# IEC 61784-3-12

Edition 1.1 2019-11

# CONSOLIDATED VERSION

# VERSION CONSOLIDÉE

colour inside

## Industrial communication networks – Profiles – Part 3-12: Functional safety fieldbuses – Additional specifications for CPF 12

## Réseaux de communication industriels – Profils – Partie 3-12: Bus de terrain de sécurité fonctionnelle – Spécifications supplémentaires pour CPF 12

IEC 61784-3-12:2010-06+AMD1:2019-11 CSV(en-fr)

Documents
Document Sharing Hub

Full document details: IEC 61784-3-12-2019

**THIS PUBLICATION IS COPYRIGHT PROTECTED**
**Copyright © 2019 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 Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

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

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

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 It also gives information on projects, replaced and withdrawn publications.

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

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

**Electropedia - www.electropedia.org**
The world's leading online dictionary on electrotechnology, containing more than 22 000 terminological entries in English and French, with equivalent terms in 16 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

**IEC Glossary - std.iec.ch/glossary**
67 000 electrotechnical terminology entries in English and French extracted from the Terms and definitions clause of IEC publications issued between 2002 and 2015. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

---

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

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

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

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

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

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

**Glossaire IEC - std.iec.ch/glossary**
67 000 entrées terminologiques électrotechniques, en anglais et en français, extraites des articles Termes et définitions des publications IEC parues entre 2002 et 2015. Plus certaines entrées antérieures extraites des publications des CE 37, 77, 86 et CISPR de l'IEC.

Documents
Document Sharing Hub

Full document details: IEC 61784-3-12-2019

# IEC 61784-3-12

Edition 1.1 2019-11

# CONSOLIDATED VERSION

# VERSION CONSOLIDÉE

colour inside

## Industrial communication networks – Profiles – Part 3-12: Functional safety fieldbuses – Additional specifications for CPF 12

## Réseaux de communication industriels – Profils – Partie 3-12: Bus de terrain de sécurité fonctionnelle – Spécifications supplémentaires pour CPF 12

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

ICS 25.040.40; 35.100.05

ISBN 978-2-8322-7994-6

**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.**

AVA Documents
Document Sharing Hub

® Registered trademark of the International Electrotechnical Commission
Marque déposée de la Commission Electrotechnique Internationale

Full document details: IEC 61784-3-12-2019

Documents
Document Sharing Hub

Full document details: IEC 61784-3-12-2019

# IEC 61784-3-12

Edition 1.1 2019-11

# REDLINE VERSION

# VERSION REDLINE

colour inside

## Industrial communication networks – Profiles – Part 3-12: Functional safety fieldbuses – Additional specifications for CPF 12

## Réseaux de communication industriels – Profils – Partie 3-12: Bus de terrain de sécurité fonctionnelle – Spécifications supplémentaires pour CPF 12

IEC 61784-3-12:2010-06+AMD1:2019-11 CSV(en-fr)

Documents
Document Sharing Hub

Full document details: IEC 61784-3-12-2019

CONTENTS

FOREWORD ..... 6
0 Introduction ..... 8
0.1 General ..... 8
0.2 Patent declaration ..... 10
INTRODUCTION to Amendment 1 ..... 10
1 Scope ..... 11
2 Normative references ..... 11
3 Terms, definitions, symbols, abbreviated terms and conventions ..... 12
3.1 Terms and definitions ..... 12
3.1.1 Common terms and definitions ..... 12
3.1.2 CPF 12: Additional terms and definitions ..... 17
3.2 Symbols and abbreviated terms ..... 17
3.2.1 Common symbols and abbreviated terms ..... 17
3.2.2 CPF 12: Additional symbols and abbreviated terms ..... 18
3.3 Conventions ..... 18
4 Overview of FSCP 12/1 (Safety-over-EtherCAT™) ..... 18
5 General ..... 20
5.1 External document providing specifications for the profile ..... 20
5.2 Safety functional requirements ..... 20
5.3 Safety measures ..... 21
5.4 Safety communication layer structure ..... 21
5.5 Relationships with FAL (and DLL, PhL) ..... 22
5.5.1 General ..... 22
5.5.2 Data types ..... 22
6 Safety communication layer services ..... 22
6.1 FSoE Connection ..... 22
6.2 FSoE Cycle ..... 22
6.3 FSoE services ..... 23
7 Safety communication layer protocol ..... 24
7.1 Safety PDU format ..... 24
7.1.1 Safety PDU structure ..... 24
7.1.2 Safety PDU command ..... 25
7.1.3 Safety PDU CRC ..... 25
7.2 FSCP 12/1 communication procedure ..... 29
7.2.1 Message cycle ..... 29
7.2.2 FSCP 12/1 node states ..... 29
7.3 Reaction on communication errors ..... 39
7.4 State table for FSoE Master ..... 40
7.4.1 FSoE Master state machine ..... 40
7.4.2 Reset state ..... 44
7.4.3 Session state ..... 45
7.4.4 Connection state ..... 48
7.4.5 Parameter state ..... 52
7.4.6 Data state ..... 55
7.5 State table for FSoE Slave ..... 58

AVA Documents
Document Sharing Hub
Full document details: IEC 61784-3-12-2019

7.5.1 FSoE Slave state machine ... 58
7.5.2 Reset state ... 62
7.5.3 Session state ... 64
7.5.4 Connection state ... 68
7.5.5 Parameter state ... 73
7.5.6 Data state ... 78
8 Safety communication layer management ... 81
8.1 FSCP 12/1 parameter handling ... 81
8.2 FSoE communication parameters ... 81
9 System requirements ... 82
9.1 Indicators and switches ... 82
9.1.1 Indicator states and flash rates ... 82
9.1.2 Indicators ... 83
9.2 Installation guidelines ... 84
9.3 Safety function response time ... 84
9.3.1 General ... 84
9.3.2 Determination of FSoE Watchdog time ... 85
9.3.3 Calculation of the worst case safety function response time ... 86
9.4 Duration of demands ... 87
9.5 Constraints for calculation of system characteristics ... 87
9.5.1 General ... 87
9.5.2 Probabilistic considerations ... 87
9.6 Maintenance ... 89
9.7 Safety manual ... 89
10 Assessment ... 89
Annex A (informative) Additional information for functional safety communication profiles of CPF 12 ... 90
Annex B (informative) Information for assessment of the functional safety communication profiles of CPF 12 ... 95
Bibliography ... 96

Figure 1 – Relationships of IEC 61784-3 with other standards (machinery) ... 8
Figure 2 – Relationships of IEC 61784-3 with other standards (process) ... 9
Figure 3 – Basic FSCP 12/1 system ... 19
Figure 4 – FSCP 12/1 software architecture ... 21
Figure 5 – FSoE Cycle ... 23
Figure 6 – FSCP 12/1 communication structure ... 23
Figure 7 – Safety PDU for CPF 12 embedded in Type 12 PDU ... 24
Figure 8 – FSCP 12/1 node states ... 30
Figure 9 – State diagram for FSoE Master ... 41
Figure 10 – State diagram for FSoE Slave ... 59
Figure 11 – Indicator flash rates ... 83
Figure 12 – Components of a safety function ... 84
Figure 13 – Calculation of the FSoE Watchdog times for input and output connections ... 85
Figure 14 – Calculation of the worst case safety function response time ... 86
Figure 15 – Safety PDU embedded in standard PDU ... 88
AVA Documents
Document Sharing Hub
Full document details: IEC 61784-3-12-2019

Figure 16 – Residual error rate for 8/16/24 bit safety data and up to 12 144 bit standard data ..... 89

Table 1 – State machine description elements ..... 18
Table 2 – Communication errors and detection measures ..... 21
Table 3 – General Safety PDU ..... 24
Table 4 – Shortest Safety PDU ..... 25
Table 5 – Safety PDU command ..... 25
Table 6 – CRC_0 calculation sequence ..... 26
Table 7 – CRC_i calculation sequence (i>0) ..... 26
Table 8 – Example for CRC_0 inheritance ..... 27
Table 9 – Example for 4 octets of safety data with interchanging of octets 1-4 with 5-8 ..... 28
Table 10 – Safety Master PDU for 4 octets of safety data with command = Reset after restart (reset connection) or error ..... 31
Table 11 – Safety Slave PDU for 4 octets of safety data with command = Reset for acknowledging a Reset command from the FSoE Master ..... 31
Table 12 – Safety Slave PDU for 4 octets of safety data with command = Reset after restart (reset connection) or error ..... 32
Table 13 – Safety Master PDU for 4 octets of safety data with command = Session ..... 32
Table 14 – Safety Slave PDU for 4 octets of safety data with command = Session ..... 33
Table 15 – Safety data transferred in the connection state ..... 34
Table 16 – Safety Master PDU for 4 octets of safety data in Connection state ..... 34
Table 17 – Safety Slave PDU for 4 octets of safety data in Connection state ..... 34
Table 18 – Safety data transferred in the parameter state ..... 35
Table 19 – First Safety Master PDU for 4 octets of safety data in parameter state ..... 35
Table 20 – First Safety Slave PDU for 4 octets of safety data in parameter state ..... 36
Table 21 – Second Safety Master PDU for 4 octets of safety data in parameter state ..... 36
Table 22 – Second Safety Slave PDU for 4 octets of safety data in parameter state ..... 37
Table 23 – Safety Master PDU for 4 octets of ProcessData in data state ..... 37
Table 24 – Safety Slave PDU for 4 octets of ProcessData in data state ..... 38
Table 25 – Safety Master PDU for 4 octets of fail-safe data in data state ..... 38
Table 26 – Safety Slave PDU for 4 octets of fail-safe data in data state ..... 39
Table 27 – FSoE communication error ..... 39
Table 28 – FSoE communication error codes ..... 40
Table 29 – States of the FSoE Master ..... 40
Table 30 – Events in the FSoE Master state table ..... 42
Table 31 – Functions in the FSoE Master state table ..... 42
Table 32 – Variables in the FSoE Master state table ..... 43
Table 33 – Macros in the FSoE Master state table ..... 43
Table 34 – States of the FSoE Slave ..... 58
Table 35 – Events in the FSoE Slave state table ..... 60
Table 36 – Functions in the FSoE Slave state table ..... 60
Table 37 – Variables in the FSoE Slave state table ..... 61
Table 38 – Macros in the FSoE Slave state table ..... 61

AVA Documents
Document Sharing Hub

Full document details: IEC 61784-3-12-2019

Table 39 – FSoE Communication parameters ..... 82
Table 40 – Indicator States ..... 82
Table 41 – FSoE STATUS indicator states ..... 83
Table 42 – Definition of times ..... 85

Documents
Document Sharing Hub

Full document details: IEC 61784-3-12-2019

INTERNATIONAL ELECTROTECHNICAL COMMISSION

# INDUSTRIAL COMMUNICATION NETWORKS – PROFILES –

## Part 3-12: Functional safety fieldbuses – Additional specifications for CPF 12

## FOREWORD

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

**DISCLAIMER**
**This Consolidated version is not an official IEC Standard and has been prepared for user convenience. Only the current versions of the standard and its amendment(s) are to be considered the official documents.**

**This Consolidated version of IEC 61784-3-12 bears the edition number 1.1. It consists of the first edition (2010-06) [documents 65C/591A/FDIS and 65C/603/RVD] and its amendment 1 (2019-11) [documents 65C/960/CDV and 65C/980/RVC]. The technical content is identical to the base edition and its amendment.**

**In this Redline version, a vertical line in the margin shows where the technical content is modified by amendment 1. Additions are in green text, deletions are in strikethrough red text. A separate Final version with all changes accepted is available in this publication.**

Documents
Document Sharing Hub

Full document details: IEC 61784-3-12-2019

International Standard IEC 61784-3-12 has been prepared by subcommittee 65C: Industrial networks, of IEC technical committee 65: Industrial process measurement, control and automation.

