	7.Terminate
MT20	6.Refresh	Recevoir S-RefershGO-rsp [Error]	Arrêter roundtrip_timer	7.Terminate
MT21	7.Terminate	Nécessité de collecter des informations sur l'erreur	Envoyer S-ReadErrorInfo-req && Arrêter roundtrip_timer	7.Terminate
MT22	7.Terminate	Recevoir S-ReadErrorInfo-rsp [No more data]	Arrêter roundtrip_timer	7.Terminate
MT34	7.Terminate	Recevoir S-ReadErrorInfo-rsp [More data]	Arrêter roundtrip_timer && S-ReadErrorInfo-req && Lancer roundtrip_timer	7.Terminate
MT35	7.Terminate	Recevoir S-ReadErrorInfo-rsp [Busy]	Arrêter roundtrip_timer && Envoyer S-ReadErrorInfo-req déjà envoyé && Lancer roundtrip_timer	7.Terminate
MT23	7.Terminate	Nécessité d'envoyer des informations sur l'erreur	Envoyer S-WriteErrorInfo-req && Lancer roundtrip_timer	7.Terminate
MT24	7.Terminate	Recevoir S-WriteErrorInfo-rsp [No more data]	Arrêter roundtrip_timer	7.Terminate
MT36	7.Terminate	Recevoir S-WriteErrorInfo-rsp [More data]	Arrêter roundtrip_timer && S-WriteErrorInfo-req && Lancer roundtrip_timer	7.Terminate
MT37	7.Terminate	Recevoir S-WriteErrorInfo-rsp [Busy]	Arrêter roundtrip_timer && Envoyer S-WriteErrorInfo-req déjà envoyé && Lancer roundtrip_timer	7.Terminate
MT25	7.Terminate	Erreur résolue	—	0.Close
MT26	7.Terminate	Nécessité d'appeler la fonction	Envoyer S-InvokeFunc-req && Lancer roundtrip_timer	7.Terminate
MT27	7.Terminate	Recevoir S-InvokeFunc-rsp	Arrêter roundtrip_timer	7.Terminate
MT28	7.Terminate	Recevoir S-InvokeFunc-rsp [Busy]	Envoyer S-InvokeFunc-req déjà envoyé	7.Terminate
Erreurs MT4, MT6, MT9, MT13 et MT15: CTRL anormal, Bit d'état d'erreur = 1, S-Data anormal Erreur MT20: Ordre incorrect, Perte, Délai inadmissible, CTRL anormal, Bit d'état d'erreur = 1				

12.7.2.3.2 Opérations autres que celles réalisées lors du rafraîchissement de sécurité

SFSPM-M lance le temporisateur roundtrip_timer au même moment que l'envoi d'une demande. SFSPM-M reçoit une réponse à la demande de la part de SFSPM-S et arrête le temporisateur roundtrip_timer. Le temporisateur roundtrip_timer expire à allowable_roundtrip_delay. Si SFSPM-M ne reçoit pas de réponse à la demande avant l'expiration du temporisateur roundtrip_timer, un délai inadmissible se produit. La Figure 25 représente la séquence qui correspond aux états autres que le rafraîchissement de sécurité.

Lors de l'envoi d'une demande, SFSPM-M insère les 16 bits inférieurs de la valeur d'horloge de sécurité dans le TS du PDU de sécurité et envoie la demande. Lors de l'envoi d'une réponse, SFSPM-S insère la valeur du TS inclus dans le PDU de sécurité de la demande correspondante dans le TS du PDU de sécurité qui doit faire office de réponse. SFSPM-M vérifie que la réponse correspond à la demande en comparant la valeur du TS inclus dans la réponse à celle du TS envoyé. Si elles ne correspondent pas, SFSPM-M doit ignorer le PDU de sécurité reçu.

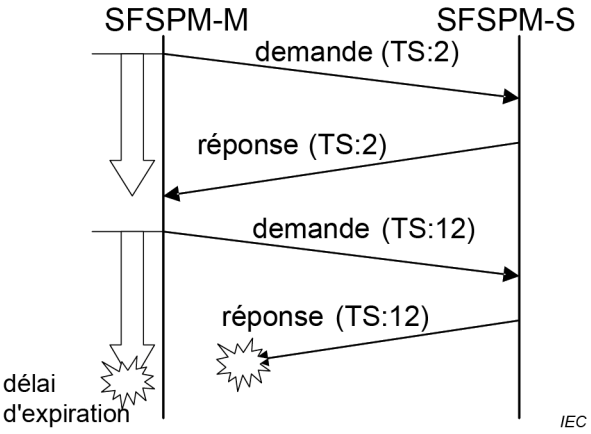


Figure 25 – Séquence autre que celle réalisée lors du rafraîchissement de sécurité

12.7.2.3.3 Syntaxe S-Data

12.7.2.3.3.1 S-Connect-req

S-Connect-req utilise le format S-Data représenté à la Figure 15. La zone safety_data stocke les données décrites à la Figure 26.

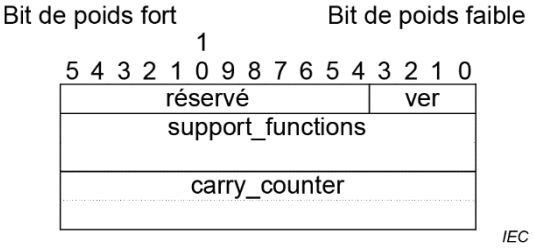


Figure 26 – S-Connect-req

ver
Indique la version du protocole de FSCP 8/2 prise en charge par SFSPM-M. La version du protocole est 0000b.

réservé
Réservé pour une extension ultérieure.

support_functions
Le Tableau 35 décrit les détails des fonctions auxiliaires de S-Connect-req. Chaque bit indique si la fonction indiquée dans le tableau est prise en charge ou pas. 1 indique que la fonction est prise en charge et 0 qu'elle ne l'est pas.

Tableau 35 – support_functions

Bit	Fonction	Description
0	Vérification de paramètre de réseau de sécurité	Vérifie les paramètres de sécurité du réseau gérés par SFSPM-M et SFSPM-S.
1	Vérification de paramètre de poste de sécurité	Vérifie les paramètres de poste de sécurité gérés par SFSPM-M et SFSPM-S.
2 – 31	Pour une extension ultérieure	Pour une extension ultérieure

carry_counter
La valeur initiale de carry_counter utilisée par SFSPM-M et SFSPM-S après la transmission/réception S-Connect.

Si S-Data du PDU de sécurité est S-connect-req, la valeur du carry_counter utilisé dans la génération de CRC32 comme valeur initiale est 0.

12.7.2.3.3.2 S-InitConfirmNetPrm-req

S-InitConfirmNetPrm-req utilise le format S-Data présenté à la Figure 15. La zone safety_data stocke les données décrites à la Figure 27.

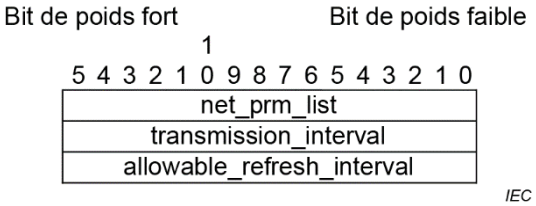


Figure 27 – S-InitConfirmNetPrm-req

net_prm_list
Liste des paramètres de réseau de sécurité à confirmer. La Figure 28 représente la configuration de net_prm_list. 1 indique que le paramètre est à confirmer et 0 qu'il ne l'est pas. La valeur 1 est attribuée aux bits de transmission_interval et d'allowable_refresh_interval.

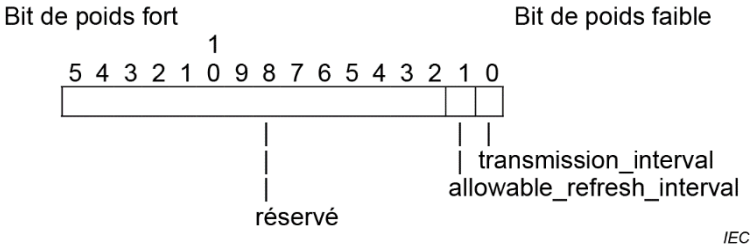


Figure 28 – net_prm_list

transmission_interval
Intervalle de transmission des PDU de sécurité de SFSPM-M lors du rafraîchissement de sécurité. L'unité est 128 µs.

allowable_refresh_interval
Intervalle de réception admissible utilisé par SFSPM-M et SFSPM-S lors du rafraîchissement de sécurité. L'unité est 128 µs.

12.7.2.3.3.3 S-InitVerifyStnPrm-req

S-InitVerifyStnPrm-req utilise le format S-Data représenté à la Figure 15. La zone safety_data stocke les données décrites à la Figure 29.

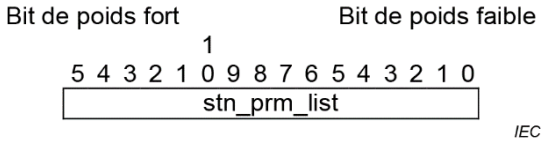


Figure 29 – S-InitVerifyStnPrm-req

stn_prm_list
Liste des paramètres de poste de sécurité à vérifier. La Figure 30 représente la configuration de stn_prm_list. 1 indique que le paramètre est à vérifier et 0 qu'il ne l'est pas.

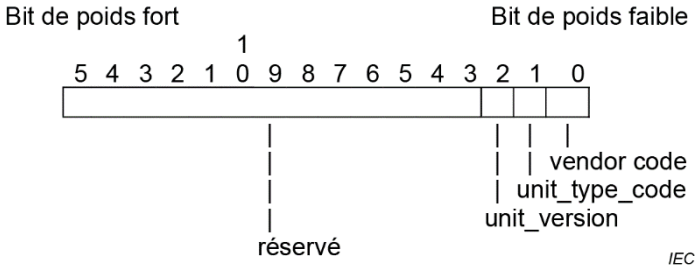


Figure 30 – stn_prm_list

12.7.2.3.3.4 S-InvokeFunc-req

S-InvokeFunc-req utilise le format S-Data représenté à la Figure 15. La zone safety_data stocke les données décrites à la Figure 31.

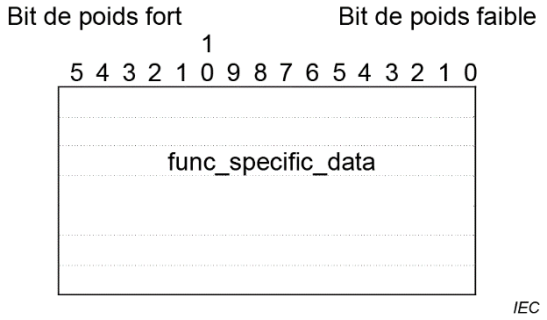


Figure 31 – S-InvokeFunc-req

func_specific_data
Données relatives à la fonction spécifiée par la commande fonctionnelle de S-DataHeader. funcspecific_data est déterminé pour chaque commande fonctionnelle.

12.7.2.3.3.5 S-RefreshReady-req

S-RefreshReady-req utilise le format S-Data représenté à la Figure 15. La zone safety_data ne stocke aucune information.

12.7.2.3.3.6 S-ReadErrorInfo-req

S-ReadErrorInfo-req utilise le format S-Data représenté à la Figure 15. La zone safety_data ne stocke aucune information.

12.7.2.3.3.7 S-WriteErrorInfo-req

S-WriteErrorInfo-req utilise le format S-Data représenté à la Figure 15. La zone safety_data stocke les données décrites à la Figure 32.

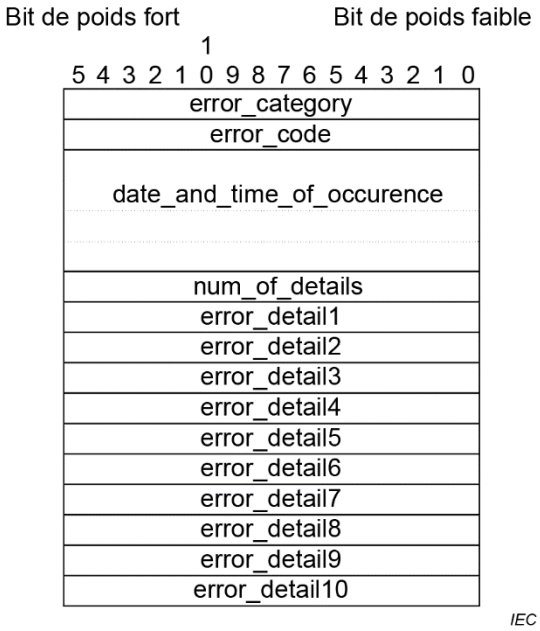


Figure 32 – S-WriteErrorInfo-req

error_category
Indique la catégorie d'une erreur et utilise les valeurs indiquées dans le Tableau 36 et dans le Tableau 37.

