

# INTERNATIONAL STANDARD

## NORME INTERNATIONALE



**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**

IECNORM.COM : Click to view the full PDF of IEC 61784-3-8:2016



## THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2016 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'IEC ou du Comité national de l'IEC du pays du demandeur. Si vous avez des questions sur le copyright de l'IEC ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de l'IEC de votre pays de résidence.

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

Tel.: +41 22 919 02 11  
Fax: +41 22 919 03 00  
[info@iec.ch](mailto:info@iec.ch)  
[www.iec.ch](http://www.iec.ch)

### About the IEC

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

### About IEC publications

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

#### IEC Catalogue - [webstore.iec.ch/catalogue](http://webstore.iec.ch/catalogue)

The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

#### IEC publications search - [www.iec.ch/searchpub](http://www.iec.ch/searchpub)

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](http://webstore.iec.ch/justpublished)

Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and also once a month by email.

#### Electropedia - [www.electropedia.org](http://www.electropedia.org)

The world's leading online dictionary of electronic and electrical terms containing 20 000 terms and definitions in English and French, with equivalent terms in 15 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

#### IEC Glossary - [std.iec.ch/glossary](http://std.iec.ch/glossary)

65 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

#### IEC Customer Service Centre - [webstore.iec.ch/csc](http://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: [csc@iec.ch](mailto:csc@iec.ch).

### 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.

#### Catalogue IEC - [webstore.iec.ch/catalogue](http://webstore.iec.ch/catalogue)

Application autonome pour consulter tous les renseignements bibliographiques sur les Normes internationales, Spécifications techniques, Rapports techniques et autres documents de l'IEC. Disponible pour PC, Mac OS, tablettes Android et iPad.

#### Recherche de publications IEC - [www.iec.ch/searchpub](http://www.iec.ch/searchpub)

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](http://webstore.iec.ch/justpublished)

Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et aussi une fois par mois par email.

#### Electropedia - [www.electropedia.org](http://www.electropedia.org)

Le premier dictionnaire en ligne de termes électroniques et électriques. Il contient 20 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans 15 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

#### Glossaire IEC - [std.iec.ch/glossary](http://std.iec.ch/glossary)

65 000 entrées terminologiques électrotechniques, en anglais et en français, extraites des articles Termes et Définitions des publications IEC parues depuis 2002. Plus certaines entrées antérieures extraites des publications des CE 37, 77, 86 et CISPR de l'IEC.

#### Service Clients - [webstore.iec.ch/csc](http://webstore.iec.ch/csc)

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: [csc@iec.ch](mailto:csc@iec.ch).

# INTERNATIONAL STANDARD

## NORME INTERNATIONALE



**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 978-2-8322-3491-4

**Warning! Make sure that you obtained this publication from an authorized distributor.  
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.**

## CONTENTS

|                                                                                     |    |
|-------------------------------------------------------------------------------------|----|
| FOREWORD.....                                                                       | 7  |
| 0 Introduction .....                                                                | 9  |
| 0.1 General.....                                                                    | 9  |
| 0.2 Patent declaration .....                                                        | 11 |
| 1 Scope.....                                                                        | 12 |
| 2 Normative references.....                                                         | 12 |
| 3 Terms, definitions, symbols, abbreviated terms and conventions.....               | 13 |
| 3.1 Terms and definitions .....                                                     | 13 |
| 3.1.1 Common terms and definitions .....                                            | 14 |
| 3.1.2 CPF 8: Additional terms and definitions .....                                 | 20 |
| 3.2 Symbols and abbreviated terms.....                                              | 21 |
| 3.2.1 Common symbols and abbreviated terms.....                                     | 21 |
| 3.2.2 CPF 8: Additional symbols and abbreviated terms.....                          | 22 |
| 3.3 Conventions.....                                                                | 22 |
| 4 Overview .....                                                                    | 22 |
| 5 General .....                                                                     | 22 |
| 6 Safety communication layer services.....                                          | 23 |
| 7 Safety communication layer protocol .....                                         | 23 |
| 8 Safety communication layer management.....                                        | 23 |
| 9 System requirements .....                                                         | 23 |
| 10 Assessment.....                                                                  | 23 |
| 11 FSCP 8/1 .....                                                                   | 23 |
| 11.1 Scope – FSCP 8/1.....                                                          | 23 |
| 11.2 Normative references – FSCP 8/1.....                                           | 23 |
| 11.3 Terms, definitions, symbols, abbreviated terms and conventions – FSCP 8/1..... | 23 |
| 11.4 Overview of FSCP 8/1 (CC-Link Safety™) .....                                   | 23 |
| 11.5 General – FSCP 8/1 .....                                                       | 24 |
| 11.5.1 External documents providing specifications for the profile.....             | 24 |
| 11.5.2 Safety functional requirements .....                                         | 24 |
| 11.5.3 Safety measures .....                                                        | 24 |
| 11.5.4 Safety communication layer structure .....                                   | 26 |
| 11.5.5 Relationships with FAL (and DLL, PhL).....                                   | 26 |
| 11.6 Safety communication layer services for FSCP 8/1.....                          | 27 |
| 11.6.1 General .....                                                                | 27 |
| 11.6.2 SASEs .....                                                                  | 27 |
| 11.6.3 SARs .....                                                                   | 28 |
| 11.6.4 Process data SAR ASEs .....                                                  | 28 |
| 11.7 Safety communication layer protocol for FSCP 8/1 .....                         | 29 |
| 11.7.1 Safety PDU format .....                                                      | 29 |
| 11.7.2 State description .....                                                      | 36 |
| 11.8 Safety communication layer management for FSCP 8/1 .....                       | 40 |
| 11.8.1 General .....                                                                | 40 |
| 11.8.2 Connection establishment and confirmation processing.....                    | 41 |
| 11.8.3 Safety slave verification .....                                              | 41 |
| 11.9 System requirements for FSCP 8/1 .....                                         | 42 |

|                       |                                                                                          |     |
|-----------------------|------------------------------------------------------------------------------------------|-----|
| 11.9.1                | Indicators and switches .....                                                            | 42  |
| 11.9.2                | Installation guidelines.....                                                             | 43  |
| 11.9.3                | Safety function response time .....                                                      | 43  |
| 11.9.4                | Duration of demands .....                                                                | 45  |
| 11.9.5                | Constraints for calculation of system characteristics .....                              | 45  |
| 11.9.6                | Maintenance .....                                                                        | 46  |
| 11.9.7                | Safety manual.....                                                                       | 47  |
| 11.10                 | Assessment for FSCP 8/1.....                                                             | 47  |
| 12                    | FSCP 8/2 .....                                                                           | 47  |
| 12.1                  | Scope – FSCP 8/2.....                                                                    | 47  |
| 12.2                  | Normative references – FSCP 8/2.....                                                     | 47  |
| 12.3                  | Terms, definitions, symbols, abbreviated terms and conventions – FSCP 8/2.....           | 47  |
| 12.4                  | Overview of FSCP 8/2 (CC-Link IE™ Safety communication function).....                    | 47  |
| 12.5                  | General – FSCP 8/2 .....                                                                 | 48  |
| 12.5.1                | External documents providing specifications for the profile.....                         | 48  |
| 12.5.2                | Safety functional requirements .....                                                     | 48  |
| 12.5.3                | Safety measures .....                                                                    | 49  |
| 12.5.4                | Safety communication layer structure .....                                               | 53  |
| 12.5.5                | Relationships with FAL (and DLL, PhL).....                                               | 54  |
| 12.6                  | Safety communication layer services for FSCP 8/2.....                                    | 54  |
| 12.6.1                | General .....                                                                            | 54  |
| 12.6.2                | Connection reestablishment services.....                                                 | 54  |
| 12.6.3                | Data transmission services.....                                                          | 55  |
| 12.6.4                | Connection termination notification services .....                                       | 56  |
| 12.7                  | Safety communication layer protocol for FSCP 8/2.....                                    | 56  |
| 12.7.1                | Safety PDU format .....                                                                  | 56  |
| 12.7.2                | Safety FAL service protocol machine (SFSPM).....                                         | 62  |
| 12.8                  | Safety communication layer management for FSCP 8/2 .....                                 | 85  |
| 12.8.1                | Parameter Definitions.....                                                               | 85  |
| 12.8.2                | Parameter Setup.....                                                                     | 89  |
| 12.8.3                | Management Services.....                                                                 | 89  |
| 12.9                  | System requirements for FSCP 8/2.....                                                    | 92  |
| 12.9.1                | Indicators and switches .....                                                            | 92  |
| 12.9.2                | Installation guidelines.....                                                             | 94  |
| 12.9.3                | Safety function response time .....                                                      | 94  |
| 12.9.4                | Duration of demands .....                                                                | 95  |
| 12.9.5                | Constraints for calculation of system characteristics .....                              | 95  |
| 12.9.6                | Maintenance .....                                                                        | 97  |
| 12.9.7                | Safety manual.....                                                                       | 97  |
| 12.10                 | Assessment for FSCP 8/2.....                                                             | 98  |
| Annex A (informative) | Additional information for functional safety communication profiles of CPF 8.....        | 99  |
| A.1                   | Hash function calculation for FSCP 8/1.....                                              | 99  |
| A.2                   | Hash function calculation for FSCP 8/2.....                                              | 99  |
| A.3                   | Meaning of response time calculation formula for FSCP 8/2 .....                          | 99  |
| Annex B (informative) | Information for assessment of the functional safety communication profiles of CPF 8..... | 100 |
| Bibliography          | .....                                                                                    | 101 |

|                                                                                                       |    |
|-------------------------------------------------------------------------------------------------------|----|
| Figure 1 – Relationships of IEC 61784-3 with other standards (machinery).....                         | 9  |
| Figure 2 – Relationships of IEC 61784-3 with other standards (process) .....                          | 10 |
| Figure 3 – Relationship between SCL and the other layers of IEC 61158 Type 18 .....                   | 26 |
| Figure 4 – State diagram.....                                                                         | 37 |
| Figure 5 – Detection of unintended repetition .....                                                   | 50 |
| Figure 6 – Detection of incorrect sequence.....                                                       | 51 |
| Figure 7 – Detection of loss .....                                                                    | 51 |
| Figure 8 – Detection of unacceptable delay by time stamps .....                                       | 52 |
| Figure 9 – Detection of unacceptable delay by timer .....                                             | 53 |
| Figure 10 – Protocol Hierarchy .....                                                                  | 54 |
| Figure 11 – Safety PDU Structure .....                                                                | 57 |
| Figure 12 – CTRL Configuration .....                                                                  | 57 |
| Figure 13 – SASE-M and SASE-S TS .....                                                                | 60 |
| Figure 14 – S-Data during safety refresh .....                                                        | 60 |
| Figure 15 – S-Data not during safety refresh .....                                                    | 61 |
| Figure 16 – S-Data header configuration .....                                                         | 61 |
| Figure 17 – CRC calculation.....                                                                      | 62 |
| Figure 18 – Communication models.....                                                                 | 62 |
| Figure 19 – SFSPM state transition diagram.....                                                       | 63 |
| Figure 20 – Connection establishment sequence .....                                                   | 65 |
| Figure 21 – Communication sequence during safety refresh communication.....                           | 65 |
| Figure 22 – Offset measurement and generation sequence during safety refresh<br>communication .....   | 66 |
| Figure 23 – SFSPM-M state transition diagram.....                                                     | 67 |
| Figure 24 – Sequence other than during safety refresh .....                                           | 70 |
| Figure 25 – S-Connect-req .....                                                                       | 71 |
| Figure 26 – S-InitConfirmNetPrm-req .....                                                             | 71 |
| Figure 27 – net_prm_list .....                                                                        | 72 |
| Figure 28 – S-InitVerifyStnPrm-req.....                                                               | 72 |
| Figure 29 – stn_prm_list .....                                                                        | 72 |
| Figure 30 – S-InvokeFunc-req .....                                                                    | 73 |
| Figure 31 – S-WriteErrorInfo-req .....                                                                | 73 |
| Figure 32 – date_and_time_of_occurrence .....                                                         | 74 |
| Figure 33 – SFSPM-S state transition diagram .....                                                    | 75 |
| Figure 34 – Sequence other than during safety refresh .....                                           | 80 |
| Figure 35 – S-Connect-rsp .....                                                                       | 80 |
| Figure 36 – S-InitConfirmNetPrm-rsp.....                                                              | 81 |
| Figure 37 – S-InitVerifyStnPrm-rsp .....                                                              | 81 |
| Figure 38 – S-InvokeFunc-rsp .....                                                                    | 82 |
| Figure 39 – Offset calculation procedure of safety clock .....                                        | 83 |
| Figure 40 – Relationship between transmission interval fluctuation and<br>transmission_interval ..... | 86 |
| Figure 41 – Calculation of allowable_refresh_interval .....                                           | 88 |
| Figure 42 – Calculation of allowable_delay .....                                                      | 89 |

|                                                                                   |    |
|-----------------------------------------------------------------------------------|----|
| Figure 43 – Calculation of response time between safety PLCs.....                 | 94 |
| Figure 44 – Relationship between safety connections and residual error rate ..... | 97 |
| Figure A.1 – allowable_delay and offset calculation deviation .....               | 99 |
| Table 1 – Selection of the various measures for possible errors.....              | 25 |
| Table 2 – M1 safety device manager attribute format.....                          | 30 |
| Table 3 – S1 safety device manager attribute format .....                         | 30 |
| Table 4 – M1 safety connection manager attribute format .....                     | 30 |
| Table 5 – S1 safety connection manager attribute format.....                      | 30 |
| Table 6 – M1 safety cyclic transmission attribute format .....                    | 31 |
| Table 7 – S1 safety cyclic transmission attribute format.....                     | 31 |
| Table 8 – M1 safety device manager attribute encoding.....                        | 32 |
| Table 9 – S1 safety device manager attribute encoding .....                       | 32 |
| Table 10 – M1 safety connection manager attribute encoding .....                  | 32 |
| Table 11 – S1 safety connection manager attribute encoding.....                   | 33 |
| Table 12 – M1 safety cyclic transmission attribute encoding.....                  | 33 |
| Table 13 – S1 safety cyclic transmission attribute encoding.....                  | 35 |
| Table 14 – Safety master monitor timer operation.....                             | 39 |
| Table 15 – Safety slave monitor timer operation .....                             | 39 |
| Table 16 – Safety data monitor timer operation.....                               | 39 |
| Table 17 – Details of connection establishment and confirmation processing.....   | 41 |
| Table 18 – Details of slave information verification processing.....              | 41 |
| Table 19 – Details of safety slave parameter transmission processing.....         | 42 |
| Table 20 – Monitor LEDs.....                                                      | 43 |
| Table 21 – Safety function response time calculation.....                         | 44 |
| Table 22 – Safety function response time definition of terms.....                 | 44 |
| Table 23 – Number of occupied slots and safety data .....                         | 45 |
| Table 24 – Residual error rate $\Lambda$ (occupied slots = 1).....                | 46 |
| Table 25 – Residual error rate $\Lambda$ (occupied slots = 2).....                | 46 |
| Table 26 – Selection of the various measures for possible errors .....            | 49 |
| Table 27 – SS-Start .....                                                         | 54 |
| Table 28 – SS-Restart .....                                                       | 55 |
| Table 29 – SS-InvokeFunc.....                                                     | 55 |
| Table 30 – SS-Read .....                                                          | 55 |
| Table 31 – SS-Write.....                                                          | 56 |
| Table 32 – SS-Terminate .....                                                     | 56 |
| Table 33 – Safety PDU elements.....                                               | 57 |
| Table 34 – CTRL Elements .....                                                    | 58 |
| Table 35 – State list.....                                                        | 63 |
| Table 36 – SFSPM-M timers .....                                                   | 67 |
| Table 37 – SFSPM-M state transition table.....                                    | 67 |
| Table 38 – support_functions .....                                                | 71 |
| Table 39 – error_category.....                                                    | 74 |

|                                                                                              |    |
|----------------------------------------------------------------------------------------------|----|
| Table 40 – error_category for AL errors .....                                                | 74 |
| Table 41 – error_code .....                                                                  | 74 |
| Table 42 – SFSPM-S timers .....                                                              | 76 |
| Table 43 – SFSPM-S state transition table .....                                              | 76 |
| Table 44 – Parameters used by safety communication layer .....                               | 85 |
| Table 45 – SM-SetSafetyStationInfo .....                                                     | 89 |
| Table 46 – Safety station information setting parameters of SM-SetSafetyStationInfo .....    | 90 |
| Table 47 – SM-SetSafetyNetworkParameter .....                                                | 90 |
| Table 48 – Safety network parameters of SM-SetSafetyNetworkParameter .....                   | 90 |
| Table 49 – SM-GetSafetyStationInfo .....                                                     | 91 |
| Table 50 – Safety station information parameters of SM-GetSafetyStationInfo (Request) .....  | 91 |
| Table 51 – Safety station information parameters of SM-GetSafetyStationInfo (Response) ..... | 91 |
| Table 52 – SM-GetSafetyNetworkParameter .....                                                | 92 |
| Table 53 – Parameters of SM-GetSafetyNetworkParameter request .....                          | 92 |
| Table 54 – Parameters of SM-GetSafetyNetworkParameter response .....                         | 92 |
| Table 55 – Monitor LEDs .....                                                                | 93 |
| Table 56 – Communication port monitor LEDs .....                                             | 93 |

IECNORM.COM : Click to view the full PDF of IEC 61784-3-8:2016

## 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.

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

This second edition cancels and replaces the first edition published in 2010. This edition constitutes a technical revision. This edition includes the following significant technical changes with respect to the previous edition:

- Added FSCP 8/2;
- Added FSCP 8/2 Clause 12;
- Added content for FSCP 8/2 to Clauses 1 to 3 (scope, references, terms);
- Moved previous FSCP 8/1 to Clause 11 (demoting all old heading levels by one);
- Restructured old Clauses 4 to 10 to point to appropriate subclauses as appropriate.

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

| FDIS         | Report on voting |
|--------------|------------------|
| 65C/851/FDIS | 65C/854/RVD      |

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

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

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

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

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

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

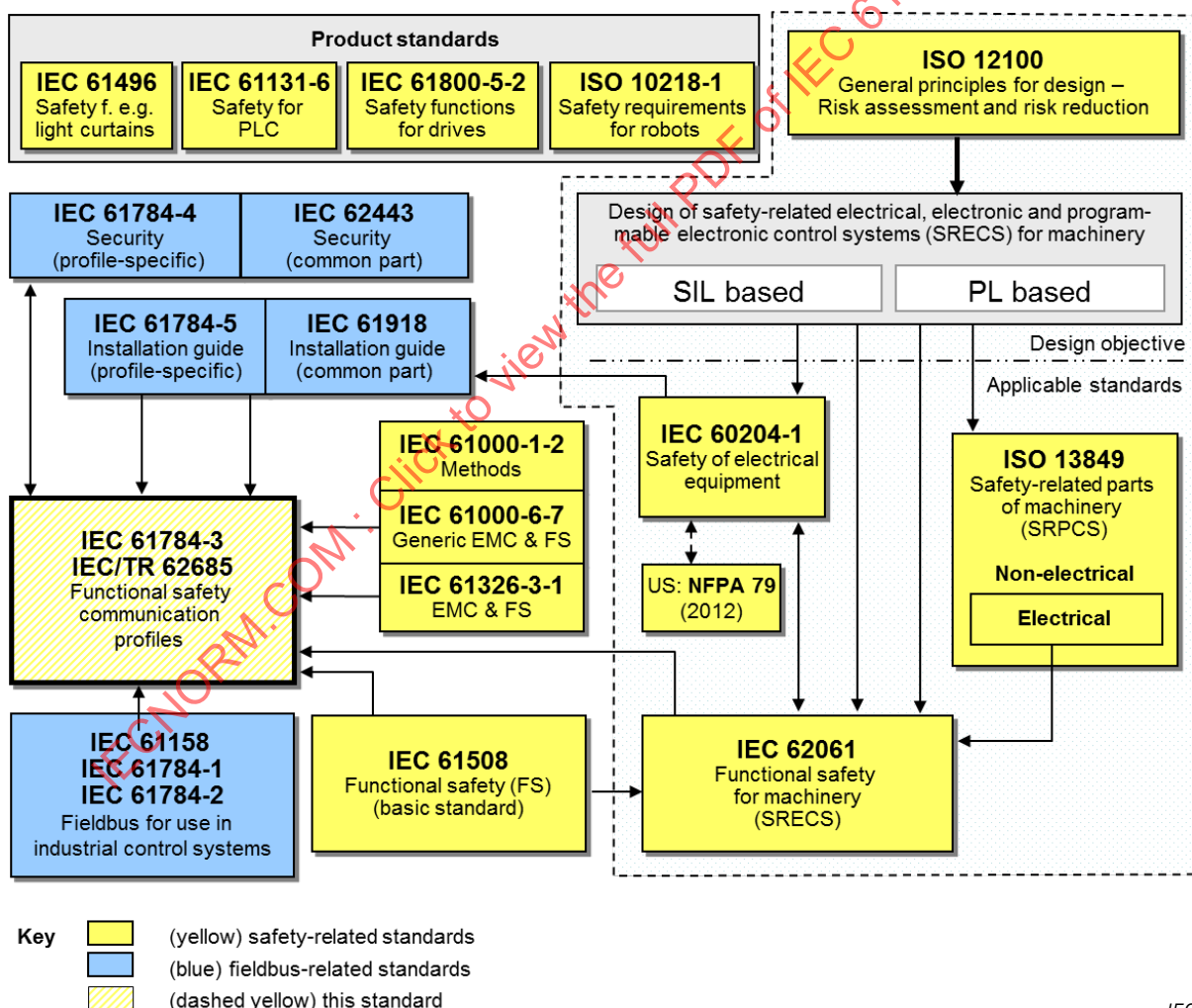
## 0 Introduction

### 0.1 General

The IEC 61158 fieldbus standard together with its companion standards IEC 61784-1 and IEC 61784-2 defines a set of communication protocols that enable distributed control of automation applications. Fieldbus technology is now considered well accepted and well proven. Thus fieldbus enhancements continue to emerge, addressing applications for areas such as real time, safety-related and security-related applications.

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

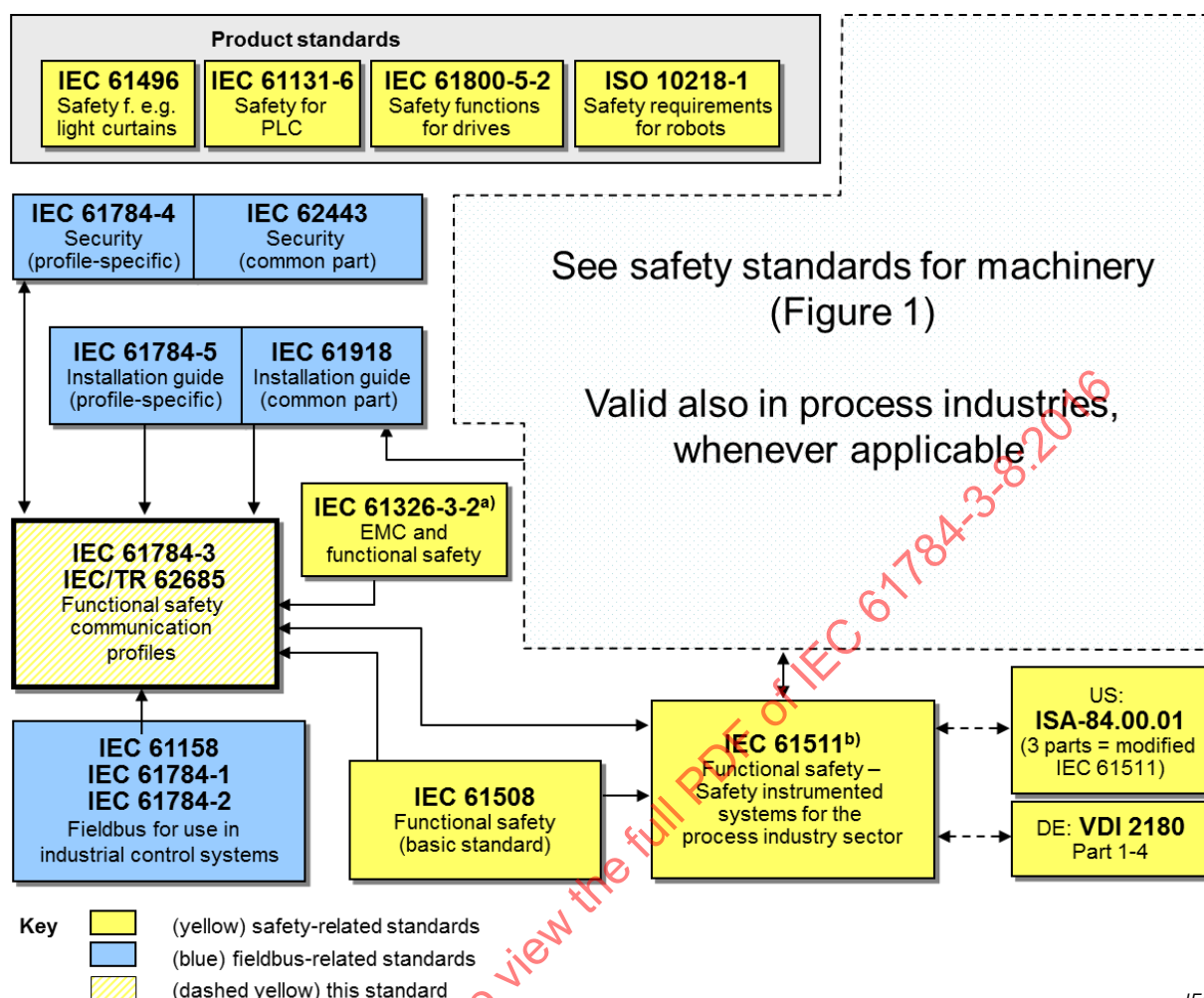
Figure 1 shows the relationships between this standard and relevant safety and fieldbus standards in a machinery environment.



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

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

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



<sup>a</sup> For specified electromagnetic environments; otherwise IEC 61326-3-1 or IEC 61000-6-7.

<sup>b</sup> EN ratified.

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

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

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

The resulting SIL claim of a system depends on the implementation of the selected functional safety communication profile (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.

This standard describes:

- basic principles for implementing the requirements of IEC 61508 series for safety-related data communications, including possible transmission faults, remedial measures and considerations affecting data integrity;

- 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 the IEC 61158 series.

## 0.2 Patent declaration

The International Electrotechnical Commission (IEC) draws attention to the fact that it is claimed that compliance with this document may involve the use of a patent concerning FSCP 8/2 given in Clause 12 as follows:

|                                                                                                |       |                                                    |
|------------------------------------------------------------------------------------------------|-------|----------------------------------------------------|
| JP 2012-533784<br>US 13/821733<br>DE 112010005881.4<br>KR 10-2013-7006469<br>CN 201080069108.6 | [MEC] | Communication apparatus and delay detecting method |
|------------------------------------------------------------------------------------------------|-------|----------------------------------------------------|

IEC takes no position concerning the evidence, validity and scope of this patent right.

The holder of this patent right has assured the IEC that he/she is willing to negotiate licences either free of charge or 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:

|       |                                                                                                                         |
|-------|-------------------------------------------------------------------------------------------------------------------------|
| [MEC] | Mitsubishi Electric Corporation<br>Corporate Licensing Division<br>2-7-3 Marunouchi, Chiyoda-ku<br>Tokyo 100-8310 Japan |
|-------|-------------------------------------------------------------------------------------------------------------------------|

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

ISO ([www.iso.org/patents](http://www.iso.org/patents)) and IEC (<http://patents.iec.ch>) maintain on-line data bases of patents relevant to their standards. Users are encouraged to consult the data bases for the most up-to-date information concerning patents.

## INDUSTRIAL COMMUNICATION NETWORKS – PROFILES –

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

#### 1 Scope

This part of the IEC 61784-3 series 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 part<sup>1</sup> defines mechanisms for the transmission of safety-relevant messages among participants within a distributed network using fieldbus technology in accordance with the requirements of IEC 61508 series<sup>2</sup> for functional safety. These mechanisms may be used in various industrial applications such as process control, manufacturing automation and machinery.

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

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

#### 2 Normative references

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

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

IEC 61131-2:2007, *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*

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

<sup>2</sup> In the following pages of this standard, “IEC 61508” will be used for “IEC 61508 series”.

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

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 8802-3*

IEC 61784-3:—<sup>3</sup>, *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*

IEEE 802.3, *IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method And Physical Layer Specifications*

### **3 Terms, definitions, symbols, abbreviated terms and conventions**

#### **3.1 Terms and definitions**

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

---

<sup>3</sup> To be published.

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:—.

#### 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 devices and fieldbus]

#### 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 61918:2013, 3.1.2]

#### 3.1.1.3

##### **availability**

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

#### 3.1.1.4

##### **bit error probability**

$P_e$

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

#### 3.1.1.5

##### **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.

#### 3.1.1.6

##### **bridge**

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

#### 3.1.1.7

##### **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]

#### 3.1.1.8

##### **communication channel**

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

#### 3.1.1.9

##### **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

**3.1.1.10  
connection**

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

**3.1.1.11  
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 standard to refer to the redundant data.

Note 2 to entry: See also [29], [30]<sup>4</sup>.

**3.1.1.12  
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, using for example zones and conduits

**3.1.1.13  
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]

**3.1.1.14  
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]

---

<sup>4</sup> 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**

denigrated synonym for DLPDU

### 3.1.1.20

#### **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 [29], [30].

### 3.1.1.21

#### **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.

[SOURCE: IEC TR 62210:2003, 4.1.12, modified – addition of “usually” and notes]

### 3.1.1.22

#### **hazard**

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

### 3.1.1.23

#### **master**

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

### 3.1.1.24

#### **message**

ordered series of octets intended to convey information

[SOURCE: ISO/IEC 2382-16:1996, 16.02.01, modified – character replaced by octet]

**3.1.1.25****message sink**

part of a *communication system* in which *messages* are considered to be received

[SOURCE: ISO/IEC 2382-16:1996, 16.02.03]

**3.1.1.26****message source**

part of a *communication system* from which *messages* are considered to originate

[SOURCE: ISO/IEC 2382-16:1996, 16.02.02]

**3.1.1.27****nuisance trip**

*spurious trip* with no harmful effect

Note 1 to entry: Internal abnormal *errors* can be caused in *communication systems* such as wireless transmission, for example by too many retries in the presence of interferences.

**3.1.1.28****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 13849-1:2006, 3.1.23]

**3.1.1.29****protective extra-low-voltage**

PELV

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

Note 1 to entry: A PELV circuit is similar to an SELV circuit that is connected to protective earth.

[SOURCE: IEC 61131-2:2007, 3.54]

**3.1.1.30****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]

**3.1.1.31****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]

**3.1.1.32****reliability**

probability that an automated system can perform a required function under given conditions for a given time interval (t1,t2)

Note 1 to entry: It is generally assumed that the automated system is in a state to perform this required function at the beginning of the time interval.

Note 2 to entry: The term "reliability" is also used to denote the reliability performance quantified by this probability.

Note 3 to entry: Within the MTBF or MTTF period of time, the probability that an automated system will perform a required function under given conditions is decreasing.

Note 4 to entry: Reliability differs from *availability*.

[SOURCE: IEC 62059-11:2002, 3.17, modified – use automated system, two notes added]

### 3.1.1.33

#### **residual error probability**

RP

probability of an *error* undetected by the SCL *safety measures*

### 3.1.1.34

#### **residual error rate**

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

### 3.1.1.35

#### **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], [SOURCE: ISO/IEC Guide 51:2014, definition 3.9, modified – different note]

### 3.1.1.36

#### **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*.

### 3.1.1.37

#### **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

Note 1 to entry: This note applies to the French language only.

### 3.1.1.38

#### **safety connection**

*connection* that utilizes the safety protocol for communications transactions

### 3.1.1.39

#### **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.

### 3.1.1.40

#### **safety device**

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

**3.1.1.41****safety extra-low-voltage****SELV**

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

Note 1 to entry: An SELV circuit is not connected to protective earth.

[SOURCE: IEC 61131-2:2007, 3.59]

**3.1.1.42****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]

**3.1.1.43****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:—, 5.2.4 and addressed by the functional safety communication profiles defined in this part.

**3.1.1.44****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]

**3.1.1.45****safety measure**

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

Note 1 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:—, 5.3 and 5.4.

**3.1.1.46****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*.

#### 3.1.1.47

##### **safety-related application**

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

#### 3.1.1.48

##### **safety-related system**

system performing *safety functions* according to IEC 61508

#### 3.1.1.49

##### **slave**

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

#### 3.1.1.50

##### **spurious trip**

trip caused by the safety system without a process demand

#### 3.1.1.51

##### **time stamp**

time information included in a *message*

#### 3.1.1.52

##### **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.

#### 3.1.1.53

##### **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

Note 1 to entry: This note applies to the French language only.

#### 3.1.2.3

##### **safety application service element**

SASE

safety related application service element

Note 1 to entry: This note applies to the French language only.

**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**

|        |                                               |                    |
|--------|-----------------------------------------------|--------------------|
| 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]      |
| 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                         |                    |
| PELV   | Protective Extra Low Voltage                  |                    |
| PhL    | Physical Layer                                | [ISO/IEC 7498-1]   |

|      |                               |                    |
|------|-------------------------------|--------------------|
| PL   | Performance Level             | [ISO 13849-1]      |
| PLC  | Programmable Logic Controller |                    |
| SCL  | Safety Communication Layer    |                    |
| SELV | Safety Extra Low Voltage      |                    |
| SIL  | Safety Integrity Level        | [IEC 61508-4:2010] |
| SPDU | Safety PDU                    |                    |

### 3.2.2 CPF 8: Additional symbols and abbreviated terms

|       |                                                        |
|-------|--------------------------------------------------------|
| AR    | Application Relationship                               |
| ASE   | Application Service Element                            |
| CID   | Connection Identifier                                  |
| CMD   | Command Data                                           |
| LED   | Light Emitting Diode                                   |
| LID   | Link Identifier                                        |
| OBL   | Offset Base Line                                       |
| PSD   | Protocol Support Data                                  |
| 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 Master)      |
| 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 FSCP 8/1, see 11.4. For FSCP 8/2, see 12.4.

## 5 General

For FSCP 8/1, see 11.5. For FSCP 8/2, see 12.5.

## **6 Safety communication layer services**

For FSCP 8/1, see 11.6. For FSCP 8/2, see 12.6.

## **7 Safety communication layer protocol**

For FSCP 8/1, see 11.7. For FSCP 8/2, see 12.7.

## **8 Safety communication layer management**

For FSCP 8/1, see 11.8. For FSCP 8/2, see 12.8.