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 the base publication and its amendment 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.**

Documents
Document Sharing Hub

Full document details: IEC 61784-3-12-2019

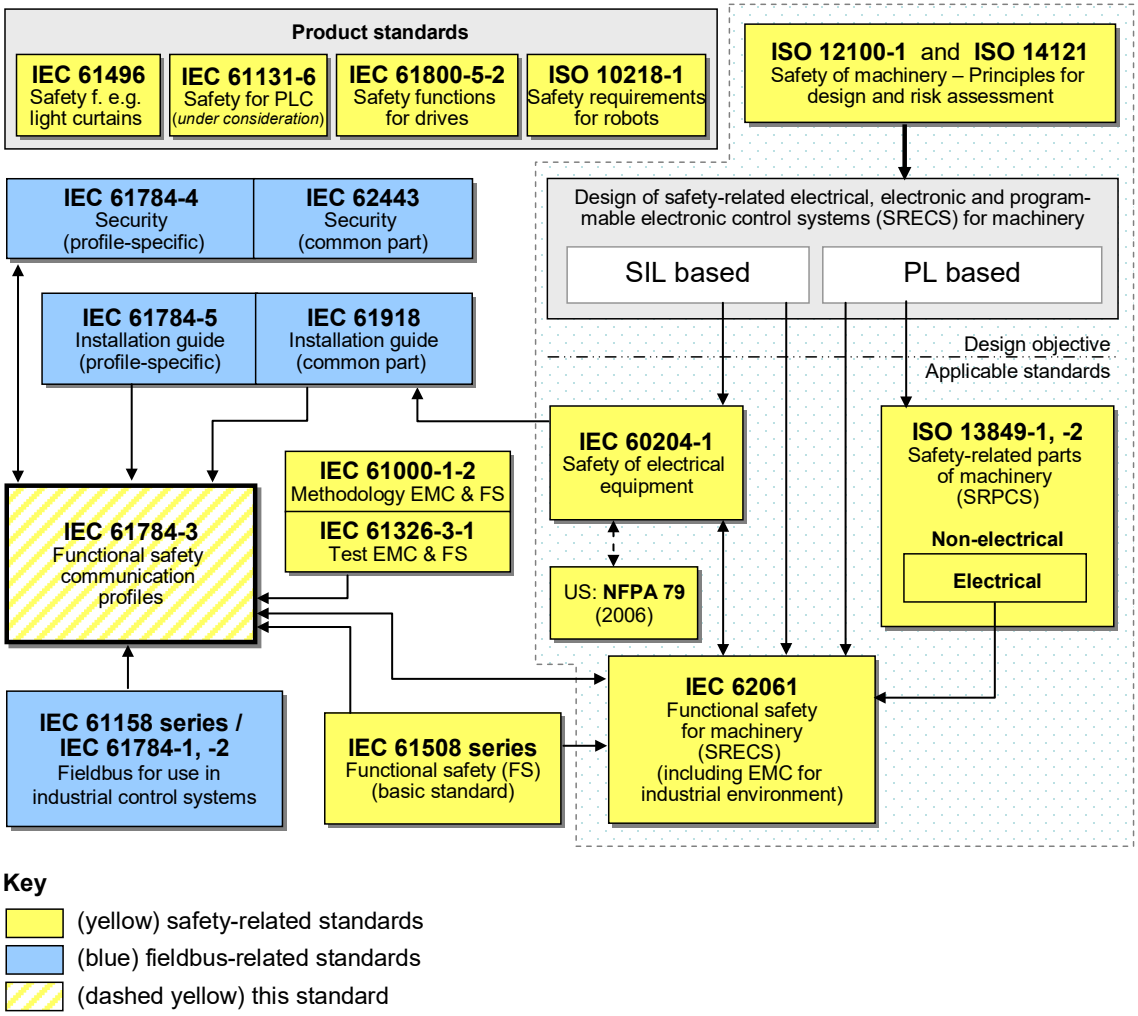
# 0 Introduction

## 0.1 General

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

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

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

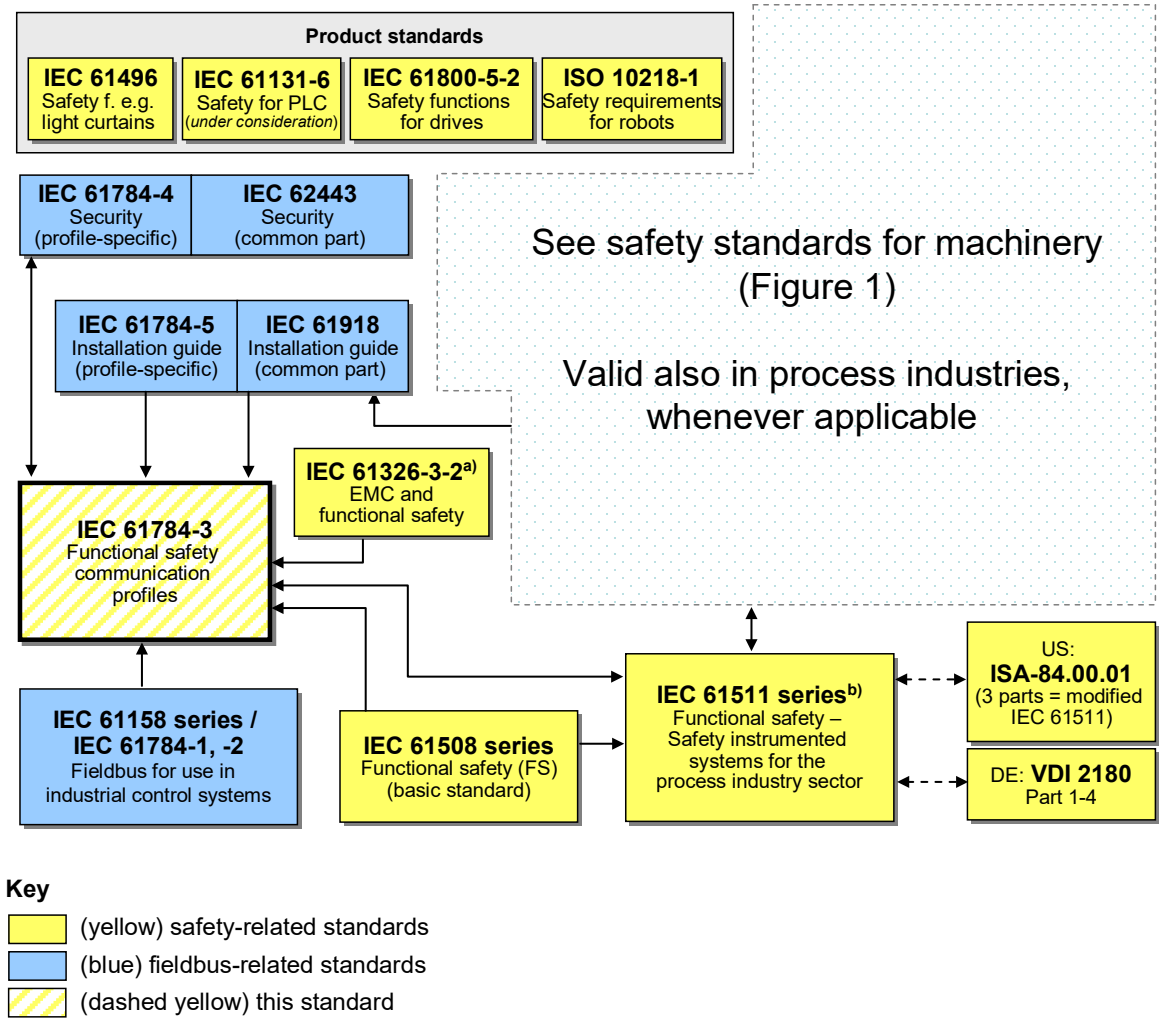



NOTE Subclauses 6.7.6.4 (high complexity) and 6.7.8.1.6 (low complexity) of IEC 62061 specify the relationship between PL (Category) and SIL.

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

Documents
Document Sharing Hub
Full document details: IEC 61784-3-12-2019

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




a For specified electromagnetic environments; otherwise IEC 61326-3-1.

b EN ratified.

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

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

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

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

Documents
Document Sharing Hub
Full document details: IEC 61784-3-12-2019

This standard describes:

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

— individual description of functional safety profiles for several communication profile families in IEC 61784-1 and IEC 61784-2;

— safety layer extensions to the communication service and protocols sections of the IEC 61158 series.

## 0.2 Patent declaration

The International Electrotechnical Commission (IEC) draws attention to the fact that it is claimed that compliance with this document may involve the use of patents concerning the functional safety communication profiles for family 12 as follows, where the [xx] notation indicates the holder of the patent right:

| | | |
|---|---|---|
| DE 10 2004 044 764.0 | [BE] | Datenübertragungsverfahren und Automatisierungssystem zum Einsatz eines solchen Datenübertragungsverfahrens |
| EP 05 733 921.0 | [BE] | Sicherheitssteuerung |

IEC takes no position concerning the evidence, validity and scope of these patent rights.

The holders of these patents rights have assured the IEC that they are willing to negotiate licences under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statement of the holders of these patent rights are registered with IEC.

Information may be obtained from:

[BE] Beckhoff Automation GmbH
Eiserstrasse 5, 33415 Verl
GERMANY

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

## INTRODUCTION to Amendment 1

This Amendment 1 corrects technical errors in state tables for the FSoE Slave.

- Correct invalid value for the “bNew” parameter of SendFrame in transitions RESET_OK (Reset state), SESSION_STAY2 (Session state), CONN_RESET2 (Connection state), PARA_RESET2 (Parameter state), and DATA_RESET2 (Data state). This parameter shall only be set to “FALSE” in all back-to-reset-transitions when all values are set to their defaults.
- Add missing action in Transition SESSION_FAIL5 (Session state).
- Correct invalid value for the address parameter of STORE_DATA in transition CONN_STAY1 (Connection state).

Documents
Document Sharing Hub
Full document details: IEC 61784-3-12-2019

© IEC 2019

# INDUSTRIAL COMMUNICATION NETWORKS – PROFILES –

## Part 3-12: Functional safety fieldbuses – Additional specifications for CPF 12

## 1 Scope

This part of the IEC 61784-3 series specifies a safety communication layer (services and protocol) based on CPF 12 of IEC 61784-2 and IEC 61158 Type 12. It identifies the principles for functional safety communications defined in IEC 61784-3 that are relevant for this safety communication layer.

NOTE 1 It does not cover electrical safety and intrinsic safety aspects. Electrical safety relates to hazards such as electrical shock. Intrinsic safety relates to hazards associated with potentially explosive atmospheres.

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

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

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

## 2 Normative references

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

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

IEC 61000-6-2, *Electromagnetic compatibility (EMC) – Part 6-2: Generic standards – Immunity for industrial environments*

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

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

IEC 61158-3-12, *Industrial communication networks – Fieldbus specifications – Part 3-12: Data-link layer service definition – Type 12 elements*

---

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

[2] In the following pages of this standard, “IEC 61508” will be used for “IEC 61508 series”.

Documents
Document Sharing Hub

Full document details: IEC 61784-3-12-2019

IEC 61158-4-12, *Industrial communication networks – Fieldbus specifications – Part 4-12: Data-link layer protocol specification – Type 12 elements*

IEC 61158-5-12, *Industrial communication networks – Fieldbus specifications – Part 5-12: Application layer service definition – Type 12 elements*

IEC 61158-6-12, *Industrial communication networks – Fieldbus specifications – Part 6-12: Application layer protocol specification – Type 12 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 61784-2, *Industrial communication networks – Profiles – Part 2: Additional fieldbus profiles for real-time networks based on ISO/IEC 8802-3*

IEC 61784-3:2010[3], *Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions*

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

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

### 3.1 Terms and definitions

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

#### 3.1.1 Common terms and definitions

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

**3.1.1.2**
**black channel**
*communication channel* without available evidence of design or validation according to IEC 61508

**3.1.1.3**
**communication channel**
logical connection between two end-points within a *communication system*

[3] In preparation.

Documents
Document Sharing Hub
Full document details: IEC 61784-3-12-2019

**3.1.1.4**
**communication system**
arrangement of hardware, software and propagation media to allow the transfer of *messages* (ISO/IEC 7498 application layer) from one application to another

**3.1.1.5**
**connection**
logical binding between two application objects within the same or different devices

**3.1.1.6**
**Cyclic Redundancy Check (CRC)**
<value> redundant data derived from, and stored or transmitted together with, a block of data in order to detect data corruption

<method> procedure used to calculate the redundant data

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

NOTE 2 See also [34], [35][4].

**3.1.1.7**
**error**
discrepancy between a computed, observed or measured value or condition and the true, specified or theoretically correct value or condition

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

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

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

**3.1.1.8**
**failure**
termination of the ability of a functional unit to perform a required function or operation of a functional unit in any way other than as required

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

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

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

**3.1.1.9**
**fault**
abnormal condition that may cause a reduction in, or loss of, the capability of a functional unit to perform a required function

NOTE IEV 191-05-01 defines “fault” as a state characterized by the inability to perform a required function, excluding the inability during preventive maintenance or other planned actions, or due to lack of external resources.

[IEC 61508-4:2010, modified], [ISO/IEC 2382-14.01.10, modified]

---

4 Figures in square brackets refer to the bibliography.

5 To be published.

Documents
Document Sharing Hub

Full document details: IEC 61784-3-12-2019

**3.1.1.10**
**fieldbus**
*communication system* based on serial data transfer and used in industrial automation or process control applications

**3.1.1.11**
**fieldbus system**
system using a *fieldbus* with connected devices

**3.1.1.12**
**frame**
denigrated synonym for DLPDU

**3.1.1.13**
**Frame Check Sequence (FCS)**
redundant data derived from a block of data within a DLPDU (frame), using a hash function, and stored or transmitted together with the block of data, in order to detect data corruption

NOTE 1 An FCS can be derived using for example a CRC or other hash function.

NOTE 2 See also [34], [35].

**3.1.1.14**
**hash function**
(mathematical) function that maps values from a (possibly very) large set of values into a (usually) smaller range of values

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

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

[IEC/TR 62210, modified]

**3.1.1.15**
**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

**3.1.1.16**
**master**
active communication entity able to initiate and schedule communication activities by other stations which may be masters or slaves

**3.1.1.17**
**message**
ordered series of octets intended to convey information
[ISO/IEC 2382-16.02.01, modified]

**3.1.1.18**
**performance level (PL)**
discrete level used to specify the ability of safety-related parts of control systems to perform a safety function under foreseeable conditions
[ISO 13849-1]

**3.1.1.19**
**protective extra-low-voltage (PELV)**
electrical circuit in which the voltage cannot exceed a.c. 30 V r.m.s., 42,4 V peak or d.c. 60 V in normal and single-fault condition, except earth faults in other circuits

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

Documents
Document Sharing Hub
Full document details: IEC 61784-3-12-2019

[IEC 61131-2]

**3.1.1.20**
**redundancy**
existence of means, in addition to the means which would be sufficient for a functional unit to perform a required function or for data to represent information

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

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

**3.1.1.21**
**reliability**
probability that an automated system can perform a required function under given conditions for a given time interval (t1,t2)

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

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

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

NOTE 4 Reliability differs from availability.