Tableau 36 – error_category

Valeur	Signification
0 – 299	Pour une extension ultérieure
300 – 349	Erreur commune de couche d'application (voir Tableau 37)
350	Erreur de définition du fournisseur de couche d'application
351 – 399	Pour une extension ultérieure (erreur de couche d'application)
400 ~ 449	Pour une extension ultérieure (erreur commune de couche d'utilisateur de service)
450	Erreur de définition du fournisseur de couche d'utilisateur de service
451 – 449	Pour une extension ultérieure (erreur de couche d'utilisateur de service)
500 – 66535	Pour une extension ultérieure

Tableau 37 – error_category correspondant aux erreurs AL

Valeur	Signification
300 – 309	Pour une extension ultérieure
310 – 314	Erreur de couche d'application

error_code
Indique le numéro d'erreur. Les numéros utilisés sont présentés dans le Tableau 38.

Tableau 38 – error_code

error_category	error_code	Signification
310	0	Détection d'erreur CRC
	1	Erreur TS
	2	Erreur CID
311	0	Temporisation delay_detection_timer
	1	Temporisation roundtrip_timer
312	0	Erreur de numéro de fragment
313	0	Erreur de paramètre de réseau de sécurité
314	0	Erreur de paramètre de poste de sécurité

date_and_time_of_occurence
Indique la date et l'heure d'occurrence de l'erreur. Le format utilisé est représenté à la Figure 33. year_upper (deux premiers chiffres de l'année), year_lower (deux derniers chiffres de l'année), month, day, hour, minute, second, et day_of_week sont exprimés en code BCD.

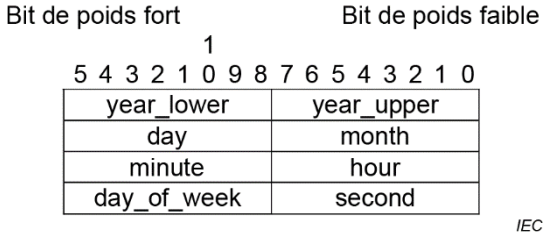


Figure 33 – date_and_time_of_occurence

num_of_details
Indique le nombre de détails d'erreur exprimés par error_detail1 à error_detail10.

error_detail
Indique les détails de l'erreur (1 – 10).

réservé
Réservé pour une extension ultérieure.

12.7.2.3.3.8 S-RefreshMO-req

S-RefreshMO-req utilise le format S-Data représenté à la Figure 14. safety_data désigne les données de rafraîchissement de sécurité.

12.7.2.3.3.9 S-RefreshGO-req

S-RefreshGO-req utilise le format S-Data représenté à la Figure 14. safety_data désigne les données de rafraîchissement de sécurité.

12.7.2.3.3.10 S-Refresh-req

S-Refresh-req utilise le format S-Data représenté à la Figure 14. safety_data désigne les données de rafraîchissement de sécurité.

12.7.2.4 SFSPM-S

12.7.2.4.1 Transitions d'état

La Figure 34 représente un diagramme de transition d'état SFSPM-S.

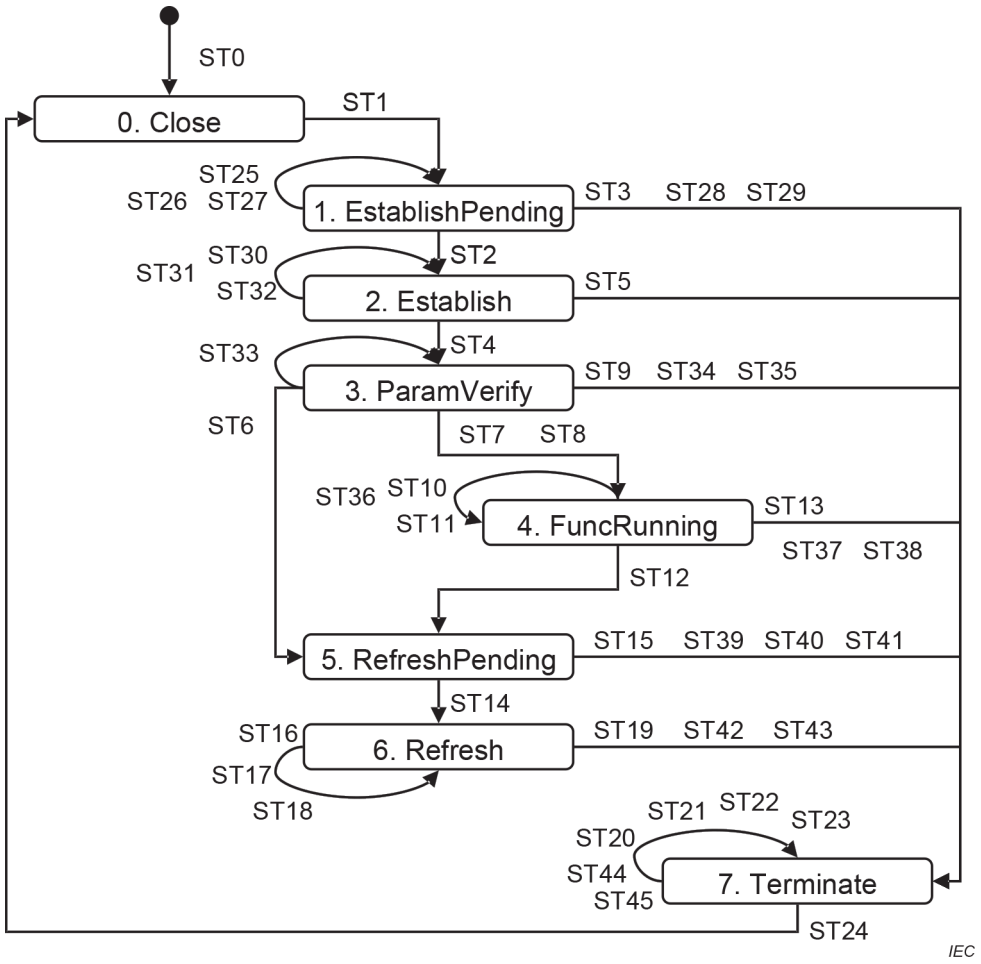


Figure 34 – Diagramme de transition d'état SFSPM-S

Le Tableau 39 décrit les temporisateurs utilisés par SFSPM-S.

Tableau 39 – Temporisateurs SFSPM-S

Nom	Description
roundtrip_timer	Utilisé pour détecter les délais inadmissibles autres que ceux qui se produisent lors du rafraîchissement de sécurité. Il expire lorsque allowable_roundtrip_delay s'est écoulé.
delay_detection_timer	Utilisé pour détecter les délais inadmissibles. Il expire lorsque allowable_refresh_interval s'est écoulé.

Le Tableau 40 présente la table des transitions d'état SFSPM-S.

Tableau 40 – Table des transitions d'état SFSPM-S

Transition	Etat	Condition	Action	Etat suivant
ST0	—	Canal noir prêt	—	0.Close
ST1	0.Close	Recevoir S-Connect-req [NoError]	Envoyer S-Connect-rsp && Lancer roundtrip_timer	1.EstablishPending
ST2	1.EstablishPending	Recevoir S-InitConfirmNetPrm-req [NoError]	Arrêter roundtrip_timer && Envoyer S-InitConfirmNetPrm-rsp && Lancer roundtrip_timer	2.Establish
ST25	1.EstablishPending	Recevoir S-Connect-req [NoError]	Arrêter roundtrip_timer && Envoyer S-Connect-rsp && Lancer roundtrip_timer	1.EstablishPending
ST26	1.EstablishPending	Recevoir S-InitConfirmNetPrm-req [Busy]	Arrêter roundtrip_timer && Envoyer S-InitConfirmNetPrm-rsp && Lancer roundtrip_timer	1.EstablishPending
ST27	1.EstablishPending	Temporisation roundtrip_timer	—	7.Terminate
ST3	1.EstablishPending	Recevoir S-InitConfirmNetPrm-req [Error]	Arrêter roundtrip_timer && Envoyer S-InitConfirmNetPrm-rsp	7.Terminate
ST28	1.EstablishPending	Recevoir S-WriteErrorInfo-req [No more data]	Arrêter roundtrip_timer && Envoyer S-WriteErrorInfo-rsp	7.Terminate
ST29	1.EstablishPending	Recevoir S-WriteErrorInfo-req [More data]	Arrêter roundtrip_timer && Envoyer S-WriteErrorInfo-rsp && Lancer roundtrip_timer	7.Terminate
ST4	2.Establish	Recevoir S-InitVerifyStnPrm-req [NoError]	Arrêter roundtrip_timer && Envoyer S-InitVerifyStnPrm-rsp && Lancer roundtrip_timer	3.ParamVerify
ST30	2.Establish	Recevoir S-InitVerifyStnPrm-req [Busy]	Arrêter roundtrip_timer && Envoyer S-InitVerifyStnPrm-rsp && Lancer roundtrip_timer	2.Establish

Transition	Etat	Condition	Action	Etat suivant
ST31	2.Establish	Recevoir S-WriteErrorInfo-req [No more data]	Arrêter roundtrip_timer && Envoyer S-WriteErrorInfo-rsp	7.Terminate
ST32	2.Establish	Recevoir S-WriteErrorInfo-req [More data]	Arrêter roundtrip_timer && Envoyer S-WriteErrorInfo-rsp && Lancer roundtrip_timer	7.Terminate
ST5	2.Establish	Temporisation roundtrip_timer	—	7.Terminate
ST5	2.Establish	Recevoir S-InitVerifyStnPrm-req [Error]	Arrêter roundtrip_timer && Envoyer S-InitVerifyStnPrm-rsp	7.Terminate
ST6	3.ParamVerify	Recevoir S-RefreshReady-req [NoError]	Arrêter roundtrip_timer && Envoyer S-RefreshReady-rsp && Lancer roundtrip_timer	5.RefreshPending
ST33	3.ParamVerify	Recevoir S-RefreshReady-req [Busy]	Arrêter roundtrip_timer && Envoyer S-RefreshReady-rsp && Lancer roundtrip_timer	3.ParamVerify
ST7	3.ParamVerify	Recevoir S-InvokeFunc-req [NoError] && Traitement terminé	Arrêter roundtrip_timer && Envoyer S-InvokeFunc-rsp [NoBusy] && Start roundtrip_timer	4.FuncRunning
ST8	3.ParamVerify	Recevoir S-InvokeFunc-req [NoError] && Fonction en cours	Arrêter roundtrip_timer && Envoyer S-InvokeFunc-rsp [Busy] && Lancer roundtrip_timer	4.FuncRunning
ST34	3.ParamVerify	Recevoir S-WriteErrorInfo-req [No more data]	Arrêter roundtrip_timer && Envoyer S-WriteErrorInfo-rsp	7.Terminate
ST35	3.ParamVerify	Recevoir S-WriteErrorInfo-req [More data]	Arrêter roundtrip_timer && Envoyer S-WriteErrorInfo-rspStart roundtrip_timer	7.Terminate
ST9	3.ParamVerify	Temporisation roundtrip_timer	—	7.Terminate
ST9	3.ParamVerify	Recevoir S-InvokeFunc-req [Error]	Arrêter roundtrip_timer	7.Terminate
ST9	3.ParamVerify	Recevoir S-RefreshReady-req [Error]	Arrêter roundtrip_timer && Envoyer S-RefreshReady-rsp	7.Terminate
ST10	4.FuncRunning	Recevoir S-InvokeFunc-req [NoError] && Traitement terminé	Arrêter roundtrip_timer && Envoyer S-InvokeFunc-rsp [NoBusy] && Start roundtrip_timer	4.FuncRunning
ST11	4.FuncRunning	Recevoir S-InvokeFunc-req [NoError] && Fonction en cours	Arrêter roundtrip_timer && Envoyer S-InvokeFunc-rsp [Busy] && Lancer roundtrip_timer	4.FuncRunning