## **9 System requirements**

For FSCP 8/1, see 11.9. For FSCP 8/2, see 12.9.

## **10 Assessment**

For FSCP 8/1, see 11.10. For 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™ <sup>5</sup>) 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™ <sup>5</sup>) is based on the CPF 8 basic profiles in IEC 61784-1 and the safety communication layer specifications defined in this part.

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

---

<sup>5</sup> 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 International Standard and does not constitute an endorsement by IEC of the trade name holder or any of its products. Compliance to this standard 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).

accordance with the requirements of IEC 61508 for functional safety. This protocol may be 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 part. However, since they inherit 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 [34], [35] and [36] which provide additional specifications relevant for implementation of the SCL defined in this part.

### **11.5.2 Safety functional requirements**

This standard specifies the services and protocols for a functional safety communication system based on IEC 61158 Type 18. The communication technologies specified in this standard 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 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 part, 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 standard provides the following deterministic remedial measures to implement its safety communication layer:

- sequence number;
- time expectation;
- connection authentication;
- feedback message;
- data integrity assurance (CRC 32);

- 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                        |                                |                                            |
| Unintended repetition                  | X                               |            |                  |                           |                  |                          |                                |                                            |
| Incorrect sequence                     | X                               |            |                  |                           |                  |                          |                                |                                            |
| Loss                                   | X                               |            |                  |                           |                  |                          |                                |                                            |
| Unacceptable delay                     |                                 |            | X                |                           |                  |                          |                                |                                            |
| Insertion                              | X                               |            |                  | X                         | X                |                          |                                |                                            |
| Masquerade                             |                                 |            |                  | 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 4 bits and a specified sequence (see 11.7.1 and 11.7.2). 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, command ID and protocol support data field.

### 11.5.3.6 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 a 16-bit protocol support data field, an 8-bit command ID, a 3-bit link ID and a 4-bit RNO.

### 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 manger;
- 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 manger;
- M1 and S1 type safety cyclic transmission.

All management, behaviors and functions of the SCL is 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.

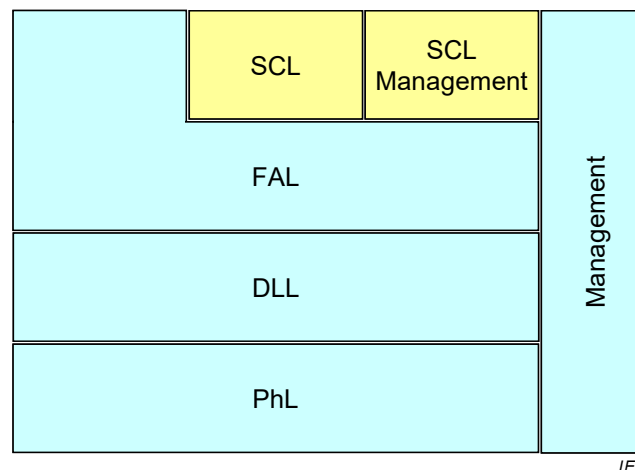


Figure 3 – Relationship between SCL and the other layers of IEC 61158 Type 18

### 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 are 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       |

|         |     |            |                   |
|---------|-----|------------|-------------------|
| 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.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 manger.

|               |                               |            |                 |
|---------------|-------------------------------|------------|-----------------|
| 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    |
| 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    |

### 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:               | $96 \times n$         |
| Safety RY data   | Bit-oriented data structure            | $32 \times n$         |
| RWw data         | Word-oriented data structure           | $64 \times n$         |
| Safety RWw data  | Word-oriented data                     | $64 \times (n - m)$   |
| Safety TPI-T     | Safety transmission packet information | $64 \times m$         |
| Data in          | Structure of n elements                | $96 \times n$         |
| Safety data in 1 | Structure of 2 elements                | $96 \times p_1$       |
| Safety RX data   | Bit-oriented data structure            | $32 \times p_1$       |
| RWr data         | Word-oriented data structure           | $64 \times p_1$       |
| Safety RWr data  | Word-oriented data                     | $64 \times (p_1 - 1)$ |
| Safety TPI-R     | Safety transmission packet information | 64                    |
| ...              | ...                                    | ...                   |
| Safety data in n | Structure of 2 elements                | $96 \times p_n$       |

NOTE The values of n and m are dependent upon the values of the corresponding configuration settings in the master status. The value of p depends on the number of slots occupied by the slave station.

#### 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:               | $96 \times p$       |
| Safety RY data  | Bit-oriented data structure            | $32 \times p$       |
| RWw data        | Word-oriented data structure           | $64 \times p$       |
| Safety RWw data | Word-oriented data                     | $64 \times (p - 1)$ |
| Safety TPI-T    | Safety transmission packet information | 64                  |
| Data in         | Structure of 2 elements:               | $96 \times p$       |
| Safety RX data  | Bit-oriented data structure            | $32 \times p$       |
| RWr data        | Word-oriented data structure           | $64 \times p$       |
| Safety RWr data | Word-oriented data                     | $64 \times (p - 1)$ |
| Safety TPI-R    | Safety transmission packet information | 64                  |

NOTE The value of p depends on the number of slots occupied by the slave station.

#### 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<br>1 = Version 2<br>2 = Version 3<br>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<br>1 = Version 2<br>2 = Version 3<br>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<br>1 = Version 2<br>2 = Version 3<br>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:<br>0 = SCL not supported<br>1 = SCL supported                                       |
| Safety slave specification source | Bit 0 – 63 correspond to slot 1 – 64, where:<br>0 = SCL-user specification not supported<br>1 = SCL-user specification supported |

| Attribute                               | Encoding                                                                                                                 |
|-----------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| 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:<br>0 = Safety slave station not running<br>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 per slot                                                                                                                                 |
| 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 |

| Attribute       | Encoding                                                                                                                                                                                                                                     |        |                                                             |                                  |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|-------------------------------------------------------------|----------------------------------|
|                 | Octet                                                                                                                                                                                                                                        | Bit    | Description                                                 | Values                           |
| Safety TPI-T    | 0 – 1                                                                                                                                                                                                                                        | –      | Protocol support data (PSD) which is used by SCL management | 0 – 65 535                       |
|                 | 2 – 3                                                                                                                                                                                                                                        | 0 – 3  | Running number                                              | 0 – 15                           |
|                 |                                                                                                                                                                                                                                              | 4 – 6  | Link id                                                     | 0 – 7                            |
|                 |                                                                                                                                                                                                                                              | 7      | reserved                                                    | 0                                |
|                 |                                                                                                                                                                                                                                              | 8 – 11 | Transmission data type                                      | 0 – 15                           |
|                 |                                                                                                                                                                                                                                              | 12     | Busy flag                                                   | 0 = busy<br>1 = not busy         |
|                 |                                                                                                                                                                                                                                              | 13     | reserved                                                    | 0                                |
|                 |                                                                                                                                                                                                                                              | 14     | Read request                                                | 0 = no request<br>1 = request    |
|                 |                                                                                                                                                                                                                                              | 15     | SCL user application mode                                   | 0 = test mode<br>1 = safety mode |
|                 | 4 – 7                                                                                                                                                                                                                                        | –      | CRC32                                                       | CRC32                            |
| 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 per slot. The number of slots occupied by the slave device determines the total length of this field                                         |        |                                                             |                                  |
| RWr data        | A field containing the word-oriented input data from slave device n ordered by slot with 4 words per slot. The number of slots occupied by the slave device determines the total length of this field                                        |        |                                                             |                                  |
| Safety RWr data | 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 |        |                                                             |                                  |

| Attribute    | Encoding |                                                             |                                  |
|--------------|----------|-------------------------------------------------------------|----------------------------------|
|              | Bit      | Description                                                 | Values                           |
| Safety TPI-R | 0 – 15   | Protocol support data (PSD) which is used by SCL management | 0 – 65 535                       |
|              | 16 – 19  | Running number                                              | 0 – 15                           |
|              | 20 – 22  | Link id                                                     | 0 – 7                            |
|              | 23       | reserved                                                    | 0                                |
|              | 24 – 27  | Transmission data type                                      | 0 – 15                           |
|              | 28       | Busy flag                                                   | 0 = busy<br>1 = not busy         |
|              | 29       | Error notification                                          | 0 = no error<br>1 = error        |
|              | 30       | reserved                                                    | 0                                |
|              | 31       | SCL-user application mode                                   | 0 = test mode<br>1 = safety mode |
|              | 32 – 63  | CRC32                                                       | CRC32                            |

#### 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 per slot. The number of slots occupied by the slave device determines the total length of this field                                                               |
| 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 |

| Attribute       | Encoding                                                                                                                                                                                                                                      |                                                             |                                  |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------|----------------------------------|
| Safety TPI-T    | <b>Bit</b>                                                                                                                                                                                                                                    | <b>Description</b>                                          | <b>Values</b>                    |
|                 | 0 – 15                                                                                                                                                                                                                                        | Protocol support data (PSD) which is used by SCL management | 0 – 65 535                       |
|                 | 16 – 19                                                                                                                                                                                                                                       | Running number                                              | 0 – 15                           |
|                 | 20 – 22                                                                                                                                                                                                                                       | Link id                                                     | 0 – 7                            |
|                 | 23                                                                                                                                                                                                                                            | reserved                                                    | 0                                |
|                 | 24 – 27                                                                                                                                                                                                                                       | Transmission data type                                      | 0 – 15                           |
|                 | 28                                                                                                                                                                                                                                            | Busy flag                                                   | 0 = busy<br>1 = not busy         |
|                 | 29                                                                                                                                                                                                                                            | reserved                                                    | 0                                |
|                 | 30                                                                                                                                                                                                                                            | Read request                                                | 0 = no request<br>1 = request    |
|                 | 31                                                                                                                                                                                                                                            | SCL-user application mode                                   | 0 = test mode<br>1 = safety mode |
| 32 – 63         | CRC32                                                                                                                                                                                                                                         | CRC32                                                       | CRC32                            |
| 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 per slot. The number of slots occupied by the slave device determines the total length of this field                                                              |                                                             |                                  |
| RWr data        | A field containing the word-oriented input data from the master. The number of slots occupied by the slave device determines the total length of this field                                                                                   |                                                             |                                  |
| 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 |                                                             |                                  |
| Safety TPI-R    | <b>Bit</b>                                                                                                                                                                                                                                    | <b>Description</b>                                          | <b>Values</b>                    |
|                 | 0 – 15                                                                                                                                                                                                                                        | Protocol support data (PSD) which is used by SCL management | 0 – 65 535                       |
|                 | 16 – 19                                                                                                                                                                                                                                       | Running number                                              | 0 – 15                           |
|                 | 20 – 22                                                                                                                                                                                                                                       | Link id                                                     | 0 – 7                            |
|                 | 23                                                                                                                                                                                                                                            | reserved                                                    | 0                                |
|                 | 24 – 27                                                                                                                                                                                                                                       | Transmission data type                                      | 0 – 15                           |
|                 | 28                                                                                                                                                                                                                                            | Busy flag                                                   | 0 = busy<br>1 = not busy         |
|                 | 29                                                                                                                                                                                                                                            | Error notification                                          | 0 = no error<br>1 = error        |
|                 | 30                                                                                                                                                                                                                                            | reserved                                                    | 0                                |
|                 | 31                                                                                                                                                                                                                                            | SCL-user application mode                                   | 0 = test mode<br>1 = safety mode |
| 32 – 63         | CRC32                                                                                                                                                                                                                                         | CRC32                                                       | CRC32                            |

## 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, as shown in Figure 4. 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.

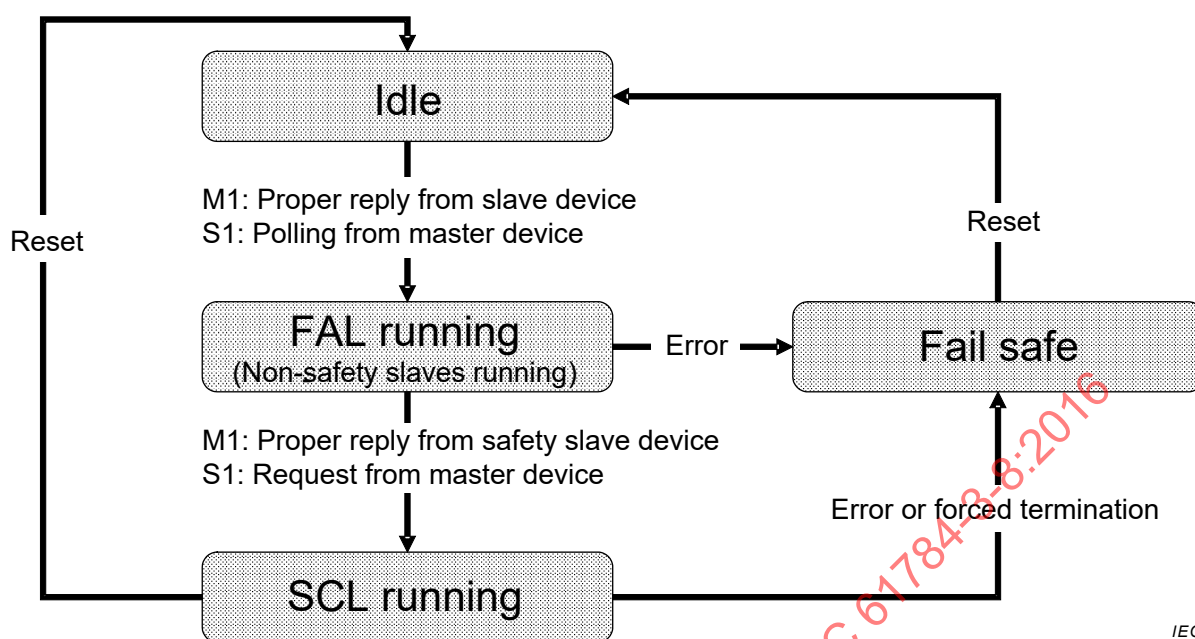


Figure 4 – State diagram

IEC

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

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 any of the following error types:

- sequence number;
- time expectation;
- connection authentication;
- feedback message;
- data integrity assurance;
- 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;
- 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 4 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 value to a value 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 and Table 15 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<br>(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<br>(2) At detection of an RNO error<br>(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<br>(2) At detection of an RNO error<br>(3) At reception of a forced termination request |
| <p>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.</p> |                                                                                                                                             |                                                                                                                                   |

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**

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.

Additionally, the transmitted 16-bit logical connection ID is appended to the SPDU for validation. This field, which is comprised of A1 (8-bit source ID) and A2 (8-bit destination ID), is checked for correctness and also included in the data integrity measures, as shown in 11.9.5.2.

#### **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, command ID and protocol support data field.

#### **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 discussed in 11.9.5.2.

#### **11.7.2.6.7 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), a 16-bit protocol support data field, an 8-bit command ID, a 3-bit link ID and a 4-bit RNO.

The IEC 61158 Type 18 protocol uses a different CRC algorithm (16-bit CRC) and no inclusion of protocol support data field, 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.<br>(This is confirmed by communicating the safety cyclic data.)<br>(2) Confirm that the safety slave has received the establish connection command.<br>(This is confirmed by checking that the CMD and PSD of the response data are identical with the send data.)<br>(3) Transmit the safety monitor timer value. |
| Safety slave  | (1) Confirm that the master is a safety master device.<br>(This is confirmed by communicating the safety cyclic data.)<br>(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 actually 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.<br>(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.<br>(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<br>Out: Watchdog timer error                                                                                                                                                                                                                                                                                                           | M                     | O                            | O                         |
| 2   | ERR      | Lit: Communication with all stations error<br>This LED lights when one of the following occurs:<br>· Switch setting error<br>· Master station duplicated on same line<br>· Parameter content error<br>· Data link monitor timer activated<br>· Cable wire break<br>Or cable influenced by noise on the transmission path<br>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)<br>Flashing: Switch type setting was changed with power ON                                                                                                                                                                                                                                                        | M                     | O                            | O                         |

### 11.9.2 Installation guidelines

This standard specifies protocol and services for a safety communication system based on IEC 61158 Type 18. However, usage of safety devices with the safety protocol specified in this standard requires proper installation. All devices connected to a safety communication system defined in this part shall fulfill SELV/PELV requirements, which are specified in the relevant IEC standards such as IEC 60204-1.

Additional installation information is also given in [34] and [35] 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, which is the time between the detection of an event at the safety input slave and the response at the corresponding output channel(s) on the safety output slave(s).

The 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 each safety slave (input and output), and the processing time within the 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.

#### 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 –  $((WDT \times n) \times 2)$ .

NOTE 2  $(WDT \times n) \times 2$  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:<br>Safety refresh monitor time × 2 – $((WDT \times n) \times m) - 10$ [ms]                                                                                                                                                                                                                                                                          |
| Safety refresh monitor time  | Time set in network parameter. Use the value gained by the following calculation formula as the measure.<br><br>In triggered mode:<br>$(WDT \times n) \times 3 + (WDT \times n) \times m \times 2 + (WDT \times \alpha)$ [ms]<br><br>In free-running mode:<br>$(WDT \times n) \times 3 + LS + (WDT \times n) \times m \times 2 + (WDT \times \alpha)$ [ms]<br><br>where:<br>$\alpha = 0$ , for $LS \leq 1,5$ ms<br>$\alpha = 1$ , for $LS > 1,5$ ms |
| WDT (Watchdog timer)         | Time set in configuration parameter.                                                                                                                                                                                                                                                                                                                                                                                                                |

| Item              | Definition                                                                                                                                                      |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Triggered mode    | Mode which performs data link when sequence scan is synchronized with link scan.<br><br>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

##### 11.9.5.1 System characteristics

The following basic data have to be adhered:

- 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

##### 11.9.5.2 Residual error rate ( $\Lambda$ )

The residual error rate,  $\Lambda$ , for the safety system is directly impacted by the number of safety slave devices and their corresponding number of occupied slots in the system configuration. Table 23 shows the impact of the number of occupied slots of the safety slave on the resulting frame length for its relevant safety PDU.

**Table 23 – Number of occupied slots and safety data**

| Occupied slots | Structure of safety PDU                            |           | Frame length (bits) |
|----------------|----------------------------------------------------|-----------|---------------------|
|                | SAR                                                | Structure |                     |
| 1              | Safety master station<br>→<br>Safety slave station |           | 112                 |
|                | Safety slave station<br>→<br>Safety master station |           | 112                 |

| Occupied slots | Structure of safety PDU                            |           | Frame length (bits) |
|----------------|----------------------------------------------------|-----------|---------------------|
|                | SAR                                                | Structure |                     |
| 2              | Safety master station<br>→<br>Safety slave station |           | 208                 |
|                | Safety slave station<br>→<br>Safety master station |           | 208                 |

Based on the frame length and the number of safety slaves in the safety system,  $\Lambda$  is found in Table 24 and Table 25.

**Table 24 – Residual error rate  $\Lambda$  (occupied slots = 1)**

| Residual error rate probability, $R_{pCRC32}$ | Number of safety slaves | Minimum cycle time ms | Residual error rate, $\Lambda$ |
|-----------------------------------------------|-------------------------|-----------------------|--------------------------------|
| $1,01 \times 10^{-24}$                        | 1                       | 10,0                  | $7,27 \times 10^{-17}$         |
|                                               | 8                       | 10,0                  | $5,81 \times 10^{-16}$         |
|                                               | 16                      | 10,0                  | $1,16 \times 10^{-15}$         |
|                                               | 32                      | 10,0                  | $2,33 \times 10^{-15}$         |
|                                               | 42                      | 10,0                  | $3,05 \times 10^{-15}$         |

**Table 25 – Residual error rate  $\Lambda$  (occupied slots = 2)**

| Residual error rate probability, $R_{pCRC32}$ | Number of safety slaves | Minimum cycle time ms | Residual error rate, $\Lambda$ |
|-----------------------------------------------|-------------------------|-----------------------|--------------------------------|
| $2,05 \times 10^{-19}$                        | 1                       | 10,0                  | $1,47 \times 10^{-11}$         |
|                                               | 8                       | 10,0                  | $1,18 \times 10^{-10}$         |
|                                               | 16                      | 10,0                  | $2,36 \times 10^{-10}$         |
|                                               | 32                      | 10,0                  | $4,72 \times 10^{-10}$         |

The resulting residual error rate for all specified configurations of FSCP 8/1 is maintained below the  $10^{-7}$  ( $10^{-9}$  attributable to the network) required in order to satisfy SIL3 and Category 4.

#### 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 standard. 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. Besides, it is recommended to take into account the documents [34] and [35] from the Bibliography. 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 standard 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 [34], [35] and [36] of the Bibliography.

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).

### **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™<sup>6</sup>) defines communication profiles based on IEEE 802.3, 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<sup>5</sup>) is

<sup>6</sup> CC-Link IE™ are trade names of the non-profit organization CC-Link Partner Association. This information is given for the convenience of users of this International Standard and does not constitute an endorsement by IEC of the trade name holder or any of its products. Compliance to this standard does not require use of the trade names CC-Link IE™. Use of the trade names CC-Link IE™ requires permission of CC-Link Partner Association and compliance with conditions for their use (such as testing and validation).

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 part.

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 may be 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 sequence number, 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 part. However, since they inherit 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 part.

NOTE Documents [34] and [35] contain important information related to FSCP 8/2.

### **12.5.2 Safety functional requirements**

This standard specifies the services and protocols for a functional safety communication system based on IEC 61158 Type 23. The communication technologies specified in this standard 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 part, 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 standard provides the following deterministic remedial measures to implement its safety communication layer:

- time stamp;
- time expectation;
- connection authentication;
- feedback message;
- data integrity assurance;
- different data integrity assurance systems.

The selection of the various measures for possible errors is shown in Table 26.

**Table 26 – Selection of the various measures for possible errors**

| Communication errors                                                                                                                              | Deterministic Remedial Measures |                   |                  |                           |                  |                          |                                |                                            |
|---------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------|-------------------|------------------|---------------------------|------------------|--------------------------|--------------------------------|--------------------------------------------|
|                                                                                                                                                   | Sequence Number                 | Time Stamp        | Time Expectation | Connection Authentication | Feedback Message | Data Integrity Assurance | Redundancy With Cross Checking | Different Data Integrity Assurance Systems |
| Corruption                                                                                                                                        |                                 |                   |                  |                           |                  | X                        |                                |                                            |
| Unintended repetition                                                                                                                             |                                 | X                 |                  |                           |                  |                          |                                |                                            |
| Incorrect sequence                                                                                                                                |                                 | X                 |                  |                           |                  |                          |                                |                                            |
| Loss                                                                                                                                              |                                 | X <sup>a, c</sup> |                  |                           | X <sup>b</sup>   |                          |                                |                                            |
| Unacceptable delay                                                                                                                                |                                 | X <sup>c</sup>    | X                |                           |                  |                          |                                |                                            |
| Insertion                                                                                                                                         |                                 |                   |                  | X                         |                  |                          |                                |                                            |
| Masquerade                                                                                                                                        |                                 |                   |                  |                           |                  |                          |                                | X                                          |
| Addressing                                                                                                                                        |                                 |                   |                  | X                         |                  |                          |                                |                                            |
| <sup>a</sup> Assessed by received time stamp.<br><sup>b</sup> Used in request/response model.<br><sup>c</sup> Not used in request/response model. |                                 |                   |                  |                           |                  |                          |                                |                                            |

#### 12.5.3.2 Corruption

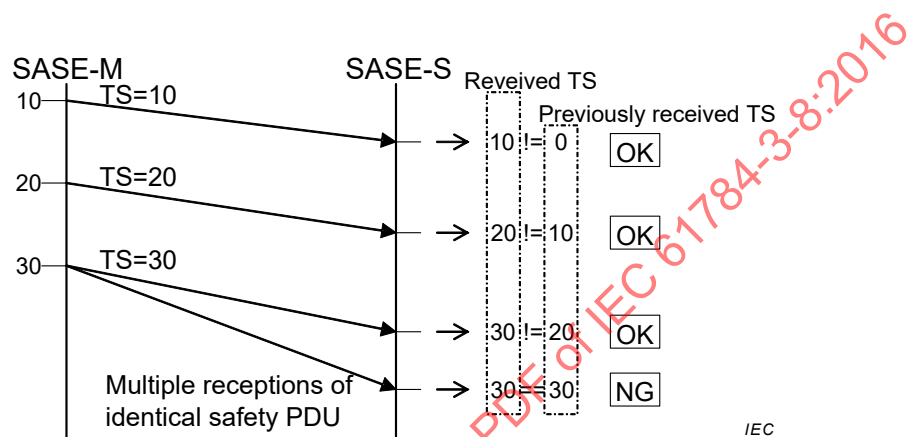
Corruption is detected using the CRC included in the safety PDU. The transmitting node sends the safety PDU including its calculated CRC. The receiving node compares the CRC included in the received safety PDU with the CRC calculated from the received safety PDU, and determines if corruption occurred. If the comparison 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 time stamp included in the safety PDU. The transmitting node sends safety PDUs that includes a timestamp (TS).

The receiving node receives the safety PDU and holds the TS 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 TS included in the safety PDU with the held TS of the safety PDU previously received. If the TS of the received safety PDU is the same as the TS of the previously received TS, the receiving node deems that unintended repetition has occurred, and shall discard the received safety PDU. When a safety PDU having the same TS 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. The order is detected using the time stamps included in the safety PDUs. The transmitting node sends safety PDUs that include a TS.

The receiving node receives a safety PDU and holds the TS of the received safety PDU. Upon receipt of the next safety PDU, the receiving node compares the TS included in the safety PDU with the held TS of the safety PDU previously received. If the TS of the received PDU is less than the TS of the previously received TS, 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.

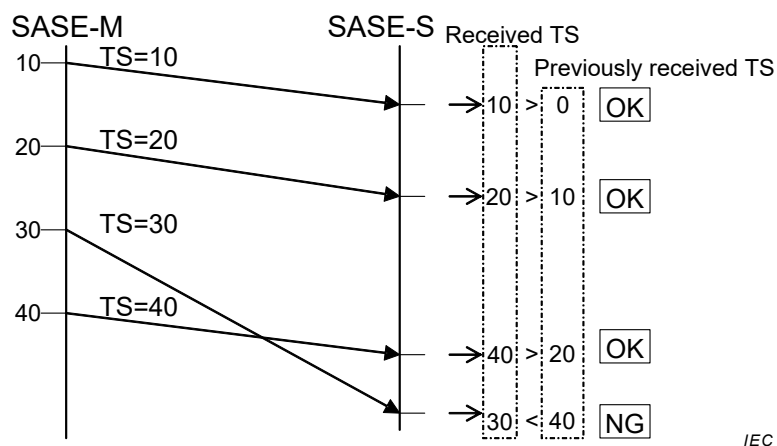


Figure 6 – Detection of incorrect sequence

### 12.5.3.5 Loss

Loss is detected using time stamps.

SASE-M periodically sends safety PDUs to SASE-S based on the SASE-M transmission interval (transmission\_interval). The TS 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 TS 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 TS of the received safety PDU is not larger than the sum of the transmission interval of the transmitting node added to the TS 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.

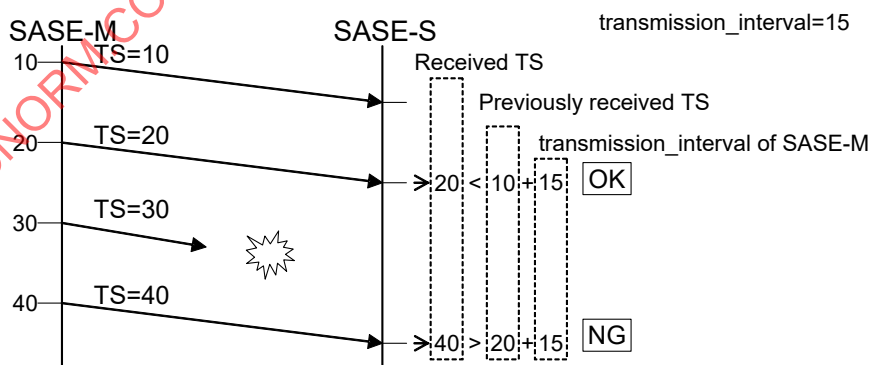


Figure 7 – Detection of loss

### 12.5.3.6 Unacceptable delay

An unacceptable delay is detected using timers and time stamps.

SASE-M periodically sends safety PDUs to SASE-S based on the SASE-M transmission interval (transmission\_interval). The TS 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

PDU to SASE-M based on the SASE-S transmission interval (transmission\_interval). The TS 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.

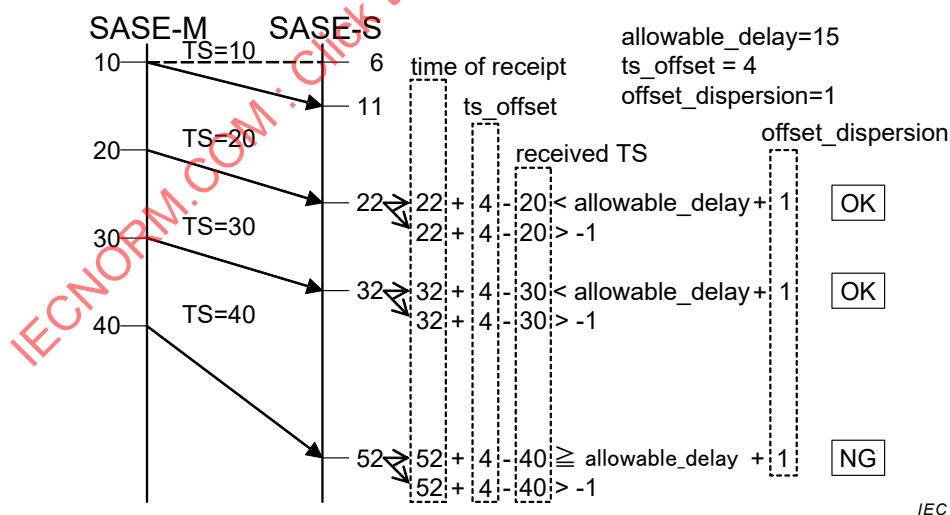
SASE-S on the receiving node receives a safety PDU from SASE-M, records the safety clock value at the time of safety PDU reception, and starts or resets the timer delay\_detection\_timer. SASE-S calculates the difference between the sum of the recorded safety clock value and the offset ts\_offset and the received TS, 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\_dispersions), the receiving node deems that an unacceptable delay has occurred.

$$\text{offset\_dispersion} < \text{Calculated value} < \text{allowable\_delay} + \text{offset\_dispersion}$$

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 TS, 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.



IEC

Figure 8 – Detection of unacceptable delay by time stamps

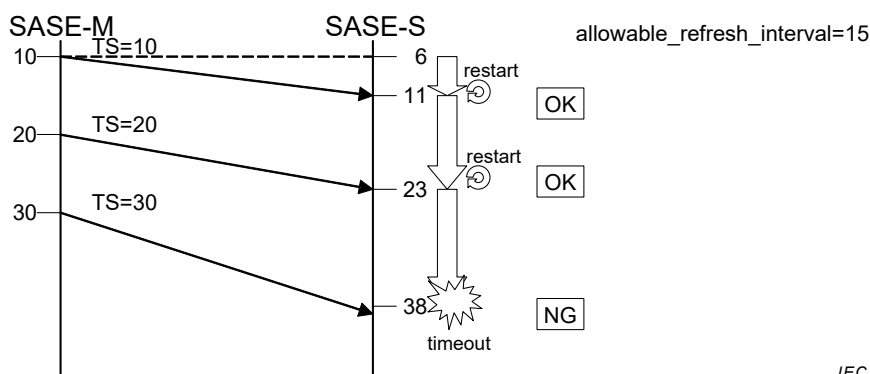


Figure 9 – Detection of unacceptable delay by timer

#### 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 an unsafe 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 CRC generated by a generator polynomial that differs from that for non-safety communication.

The transmitting node sends a safety PDU that includes its calculated CRC. The receiving node compares the CRC included in the safety PDU with the CRC calculated from the received safety PDU. 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.

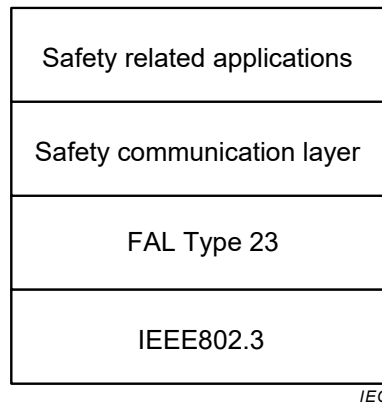
#### 12.5.3.9 Addressing

Addressing 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 (IEEE 802.3 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 27 shows the SS-Start parameters.

**Table 27 – 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 28 shows the SS-Restart parameters.

**Table 28 – 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 29 shows the SS-InvokeFunc parameters.

**Table 29 – 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 30 shows the parameters of this service.

**Table 30 – 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 31 shows the parameters of this service.

**Table 31 – 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 32 shows the parameters of this service.

**Table 32 – 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 size of S-Data is 128 bits, maximum.

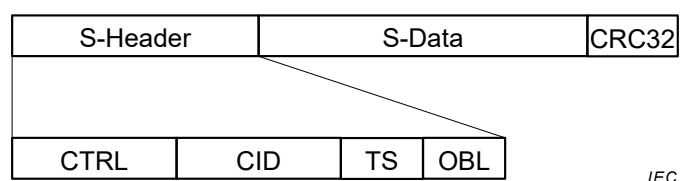
**Figure 11 – Safety PDU Structure**

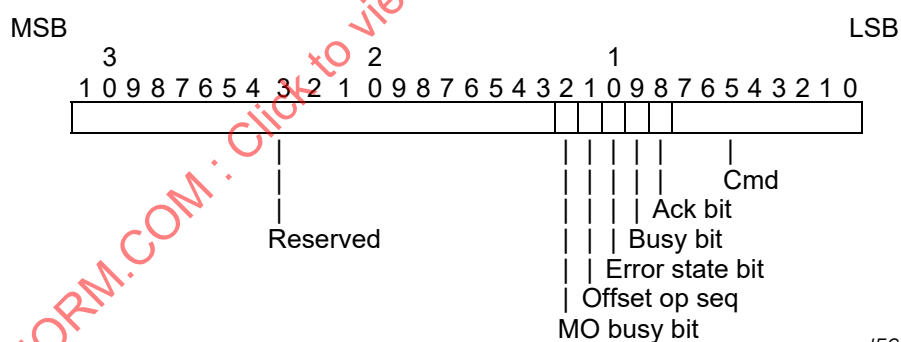
Table 33 shows the names, sizes, and contents of the elements that make up the safety PDU.