[IEC 62059-11, modified]

**3.1.1.22**
**risk**
combination of the probability of occurrence of harm and the severity of that harm

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

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

**3.1.1.23**
**safety communication layer (SCL)**
communication layer that includes all the necessary measures to ensure safe transmission of data in accordance with the requirements of IEC 61508

**3.1.1.24**
**safety data**
data transmitted across a safety network using a safety protocol

NOTE The Safety Communication Layer does not ensure safety of the data itself, only that the data is transmitted safely.

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

**3.1.1.26**
**safety extra-low-voltage (SELV)**
electrical circuit in which the voltage cannot exceed a.c. 30 V r.m.s., 42,4 V peak or d.c. 60 V in normal and single-fault condition, including earth faults in other circuits

NOTE An SELV circuit is not connected to protective earth.

6 To be published.

Documents
Document Sharing Hub
Full document details: IEC 61784-3-12-2019

[IEC 61131-2]

**3.1.1.27**
**safety function**
function to be implemented by an E/E/PE safety-related system or other risk reduction measures, that is intended to achieve or maintain a safe state for the EUC, in respect of a specific hazardous event

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

[IEC 61508-4:2010, modified]

**3.1.1.28**
**safety function response time**
worst case elapsed time following an actuation of a safety sensor connected to a fieldbus, before the corresponding safe state of its safety actuator(s) is achieved in the presence of errors or failures in the safety function channel

NOTE This concept is introduced in IEC 61784-3:2010[7], 5.2.4 and addressed by the functional safety communication profiles defined in this part.

**3.1.1.29**
**safety integrity level (SIL)**
discrete level (one out of a possible four), corresponding to a range of safety integrity values, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest

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

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

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

[IEC 61508-4:2010]

**3.1.1.30**
**safety measure**
<this standard> measure to control possible communication *errors* that is designed and implemented in compliance with the requirements of IEC 61508

NOTE 1 In practice, several safety measures are combined to achieve the required safety integrity level.

NOTE 2 Communication *errors* and related safety measures are detailed in IEC 61784-3:2010, 5.3 and 5.4.

**3.1.1.31**
**safety-related application**
programs designed in accordance with IEC 61508 to meet the SIL requirements of the application

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

---

7 In preparation.

8 To be published.

Documents
Document Sharing Hub

Full document details: IEC 61784-3-12-2019

**3.1.1.33**
**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

### 3.1.2 CPF 12: Additional terms and definitions

**3.1.2.1**
**fail-safe data**
expression for data that are set to a predefined value in case of initialization or error

NOTE In this part, the value of the fail-safe data should always be set to "0".

**3.1.2.2**
**FSoE Connection**
unique relationship between the FSoE Master and an FSoE Slave

**3.1.2.3**
**FSoE Cycle**
communication cycle with one Safety Master PDU and the corresponding Safety Slave PDU

**3.1.2.4**
**SafeInput**
safety process data transferred from the FSoE Slave to the FSoE Master

**3.1.2.5**
**SafeOutput**
safety process data transferred from the FSoE Master to the FSoE Slave

**3.1.2.6**
**Safety Master PDU**
safety PDU transferred from the FSoE Master to the FSoE Slave

**3.1.2.7**
**Safety Slave PDU**
safety PDU transferred from the FSoE Slave to the FSoE Master

## 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] |
| FCS | Frame Check Sequence | |
| FS | Functional Safety | |
| FSCP | Functional Safety Communication Profile | |
| MTBF | Mean Time Between Failures | |
| MTTF | Mean Time To Failure | |
| PDU | Protocol Data Unit | [ISO/IEC 7498-1] |

Documents
Document Sharing Hub
Full document details: IEC 61784-3-12-2019

| | | |
|---|---|---|
| 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] |

### 3.2.2 CPF 12: Additional symbols and abbreviated terms

| | | |
|---|---|---|
| ASIC | Application specific integrated circuit | |
| FSoE | Failsafe over CPF 12 | |
| ID | Identifier | |
| UML | Unified Modeling Language | [ISO/IEC 19501] |

## 3.3 Conventions

The conventions used for the descriptions of objects services and protocols are described in IEC 61158-3-12, IEC 61158-4-12, IEC 61158-5-12 and IEC 61118-6-12.

As appropriate, this part uses flow charts and UML Sequence Diagrams to describe concepts.

In state diagrams states are represented as boxes, state transitions are shown as arrows. Names of states and transitions of the state diagram correspond to the names in the textual listing of the state transitions.

The textual listing of the state transitions is structured as follows, see also Table 1.

The first row contains the name of the transition. The second row contains the condition for the transition. The third row contains the action(s) that shall take place. The last row contains the next state.

**Table 1 – State machine description elements**

| Transition | Condition | Action | Next State |
|---|---|---|---|
| | | | |

Each state with its transitions is described in a separate subclause. For each event that can occur in a state a separate subclause is inserted.

# 4 Overview of FSCP 12/1 (Safety-over-EtherCAT™)

Communication Profile Family 12 (commonly known as EtherCAT™[9]) defines communication profiles based on IEC 61158-2 Type 12, IEC 61158-3-12, IEC 61158-4-12, IEC 61158-5-12 and IEC 61158-6-12.

[9] EtherCAT™ and Safety-over-EtherCAT™ are trade names of Beckhoff, Verl. 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 EtherCAT™ or Safety-over-EtherCAT™. Use of the trade names EtherCAT™ or Safety-over-EtherCAT™ requires permission of Beckhoff, Verl.

AVA Documents
Document Sharing Hub
Full document details: IEC 61784-3-12-2019

The basic profile(s) CP 12/1 and CP 12/2 are defined in IEC 61784-2. The CPF 12 functional safety communication profile FSCP 12/1 (Safety-over-EtherCAT™[9]) is based on the CPF 12 basic profiles in IEC 61784-2 and the safety communication layer specifications defined in this part.

FSCP 12/1 describes a protocol for transferring safety data up to SIL3 between FSCP 12/1 devices. Safety PDUs are transferred by a subordinate fieldbus that is not included in the safety considerations, since it can be regarded as a black channel. The Safety PDU exchanged between two communication partners is regarded by the subordinate fieldbus as process data that are exchanged cyclically.

FSCP 12/1 uses a unique master/slave relationship between the FSoE Master and an FSoE Slave; it is called FSoE Connection (Figure 3).In the FSoE Connection, each device only returns its own new message once a new message has been received from the partner device. The complete transfer path between FSoE Master and FSoE Slave is monitored by a separate watchdog timer on both devices, in each FSoE Cycle.

The FSoE Master can handle more than one FSoE Connection to support several FSoE Slaves.

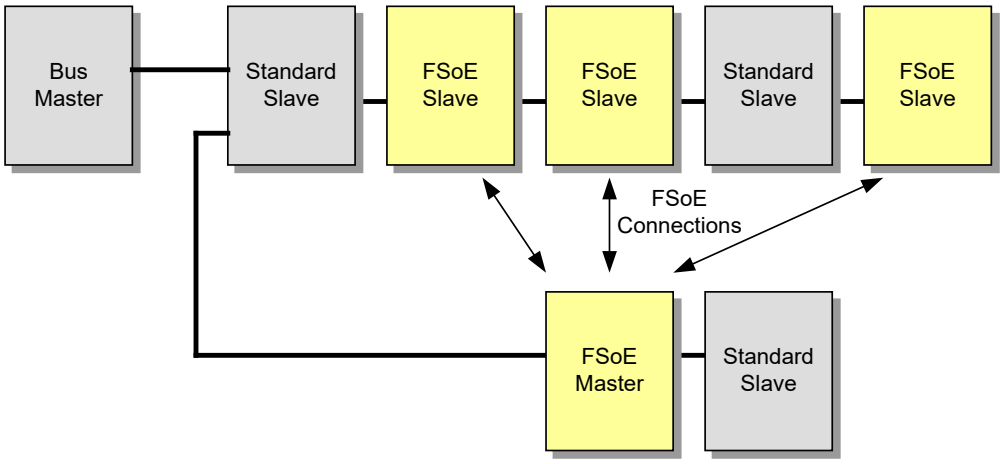



**Figure 3 – Basic FSCP 12/1 system**

The integrity of the safety data transfers is ensured as follows:

— session-number for detecting buffering of a complete startup sequence;

— sequence number for detecting interchange, repetition, insertion or loss of whole messages;

— unique connection identification for safely detecting misrouted messages via a unique address relationship;

— watchdog monitoring for safely detecting delays not allowed on the communication path

— cyclic redundancy checking for data integrity for detecting message corruption from source to sink.

State transitions are initiated by the FSoE Master and acknowledged by the FSoE Slave. The FSoE state machine also involves exchange and checking of information for the communication relation.

Documents
Document Sharing Hub
Full document details: IEC 61784-3-12-2019

# 5 General

## 5.1 External document providing specifications for the profile

The following document is useful in understanding the design of FSCP 12/1 protocol:

- GS-ET-26 [33]

## 5.2 Safety functional requirements

The following requirements shall apply to the development of devices that implement the FSCP 12/1 protocol. The same requirements were used in the development of FSCP 12/1.

- The FSCP 12/1 protocol is designed to support Safety Integrity Level 3 (SIL 3) (see IEC 61508).
- Implementations of FSCP 12/1 shall comply with IEC 61508.
- The basic requirements for the development of the FSCP 12/1 protocol are defined in IEC 61784-3.
- FSCP 12/1 protocol is implemented using a black channel approach; there is no safety related dependency on the standard CPF 12 communication profiles. Transmission equipment such as controllers, ASICs, links, couplers, etc. shall remain unmodified.
- Environmental conditions shall be according to general automation requirements mainly IEC 61326-3-1 for the safety margin tests, unless there are specific product standards.
- Safety communication and non safety relevant communication shall be independent. However, non safety relevant devices and safety devices shall be able to use the same communication channel.
- Implementation of the FSCP 12/1 protocol shall be restricted to the communication end devices (FSoE Master and FSoE Slave).
- There shall always be a 1:1 communication relationship between an FSoE Slave and its FSoE Master.
- The safety communication shall not restrict the minimum cycle time of the communication system.

Documents
Document Sharing Hub
Full document details: IEC 61784-3-12-2019

### 5.3 Safety measures

The safety measures used in the FSCP 12/1 to detect communication errors are listed in Table 2. The safety measures shall be processed and monitored within each safety device.

**Table 2 – Communication errors and detection measures**

| Communication errors | Safety measures | | | | |
|---|---|---|---|---|---|
| | Sequence number (see 7.1.3.4) | Time expectation (see 6.2) [a] | Connection authentication (see 7.2.2.4) [b] | Feedback Message (see 7.2.1) | Data integrity assurance (see 7.1.3) |
| Corruption | | | | | X |
| Unintended repetition | X | | | | X |
| Incorrect sequence | X | | | | X |
| Loss | X | X | | X | X |
| Unacceptable delay | | X | | X | X |
| Insertion | X | | | | X |
| Masquerade | | X | | X | X |
| Addressing | | | X | | |
| Revolving memory failures within switches | X | | | | X |

[a] In this standard the instance is called "FSoE Watchdog".

[b] In this standard the instance is called "FSoE Connection ID".

### 5.4 Safety communication layer structure

The FSCP 12/1 protocol is layered on top of the standard network protocol. Figure 4 shows how the protocol is related to the CPF 12 layer. The safety layer accept safety data from the safety-related application and transfers these data via the FSCP 12/1 protocol.

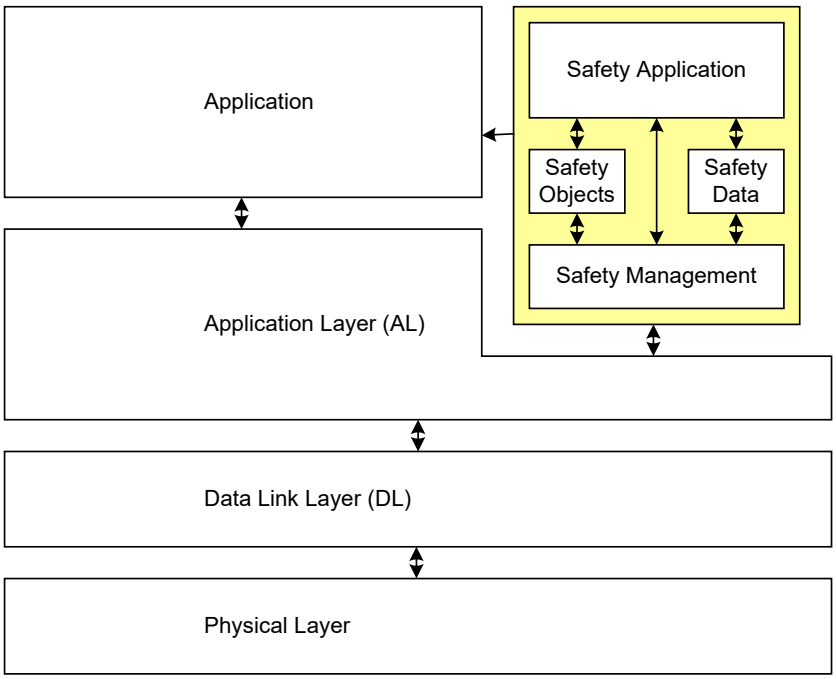



**Figure 4 – FSCP 12/1 software architecture**

Documents
Document Sharing Hub
Full document details: IEC 61784-3-12-2019

A safety PDU containing the safety data and the required error detection measures is included in the communication process data objects (PDO). The mapping in the process data of the communication system and the start-up of the communication state machine is not part of the safety protocol.

The calculation of the residual error probability for the FSCP 12/1 protocol takes no credit of the error detection mechanisms of the communication system. This means that the protocol can also be transferred via other communication systems. Any transmission link can be used, including fieldbus systems, Ethernet or similar transfer routes, optical fibre cables, copper cables, or even radio links.