Transition	Etat	Condition	Action	Etat suivant
ST12	4.FuncRunning	Recevoir S-RefreshReady-req [NoError]	Arrêter roundtrip_timer && Envoyer S-RefreshReady-rsp && Lancer roundtrip_timer	5.RefreshPending
ST36	4.FuncRunning	Recevoir S-InvokeFunc-req [Busy]	Arrêter roundtrip_timer && Envoyer S-InvokeFunc-rsp && Lancer roundtrip_timer	4.FuncRunning
ST37	4.FuncRunning	Recevoir S-WriteErrorInfo-req [No more data]	Arrêter roundtrip_timer && Envoyer S-WriteErrorInfo-rsp	7.Terminate
ST38	4.FuncRunning	Recevoir S-WriteErrorInfo-req [More data]	Arrêter roundtrip_timer && Envoyer S-WriteErrorInfo-rsp && Lancer roundtrip_timer	7.Terminate
ST13	4.FuncRunning	Temporisation roundtrip_timer	—	7.Terminate
ST13	4.FuncRunning	Recevoir S-InvokeFunc-req [Error]	Arrêter roundtrip_timer && Envoyer S-InvokeFunc-rsp	7.Terminate
ST13	4.FuncRunning	Recevoir S-RefreshReady-req [Error]	Arrêter roundtrip_timer && Envoyer S-RefreshReady-rsp	7.Terminate
ST14	5.RefreshPending	Recevoir S-RefreshGO-req [NoError]	Arrêter roundtrip_timer && Envoyer S-RefreshGO-rsp	6.Refresh
ST39	5.RefreshPending	Recevoir S-WriteErrorInfo-req [No more data]	Arrêter roundtrip_timer && Envoyer S-WriteErrorInfo-rsp	7.Terminate
ST40	5.RefreshPending	Recevoir S-WriteErrorInfo-req [More data]	Arrêter roundtrip_timer && Envoyer S-WriteErrorInfo-rsp && Lancer roundtrip_timer	7.Terminate
ST15	5.RefreshPending	Temporisation roundtrip_timer	—	7.Terminate
ST15	5.RefreshPending	Recevoir S-RefreshGO-req [ErrorA]	Arrêter roundtrip_timer	7.Terminate
ST15	5.RefreshPending	Recevoir S-RefreshGO-req [ErrorB]	Arrêter roundtrip_timer && Envoyer S-RefreshGO-rsp && Lancer roundtrip_timer	7.Terminate
ST16	6.Refresh	Durée d'envoi [NoError]	Envoyer S-Refresh-req	6.Refresh
ST17	6.Refresh	Recevoir S-RefreshMO-req [NoError]	Arrêter roundtrip_timer	6.Refresh
ST17	6.Refresh	Durée d'envoi [en premier lieu après S-RefreshMO-req avec NoError reçu]	Envoyer S-RefreshMO-rsp && Lancer roundtrip_timer	6.Refresh
ST18	6.Refresh	Recevoir S-RefreshGO-req [NoError]	—	6.Refresh
ST18	6.Refresh	Durée d'envoi [en premier lieu après S-RefreshGO-req avec NoError reçu]	Envoyer S-RefreshGO-rsp	6.Refresh
ST41	6.Refresh	Recevoir S-WriteErrorInfo-req [No more data]	Arrêter roundtrip_timer && Envoyer S-WriteErrorInfo-rsp	7.Terminate

Transition	Etat	Condition	Action	Etat suivant
ST42	6.Refresh	Recevoir S-WriteErrorInfo-req [More data]	Arrêter roundtrip_timer && Envoyer S-WriteErrorInfo-rsp && Lancer roundtrip_timer	7.Terminate
ST19	6.Refresh	Recevoir S-Refresh-req [Error]	—	7.Terminate
ST19	6.Refresh	Durée d'envoi [en premier lieu après S-Refresh-req avec ErrorA reçu]	Envoyer S-Refresh-req && Lancer roundtrip_timer	7.Terminate
ST19	6.Refresh	Recevoir S-RefreshMO-req [Error]	—	7.Terminate
ST19	6.Refresh	Durée d'envoi [en premier lieu après S-RefreshMO-req avec ErrorA reçu]	Envoyer S-RefreshMO-rsp && Lancer roundtrip_timer	7.Terminate
ST19	6.Refresh	Recevoir S-RefreshGO-req [Error]	Arrêter roundtrip_timer	7.Terminate
ST19	6.Refresh	Durée d'envoi [en premier lieu après S-RefreshGO-req avec ErrorA reçu]	Envoyer S-RefreshGO-rsp && Lancer roundtrip_timer	7.Terminate
ST19	6.Refresh	Temporisation roundtrip_timer	—	7.Terminate
ST20	7.Terminate	Recevoir S-ReadErrorInfo-req [No more data]	Envoyer S-ReadErrorInfo-rsp	7.Terminate
ST43	7.Terminate	Recevoir S-ReadErrorInfo-req [More data]	Arrêter roundtrip_timer && Envoyer S-ReadErrorInfo-rsp && Lancer roundtrip_timer	7.Terminate
ST21	7.Terminate	Recevoir S-WriteErrorInfo-req [No more data]	Envoyer S-WriteErrorInf-rsp	7.Terminate
ST44	7.Terminate	Recevoir S-WriteErrorInfo-req [More data]	Arrêter roundtrip_timer && Envoyer S-WriteErrorInfo-rsp && Lancer roundtrip_timer	7.Terminate
ST22	7.Terminate	Recevoir S-InvokeFunc-req [NoError] && Traitement terminé	Envoyer S-InvokeFunc-rsp [NoBusy]	7.Terminate
ST23	7.Terminate	Recevoir S-InvokeFunc-req [NoError] && Fonction en cours	Envoyer S-InvokeFunc-rsp [Busy]	7.Terminate
ST24	7.Terminate	Erreur résolue	—	0.Close
Erreurs ST3, ST5, ST9 et ST13: CTRL anormal, Bit d'état d'erreur = 1, S-Data anormal Erreur ST15 A: Délai inadmissible Erreur ST15 B: Ordre incorrect, CTRL anormal, Bit d'état d'erreur = 1 Erreur ST19: Ordre incorrect, Perte, Délai inadmissible, CTRL anormal, Bit d'état d'erreur = 1 Erreur ST19 A: Ordre incorrect, CTRL anormal, Bit d'état d'erreur = 1				

12.7.2.4.2 Opérations autres que celles réalisées lors du rafraîchissement de sécurité

SFSPM-S lance le temporisateur roundtrip_timer au même moment que l'envoi d'une réponse. SFSPM-S reçoit la demande suivante après sa réponse de la part de SFSPM-M, puis arrête le temporisateur roundtrip_timer. Le temporisateur roundtrip_timer expire à allowable_roundtrip_delay. Si SFSPM-S ne reçoit pas la demande suivante après sa réponse avant l'expiration du temporisateur roundtrip_timer, un délai inadmissible se produit. La Figure 35 représente la séquence qui correspond aux états autres que le rafraîchissement de sécurité.

Lors de l'envoi d'une réponse, SFSPM-S insère la valeur de TS inclus dans le PDU de sécurité de la demande correspondante dans le TS du PDU de sécurité.

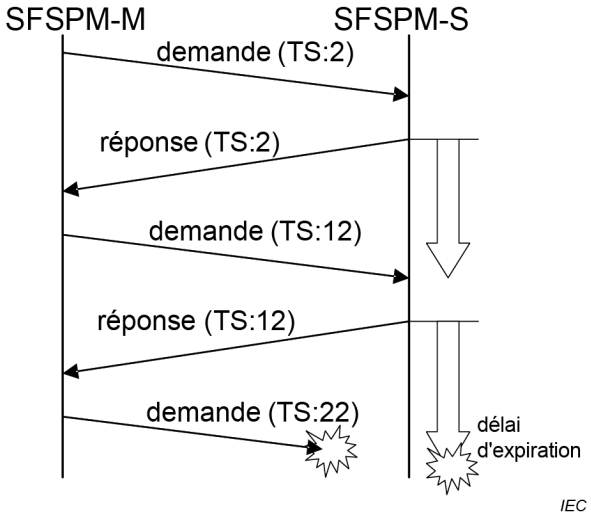


Figure 35 – Séquence autre que celle réalisée lors du rafraîchissement de sécurité

12.7.2.4.3 Syntaxe S-Data

12.7.2.4.3.1 S-Connect-rsp

S-Connect-rsp utilise le format S-Data représenté à la Figure 15. La zone safety_data stocke les données décrites à la Figure 36.

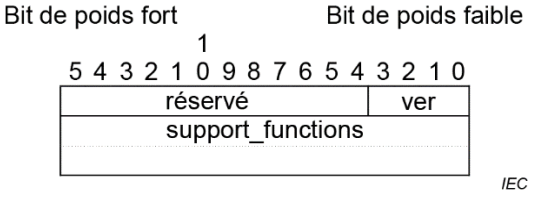


Figure 36 – S-Connect-rsp

ver
Indique la version du protocole de la fonction de communication de sécurité FSCP 8/2 prise en charge par SFSPM-S. La version du protocole est 0000b.

réservé
Réservé pour une extension ultérieure.

support_functions
Indique les fonctions prises en charge par SFSPM-S parmi les support_functions que SFSPM-M a signalées à SFSPM-S. Le Tableau 35 décrit les détails à spécifier. Chaque bit indique si la fonction indiquée dans le tableau est prise en charge ou pas. 1 indique que la fonction est prise en charge et 0 qu'elle ne l'est pas. SFSPM-S considère la valeur du produit logique des support_functions indiquées par SFSPM-M et les fonctions prises en charge par SFSPM-S en tant que support_functions.

12.7.2.4.3.2 S-InitConfirmNetPrm-rsp

S-InitConfirmNetPrm-rsp utilise le format S-Data représenté à la Figure 15. La zone safety_data stocke les données décrites à la Tableau 37.

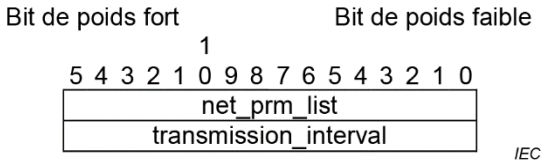


Figure 37 – S-InitConfirmNetPrm-rsp

net_prm_list
Liste des paramètres de réseau de sécurité à confirmer. 1 indique que le paramètre est à confirmer et 0 qu'il ne l'est pas. Pour la configuration de net_prm_list, voir Figure 28. La valeur 1 est attribuée au bit de transmission_interval.

transmission_interval
Intervalle de transmission des PDU de sécurité de SFSPM-S lors du rafraîchissement de sécurité. L'unité est 128 µs.

12.7.2.4.3.3 S-InitVerifyStnPrm-rsp

S-InitVerifyStnPrm-rsp utilise le format S-Data représenté à la Figure 15. La zone safety_data stocke les données décrites à la Figure 38.

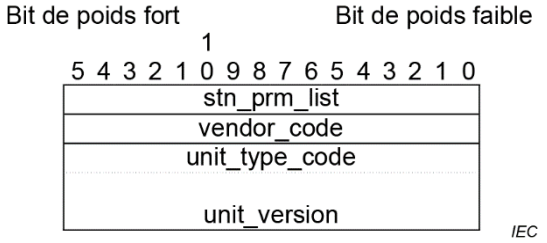


Figure 38 – S-InitVerifyStnPrm-rsp

stn_prm_list
Liste des paramètres de poste de sécurité à vérifier. Pour plus d'informations, voir 12.7.2.3.3.3.

vendor_code
Code unique attribué à un fournisseur pour l'identifier.

unit_type_code
Code unique attribué à chaque modèle de produit géré par le fournisseur.

unit_version
Version des spécifications de fonctionnement du produit géré par le fournisseur.

12.7.2.4.3.4 S-InvokeFunc-rsp

S-InvokeFunc-rsp utilise le format S-Data représenté à la Figure 15. La zone safety_data stocke les données décrites à la Figure 39.

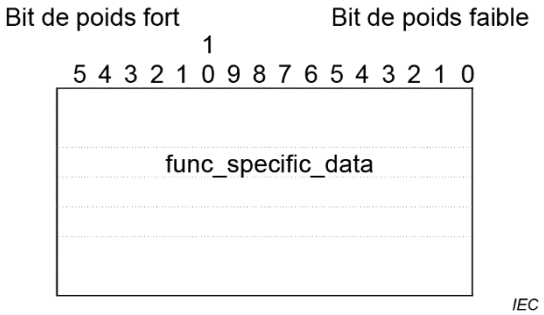


Figure 39 – S-InvokeFunc-rsp

func_specific_data
Données relatives à la fonction spécifiée par la commande fonctionnelle de S-DataHeader. funcspecific_data est déterminé pour chaque commande fonctionnelle.