**Table 33 – Safety PDU elements**

| Attribute | Description                   | Size (bits) |
|-----------|-------------------------------|-------------|
| S-Header  | Structure of 4 elements:      | 96          |
| CTRL      | Command type, status          | 32          |
| CID       | Safety connection identifier  | 32          |
| TS        | Time stamp                    | 16          |
| OBL       | Offset generation information | 16          |
| S-Data    | Safety data                   | 128 max     |
| CRC32     | Cyclic Redundancy Check       | 32          |

### 12.7.1.2 CTRL

Figure 12 shows the configuration of CTRL. Table 34 describes the contents of the elements that make up CTRL.

**Figure 12 – CTRL Configuration**

**Table 34 – 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 – 0xF0 | For future expansion                                       |
|                 | 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                                    |
| Reserved        |                     | —           | For future expansion                                       |

**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.

#### 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

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.

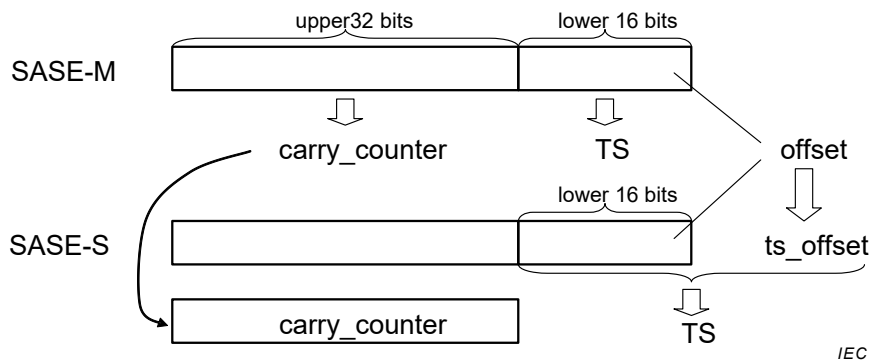
When SASE-M executes a Cmd request, the value of the lower 16 bits of the safety clock during the Cmd request shall be stored in TS.

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

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

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.

The upper 32 bits of the 48-bit safety clock are called the `carry_counter`, and are derived from the upper 32 bits of the SASE-M safety clock. SASE-M notifies SASE-S of the initial value of `carry_counter` when connection is established.

SASE-S then uses the value identified by SASE-M as the `carry_counter`. The `carry_counter` is used as the initial value of CRC generation that is stored in the safety PDU.

The accuracy of the safety clock implemented shall satisfy  $\pm 100$  ppm.

#### 12.7.1.5 OBL

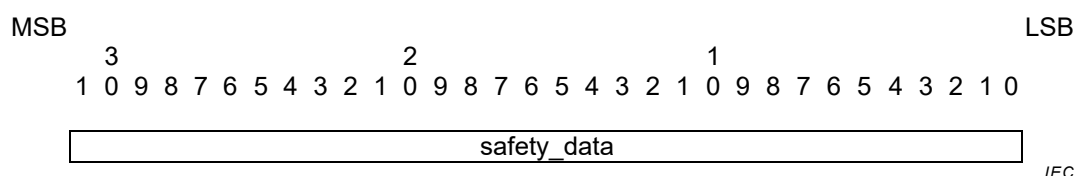
OBL is information used to generate the offset `ts_offset` of the safety clock. OBL is used in the request S-RefreshGO-req sent by SASE-M and in the response S-RefreshGO-rsp sent by SASE-S.

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.



**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.

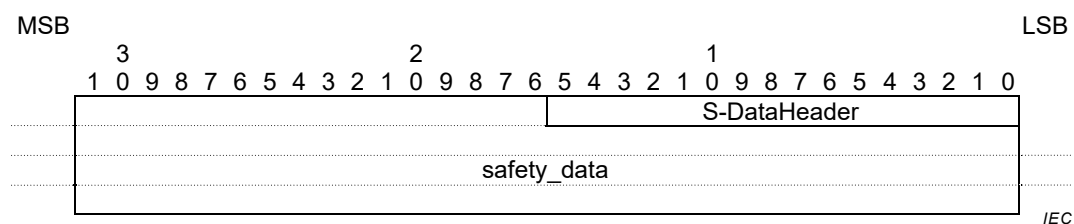


Figure 15 – S-Data not during safety refresh

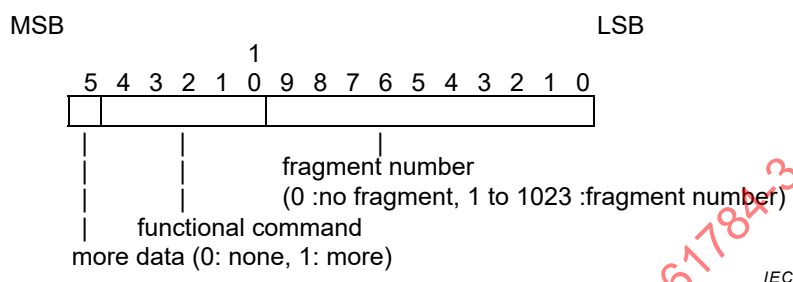


Figure 16 – S-Data header configuration

**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 [36]. 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  $99 \leq n \leq 1\,024$ , the minimum hamming distance of this CRC generator polynomial is 8.

CRC32 shall be calculated using CTRL, CID, TS, OBL, S-Data, and carry\_counter included in the safety PDU as shown in Figure 17.

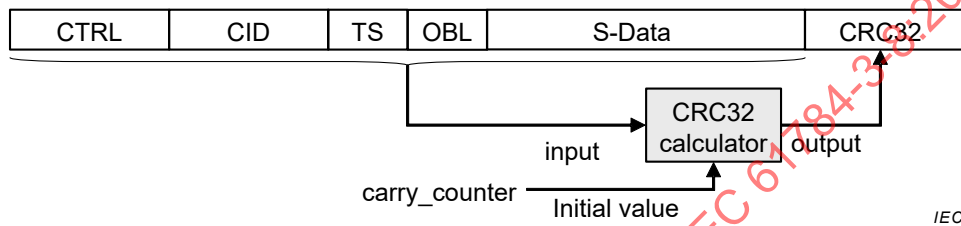


Figure 17 – CRC calculation

### 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.

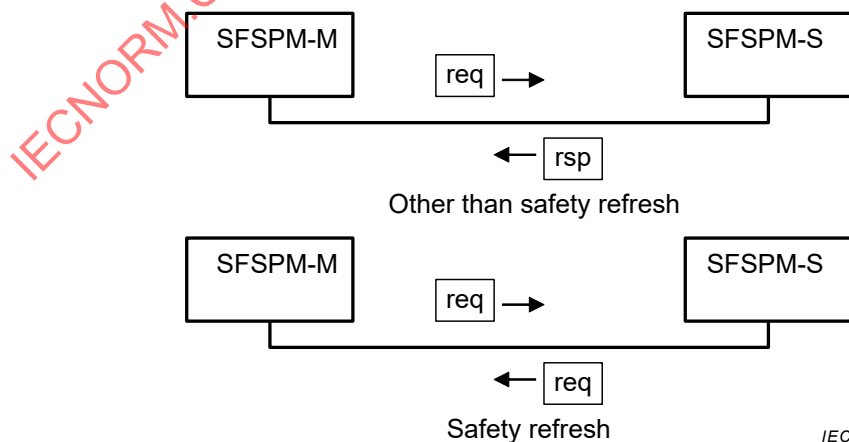
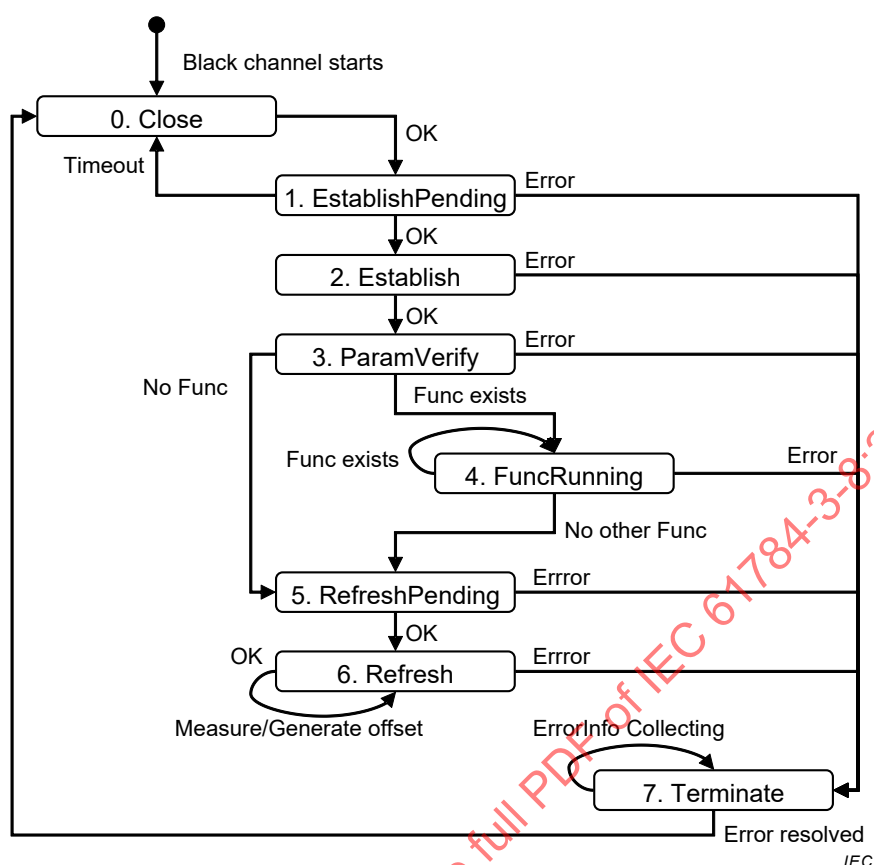


Figure 18 – Communication models

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



**Figure 19 – SFSPM state transition diagram**

Table 35 describes the states shown in Figure 19.

**Table 35 – State list**

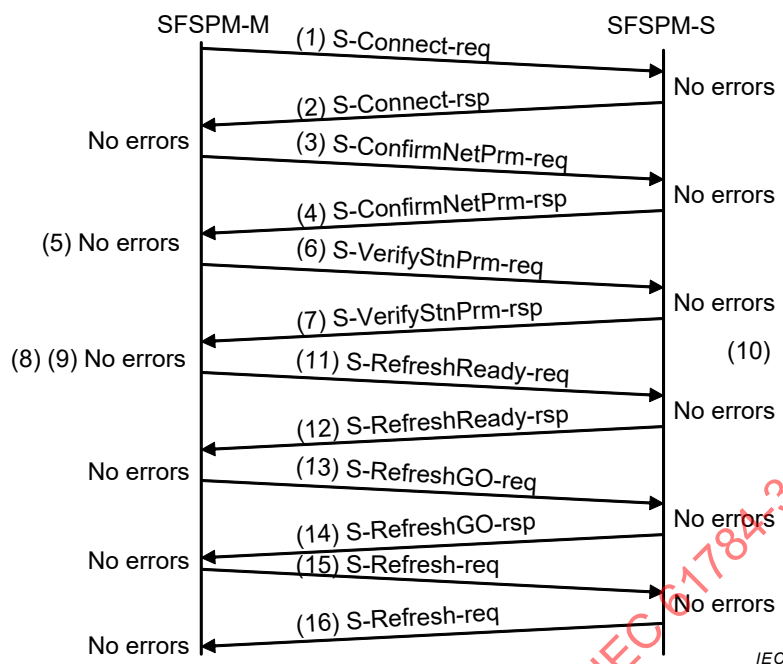
| No. | State Name       | State                                   | Description                                                                                                                                                                                                 |
|-----|------------------|-----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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.<br><br>For executable support function, see Table 38, 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 following the procedure below:

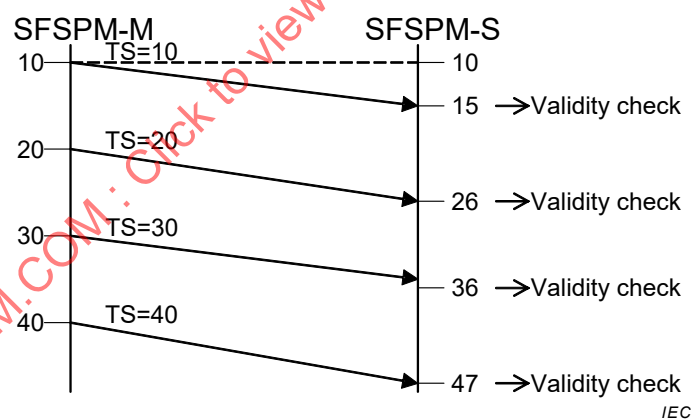
- 1) SFSPM-M starts. SFSPM-M sends a safety connection establishment request to SFSPM-S based on parameters provided in advance.
- 2) SFSPM-S receives the safety connection establishment request from SFSPM-M and sends a safety connection establishment response to SFSPM-M.
- 3) SFSPM-M receives the safety connection establishment response from SFSPM-S and, based on support function information agreed upon at the time of safety connection establishment, sends a request related to support functions to SFSPM-S. SFSPM-M sends a safety network parameter confirmation request related to support functions to SFSPM-S.
- 4) SFSPM-S receives the safety network parameter confirmation request from SFSPM-M, stores the received parameters, and sends a safety network parameter confirmation response to SFSPM-M.
- 5) SFSPM-M receives the safety network parameter confirmation response from SFSPM-S and stores the received parameters.
- 6) If safety network parameter confirmation ends successfully, SFSPM-M sends a safety station parameter verification request to SFSPM-S.
- 7) SFSPM-S receives the safety station parameter verification request from SFSPM-M and sends the safety station parameter verification response, including parameters provided in advance, to SFSPM-M.
- 8) SFSPM-M receives the safety station parameter verification response from SFSPM-S and checks if the safety station parameters are correct.
- 9) SFSPM-M verifies that the safety station parameters are correct, and repeatedly sends requests and receives responses until all requests related to support functions have been performed.
- 10) SFSPM-S repeatedly receives requests and sends responses during the period the requests related to support functions continue.
- 11) Once all requests related to support functions have been performed, SFSPM-M sends a refresh preparation + offset measurement request to SFSPM-S.
- 12) SFSPM-S receives the refresh preparation + offset measurement request from SFSPM-M and sends a refresh preparation + offset measurement response to SFSPM-M.
- 13) SFSPM-M receives the refresh preparation + offset measurement response, generates the information required for offset calculation, and sends a safety refresh + offset generation request, including the generated information, to SFSPM-S.
- 14) SFSPM-S receives the safety refresh + offset generation request from SFSPM-M, generates an offset from the notified information, and sends a safety refresh + offset generation response to SFSPM-M.
- 15) SFSPM-M starts safety refresh by sending a safety refresh + offset generation request and, after the transmission interval has passed, sends a safety refresh request.
- 16) SFSPM-S starts safety refresh by sending a safety refresh + offset generation response and, after the transmission interval has passed, sends a safety refresh request.



**Figure 20 – Connection establishment sequence**

#### 12.7.2.2.2 Safety refresh

Figure 21 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 21 – Communication sequence during safety refresh communication**

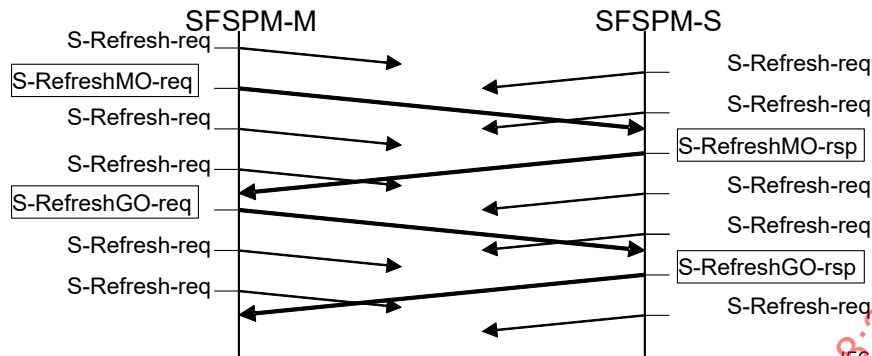
SFSPM-M periodically sends safety PDUs to SFSPM-S based on the SFSPM-M transmission interval (transmission\_interval). SFSPM-S verifies the received safety PDUs.

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 22 shows the sequence at the time of offset measurement and generation between SFSPM-M and SFSPM-S.



**Figure 22 – 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 23 shows an SFSPM-M state transition diagram.

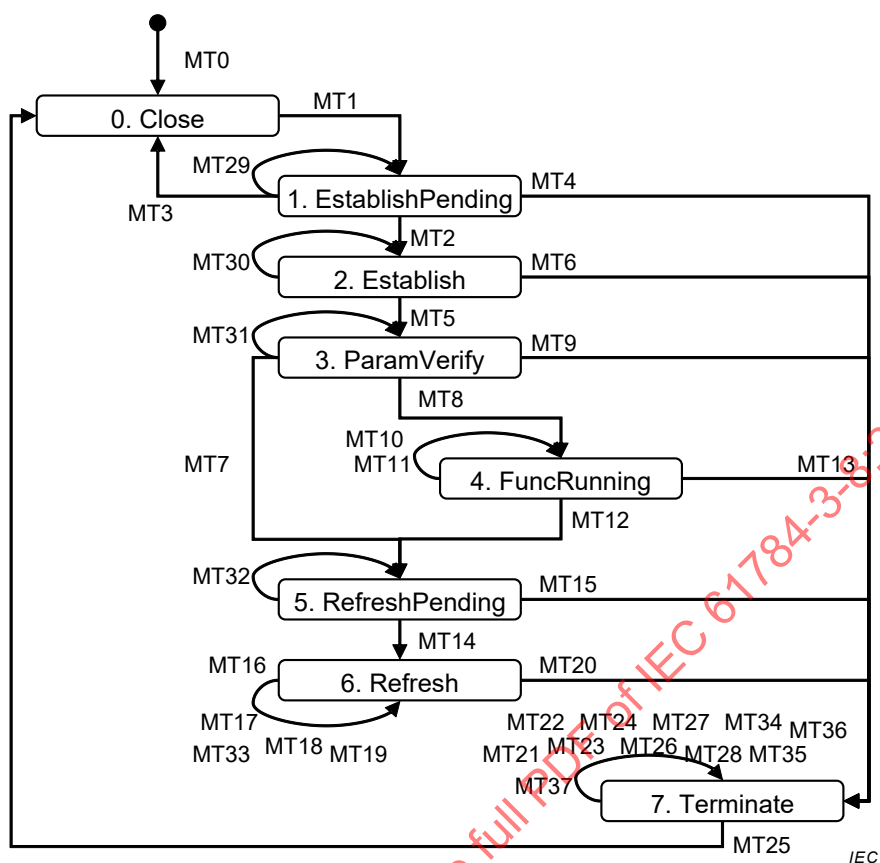


Figure 23 – SFSPM-M state transition diagram

Table 36 describes the timers used by SFSPM-M.

Table 36 – 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 37 shows the SFSPM-M state transition table.

Table 37 – SFSPM-M state transition table

| Trans | State              | Condition                          | Action                                                                                       | Next State         |
|-------|--------------------|------------------------------------|----------------------------------------------------------------------------------------------|--------------------|
| MT0   | —                  | Black channel ready                | —                                                                                            | 0.Close            |
| MT1   | 0.Close            | —                                  | Send S-Connect-req<br>&&<br>Start roundtrip_timer                                            | 1.EstablishPending |
| MT2   | 1.EstablishPending | Receive S-Connect-rsp<br>[NoError] | Stop roundtrip_timer<br>&&<br>Send<br>S-InitConfirmNetPrm-req<br>&&<br>Start roundtrip_timer | 2.Establish        |
| MT29  | 1.EstablishPending | Receive S-Connect-rsp<br>[Busy]    | Stop roundtrip_timer<br>&&<br>Send previously sent                                           | 1.EstablishPending |

| Trans | State              | Condition                                                                  | Action                                                                                                       | Next State       |
|-------|--------------------|----------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|------------------|
|       |                    |                                                                            | S-Connect-req<br>&&<br>Start roundtrip_timer                                                                 |                  |
| MT3   | 1.EstablishPending | roundtrip_timer timeout                                                    | —                                                                                                            | 0.Close          |
| MT4   | 1.EstablishPending | Receive S-Connect-rsp<br>[Error]                                           | Stop roundtrip_timer                                                                                         | 7.Terminate      |
| MT5   | 2.Establish        | Receive<br>S-InitConfirmNetPrm-rsp<br>[NoError]                            | Stop roundtrip_timer<br>&&<br>Send S-InitVerifyStnPrm-req<br>&&<br>Start roundtrip_timer                     | 3.ParamVerify    |
| MT30  | 2.Establish        | Receive<br>S-InitConfirmNetPrm-rsp<br>[Busy]                               | Stop roundtrip_timer<br>&&<br>Send previously sent<br>S-InitConfirmNetPrm-req<br>&&<br>Start roundtrip_timer | 2.Establish      |
| MT6   | 2.Establish        | roundtrip_timer timeout                                                    | —                                                                                                            | 7.Terminate      |
| MT6   | 2.Establish        | Receive<br>S-InitConfirmNetPrm-rsp<br>[Error]                              | Stop roundtrip_timer                                                                                         | 7.Terminate      |
| MT7   | 3.ParamVerify      | Receive<br>S-InitVerifyStnPrm-rsp<br>[NoError]<br>&&<br>OptFuncs not exist | Stop roundtrip_timer<br>&&<br>Send S-RefreshReady-req<br>&&<br>Start roundtrip_timer                         | 6.RefreshPending |
| MT8   | 3.ParamVerify      | Receive<br>S-InitVerifyStnPrm-rsp<br>[NoError]<br>&&<br>OptFuncs exist     | Stop roundtrip_timer<br>&&<br>Send S-InvokeFunc-req<br>&&<br>Start roundtrip_timer                           | 4.FuncRunning    |
| MT31  | 3.ParamVerify      | Receive<br>S-InitVerifyStnPrm-rsp [Busy]                                   | Stop roundtrip_timer<br>&&<br>Send previously sent<br>S-InitVerifyStnPrm-req<br>&&<br>Start roundtrip_timer  | 3.ParamVerify    |
| MT9   | 3.ParamVerify      | roundtrip_timer timeout                                                    | —                                                                                                            | 7.Terminate      |
| MT9   | 3.ParamVerify      | Receive<br>S-InitVerifyStnPrm-rsp [Error]                                  | Stop roundtrip_timer                                                                                         | 7.Terminate      |
| MT10  | 4.FuncRunning      | Receive S-InvokeFunc-rsp<br>[NoError]<br>&&<br>Another OptFunc exists      | Stop roundtrip_timer<br>&&<br>Send S-InvokeFunc-req<br>&&<br>Start roundtrip_timer                           | 4.FuncRunning    |
| MT11  | 4.FuncRunning      | Receive S-InvokeFunc-rsp<br>[Busy]                                         | Stop roundtrip_timer<br>&&<br>Send previously sent<br>S-InvokeFunc-req<br>&&<br>Start roundtrip_timer        | 4.FuncRunning    |
| MT12  | 4.FuncRunning      | Receive S-InvokeFunc-rsp<br>[NoError]<br>&&<br>No other OptFunc exists     | Stop roundtrip_timer<br>&&<br>Send S-RefreshReady-req<br>&&<br>Start roundtrip_timer                         | 6.RefreshPending |
| MT13  | 4.FuncRunning      | roundtrip_timer timeout                                                    | —                                                                                                            | 7.Terminate      |
| MT13  | 4.FuncRunning      | Receive S-InvokeFunc-rsp<br>[Error]                                        | Stop roundtrip_timer                                                                                         | 7.Terminate      |
| MT14  | 5.RefreshPending   | ReceiveS-RefreshReady-rsp                                                  | Stop roundtrip_timer                                                                                         | 6.Refresh        |

| Trans | State            | Condition                                                                  | Action                                                                                                   | Next State       |
|-------|------------------|----------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|------------------|
|       |                  | [NoError]                                                                  | &&<br>Send S-RefreshGO-req<br>&&<br>Start roundtrip_timer                                                |                  |
| MT32  | 5.RefreshPending | ReceiveS-RefreshReady-rsp<br>[Busy]                                        | Stop roundtrip_timer<br>&&<br>Send previously sent<br>S-RefreshReady-req<br>&&<br>Start roundtrip_timer  | 6.RefreshPending |
| MT15  | 5.RefreshPending | roundtrip_timer timeout                                                    | —                                                                                                        | 7.Terminate      |
| MT15  | 5.RefreshPending | ReceiveS-RefreshReady-rsp<br>[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<br>&&<br>Start roundtrip_timer                                                      | 6.Refresh        |
| MT18  | 6.Refresh        | ReceiveS-RefreshMO-rsp<br>[NoError]                                        | Stop roundtrip_timer                                                                                     | 6.Refresh        |
| MT18  | 6.Refresh        | Time to send [at first after<br>S-RefreshMO-rsp with<br>NoMOBusy received] | Send S-RefreshGO-req<br>&&<br>Start roundtrip_timer                                                      | 6.Refresh        |
| MT33  | 6.Refresh        | ReceiveS-RefreshMO-rsp<br>[MOBusy]                                         | Stop roundtrip_timer<br>&&<br>Start roundtrip_timer                                                      | 6.Refresh        |
| MT19  | 6.Refresh        | ReceiveS-RefreshGO-rsp<br>[NoError]                                        | Stop roundtrip_timer                                                                                     | 6.Refresh        |
| MT20  | 6.Refresh        | Receive S-Refresh-req<br>[Error]                                           | —                                                                                                        | 7.Terminate      |
| MT20  | 6.Refresh        | roundtrip_timer timeout                                                    | —                                                                                                        | 7.Terminate      |
| MT20  | 6.Refresh        | ReceiveS-RefreshMO-rsp<br>[Error]                                          | Stop roundtrip_timer                                                                                     | 7.Terminate      |
| MT20  | 6.Refresh        | ReceiveS-RefreshGO-rsp<br>[Error]                                          | Stop roundtrip_timer                                                                                     | 7.Terminate      |
| MT21  | 7.Terminate      | Need to collect error<br>information                                       | Send S-ReadErrorInfo-req<br>&&<br>Start roundtrip_timer                                                  | 7.Terminate      |
| MT22  | 7.Terminate      | Receive S-ReadErrorInfo-rsp<br>[No more data]                              | Stop roundtrip_timer                                                                                     | 7.Terminate      |
| MT34  | 7.Terminate      | Receive S-ReadErrorInfo-rsp<br>[More data]                                 | Stop roundtrip_timer<br>&&<br>S-ReadErrorInfo-req<br>&&<br>Start roundtrip_timer                         | 7.Terminate      |
| MT35  | 7.Terminate      | ReceiveS-ReadErrorInfo-rsp<br>[Busy]                                       | Stop roundtrip_timer<br>&&<br>Send previously sent<br>S-ReadErrorInfo-req<br>&&<br>Start roundtrip_timer | 7.Terminate      |
| MT23  | 7.Terminate      | Need to send error<br>information                                          | Send S-WriteErrorInfo-req<br>&&<br>Start roundtrip_timer                                                 | 7.Terminate      |
| MT24  | 7.Terminate      | Receive S-WriteErrorInfo-rsp<br>[No more data]                             | Stop roundtrip_timer                                                                                     | 7.Terminate      |
| MT36  | 7.Terminate      | Receive S-WriteErrorInfo-rsp<br>[More data]                                | Stop roundtrip_timer<br>&&<br>S-WriteErrorInfo-req<br>&&<br>Start roundtrip_timer                        | 7.Terminate      |

| Trans                                                                                     | State       | Condition                              | Action                                                                                                    | Next State  |
|-------------------------------------------------------------------------------------------|-------------|----------------------------------------|-----------------------------------------------------------------------------------------------------------|-------------|
| MT37                                                                                      | 7.Terminate | Receive S-WriteErrorInfo-rsp<br>[Busy] | Stop roundtrip_timer<br>&&<br>Send previously sent<br>S-WriteErrorInfo-req<br>&&<br>Start roundtrip_timer | 7.Terminate |
| MT25                                                                                      | 7.Terminate | Error resolved                         | —                                                                                                         | 0.Close     |
| MT26                                                                                      | 7.Terminate | Need to invoke Function                | Send S-InvokeFunc-req<br>&&<br>Start roundtrip_timer                                                      | 7.Terminate |
| MT27                                                                                      | 7.Terminate | Receive S-InvokeFunc-rsp               | Stop roundtrip_timer                                                                                      | 7.Terminate |
| MT28                                                                                      | 7.Terminate | Receive S-InvokeFunc-rsp<br>[Busy]     | Send previously sent<br>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 24 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.

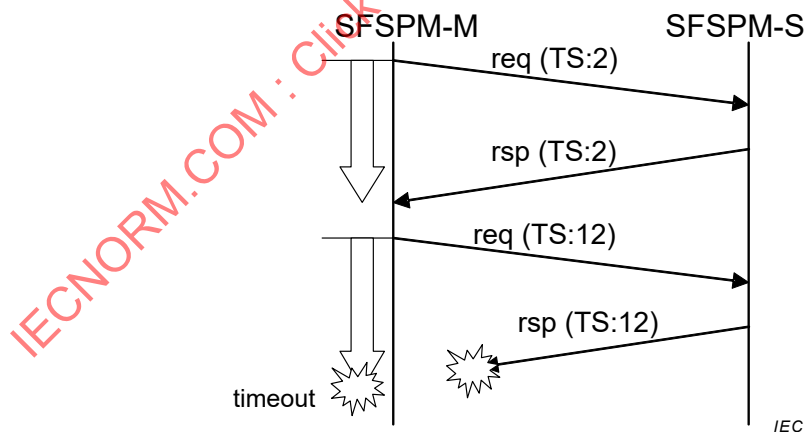
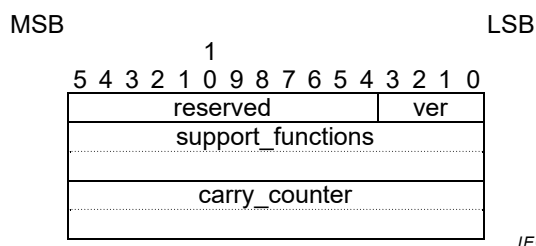


Figure 24 – Sequence other than during safety refresh

### 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 25.

**Figure 25 – 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 38 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 38 – 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                                                |

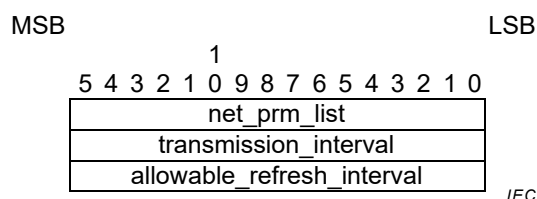
**carry\_counter**

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 26.

**Figure 26 – S-InitConfirmNetPrm-req****net\_prm\_list**

A list of the safety network parameters to be confirmed. Figure 27 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 27 – net\_prm\_list**

The transmission interval of the safety PDUs of SFSPM-M during safety refresh. The unit is 128  $\mu$ s.

The allowable reception interval used by SFSPM-M and SFSPM-S during safety refresh. The unit is 128  $\mu$ s.

S-InitVerifyStnPrm-req uses the S-Data format shown in Figure 15. The safety\_data area stores the data described in Figure 28.



**Figure 28 – S-InitVerifyStnPrm-req**

A list of safety station parameters to be verified. Figure 29 shows the configuration of stn\_prm\_list. 1 indicates that the parameter is to be verified, and 0 indicates that it is not.



**Figure 29 – stn\_prm\_list**

S-InvokeFunc-req uses the S-Data format shown in Figure 15. The safety\_data areas stores the data described in Figure 30.

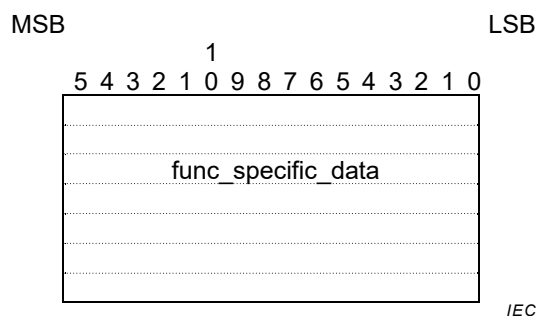


Figure 30 – S-InvokeFunc-req

**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 31.

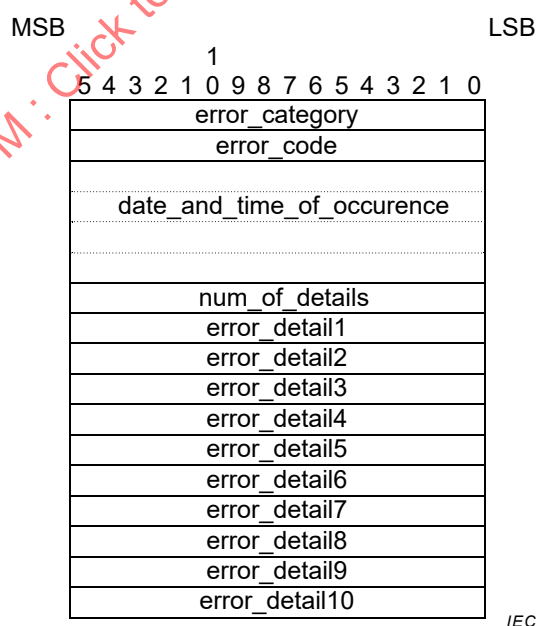


Figure 31 – S-WriteErrorInfo-req

**error\_category**

Indicates the category of an error, and uses the values indicated in Table 39 and Table 40.

**Table 39 – error\_category**

| Value       | Meaning                                                |
|-------------|--------------------------------------------------------|
| 0 – 299     | For future expansion                                   |
| 300 – 349   | Application layer common error (see Table 40)          |
| 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 40 – error\_category for AL errors**

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

**error\_code**

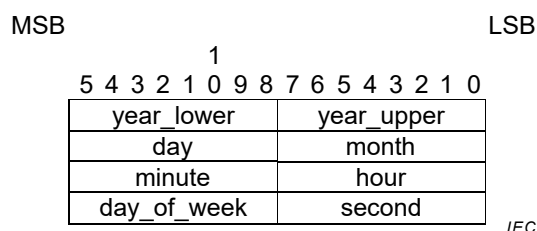
Indicates the error number. The numbers used are shown in Table 41.

**Table 41 – 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\_occurrence**

Indicates the date and time of error occurrence. The format used is that shown in Figure 32. 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 32 – date\_and\_time\_of\_occurrence****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 transitions**

Figure 33 shows an SFSPM-S state transition diagram.