### 5.5 Relationships with FAL (and DLL, PhL)

#### 5.5.1 General

This safety communication layer is designed to be used in conjunction with CPF 12 communication profiles. But it is not restricted to this communication profile.

#### 5.5.2 Data types

Profiles defined in this part support all the CPF 12 data types as defined in IEC 61158-5-12.

## 6 Safety communication layer services

### 6.1 FSoE Connection

The connection between two FSCP 12/1 communication partners (FSCP 12/1 nodes) is referred to as FSoE Connection. In an FSoE Connection one communication partner is always the FSoE Master, the other one the FSoE Slave.

The FSoE Master initialises the FSoE Connection after power-on or after a communication fault, while the FSoE Slave is limited to responses. The FSoE Master sets the safety-related communication parameters and optionally the safety-related application parameters of the FSoE Slave.

The safety process data transferred from the FSoE Master to the FSoE Slave are referred to as SafeOutputs. The safety data transferred from the FSoE Slave to the FSoE Master are referred to as SafeInputs.

The Safety PDU transferred from the FSoE Master to the FSoE Slave is referred to as Safety Master PDU. The Safety PDU transferred from the FSoE Slave to the FSoE Master is referred to as Safety Slave PDU.

### 6.2 FSoE Cycle

The FSoE Master sends the Safety Master PDU to the FSoE Slave and starts the FSoE Watchdog.

After checking the integrity of the Safety PDU, the FSoE Slave transfers the SafeOutputs to the Safety Application. It calculates the Safety Slave PDU with the SafeInputs from the Safety Application and sends this PDU to the FSoE Master. The FSoE Slave also starts its FSoE watchdog. This is shown in Figure 5.

After receiving a valid Safety Slave PDU an FSoE Cycle is finished.

Documents
Document Sharing Hub
Full document details: IEC 61784-3-12-2019

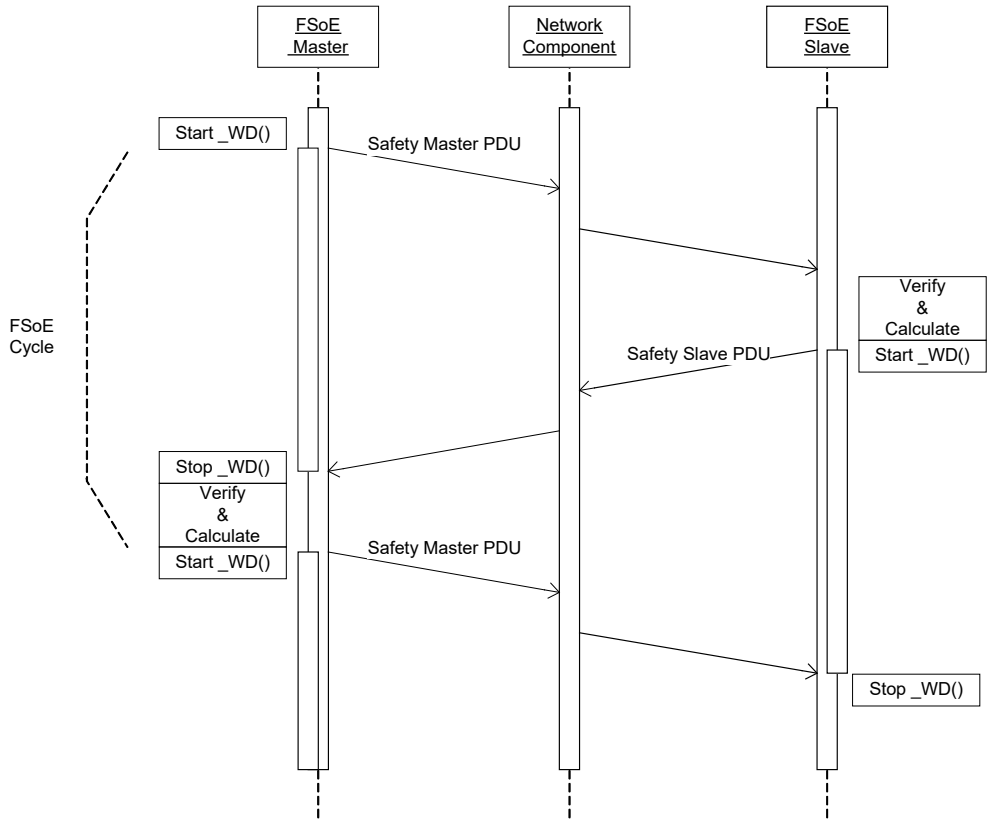



**Figure 5 – FSoE Cycle**

## 6.3 FSoE services

For each FSoE Connection, the FSoE Master shall support an FSoE Master handler to control the associated FSoE Slave.

For FSoE Master to FSoE Master Communication, the FSoE Master should support one or several FSoE Slave handler. Figure 6 shows the possible FSoE functionalities in the FSoE Master and FSoE Slave devices.

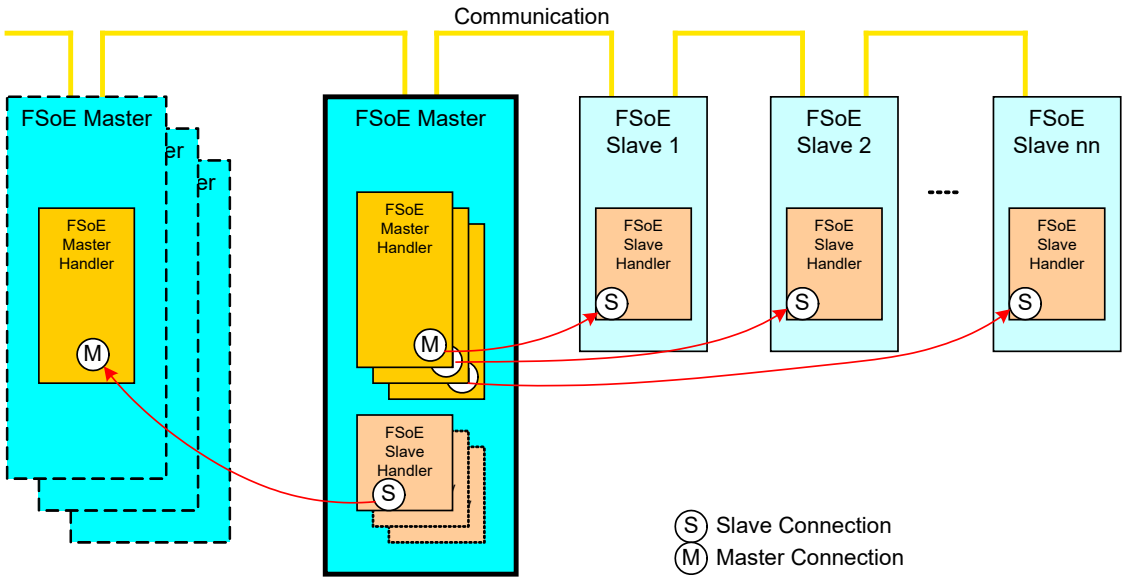



**Figure 6 – FSCP 12/1 communication structure**

Documents
Document Sharing Hub
Full document details: IEC 61784-3-12-2019

# 7 Safety communication layer protocol

## 7.1 Safety PDU format

### 7.1.1 Safety PDU structure

Figure 7 shows the structure of one safety PDU embedded in a Type 12 PDU. In Table 3 the general structure of the Safety PDU is listed.

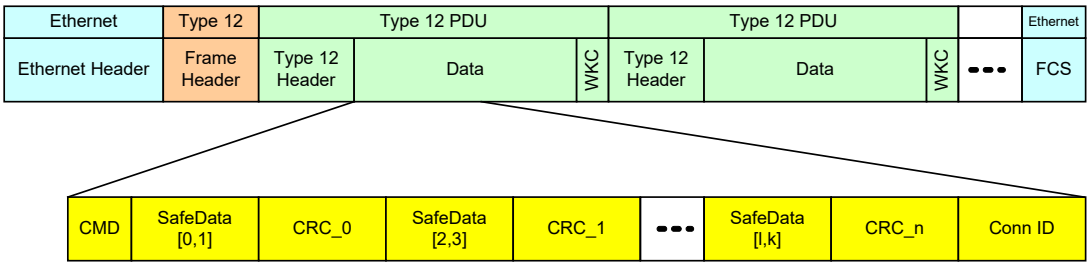



**Figure 7 – Safety PDU for CPF 12 embedded in Type 12 PDU**

The Safety PDU is cyclically transferred via the subordinate fieldbus. Each FSCP 12/1 node detects a new Safety PDU if at least one bit within the Safety PDU has changed.

The Safety PDU has a variable length specified in the device description of the FSoE Slave. The safety data length can be 1 octet or an even number of octets. The safety data length can be different in input and output direction.

The shorter of the two safety data lengths in the Safety Master PDU and the Safety Slave PDU determines how many safety data are used during the initialisation phase of the FSoE Connection with parameter information. In the longer of the two PDUs the remaining safety data are assigned zero.

**Table 3 – General Safety PDU**

| Octet | Name | Description |
|---|---|---|
| 0 | Command | Command |
| 1 | SafeData[0] | safety data, octet 0 |
| 2 | SafeData[1] | safety data, octet 1 |
| 3 | CRC_0_Lo | low octet (bits 0-7) of the 16-bit CRC_0 |
| 4 | CRC_0_Hi | high octet (bits 8-15) of the 16-bit CRC_0 |
| 5 | SafeData[2] | safety data, octet 2 |
| 6 | SafeData[3] | safety data, octet 3 |
| 7 | CRC_1_Lo | low octet (bits 0-7) of the 16-bit CRC_1 |
| 8 | CRC_1_Hi | high octet (bits 8-15) of the 16-bit CRC_1 |
| … | … | … |
| (n-1) × 2-1 | SafeData[n-2] | safety data, octet n-2 |
| (n-1) × 2 | SafeData[n-1] | safety data, octet n-1 |
| (n-1) × 2+1 | CRC_(n-2)/2_Lo | low octet (bits 0-7) of the 16-bit CRC_(n-2)/2 |
| (n-1) × 2+2 | CRC_(n-2)/2_Hi | high octet (bits 8-15) of the 16-bit CRC_(n-2)/2 |
| (n-1) × 2+3 | Conn_Id_Lo | unique connection ID, low octet |
| (n-1) × 2+4 | Conn_Id_Hi | unique connection ID, high octet |

Documents
Document Sharing Hub
Full document details: IEC 61784-3-12-2019

The Safety PDU can transfer n safety data octets. Two octets of data are transferred by a 2-octet CRC.

The shortest Safety PDU consists of 6 octets, which can be used to transfer 1 octet of safety data, as shown in Table 4.

**Table 4 – Shortest Safety PDU**

| Octet | Name | Description |
|---|---|---|
| 0 | Command | Command |
| 1 | SafeData[0] | safety data, octet 0 |
| 2 | CRC_0_Lo | low octet (bits 0-7) of the 16-bit CRC_0 |
| 3 | CRC_0_Hi | high octet (bits 8-15) of the 16-bit CRC_0 |
| 4 | Conn_Id_Lo | unique connection ID, low octet |
| 5 | Conn_Id_Hi | unique connection ID, high octet |

### 7.1.2 Safety PDU command

The Safety PDU command determines the meaning of the safety data based on the scheme shown in Table 5.

**Table 5 – Safety PDU command**

| Command | Description |
|---|---|
| 0x36 | ProcessData |
| 0x2A | Reset |
| 0x4E | Session |
| 0x64 | Connection |
| 0x52 | Parameter |
| 0x08 | FailSafeData |

### 7.1.3 Safety PDU CRC

#### 7.1.3.1 CRC calculation

Two octets of safety data are transferred by a corresponding two octet CRC.

In addition to the transferred data (command, data, ConnID), the CRC_0 of the Safety PDU also includes a virtual sequence number, the CRC_0 of the last received Safety PDU and three additional zero octets. If only one octet safety data is transferred, the SafeData[1] is skipped in the calculation.

```
CRC_0 :=     f(received CRC_0, ConnID, Sequence_Number, command, SafeData[0],
               SafeData[1], 0x000000)
```

Table 6 shows the calculation sequence for CRC_0.

Documents
Document Sharing Hub
Full document details: IEC 61784-3-12-2019

**Table 6 – CRC_0 calculation sequence**

| Step | Argument |
|---|---|
| 1 | received CRC_0 (bit 0-7) |
| 2 | received CRC_0 (bit 8-15) |
| 3 | ConnID (bit 0-7) |
| 4 | ConnID (bit 8-15) |
| 5 | Sequence_Number (bit 0-7) |
| 6 | Sequence_Number (bit 8-15) |
| 7 | Command |
| 8 | SafeData[0] |
| 9 | SafeData[1] |
| 10 | 0 |
| 11 | 0 |
| 12 | 0 |

The CRC_i (0 < i <= ((n-2)/2)) of the Safety PDU additionally includes the index i of the CRC.

```
CRC_i :=      f(received CRC_0, ConnID, Sequence_Number, command, i,
              SafeData[i × 2], SafeData[i × 2 + 1], 0)
```

Table 7 shows the calculation sequence for CRC_i.

**Table 7 – CRC_i calculation sequence (i>0)**

| Step | Argument |
|---|---|
| 1 | received CRC_0 (bit 0-7) |
| 2 | received CRC_0 (bit 8-15) |
| 3 | ConnID (bit 0-7) |
| 4 | ConnID (bit 8-15) |
| 5 | Sequence_Number (bit 0-7) |
| 6 | Sequence_Number (bit 8-15) |
| 7 | Command |
| 8 | Index i (bit 0-7) |
| 9 | Index i (bit 8-15) |
| 10 | SafeData[2 × i] |
| 11 | SafeData[2 × I + 1] |
| 12 | 0 |
| 13 | 0 |
| 14 | 0 |

#### 7.1.3.2 CRC polynomial selection

The polynomial 0x139B7 is used for calculating the CRCs and is referred to as the Safety polynomial.