12.7.2.4.3.5 S-RefreshReady-rsp

S-RefreshReady-rsp utilise le format S-Data représenté à la Figure 15. La zone safety_data ne stocke aucune information.

12.7.2.4.3.6 S-ReadErrorInfo-rsp

S-ReadErrorInfo-req utilise le format S-Data représenté à la Figure 15. La zone safety_data stocke les données représentées à la Figure 32. Pour plus d'informations sur safety_data, voir 12.7.1.6.

12.7.2.4.3.7 S-WriteErrorInfo-rsp

S-WriteErrorInfo-rsp utilise le format S-Data représenté à la Figure 15. La zone safety_data ne stocke aucune information.

12.7.2.4.3.8 S-RefreshMO-rsp

S-RefreshMO-rsp utilise le format S-Data représenté à la Figure 14. safety_data désigne les données de rafraîchissement de sécurité.

12.7.2.4.3.9 S-RefreshGO-rsp

S-RefreshGO-rsp utilise le format S-Data représenté à la Figure 14. safety_data désigne les données de rafraîchissement de sécurité.

12.7.2.4.3.10 S-Refresh-req

S-Refresh-req utilise le format S-Data représenté à la Figure 14. safety_data désigne les données de rafraîchissement de sécurité.

12.7.2.5 Correction du décalage de l'horloge

La différence entre les horloges de sécurité de SFSPM-M et SFSPM-S est le décalage ts_offset.

SFSPM-M doit utiliser la valeur des 16 bits inférieurs de l'horloge de sécurité de son propre nœud pour générer des horodatages.

SFSPM-S doit utiliser la valeur current_time des 16 bits inférieurs de l'horloge de sécurité de son propre nœud et le décalage ts_offset pour générer des horodatages. SFSPM-S doit utiliser la Formule (1) pour ce calcul.

$$TS = (current\_time + ts\_offest) \bmod 2^{16} \quad (1)$$

La Figure 40 représente la procédure de calcul du décalage de l'horloge de sécurité.

NOTE 1 Ce calcul est une version modifiée du célèbre algorithme de Cristian.

NOTE 2 FSCP 8/2 utilise le contrôle d'accès au support déterministe qui repose sur le passage de jeton. La transmission étant assurée uniquement par le nœud qui contient le jeton, plusieurs trames ne sont jamais en conflit ni placées en file d'attente dans les nœuds intermédiaires. De plus, un seul chemin logique est établi entre deux nœuds.

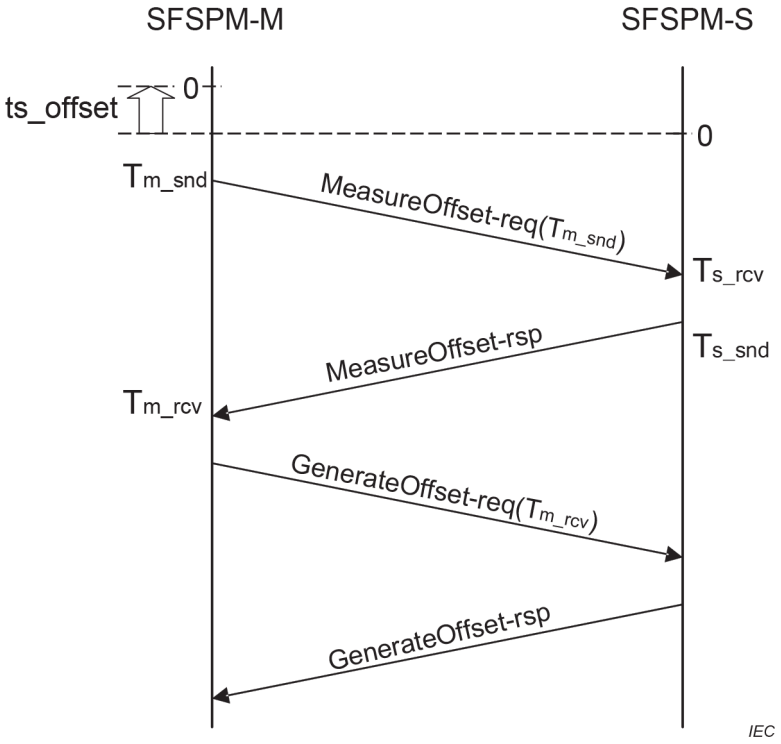


Figure 40 – Procédure de calcul du décalage de l'horloge de sécurité

SFSPM-M génère MeasureOffset-req, puis envoie MeasureOffset-req, qui inclut la valeur d'horloge de sécurité au moment de la transmission de MeasureOffset-req à SFSPM-S.

SFSPM-S reçoit MeasureOffset-req et enregistre la valeur d'horloge de sécurité au moment de la réception, ainsi que la valeur d'horloge de sécurité incluse dans MeasureOffset-req. SFSPM-S génère ensuite MeasureOffset-rsp, enregistre la valeur d'horloge de sécurité au moment de la transmission de MeasureOffset-rsp, puis envoie le MeasureOffset-rsp généré à SFSPM-M.

SFSPM-M reçoit MeasureOffset-rsp et enregistre la valeur d'horloge de sécurité au moment de la réception. SFSPM-M, qui a reçu MeasureOffset-rsp, génère alors GenerateOffset-req avec des informations sur le calcul du décalage, à savoir la valeur d'horloge de sécurité au moment de la réception de MeasureOffset-rsp, puis envoie GenerateOffset-req à SFSPM-S.

SFSPM-S reçoit GenerateOffset-req, calcule et stocke le ts_offset en fonction de la valeur d'horloge de sécurité enregistrée et des informations sur le calcul du décalage dans GenerateOffset-req. SFSPM-S génère alors GenerateOffset-rsp, qui stocke la différence entre le ts_offset utilisé et le ts_offset calculé dans OBL, puis envoie GenerateOffset-rsp à SFSPM-M.

SFSPM-S vérifie que le délai de transmission en boucle au moment du calcul du décalage se trouve dans la plage avant de calculer ts_offset à l'aide de la Formule (2). Si la valeur ne se trouve pas dans la plage, SFSPM-S ne doit pas utiliser les informations collectées dans le calcul de décalage.

$$0 < \left(T_{m\_rcv} - T_{m\_snd}\right) - \left(T_{s\_snd} - T_{s\_rcv}\right) \leq 2 \times link\_transmission\_delay \quad (2)$$

link_transmission_delay est le délai de transmission du réseau FSCP 8/2, qui est calculé à partir des trois paramètres suivants: allowable_refresh_interval, transmission_interval de SFSPM-M et transmission_interval de SFSPM-S (décrits en 12.7.2). D_{lt} est calculé à l'aide de la Formule (3).

$$D_{lt} = I_{ar} - I_{mt} - I_{st} \quad (3)$$

où

D_{lt} est le délai de transmission de liaison;

I_{ar} est l'intervalle de rafraîchissement admissible;

I_{mt} est l'intervalle de transmission de SFSPM-M;

I_{st} est l'intervalle de transmission de SFSPM-S.

La Formule (4) doit être utilisée pour calculer le décalage *ts_offset*:

$$ts\_offset = 0{,}5 \times \left(\left(T_{m\_rcv} + T_{m\_snd}\right) - \left(T_{s\_snd} + T_{s\_rcv}\right)\right) \quad (4)$$

La dispersion calculée *offset_dispersion* de la Formule (5) est incluse dans le décalage *ts_offset* calculé:

$$offset\_dispersion = 0{,}5 \times \left(\left(T_{m\_rcv} - T_{m\_snd}\right) + \left(T_{s\_rcv} - T_{s\_snd}\right)\right) \quad (5)$$

La valeur maximale de l'écart de calcul *offset_dispersion* est *link_transmission_delay*.

SFSPM-M confirme que le SFSPM-S a calculé le décalage avec la réception de GenerateOffset-rsp. SFSPM-M reçoit GenerateOffset-rsp et utilise un TS ajusté à la place du TS inclus dans GenerateOffset-rsp pour détecter l'ordre incorrect et la perte du GenerateOffset-rsp reçu, et déterminer l'intervalle de transmission décrit en 12.7.2. Le TS ajusté est une valeur obtenue en soustrayant la valeur stockée dans l'OBL du GenerateOffset-rsp reçu par SFSPM-M, c'est-à-dire en calculant la différence entre le ts_offset calculé par SFSPM-S et le ts_offset utilisé par SFSPM-S, à partir de la valeur stockée dans le TS du GenerateOffset-rsp reçu.

NOTE Si SFSPM-S modifie le ts_offset par suite d'un calcul de décalage réalisé pendant le rafraîchissement de sécurité, l'intervalle de transmission réel de SFSPM-S diffère de la valeur calculée par soustraction du TS du PDU déjà reçu du TS de GenerateOffset-rsp. La mise en œuvre de cette procédure donne deux valeurs correspondantes.

Le décalage est calculé au moment de l'établissement de la connexion de sécurité, puis régulièrement pendant le rafraîchissement de sécurité. Au moment de l'établissement de la connexion de sécurité, S-RefreshReady est utilisé comme MeasureOffset, et S-RefreshGO comme GenerateOffset. T_{m_snd} et T_{m_rcv} issus de SFSPM-M sont livrés à SFSPM-S comme le TS de S-RefreshReady et l'OBL de S-RefreshGO, respectivement. Lors du rafraîchissement de sécurité, S-RefreshMO est utilisé comme MeasureOffset, et S-RefreshGO comme GenerateOffset. T_{m_snd} and T_{m_rcv} issus de SFSPM-M sont livrés à SFSPM-S comme le TS de S-RefreshMO et l'OBL de S-RefreshGO, respectivement.

Lors du rafraîchissement de sécurité, SFSPM-M doit corriger le décalage d'horloge à l'intervalle défini ci-dessous. Le resolution_factor doit être déterminé de manière à ce que l'erreur générée par la dérive d'horloge soit toujours inférieure à 128 microsecondes, qui est l'unité de mesure de l'horloge de sécurité conformément à la Formule (6).

$$interval = transmission\_intercal \times resolution\_factor \tag{6}$$

Si l'exactitude de l'horloge de sécurité est de 100 ppm, l'erreur est de ± 100 µs par seconde, au maximum. Si les erreurs des horloges de sécurité SFSPM-M et SFSPM-S sont dans le sens opposé, la différence générée par la dérive d'horloge est de 200 µs par seconde, au maximum. A cet instant, le décalage d'horloge peut être corrigé toutes les 640 ms, voire moins, afin de maintenir l'erreur inférieure à 128 µs. Le *resolution_factor* est calculé à l'aide de la Formule (7).

$$resolution\_factor < \frac{640}{transmission\_interval} \tag{7}$$

12.7.2.6 Calcul du temps de réception

SFSPM-M doit utiliser la valeur des 16 bits inférieurs de l'horloge de sécurité au moment de la réception.

SFSPM-S doit utiliser la valeur calculée à l'aide de la Formule (8), qui repose sur *receipt_time*, qui est la valeur des 16 bits inférieurs de l'horloge de sécurité au moment de la réception, et le décalage *ts_offset*.

$$time = (receipt\_time + ts\_offset) \bmod 2^{16} \tag{8}$$

12.7.2.7 Fonctionnement de carry_counter

SFSPM-S calcule le *SFSPM_M_current_time* à l'aide de la Formule (9) à partir de *current_time*, qui représente les 16 bits inférieurs de l'horloge de sécurité de SFSPM-S, et du décalage *ts_offset*, à chaque réception et envoi d'un PDU de sécurité.

$$SFSPM\_M\_current\_time = (current\_time + ts\_offset) \bmod 2^{16} \tag{9}$$

Si la Formule (10) est respectée, carry_counter est augmenté de 1.

$$prev\_SFSPM\_M\_current\_time > SFSPM\_M\_current\_time \quad (10)$$

Ici, *prev_SFSPM_M_current_time* est le *SFSPM_M_current_time* précédemment calculé.

L'intervalle de transmission transmission_interval et l'unité de mesure et de taille current_time sont identiques. Par conséquent, le compte de dépassement de current_time est égal à 1 (valeur maximale, tant que la transmission se trouve dans le transmission_interval). Il en résulte que carry_counter est augmenté de 1.