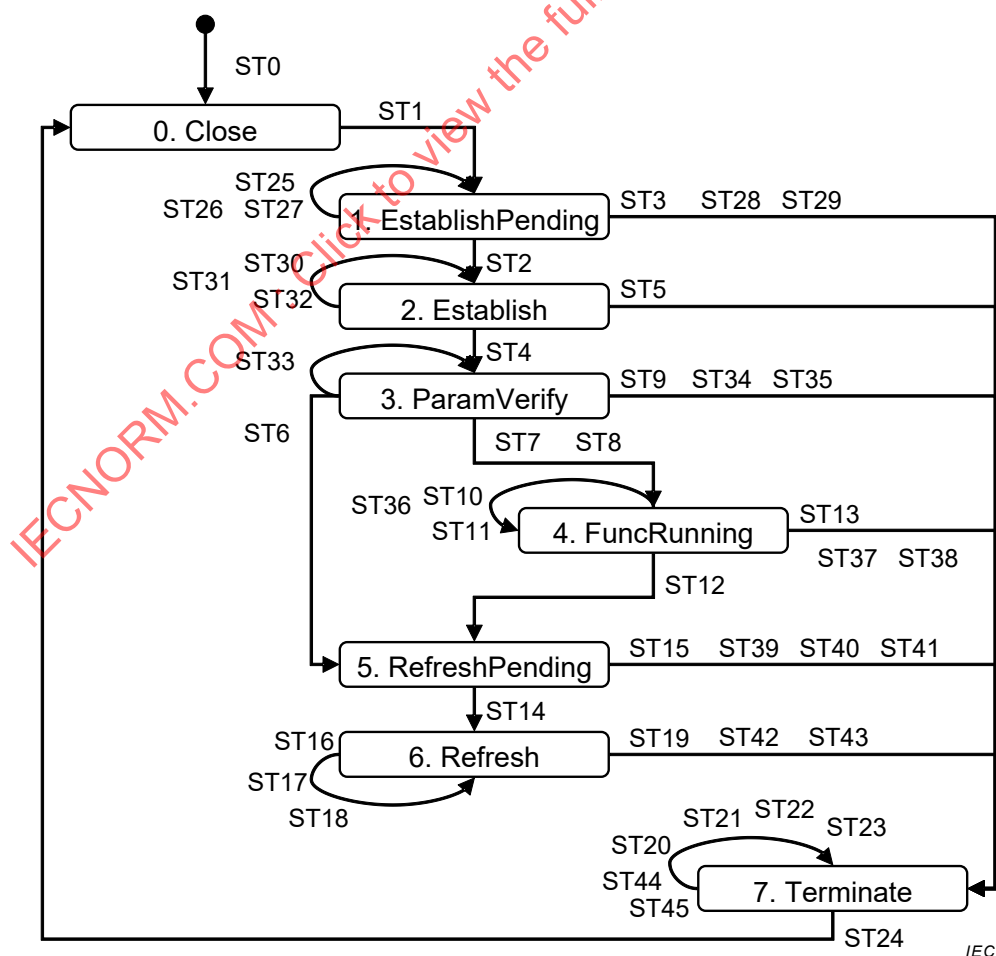


Figure 33 – SFSPM-S state transition diagram

Table 42 describes the timers used by SFSPM-S.

**Table 42 – 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 43 shows the SFSPM-S state transition table.

**Table 43 – SFSPM-S state transition table**

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

| Transition | State         | Condition                                                           | Action                                                                                         | Next State       |
|------------|---------------|---------------------------------------------------------------------|------------------------------------------------------------------------------------------------|------------------|
|            |               |                                                                     | Send S-WriteErrorInfo-rsp<br>&&<br>Start roundtrip_timer                                       |                  |
| ST5        | 2.Establish   | roundtrip_timer timeout                                             | —                                                                                              | 7.Terminate      |
| ST5        | 2.Establish   | Receive S-InitVerifyStnPrm-req [Error]                              | Stop roundtrip_timer<br>&&<br>Send S-InitVerifyStnPrm-rsp                                      | 7.Terminate      |
| ST6        | 3.ParamVerify | Receive S-RefreshReady-req<br>[NoError]                             | Stop roundtrip_timer<br>&&<br>Send S-RefreshReady-rsp<br>&&<br>Start roundtrip_timer           | 5.RefreshPending |
| ST33       | 3.ParamVerify | Receive S-RefreshReady-req<br>[Busy]                                | Stop roundtrip_timer<br>&&<br>Send S-RefreshReady-rsp<br>&&<br>Start roundtrip_timer           | 3.ParamVerify    |
| ST7        | 3.ParamVerify | Receive S-InvokeFunc-req<br>[NoError]<br>&&<br>Processing complete  | Stop roundtrip_timer<br>&&<br>Send S-InvokeFunc-rsp<br>[NoBusy]<br>&&<br>Start roundtrip_timer | 4.FuncRunning    |
| ST8        | 3.ParamVerify | Receive S-InvokeFunc-req<br>[NoError]<br>&&<br>Function in progress | Stop roundtrip_timer<br>&&<br>Send S-InvokeFunc-rsp [Busy]<br>&&<br>Start roundtrip_timer      | 4.FuncRunning    |
| ST34       | 3.ParamVerify | Receive S-WriteErrorInfo-req<br>[No more data]                      | Stop roundtrip_timer<br>&&<br>Send S-WriteErrorInfo-rsp                                        | 7.Terminate      |
| ST35       | 3.ParamVerify | Receive S-WriteErrorInfo-req<br>[More data]                         | Stop roundtrip_timer<br>&&<br>Send S-WriteErrorInfo-rspStart<br>roundtrip_timer                | 7.Terminate      |
| ST9        | 3.ParamVerify | roundtrip_timer timeout                                             | —                                                                                              | 7.Terminate      |
| ST9        | 3.ParamVerify | Receive S-InvokeFunc-req<br>[Error]                                 | Stop roundtrip_timer                                                                           | 7.Terminate      |
| ST9        | 3.ParamVerify | Receive S-RefreshReady-req<br>[Error]                               | Stop roundtrip_timer<br>&&<br>Send S-RefreshReady-rsp                                          | 7.Terminate      |
| ST10       | 4.FuncRunning | Receive S-InvokeFunc-req<br>[NoError]<br>&&<br>Processing complete  | Stop roundtrip_timer<br>&&<br>Send S-InvokeFunc-rsp<br>[NoBusy]<br>&&<br>Start roundtrip_timer | 4.FuncRunning    |
| ST11       | 4.FuncRunning | Receive S-InvokeFunc-req<br>[NoError]<br>&&<br>Function in progress | Stop roundtrip_timer<br>&&<br>Send S-InvokeFunc-rsp [Busy]<br>&&<br>Start roundtrip_timer      | 4.FuncRunning    |
| ST12       | 4.FuncRunning | Receive S-RefreshReady-req<br>[NoError]                             | Stop roundtrip_timer<br>&&<br>Send S-RefreshReady-rsp<br>&&<br>Start roundtrip_timer           | 5.RefreshPending |
| ST36       | 4.FuncRunning | Receive S-InvokeFunc-req<br>[Busy]                                  | Stop roundtrip_timer<br>&&<br>Send S-InvokeFunc-rsp<br>&&<br>Start roundtrip_timer             | 4.FuncRunning    |
| ST37       | 4.FuncRunning | Receive S-WriteErrorInfo-req                                        | Stop roundtrip_timer                                                                           | 7.Terminate      |

| Transition | State            | Condition                                                                 | Action                                                                                 | Next State  |
|------------|------------------|---------------------------------------------------------------------------|----------------------------------------------------------------------------------------|-------------|
|            |                  | [No more data]                                                            | &&<br>Send S-WriteErrorInfo-rsp                                                        |             |
| ST38       | 4.FuncRunning    | Receive S-WriteErrorInfo-req<br>[More data]                               | Stop roundtrip_timer<br>&&<br>Send S-WriteErrorInfo-rsp<br>&&<br>Start roundtrip_timer | 7.Terminate |
| ST13       | 4.FuncRunning    | roundtrip_timer timeout                                                   | —                                                                                      | 7.Terminate |
| ST13       | 4.FuncRunning    | Receive S-InvokeFunc-req<br>[Error]                                       | Stop roundtrip_timer<br>&&<br>Send S-InvokeFunc-rsp                                    | 7.Terminate |
| ST13       | 4.FuncRunning    | Receive S-RefreshReady-req<br>[Error]                                     | Stop roundtrip_timer<br>&&<br>Send S-RefreshReady-rsp                                  | 7.Terminate |
| ST14       | 5.RefreshPending | ReceiveS-RefreshGO-req<br>[NoError]                                       | Stop roundtrip_timer<br>&&<br>Send S-RefreshGO-rsp                                     | 6.Refresh   |
| ST39       | 5.RefreshPending | Receive S-WriteErrorInfo-req<br>[No more data]                            | Stop roundtrip_timer<br>&&<br>Send S-WriteErrorInfo-rsp                                | 7.Terminate |
| ST40       | 5.RefreshPending | Receive S-WriteErrorInfo-req<br>[More data]                               | Stop roundtrip_timer<br>&&<br>Send S-WriteErrorInfo-rsp<br>&&<br>Start roundtrip_timer | 7.Terminate |
| ST15       | 5.RefreshPending | roundtrip_timer timeout                                                   | —                                                                                      | 7.Terminate |
| ST15       | 5.RefreshPending | ReceiveS-RefreshGO-req<br>[ErrorA]                                        | Stop roundtrip_timer                                                                   | 7.Terminate |
| ST15       | 5.RefreshPending | ReceiveS-RefreshGO-req<br>[ErrorB]                                        | Stop roundtrip_timer<br>&&<br>Send S-RefreshGO-rsp<br>&&<br>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<br>[NoError]                                      | Stop roundtrip_timer                                                                   | 6.Refresh   |
| ST17       | 6.Refresh        | Time to send [at first after<br>S-RefreshMO-req with<br>NoError received] | Send S-RefreshMO-rsp<br>&&<br>Start roundtrip_timer                                    | 6.Refresh   |
| ST18       | 6.Refresh        | Receive S-RefreshGO-req<br>[NoError]                                      | —                                                                                      | 6.Refresh   |
| ST18       | 6.Refresh        | Time to send [at first after<br>S-RefreshGO-req with<br>NoError received] | Send S-RefreshGO-rsp                                                                   | 6.Refresh   |
| ST41       | 6.Refresh        | Receive S-WriteErrorInfo-req<br>[No more data]                            | Stop roundtrip_timer<br>&&<br>Send S-WriteErrorInfo-rsp                                | 7.Terminate |
| ST42       | 6.Refresh        | Receive S-WriteErrorInfo-req<br>[More data]                               | Stop roundtrip_timer<br>&&<br>Send S-WriteErrorInfo-rsp<br>&&<br>Start roundtrip_timer | 7.Terminate |
| ST19       | 6.Refresh        | Receive S-Refresh-req [Error]                                             | —                                                                                      | 7.Terminate |
| ST19       | 6.Refresh        | Time to send [at first after<br>S-Refresh-req with ErrorA<br>received]    | Send S-Refresh-req<br>&&<br>Start roundtrip_timer                                      | 7.Terminate |
| ST19       | 6.Refresh        | Receive S-RefreshMO-req<br>[Error]                                        | —                                                                                      | 7.Terminate |
| ST19       | 6.Refresh        | Time to send [at first after<br>S-RefreshMO-req with ErrorA               | Send S-RefreshMO-rsp<br>&&                                                             | 7.Terminate |

| Transition                                                                                                                                                                                                                                                                                                                                                   | State       | Condition                                                                | Action                                                                                 | Next State  |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|--------------------------------------------------------------------------|----------------------------------------------------------------------------------------|-------------|
|                                                                                                                                                                                                                                                                                                                                                              |             | received]                                                                | Startroundtrip_timer                                                                   |             |
| ST19                                                                                                                                                                                                                                                                                                                                                         | 6.Refresh   | Receive S-RefreshGO-req<br>[Error]                                       | Stop roundtrip_timer                                                                   | 7.Terminate |
| ST19                                                                                                                                                                                                                                                                                                                                                         | 6.Refresh   | Time to send [at first after<br>S-RefreshGO-req with ErrorA<br>received] | Send S-RefreshGO-rsp<br>&&<br>Startroundtrip_timer                                     | 7.Terminate |
| ST19                                                                                                                                                                                                                                                                                                                                                         | 6.Refresh   | roundtrip_timer timeout                                                  | —                                                                                      | 7.Terminate |
| ST20                                                                                                                                                                                                                                                                                                                                                         | 7.Terminate | Receive S-ReadErrorInfo-req<br>[No more data]                            | Send S-ReadErrorInfo-rsp                                                               | 7.Terminate |
| ST43                                                                                                                                                                                                                                                                                                                                                         | 7.Terminate | Receive S-ReadErrorInfo-req<br>[More data]                               | Stop roundtrip_timer<br>&&<br>Send S-ReadErrorInfo-rsp<br>&&<br>Startp roundtrip_timer | 7.Terminate |
| ST21                                                                                                                                                                                                                                                                                                                                                         | 7.Terminate | Receive S-WriteErrorInfo-req<br>[No more data]                           | Send S-WriteErrorInfo-rsp                                                              | 7.Terminate |
| ST44                                                                                                                                                                                                                                                                                                                                                         | 7.Terminate | Receive S-WriteErrorInfo-req<br>[More data]                              | Stop roundtrip_timer<br>&&<br>Send S-WriteErrorInfo-rsp<br>&&<br>Start roundtrip_timer | 7.Terminate |
| ST22                                                                                                                                                                                                                                                                                                                                                         | 7.Terminate | Receive S-InvokeFunc-req<br>[NoError]<br><br>&&<br>Processing complete   | Send S-InvokeFunc-rsp<br>[NoBusy]                                                      | 7.Terminate |
| ST23                                                                                                                                                                                                                                                                                                                                                         | 7.Terminate | Receive S-InvokeFunc-req<br>[NoError]<br><br>&&<br>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<br>ST15 Error A: Unallowable delay<br>ST15 Error B: Incorrect order, Abnormal CTRL, Error state bit = 1<br>ST19 Error: Incorrect order, Loss, Unallowable delay, Abnormal CTRL, Error state bit = 1<br>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 34 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.

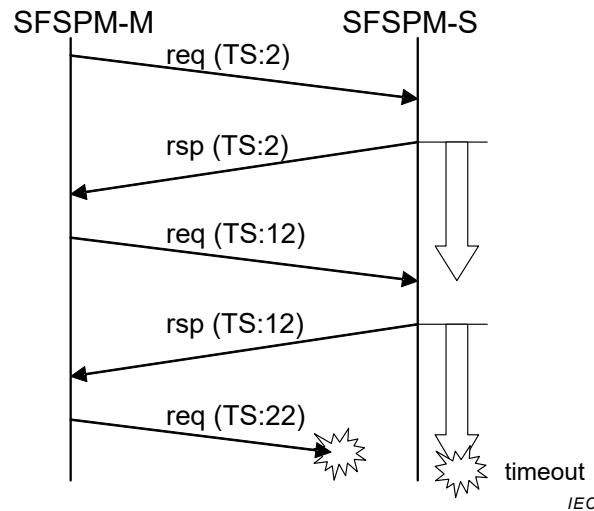


Figure 34 – Sequence other than during safety refresh

#### 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 35.

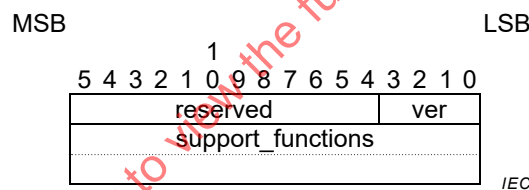


Figure 35 – S-Connect-rsp

#### Ver

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

#### reserved

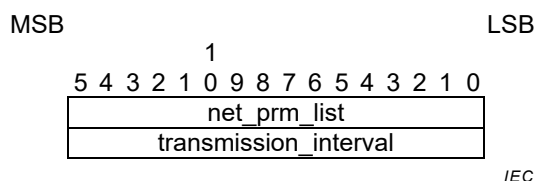
Reserved for future expansion.

#### support\_functions

Indicate the functions supported by SFSPM-S out of the support\_functions that SFSPM-M reported to SFSPM-S. Table 38 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 Figure 36.

**Figure 36 – S-InitConfirmNetPrm-rsp****net\_prm\_list**

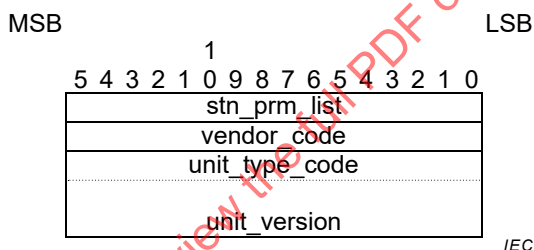
A list of safety network parameters to be confirmed. 1 indicates that the parameter is to be confirmed and 0 indicates that it is not. For the configuration of net\_prm\_list, see Figure 27. The bit of transmission\_interval is set to 1.

**transmission\_interval**

The transmission interval of the safety PDUs of SFSPM-S during safety refresh. The unit is 128  $\mu$ s.

**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 37.

**Figure 37 – 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**

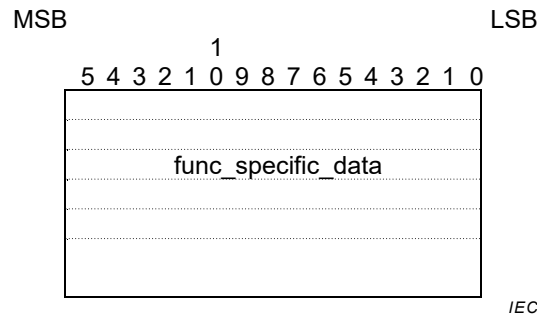
A unique code assigned to each product model managed by the vendor.

**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 38.



**Figure 38 – 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 31. 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.

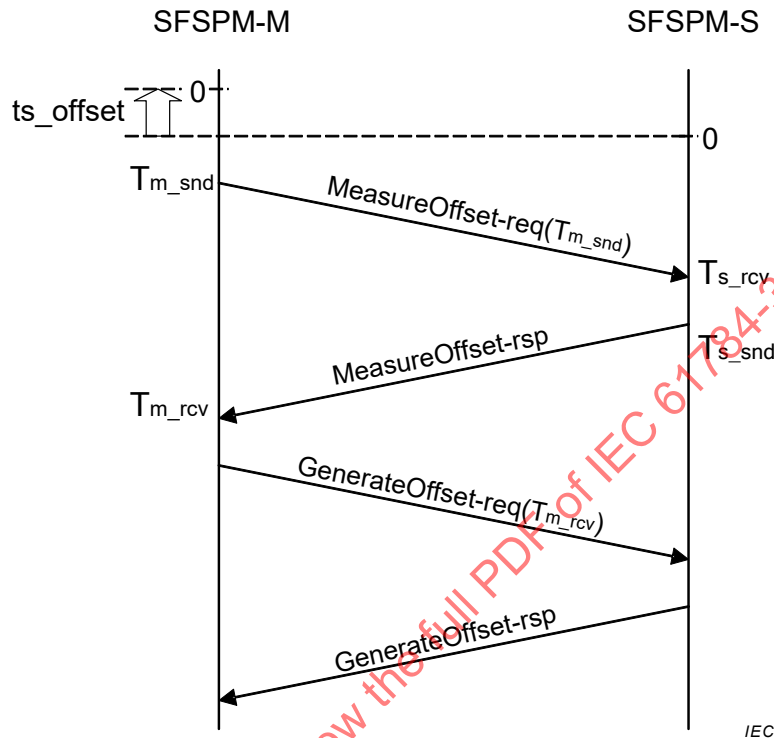
SFSPM-S shall use the value current\_time of the lower 16 bits of the safety clock of its own node and the offset ts\_offset to generate time stamps. SFSPM-S shall use the following formula for this calculation:

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

Figure 39 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 39 – 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 the formula below. If the value is out of range, SFSPM-S shall not use the collected information in offset calculation.

$$0 < (T_{m\_rcv} - T_{m\_snd}) - (T_{s\_snd} - T_{s\_rcv}) \leq 2 * \text{link\_transmission\_delay}$$

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). The calculation formula is as follows:

$$D_{lt} = I_{ar} - I_{mt} - I_{st}$$

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.

The following formula shall be used to calculate the offset ts\_offset:

$$ts\_offset = 0.5 * ( (T_{m\_rcv} + T_{m\_snd}) - (T_{s\_snd} + T_{s\_rcv}) )$$

The calculated dispersion offset\_dispersions of the following formula is included in the calculated offset ts\_offset:

$$offset\_dispersion = 0.5 * ( (T_{m\_rcv} - T_{m\_snd}) + (T_{s\_rcv} - T_{s\_snd}) )$$

The maximum value of the calculation deviation offset\_dispersions 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.

$$interval = transmission\_interval * resolution\_factor$$

If the safety clock accuracy is 100 ppm, the error is  $\pm 100 \mu s$  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  $200 \mu s$  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  $128 \mu s$ . The resolution\_factor calculation formula in such a case is as follows:

$$resolution\_factor < 640 / transmission\_interval$$

#### 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 the formula below, 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.

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

#### 12.7.2.7 Operating carry\_counter

SFSPM-S calculates the SFSPM-M\_current\_time using the formula below 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.

$$\text{SFSPM-M\_current\_time} = (\text{current\_time} + \text{ts\_offset}) \bmod 2^{16}$$

If the following formula is satisfied, the carry\_counter is incremented by 1.

$$\text{prev\_SFSPM-M\_current\_time} > \text{SFSPM-M\_current\_time}$$

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 44 lists the parameters used by FSCP 8/2.

**Table 44 – 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).

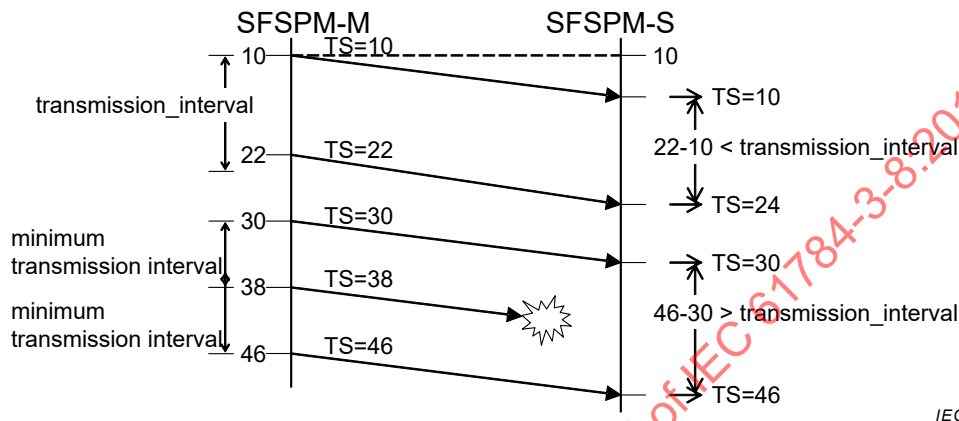
##### 12.8.1.3 transmission\_interval

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 fluctuation of the transmission interval shall be within the range below:

$$\text{transmission\_interval} / 2 < \text{actual transmission interval} \leq \text{transmission\_interval}$$

To normally receive safety PDUs sent at the maximum transmission interval ( $\text{transmission\_interval}$ ), 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 40 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 40 – Relationship between transmission interval fluctuation and transmission\_interval**

#### 12.8.1.4 allowable\_refresh\_interval

$\text{allowable\_refresh\_interval}$  is a configurable parameter that specifies the allowable refresh interval by the receiving node. The size is 16 bits, and the unit is 128  $\mu\text{s}$ .

The following formula is used to calculate  $\text{allowable\_refresh\_interval}$  in SFSPM-S when safety PDUs are sent from SFSPM-M to SFSPM-S:

SFSPM-S allowable refresh interval

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

where

- $I_{\text{sar}}$  is the SFSPM-S allowable refresh interval
- $I_t$  SFSPM-M transmission interval
- $D_{\text{lt}}$  link transmission delay of the FAL Type 23 network
- $T_{\text{spc}}$  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 41 illustrates the concept of determining the  $\text{allowable\_refresh\_interval}$  of SFSPM-S and SFSPM-M.

When the maximum delay time ( $\text{TS3} - \text{TS4}$ ) follows the shortest delay time ( $\text{TS1} - \text{TS2}$ ) during communication from SFSPM-M to SFSPM-S, the reception interval is calculated as shown below, where  $\text{transmission\_interval}$  (SFSPM-M) indicates the  $\text{transmission\_interval}$  of SFSPM-M.

SFSPM-S reception interval

$$I_{sr} = I_t + D_t + T_{soc}$$

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

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

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

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. The calculation formula is as follows:

Allowable refresh interval

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

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.

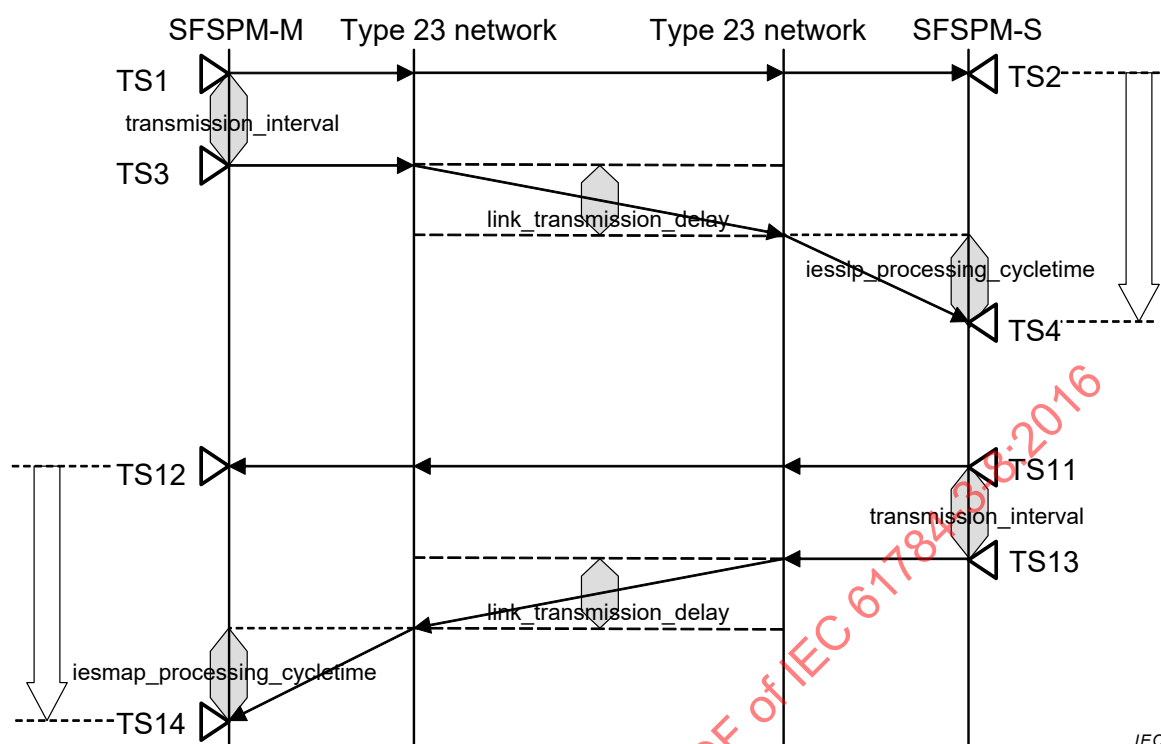


Figure 41 – Calculation of allowable\_refresh\_interval

#### 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  $\mu$ s.

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

$$D_{ma} = D_{lt} + T_{mpc}$$

$$D_{ma} = I_{ar} - I_{st}$$

Allowable delay for SFSPM-S

$$D_{sa} = D_{lt} + T_{spc}$$

$$D_{sa} = I_{ar} - I_{mt}$$

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 42 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.

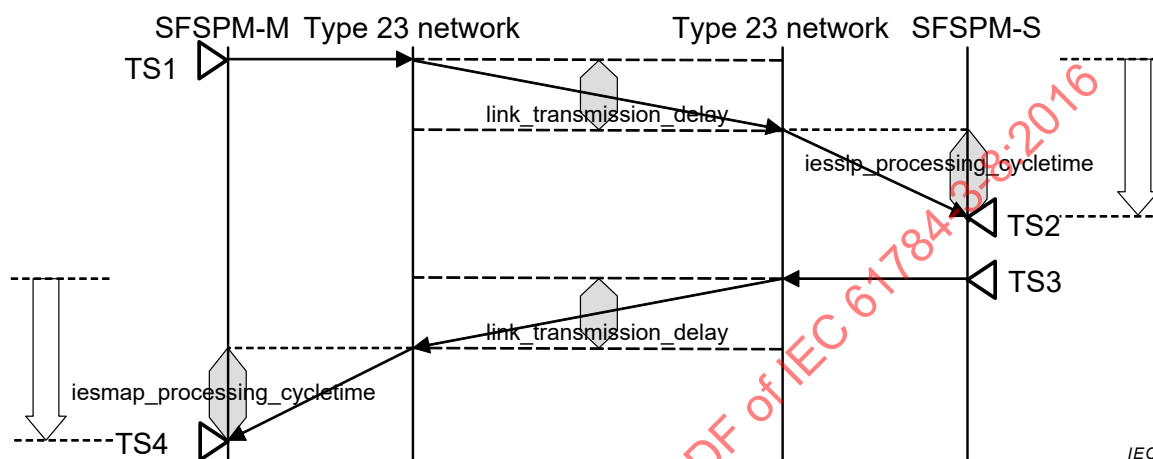


Figure 42 – Calculation of `allowable_delay`

#### 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  $\mu$ s, 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 44 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 45 shows the parameters of SM-SetSafetyStationInfo.

Table 45 – 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 46.

### R Data

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

**Table 46 – 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<br>0x1-0x3: Reserved<br>0x4: Safety remote device<br>0x5: Safety remote I/O<br>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 47 shows the parameters of SM-SetSafetyNetworkParameter.

**Table 47 – 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 48.

### R Data

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

**Table 48 – 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<br>0x1:SFSPM-S |
| 5  | Maximum transmission interval | 2             | 2 – 65535               |                            |

| No | Item                       | Size (Octets) | Range     | Remarks      |
|----|----------------------------|---------------|-----------|--------------|
| 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 49 shows the parameters of SM-GetSafetyStationInfo.

**Table 49 – 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 50.

#### R Data

Contains the acquisition result. See Table 51.

**Table 50 – 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 51 – Safety station information parameters of SM-GetSafetyStationInfo (Response)**

| No | Item                            | Size (Octets) | Range                   | Remarks                                                                                                             |
|----|---------------------------------|---------------|-------------------------|---------------------------------------------------------------------------------------------------------------------|
| 1  | Safety station type             | 2             | 0x0000 – 0xFFFF         | 0x0: Safety PLC<br>0x1-0x3: Reserved<br>0x4: Safety remote device<br>0x5: Safety remote I/O<br>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 52 shows the parameters of SM-GetSafetyNetworkParameter.

**Table 52 – 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 53.

#### R Data

Contains the acquisition result. See Table 54.

**Table 53 – 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 54 – Parameters of SM-GetSafetyNetworkParameter response**

| No | Item                          | Size (Octets) | Range     | Remarks                    |
|----|-------------------------------|---------------|-----------|----------------------------|
| 1  | Safety connection end type    | 1             | 0x0 – 0x1 | 0x0:SFSPM-M<br>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 and Table 56 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 55 – 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<br>Out: Power is off                                                                                                                                                                                                                                                                                                                                                                                                                             | R                     | R                          | R                                       | R                                  | R                               |
| 2   | RUN      | Lit: Operation is normal<br>Out: Error has occurred at station                                                                                                                                                                                                                                                                                                                                                                                                    | M                     | R                          | R                                       | O                                  | O                               |
| 3   | ERR      | Lit: Error<br>Safety master:<br><ul style="list-style-type: none"> <li>Station number conflict</li> <li>Inconsistency in sampled network information</li> <li>Error occurred at station</li> </ul> Safety slave:<br><ul style="list-style-type: none"> <li>Error occurred at station</li> </ul> Flashing: Data link error<br>Safety master:<br><ul style="list-style-type: none"> <li>A station exists with a data link error</li> </ul> Out: Operation is normal | M                     | R                          | R                                       | O                                  | O                               |
| 4   | MST      | Lit: Station is operating as the master station<br>Out: Station is not operating as the master station                                                                                                                                                                                                                                                                                                                                                            | O                     | —                          | —                                       | —                                  | —                               |
| 5   | D LINK   | Lit: Cyclic transmission is being performed<br>Out: Disconnection                                                                                                                                                                                                                                                                                                                                                                                                 | M                     | R                          | R                                       | O                                  | O                               |
| 6   | L.ERR    | Lit: Received data error<br>Out: Received data are normal                                                                                                                                                                                                                                                                                                                                                                                                         | M                     | R                          | R                                       | R                                  | R                               |
| 7   | SD       | Lit: Data are being transmitted<br>Out: Data are not being transmitted                                                                                                                                                                                                                                                                                                                                                                                            | R                     | R                          | R                                       | R                                  | R                               |
| 8   | RD       | Lit: Data are being received<br>Out: Data are not being received                                                                                                                                                                                                                                                                                                                                                                                                  | R                     | R                          | R                                       | R                                  | R                               |

**Table 56 – 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<br>Out: Link is not operational  | O                     | O                          | O                                       | O                                  | O                               |
| 2   | L.ER     | Lit: Received data error<br>Out: Received data are normal | O                     | O                          | O                                       | O                                  | O                               |

### 12.9.2 Installation guidelines

This standard 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 standard requires proper installation. All devices connected to a safety communication system defined in this part shall follow the recommendations and comply with the specifications given in IEC 61784-5-8.

### 12.9.3 Safety function response time

Figure 43 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.