In order to allow the Safety PDU to be transported via a black channel whose transfer characteristics are not included in the safety considerations, a bit fault rate of $10^{-2}$ shall be

AVA Documents
Document Sharing Hub
Full document details: IEC 61784-3-12-2019

used for determining the residual error probability. The residual error probability shall not exceed $10^{-9}$.

Safety is ensured based on the FSoE Master and the FSoE Slave switching to the reset state (i.e. safe state) as soon as an error is detected.

All CRC calculation factors except safety data have a fixed expected value, so that only safety data have to be considered in the calculation of the residual error probability.

The mathematical proof showing that the residual error probability with the Safety polynomial for 16-bit safety data and a bit fault rate of $10^{-2}$ does not exceed $10^{-9}$ is included in separate document covering quantitative fault detection.

#### 7.1.3.3 CRC inheritance

Inclusion (inheritance) of the CRC_0 of the last received telegram in the CRC calculation ensures that two consecutive Safety Master PDUs or Safety Slave PDUs differ, even if the other data remain unchanged.

Inheritance of CRC_0 also ensures safe and consistent transfer of data that are distributed over several Type 12 PDUs due to their length.

The CRC_0 of the received Safety PDU is included in the calculation of all CRC_i for the Safety PDU to be sent.

Table 8 shows an example for CRC_0 inheritance.

**Table 8 – Example for CRC_0 inheritance**

| FSoE Cycle | FSoE Master | | FSoE Slave | |
|---|---|---|---|---|
| | old CRC_0 | new CRC_0 | old CRC_0 | new CRC_0 |
| j-1 | CRC_0 (2 × j - 3) | CRC_0 (2 × j - 2) | CRC_0 (2 × j - 2) | CRC_0 (2 × j - 1) |
| j | CRC_0 (2 × j - 1) | CRC_0 (2 × j) | CRC_0 (2 × j) | CRC_0 (2 × j + 1) |
| j+1 | CRC_0 (2 × j + 1) | CRC_0 (2 × j + 2) | CRC_0 (2 × j + 2) | CRC_0 (2 × j + 3) |

In FSoE Cycle j the FSoE Master receives a Safety Slave PDU with CRC_0 (2 × j - 1). Since the value of CRC_0 (2 × j - 2), which was included in the calculation of CRC_0 (2 × j - 1), was calculated by the FSoE Master in FSoE Cycle (j – 1), the FSoE Master can check CRC_0 (2 × j - 1) in the Safety Slave PDU.

In turn, in FSoE Cycle j, the FSoE Slave receives the Safety Master PDU with CRC_0 (2 × j) and is also able to check this PDU, since CRC_0 (2 × j - 1) calculated by the FSoE Slave in FSoE Cycle (j – 1) was included in the calculation.

#### 7.1.3.4 Sequence number

In Table 8 CRC_0 (2 × j) may equal CRC_0 (2 × j - 2). With short Safety PDUs this could lead to the Safety Master PDU in FSoE Cycle (j – 1) being the same as the Safety Master PDU in FSoE Cycle j, with the result that the FSoE Slave would not recognise the Safety Master PDU as a new PDU in FSoE Cycle j and the FSoE Watchdog would be triggered.

The CRCs of the Safety Master PDU therefore includes a virtual 16-bit master sequence number, which the FSoE Master increments with each new Safety Master PDU. The CRC of the Safety Slave PDU also includes a virtual 16-bit slave sequence number, which is incremented by the FSoE Slave with each new Safety Slave PDU.

Documents
Document Sharing Hub
Full document details: IEC 61784-3-12-2019

If CRC_0 (2 × j) equals CRC_0 (2 × j - 2) despite these measures, the master sequence number is incremented further until CRC_0 (2 × j) is not equal CRC_0 (2 × j - 2). This algorithm is used both for generating the Safety Master PDU by the FSoE Master and for checking the Safety Master PDU by the FSoE Slave.

If CRC_0 (2 × j + 1) equals CRC_0 (2 × j - 1), the slave sequence number is incremented further until CRC_0 (2 × j + 1) is not equal CRC_0 (2 × j - 1). This algorithm is used both for generating the Safety Slave PDU by the FSoE Slave and for checking the Safety Slave PDU by the FSoE Master.

The sequence number can assume values between 1 and 65 535. After 65 535 the sequence starts again with 1, i.e. 0 is left out.

#### 7.1.3.5 CRC index

If more than 2 octets of safety data and therefore 2 or several CRCs (for example CRC_0 and CRC_1) are transferred, the measures described above are not sufficient for detecting all reversal options within a Safety PDU, see example in Table 9.

**Table 9 – Example for 4 octets of safety data with interchanging of octets 1-4 with 5-8**

| Octet | Name | Description |
|---|---|---|
| 0 | Command | Command |
| 1 | SafeData[2] | safety data, octet 2 |
| 2 | SafeData[3] | safety data, octet 3 |
| 3 | CRC_1_Lo | low octet (bits 0-7) of the 16-bit CRC_1 |
| 4 | CRC_1_Hi | high octet (bits 8-15) of the 16-bit CRC_1 |
| 5 | SafeData[0] | safety data, octet 0 |
| 6 | SafeData[1] | safety data, octet 1 |
| 7 | CRC_0_Lo | low octet (bits 0-7) of the 16-bit CRC_0 |
| 8 | CRC_0_Hi | high octet (bits 8-15) of the 16-bit CRC_0 |
| 9 | Conn_Id_Lo | low octet (bits 0-7) of the unique connection ID |
| 10 | Conn_Id_Hi | low octet (bits 0-7) of the unique connection ID |

Index i (2 octect value) is therefore also included in the respective CRC_i. This enables detection of reversal of octets 1-4 and 5-8.

#### 7.1.3.6 Additional zero octets

The residual error probability is calculated via the ratio of detected errors and undetected errors. Undetected errors are essentially errors already detected by the CRC polynomial for the black channel (standard polynomial), since these errors are not apparent in the Safety layer due to the fact that they are filtered out beforehand. The worst case ratio between detected errors (errors that are not detected by the standard polynomial but by the CRC polynomial of the Safety layer) and undetected errors (errors already detected by the standard polynomial) occurs if the standard polynomial is divisible by the Safety polynomial.

Three zero octets are included in the calculation in order to ensure adequate independence between the two polynomials in this case.

#### 7.1.3.7 Session ID

Particularly in fieldbuses transferred via Ethernet, a faulty device storing telegrams (for example a switch) may lead to a correct sequence of telegrams being inserted at the wrong time. CRC inheritance means that a Safety PDU sequence always depends on the history.

AVA Documents
Document Sharing Hub
Full document details: IEC 61784-3-12-2019

Transferring a randomly generated session ID during setup of the FSoE Connection ensures that two Safety PDU sequences differ after power-on.

The session ID can assume values between 0 and 65 535.

## 7.2 FSCP 12/1 communication procedure

### 7.2.1 Message cycle

FSCP 12/1 communication operates with an acknowledged message cycle (FSoE Cycle), i.e. the FSoE Master sends a Safety Master PDU to the FSoE Slave and expects a Safety Slave PDU back. Only then is the next Safety Master PDU generated.

### 7.2.2 FSCP 12/1 node states

#### 7.2.2.1 General

While the FSoE Connection is established, the FSCP 12/1 nodes take on different states before the safety data become valid and the safely state is exited.

Documents
Document Sharing Hub

Full document details: IEC 61784-3-12-2019

Figure 8 shows the FSoE node states.

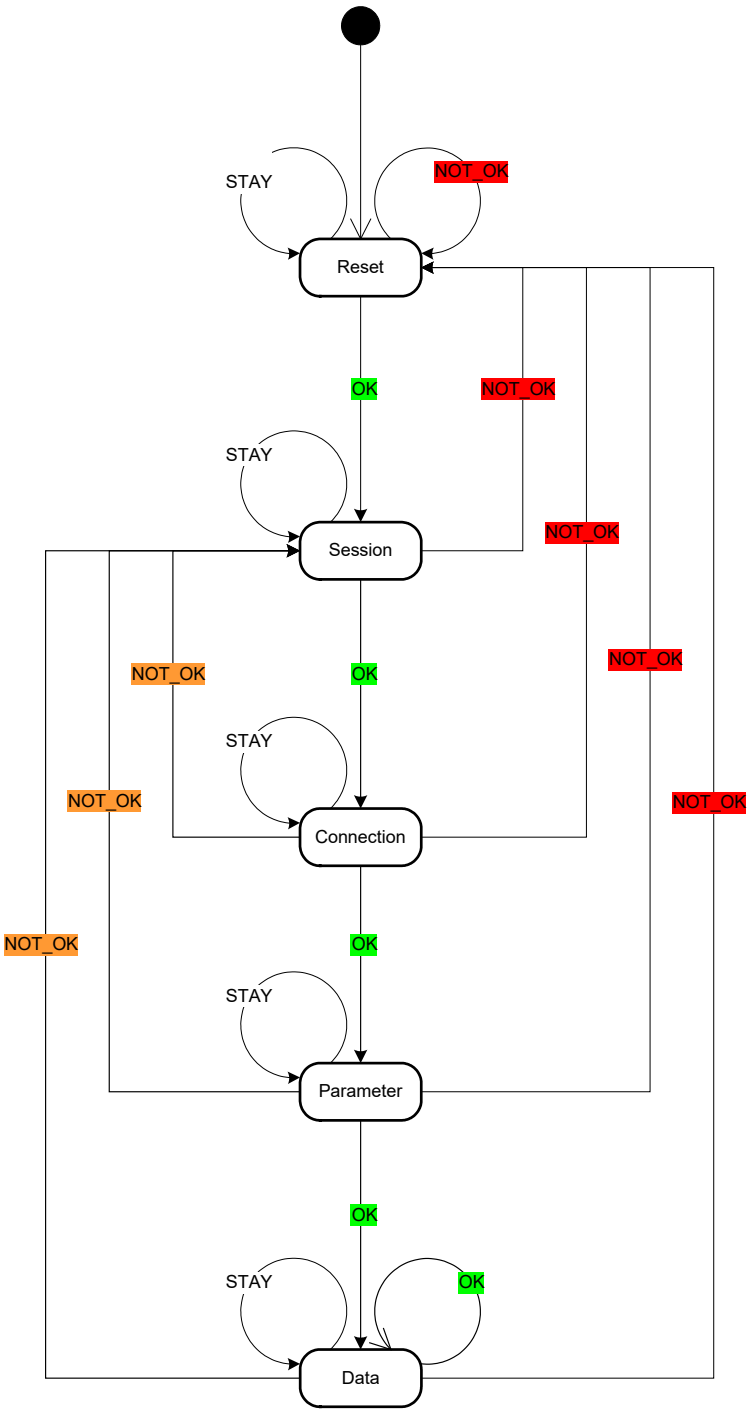



**Figure 8 – FSCP 12/1 node states**

After a power-on or an FSoE communication error the FSoE Master and Slave are in the reset state. The FSoE nodes also switch to reset-state if they detect an error in the communication or the local application. After an FSoE Reset command from the FSoE Slave, the FSoE Master switches to session state (transitions in orange). After a reset command from the FSoE Master, the FSoE Slave switches to reset state. The data state can then be assumed via the session, connection and parameter states. The safe output state can only be exited in the data state.

Documents
Document Sharing Hub
Full document details: IEC 61784-3-12-2019

#### 7.2.2.2 Reset state

The reset state is used to re-initialise the FSoE Connection after the power-on or an FSoE communication error. The FSoE Master exits the reset state when it sends a Safety Master PDU with the Session command to the FSoE Slave. The FSoE Slave exits the reset state when it receives a valid Safety Master PDU with the Session command.

In the reset state the sequence number and the CRC of the last telegram used in the CRC calculation are reset.

Table 10 shows an example of the Safety Master PDU for 4 octets of safety data with the reset command.

**Table 10 – Safety Master PDU for 4 octets of safety data with command = Reset after restart (reset connection) or error**

| Octet | Name | Description |
|---|---|---|
| 0 | Command | *Reset* |
| 1 | SafeData[0] | error code (bit 0-7), 0 for restart |
| 2 | SafeData[1] | unused (= 0) |
| 3 | CRC_0_Lo | low octet (bits 0-7) of the 16-bit CRC_0 |
| 4 | CRC_0_Hi | high octet (bits 8-15) of the 16-bit CRC_0 |
| 5 | SafeData[2] | unused (= 0) |
| 6 | SafeData[3] | unused (= 0) |
| 7 | CRC_1_Lo | low octet (bits 0-7) of the 16-bit CRC_1 |
| 8 | CRC_1_Hi | high octet (bits 8-15) of the 16-bit CRC_1 |
| 9 | Conn_Id_Lo | unused (= 0) |
| 10 | Conn_Id_Hi | unused (= 0) |

The FSoE Slave acknowledges Reset command by setting the SafeData to 0.

Table 11 shows an example of the Safety Slave PDU for 4 octets of safety data with the reset command.