12.8 Gestion de la couche de communication de sécurité pour FSCP 8/2

12.8.1 Définitions de paramètre

12.8.1.1 Liste de paramètres

Le Tableau 41 répertorie les paramètres utilisés par FSCP 8/2.

Tableau 41 – Paramètres utilisés par la couche de communication de sécurité

Nom de paramètre	Contenu	Configurable/Généré
connection_id	Identifiant de connexion de sécurité	Configurable
transmission_interval	Intervalle de transmission	Configurable
allowable_refresh_interval	Intervalle de rafraîchissement admissible	Configurable
allowable_delay	Délai maximal admissible	Généré par la couche de communication de sécurité
allowable_roundtrip_delay	Délai de propagation en boucle admissible	Généré par la couche de communication de sécurité

12.8.1.2 connection_id

Connection_id est un paramètre configurable qui indique l'identifiant de la relation entre la source de transmission et la destination de transmission. Sa taille est de 32 bits. Une valeur unique doit être attribuée à connection_id au sein du réseau. Pour assurer le caractère unique, connection_id doit être une valeur déduite de l'adresse de la source de transmission et de l'adresse de la destination de transmission (16 bits chacune). L'adresse de la source de transmission et l'adresse de la destination de transmission sont générées à partir du numéro de réseau et du numéro de poste (8 bits chacun).

12.8.1.3 transmission_interval

transmission_interval est un paramètre configurable qui spécifie l'intervalle maximal de transmission des PDU de sécurité lors du rafraîchissement de sécurité. Sa taille est de 16 bits, et l'unité est de 128 µs. La valeur minimale est 2.

Parfois, l'intervalle de transmission des PDU de sécurité varie. *actual_transmission_interval* doit se trouver dans la plage donnée par la Formule (11).

$$\frac{transmission\_interval}{2} < actual\_transmission\_interval \leq transmission\_interval \quad (11)$$

Pour recevoir normalement les PDU de sécurité envoyés à intervalle de transmission maximal (transmission_interval), la limite supérieure de l'intervalle de transmission réel doit être inférieure ou égale à l'intervalle de transmission maximal. D'autre part, l'intervalle de transmission réel exige la présence d'une limite inférieure pour détecter la perte d'un PDU de sécurité médian parmi trois PDU de sécurité envoyés à intervalle de transmission minimale. La Figure 41 représente la séquence dans ce type de situation. La perte du deuxième PDU de sécurité peut être détectée si la valeur est inférieure à deux fois l'intervalle de transmission minimal.

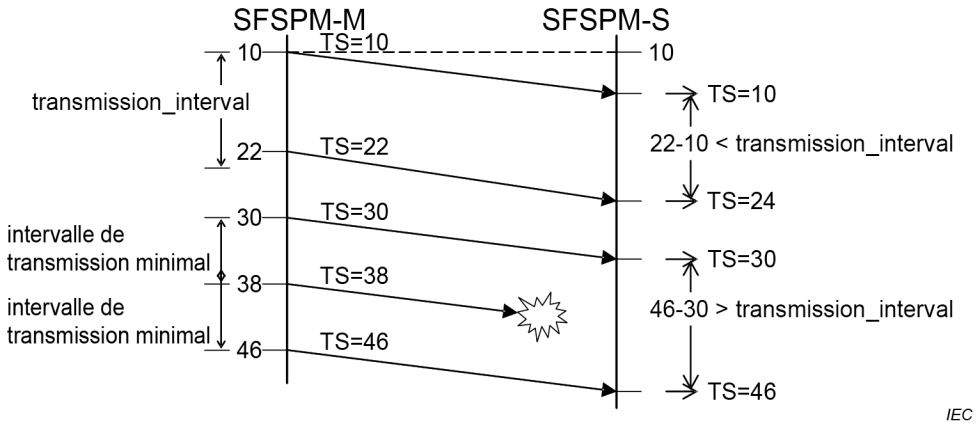


Figure 41 – Relation entre la variation de l'intervalle de transmission et transmission_interval

12.8.1.4 allowable_refresh_interval

allowable_refresh_interval est un paramètre configurable qui spécifie l'intervalle de rafraîchissement admissible par le nœud de réception. Sa taille est de 16 bits, et l'unité est de 128 µs.

La formule suivante est utilisée pour calculer allowable_refresh_interval dans le SFSPM-S lorsque des PDU de sécurité sont envoyés de SFSPM-M à SFSPM-S:

L'intervalle de rafraîchissement admissible de SFSPM-S, I_{sar}, est calculé à l'aide de la Formule (12).

$$I_{sar} = I_t + D_{lt} + T_{spc} \tag{12}$$

où

I_{sar} est l'intervalle de rafraîchissement admissible de SFSPM-S;

I_t est l'intervalle de transmission de SFSPM-M;

D_{lt} est le délai de transmission de liaison du réseau FAL Type 23;

T_{spc} est la durée du cycle de traitement de SFSPM-S.

Si SFSPM-S est un appareil logique de sécurité, la durée du cycle de traitement de SFSPM-S dépend du contenu traité. Si SFSPM-S est un appareil d'entrée/sortie de sécurité, la durée du cycle de traitement de SFSPM-S dépend de la mise en œuvre.

La Figure 42 représente le concept de détermination d'allowable_refresh_interval de SFSPM-S et de SFSPM-M.

Si le temps de retard maximal (TS3 – TS4) suit le temps de retard le plus court (TS1 – TS2) lors de la communication entre SFSPM-M et SFSPM-S, l'intervalle de réception est calculé comme suit, où transmission_interval (SFSPM-M) indique le transmission_interval de SFSPM-M.

L'intervalle de réception de SFSPM-S, I_{sr}, est calculé à l'aide de la Formule (13) et de la Formule (14).

$$I_{sr} = I_t + D_t + T_{soc} \tag{13}$$

$$I_{sr} = I_{tm} + D_{lt} + T_{spc} \tag{14}$$

où

I_{sr} est l'intervalle de réception de SFSPM-S (TS4 – TS2);

I_t est l'intervalle de transmission (TS3 – TS1);

D_t est le délai de transmission du réseau Type 23;

T_{soc} est la durée de cycle de fonctionnement de SFSPM-S;

I_{tm} est l'intervalle de transmission de SFSPM-M;

D_{lt} est le délai de transmission de liaison;

T_{spc} est la durée de cycle de traitement de SFSPM-S.

Le même concept s'applique à SFSPM-S. transmission_interval (SFSPM-S) indique le transmission_interval de SFSPM-S.

L'intervalle de rafraîchissement admissible de SFSPM-S, I_{sar}, est calculé à l'aide de la Formule (15).

$$I_{sar} = I_t + D_{lt} + T_{mpc} \tag{15}$$

où

I_{sar} est l'intervalle de rafraîchissement admissible de SFSPM-S;

I_t est l'intervalle de transmission;

D_{lt} est le délai de transmission de liaison;

T_{mpc} est la durée de cycle de traitement de SFSPM-M.

Etant donné que transmission_interval est égal à la durée de cycle de fonctionnement, la formule du calcul devient la même pour SFSPM-M et pour SFSPM-S. L'intervalle de rafraîchissement admissible, I_{ar}, est calculé à l'aide de la Formule (16).

$$I_{ar} = D_{lt} + T_{mpc} + T_{spc} \tag{16}$$

où

I_{ar} est l'intervalle de rafraîchissement admissible;

D_{lt} est le délai de transmission de liaison;

T_{mpc} est la durée de cycle de traitement de SFSPM-M;

T_{spc} est la durée de cycle de traitement de SFSPM-S.

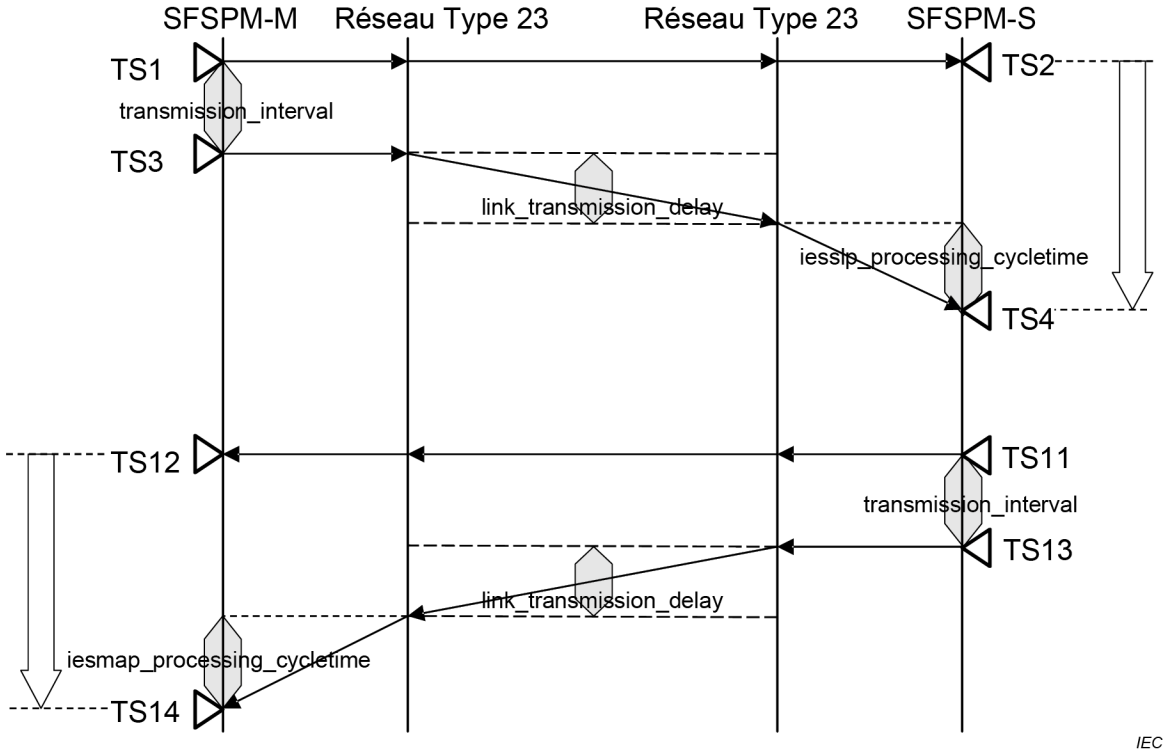


Figure 42 – Calcul d'allowable_refresh_interval

12.8.1.5 allowable_delay

allowable_delay est le délai maximal admissible. Il s'agit d'un paramètre utilisé pour détecter la présence de délais inadmissibles. Sa taille est de 16 bits, et l'unité est de 128 µs.

La formule utilisée pour calculer allowable_delay est présentée ci-dessous. Transmission_interval (SFSPM-M) et transmission_interval (SFSPM-S) indiquent respectivement les intervalles de transmission de SFSPM-M et de SFSPM-S. Comme pour allowable_refresh_interval, transmission_interval est par hypothèse égal à la durée de cycle de fonctionnement.

Le délai admissible pour SFSPM-M, D_{ma}, est calculé à l'aide de la Formule (17) et de la Formule (18).

$$D_{ma} = D_{lt} + T_{mpc} \tag{17}$$

$$D_{ma} = I_{ar} - I_{st} \tag{18}$$

Le délai admissible pour SFSPM-S, D_{sa}, est calculé à l'aide de la Formule (19) et de la Formule (20).

$$D_{sa} = D_{lt} + T_{spc} \tag{19}$$

$$D_{sa} = I_{ar} - I_{mt} \tag{20}$$

où

D_{ma} est le délai admissible de SFSPM-M;

D_{ms} est le délai admissible de SFSPM-S;

D_{lt} est le délai de transmission de liaison;

T_{mpc} est la durée de cycle de traitement de SFSPM-M;

T_{spc} est la durée de cycle de traitement de SFSPM-S;

I_{ar} est l'intervalle de rafraîchissement admissible;

I_{mt} est l'intervalle de transmission de SFSPM-M;

I_{st} est l'intervalle de transmission de SFSPM-S.

La Figure 43 représente le concept de détermination d'allowable_delay pour la transmission entre SFSPM-M et SFSPM-S, et pour la transmission entre SFSPM-S et SFSPM-M.