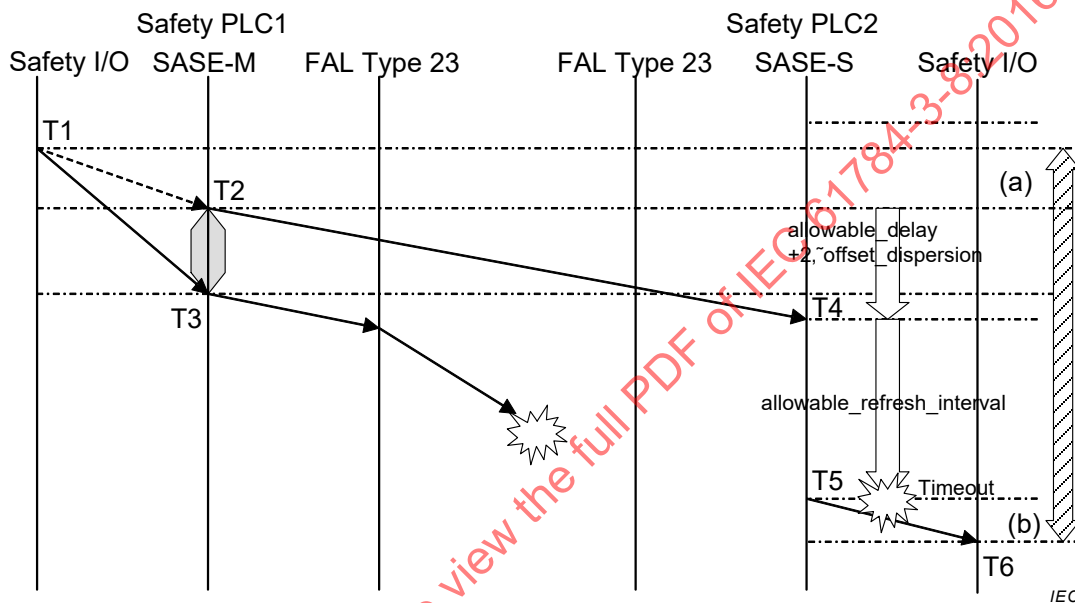


Figure 43 – Calculation of response time between safety PLCs

The response time of safety communication from safety PLC1 to safety PLC2 in Figure 43 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 is calculated using the formula below:

Response Time

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

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

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

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  $2 \times$  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

##### 12.9.5.1 Number of stations

The number of stations is not restricted. The maximum number of connections depends on the transmission interval. With 1 ms as the shortest actual transmission interval, the maximum number of connections is 1 814.

##### 12.9.5.2 Probability considerations

The residual error rate shall be calculated using the following formula which is defined in IEC 61784-3:

Residual error rate

$$\Lambda_{SL}(P_e) = 3600 \times (v) \times (m) \times (R_{SL}(P_e))$$

where

|                     |                                                                                                         |
|---------------------|---------------------------------------------------------------------------------------------------------|
| $\Lambda_{SL}(P_e)$ | is the residual error rate per hour of the safety communication layer related to bit error probability; |
| $P_e$               | is the bit error probability;                                                                           |
| $R_{SL}(P_e)$       | is the residual error probability of safety messages;                                                   |
| $v$                 | is the maximum number of safety messages per second;                                                    |
| $m$                 | is the maximum number of information reception connections allowed per safety function.                 |

The CRC generator polynomial described in 12.7.1.7 is the generator polynomial indicated as 0x1F1922815. This CRC generator polynomial exhibits properness when the sum of the message length and CRC length ( $n$ ) is less than 2046. The CRC generator polynomial has a minimum hamming distance of 8 when  $n$  is within the range 99 to 1024 inclusively.

NOTE 1 Document [36] contains important information related to CRC.

When the CRC generator polynomial exhibits properness, approximate calculation of the residual error rate with a weighting factor of  $2^{-r}$  is possible. See IEC 61784-3.

The safety PDU size of the FSCP 8/2 safety communication function is 256 bits (less than 2046), and the CRC generator polynomial exhibits properness. The residual error rate  $\Lambda$  is calculated using the following formula which applies  $2^{-r}$ :

Residual error rate

$$\Lambda(P_e) = 3\,600 \times v \times m \times R_{CRC}(P_e)$$

$$\begin{aligned} \Lambda(P_e) &\approx 3\,600 \times v \times m \times 2^{-r} \times \sum_{k=d_{\min}}^n \binom{n}{k} \times P_e^k \times (1-P_e)^{n-k} \\ &\approx 3\,600 \times v \times m \times 2^{-r} \times \sum_{k=d_{\min}}^n \frac{n!}{k! \times (n-k)!} \times P_e^k \times (1-P_e)^{n-k} \end{aligned}$$

where

|                |                                                                        |
|----------------|------------------------------------------------------------------------|
| $v$            | is the maximum number of safety messages per second;                   |
| $m$            | is the number of connections $\times 2$ (for both directions);         |
| $R_{CRC}(P_e)$ | is the residual error probability with cyclic redundancy test applied; |
| $d_{\min}$     | is the minimum hamming distance;                                       |
| $P_e$          | is the bit error probability;                                          |
| $n$            | is the bit stream length, including CRC;                               |
| $r$            | is the CRC bit length.                                                 |

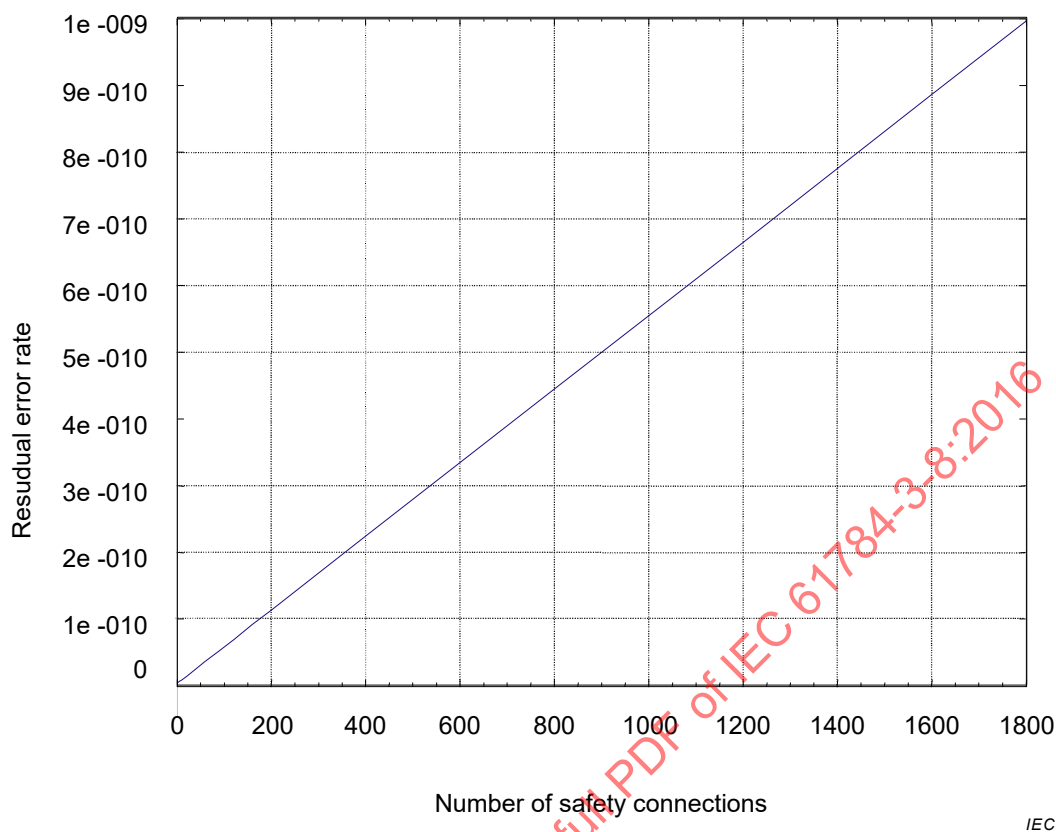
Here the bit stream length including CRC is 256 bits, the CRC bit length is 32, and the minimum hamming distance is 8.  $10^{-3}$  is used for bit error probability.

NOTE 2 The  $P_e$  value of  $10^{-3}$  has been validated by an independent assessment organisation for FAL Type 23.

To achieve the safety level SL3,  $\Lambda$  less than  $10^{-9}$  shall be satisfied.

Figure 44 shows the relationship between the number of safety connections and the residual error rate given a minimum transmission interval of 1ms on the transmission side.  $\Lambda$  less than  $10^{-9}$ , which is required for SIL3, is satisfied in the range up to 1 814 connections.

transmission\_interval is the maximum transmission interval, and the minimum value is 2 ms. See 12.7.2. The actual transmission interval is one half of the transmission\_interval, and thus 1 ms is used as the minimum transmission interval.



**Figure 44 – Relationship between safety connections and residual error rate**

### 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 standard. 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. 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 [34] and [35] 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 [34] and [35] 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).

IECNORM.COM : Click to view the full PDF of IEC 61784-3-8:2016

## 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 by IEEE 802.3.

#### A.2 Hash function calculation for FSCP 8/2

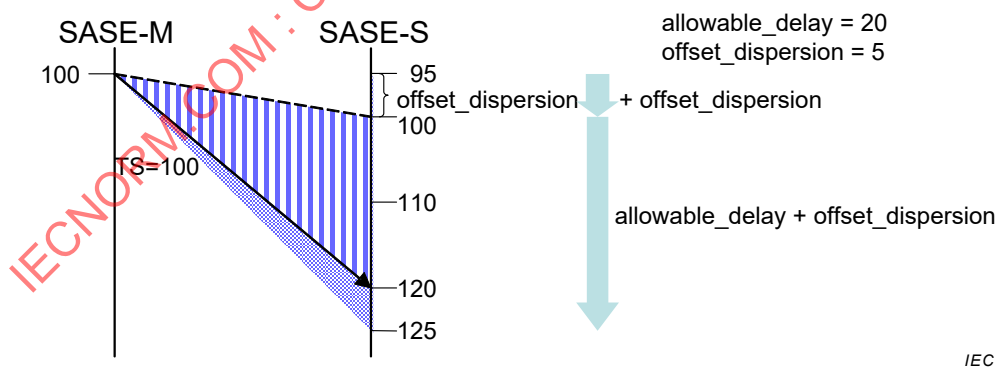
The CRC32 for FSCP 8/2 is calculated using the following algorithm:

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

This is the algorithm defined as 0x1F1922815 given in [36].

#### 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 43 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 standard 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 standard 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](http://www.cc-link.org).

IECNORM.COM : Click to view the full PDF of IEC 61784-3-8:2016

## Bibliography

- [1] IEC 60050 (all parts), *International Electrotechnical Vocabulary* (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 TS 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*
- [3] 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*
- [4] IEC 61131-6, *Programmable controllers – Part 6: Functional safety*
- [5] IEC 61496 (all parts), *Safety of machinery – Electro-sensitive protective equipment*
- [6] IEC 61508-1:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements*
- [7] IEC 61508-4:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations*
- [8] 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*
- [9] IEC 61784-2, *Industrial communication networks – Profiles – Part 2: Additional fieldbus profiles for real-time networks based on ISO/IEC 8802-3*
- [10] IEC 61784-4<sup>7</sup>, *Industrial communication networks – Profiles – Part 4: Secure communications for fieldbuses*
- [11] IEC 61784-5 (all parts), *Industrial communication networks – Profiles – Part 5: Installation of fieldbuses – Installation profiles for CPF x*
- [12] IEC 61800-5-2, *Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional*
- [13] IEC 61918, *Industrial communication networks – Installation of communication networks in industrial premises*
- [14] IEC TR 62059-11:2002, *Electricity metering equipment – Dependability – Part 11: General concepts*
- [15] IEC TR 62210:2003, *Power system control and associated communications – Data and communication security*
- [16] IEC 62280:2014, *Railway applications – Communication, signalling and processing systems – Safety related communication in transmission systems*

---

<sup>7</sup> Proposed new work item under consideration.

- [17] IEC 62443 (all parts), *Industrial communication networks – Network and system security*
- [18] IEC TR 62685, *Industrial communication networks – Profiles – Assessment guideline for safety devices using IEC 61784-3 functional safety communication profiles (FSCPs)*
- [19] ISO/IEC Guide 51:2014, *Safety aspects – Guidelines for their inclusion in standards*
- [20] ISO/IEC 2382-14, *Information technology – Vocabulary – Part 14: Reliability, maintainability and availability*
- [21] ISO/IEC 2382-16:1996, *Information technology – Vocabulary – Part 16: Information theory*
- [22] ISO/IEC 7498-1, *Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model*
- [23] ISO 10218-1, *Robots and robotic devices – Safety requirements for industrial robots – Part 1: Robots*
- [24] ISO 12100, *Safety of machinery – General principles for design – Risk assessment and risk reduction*
- [25] ISO 13849-1:2006, *Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design*
- [26] ISO 13849-2, *Safety of machinery – Safety-related parts of control systems – Part 2: Validation*
- [27] ANSI/ISA-84.00.01-2004 (all parts), *Functional Safety: Safety Instrumented Systems for the Process Industry Sector*
- [28] VDI/VDE 2180 (all parts), *Safeguarding of industrial process plants by means of process control engineering*
- [29] ANDREW S. TANENBAUM, DAVID J. WETHERALL, *Computer Networks*, 5<sup>th</sup> Edition, Prentice Hall, N.J., ISBN-10: 0132126958, ISBN-13: 978-0132126953
- [30] W. WESLEY PETERSON, EDWARD J. WELDON, *Error-Correcting Codes*, 2nd Edition 1972, MIT-Press, ISBN 0-262-16-039-0
- [31] NFPA79 (2012), *Electrical Standard for Industrial Machinery*
- [32] GUY E. CASTAGNOLI, *On the Minimum Distance of Long Cyclic Codes and Cyclic Redundancy-Check Codes*, 1989, Dissertation No. 8979 of ETH Zurich, Switzerland
- [33] 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
- [34] CC-Link Safety Specifications, *Overview/Protocol*, BAP-C1603-001, CLPA
- [35] CC-Link Safety Specifications, *Implementation*, BAP-C1603-002, CLPA
- [36] CC-Link Safety Specifications, *Profiles*, BAP-C1603-003, CLPA

- [37] CC-Link IE Safety Specifications, *Overview, BAP-C1606-001, CLPA*
  - [38] CC-Link IE Safety Specifications, *Application Layer Service and Protocol Communication profile, BAP-C1606-002, CLPA*
- 

IECNORM.COM : Click to view the full PDF of IEC 61784-3-8:2016

## SOMMAIRE

|                                                                                  |     |
|----------------------------------------------------------------------------------|-----|
| AVANT-PROPOS .....                                                               | 109 |
| 0 Introduction .....                                                             | 111 |
| 0.1 Généralités .....                                                            | 111 |
| 0.2 Déclaration de droits de propriété .....                                     | 114 |
| 1 Domaine d'application .....                                                    | 116 |
| 2 Références normatives .....                                                    | 116 |
| 3 Termes, définitions, symboles, abréviations et conventions .....               | 118 |
| 3.1 Termes et définitions .....                                                  | 118 |
| 3.1.1 Termes et définitions communs .....                                        | 118 |
| 3.1.2 CPF 8: Termes et définitions supplémentaires .....                         | 125 |
| 3.2 Symboles et abréviations .....                                               | 126 |
| 3.2.1 Symboles et abréviations communs .....                                     | 126 |
| 3.2.2 CPF 8: Symboles et abréviations supplémentaires .....                      | 126 |
| 3.3 Conventions .....                                                            | 127 |
| 4 Présentation générale .....                                                    | 127 |
| 5 Généralités .....                                                              | 127 |
| 6 Services de la couche de communication de sécurité .....                       | 127 |
| 7 Protocole de couche de communication de sécurité .....                         | 127 |
| 8 Gestion de la couche de communication de sécurité .....                        | 128 |
| 9 Exigences système .....                                                        | 128 |
| 10 Évaluation .....                                                              | 128 |
| 11 FSCP 8/1 .....                                                                | 128 |
| 11.1 Domaine d'application – FSCP 8/1 .....                                      | 128 |
| 11.2 Références normatives – FSCP 8/1 .....                                      | 128 |
| 11.3 Termes, définitions, symboles, abréviations et conventions – FSCP 8/1 ..... | 128 |
| 11.4 Aperçu de FSCP 8/1 (CC-Link Safety™) .....                                  | 128 |
| 11.5 Généralités – FSCP 8/1 .....                                                | 129 |
| 11.5.1 Documents externes de spécifications applicables au profil .....          | 129 |
| 11.5.2 Exigences fonctionnelles de sécurité .....                                | 129 |
| 11.5.3 Mesures de sécurité .....                                                 | 129 |
| 11.5.4 Structure de la couche de communication de sécurité .....                 | 131 |
| 11.5.5 Relations avec la FAL (et DLL, PhL) .....                                 | 131 |
| 11.6 Services de la couche de communication de sécurité pour FSCP 8/1 .....      | 132 |
| 11.6.1 Généralités .....                                                         | 132 |
| 11.6.2 SASE .....                                                                | 132 |
| 11.6.3 SAR .....                                                                 | 133 |
| 11.6.4 ASE SAR des données de processus .....                                    | 134 |
| 11.7 Protocole de couche de communication de sécurité pour FSCP 8/1 .....        | 135 |
| 11.7.1 Format PDU de sécurité .....                                              | 135 |
| 11.7.2 Description d'état .....                                                  | 141 |
| 11.8 Gestion de la couche de communication de sécurité pour FSCP 8/1 .....       | 146 |
| 11.8.1 Généralités .....                                                         | 146 |
| 11.8.2 Établissement de connexion et processus de confirmation .....             | 147 |
| 11.8.3 Vérification des esclaves de sécurité .....                               | 147 |
| 11.9 Exigences système pour FSCP 8/1 .....                                       | 148 |

|                        |                                                                                                         |     |
|------------------------|---------------------------------------------------------------------------------------------------------|-----|
| 11.9.1                 | Voyants et commutateurs .....                                                                           | 148 |
| 11.9.2                 | Lignes directrices d'installation.....                                                                  | 149 |
| 11.9.3                 | Temps de réponse de la fonction de sécurité .....                                                       | 149 |
| 11.9.4                 | Durée des sollicitations .....                                                                          | 151 |
| 11.9.5                 | Contraintes liées au calcul des caractéristiques du système.....                                        | 151 |
| 11.9.6                 | Maintenance .....                                                                                       | 153 |
| 11.9.7                 | Manuel de sécurité.....                                                                                 | 153 |
| 11.10                  | Évaluation de FSCP 8/1 .....                                                                            | 154 |
| 12                     | FSCP 8/2 .....                                                                                          | 154 |
| 12.1                   | Domaine d'application – FSCP 8/2.....                                                                   | 154 |
| 12.2                   | Références normatives – FSCP 8/2 .....                                                                  | 154 |
| 12.3                   | Termes, définitions, symboles, abréviations et conventions – FSCP 8/2.....                              | 154 |
| 12.4                   | Présentation de FSCP 8/2 (fonction de communication de sécurité CC-Link IE™).....                       | 154 |
| 12.5                   | Généralités – FSCP 8/2.....                                                                             | 155 |
| 12.5.1                 | Documents externes de spécifications applicables au profil.....                                         | 155 |
| 12.5.2                 | Exigences fonctionnelles de sécurité .....                                                              | 155 |
| 12.5.3                 | Mesures de sécurité.....                                                                                | 155 |
| 12.5.4                 | Structure de la couche de communication de sécurité .....                                               | 161 |
| 12.5.5                 | Relations avec la FAL (et DLL, PhL) .....                                                               | 161 |
| 12.6                   | Services de la couche de communication de sécurité pour FSCP 8/2 .....                                  | 161 |
| 12.6.1                 | Généralités .....                                                                                       | 161 |
| 12.6.2                 | Services de rétablissement de la connexion.....                                                         | 161 |
| 12.6.3                 | Services de transmission de données.....                                                                | 163 |
| 12.6.4                 | Service de notification de fin de connexion .....                                                       | 163 |
| 12.7                   | Protocole de couche de communication de sécurité pour FSCP 8/2.....                                     | 164 |
| 12.7.1                 | Format PDU de sécurité .....                                                                            | 164 |
| 12.7.2                 | Machine de protocole de service FAL de sécurité (SFSPM).....                                            | 170 |
| 12.8                   | Gestion de la couche de communication de sécurité pour FSCP 8/2 .....                                   | 195 |
| 12.8.1                 | Définitions de paramètre .....                                                                          | 195 |
| 12.8.2                 | Configuration de paramètre .....                                                                        | 200 |
| 12.8.3                 | Services de gestion.....                                                                                | 200 |
| 12.9                   | Exigences système pour FSCP 8/2 .....                                                                   | 204 |
| 12.9.1                 | Voyants et commutateurs .....                                                                           | 204 |
| 12.9.2                 | Lignes directrices d'installation.....                                                                  | 206 |
| 12.9.3                 | Temps de réponse de la fonction de sécurité .....                                                       | 206 |
| 12.9.4                 | Durée des sollicitations .....                                                                          | 207 |
| 12.9.5                 | Contraintes liées au calcul des caractéristiques du système.....                                        | 207 |
| 12.9.6                 | Maintenance .....                                                                                       | 209 |
| 12.9.7                 | Manuel de sécurité.....                                                                                 | 210 |
| 12.10                  | Évaluation pour FSCP 8/2 .....                                                                          | 210 |
| Annexe A (informative) | Informations supplémentaires pour les profils de communication de sécurité fonctionnelle de CPF 8 ..... | 211 |
| A.1                    | Calcul de la fonction de hachage pour FSCP 8/1.....                                                     | 211 |
| A.2                    | Calcul de la fonction de hachage pour FSCP 8/2.....                                                     | 211 |
| A.3                    | Signification de la formule de calcul du temps de réponse pour FSCP 8/2 .....                           | 211 |
| Annexe B (informative) | Informations pour l'évaluation des profils de communication de sécurité fonctionnelle de CPF 8.....     | 212 |
| Bibliographie          | .....                                                                                                   | 213 |

|                                                                                                                           |     |
|---------------------------------------------------------------------------------------------------------------------------|-----|
| Figure 1 – Relation entre l'IEC 61784–3 et d'autres normes (machines) .....                                               | 112 |
| Figure 2 – Relation entre l'IEC 61784–3 et d'autres normes (transformation).....                                          | 114 |
| Figure 3 – Relation entre la SCL et les autres couches du Type 18 de l'IEC 61158.....                                     | 132 |
| Figure 4 – Diagramme d'états .....                                                                                        | 142 |
| Figure 5 – Détection d'une répétition non prévue .....                                                                    | 157 |
| Figure 6 – Détection d'une séquence incorrecte .....                                                                      | 157 |
| Figure 7 – Détection d'une perte .....                                                                                    | 158 |
| Figure 8 – Détection d'un retard inacceptable par les horodatages.....                                                    | 159 |
| Figure 9 – Détection d'un retard inacceptable par le temporisateur .....                                                  | 160 |
| Figure 10 – Hiérarchie de protocole.....                                                                                  | 161 |
| Figure 11 – Structure du PDU de sécurité.....                                                                             | 164 |
| Figure 12 – Configuration CTRL .....                                                                                      | 165 |
| Figure 13 – TS du SASE-M et du SASE-S .....                                                                               | 167 |
| Figure 14 – S-Data lors du rafraîchissement de sécurité .....                                                             | 168 |
| Figure 15 – S-Data hors du rafraîchissement de sécurité .....                                                             | 168 |
| Figure 16 – Configuration d'en-tête S-Data.....                                                                           | 169 |
| Figure 17 – Calcul de CRC.....                                                                                            | 170 |
| Figure 18 – Modèles de communication.....                                                                                 | 171 |
| Figure 19 – Diagramme de transition d'état SFSPM.....                                                                     | 172 |
| Figure 20 – Séquence d'établissement d'une connexion .....                                                                | 174 |
| Figure 21 – Séquence de communication lors de la communication de rafraîchissement de sécurité .....                      | 174 |
| Figure 22 – Séquence de mesure et de génération du décalage lors de la communication de rafraîchissement de sécurité..... | 175 |
| Figure 23 – Diagramme de transition d'état SFSPM-M .....                                                                  | 176 |
| Figure 24 – Séquence autre que celle réalisée lors du rafraîchissement de sécurité .....                                  | 179 |
| Figure 25 – S-Connect-req .....                                                                                           | 180 |
| Figure 26 – S-InitConfirmNetPrm-req .....                                                                                 | 180 |
| Figure 27 – net_prm_list .....                                                                                            | 181 |
| Figure 28 – S-InitVerifyStnPrm-req.....                                                                                   | 181 |
| Figure 29 – stn_prm_list .....                                                                                            | 182 |
| Figure 30 – S-InvokeFunc-req .....                                                                                        | 182 |
| Figure 31 – S-WriteErrorInfo-req .....                                                                                    | 183 |
| Figure 32 – date_and_time_of_occurence .....                                                                              | 184 |
| Figure 33 – Diagramme de transition d'état SFSPM-S.....                                                                   | 185 |
| Figure 34 – Séquence autre que celle réalisée lors du rafraîchissement de sécurité .....                                  | 190 |
| Figure 35 – S-Connect-rsp .....                                                                                           | 190 |
| Figure 36 – S-InitConfirmNetPrm-rsp.....                                                                                  | 191 |
| Figure 37 – S-InitVerifyStnPrm-rsp.....                                                                                   | 191 |
| Figure 38 – S-InvokeFunc-rsp .....                                                                                        | 192 |
| Figure 39 – Procédure de calcul du décalage de l'horloge de sécurité.....                                                 | 193 |
| Figure 40 – Relation entre la variation de l'intervalle de transmission et transmission_interval .....                    | 197 |

|                                                                                                   |     |
|---------------------------------------------------------------------------------------------------|-----|
| Figure 41 – Calcul d'allowable_refresh_interval .....                                             | 199 |
| Figure 42 – Calcul d'allowable_delay.....                                                         | 200 |
| Figure 43 – Calcul du temps de réponse entre des PLC de sécurité .....                            | 206 |
| Figure 44 – Relation entre les connexions de sécurité et le taux d'erreurs résiduelles .....      | 209 |
| Figure A.1 – allowable_delay et écart de calcul de décalage.....                                  | 211 |
|                                                                                                   |     |
| Tableau 1 – Sélection des différentes mesures correspondant aux erreurs possibles .....           | 130 |
| Tableau 2 – Format d'attributs de gestionnaire d'appareil de sécurité M1 .....                    | 135 |
| Tableau 3 – Format d'attributs de gestionnaire d'appareil de sécurité S1.....                     | 135 |
| Tableau 4 – Format d'attributs de gestionnaire de connexion de sécurité M1.....                   | 135 |
| Tableau 5 – Format d'attributs de gestionnaire de connexion de sécurité S1 .....                  | 136 |
| Tableau 6 – Format d'attributs de transmission cyclique de sécurité M1 .....                      | 136 |
| Tableau 7 – Format d'attributs de transmission cyclique de sécurité S1 .....                      | 137 |
| Tableau 8 – Codage d'attributs de gestionnaire d'appareil de sécurité M1.....                     | 137 |
| Tableau 9 – Codage d'attributs de gestionnaire d'appareil de sécurité S1 .....                    | 138 |
| Tableau 10 – Codage d'attributs de gestionnaire de connexion de sécurité M1.....                  | 138 |
| Tableau 11 – Codage d'attributs de gestionnaire de connexion de sécurité S1 .....                 | 138 |
| Tableau 12 – Codage d'attributs de transmission cyclique de sécurité M1 .....                     | 139 |
| Tableau 13 – Codage d'attributs de transmission cyclique de sécurité S1.....                      | 140 |
| Tableau 14 – Fonctionnement du temporisateur de contrôle des appareils maîtres de sécurité .....  | 145 |
| Tableau 15 – Fonctionnement du temporisateur de contrôle des appareils esclaves de sécurité ..... | 145 |
| Tableau 16 – Fonctionnement du temporisateur de contrôle des données de sécurité .....            | 145 |
| Tableau 17 – Détails de l'établissement de connexion et du processus de confirmation .....        | 147 |
| Tableau 18 – Détails du processus de vérification des informations sur les esclaves .....         | 147 |
| Tableau 19 – Détails du processus de transmission des paramètres des esclaves de sécurité .....   | 148 |
| Tableau 20 – LED de contrôle .....                                                                | 149 |
| Tableau 21 – Calcul du temps de réponse de la fonction de sécurité.....                           | 150 |
| Tableau 22 – Définitions des termes relatifs au temps de réponse de la fonction de sécurité ..... | 150 |
| Tableau 23 – Nombre de créneaux occupés et données de sécurité.....                               | 152 |
| Tableau 24 – Taux d'erreurs résiduelles $\Lambda$ (créneaux occupés = 1) .....                    | 152 |
| Tableau 25 – Taux d'erreurs résiduelles $\Lambda$ (créneaux occupés = 2) .....                    | 153 |
| Tableau 26 – Sélection des différentes mesures correspondant aux erreurs possibles.....           | 156 |
| Tableau 27 – SS-Start .....                                                                       | 162 |
| Tableau 28 – SS-Restart.....                                                                      | 162 |
| Tableau 29 – SS-InvokeFunc .....                                                                  | 162 |
| Tableau 30 – SS-Read.....                                                                         | 163 |
| Tableau 31 – SS-Write.....                                                                        | 163 |
| Tableau 32 – SS-Terminate .....                                                                   | 164 |
| Tableau 33 – Éléments du PDU de sécurité.....                                                     | 164 |
| Tableau 34 – Éléments de CTRL.....                                                                | 165 |

|                                                                                                                           |     |
|---------------------------------------------------------------------------------------------------------------------------|-----|
| Tableau 35 – Liste des états .....                                                                                        | 172 |
| Tableau 36 – Temporisateurs SFSPM-M .....                                                                                 | 176 |
| Tableau 37 – Table des transitions d'état SFSPM-M .....                                                                   | 176 |
| Tableau 38 – support_functions .....                                                                                      | 180 |
| Tableau 39 – error_category .....                                                                                         | 183 |
| Tableau 40 – error_category correspondant aux erreurs AL .....                                                            | 183 |
| Tableau 41 – error_code .....                                                                                             | 184 |
| Tableau 42 – Temporisateurs SFSPM-S .....                                                                                 | 185 |
| Tableau 43 – Table des transitions d'état SFSPM-S .....                                                                   | 186 |
| Tableau 44 – Paramètres utilisés par la couche de communication de sécurité .....                                         | 196 |
| Tableau 45 – SM-SetSafetyStationInfo .....                                                                                | 201 |
| Tableau 46 – Paramètres de configuration des informations relatives au poste de sécurité de SM-SetSafetyStationInfo ..... | 201 |
| Tableau 47 – SM-SetSafetyNetworkParameter .....                                                                           | 202 |
| Tableau 48 – Paramètres de réseau de sécurité de SM-SetSafetyNetworkParameter .....                                       | 202 |
| Tableau 49 – SM-GetSafetyStationInfo .....                                                                                | 202 |
| Tableau 50 – Paramètres des informations relatives au poste de sécurité de SM-GetSafetyStationInfo (Demande) .....        | 203 |
| Tableau 51 – Paramètres des informations relatives au poste de sécurité de SM-GetSafetyStationInfo (Réponse) .....        | 203 |
| Tableau 52 – SM-GetSafetyNetworkParameter .....                                                                           | 203 |
| Tableau 53 – Paramètres de la demande SM-GetSafetyNetworkParameter .....                                                  | 204 |
| Tableau 54 – Paramètres de la réponse SM-GetSafetyNetworkParameter .....                                                  | 204 |
| Tableau 55 – LED du moniteur .....                                                                                        | 205 |
| Tableau 56 – LED du moniteur de port de communication .....                                                               | 206 |

## 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 Électrotechnique 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. À 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.

La Norme internationale 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.

Cette deuxième édition annule et remplace la première édition, parue en 2010. Cette édition constitue une révision technique. Les modifications techniques majeures par rapport à l'édition précédente sont énumérées ci-dessous.

- FSCP 8/2 ajouté;
- FSCP 8/2, Article 12 ajouté;
- Contenu relatif à FSCP 8/2 ajouté aux Articles 1 à 3 (domaine d'application, références, termes);
- FSCP 8/1 précédent déplacé vers l'Article 11 (rétrogradant tous les anciens en-têtes d'un niveau);

- Anciens Articles 4 à 10 restructurés pour pointer vers les paragraphes appropriés, selon le cas.

Le texte de cette norme est issu des documents suivants:

| FDIS         | Rapport de vote |
|--------------|-----------------|
| 65C/851/FDIS | 65C/854/RVD     |

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

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

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*, peut être consultée sur le site web de l'IEC.