**Table 11 – Safety Slave PDU for 4 octets of safety data with command = Reset for acknowledging a Reset command from the FSoE Master**

| Octet | Name | Description |
|---|---|---|
| 0 | Command | *Reset* |
| 1 | SafeData[0] | 0 |
| 2 | SafeData[1] | 0 |
| 3 | CRC_0_Lo | low octet (bits 0-7) of the 16-bit CRC_0 |
| 4 | CRC_0_Hi | high octet (bits 8-15) of the 16-bit CRC_0 |
| 5 | SafeData[2] | unused (= 0) |
| 6 | SafeData[3] | unused (= 0) |
| 7 | CRC_1_Lo | low octet (bits 0-7) of the 16-bit CRC_1 |
| 8 | CRC_1_Hi | high octet (bits 8-15) of the 16-bit CRC_1 |
| 9 | Conn_Id_Lo | unused (= 0) |
| 10 | Conn_Id_Hi | unused (= 0) |

The FSoE Slave also sends a Safety PDU with the Reset command during a restart (reset connection) or in the event of an error. This is shown in Table 12 as an example for 4 octets of safety data.

AVA Documents
Document Sharing Hub
Full document details: IEC 61784-3-12-2019

**Table 12 – Safety Slave PDU for 4 octets of safety data with command = Reset after restart (reset connection) or error**

| Octet | Name | Description |
|---|---|---|
| 0 | Command | *Reset* |
| 1 | SafeData[0] | error code (bit 0-7), 0 for restart |
| 2 | SafeData[1] | unused (= 0) |
| 3 | CRC_0_Lo | low octet (bits 0-7) of the 16-bit CRC_0 |
| 4 | CRC_0_Hi | high octet (bits 8-15) of the 16-bit CRC_0 |
| 5 | SafeData[2] | unused (= 0) |
| 6 | SafeData[3] | unused (= 0) |
| 7 | CRC_1_Lo | low octet (bits 0-7) of the 16-bit CRC_1 |
| 8 | CRC_1_Hi | high octet (bits 8-15) of the 16-bit CRC_1 |
| 9 | Conn_Id_Lo | unused (= 0) |
| 10 | Conn_Id_Hi | unused (= 0) |

The FSoE Master acknowledges the Reset command by sending a Safety Master PDU with the Session command.

#### 7.2.2.3 Session state

During the transition to or in the session state, a 16-bit Master Session ID is transferred from the FSoE Master to the FSoE Slave, which in turn responds with its own Slave Session ID. Both FSoE nodes generate the Session ID as a random number that is only used to differentiate multiple Safety PDU sequences in the event of several restarts of the FSoE Connection.

Table 13 shows an example of the Safety Master PDU for 4 octets of safety data with the Session command.

**Table 13 – Safety Master PDU for 4 octets of safety data with command = Session**

| Octet | Name | Description |
|---|---|---|
| 0 | Command | *Session* |
| 1 | SafeData[0] | *Master Session Id*, octet 0 |
| 2 | SafeData[1] | *Master Session Id*, octet 1 |
| 3 | CRC_0_Lo | low octet (bits 0-7) of the 16-bit CRC_0 |
| 4 | CRC_0_Hi | high octet (bits 8-15) of the 16-bit CRC_0 |
| 5 | SafeData[2] | unused (= 0) |
| 6 | SafeData[3] | unused (= 0) |
| 7 | CRC_1_Lo | low octet (bits 0-7) of the 16-bit CRC_1 |
| 8 | CRC_1_Hi | high octet (bits 8-15) of the 16-bit CRC_1 |
| 9 | Conn_Id_Lo | unused (= 0) |
| 10 | Conn_Id_Hi | unused (= 0) |

The FSoE Slave acknowledges Session command by sending back the Slave Session ID. Table 14 shows an example of the Safety Slave PDU for 4 octets of SafeData with the Session command.

Documents
Document Sharing Hub
Full document details: IEC 61784-3-12-2019

**Table 14 – Safety Slave PDU for 4 octets of safety data with command = Session**

| Octet | Name | Description |
|---|---|---|
| 0 | Command | *Session* |
| 1 | SafeData[0] | *Slave Session Id*, octet 0 |
| 2 | SafeData[1] | *Slave Session Id*, octet 1 |
| 3 | CRC_0_Lo | low octet (bits 0-7) of the 16-bit CRC_0 |
| 4 | CRC_0_Hi | high octet (bits 8-15) of the 16-bit CRC_0 |
| 5 | SafeData[2] | unused (= 0) |
| 6 | SafeData[3] | unused (= 0) |
| 7 | CRC_1_Lo | low octet (bits 0-7) of the 16-bit CRC_1 |
| 8 | CRC_1_Hi | high octet (bits 8-15) of the 16-bit CRC_1 |
| 9 | Conn_Id_Lo | unused (= 0) |
| 10 | Conn_Id_Hi | unused (= 0) |

If the Safety PDU contains at least 2 octets of safety data, the Session ID can be transferred with one FSoE Cycle. If, on the other hand, the Safety PDU only contains 1 octet of safety data, the Session ID shall be transferred with two FSoE Cycles.

The value of the Session ID has no safety relevance, i.e. a switch in the FSoE Node receiving the Safety PDU does not need to be examined from a safety perspective. The Connection ID for the Session command is therefore set to 0.

The FSoE Master exits the session state once it has transferred the complete session ID and received the associated acknowledgements from the FSoE Slave by sending a Safety PDU with the Connection command to the FSoE Slave. The FSoE Slave exits the session state when it receives a Safety PDU with the Connection command from the FSoE Master.

Both the FSoE Master and the FSoE Slave would also exit the Session state if they detect an FSoE communication error.

In the FSoE Master, after receipt of a RESET command, both the sequence number and the CRC of the last telegram used in the CRC calculation are reset.

#### 7.2.2.4 Connection state

In the connection state, a 16-bit Connection ID is transferred from the FSoE Master to the FSoE Slave. The Connection ID shall be unique and is generated by the safety configurator of the FSoE Master. If several FSoE Masters are present in the communication system, the user shall ensure that the Connection IDs used are unique.

In addition to the 16-bit Connection ID the unique FSoE Slave Address is also transferred. Table 15 shows the content of the safety data transferred in the connection state.

Documents
Document Sharing Hub
Full document details: IEC 61784-3-12-2019

**Table 15 – Safety data transferred in the connection state**

| SafetyData Octet | Description |
|---|---|
| 0 | low octet (bits 0-7) of the connection ID |
| 1 | high octet (bits 8-15) of the connection ID |
| 2 | low octet (bits 0-7) of the FSoE Slave Address |
| 3 | high octet (bits 8-15) of the FSoE Slave Address |

Depending on the length of the safety data, up to 4 FSoE Cycles are required. For a Safety PDU with 4 octets of safety data only one FSoE Cycle is required, this is shown in Table 16 and Table 17.

**Table 16 – Safety Master PDU for 4 octets of safety data in Connection state**

| Octet | Name | Description |
|---|---|---|
| 0 | Command | *Connection* |
| 1 | SafeData[0] | Connection Id, low octet |
| 2 | SafeData[1] | Connection Id, high octet |
| 3 | CRC_0_Lo | low octet (bits 0-7) of the 16-bit CRC_0 |
| 4 | CRC_0_Hi | high octet (bits 8-15) of the 16-bit CRC_0 |
| 5 | SafeData[2] | FSoE Slave Address, low octet |
| 6 | SafeData[3] | FSoE Slave Address, high octet |
| 7 | CRC_1_Lo | low octet (bits 0-7) of the 16-bit CRC_1 |
| 8 | CRC_1_Hi | high octet (bits 8-15) of the 16-bit CRC_1 |
| 9 | Conn_Id_Lo | Connection Id, low octet |
| 10 | Conn_Id_Hi | Connection Id, high octet |

The FSoE Slave acknowledges the Connection command by sending back the safety data.

**Table 17 – Safety Slave PDU for 4 octets of safety data in Connection state**

| Octet | Name | Description |
|---|---|---|
| 0 | Command | *Connection* |
| 1 | SafeData[0] | Connection Id, low octet |
| 2 | SafeData[1] | Connection Id, high octet |
| 3 | CRC_0_Lo | low octet (bits 0-7) of the 16-bit CRC_0 |
| 4 | CRC_0_Hi | high octet (bits 8-15) of the 16-bit CRC_0 |
| 5 | SafeData[2] | FSoE Slave Address, low octet |
| 6 | SafeData[3] | FSoE Slave Address, high octet |
| 7 | CRC_1_Lo | low octet (bits 0-7) of the 16-bit CRC_1 |
| 8 | CRC_1_Hi | high octet (bits 8-15) of the 16-bit CRC_1 |
| 9 | Conn_Id_Lo | Connection Id, low octet |
| 10 | Conn_Id_Hi | Connection Id, high octet |

The FSoE Slave Address shall be unique in the communication system. It can be set at the respective FSoE Slave device. By transferring the FSoE Slave Address together with the Connection ID, the FSoE Slave can check whether it was actually addressed, so that invalid addressing would be detected. Since the Connection ID is also unique in the communication system, the Connection ID is always sent in the following Safety PDUs, so that both the FSoE

Documents
Document Sharing Hub

Master and the FSoE Slave can detect whether they are addressed with the telegram. The unique Connection ID therefore enables 65 535 FSoE Connections to be realised in the communication system (Connection ID = 0 is not permitted).

#### 7.2.2.5 Parameter state

In the parameter state, safety-related communication and device specific safety-related application parameters are transferred. The latter can have any length. CRC inheritance ensures safety and consistent parameter transfer.

Table 18 shows the content of the safety data transferred in the parameter state.

**Table 18 – Safety data transferred in the parameter state**

| Safety data Octet | Description |
|---|---|
| 0 | low octet (bits 0-7) length of the communication parameters in octets (= 2) |
| 1 | high octet (bits 8-15) length of the communication parameters in octets (= 0) |
| 2 | low octet (bits 0-7) of the FSoE watchdog (in ms) |
| 3 | high octet (bits 8-15) of the FSoE watchdog (in ms) |
| 4 | low octet (bits 0-7) length of the application parameters in octets |
| 5 | high octet (bits 8-15) length of the application parameters in octets |
| 6 | 1st octet of the safety-related application parameter |
| … | |
| n+5 | nth octet of the safety-related application parameter |

The number of FSoE Cycles in the parameter state depends on the length of the safety-related application parameters and the length of the safety data in the Safety PDU. If not all safety data octets are required in the last FSoE Cycle, they shall be transferred as 0.

Two FSoE Cycles are required for a Safety PDU with 4 octets of safety data and 2 octets of safety-related application parameter; this is shown in Table 19 to Table 22.

**Table 19 – First Safety Master PDU for 4 octets of safety data in parameter state**

| Octet | Name | Description |
|---|---|---|
| 0 | Command | *Parameter* |
| 1 | SafeData[0] | low octet (bits 0-7) length of the communication parameters in octets (= 2) |
| 2 | SafeData[1] | high octet (bits 8-15) length of the communication parameters in octets (= 0) |
| 3 | CRC_0_Lo | low octet (bits 0-7) of the 16-bit CRC_0 |
| 4 | CRC_0_Hi | high octet (bits 8-15) of the 16-bit CRC_0 |
| 5 | SafeData[2] | low octet (bits 0-7) of the FSoE watchdog (in ms) |
| 6 | SafeData[3] | high octet (bits 8-15) of the FSoE watchdog (in ms) |
| 7 | CRC_1_Lo | low octet (bits 0-7) of the 16-bit CRC_1 |
| 8 | CRC_1_Hi | high octet (bits 8-15) of the 16-bit CRC_1 |
| 9 | Conn_Id_Lo | Connection Id, low octet |
| 10 | Conn_Id_Hi | Connection Id, high octet |

Documents
Document Sharing Hub
Full document details: IEC 61784-3-12-2019

The FSoE Slave acknowledges a correct Parameter command by sending back the safety data.

**Table 20 – First Safety Slave PDU for 4 octets of safety data in parameter state**

| Octet | Name | Description |
|---|---|---|
| 0 | Command | *Parameter* |
| 1 | SafeData[0] | low octet (bits 0-7) length of the communication parameters in octets (= 2) |
| 2 | SafeData[1] | high octet (bits 8-15) length of the communication parameters in octets (= 0) |
| 3 | CRC_0_Lo | low octet (bits 0-7) of the 16-bit CRC_0 |
| 4 | CRC_0_Hi | high octet (bits 8-15) of the 16-bit CRC_0 |
| 5 | SafeData[2] | low octet (bits 0-7) of the FSoE watchdog (in ms) |
| 6 | SafeData[3] | high octet (bits 8-15) of the FSoE watchdog (in ms) |
| 7 | CRC_1_Lo | low octet (bits 0-7) of the 16-bit CRC_1 |
| 8 | CRC_1_Hi | high octet (bits 8-15) of the 16-bit CRC_1 |
| 9 | Conn_Id_Lo | Connection Id, low octet |
| 10 | Conn_Id_Hi | Connection Id, high octet |

The FSoE Master sends the second Safety Master PDU once it has correctly received the first Safety Slave PDU.

**Table 21 – Second Safety Master PDU for 4 octets of safety data in parameter state**

| Octet | Name | Description |
|---|---|---|
| 0 | Command | *Parameter* |
| 1 | SafeData[0] | low octet (bits 0-7) length of the application parameters in octets (= 2) |
| 2 | SafeData[1] | high octet (bits 8-15) length of the application parameters in octets (= 0) |
| 3 | CRC_0_Lo | low octet (bits 0-7) of the 16-bit CRC_0 |
| 4 | CRC_0_Hi | high octet (bits 8-15) of the 16-bit CRC_0 |
| 5 | SafeData[2] | 1st octet of the safety-related application parameter |
| 6 | SafeData[3] | 2nd octet of the safety-related application parameter |
| 7 | CRC_1_Lo | low octet (bits 0-7) of the 16-bit CRC_1 |
| 8 | CRC_1_Hi | high octet (bits 8-15) of the 16-bit CRC_1 |
| 9 | Conn_Id_Lo | Connection Id, low octet |
| 10 | Conn_Id_Hi | Connection Id, high octet |

The FSoE Slave acknowledges a correct Parameter command by sending back the safety data.