La période entre le moment où SFSPM-M envoie un PDU de sécurité en TS1 et le moment où SFSPM-S le reçoit en TS2 est égale à la somme du délai de transmission du réseau FSCP 8/2 et de la durée de cycle de fonctionnement de SFSPM-S côté réception. Inversement, la période entre le moment où SFSPM-S envoie un PDU de sécurité en TS3 et le moment où SFSPM-M le reçoit en TS4 est égale à la somme du délai de transmission et de la durée de cycle de fonctionnement de SFSPM-M côté réception.

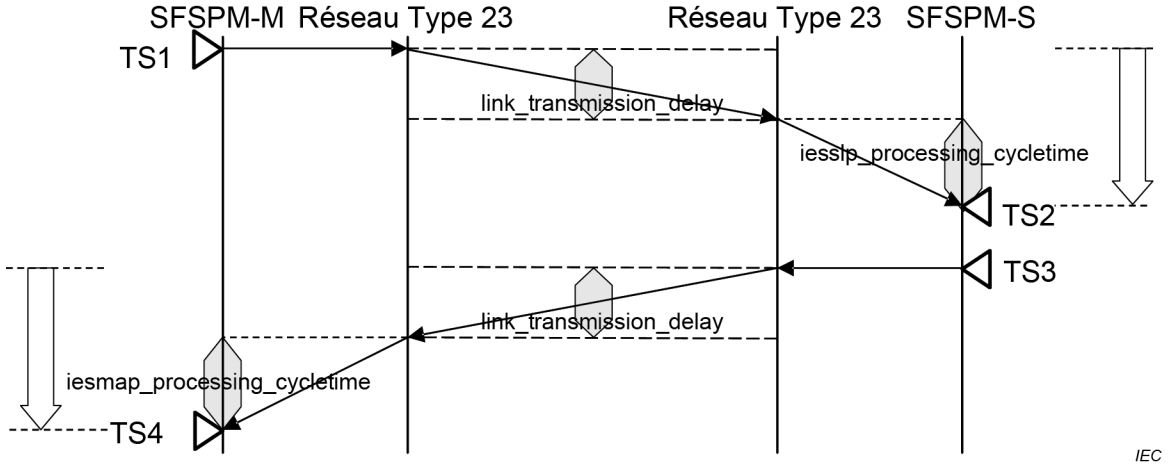


Figure 43 – Calcul d'allowable_delay

12.8.1.6 allowable_roundtrip_delay

allowable_roundtrip_delay est un paramètre que SFSPM-M utilise dans le cadre d'opérations autres que le rafraîchissement de sécurité. L'unité est de 128 µs. Elle est égale à trois fois allowable_refresh_interval. SFSPM-S utilise une valeur préalablement déterminée tant qu'il n'a pas été informé de l'allowable_refresh_interval par SFSPM-M.

12.8.2 Configuration de paramètre

Les paramètres présentés dans le Tableau 41 sont configurés dans la couche de communication de sécurité à l'aide des services décrits en 12.6.

12.8.3 Services de gestion

12.8.3.1 SM-SetSafetyStationInfo

SM-SetSafetyStationInfo est un service utilisé pour configurer les informations relatives au poste de sécurité. Le Tableau 42 présente les paramètres de SM-SetSafetyStationInfo.

Tableau 42 – SM-SetSafetyStationInfo

Nom de paramètre	Req	Ind	Rsp	Cnf
Argument	M	M(=)		
Parameter	M	M(=)		
Result			U	U(=)
R Data			U	U(=)

Parameter
Spécifie les paramètres configurés des informations relatives au poste de sécurité. Voir Tableau 43.

R Data
Contient le résultat de la configuration de paramètre. Il s'agit de n'importe quelle valeur.

Tableau 43 – Paramètres de configuration des informations relatives au poste de sécurité de SM-SetSafetyStationInfo

N°	Elément	Taille (octets)	Plage	Remarques
1	Numéro de réseau	1	0 – 255	0 et 240 à 255: Réservé
2	Numéro de poste	1	0 – 255	121-255: Réservé
3	Type de poste de sécurité	2	0x0000 – 0xFFFF	0x0: Safety PLC (PDU de sécurité) 0x1-0x3: Réservé 0x4: Appareil distant de sécurité 0x5: E/S distante de sécurité 0x6-0xFFFF: Réservé
4	Code fournisseur	2	0x0000 – 0xFFFF	Code attribué à chaque fournisseur
5	Code de modèle de fournisseur	4	0x00000000 – 0xFFFFFFFF	Code unique attribué à chaque modèle de produit géré par le fournisseur
6	Version de spécification de fonctionnement	2	0x0000 – 0xFFFF	Version des spécifications de fonctionnement du produit géré par le fournisseur
7	Version de protocole de sécurité	2	0x00 – 0xFF	Cette version: 00

12.8.3.2 SM-SetSafetyNetworkParameter

SM-SetSafetyNetworkParameter est un service utilisé pour configurer les paramètres de réseau de sécurité. Le Tableau 44 présente les paramètres de SM-SetSafetyNetworkParameter.

Tableau 44 – SM-SetSafetyNetworkParameter

Nom de paramètre	Req	Ind	Rsp	Cnf
Argument	M	M(=)		
Parameter	M	M(=)		
Result			U	U(=)
R Data			U	U(=)

Parameter
Spécifie les paramètres de réseau de sécurité. Voir Tableau 45.

R Data
Contient le résultat de la configuration de paramètre. Il s'agit de n'importe quelle valeur.

Tableau 45 – Paramètres de réseau de sécurité de SM-SetSafetyNetworkParameter

N°	Elément	Taille (octets)	Plage	Remarques
1	Numéro de réseau	1	0 – 255	0 et 240 à 255: Réservé
2	Numéro de poste	1	0 – 255	121-255: Réservé
3	Identifiant de connexion de sécurité	4	0x00000000 – 0xFFFFFFFF	
4	Type de fin de connexion de sécurité	1	0x0 – 0x1	0x0:SFSPM-M 0x1:SFSPM-S
5	Intervalle de transmission maximal	2	2 – 65535	
6	Intervalle de rafraîchissement admissible	2	1 – 65535	
7	Taille de données de sécurité	1	0-16	Unité: octets

12.8.3.3 SM-GetSafetyStationInfo

SM-GetSafetyStationInfo est un service utilisé pour lire les informations relatives au poste de sécurité. Le Tableau 46 présente les paramètres de SM-GetSafetyStationInfo.

Tableau 46 – SM-GetSafetyStationInfo

Nom de paramètre	Req	Ind	Rsp	Cnf
Argument	M	M(=)		
Parameter	M	M(=)		
Result			M	M(=)
R Data			M	M(=)

Parameter
Spécifie la destination d'acquisition. Voir Tableau 47.

R Data
Contient le résultat de l'acquisition. Voir Tableau 48.

Tableau 47 – Paramètres des informations relatives au poste de sécurité de SM-GetSafetyStationInfo (Demande)

N°	Elément	Taille (octets)	Plage	Remarques
1	Numéro de réseau	1	0 – 255	0 et 240 à 255: Réservé
2	Numéro de poste	1	0 – 255	121-255: Réservé

Tableau 48 – Paramètres des informations relatives au poste de sécurité de SM-GetSafetyStationInfo (Réponse)

N°	Elément	Taille (octets)	Plage	Remarques
1	Type de poste de sécurité	2	0x0000 – 0xFFFF	0x0: Safety PLC (PDU de sécurité) 0x1-0x3: Réservé 0x4: Appareil distant de sécurité 0x5: E/S distante de sécurité 0x6-0xFFFF: Réservé
2	Code fournisseur	2	0x0000 – 0xFFFF	Code attribué à un fournisseur pour l'identifier.
3	Code de modèle de fournisseur	4	0x00000000 – 0xFFFFFFFF	Code unique attribué à chaque modèle de produit géré par les fournisseurs.
4	Version de spécification de fonctionnement	2	0x0000 – 0xFFFF	Version des spécifications de fonctionnement du produit géré par le fournisseur.
5	Version de protocole de sécurité	2	0x00 – 0xFF	Cette version: 00

12.8.3.4 SM-GetSafetyNetworkParameter

SM-GetSafetyNetworkParameter est un service utilisé pour lire les paramètres de réseau de sécurité. Le Tableau 49 présente les paramètres de SM-GetSafetyNetworkParameter.

Tableau 49 – SM-GetSafetyNetworkParameter

Nom de paramètre	Req	Ind	Rsp	Cnf
Argument	M	M(=)		
Parameter	M	M(=)		
Result			M	M(=)
R Data			M	M(=)

Parameter
Spécifie la destination d'acquisition. Voir Tableau 50.

R Data
Contient le résultat de l'acquisition. Voir Tableau 51.

Tableau 50 – Paramètres de la demande SM-GetSafetyNetworkParameter

N°	Elément	Taille (octets)	Plage	Remarques
1	Numéro de réseau	1	0 – 255	0 et 240 à 255: Réservé
2	Numéro de poste	1	0 – 255	121-255: Réservé
3	Identifiant de connexion de sécurité	4	0x00000000 – 0xFFFFFFFF	

Tableau 51 – Paramètres de la réponse SM-GetSafetyNetworkParameter

N°	Elément	Taille (octets)	Plage	Remarques
1	Type de fin de connexion de sécurité	1	0x0 – 0x1	0x0:SFSPM-M 0x1:SFSPM-S
2	Intervalle de transmission maximal	2	1 – 65535	
3	Intervalle de rafraîchissement admissible	2	1 – 65535	
4	Taille de données de sécurité	1	0 – 16	Unité: octets

12.9 Exigences système pour FSCP 8/2

12.9.1 Voyants et commutateurs

12.9.1.1 Commutateurs

Aucun commutateur n'est spécifié pour FSCP 8/2.

12.9.1.2 Voyants

Les exigences relatives aux voyants sont spécifiées dans le Tableau 20, le Tableau 52 et le Tableau 53 avec l'interprétation suivante:

M = obligatoire (mandatory)

O = facultatif (optional)

R = recommandé

Le type, la couleur et la forme des voyants ne sont pas spécifiés. De même, lorsque des ordinateurs ou autres appareils avec écrans sont utilisés, l'indication peut être prise en charge par une indication visuelle sur l'écran. Pour la surveillance du port de communication, il est recommandé de prévoir des écrans qui permettent d'identifier le numéro de chaque port de communication sur le poste de maître de sécurité et le poste d'esclave de sécurité.

Tableau 52 – LED du moniteur

Nº	Nom de LED	Description	Poste de maître de sécurité	Poste local d'esclave de sécurité	Poste d'appareil intelligent d'esclave de sécurité	Poste d'appareil distant d'esclave de sécurité	Poste E/S distant d'esclave de sécurité
1	PW	Allumée: alimentation activée Sortie: alimentation désactivée	R	R	R	R	R
2	RUN	Allumée: fonctionnement normal Sortie: une erreur s'est produite au niveau du poste	M	R	R	O	O
3	ERR	Allumée: Erreur Maître de sécurité: ▪ conflit de numéro de poste ▪ incohérence des informations relatives au réseau échantillonné ▪ erreur au niveau du poste Esclave de sécurité: ▪ erreur au niveau du poste Clignotement: erreur de liaison de données Maître de sécurité: ▪ un poste contient une erreur de liaison de données Sortie: fonctionnement normal	M	R	R	O	O
4	MST	Allumée: le poste fonctionne comme le poste maître Sortie: le poste ne fonctionne pas comme le poste maître	O	—	—	—	—
5	D LINK	Allumée: transmission cyclique en cours Sortie: déconnexion	M	R	R	O	O
6	L.ERR	Allumée: erreur de données reçue Sortie: les données reçues sont normales	M	R	R	R	R
7	SD	Allumée: les données sont en cours de transmission Sortie: les données ne sont pas en cours de transmission	R	R	R	R	R
8	RD	Allumée: les données sont en cours de réception Sortie: les données ne sont pas en cours de réception	R	R	R	R	R

Tableau 53 – LED du moniteur de port de communication

Nº	Nom de LED	Description	Poste de maître de sécurité	Poste local d'esclave de sécurité	Poste d'appareil intelligent d'esclave de sécurité	Poste d'appareil distant d'esclave de sécurité	Poste E/S distant d'esclave de sécurité
1	LINK	Allumée: la liaison est opérationnelle Sortie: la liaison n'est pas opérationnelle	O	O	O	O	O
2	L.ER	Allumée: erreur de données reçue Sortie: les données reçues sont normales	O	O	O	O	O

12.9.2 Lignes directrices d'installation

Le présent document spécifie le protocole et les services d'un système de communication de sécurité qui repose sur le Type 23 de l'IEC 61158. Toutefois, l'utilisation d'appareils de sécurité avec le protocole de sécurité spécifié dans le présent document exige une installation correcte. Tous les appareils connectés à un système de communication de sécurité défini dans le présent document doivent suivre les recommandations et satisfaire aux spécifications données dans l'IEC 61784-5-8.