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

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

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

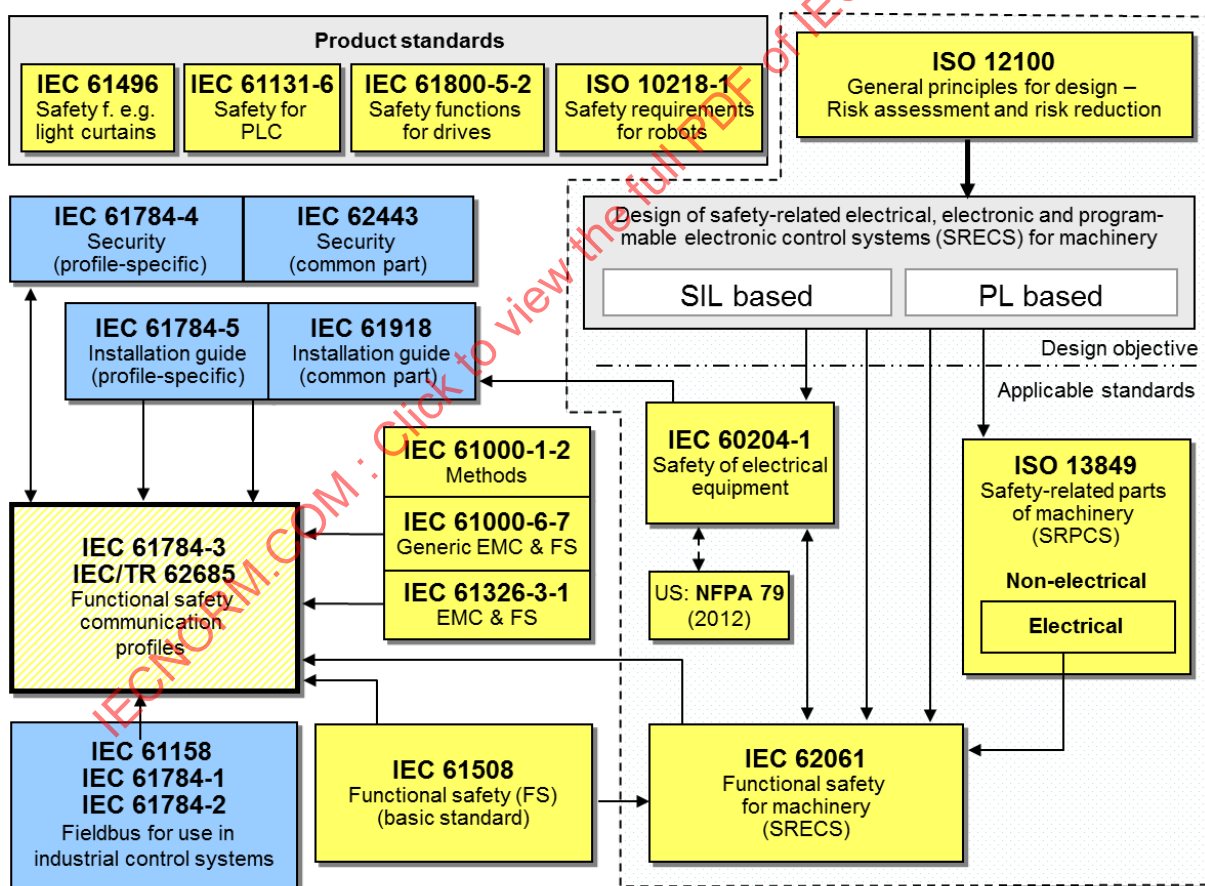
## 0 Introduction

### 0.1 Généralités

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

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

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



IEC

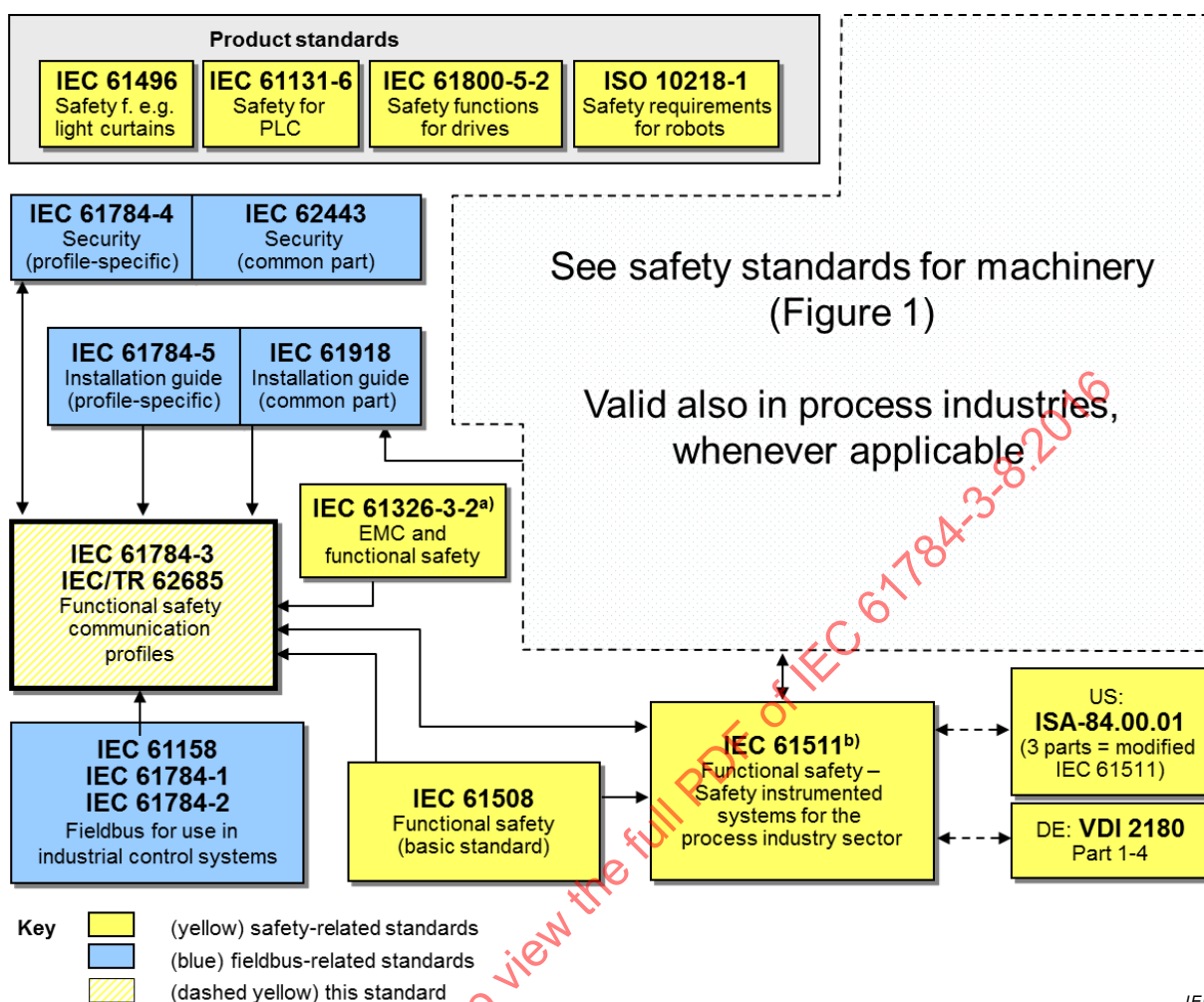
| Anglais                              | Français                                             |
|--------------------------------------|------------------------------------------------------|
| Product standards                    | Normes de produits                                   |
| Safety function, e.g. light curtains | Fonction de sécurité, par exemple rideaux de lumière |

| Anglais                                                                                                           | Français                                                                                                                               |
|-------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| Safety for PLC                                                                                                    | Sécurité relative aux automates programmables                                                                                          |
| Safety functions for drives                                                                                       | Fonctions de sécurité applicables aux entraînements                                                                                    |
| Safety requirements for robots                                                                                    | Exigences de sécurité applicables aux robots                                                                                           |
| General principles for design – Risk assessment and risk reduction                                                | Principes généraux de conception – Appréciation du risque et réduction du risque                                                       |
| Security (profile-specific)                                                                                       | Sûreté (spécifique au profil)                                                                                                          |
| Security (common part)                                                                                            | Sûreté (partie commune)                                                                                                                |
| Design of safety-related electrical, electronic and programmable electronic control systems (SRECS) for machinery | Conception des systèmes de commande électriques, électroniques et électroniques programmables relatifs à la sécurité pour les machines |
| SIL based                                                                                                         | Basé sur SIL                                                                                                                           |
| PL based                                                                                                          | Basé sur PL                                                                                                                            |
| Installation guide (profile-specific)                                                                             | Guide d'installation (spécifique au profil)                                                                                            |
| Installation guide (common part)                                                                                  | Guide d'installation (partie commune)                                                                                                  |
| Design objective                                                                                                  | Objectif de conception                                                                                                                 |
| Applicable standards                                                                                              | Normes applicables                                                                                                                     |
| Methods                                                                                                           | Méthodes                                                                                                                               |
| Generic EMC & FS                                                                                                  | CEM & FS génériques                                                                                                                    |
| EMC & FS                                                                                                          | CEM & FS                                                                                                                               |
| Safety of electrical equipment                                                                                    | Sécurité des équipements électriques                                                                                                   |
| Safety-related parts of machinery (SRPCS)                                                                         | Sécurité des machines – Parties des systèmes de commande relatives à la sécurité                                                       |
| Non-electrical                                                                                                    | Non électrique                                                                                                                         |
| Electrical                                                                                                        | Électrique                                                                                                                             |
| Functional safety communication profiles                                                                          | Profil de communication de sécurité fonctionnelle                                                                                      |
| Fieldbus for use in industrial control systems                                                                    | Bus de terrain pour utilisation dans des systèmes de commande industriels                                                              |
| Functional safety (FS) (basic standard)                                                                           | Sécurité fonctionnelle (FS) (norme de base)                                                                                            |
| Functional safety for machinery (SRECS)                                                                           | Sécurité fonctionnelle des machines                                                                                                    |
| Key                                                                                                               | Légende                                                                                                                                |
| (yellow) safety-related standards                                                                                 | (jaune) normes relatives à la sécurité                                                                                                 |
| (blue) fieldbus-related standards                                                                                 | (bleu) normes relatives au bus de terrain                                                                                              |
| (dashed yellow) this standard                                                                                     | (jaune pointillé) la présente norme                                                                                                    |

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

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

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



| Anglais                                                                       | Français                                                                                                    |
|-------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|
| Product standards                                                             | Normes de produits                                                                                          |
| Safety function, e.g. light curtains                                          | Fonction de sécurité, par exemple rideaux de lumière                                                        |
| Safety for PLC                                                                | Sécurité relative aux automates programmables                                                               |
| Safety functions for drives                                                   | Fonctions de sécurité applicables aux entraînements                                                         |
| Safety requirements for robots                                                | Exigences de sécurité applicables aux robots                                                                |
| Security (profile-specific)                                                   | Sûreté (spécifique au profil)                                                                               |
| Security (common part)                                                        | Sûreté (partie commune)                                                                                     |
| Installation guide (profile-specific)                                         | Guide d'installation (spécifique au profil)                                                                 |
| Installation guide (common part)                                              | Guide d'installation (partie commune)                                                                       |
| See safety standards for machinery (Figure 1)                                 | Voir normes de sécurité pour les machines (Figure 1)                                                        |
| Valid also in process industries, whenever applicable                         | Valable également dans les industries de transformation, le cas échéant                                     |
| Functional safety communication profiles                                      | Profils de communication de sécurité fonctionnelle                                                          |
| EMC and functional safety                                                     | CEM et sécurité fonctionnelle                                                                               |
| Fieldbus for use in industrial control systems                                | Bus de terrain pour utilisation dans des systèmes de commande industriels                                   |
| Functional safety (basic standard)                                            | Sécurité fonctionnelle (norme de base)                                                                      |
| Functional safety–safety instrumented systems for the process industry sector | Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur des industries de transformation |
| 3 parts = modified IEC 61511                                                  | 3 parties = IEC 61511 modifiée                                                                              |

| Anglais                           | Français                                  |
|-----------------------------------|-------------------------------------------|
| Part 1 –4                         | Parties 1 à 4                             |
| Key                               | Légende                                   |
| (yellow) safety-related standards | (jaune) normes relatives à la sécurité    |
| (blue) fieldbus-related standards | (bleu) normes relatives au bus de terrain |
| (dashed yellow) this standard     | (jaune pointillé) la présente norme       |

- a Pour des environnements électromagnétiques spécifiés, sinon IEC 61326-3-1 ou IEC 61000-6-7.
- b EN ratifiée.

## Figure 2 – Relation 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 la série IEC 61508, assurent la confiance nécessaire à accorder à la transmission de messages (information) entre deux participants ou plus sur un bus de terrain dans un système relatif à la sécurité, ou une fiabilité suffisante dans le comportement de sécurité en cas d'erreurs ou de défaillances du bus de terrain.

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

La revendication du SIL qui en résulte pour un système dépend de la mise en œuvre du profil de communication de sécurité fonctionnelle (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.

La présente norme décrit:

- les principes de base de mise en œuvre des exigences de la série IEC 61508 pour les communications de données relatives à la sécurité, y compris les défauts de transmission potentiels, les mesures correctives et les considérations concernant l'intégrité des données,
- 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 la série IEC 61158.

## 0.2 Déclaration de droits de propriété

La Commission Électrotechnique Internationale (IEC) attire l'attention sur le fait qu'il est déclaré que la conformité aux dispositions du présent document peut impliquer l'utilisation d'un brevet intéressant le FSCP 8/2 traité à l'Article 12, comme suit:

|                                                                                                |       |                                                               |
|------------------------------------------------------------------------------------------------|-------|---------------------------------------------------------------|
| JP 2012-533784<br>US 13/821733<br>DE 112010005881.4<br>KR 10-2013-7006469<br>CN 201080069108.6 | [MEC] | Appareil de communication et méthode de détection des retards |
|------------------------------------------------------------------------------------------------|-------|---------------------------------------------------------------|

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, gratuitement ou à des termes et

conditions raisonnables et non discriminatoires. À ce propos, la déclaration du détenteur des droits de propriété est enregistrée à l'IEC. Des informations peuvent être demandées à:

|       |                                                                                                                         |
|-------|-------------------------------------------------------------------------------------------------------------------------|
| [MEC] | Mitsubishi Electric Corporation<br>Corporate Licensing Division<br>2-7-3 Marunouchi, Chiyoda-ku<br>Tokyo 100-8310 Japon |
|-------|-------------------------------------------------------------------------------------------------------------------------|

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 intellectuelle autres que ceux identifiés ci-dessus. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et de ne pas avoir signalé leur existence.

L'ISO ([www.iso.org/patents](http://www.iso.org/patents)) et l'IEC (<http://patents.iec.ch>) maintiennent à disposition des bases de données en ligne des brevets relatifs à leurs normes. Les utilisateurs sont invités à les consulter pour obtenir les dernières informations relatives à ces brevets.

IECNORM.COM : Click to view the full PDF of IEC 61784-3-8:2016

## 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 la série IEC 61784-3 spécifie une couche de communication de sécurité (services et protocole) reposant sur 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 en matière de communications de sécurité fonctionnelle définies dans l'IEC 61784-3 pertinents pour 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.

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

La présente partie fournit des lignes directrices tant pour les développeurs que pour les évaluateurs d'appareils et systèmes conformes.

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

#### 2 Références normatives

Les documents suivants sont cités en référence de manière normative, en intégralité ou en partie, dans le présent document et sont indispensables pour son application. 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 60204-1, *Sécurité des machines – Équipement électrique des machines – Partie 1: Règles générales*

IEC 61131-2:2007, *Automates programmables – Partie 2: Exigences et essais des équipements*

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

<sup>1</sup> Dans les pages suivantes de la présente norme, "la présente partie" se substitue à "cette partie de la série IEC 61784-3".

<sup>2</sup> Dans les pages suivantes de la présente norme, "IEC 61508" se substitue à "série IEC 61508".

IEC 61158-2, *Réseaux de communication 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 la couche liaison de données – Éléments de Type 18*

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

IEC 61158-5-18, *Industrial communication networks – Fieldbus specifications – Part 5-18: Application layer service definition – Type 18 elements* (disponible en anglais seulement)

IEC 61158-5-23, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 5-23: Définition des services de la couche application – Éléments de type 23*

IEC 61158-6-18, *Industrial communication networks – Fieldbus specifications – Part 6-18: Application layer protocol specification – Type 18 elements* (disponible en anglais seulement)

IEC 61158-6-23, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 6-23: Spécification du protocole de la couche application – Éléments 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 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 basés sur l'ISO/CEI 8802-3*

IEC 61784-3: —<sup>3</sup>, *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*

IEEE 802.3, *IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method And Physical Layer Specifications*

<sup>3</sup> A publier.

### 3 Termes, définitions, symboles, abréviations et conventions

#### 3.1 Termes et définitions

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

NOTE Les définitions des termes eux-mêmes définis à l'article 3.1 sont marquées en italique.

##### 3.1.1 Termes et définitions communs

NOTE Ces termes et définitions communs proviennent de l'IEC 61784-3:—.

###### 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 utilisant d'appareils et de bus de terrain]

###### 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 61918:2013, 3.1.2]

###### 3.1.1.3

###### **disponibilité**

probabilité, pour un système automatisé, qu'il ne se produise pas de condition opérationnelle non satisfaisante, par exemple la perte de production, pendant une période donnée

###### 3.1.1.4

###### **probabilité d'erreurs sur les éléments binaires**

$P_e$

probabilité de réception d'un bit donné avec la valeur incorrecte

###### 3.1.1.5

###### **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.

###### 3.1.1.6

###### **pont**

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

###### 3.1.1.7

###### **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 considéré comme négligeable

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

**3.1.1.8****canal de communication**

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

**3.1.1.9****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

**3.1.1.10****connexion**

liaison logique entre objets applicatifs au sein du même appareil ou d'appareils différents

**3.1.1.11****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 la présente norme pour se référer aux données redondantes.

Note 2 à l'article: Voir également [29], [30]<sup>4</sup>.

**3.1.1.12****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 tolérable conformément au modèle de cycle de vie de l'IEC 62443, en utilisant par exemple des zones et des conduits

**3.1.1.13****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]

**3.1.1.14****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]

<sup>4</sup> Les chiffres entre crochets font référence à la bibliographie.

### 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 de capacité 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'incapacité à accomplir une fonction requise, en excluant l'incapacité 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* basé 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

#### **DLPDU**

DÉCONSEILLÉ: trame

Data Link Protocol Data Unit (Unité de données de protocole de liaison de données)

### 3.1.1.20

#### **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 [29], [30].

Note 3 à l'article: L'abréviation «FCS» est dérivée du terme anglais développé correspondant "Frame Check Sequence".

### 3.1.1.21

#### **fonction de hachage**

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

Note 1 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.

[SOURCE: IEC TR 62210:2003, 4.1.12, modifié – ajout de "habituellement" et de notes]

**3.1.1.22****danger**

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

**3.1.1.23****maître**

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

**3.1.1.24****message**

série ordonnée d'octets, destinée à véhiculer des informations

[SOURCE: ISO/IEC 2382-16:1996, 16.02.01, modifié – caractère remplacé par octet]

**3.1.1.25****collecteur de messages**

partie d'un *système de communication* destiné à recevoir des *messages*

[SOURCE: ISO/IEC 2382-16:1996, 16.02.03]

**3.1.1.26****source de messages**

partie d'un *système de communication* destiné à envoyer des *messages*

[SOURCE: ISO/IEC 2382-16:1996, 16.02.02]

**3.1.1.27****déclenchement de nuisance**

déclenchement parasite sans effet préjudiciable

Note 1 à l'article: Les erreurs anormales internes peuvent être générées dans des systèmes de communication, par exemple des systèmes de transmission par ondes radioélectriques, du fait d'un trop grand nombre de nouvelles tentatives en présence de perturbations.

**3.1.1.28****niveau de performance**

PL

niveau discret utilisé pour spécifier la capacité des parties relatives à la sécurité des systèmes de commande à accomplir une fonction de sécurité dans des conditions prévisibles

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

[SOURCE: ISO 13849-1:2006, 3.1.23, traduction française modifiée – amélioration]

**3.1.1.29****très basse tension de protection**

TBTP

circuit électrique dans lequel la tension ne peut pas dépasser 30 V eff. c.a., 42,4 V crête ou 60 V c.c. en conditions normales et en conditions de défaut isolé, sauf en conditions de défauts de terre dans d'autres circuits

Note 1 à l'article: Un circuit TBTP comprend un raccordement à un conducteur de protection. En l'absence de raccordement à un conducteur de protection, ou si une défaillance existe au niveau du raccordement, les tensions ne sont pas corrigées.

[SOURCE: IEC 61010-2-201:2013, 3.109, modifié – suppression de "circuit" dans le terme, et suppression de la seconde note à l'article]

**3.1.1.30**  
**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]

**3.1.1.31**  
**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]

**3.1.1.32**  
**fiabilité**

probabilité pour qu'un système automatisé puisse accomplir une fonction requise, dans des conditions données, pendant un intervalle de temps donné ( $t_1$ ,  $t_2$ )

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

Note 2 à l'article: Le terme "fiabilité" est aussi employé pour désigner l'aptitude caractérisée par cette probabilité.

Note 3 à l'article: Au cours de la période MTBF ou MTTF, la probabilité qu'un système automatisé exécute une fonction exigée dans les conditions données décroît.

Note 4 à l'article: La fiabilité diffère de la disponibilité.

[SOURCE: IEC TR 62059-11:2002, 3.17, modifié – utilisation des mots "un système automatisé" à la place de "une entité" et ajout de deux notes]

**3.1.1.33**  
**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».

**3.1.1.34**  
**taux d'erreurs résiduelles**

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

**3.1.1.35**  
**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 l'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, modifiés – note différente]

**3.1.1.36**  
**canal de communication de sécurité**

canal de communication qui débute 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.

**3.1.1.37****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

Note 1 à l'article: L'abréviation «SCL» est dérivée du terme anglais développé correspondant «safety communication layer».

**3.1.1.38****connexion de sécurité**

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

**3.1.1.39****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 ne garantit pas la sécurité des données proprement dites, mais uniquement la transmission en toute sécurité de ces dernières.

**3.1.1.40****appareil de sécurité**

appareil conçu conformément à l'IEC 61508 et qui met en œuvre le profil de communication de sécurité fonctionnelle

**3.1.1.41****très basse tension de sécurité**

TBTS

circuit électrique dans lequel la tension ne peut pas dépasser 30 V eff. c.a., 42,4 V crête ou 60 V c.c. en conditions normales et en conditions de défaut isolé, y compris en conditions de défauts de terre dans d'autres circuits

[SOURCE: IEC 61010-2-201:2013, 3.110, suppression de "circuit" dans le terme, et suppression de la note à l'article]

**3.1.1.42****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]

**3.1.1.43****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 que ne soit atteint 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:—, 5.2.4, est traité dans le cadre des profils de communication de sécurité fonctionnelle définis dans la présente partie.

**3.1.1.44****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 SIL *n*" (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, modifié — ajout de la Note 4]

### 3.1.1.45

#### **mesure de sécurité**

mesure permettant 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 détaillées dans l'IEC 61784-3:—, 5.3 et 5.4.

### 3.1.1.46

#### **PDU de sécurité**

##### **SPDU**

PDU transféré via 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 d'horodatage.

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 protocol data unit».

### 3.1.1.47

#### **application relative à la sécurité**

programmes conçus conformément à l'IEC 61508 pour satisfaire aux exigences SIL de l'application

### 3.1.1.48

#### **système relatif à la sécurité**

système qui exécute les *fonctions de sécurité* conformément à l'IEC 61508

### 3.1.1.49

#### **esclave**

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

### 3.1.1.50

#### **déclenchement parasite**

déclenchement provoqué par le système de sécurité sans injonction du processus

### 3.1.1.51

#### **horodatage**

information temporelle incluse dans un *message*

**3.1.1.52****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.

**3.1.1.53****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

Note 1 à l'article: L'abréviation «SAR» est dérivée du terme anglais développé correspondant "safety application relationship".

**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) permettant 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

|        |                                                                                                   |                    |
|--------|---------------------------------------------------------------------------------------------------|--------------------|
| CP     | Communication Profile (Profil de communication)                                                   | [IEC 61784-1]      |
| CPF    | Communication Profile Family (Famille de profils de communication)                                | [IEC 61784-1]      |
| CRC    | Cyclic Redundancy Check (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 (Équipement commandé)                                                     | [IEC 61508-4:2010] |
| E/E/PE | Electrical/Electronic/Programmable Electronic (Électrique/électronique/électronique programmable) | [IEC 61508-4:2010] |
| FAL    | Fieldbus Application Layer (Couche application de bus de terrain)                                 | [IEC 61158-5]      |
| 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     | Bit error probability (Probabilité d'erreurs sur les éléments binaires)                           |                    |
| TBTP   | Très basse tension de protection                                                                  |                    |
| 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)                                  |                    |
| TBTS   | Très basse tension de sécurité                                                                    |                    |
| SIL    | Safety Integrity Level (Niveau d'intégrité de sécurité)                                           | [IEC 61508-4:2010] |
| SPDU   | Safety PDU (PDU de sécurité)                                                                      |                    |

### 3.2.2 CPF 8: Symboles et abréviations supplémentaires

|     |                                                                |
|-----|----------------------------------------------------------------|
| AR  | Application Relationship (Relation d'application)              |
| ASE | Application Service Element (Élément de service d'application) |

|       |                                                                                                                                 |
|-------|---------------------------------------------------------------------------------------------------------------------------------|
| CID   | Connection Identifier (Identifiant de connexion)                                                                                |
| CMD   | Command Data (Données de commande)                                                                                              |
| LED   | Light Emitting Diode (Diode Electroluminescente)                                                                                |
| LID   | Link Identifier (Identifiant de liaison)                                                                                        |
| OBL   | Offset Base Line (Ligne de base décalée)                                                                                        |
| PSD   | Protocol Support Data (Données de soutien au protocole)                                                                         |
| 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 (Élément de service d'application de sécurité)                                               |
| SFSPM | Safety FSPM (appended with -S Slave or -M Master) (FSPM de sécurité [suivi d'un -S pour Esclave 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 | Safety Transmission Packet Information from master (Informations de paquets de transmission de sécurité fournies par le maître) |
| TPI-R | Safety Transmission Packet Information from slave (Informations de paquets de transmission de sécurité fournies par l'esclave)  |
| TS    | Time Stamp (Datation [horodatage])                                                                                              |

### 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 avec 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 FSCP 8/1, voir 11.4. Pour FSCP 8/2, voir 12.4.

## 5 Généralités

Pour FSCP 8/1, voir 11.5. Pour FSCP 8/2, voir 12.5.

## 6 Services de la couche de communication de sécurité

Pour FSCP 8/1, voir 11.6. Pour FSCP 8/2, voir 12.6.

## 7 Protocole de couche de communication de sécurité

Pour FSCP 8/1, voir 11.7. Pour FSCP 8/2, voir 12.7.

## 8 Gestion de la couche de communication de sécurité

Pour FSCP 8/1, voir 11.8. Pour FSCP 8/2, voir 12.8.

## 9 Exigences système

Pour FSCP 8/1, voir 11.9. Pour FSCP 8/2, voir 12.9.

## 10 Évaluation

Pour FSCP 8/1, voir 11.10. Pour FSCP 8/2, voir 12.10.

## 11 FSCP 8/1

### 11.1 Domaine d'application – FSCP 8/1

Voir l'Article 1

### 11.2 Références normatives – FSCP 8/1

Voir l'Article 2.

### 11.3 Termes, définitions, symboles, abréviations et conventions – FSCP 8/1

Voir l'Article 3.

### 11.4 Aperçu de FSCP 8/1 (CC-Link Safety™)

La Famille de profils de communication 8 (souvent appelée CC-Link™<sup>5</sup>) définit les profils de communication reposant 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™<sup>5</sup>) repose sur les profils de base CPF 8 de l'IEC 61784-1 et les spécifications de couche de communication de sécurité définies dans la présente partie.

Le FSCP 8/1 est un protocole de communication des données relatives à la sécurité tel 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 peut être utilisé dans diverses 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.

---

<sup>5</sup> CC-Link™ et CC-Link Safety™ désignent les appellations commerciales de l'organisme sans but lucratif CC-Link Partner Association. Ces informations sont données pour des raisons de commodité des utilisateurs de la présente norme internationale et ne constituent en aucun cas un entérinement par l'IEC du titulaire de la marque ou de l'un de ses produits. La conformité à la présente norme n'exige pas l'emploi des appellations CC-Link™ ou CC-Link Safety™. L'emploi des appellations CC-Link™ ou CC-Link Safety™ exige l'autorisation de la CC-Link Partner Association et la conformité aux conditions d'utilisation (essais et validation).

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 la présente partie. 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 [34], [35] et [36] qui donnent des spécifications supplémentaires relatives à la mise en œuvre de la SCL définie dans la présente partie.

### **11.5.2 Exigences fonctionnelles de sécurité**

La présente norme spécifie les services et protocoles d'un système de communication de sécurité fonctionnelle reposant sur le Type 18 de l'IEC 61158. Les technologies de communication spécifiées dans la présente norme 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 la présente partie, 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 la présente norme 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 (CRC 32);
- différents systèmes d'assurance d'intégrité des données.

La sélection des différentes mesures correspondant aux erreurs possibles est présentée au Tableau 1.

**Tableau 1 – Sélection des différentes mesures correspondant 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                                 |                                     |                                                         |
| Répétition non prévue                    | X                                 |                       |       |                               |                     |                                   |                                     |                                                         |
| Séquence incorrecte                      | X                                 |                       |       |                               |                     |                                   |                                     |                                                         |
| Perte                                    | X                                 |                       |       |                               |                     |                                   |                                     |                                                         |
| Retard inacceptable                      |                                   |                       | X     |                               |                     |                                   |                                     |                                                         |
| Insertion                                | X                                 |                       |       | X                             | X                   |                                   |                                     |                                                         |
| Déguisement                              |                                   |                       |       | 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 4 bits et une séquence spécifiée (voir 11.7.1 et 11.7.2). 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 intégré indiquant 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(s) canal(aux) de sortie correspondant(s) de l'(des) esclave(s) de sortie de sécurité, hors temps de traitement de l'entrée de sécurité. Pour plus de détails, 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, de l'ID de commande et du champ de données de soutien au protocole.

#### 11.5.3.6 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 message transmis contient un champ de données de soutien au protocole de 16 bits, un ID de commande de 8 bits, un ID de liaison de 3 bits et un RNO de 4 bits.

#### 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:

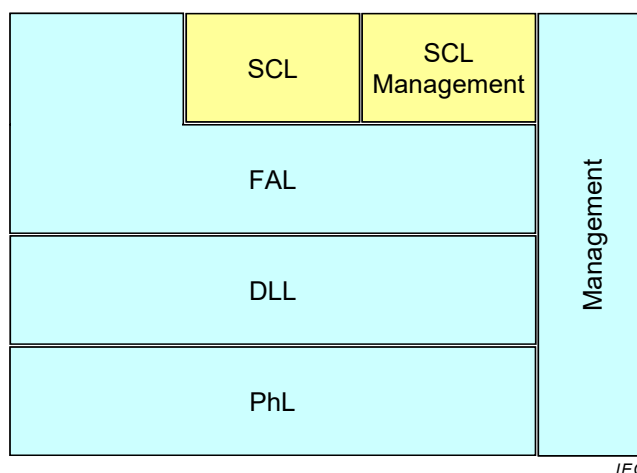
- gestionnaire d'appareil de sécurité de types M1 et S1;
- gestionnaire de connexion de sécurité de types M1 et S1;
- transmission cyclique de sécurité de types M1 et S1;

L'ensemble des gestions, comportements et fonctions de la SCL est traité 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

La Figure 3 représente la relation entre la SCL et les autres couches de la pile de communication du Type 18 de l'IEC 61158.



| Anglais        | Français    |
|----------------|-------------|
| SCL Management | Gestion SCL |
| Management     | Gestion     |

**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                                             |
| CLASS:        | gestionnaire d'appareil de sécurité M1                      |
| CLASS ID:     | non utilisé                                                 |
| PARENT CLASS: | gestionnaire d'appareil M1                                  |
| ATTRIBUTES:   |                                                             |
| 1             | (m) Attribut: Information de gestion                        |
| 1.1           | (m) Attribut: Id de liaison                                 |
| 1.2           | (o) Attribut: Version de logiciel/protocole                 |
| 2             | (m) Attribut: Information 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                        |
| CLASS:        |     |           | gestionnaire d'appareil de sécurité S1 |
| CLASS ID:     |     |           | non utilisé                            |
| PARENT CLASS: |     |           | gestionnaire d'appareil S1             |
| ATTRIBUTES:   |     |           |                                        |
| 1             | (m) | Attribut: | Information 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                                                   |
| CLASS:        |     |           | Gestionnaire de connexion de sécurité M1                          |
| CLASS ID:     |     |           | non utilisé                                                       |
| PARENT CLASS: |     |           | Gestionnaire de connexion M1                                      |
| ATTRIBUTES:   |     |           |                                                                   |
| 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: | État 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                                          |
| CLASS:        |     |           | Gestionnaire de connexion de sécurité S1                 |
| CLASS ID:     |     |           | non utilisé                                              |
| PARENT CLASS: |     |           | Gestionnaire de connexion S1                             |
| ATTRIBUTES:   |     |           |                                                          |
| 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     |                                   |
| CLASS:        |     | Transmission cyclique de sécurité M1 |                                   |
| CLASS ID:     |     | non utilisé                          |                                   |
| PARENT CLASS: |     | Transmission cyclique M1             |                                   |
| ATTRIBUTES:   |     |                                      |                                   |
| 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                 |
| 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 RWw 1                     |
| 2.1.2.1       | (m) | Attribut:                            | Données RWr de sécurité 1         |
| 2.1.2.2       | (m) | Attribut:                            | TPI-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     |
| CLASS:        |     |           | Transmission cyclique de sécurité S1 |
| CLASS ID:     |     |           | non utilisé                          |
| PARENT CLASS: |     |           | Transmission cyclique S1             |
| ATTRIBUTES:   |     |           |                                      |
| 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                    |
| 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                    |

## 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 en termes de syntaxe abstraite et de 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 appartenant à cette classe est décrite au Tableau 2.

**Tableau 2 – Format d'attributs de gestionnaire d'appareil de sécurité M1**

| Attribut                                      | Format                   | Taille (bits) |
|-----------------------------------------------|--------------------------|---------------|
| Information de gestion                        | Structure de 2 éléments: | 11            |
| Id de liaison                                 | Unsigned3                | 3             |
| Version de logiciel/protocole                 | 1 octet, en mode points  | 8             |
| Information de gestion des esclaves connectés | Matrice de 64 membres    | 64 octets     |
| Version de logiciel/protocole                 | 1 octet, en mode points  | 8             |

##### 11.7.1.2.2 Syntaxe abstraite PDU de gestionnaire d'appareil de sécurité S1

La syntaxe abstraite applicable aux attributs appartenant à cette classe est décrite au Tableau 3.

**Tableau 3 – Format d'attributs de gestionnaire d'appareil de sécurité S1**

| Attribut                      | Format                   | Taille (bits) |
|-------------------------------|--------------------------|---------------|
| Information de gestion        | Structure de 3 éléments: | 11            |
| Id de liaison                 | Unsigned3                | 3             |
| Version de logiciel/protocole | 1 octet, en mode points  | 8             |

##### 11.7.1.2.3 Syntaxe abstraite PDU de gestionnaire de connexion de sécurité M1

La syntaxe abstraite applicable aux attributs appartenant à cette classe est décrite au 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 points | 64            |
| Source de spécification relative aux esclaves de sécurité         | 8 octets, en mode points | 64            |
| Informations sur les produits concernant les esclaves de sécurité | Matrice de 64 membres    | 1 984 octets  |

| 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 – 52 224 octets           | 16 – 52 224 octets |
| État de liaison des esclaves de sécurité                 | 8 octets, en mode points     | 64                 |

#### 11.7.1.2.4 Syntaxe abstraite PDU de gestionnaire de connexion de sécurité S1

La syntaxe abstraite applicable aux attributs appartenant à cette classe est décrite au 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 appartenant à cette classe est décrite au Tableau 6.

**Tableau 6 – Format d'attributs de transmission cyclique de sécurité M1**

| Attribut                          | Format                                              | Taille (bits)         |
|-----------------------------------|-----------------------------------------------------|-----------------------|
| Données de sortie                 | Structure de 2 éléments:                            | $96 \times n$         |
| Données RY de sécurité            | Structure de données orientées sur les bits         | $32 \times n$         |
| Données RWw                       | Structure de données par mot                        | $64 \times n$         |
| Données RWw de sécurité           | Données par mot                                     | $64 \times (n - m)$   |
| TPI-T de sécurité                 | Informations de paquets de transmission de sécurité | $64 \times m$         |
| Données d'entrée                  | Structure de n éléments:                            | $96 \times n$         |
| Données de sécurité en 1          | Structure de 2 éléments:                            | $96 \times p_1$       |
| Données RX de sécurité            | Structure de données orientées sur les bits         | $32 \times p_1$       |
| Données RWr                       | Structure de données par mot                        | $64 \times p_1$       |
| Données RWr de sécurité           | Données par mot                                     | $64 \times (p_1 - 1)$ |
| TPI-R de sécurité                 | Informations de paquets de transmission de sécurité | 64                    |
| ...                               | ...                                                 | ...                   |
| Données de sécurité d'entrée en n | Structure de 2 éléments:                            | $96 \times p_n$       |

NOTE Les valeurs de n et de m dépendent des valeurs des paramètres de configuration correspondants dans l'état du maître. La valeur de p dépend du nombre de créneaux occupés par le poste esclave.