Documents
Document Sharing Hub
Full document details: IEC 61784-3-12-2019

**Table 22 – Second Safety Slave PDU for 4 octets of safety data in parameter state**

| Octet | Name | Description |
|---|---|---|
| 0 | Command | *Parameter* |
| 1 | SafeData[0] | low octet (bits 0-7) length of the application parameters in octets (= 2) |
| 2 | SafeData[1] | high octet (bits 8-15) length of the application parameters in octets (= 0) |
| 3 | CRC_0_Lo | low octet (bits 0-7) of the 16-bit CRC_0 |
| 4 | CRC_0_Hi | high octet (bits 8-15) of the 16-bit CRC_0 |
| 5 | SafeData[2] | 1st octet of the safety-related application parameter |
| 6 | SafeData[3] | 2nd octet of the safety-related application parameter |
| 7 | CRC_1_Lo | low octet (bits 0-7) of the 16-bit CRC_1 |
| 8 | CRC_1_Hi | high octet (bits 8-15) of the 16-bit CRC_1 |
| 9 | Conn_Id_Lo | Connection Id, low octet |
| 10 | Conn_Id_Hi | Connection Id, high octet |

The FSoE Watchdog and the safety-related application parameters are configured via a safety configurator of the FSoE Master.

#### 7.2.2.6 Data state

##### 7.2.2.6.1 Valid data

While in the previous states the number of FSoE Cycles was fixed, in the data state FSoE Cycles are transferred until either a communication error occurs or an FSoE node is stopped locally. The FSoE Master sends SafeOutputs to the FSoE Slave.

Table 23 shows an example of the Safety Master PDU for 4 octets of SafeOutputs with the ProcessData command.

**Table 23 – Safety Master PDU for 4 octets of ProcessData in data state**

| Octet | Name | Description |
|---|---|---|
| 0 | Command | *ProcessData* |
| 1 | SafeData[0] | 1st octet of SafeOutputs |
| 2 | SafeData[1] | 2nd octet of SafeOutputs |
| 3 | CRC_0_Lo | low octet (bits 0-7) of the 16-bit CRC_0 |
| 4 | CRC_0_Hi | high octet (bits 8-15) of the 16-bit CRC_0 |
| 5 | SafeData[2] | 3rd octet of SafeOutputs |
| 6 | SafeData[3] | 4th octet of SafeOutputs |
| 7 | CRC_1_Lo | low octet (bits 0-7) of the 16-bit CRC_1 |
| 8 | CRC_1_Hi | high octet (bits 8-15) of the 16-bit CRC_1 |
| 9 | Conn_Id_Lo | Connection Id, low octet |
| 10 | Conn_Id_Hi | Connection Id, high octet |

The FSoE Slave acknowledges the Safety Master PDU and sends SafeInputs to the FSoE Master.

Table 24 shows an example of the Safety Slave PDU for 4 octets of SafeInputs with the ProcessData command.

AVA Documents
Document Sharing Hub
Full document details: IEC 61784-3-12-2019

**Table 24 – Safety Slave PDU for 4 octets of ProcessData in data state**

| Octet | Name | Description |
|---|---|---|
| 0 | Command | *ProcessData* |
| 1 | SafeData[0] | 1st octet of SafeInputs |
| 2 | SafeData[1] | 2nd octet of SafeInputs |
| 3 | CRC_0_Lo | low octet (bits 0-7) of the 16-bit CRC_0 |
| 4 | CRC_0_Hi | high octet (bits 8-15) of the 16-bit CRC_0 |
| 5 | SafeData[2] | 3rd octet of SafeInputs |
| 6 | SafeData[3] | 4th octet of SafeInputs |
| 7 | CRC_1_Lo | low octet (bits 0-7) of the 16-bit CRC_1 |
| 8 | CRC_1_Hi | high octet (bits 8-15) of the 16-bit CRC_1 |
| 9 | Conn_Id_Lo | Connection Id, low octet |
| 10 | Conn_Id_Hi | Connection Id, high octet |

#### 7.2.2.6.2 FailSafeData command

If the FSoE Master locally detects that the SafeOutputs are not valid or are to be switched to safe state, it sends the FailSafeData command.

Table 25 shows an example of the Safety Master PDU for 4 octets of FailsafeData with the FailsafeData command.

**Table 25 – Safety Master PDU for 4 octets of fail-safe data in data state**

| Octet | Name | Description |
|---|---|---|
| 0 | Command | *FailSafeData* |
| 1 | SafeData[0] | Fail-safe Data = 0 |
| 2 | SafeData[1] | Fail-safe Data = 0 |
| 3 | CRC_0_Lo | low octet (bits 0-7) of the 16-bit CRC_0 |
| 4 | CRC_0_Hi | high octet (bits 8-15) of the 16-bit CRC_0 |
| 5 | SafeData[2] | Fail-safe Data = 0 |
| 6 | SafeData[3] | Fail-safe Data = 0 |
| 7 | CRC_1_Lo | low octet (bits 0-7) of the 16-bit CRC_1 |
| 8 | CRC_1_Hi | high octet (bits 8-15) of the 16-bit CRC_1 |
| 9 | Conn_Id_Lo | Connection Id, low octet |
| 10 | Conn_Id_Hi | Connection Id, high octet |

If the FSoE Slave locally detects that the SafeInputs are not valid or are to be switched to safe state, it sends the FailSafeData command.

Table 26 shows an example of the Safety Slave PDU for 4 octets of FailsafeData with the FailsafeData command.

Documents
Document Sharing Hub
Full document details: IEC 61784-3-12-2019

**Table 26 – Safety Slave PDU for 4 octets of fail-safe data in data state**

| Octet | Name | Description |
|---|---|---|
| 0 | Command | *FailSafeData* |
| 1 | SafeData[0] | Fail-safe Data = 0 |
| 2 | SafeData[1] | Fail-safe Data = 0 |
| 3 | CRC_0_Lo | low octet (bits 0-7) of the 16-bit CRC_0 |
| 4 | CRC_0_Hi | high octet (bits 8-15) of the 16-bit CRC_0 |
| 5 | SafeData[2] | Fail-safe Data = 0 |
| 6 | SafeData[3] | Fail-safe Data = 0 |
| 7 | CRC_1_Lo | low octet (bits 0-7) of the 16-bit CRC_1 |
| 8 | CRC_1_Hi | high octet (bits 8-15) of the 16-bit CRC_1 |
| 9 | Conn_Id_Lo | Connection Id, low octet |
| 10 | Conn_Id_Hi | Connection Id, high octet |

The transfer of ProcessData or FailSafeData is independent of the command of the received Safety PDU. It only depends on local circumstances.

### 7.3 Reaction on communication errors

An FSoE node can detect the errors listed in Table 27.

**Table 27 – FSoE communication error**

| Error | Description |
|---|---|
| Unexpected command | The received command is not allowed in the state |
| Unknown command | The received command is not defined |
| Invalid connection ID | The connection does not match the connection ID transferred in the connection state |
| CRC error | At least one of the received CRC_i does not match the calculated CRC_i |
| Watchdog has expired | No valid Safety PDU was received within the FSoE watchdog time |
| Invalid FSoE Alave Address | The FSoE Slave Address transferred in the Connection state does not match the local address set on the FSoE Slave |
| Invalid SafeData | The safety data sent back by the FSoE Slave in the Session, Connection and Parameter states do not match the expected values |
| Faulty SafePara | The SafePara sent to the FSoE Slave in the Parameter state are faulty |
| Invalid communication parameter length | The length of the communication parameter is wrong |
| Invalid communication parameter | The content of the communication parameter is wrong |
| Invalid application parameter length | The length of the application parameter is wrong |
| Invalid application parameter | The content of the application parameter is wrong |

If an FSoE node detects a communication error, a Reset command is sent, as well as the associated error code in SafeData[0] for diagnostic purposes. The FSoE Master then switches to the Session state, the FSoE Slave to the Reset state. The FSoE communication error codes are listed in Table 28.

Documents
Document Sharing Hub
Full document details: IEC 61784-3-12-2019

**Table 28 – FSoE communication error codes**

| Error Code | Description |
|---|---|
| 0 | Local reset or acknowledgement of a RESET command |
| 1 | Unexpected command (INVALID_CMD) |
| 2 | Unknown command (UNKNOWN_CMD) |
| 3 | Invalid connection ID (INVALID_CONNID) |
| 4 | CRC error (INVALID_CRC) |
| 5 | Watchdog has expired (WD_EXPIRED) |
| 6 | Invalid FSoE Slave Address (INVALID_ADDRESS) |
| 7 | Invalid safety data (INVALID_DATA) |
| 8 | Invalid communication parameter length (INVALID_COMMPARALEN) |
| 9 | Invalid communication parameter data (INVALID_COMPARA) |
| 10 | Invalid application parameter length (INVALID_USERPARALEN) |
| 11 | Invalid application parameter data (INVALID_USERPARA) |
| 0x80-0xFF | Invalid SafePara (device-specific) |

## 7.4 State table for FSoE Master

### 7.4.1 FSoE Master state machine

#### 7.4.1.1 Overview

Depending on the communication procedure, the FSoE Master can have the states listed in Table 29.

**Table 29 – States of the FSoE Master**

| State | Description |
|---|---|
| Reset | The FSoE Connection is reset (outputs are in safe state) |
| Session | The session ID is being transferred (outputs are in safe state) |
| Connection | The connection ID is being transferred (outputs are in safe state) |
| Parameter | The parameters are being transferred (outputs are in safe state) |
| Data | Process data or fail-safe data are being transferred (outputs are only active if the *ProcessData* command is received) |

The state diagram for the FSoE Master is shown in Figure 9.

Documents
Document Sharing Hub
Full document details: IEC 61784-3-12-2019

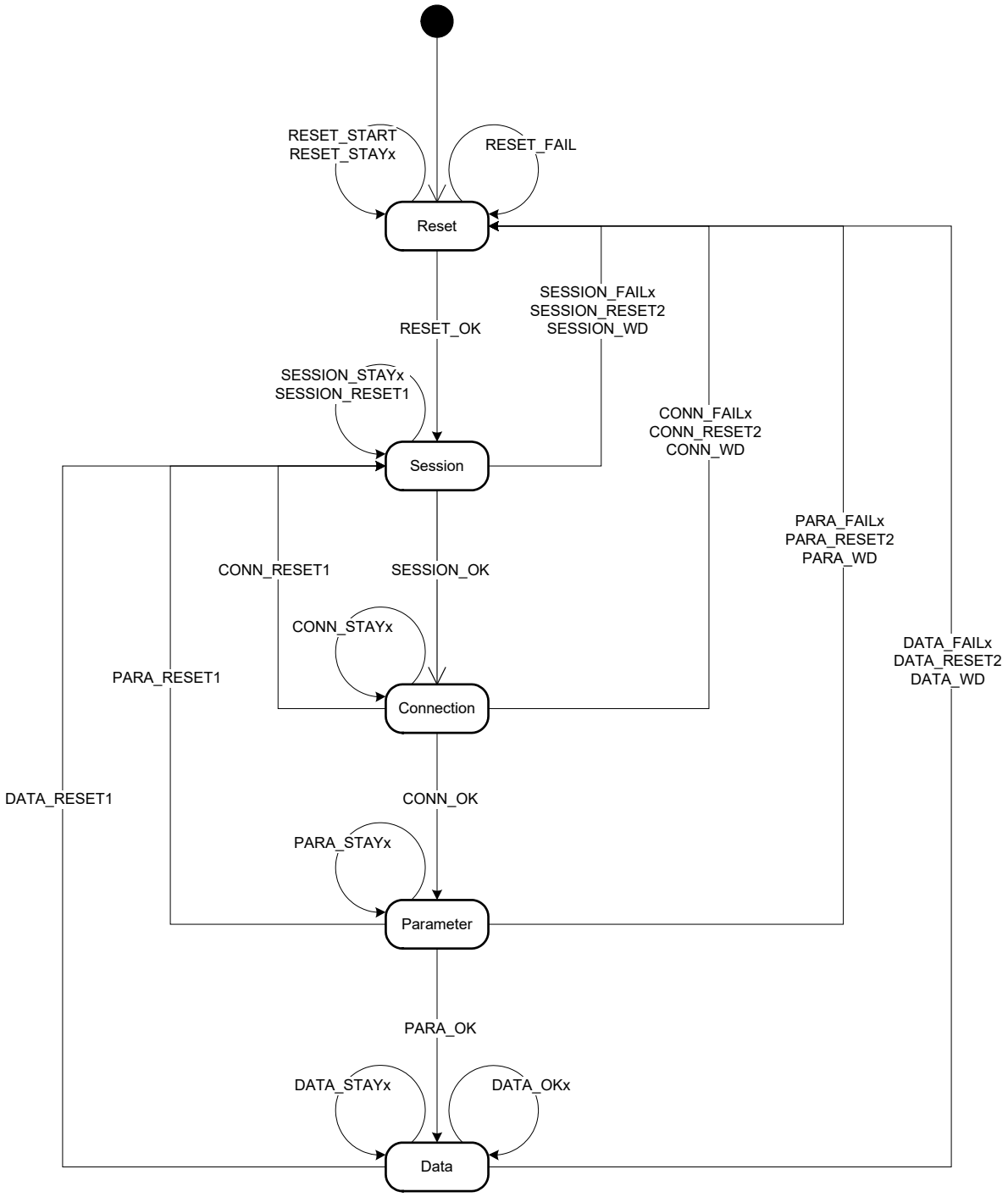



**Figure 9 – State diagram for FSoE Master**

For each state, the following sections analyse the events that can occur in the FSoE Master. Each event is considered under conditions with different actions or subsequent states.