12.9.3 Temps de réponse de la fonction de sécurité

La Figure 44 représente le concept de temps de réponse pendant la communication de sécurité entre les postes de sécurité FSCP 8/2. Les calculs sont expliqués entre deux PLC de sécurité en tant qu'exemple.

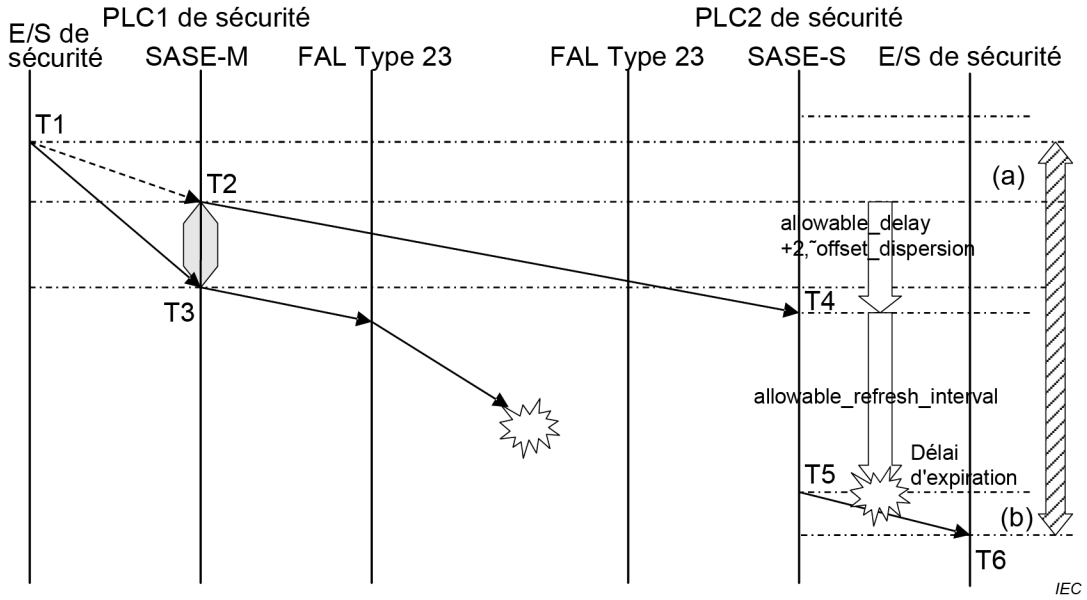


Figure 44 – Calcul du temps de réponse entre des PLC de sécurité

Le temps de réponse de la communication de sécurité entre le PLC1 de sécurité et le PLC2 de sécurité de la Figure 44 est égal à la période entre T1 et T6. La période entre T1 et T2 est le temps de réponse de l'appareil d'entrée. Si la transmission a lieu immédiatement avant T2, elle est assurée à l'intervalle de transmission suivant, et donne un temps d'attente égal à transmission_interval (SASE-M et SFSPM-M).

Le cas le plus défavorable est lorsque le PDU de sécurité envoyé en T3 est perdu. En T5, il est déterminé que le PDU de sécurité envoyé en T3 n'est pas arrivé dans le temps imparti. La période entre T5 et T6 est le temps de réponse de l'appareil d'entrée. A cet instant, le temps de réponse le plus défavorable, *TR*, est calculé à l'aide de la Formule (21), de la Formule (22) et de la Formule (23).

$$TR = a + D_a + (2 \times O_d) + I_{ar} + b \tag{21}$$

$$TR = a + D_{lt} + T_{mpc} + (2 \times D_{lt}) + I_t + D_{lt} + T_{spc} + b \tag{22}$$

$$TR = a + b + T_{mpc} + (4 \times D_{lt}) + (2 \times T_{spc}) \tag{23}$$

où

TR est le temps de réponse;

a est le temps de réponse de l'appareil d'entrée;

D_a est le délai admissible;

O_d est la dispersion de décalage;

I_{ar} est l'intervalle de rafraîchissement admissible;

b est le temps de réponse de l'appareil de sortie;

D_{lt} est le délai de transmission de la liaison de réseau FSCP 8/2;

T_{spc} est la durée de cycle de traitement de SASE-S;

T_{mpc} est la durée de cycle de traitement de SASE-M;

I_t est l'intervalle de transmission (SFSPM-M).

NOTE Plus d'informations sur l'ajout de 2 × dispersion de décalage sont fournies à l'Annexe A.

12.9.4 Durée des demandes (ou sollicitations)

La durée de la sollicitation entre l'application relative à la sécurité et la couche de communication de sécurité doit être suffisante de manière à ce que la sollicitation soit détectée par l'application dans le cadre du temps de réponse le plus long de la fonction de sécurité.

12.9.5 Contraintes liées au calcul des caractéristiques du système

FSCP 8/2 est un protocole de communication de sécurité fonctionnel SIL 3, de telle sorte que le taux d'erreur résiduel par heure de la SCL est (λ_{SCL}) < 10^{-9}.

La seule restriction de l'IEC 61158 Type 23 lors de la mise en œuvre d'un système de sécurité FSCP 8/2 est le nombre maximal d'éléments de stockage des messages (N_{SE}), tels que les commutateurs et les routeurs. Ce nombre est limité par une relation au nombre maximal de connexions logiques admises dans une seule fonction de sécurité (*m*) et dans l'intervalle de transmission (I_t).

Un système de sécurité FSCP 8/2 doit satisfaire à une contrainte sur N_{SE} en fonction de m et de I_t, comme indiqué par la Formule (24).

$$N_{SE}\,(I_T, m) < \frac{3{,}602 \times 10^7}{I_t \times m} - \frac{3{,}515 \times 10^3}{{I_t}^2} \quad (24)$$

où

N_{SE} est le nombre d'éléments de stockage dans le canal noir, tels que les commutateurs et les routeurs;

I_t est la plage de l'intervalle de transmission (ms) compris entre 1 et 2 000;

m est le nombre maximal de connexions logiques admises dans une seule fonction de sécurité.

La Figure 45 montre la relation entre N_{SE} et m pour différentes valeurs de I_t (voir légende des couleurs du graphique) obtenues à l'aide de la Formule (24).

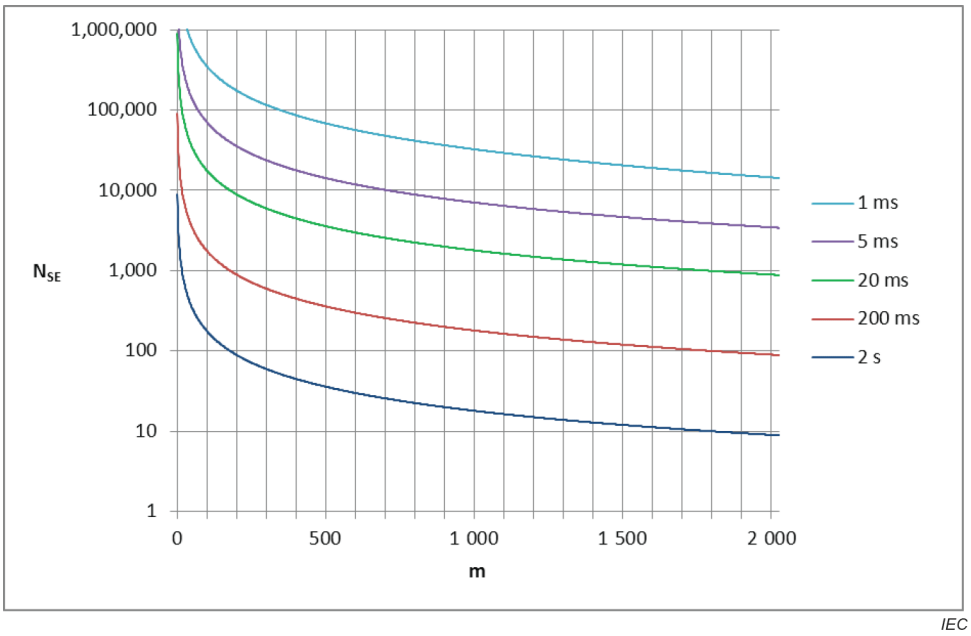


Figure 45 – Contraintes sur N_{SE} et m

Il peut être observé à la Figure 45 que, pour des limites pratiques de m < 100 et de N_{SE} < 100, l'intervalle de transmission ne pose aucun problème lors de la mise en œuvre de FSCP 8/2. Toutefois, pour des fonctions de sécurité très complexes (m > 500) ou de vastes installations de canal noir (N_{SE} > 500), les contraintes imposées aux réseaux de sécurité qui utilisent un intervalle de transmission de sécurité lent deviennent préoccupantes et la Formule (24) doit être utilisée pour calculer ces limites.

12.9.6 Maintenance

Aucune exigence spécifique à la SCL pour la maintenance n'est exigée pour FSCP 8/2.

Les spécifications du comportement du système en cas de réparation et de remplacement de l'appareil n'entrent pas dans le domaine d'application du présent document. La spécification de ces activités et les responsabilités ne concernent pas la spécification des services et des protocoles. En règle générale, cela fait partie intégrante d'un plan de gestion de sécurité fonctionnelle. Toutefois, la réparation, le remplacement et la maintenance, la validation de la sécurité globale, le fonctionnement global, les modifications, les mises à niveau et le déclassement ou la mise au rebut conformément à l'IEC 61508 sont des questions importantes qui doivent être prises en considération. Il est également recommandé de prendre contact avec le fournisseur de l'appareil ou du système.

Pour obtenir des informations relatives à la programmation du SRP et à la définition des paramètres des appareils de sécurité, il est vivement recommandé de prendre contact avec le fournisseur de l'appareil ou du système. De plus, il est recommandé de tenir compte des Spécifications de sécurité CC-Link. Ces documents contiennent des informations complémentaires destinées aux utilisateurs de système FSCP 8/2.

NOTE 3 Les documents [30] et [31] contiennent des informations importantes relatives à la maintenance.

Des exigences de maintenance supplémentaires (entre autres) sont spécifiées dans l'IEC 61508, l'IEC 61511 et/ou l'IEC 62061.

12.9.7 Manuel de sécurité

Le fournisseur d'esclaves de sécurité qui intègre la SCL conformément à FSCP 8/2 doit élaborer un manuel de sécurité approprié conformément à l'IEC 61508. Ce manuel de sécurité doit également comprendre les exigences d'installation spécifiées en 11.9.2, ainsi que les lignes directrices applicables à la configuration des commutateurs d'appareil utilisés.

Un système de communication de sécurité complet qui repose sur l'IEC 61158 Type 23 doit tenir compte des Spécifications de sécurité CC-Link.

NOTE 1 Les documents [30] et [31] contiennent des informations importantes relatives au manuel de sécurité.

NOTE 2 Avant de commencer la mise en œuvre d'un appareil de sécurité, il est judicieux de prendre contact avec la CPLA pour déterminer si des modifications ont été apportées aux lignes directrices et/ou exigences de mise en œuvre.

12.10 Evaluation de FSCP 8/2

Il revient au fabricant de développer l'appareil en fonction des processus appropriés conformes aux normes de sécurité (voir l'IEC 61508, l'IEC 61511, IEC 62061, etc.) et aux règlements juridiques pertinents (Directive européenne relative aux machines, par exemple). Des informations complémentaires sont fournies à l'Annexe B.

Annexe A
(informative)

Informations supplémentaires pour les profils de communication de sécurité fonctionnelle de la CPF 8

A.1 Calcul de la fonction de hachage pour FSCP 8/1

Le CRC32 pour le protocole FSCP 8/1 est calculé à l'aide de l'algorithme suivant:

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

Il s'agit de l'algorithme défini sous la forme 0x104C11DB7 par l'ISO/IEC/IEEE 8802-3.

La longueur du code est de 96 bits.

Le tracé de la probabilité d'erreurs résiduelles en fonction du taux d'erreurs sur les bits (TEB) démontre un comportement approprié. Les valeurs représentatives sont indiquées dans le Tableau A.1.