#### 11.7.1.2.6 Syntaxe abstraite PDU de transmission cyclique de sécurité S1

La syntaxe abstraite applicable aux attributs appartenant à cette classe est décrite au Tableau 7.

**Tableau 7 – Format d'attributs de transmission cyclique de sécurité S1**

| Attribut                                                                       | Format                                              | Taille (bits)       |
|--------------------------------------------------------------------------------|-----------------------------------------------------|---------------------|
| Données de sortie                                                              | Structure de 2 éléments:                            | $96 \times p$       |
| Données RY de sécurité                                                         | Structure de données orientées sur les bits         | $32 \times p$       |
| Données RWw                                                                    | Structure de données par mot                        | $64 \times p$       |
| Données RWw de sécurité                                                        | Données par mot                                     | $64 \times (p - 1)$ |
| TPI-T de sécurité                                                              | Informations de paquets de transmission de sécurité | 64                  |
| Données d'entrée                                                               | Structure de 2 éléments:                            | $96 \times p$       |
| Données RX de sécurité                                                         | Structure de données orientées sur les bits         | $32 \times p$       |
| Données RWr                                                                    | Structure de données par mot                        | $64 \times p$       |
| Données RWr de sécurité                                                        | Données par mot                                     | $64 \times (p - 1)$ |
| TPI-R de sécurité                                                              | Informations de paquets de transmission de sécurité | 64                  |
| NOTE La valeur de p dépend du nombre de créneaux occupés par le poste esclave. |                                                     |                     |

**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 appartenant à cette classe est décrit au Tableau 8.

**Tableau 8 – Codage d'attributs de gestionnaire d'appareil de sécurité M1**

| Attribut                                      | Codage                                                        |                      |                                                                  |
|-----------------------------------------------|---------------------------------------------------------------|----------------------|------------------------------------------------------------------|
| Information 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<br>1 = Version 2<br>2 = Version 3<br>3 = Version 4 |
| Information 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<br>1 = Version 2<br>2 = Version 3<br>3 = Version 4 |

**11.7.1.3.2 Codage PDU de gestionnaire d'appareil de sécurité S1**

Le codage PDU spécifique applicable aux attributs appartenant à cette classe est décrit au Tableau 9.

**Tableau 9 – Codage d'attributs de gestionnaire d'appareil de sécurité S1**

| Attribut                      | Codage                                         |                      |                                                                  |
|-------------------------------|------------------------------------------------|----------------------|------------------------------------------------------------------|
| Information 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<br>1 = Version 2<br>2 = Version 3<br>3 = Version 4 |

#### 11.7.1.3.3 Codage PDU de gestionnaire de connexion de sécurité M1

Le codage PDU spécifique applicable aux attributs appartenant à cette classe est décrit au 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:<br>0 = SCL non prise en charge<br>1 = SCL prise en charge                                                               |
| Source de spécification relative aux esclaves de sécurité   | Les Bits 0 – 63 correspondent aux créneaux 1 – 64, où:<br>0 = spécification de l'utilisateur SCL non prise en charge<br>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 pour les données correspondant aux informations sur les produits de sécurité                                                                                         |
| Données de paramètres de sécurité                           | 0 – 52 224 octets de données pour l'accès à la mémoire esclave                                                                                                                 |
| État de liaison des esclaves de sécurité                    | Les Bits 0 – 63 correspondent aux créneaux 1 – 64, où:<br>0 = Poste esclave de sécurité hors fonctionnement<br>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 appartenant à cette classe est décrit au 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 appartenant à cette classe est décrit au Tableau 12.

**Tableau 12 – Codage d'attributs de transmission cyclique de sécurité M1**

| Attribut                     | Codage                                                                                                                                                                                                                                                                                    |        |                                                                  |                                          |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|------------------------------------------------------------------|------------------------------------------|
| Données de sortie            | Registres de données de processus réglés par le maître pour la sortie de l'appareil esclave                                                                                                                                                                                               |        |                                                                  |                                          |
| Données RY de sécurité       | Champ à mapping positionnel de données de sortie orientées sur les bits pour tous les appareils esclaves connectés ordonnés par créneau avec 32 bits par créneau                                                                                                                          |        |                                                                  |                                          |
| Données RWw                  | Champ à mapping positionnel dans lequel sont mises en correspondance 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      |        |                                                                  |                                          |
| Données RWw de sécurité      | 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 |        |                                                                  |                                          |
| TPI-T de sécurité            | Octet                                                                                                                                                                                                                                                                                     | Bit    | Description                                                      | Valeurs                                  |
|                              | 0 – 1                                                                                                                                                                                                                                                                                     | –      | Données de soutien au protocole (PSD) utilisé par la gestion SCL | 0 – 65 535                               |
|                              | 2 – 3                                                                                                                                                                                                                                                                                     | 0 – 3  | Numéro d'exécution                                               | 0 – 15                                   |
|                              |                                                                                                                                                                                                                                                                                           | 4 – 6  | Id de liaison                                                    | 0 – 7                                    |
|                              |                                                                                                                                                                                                                                                                                           | 7      | réservé                                                          | 0                                        |
|                              |                                                                                                                                                                                                                                                                                           | 8 – 11 | Type de données de transmission                                  | 0 – 15                                   |
|                              |                                                                                                                                                                                                                                                                                           | 12     | Drapeau occupé                                                   | 0 = occupé<br>1 = non occupé             |
|                              |                                                                                                                                                                                                                                                                                           | 13     | réservé                                                          | 0                                        |
|                              |                                                                                                                                                                                                                                                                                           | 14     | Demande de lecture                                               | 0 = pas de demande<br>1 = demande        |
|                              |                                                                                                                                                                                                                                                                                           | 15     | mode d'application de l'utilisateur SCL                          | 0 = mode d'essai<br>1 = mode de sécurité |
|                              | 4 – 7                                                                                                                                                                                                                                                                                     | –      | CRC32                                                            | CRC32                                    |
| Données d'entrée             | Registres de données de processus lus par le maître représentant les entrées de l'appareil esclave                                                                                                                                                                                        |        |                                                                  |                                          |
| Données de sécurité d'entrée | Registres de données de processus lus par le maître représentant les entrées de l'appareil esclave de sécurité                                                                                                                                                                            |        |                                                                  |                                          |
| Données RX de sécurité       | Champ contenant les données d'entrée orientées sur les bits à partir de l'appareil esclave n ordonné par créneau avec 32 bits par créneau. Le nombre de créneaux occupés par l'appareil esclave détermine la longueur totale de ce champ                                                  |        |                                                                  |                                          |
| Données RWr                  | Champ contenant les données d'entrée orientées part mot à partir de l'appareil esclave n ordonné par créneau avec 4 mots par créneau. Le nombre de créneaux occupés par l'appareil esclave détermine la longueur totale de ce champ                                                       |        |                                                                  |                                          |

| Attribut                | Codage                                                                                                                                                                                                                                                                         |                                                                  |                                          |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------|------------------------------------------|
| Données RWr de sécurité | Champ à mapping positionnel des données d'entrée par mot à partir de 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 |                                                                  |                                          |
| TPI-R de sécurité       | Bit                                                                                                                                                                                                                                                                            | Description                                                      | Valeurs                                  |
|                         | 0 – 15                                                                                                                                                                                                                                                                         | Données de soutien au protocole (PSD) utilisé par la gestion SCL | 0 – 65 535                               |
|                         | 16 – 19                                                                                                                                                                                                                                                                        | Numéro d'exécution                                               | 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<br>1 = non occupé             |
|                         | 29                                                                                                                                                                                                                                                                             | Notification d'erreur                                            | 0 = pas d'erreur<br>1 = erreur           |
|                         | 30                                                                                                                                                                                                                                                                             | réservé                                                          | 0                                        |
|                         | 31                                                                                                                                                                                                                                                                             | mode d'application de l'utilisateur SCL                          | 0 = mode d'essai<br>1 = mode de sécurité |
|                         | 32 – 63                                                                                                                                                                                                                                                                        | CRC32                                                            | CRC32                                    |

#### 11.7.1.3.6 Codage PDU de transmission cyclique de sécurité S1

Le codage PDU spécifique applicable aux attributs appartenant à cette classe est décrit au Tableau 13.

**Tableau 13 – Codage d'attributs de transmission cyclique de sécurité S1**

| Attribut                | Codage                                                                                                                                                                                                                                                                 |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Données de sortie       | Données de processus transmises par le maître                                                                                                                                                                                                                          |
| Données RY de sécurité  | Champ contenant les données d'entrée orientées sur les bits ordonnées par créneau avec 32 bits par créneau. Le nombre de créneaux occupés par l'appareil esclave détermine la longueur totale de ce champ                                                              |
| Données RWw             | Champ à mapping positionnel dans lequel sont mises en correspondance les données de sortie par mot (facultativement) et les informations de paquets de transmission de sécurité fournies 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 |

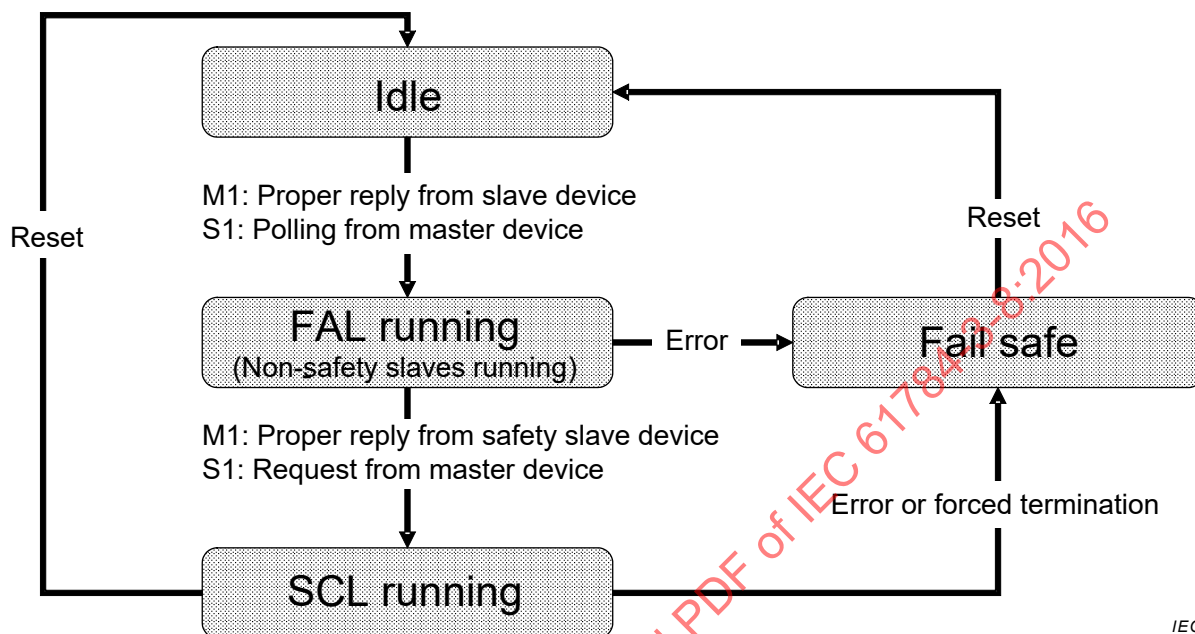
| Attribut                | Codage                                                                                                                                                                                                                                                                |                                                                  |                                          |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------|------------------------------------------|
|                         | Bit                                                                                                                                                                                                                                                                   | Description                                                      | Valeurs                                  |
| TPI-T de sécurité       | 0 – 15                                                                                                                                                                                                                                                                | Données de soutien au protocole(PSD) utilisé par la gestion SCL  | 0 – 65 535                               |
|                         | 16 – 19                                                                                                                                                                                                                                                               | Numéro d'exécution                                               | 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<br>1 = non occupé             |
|                         | 29                                                                                                                                                                                                                                                                    | réservé                                                          | 0                                        |
|                         | 30                                                                                                                                                                                                                                                                    | Demande de lecture                                               | 0 = pas de demande<br>1 = demande        |
|                         | 31                                                                                                                                                                                                                                                                    | mode d'application de l'utilisateur SCL                          | 0 = mode d'essai<br>1 = mode de sécurité |
|                         | 32 – 63                                                                                                                                                                                                                                                               | CRC32                                                            | CRC32                                    |
| Données d'entrée        | Données de processus transmises au maître                                                                                                                                                                                                                             |                                                                  |                                          |
| Données RX de sécurité  | Champ contenant les données d'entrée orientées sur les bits ordonnées par créneau avec 32 bits par créneau. Le nombre de créneaux occupés par l'appareil esclave détermine la longueur totale de ce champ                                                             |                                                                  |                                          |
| Données RWr             | Champ contenant les données d'entrée par mot fournies par le maître. Le nombre de créneaux occupés par l'appareil esclave détermine la longueur totale de ce champ                                                                                                    |                                                                  |                                          |
| Données RWr de sécurité | 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 |                                                                  |                                          |
| TPI-R de sécurité       | Bit                                                                                                                                                                                                                                                                   | Description                                                      | Valeurs                                  |
|                         | 0 – 15                                                                                                                                                                                                                                                                | Données de soutien au protocole (PSD) utilisé par la gestion SCL | 0 – 65 535                               |
|                         | 16 – 19                                                                                                                                                                                                                                                               | Numéro d'exécution                                               | 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<br>1 = non occupé             |
|                         | 29                                                                                                                                                                                                                                                                    | Notification d'erreur                                            | 0 = pas d'erreur<br>1 = erreur           |
|                         | 30                                                                                                                                                                                                                                                                    | réservé                                                          | 0                                        |
|                         | 31                                                                                                                                                                                                                                                                    | mode d'application de l'utilisateur SCL                          | 0 = mode d'essai<br>1 = mode de sécurité |
|                         | 32 – 63                                                                                                                                                                                                                                                               | CRC32                                                            | CRC32                                    |

## 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 (voir 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.



| Anglais                                 | Français                                                              |
|-----------------------------------------|-----------------------------------------------------------------------|
| Idle                                    | Repos                                                                 |
| Proper reply from slave device          | Réponse correcte de l'appareil esclave                                |
| Polling from master device              | Interrogation de l'appareil maître                                    |
| FAL running (Non-safety slaves running) | Exécution FAL (esclaves non relatifs à la sécurité en fonctionnement) |
| Proper reply from safety slave device   | Réponse correcte de l'appareil esclave de sécurité                    |
| Request from master device              | Demande de l'appareil maître                                          |
| SCL running                             | Exécution SCL                                                         |
| Reset                                   | Réinitialisation                                                      |
| Fail safe                               | Sécurité intrinsèque                                                  |
| Error                                   | Erreur                                                                |
| Error or forced termination             | Erreur ou interruption forcée                                         |

**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.

Sur réception de communications d'interrogation provenant 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**

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 provenant du maître de sécurité M1, l'appareil esclave de sécurité S1 passe à l'état d'exécution SCL.

Sur réception de réponses adaptées provenant 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 lorsque l'un des types d'erreur suivants est détecté:

- numéro de séquence;
- délai;
- authentification de connexion;
- message de réaction;
- assurance d'intégrité des données;
- 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 A 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;
- 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 4 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 la valeur du 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 et le Tableau 15 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<br>(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<br>(2) Lors de la détection d'une erreur RNO<br>(3) À 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<br>(2) Lors de la détection d'une erreur RNO<br>(3) À la réception d'une demande d'interruption forcée |
| <p>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.</p> |                                                                                                                                                                                                            |                                                                                                                                                 |

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**

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.

De plus, l'ID de connexion logique de 16 bits transmis est annexé au SPDU pour validation. Ce champ, qui est composé de A1 (ID source de 8 bits) et A2 (ID de destination de 8 bits) est vérifié quant à l'exactitude et également inclus dans les mesures d'intégrité des données, comme présenté en 11.9.5.2.

#### **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, de l'ID de commande et du champ de données de soutien au protocole.

#### **11.7.2.6.6 Intégrité des données**

Le CRC32 pour le protocole FSCP 8/1 est calculé tel que décrit à l'Annexe A. Le taux d'erreurs résiduelles pour ce protocole est traité en 11.9.5.2.

#### **11.7.2.6.7 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 garantie par la validation du caractère unique des messages de sécurité à contenir une somme de contrôle CRC à format approprié (32 bits), un champ de données de soutien au protocole de 16 bits, un ID de commande de 8 bits, un ID de liaison de 3 bits et un RNO de 4 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 Établissement 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 au Tableau 17.

**Tableau 17 – Détails de l'établissement de connexion et du processus de confirmation**

| Type de SAREP       | Détails du processus                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Maître de sécurité  | <ol style="list-style-type: none"> <li>(1) Confirmer que l'esclave est un appareil esclave de sécurité.<br/>(Cela est confirmé par la communication des données cycliques de sécurité).</li> <li>(2) Confirmer que l'esclave de sécurité a reçu la commande Établir connexion.<br/>(Ceci est confirmé par la vérification du fait que les CMD et PSD des données de réponse sont identiques aux données transmises).</li> <li>(3) Transmettre la valeur du temporisateur de contrôle de sécurité.</li> </ol> |
| Esclave de sécurité | <ol style="list-style-type: none"> <li>(1) Confirmer que le maître est un appareil maître de sécurité.<br/>(Cela est confirmé par la communication des données cycliques de sécurité).</li> <li>(2) Recevoir la valeur du temporisateur de contrôle de sécurité et enregistrer cette dernière de manière interne.</li> </ol>                                                                                                                                                                                 |

Le poste maître de sécurité transmet  $RNO = 0$  lors de la transmission de la commande Établir 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 effectivement 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 au Tableau 18.

**Tableau 18 – Détails du processus de vérification des informations sur les esclaves**

| Type de SAREP       | Détails du processus                                                                                                                                                                                                                                                                                                                                                    |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Maître de sécurité  | <ol style="list-style-type: none"> <li>(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.</li> <li>(2) Après vérification, transmettre les informations sur les produits aux postes esclaves de sécurité.</li> </ol> |
| Esclave de sécurité | <ol style="list-style-type: none"> <li>(1) Vérifier les informations sur les produits de l'esclave par rapport aux informations sur les produits fournies par le maître de sécurité.</li> </ol>                                                                                                                                                                         |

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 au Tableau 19.

**Tableau 19 – Détails du processus de transmission  
des paramètres des esclaves de sécurité**

| Type de SAREP       | Détails du processus                                                                                                                                                                                                                                                                                 |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Maître de sécurité  | <p>(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.</p> <p>(2) Transmettre les paramètres des esclaves de sécurité à l'esclave de sécurité.</p> |
| Esclave de sécurité | <p>(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.</p>                                                                                                                         |

## 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 permettant 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 permettant de régler les éléments suivants:

- Nombre de créneaux occupés – Créneaux de postes (1 ou 2) occupés par un poste esclave de sécurité.
- Vérification de ligne 1 – Vérifie que le maître est capable de se connecter à tous les postes esclaves.
- Vérification 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 au Tableau 20 avec l'interprétation suivante:

M = obligatoire

O = facultatif

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 de contrôle**

| N° | 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<br>Sortie: Erreur de temporisateur de chien de garde                                                                                                                                                                                                                                                                                                                                                                                                        | M                           | O                                    | O                             |
| 2  | ERR        | Allumée: Erreur de communication avec tous les postes<br>Cette LED s'allume lorsque l'une des situations suivantes se produit:<br>· Erreur de réglage des commutateurs<br>· Duplication du poste maître sur la même ligne<br>· Erreur de contenu des paramètres<br>· Activation du temporisateur de contrôle de liaison de données<br>· Rupture des conducteurs de câble<br>Ou câble influencé par le bruit sur le chemin de transmission<br>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)<br>Clignotement: Modification du paramétrage du type de commutateur sous tension (position ON)                                                                                                                                                                                                                                                                                                                                | M                           | O                                    | O                             |

### 11.9.2 Lignes directrices d'installation

La présente Norme spécifie le protocole et les services d'un système de communication de sécurité reposant sur le Type 18 de l'IEC 61158. Toutefois, l'utilisation d'appareils de sécurité avec le protocole de sécurité spécifié dans la présente Norme exige une installation correcte. Tous les appareils connectés à un système de communication de sécurité défini dans la présente partie doivent satisfaire aux exigences TBTS/TBTP, qui sont spécifiées dans les normes IEC correspondantes telles que l'IEC 60204-1.

Des informations supplémentaires relatives à l'installation sont également données en [34] et [35] 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 (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, 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(s) canal(aux) de sortie correspondant(s) de l'(des) esclave(s) de sortie 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 chaque esclave (d'entrée et de sortie) de sécurité et le temps de traitement du 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).

### 11.9.3.2 Calcul du temps

Un temporisateur intégré indiquant 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(s) canal(aux) de sortie correspondant(s) de l'(des) esclave(s) 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 au Tableau 21 avec les termes définis au 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 –  $((WDT \times n) \times 2)$

NOTE 2  $(WDT \times n) \times 2$  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**

| Élément                                                       | 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**

| Élément                                               | Définition                                                                                                          |
|-------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| LS                                                    | Temps d'analyse de liaison spécifié par le fabricant                                                                |
| n                                                     | Valeur après la décimale de LS/WDT (arrondi à l'unité supérieure la plus proche)                                    |
| SRRP                                                  | Temps de traitement de la réponse de rafraîchissement des données de sécurité. Tel que spécifié par le fabricant    |
| m                                                     | Valeur après la décimale de SRRP/(WDT × n) (arrondi à l'unité supérieure la plus proche)                            |
| Temps de traitement du filtre de suppression de bruit | Configuré selon les paramètres 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. Tel que spécifié par le fabricant. |

| Élément                                                       | Définition                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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:<br><br>Temps de contrôle de rafraîchissement des données de sécurité $\times 2 - ((WDT \times n) \times m) - 10$ [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:<br><br>En mode déclenché:<br>$(WDT \times n) \times 3 + (WDT \times n) \times m \times 2 + (WDT \times \alpha)$ [ms]<br><br>En mode libre:<br>$(WDT \times n) \times 3 + LS + (WDT \times n) \times m \times 2 + (WDT \times \alpha)$ [ms]<br><br>où:<br>$\alpha = 0$ , pour $LS \leq 1,5$ ms<br>$\alpha = 1$ , 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.<br><br>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 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

##### 11.9.5.1 Caractéristiques du système

Les données de base suivantes doivent être conformes:

- 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

##### 11.9.5.2 Taux d'erreurs résiduelles ( $\Lambda$ )

Les appareils esclaves de sécurité et leur nombre correspondant de créneaux occupés dans la configuration du système ont un impact direct sur le taux d'erreurs résiduelles,  $\Lambda$ . Le Tableau 23 présente l'influence du nombre de créneaux occupés de l'esclave de sécurité sur la longueur de trame obtenue pour son PDU de sécurité correspondant.

**Tableau 23 – Nombre de créneaux occupés et données de sécurité**

| Créneaux occupés | Structure du PDU de sécurité                                    |           | Longueur de trame (bits) |
|------------------|-----------------------------------------------------------------|-----------|--------------------------|
|                  | SAR                                                             | Structure |                          |
| 1                | Poste de maître de sécurité<br>→<br>Poste d'esclave de sécurité |           | 112                      |
|                  | Poste d'esclave de sécurité<br>→<br>Poste de maître de sécurité |           | 112                      |
| 2                | Poste de maître de sécurité<br>→<br>Poste d'esclave de sécurité |           | 208                      |
|                  | Poste d'esclave de sécurité<br>→<br>Poste de maître de sécurité |           | 208                      |

Sur la base de la longueur de trame et du nombre d'esclaves de sécurité dans le système correspondant,  $\Lambda$  apparaît au Tableau 24 et au Tableau 25.

**Tableau 24 – Taux d'erreurs résiduelles  $\Lambda$  (créneaux occupés = 1)**

| Probabilité du taux d'erreurs résiduelles, $R_{pCRC32}$ | Nombre d'esclaves de sécurité | Durée minimale du cycle ms | Taux d'erreurs résiduelles, $\Lambda$ |
|---------------------------------------------------------|-------------------------------|----------------------------|---------------------------------------|
| $1,01 \times 10^{-24}$                                  | 1                             | 10,0                       | $7,27 \times 10^{-17}$                |
|                                                         | 8                             | 10,0                       | $5,81 \times 10^{-16}$                |
|                                                         | 16                            | 10,0                       | $1,16 \times 10^{-15}$                |
|                                                         | 32                            | 10,0                       | $2,33 \times 10^{-15}$                |
|                                                         | 42                            | 10,0                       | $3,05 \times 10^{-15}$                |

**Tableau 25 – Taux d'erreurs résiduelles  $\Lambda$  (créneaux occupés = 2)**

| Probabilité du taux d'erreurs résiduelles, $R_{pCRC32}$ | Nombre d'esclaves de sécurité | Durée minimale du cycle ms | Taux d'erreurs résiduelles, $\Lambda$ |
|---------------------------------------------------------|-------------------------------|----------------------------|---------------------------------------|
| $2,05 \times 10^{-19}$                                  | 1                             | 10,0                       | $1,47 \times 10^{-11}$                |
|                                                         | 8                             | 10,0                       | $1,18 \times 10^{-10}$                |
|                                                         | 16                            | 10,0                       | $2,36 \times 10^{-10}$                |
|                                                         | 32                            | 10,0                       | $4,72 \times 10^{-10}$                |

Le taux d'erreurs résiduelles résultant pour toutes les configurations spécifiées du protocole FSCP 8/1 est maintenu sous le taux  $10^{-7}$  ( $10^{-9}$  imputable au réseau) exigé afin de satisfaire au niveau SIL3 et à la catégorie 4.

### 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 de la présente norme. 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 par ailleurs recommandé de s'appuyer sur les documents [34] et [35] de la Bibliographie. 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 intégrant la SCL conformément aux spécifications correspondantes données dans la présente Norme doit élaborer un manuel de sécurité approprié conformément à l'IEC 61508. Ce manuel de sécurité doit également comprendre les exigences d'installation telles que 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 reposant sur le Type 18 de l'IEC 61158, il est vivement recommandé de tenir compte des spécifications [34], [35] et [36] de la Bibliographie.

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 Évaluation 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, ...) et aux règlements juridiques pertinents (Directive européenne relative aux machines, par exemple).

## 12 FSCP 8/2

### 12.1 Domaine d'application – FSCP 8/2

Voir l'Article 1.

### 12.2 Références normatives – FSCP 8/2

Voir l'Article 2.

### 12.3 Termes, définitions, symboles, abréviations et conventions – FSCP 8/2

Voir l'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™<sup>6</sup>) définit les profils de communication reposant sur l'IEEE 802.3, 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™<sup>5</sup>) repose sur les profils de base CP 8/4 et CP 8/5 de l'IEC 61784-2 et les spécifications de couche de communication de sécurité définies dans la présente partie.

Le FSCP 8/2 est un protocole de communication des données relatives à la sécurité tel 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 peut être utilisé dans diverses 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 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 8/2 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 la présente partie. 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.

<sup>6</sup> CC-Link IE™ est une appellation commerciale de l'organisme sans but lucratif CC-Link Partner Association. Ces informations sont données pour des raisons de commodité des utilisateurs de la présente norme internationale et ne constituent en aucun cas un entérinement par l'IEC du titulaire de la marque ou de l'un de ses produits. La conformité à la présente Norme n'exige pas l'utilisation de l'appellation commerciale CC-Link IE™. L'utilisation 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).

## 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 la présente partie.

NOTE Les documents [34] et [35] contiennent des informations importantes relatives à FSCP 8/2.

### 12.5.2 Exigences fonctionnelles de sécurité

La présente partie spécifie les services et protocoles d'un système de communication de sécurité fonctionnelle reposant sur le Type 23 de l'IEC 61158. Les technologies de communication spécifiées dans la présente norme 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 8/2. 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 la présente partie, 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 la présente norme fournit les mesures correctives déterministes suivantes pour sa mise en œuvre:

- datation (horodatage);
- délai;
- authentification de connexion;
- message de réaction;
- assurance d'intégrité des données;
- différents systèmes d'assurance d'intégrité des données.

La sélection des différentes mesures correspondant aux erreurs possibles est présentée au Tableau 26.

**Tableau 26 – Sélection des différentes mesures correspondant 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                                 |                                     |                                                         |
| Répétition non prévue                                                                                                                            |                                   | X                     |       |                               |                     |                                   |                                     |                                                         |
| Séquence incorrecte                                                                                                                              |                                   | X                     |       |                               |                     |                                   |                                     |                                                         |
| Perte                                                                                                                                            |                                   | X <sup>a,c</sup>      |       |                               | X <sup>b</sup>      |                                   |                                     |                                                         |
| Retard inacceptable                                                                                                                              |                                   | X <sup>c</sup>        | X     |                               |                     |                                   |                                     |                                                         |
| Insertion                                                                                                                                        |                                   |                       |       | X                             |                     |                                   |                                     |                                                         |
| Déguisement                                                                                                                                      |                                   |                       |       |                               |                     |                                   |                                     | X                                                       |
| Adressage                                                                                                                                        |                                   |                       |       | X                             |                     |                                   |                                     |                                                         |
| <p>A Évalué par horodatage reçu.</p> <p>b Utilisé dans le modèle de demande/réponse.</p> <p>c Non utilisé dans le modèle de demande/réponse.</p> |                                   |                       |       |                               |                     |                                   |                                     |                                                         |

### 12.5.3.2 Corruption

La corruption est détectée à l'aide du CRC inclus dans le PDU de sécurité. Le nœud de transmission envoie le PDU de sécurité en incluant le CRC calculé. Le nœud de réception compare le CRC inclus dans le PDU de sécurité reçu au CRC calculé à partir de ce même PDU, puis détermine si une corruption s'est produite. Si la comparaison 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 de l'horodatage qu'il contient. Le nœud de transmission envoie des PDU de sécurité contenant un horodatage (TS).

Le nœud de réception reçoit le PDU de sécurité et conserve son TS 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 son TS au TS conservé du PDU de sécurité déjà reçu. Si le TS du PDU de sécurité reçu est identique au TS 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 comportant la même valeur de TS, le temporisateur delay\_detection\_timer utilisé pour détecter les délais inacceptables ne doit pas être réinitialisé.

La Figure 5 présente 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.

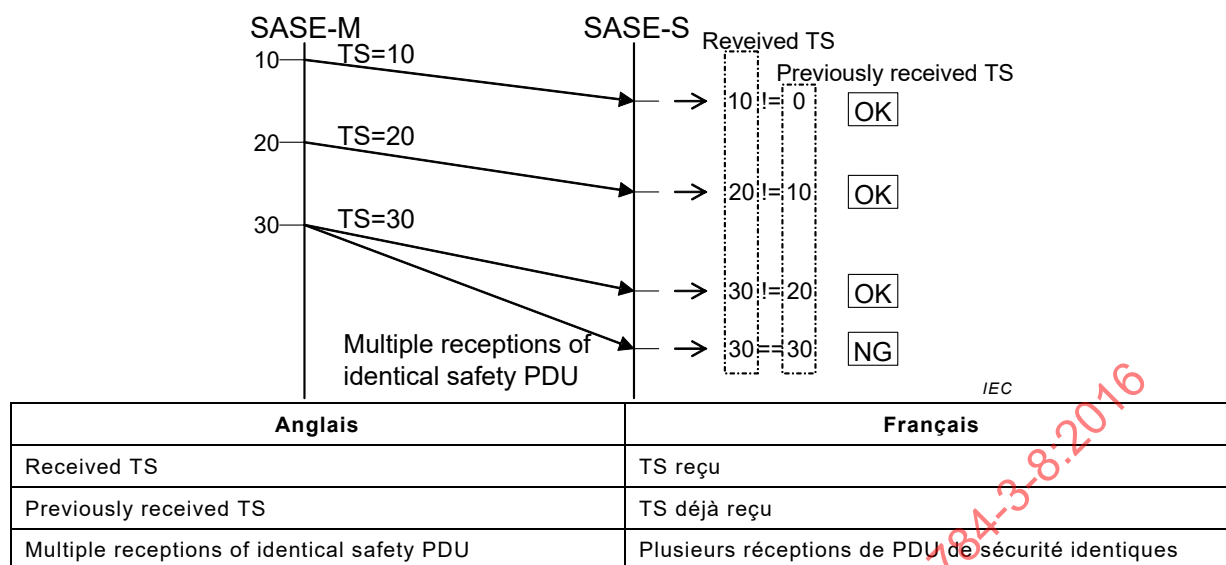


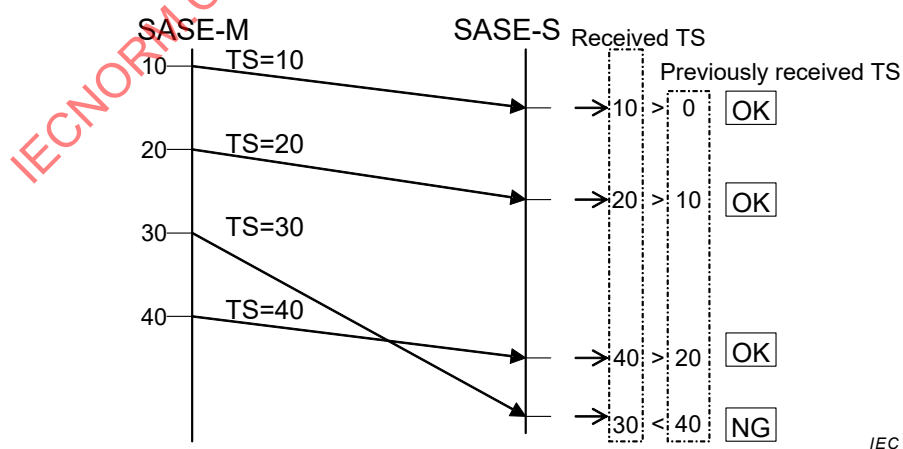
Figure 5 – Détection d'une répétition non prévue

#### 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. L'ordre est détecté à l'aide des horodatages inclus dans les PDU de sécurité. Le nœud de transmission envoie des PDU de sécurité contenant un TS.

Le nœud de réception reçoit un PDU de sécurité dont il conserve le TS. Lors de la réception du PDU de sécurité suivant, le nœud de réception compare son TS au TS conservé du PDU de sécurité déjà reçu. Si le TS du PDU reçu est inférieur au TS déjà reçu, le nœud de réception considère que l'ordre est incorrect, et doit interrompre la connexion de sécurité.