#### 7.4.1.2 Events

An event can include different parameters, which are referred to in the state tables. Table 30 lists the used events.

Documents
Document Sharing Hub
Full document details: IEC 61784-3-12-2019

**Table 30 – Events in the FSoE Master state table**

| Event | Description |
|---|---|
| Frame received | A Safety PDU was received, i.e. at least one bit within the Safety PDU has changed<br>Parameters:<br>Frame = received Safety PDU<br>Frame.Command = command of the received Safety PDU<br>Frame.Crc0 = CRC_0 of the received Safety PDU<br>Frame.ConnId = connection ID of the received Safety PDU<br>Frame.SafeData = safety data of the received Safety PDU |
| Watchdog expired | The FSoE watchdog has expired, i.e. no Safety PDU was received within the watchdog time<br>Parameters: none |
| Reset Connection | Request via a local interface to reset the FSoE Connection. This event shall be triggered on power-on in order to start communication with the FSoE Slave<br>Parameters: none |
| Set Data Command | Request via a local interface to switch the SafeOutputs to the safe state or to exit the safe state<br>Parameters:<br>DataCmd = *FailSafeData* or *ProcessData* |

#### 7.4.1.3 Actions

Depending on different conditions, certain actions are carried out if an event occurs. In the state tables the actions are shown as function calls or variable assignments.

Table 31 lists the used functions in the FSoE Master state table.

**Table 31 – Functions in the FSoE Master state table**

| Function | Description |
|---|---|
| SendFrame(cmd, safeData, lastCrc, connId, seqNo, oldCrc, bNew) | An FSoE Master frame is sent<br>Parameters:<br>cmd = frame command<br>SafeData = reference to safety data sent with the frame<br>lastCrc = CRC_0 of the last Safety Slave PDU included in the CRC calculation for the frame<br>connId = Connect ID to be entered in the frame and included in the CRC calculation<br>seqNo = Pointer to the Master Sequence Number included in the CRC calculation for the frames. The incremented (perhaps several times) seqNo is returned<br>oldCrc: Pointer to the CRC_0 of the last sent Safety Master PDU. The calculated CRC_0 is returned<br>bNew: if bNew = TRUE and oldCrc equals the calculated crc, the CRC calculation is repeated with the incremented seqNo until the calculated crc is not equal the oldCrc (procedure according to 7.1.3.4) |

Table 32 lists the used variables in the FSoE Master state table.

Documents
Document Sharing Hub
Full document details: IEC 61784-3-12-2019

**Table 32 – Variables in the FSoE Master state table**

| Variable | Description |
|---|---|
| LastCrc | CRC_0 of the last sent Safety Master PDU (initialised with 0 on power-on) |
| OldMasterCrc | CRC_0 of the last sent Safety Master PDU (initialised with 0 on power-on) |
| OldSlaveCrc | CRC_0 of the last received Safety Slave PDU (initialised with 0 on power-on) |
| MasterSeqNo | Master Sequence Number to be used in the CRC for next Safety Master PDU (initialised with 0 on power-on) |
| SlaveSeqNo | Expected Slave Sequence Number to be used in the CRC for next Safety Slave PDU (initialised with 0 on power-on) |
| SessionId | Randomly generated session ID (initialised with 0 on power-on) |
| DataCommand | Indicates whether the *ProcessData* or *FailSafeData* command is sent in the Data state. Initialised with *FailSafeData* on power-on |
| BytesToBeSent | If several Safety PDUs have to be sent in the Session, Connection or Parameter state, this variable indicates how many octets are still to be sent (initialised with 0 on power-on) |
| ConnData | ConnData consist of the connection ID and the FSoE Slave Address. Initialised by the safety configurator on power-on according to the configuration<br>ConnData.ConnId: ConnectionId of the FSoE Connection |
| SafePara | The SafePara consist of the safety communication parameters and the safety application parameters. Initialised by the safety configurator on power-on according to the configuration<br>SafePara.Watchdog: FSoE watchdog |
| SafeParaSize | Indicates the SafePara length. Initialised by the safety configurator on power-on according to the configuration data |
| SafeOutputs | Contains the process values of the safety outputs sent to the FSoE Slave. Initialised with FS_VALUE (Fail-safe Data = 0) on power-on |
| SafeInputs | Contains the process values of the safety inputs received by the FSoE Slave. Initialised with FS_VALUE (Fail-safe Data = 0) on power-on |
| CommFaultReason | Indicates the error code in the event of a communication error |
| SecondSessionFrameSent | If two Safety PDUs have to be sent in state Session this variable indicates if the second PDU is already sent. This variable is set to FALSE by the macro CREATE_SESSION_ID |

#### 7.4.1.4 Macros

Certain functionalities are consolidated in macros in order to keep the state tables transparent.

Table 33 lists the used macros in the FSoE Master state table.

**Table 33 – Macros in the FSoE Master state table**

| Macro | Description |
|---|---|
| IS_CRC_CORRECT( frame, lastCrc, seqNo, oldCrc, bNew) | This macro checks whether the CRCs of the received Safety Slave PDU are correct<br>Parameters:<br>Frame = received frame<br>lastCrc = CRC_0 of the last sent Safety Master PDU included in the CRC calculations for the received PDU<br>seqNo = Slave Sequence Number included in the CRC calculations for the received frame. The incremented (perhaps several times) seqNo is returned<br>oldCrc: Pointer to the CRC_0 of the last received Safety Slave PDU. The CRC_0 of the received telegram is returned |

Documents
Document Sharing Hub
Full document details: IEC 61784-3-12-2019

| Macro | Description |
|---|---|
| | bNew: if bNew = TRUE and oldCrc equals the calculated crc, the CRC calculation is repeated with the incremented seqNo until the calculated crc is not equal the oldCrc (procedure according to 7.1.3.4) |
| UPDATE_BYTES_TO_BE_SENT (bytesSent) | This macro checks how many octets in the Session, Connection and Parameter states are still to be sent before the state is changed<br>Parameters:<br>bytesSent = Number of octets still to be sent |
| IS_SAFEDATA_CORRECT (frame, expectedData, bytesSent) | This macro checks whether the SafeData of the received Safety Slave PDUmatch the expected data<br>Parameters:<br>Frame = received frame<br>expectedData = Reference to the expected data<br>bytesSent = Number of octets sent |
| START_WD(watchdog) | This macro resets the watchdog and starts a monitoring timer<br>Parameters:<br>Watchdog = monitoring time in ms |
| CREATE_SESSION_ID | This macro generates a random session ID<br>The variable SecondSessionFrameSent is reset to FALSE |
| ADR | This macro generates a reference (pointer) to a variable |

### 7.4.2 Reset state

#### 7.4.2.1 Frame received event

| Transition | Condition | Action | Next State |
|---|---|---|---|
| RESET_OK | `Frame.Command = Reset` | `SessionId := CREATE_SESSION_ID();`<br>`SendFrame(Session,`<br>`ADR(SessionId),`<br>`LastCrc,`<br>`0,`<br>`ADR(MasterSeqNo),`<br>`ADR(OldMasterCrc),`<br>`FALSE);`<br>`LastCrc = SendFrame.Crc0;`<br>`BytesToBeSent :=`<br>`UPDATE_BYTES_TO_BE_SENT(2);`<br>`START_WD(SafePara.Watchdog);` | Session |
| RESET_STAY1 | `Frame.Command <> Reset` | `LastCrc := 0`<br>`OldMasterCrc := 0;`<br>`OldSlaveCrc := 0;`<br>`MasterSeqNo := 1;`<br>`SlaveSeqNo := 1;`<br>`DataCommand := FailSafeData;`<br>`CommFaultReason := 0;`<br>`SendFrame(Reset,`<br>`ADR(CommFaultReason),`<br>`LastCrc,`<br>`0,`<br>`ADR(MasterSeqNo),`<br>`ADR(OldMasterCrc),`<br>`FALSE);`<br>`MasterSeqNo := 1;` | Reset |

Documents
Document Sharing Hub
Full document details: IEC 61784-3-12-2019

#### 7.4.2.2 Watchdog expired event

| Transition | Condition | Action | Next State |
|---|---|---|---|
| RESET_WD | Watchdog expired | SessionId := CREATE_SESSION_ID();<br>SendFrame(Session,<br>ADR(SessionId),<br>LastCrc,<br>0,<br>ADR(MasterSeqNo),<br>ADR(OldMasterCrc),<br>FALSE);<br>LastCrc = SendFrame.Crc0;<br>BytesToBeSent :=<br>UPDATE_BYTES_TO_BE_SENT(2);<br>START_WD(SafePara.Watchdog); | Session |

#### 7.4.2.3 Reset connection event

| Transition | Condition | Action | Next State |
|---|---|---|---|
| RESET_START | | LastCrc := 0<br>OldMasterCrc := 0;<br>OldSlaveCrc := 0;<br>MasterSeqNo := 1;<br>SlaveSeqNo := 1;<br>DataCommand := FailSafeData;<br>CommFaultReason := 0;<br>SendFrame(Reset,<br>ADR(CommFaultReason),<br>LastCrc,<br>0,<br>ADR(MasterSeqNo),<br>ADR(OldMasterCrc),<br>FALSE);<br>MasterSeqNo := 1;<br>START_WD(SafePara.Watchdog); | Reset |

#### 7.4.2.4 Set Data Command event

| Transition | Condition | Action | Next State |
|---|---|---|---|
| RESET_STAY2 | | DataCommand := DataCmd; | Reset |

### 7.4.3 Session state

#### 7.4.3.1 Frame received event

| Transition | Condition | Action | Next State |
|---|---|---|---|
| SESSION_OK | Frame.Command =<br>*Session*<br>AND<br>BytesToBeSent = 0<br>AND<br>IS_CRC_CORRECT(Frame,<br>LastCrc,<br>ADR(SlaveSeqNo),<br>ADR(OldSlaveCrc),<br>TRUE) = TRUE | LastCrc := Frame.Crc0;<br>SendFrame(Connection,<br>ADR(ConnData),<br>LastCrc,<br>ConnData.ConnId,<br>ADR(MasterSeqNo),<br>ADR(OldMasterCrc),<br>TRUE);<br>LastCrc := SendFrame.Crc0;<br>BytesToBeSent :=<br>UPDATE_BYTES_TO_BE_SENT(4);<br>START_WD(SafePara.Watchdog); | Connection |

Documents
Document Sharing Hub
Full document details: IEC 61784-3-12-2019

| Transition | Condition | Action | Next State |
|---|---|---|---|
| SESSION_FAIL1 | Frame.Command = *Session*<br>AND<br>IS_CRC_CORRECT(Frame, LastCrc, ADR(SlaveSeqNo), ADR(OldSlaveCrc), TRUE) = FALSE<br>AND<br>SecondSessionFrameSent = TRUE | LastCrc := 0<br>OldMasterCrc := 0;<br>OldSlaveCrc := 0;<br>MasterSeqNo := 1;<br>SlaveSeqNo := 1;<br>DataCommand := *FailSafeData*;<br>CommFaultReason := INVALID_CRC;<br>SendFrame(Reset,<br><br>ADR(CommFaultReason),<br>LastCrc,<br>0,<br>ADR(MasterSeqNo),<br>ADR(OldMasterCrc),<br>FALSE);<br>MasterSeqNo := 1;<br>START_WD(SafePara.Watchdog); | Reset |
| SESSION_STAY2 | Frame.Command = *Session*<br>AND<br>IS_CRC_CORRECT(Frame, LastCrc, ADR(SlaveSeqNo), ADR(OldSlaveCrc), TRUE) = FALSE<br>AND<br>SecondSessionFrameSent = FALSE | START_WD(SafePara.Watchdog); | Session |
| SESSION_STAY1 | Frame.Command = *Session*<br>AND<br>BytesToBeSent <> 0<br>AND<br>IS_CRC_CORRECT(Frame, LastCrc, ADR(SlaveSeqNo), ADR(OldSlaveCrc), TRUE) = TRUE | LastCrc := Frame.Crc0;<br>SendFrame( Session,<br>ADR(SessionId<br>[2-BytesToBeSent]),<br>Frame.Crc0,<br>0,<br>ADR(MasterSeqNo),<br>ADR(OldMasterCrc),<br>TRUE);<br>LastCrc := SendFrame.Crc0;<br>BytesToBeSent := UPDATE_BYTES_TO_BE_SENT(<br>BytesToBeSent);<br>SecondSessionFrameSent := TRUE;<br>START_WD(SafePara.Watchdog); | Session |
| SESSION_RESET1 | Frame.Command = *Reset* | LastCrc := 0<br>OldMasterCrc := 0;<br>OldSlaveCrc := 0;<br>MasterSeqNo := 1;<br>SlaveSeqNo := 1;<br>SessionId := CREATE_SESSION_ID();<br>DataCommand := *FailSafeData*;<br>SendFrame(Session,<br>ADR(SessionId),<br>LastCrc,<br>0,<br>ADR(MasterSeqNo),<br>ADR(OldMasterCrc),<br>FALSE);<br>LastCrc = SendFrame.Crc0;<br>BytesToBeSent := UPDATE_BYTES_TO_BE_SENT(2);<br>START_WD(SafePara.Watchdog); | Session |

Documents
Document Sharing Hub
Full document details: IEC 61784-3-12-2019