Tableau A.1 – Probabilité d'erreurs résiduelles du CRC pour FSCP 8/1

n (bits)	TEB = 2/n	TEB = 4/n	TEB = 0,01	TEB = 0 001	TEB = 0,0001
96	8.5046432E-14	6.0272142E-12	4.3703467E-16	6.7137731E-24	6.9713053E-32

A.2 Calcul de la fonction de hachage pour FSCP 8/2

Le CRC32 pour le protocole FSCP 8/2 est calculé à l'aide de l'algorithme suivant:

$$G(x) = x^{32} + x^{31} + x^{30} + x^{29} + x^{28} + x^{24} + x^{23} + x^{20} + x^{17} + x^{13} + x^{11} + x^4 + x^2 + 1$$

Il s'agit de l'algorithme défini sous la forme 0x1F1922815 donné en [32].

La longueur du code varie de 224 bits à 992 bits par incréments de 32 bits.

Les tracés de la probabilité d'erreurs résiduelles en fonction du taux d'erreurs sur les bits (TEB) démontrent un comportement approprié. Les valeurs représentatives sont indiquées dans le Tableau A.2.

Tableau A.2 – Probabilité d'erreurs résiduelles du CRC pour FSCP 8/2

n (bits)	TEB = 2/n	TEB = 4/n	TEB = 0,01	TEB = 0 001	TEB = 0,0001
224	4.0322236E-13	1.6638772E-11	7.9879086E-13	5.3605698E-20	6.5083171E-28
256	4.0958621E-13	1.6802011E-11	1.7536098E-12	1.5470990E-19	1.9329636E-27
288	4.1226780E-13	1.6845400E-11	3.3658478E-12	3.8931551E-19	5.0054622E-27
320	4.1234883E-13	1.6806216E-11	5.8216501E-12	8.8020027E-19	1.1645257E-26
352	4.1362666E-13	1.6817799E-11	9.3328421E-12	1.8403714E-18	2.5054735E-26
384	4.1494272E-13	1.6836188E-11	1.4028534E-11	3.5989796E-18	5.0416342E-26
416	4.1583997E-13	1.6843934E-11	1.9967756E-11	6.6464215E-18	9.5802640E-26
448	4.1662508E-13	1.6851175E-11	2.7160147E-11	1.1697734E-17	1.7349197E-25
480	4.1738988E-13	1.6860416E-11	3.5547838E-11	1.9756122E-17	3.0147964E-25
512	4.1818700E-13	1.6873006E-11	4.5015881E-11	3.2193220E-17	5.0546386E-25
544	4.1892070E-13	1.6885164E-11	5.5390975E-11	5.0825605E-17	8.2104736E-25
576	4.1948634E-13	1.6892887E-11	6.6460435E-11	7.8003437E-17	1.2964312E-24
608	4.1998645E-13	1.6899575E-11	7.8014686E-11	1.1675705E-16	1.9964542E-24
640	4.2043580E-13	1.6905565E-11	8.9834198E-11	1.7089060E-16	3.0062514E-24
672	4.2083214E-13	1.6910621E-11	1.0170590E-10	2.4511218E-16	4.4360174E-24
704	4.2120519E-13	1.6915658E-11	1.1343936E-10	3.4519998E-16	6.4270369E-24
736	4.2154801E-13	1.6920328E-11	1.2486316E-10	4.7811770E-16	9.1575007E-24
768	4.2186554E-13	1.6924719E-11	1.3583561E-10	6.5219642E-16	1.2850293E-23
800	4.2217609E-13	1.6929400E-11	1.4624685E-10	8.7732699E-16	1.7781940E-23
832	4.2247640E-13	1.6934195E-11	1.5601264E-10	1.1650838E-15	2.4291166E-23
864	4.2275033E-13	1.6938486E-11	1.6507409E-10	1.5288711E-15	3.2788831E-23
896	4.2300762E-13	1.6942569E-11	1.7340149E-10	1.9842178E-15	4.3772232E-23
928	4.2324940E-13	1.6946446E-11	1.8098527E-10	2.5488862E-15	5.7836829E-23
960	4.2347661E-13	1.6950117E-11	1.8783384E-10	3.2430792E-15	7.5691417E-23
992	4.2369108E-13	1.6953615E-11	1.9397014E-10	4.0896408E-15	9.8174726E-23

A.3 Signification de la formule de calcul du temps de réponse pour FSCP 8/2

La période entre le temps T2 de la transmission SFSPM-M et le temps T4 de la réception SFSPM-S de la Figure 44 est le délai maximal admissible. Dans la formule de calcul du temps de réponse, la période entre T2 et T4 est allowable_delay + 2 × offset_dispersion. La Figure A.1 représente la signification de l'ajout de 2 × offset_dispersion.

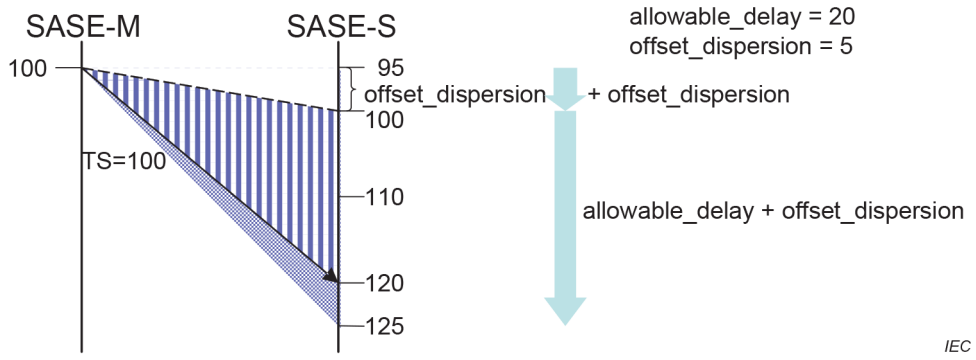


Figure A.1 – allowable_delay et écart de calcul de décalage

Compte tenu de la possibilité d'un écart de calcul d'offset_dispersion dans le calcul de décalage, une formule qui tient compte de l'écart de calcul d'offset_dispersion dans l'allowable_delay de délai admissible est utilisée en déterminant le délai admissible en 12.7.2. De plus, une différence maximale d'offset_dispersion se produit entre les horloges de sécurité SFSPM-M et SFSPM-S. En conséquence, l'ajout de 2 × offset_dispersion (valeur combinée) est exigé.

Annexe B
(informative)

Informations pour l'évaluation des profils de communication de sécurité fonctionnelle de la CPF 8

Selon les règles de l'IEC, le présent document n'énonce pas les conditions de validation de la conformité. Toutefois, les essais et validation de conformité des appareils FSCP 8/1 et FSCP 8/2 à l'IEC 61784-3-8 peuvent être exigés par la loi.

Les informations relatives aux essais et à la conformité au présent document peuvent être obtenues auprès des comités nationaux de l'IEC ou de l'organisation de bus de terrain compétente.

NOTE Pour l'IEC 61784-3-8, l'organisation de bus de terrain compétente est CC-Link Partner Association (voir www.cc-link.org).

Bibliographie

[1] IEC 60050 (toutes les parties), *Vocabulaire Electrotechnique International* (disponible à l'adresse <http://www.electropedia.org/)

NOTE Voir également le dictionnaire multilingue de l'IEC – Electricité, électronique et télécommunications (disponible sur CD-ROM et à l'adresse <http://www.electropedia.org>).

[2] IEC 60050-191:1990 [5], *Vocabulaire Electrotechnique International – Chapitre 191: Sûreté de fonctionnement et qualité de service*

[3] IEC 61000-1-2, *Compatibilité électromagnétique (CEM) – Partie 1-2: Généralités – Méthodologie pour la réalisation de la sécurité fonctionnelle des systèmes électriques et électroniques, y compris les équipements, du point de vue des phénomènes électromagnétiques*

[4] IEC 61000-6-7, *Compatibilité électromagnétique (CEM) – Partie 6-7: Normes génériques – Exigences d'immunité pour les équipements visant à exercer des fonctions dans un système lié à la sécurité (sécurité fonctionnelle) dans des sites industriels*

[5] IEC 61010-2-201, *Exigences de sécurité pour appareils électriques de mesurage, de régulation et de laboratoire – Partie 2-201: Exigences particulières pour les équipements de commande*

[6] IEC 61131-6, *Automates programmables – Partie 6: Sécurité fonctionnelle*

[7] IEC 61158-1, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 1: Présentation et lignes directrices des séries IEC 61158 et IEC 61784*

[8] IEC 61158-5 (toutes les parties), *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 5: Définition des services de la couche application*

[9] IEC 61496 (toutes les parties), *Sécurité des machines – Equipements de protection électrosensibles*

[10] IEC 61508-1:2010, *Sécurité fonctionnelle des systèmes électriques/électroniques/ électroniques programmables relatifs à la sécurité – Partie 1: Exigences générales*

[11] IEC 61508-4:2010, *Sécurité fonctionnelle des systèmes électriques/électroniques/ électroniques programmables relatifs à la sécurité – Partie 4: Définitions et abréviations*

[12] IEC 61508-5:2010, *Sécurité fonctionnelle des systèmes électriques/électroniques/ électroniques programmables relatifs à la sécurité – Partie 5: Exemples de méthodes pour la détermination des niveaux d'intégrité de sécurité*

[13] IEC 61784-3 (toutes les parties), *Réseaux de communication industriels – Profils – Partie 3: Bus de terrain de sécurité fonctionnelle*

[14] IEC 61784-5 (toutes les parties), *Réseaux de communication industriels – Profils – Partie 5: Installation des bus de terrain – Profils d'installation pour CPF x*

[15] IEC 61800-5-2, *Entraînements électriques de puissance à vitesse variable – Partie 5-2: Exigences de sécurité – Fonctionnelle*

---

5 Supprimée.

[16] IEC 61918:2018, *Réseaux de communication industriels – Installation de réseaux de communication dans des locaux industriels*

[17] IEC 62280:2014, *Applications ferroviaires – Systèmes de signalisation, de télécommunication et de traitement – Communication de sécurité dans les systèmes de transmission*

[18] IEC 62443 (toutes les parties), *Réseaux industriels de communication – Sécurité dans les réseaux et les systèmes*

[19] Guide ISO/IEC 51:2014, *Aspects liés à la sécurité – Principes directeurs pour les inclure dans les normes*

[20] ISO/IEC 2382:2015, *Technologies de l'information – Vocabulaire*

[21] ISO/IEC 7498-1, *Technologies de l'information – Interconnexion de systèmes ouverts (OSI) – Modèle de référence de base: le modèle de base*

[22] ISO 10218-1, *Robots et dispositifs robotiques – Exigences de sécurité pour les robots industriels – Partie 1: Robots*

[23] ISO 13849 (toutes les parties), *Sécurité des machines – Parties des systèmes de commande relatives à la sécurité*

[24] ISO 13849-1:2015, *Sécurité des machines – Parties des systèmes de commande relatives à la sécurité – Partie 1: Principes généraux de conception*

[25] ISO 13849-2, *Sécurité des machines – Parties des systèmes de commande relatives à la sécurité – Partie 2: Validation*

[26] ANDREW S. TANENBAUM, DAVID J. WETHERALL, *Computer Networks*, 5e édition, Prentice Hall, N.J., ISBN-10: 0132126958, ISBN-13: 978-0132126953

[27] W. WESLEY PETERSON, EDWARD J. WELDON, *Error-Correcting Codes*, 2e édition, 1972, MIT-Press, ISBN 0-262-16-039-0

[28] GUY E. CASTAGNOLI, *On the Minimum Distance of Long Cyclic Codes and Cyclic Redundancy-Check Codes*, 1989, Dissertation Nº 8979 de l'ETH Zurich, Suisse

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

[30] CC-Link Safety Specifications, *Overview/Protocol, BAP-C1603-001, CLPA* (disponible en anglais seulement)

[31] CC-Link Safety Specifications, *Implementation, BAP-C1603-002, CLPA* (disponible en anglais seulement)

[32] CC-Link Safety Specifications, *Profiles, BAP-C1603-003, CLPA* (disponible en anglais seulement)

[33] CC-Link IE Safety Specifications, *Overview, BAP-C1606-001, CLPA* (disponible en anglais seulement)

[34] CC-Link IE Safety Specifications, *Application Layer Service and Protocol Communication profile, BAP-C1606-002, CLPA* (disponible en anglais seulement)

_____

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

3, rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

Tel: + 41 22 919 02 11
info@iec.ch
www.iec.ch