La Figure 6 présente 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.



| Anglais                | Français     |
|------------------------|--------------|
| Received TS            | TS reçu      |
| Previously received TS | TS déjà reçu |

Figure 6 – Détection d'une séquence incorrecte

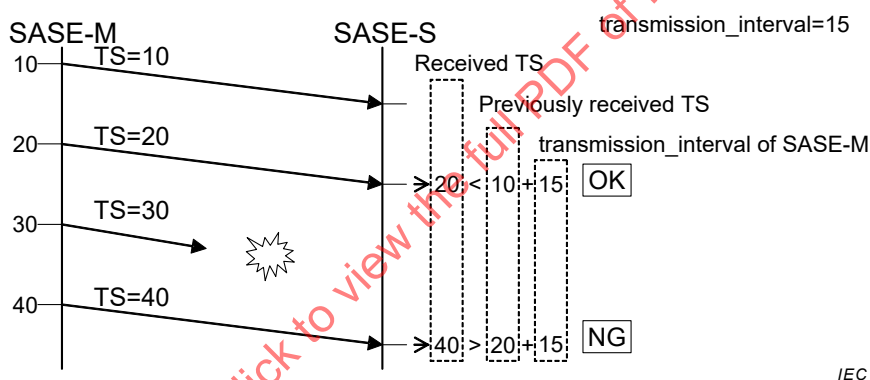
### 12.5.3.5 Perte

La perte est détectée à l'aide des horodatages.

SASE-M envoie régulièrement des PDU de sécurité à SASE-S en fonction de l'intervalle de transmission SASE-M (*transmission\_interval*). Le TS inclus dans le PDU de sécurité envoyé par SASE-M est la valeur de l'horloge de sécurité pendant 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 TS 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 TS n'est pas supérieur à la somme de *transmission\_interval* du nœud de transmission ajouté au TS du PDU de sécurité déjà reçu, et considère qu'une perte s'est produite si c'est le cas. Si une perte est détectée, le nœud de réception doit interrompre la connexion de sécurité.

La Figure 7 présente 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.



| Anglais                                | Français                               |
|----------------------------------------|----------------------------------------|
| Received TS                            | TS reçu                                |
| Previously received TS                 | TS déjà reçu                           |
| <i>transmission_interval</i> of SASE-M | <i>transmission_interval</i> de SASE-M |

Figure 7 – Détection d'une perte

### 12.5.3.6 Retard inacceptable

Un retard inacceptable est détecté à l'aide des temporisateurs et des horodatages.

SASE-M envoie régulièrement des PDU de sécurité à SASE-S en fonction de l'intervalle de transmission SASE-M (*transmission\_interval*). Le TS 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 TS 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 TS reçu,

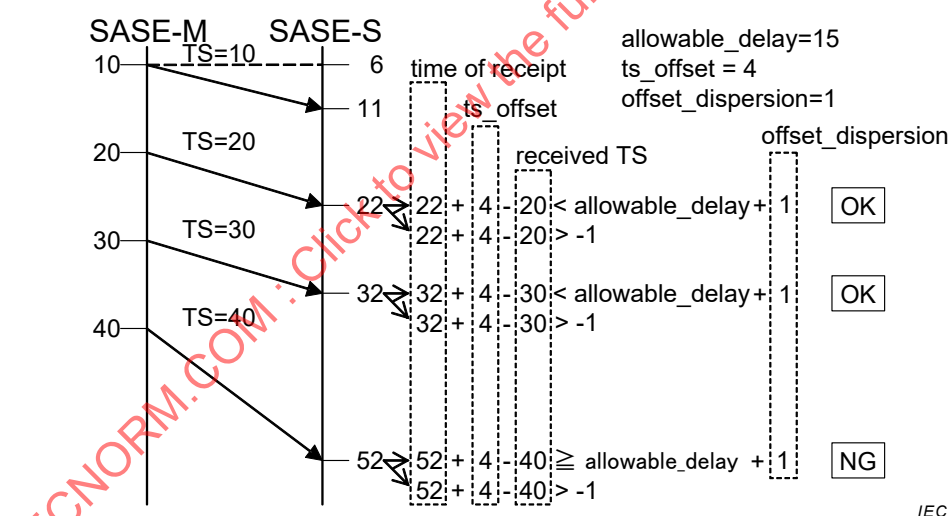
puis calcule la valeur de retard entre SASE-M et SASE-S. Si la valeur calculée ne satisfait pas la condition suivante qui tient compte de la dispersion de décalage (offset\_dispersiion), le nœud de réception considère qu'un retard inacceptable s'est produit.

$$\text{offset\_dispersion} < \text{Valeur calculée} < \text{allowable\_delay} + \text{offset\_dispersion}$$

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 TS 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 présente 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.



IEC

| Anglais         | Français           |
|-----------------|--------------------|
| time of receipt | heure de réception |
| received TS     | TS reçu            |

Figure 8 – Détection d'un retard inacceptable par les horodatages

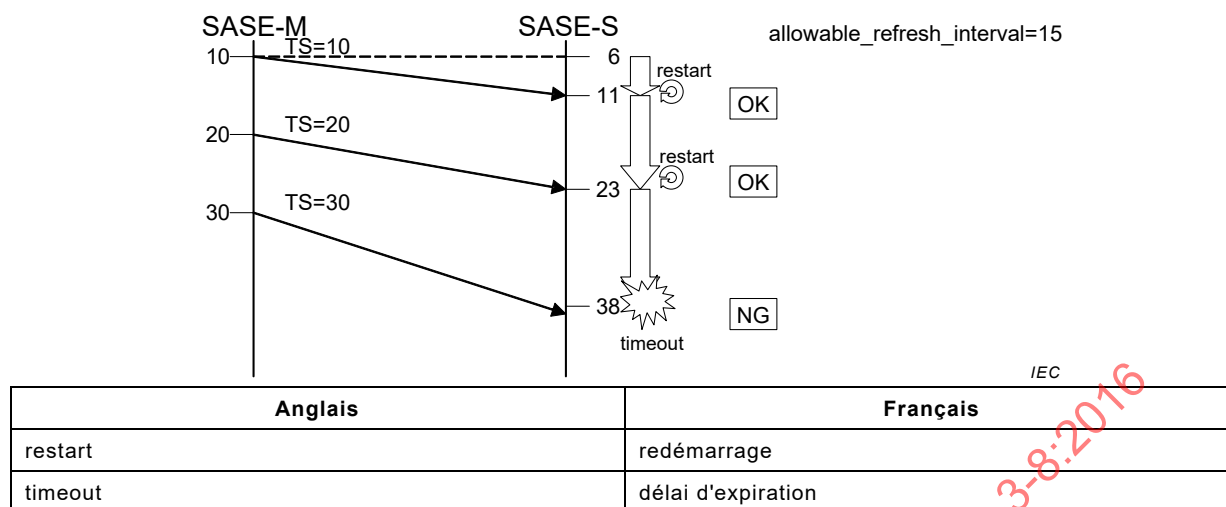


Figure 9 – Détection d'un retard inacceptable par le temporisateur

### 12.5.3.7 Insertion

L'insertion consiste à insérer un message provenant 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` convenu 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 dangereux par un poste de sécurité et l'insertion du message à partir de ce qui semble être une source de transmission valide par suite d'une anomalie ou une interférence. Le déguisement est détecté à l'aide du CRC généré par un polynôme générateur différent de celui d'une communication non sûre.

Le nœud de transmission envoie un PDU de sécurité qui contient le CRC calculé. Le nœud de réception compare le CRC inclus dans le PDU de sécurité au CRC calculé à partir du PDU de sécurité reçu. 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.

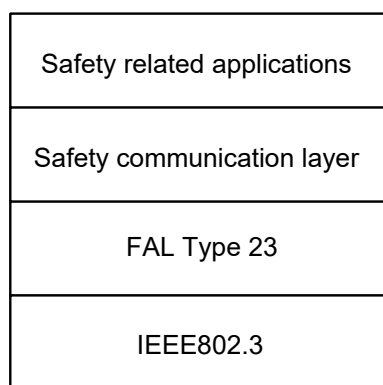
### 12.5.3.9 Adressage

L'adressage 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` convenu 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 (IEEE 802.3 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 présentée (pour CP 8/5) à la Figure 10.



IEC

| Anglais                     | Français                             |
|-----------------------------|--------------------------------------|
| Safety related applications | Applications relatives à la sécurité |
| Safety communication layer  | Couche de communication de sécurité  |

**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 établies 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 de "Read memory" et de "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 27 présente les paramètres de SS-Start.

**Tableau 27 – SS-Start**

| Nom de paramètre | Req | Ind  | Rsp | Cnf |
|------------------|-----|------|-----|-----|
| Argument         | M   | M(=) |     |     |
| ConnectionID     | M   | M(=) |     |     |

**ConnectionID**

Spécifie l'ID de la connexion de sécurité devant 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 28 présente les paramètres de SS-Restart.

**Tableau 28 – SS-Restart**

| Nom de paramètre | Req | Ind  | Rsp | Cnf |
|------------------|-----|------|-----|-----|
| Argument         | M   | M(=) |     |     |
| ConnectionID     | M   | M(=) |     |     |

**ConnectionID**

Spécifie l'ID de la connexion de sécurité devant 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 29 présente les paramètres de SS-InvokeFunc.

**Tableau 29 – 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 30 indique les paramètres de ce service.

**Tableau 30 – 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 31 indique les paramètres de ce service.

**Tableau 31 – 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 32 indique les paramètres de ce service.

**Tableau 32 – SS-Terminate**

| Nom de paramètre | Req | Ind | Rsp | Cnf |
|------------------|-----|-----|-----|-----|
| Argument         |     | M   |     |     |
| CID              |     | M   |     |     |

#### CID

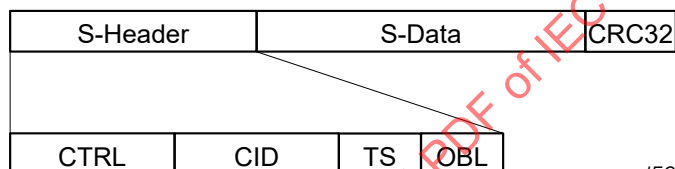
Spécifie le CID de la connexion de sécurité terminée.

### 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 présente 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 128 bits.



IEC

**Figure 11 – Structure du PDU de sécurité**

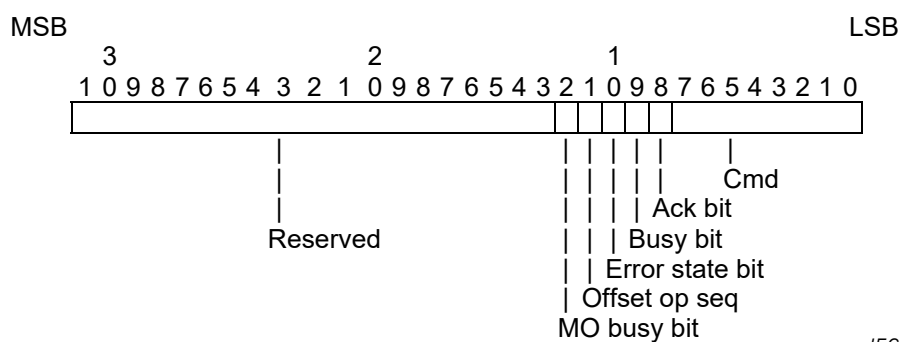
Le Tableau 33 indique les noms, tailles et contenus des éléments qui composent le PDU de sécurité.

**Tableau 33 – Éléments du PDU de sécurité**

| Attribut | Description                                               | Taille (bits) |
|----------|-----------------------------------------------------------|---------------|
| S-Header | Structure de 4 éléments:                                  | 96            |
| CTRL     | Type de commande, état                                    | 32            |
| CID      | Identifiant de connexion de sécurité                      | 32            |
| TS       | Horodatage                                                | 16            |
| OBL      | Informations de génération de décalage                    | 16            |
| S-Data   | Données de sécurité                                       | 128 max       |
| CRC32    | Contrôle de redondance cyclique (Cyclic Redundancy Check) | 32            |

##### 12.7.1.2 CTRL

La Figure 12 présente la configuration de CTRL. Le Tableau 34 décrit le contenu des éléments qui composent CTRL.



IEC

| Anglais         | Français                   |
|-----------------|----------------------------|
| MSB             | Bit de poids fort          |
| LSB             | Bit de poids faible        |
| Ack bit         | Bit d'acquittement positif |
| Busy bit        | Bit d'état occupé          |
| Error state bit | Bit d'état d'erreur        |
| Offset op seq   | Séquence op de décalage    |
| MO busy bit     | Bit d'état occupé MO       |
| Reserved        | Réservé                    |

Figure 12 – Configuration CTRL

Tableau 34 – Éléments de CTRL

| Élément                    | Valeur              | Description                                                                         |
|----------------------------|---------------------|-------------------------------------------------------------------------------------|
| Cmd                        | S-Connect           | 0x00 Établir 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 – 0xF0 Pour une extension ultérieure                                           |
|                            | S-ReadErrorInfo     | 0xFA Lire les informations relatives à l'erreur                                     |
|                            | S-WriteErrorInfo    | 0xFB Émettre la notification d'erreur                                               |
|                            | S-RefreshReady      | 0xFC Émettre 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                              |
| Bit d'acquittement positif | 0x00                | Demande                                                                             |
|                            | 0x01                | Réponse                                                                             |
| Bit d'état occupé          | 0x00                | Traitement terminé                                                                  |
|                            | 0x01                | Traitement non terminé                                                              |
| 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                                                              |
| Réservé                    | —                   | Pour une extension ultérieure                                                       |

### **Cmd**

Indique le type de PDU de sécurité.

### **Bit d'acquiescement 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. À 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. À 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 suite au 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 provenant 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.

### **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

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.

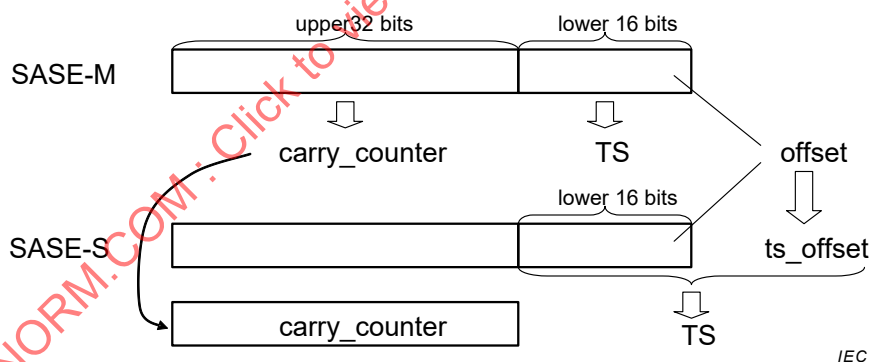
Lorsque le SASE-M exécute une demande Cmd, la valeur des 16 bits inférieurs de l'horloge de sécurité pendant la demande Cmd doit être stockée dans TS.

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.

Horodatage

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

La Figure 13 indique la relation entre les horloges de sécurité SASE-M et SASE-S et le TS lors d'une demande Cmd.



| Anglais       | Français           |
|---------------|--------------------|
| upper32 bits  | 32 bits supérieurs |
| lower 16 bits | 16 bits inférieurs |
| offset        | décalage           |

**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.

Les 32 bits supérieurs de l'horloge de sécurité de 48 bits sont appelés `carry_counter` et sont déduits des 32 bits supérieurs de l'horloge de sécurité SASE-M. SASE-M informe SASE-S de la valeur initiale de `carry_counter` lors de l'établissement de la connexion.

SASE-S utilise alors la valeur identifiée par SASE-M en tant que `carry_counter`. `carry_counter` est utilisé comme valeur initiale de la génération CRC stockée dans le PDU de sécurité.

L'exactitude de l'horloge de sécurité mise en œuvre doit être de  $\pm 100$  ppm.

#### 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 présenté à la Figure 14, dans lequel `safety_data` représente les données de rafraîchissement de sécurité.

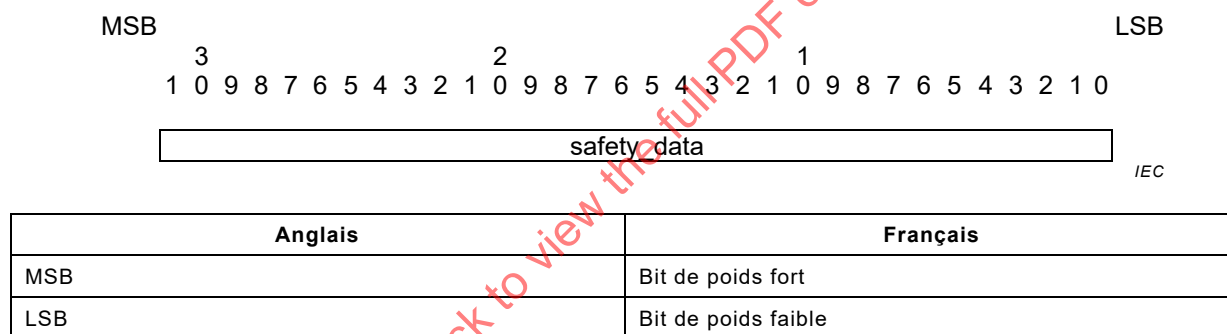


Figure 14 – S-Data lors du rafraîchissement de sécurité

La Figure 15 et la Figure 16 présentent les formats S-Data utilisés à des périodes autres que le rafraîchissement de sécurité.

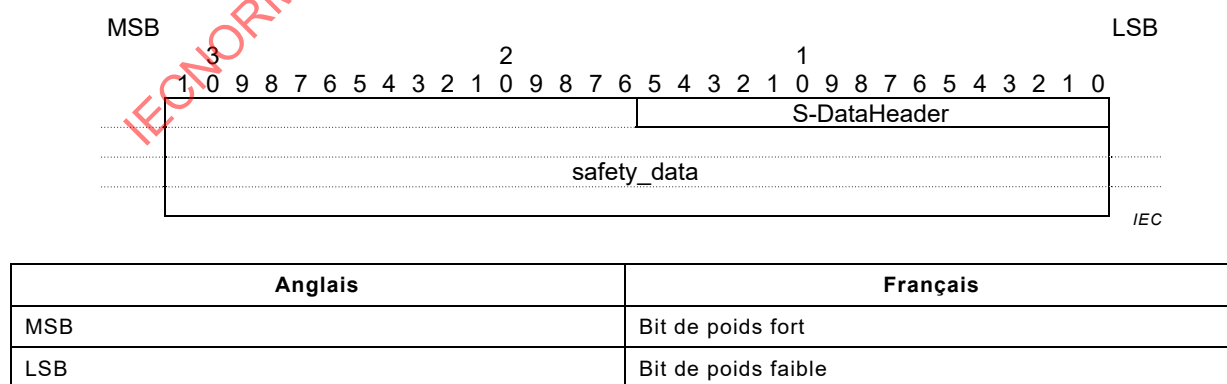
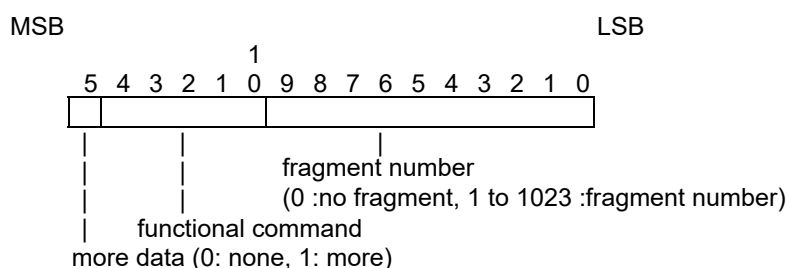


Figure 15 – S-Data hors du rafraîchissement de sécurité



IEC

| Anglais                    | Français                      |
|----------------------------|-------------------------------|
| MSB                        | Bit de poids fort             |
| LSB                        | Bit de poids faible           |
| fragment number            | numéro de fragment            |
| 0: no fragment             | 0: pas de fragment            |
| 1 to 1023: fragment number | 1 à 1 023: numéro de fragment |
| functional command         | commande fonctionnelle        |
| more data                  | données complémentaires       |
| 0: none                    | 0: aucune                     |
| 1: more                    | 1: plusieurs                  |

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 contenant 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

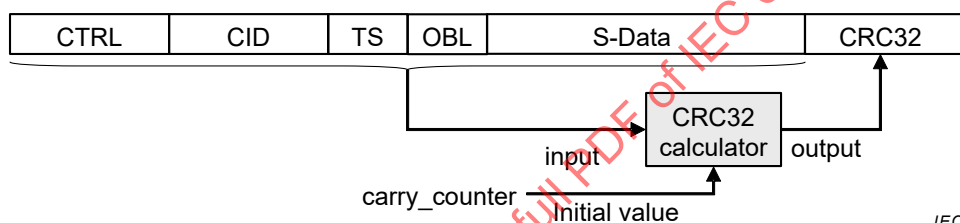
CRC32 est un CRC 32 bits destiné à la communication de sécurité. La formule suivante doit être utilisée comme le polynôme générateur de CRC avec la fonction de communication de sécurité FSCP 8/2.

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 [36]. 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 CTRL, de CID, de TS, d'OBL, de S-Data et du carry\_counter inclus dans le PDU de sécurité (voir la Figure 17).



| Anglais          | Français             |
|------------------|----------------------|
| input            | entrée               |
| output           | sortie               |
| CRC32 calculator | Calculateur de CRC32 |
| Initial value    | Valeur initiale      |

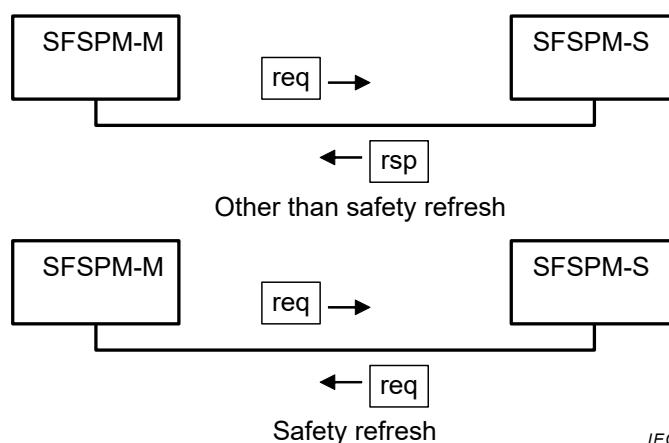
Figure 17 – Calcul de CRC

## 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 présentés 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.

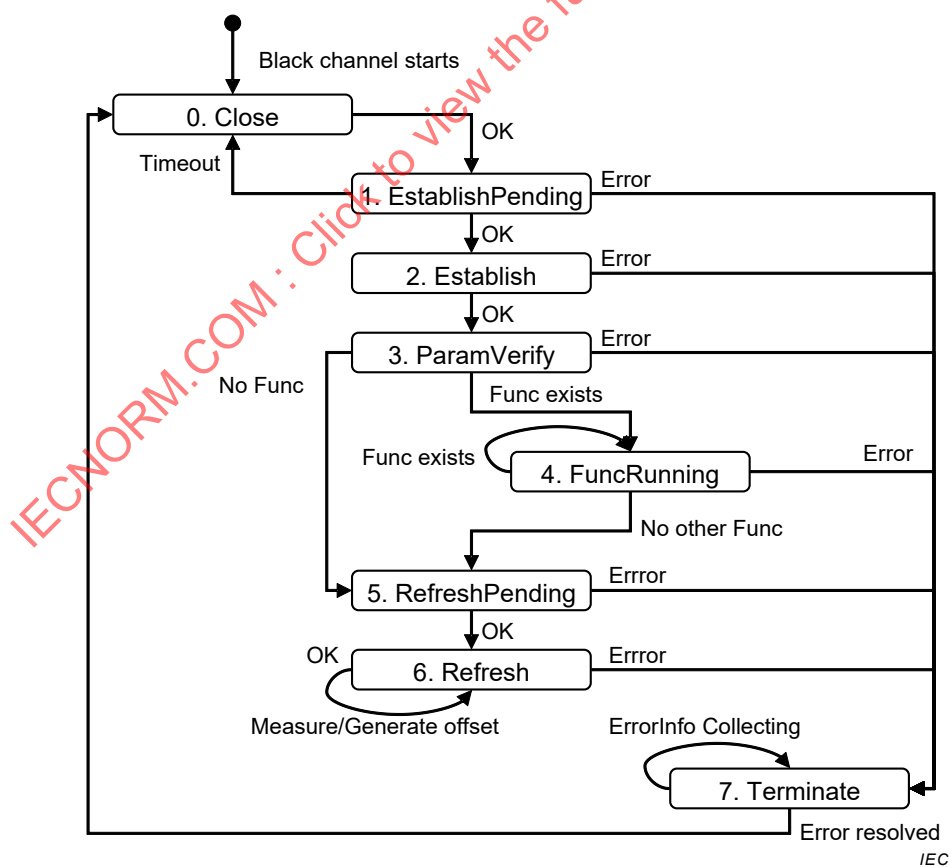
Lorsque des opérations autres que le rafraîchissement de sécurité sont réalisées, SFSPM-M envoie une demande à SFSPM-S, et SFSPM-S envoie une réponse à SFSPM-M. Lorsque des opérations de rafraîchissement de sécurité sont réalisées, SFSPM-M et SFSPM-S s'envoient indépendamment des demandes l'un à l'autre.



| Anglais                   | Français                                  |
|---------------------------|-------------------------------------------|
| Req                       | Demande                                   |
| Other than safety refresh | Autre que le rafraîchissement de sécurité |
| Safety refresh            | Rafraîchissement de sécurité              |
| Rsp                       | Réponse                                   |

Figure 18 – Modèles de communication

La Figure 19 donne un aperçu des transitions d'état de la couche de communication de sécurité.



| Anglais              | Français            |
|----------------------|---------------------|
| Black channel starts | Début du canal noir |
| Timeout              | Délai d'expiration  |

| Anglais                 | Français                    |
|-------------------------|-----------------------------|
| No Func                 | Pas de fonction             |
| Error                   | Erreur                      |
| Func exists             | La fonction existe          |
| Measure/Generate offset | Mesurer/Générer un décalage |
| Error resolved          | Erreur résolue              |
| No other func           | Pas d'autre fonction        |

**Figure 19 – Diagramme de transition d'état SFSPM**

Le Tableau 35 décrit les états présentés à la Figure 19.

**Tableau 35 – Liste des états**

| N° | Nom de l'état    | État                                                   | 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.<br>Pour la fonction auxiliaire exécutable, voir le Tableau 38, 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 la Figure 20). La connexion de sécurité est établie selon la procédure suivante:

- 1) SFSPM-M démarre. SFSPM-M envoie une demande d'établissement de connexion de sécurité à SFSPM-S en fonction de paramètres préalablement fournis.
- 2) SFSPM-S reçoit la demande d'établissement de connexion de sécurité de la part de SFSPM-M et envoie une réponse correspondante à SFSPM-M.
- 3) SFSPM-M reçoit la réponse d'établissement de connexion de sécurité de la part de SFSPM-S et, selon les informations de fonction auxiliaire convenue au moment de l'établissement de la connexion de sécurité, envoie une demande à SFSPM-S relative aux fonctions auxiliaires. SFSPM-M envoie une demande de confirmation de paramètre de réseau de sécurité à SFSPM-S concernant les fonctions auxiliaires.

- 4) SFSPM-S reçoit la demande de confirmation de paramètre de réseau de sécurité de la part de SFSPM-M, stocke les paramètres reçus et envoie une réponse de confirmation de paramètre de réseau de sécurité à SFSPM-M.
- 5) SFSPM-M reçoit la réponse de confirmation de paramètre de réseau de sécurité de la part de SFSPM-S et stocke les paramètres reçus.
- 6) Si la confirmation de paramètre de réseau de sécurité aboutit, SFSPM-M envoie une demande de vérification de paramètre de poste de sécurité à SFSPM-S.
- 7) SFSPM-S reçoit la demande de vérification de paramètre de poste de sécurité de la part de SFSPM-M et envoie la réponse correspondante à SFSPM-M, y compris les paramètres préalablement fournis.
- 8) SFSPM-M reçoit la réponse de vérification de paramètre de poste de sécurité de la part de SFSPM-S et vérifie si les paramètres de poste de sécurité sont corrects.
- 9) SFSPM-M vérifie que les paramètres de poste de sécurité sont corrects, et envoie et reçoit des réponses de manière ininterrompue tant que toutes les demandes relatives aux fonctions auxiliaires n'ont pas été formulées.
- 10) SFSPM-S reçoit de manière ininterrompue les demandes et envoie des réponses pendant la période où les demandes relatives aux fonctions auxiliaires continuent.
- 11) Une fois formulées toutes les demandes relatives aux fonctions auxiliaires, SFSPM-M envoie une demande de préparation de rafraîchissement et de mesurage du décalage à SFSPM-S.
- 12) SFSPM-S reçoit la demande de préparation de rafraîchissement et de mesurage du décalage de la part de SFSPM-M et envoie une réponse correspondante à SFSPM-M.
- 13) SFSPM-M reçoit la réponse de préparation de rafraîchissement et de mesurage du décalage, génère les informations exigées pour le calcul du décalage, et envoie une demande de rafraîchissement de sécurité et de génération de décalage à SFSPM-S, accompagnée des informations générées.
- 14) SFSPM-S reçoit la demande de rafraîchissement de sécurité et de génération de décalage de la part de SFSPM-M, génère un décalage en fonction des informations fournies et envoie une réponse de rafraîchissement de sécurité et de génération de décalage à SFSPM-M.
- 15) SFSPM-M lance le rafraîchissement de sécurité en envoyant une demande de rafraîchissement de sécurité et de génération de décalage et, à l'issue de l'intervalle de transmission, envoie une demande de rafraîchissement de sécurité.
- 16) SFSPM-S lance le rafraîchissement de sécurité en envoyant une réponse de rafraîchissement de sécurité et de génération de décalage et, à l'issue de l'intervalle de transmission, envoie une demande de rafraîchissement de sécurité.

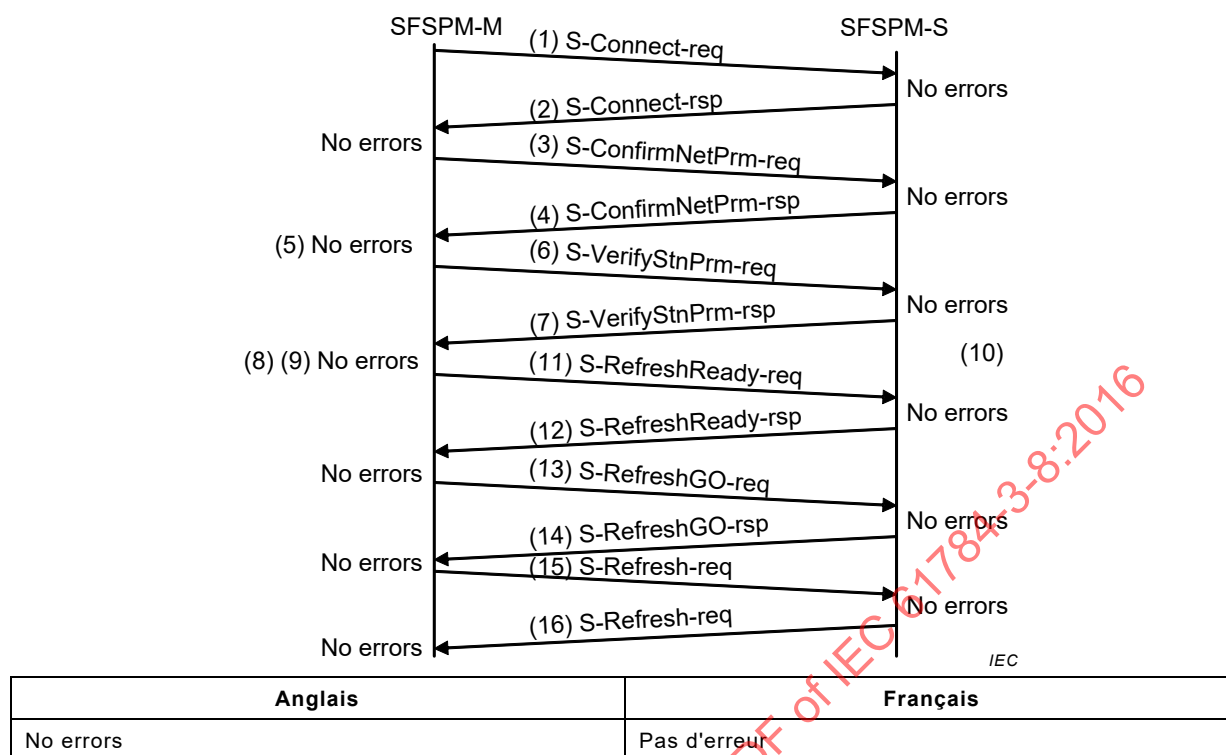


Figure 20 – Séquence d'établissement d'une connexion

#### 12.7.2.2.2 Rafraîchissement de sécurité

La Figure 21 présente 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.

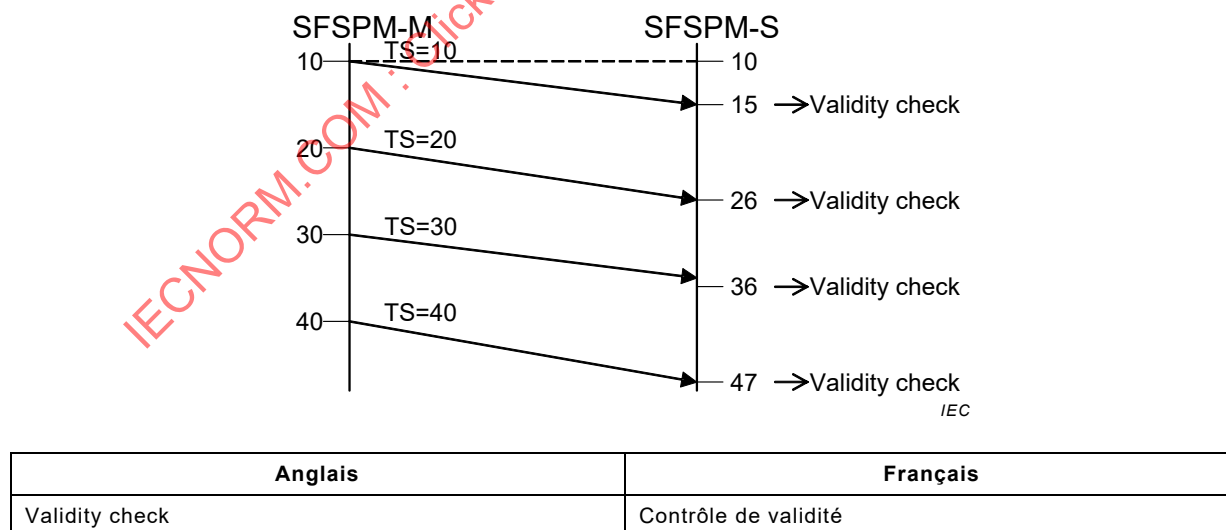


Figure 21 – Séquence de communication lors de la communication de rafraîchissement de sécurité

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.