



DPC: 13 / 30294110 DC

## BSI Group Headquarters

389 Chiswick High Road London W4 4AL

Tel: + 44 (0)20 8996 9000

Fax: + 44 (0)20 8996 7400

www.bsigroup.com

Date: 19 November 2013

Origin: International

Latest date for receipt of comments: 15 January 2014

Project No. 2013/03404

Responsible committee: AMT/7 Industrial communications: process measurement and control, including fieldbus

Interested committees:

Title: Draft BS EN 61784-3-x Ed 1.0 Industrial communication networks - Profiles

Part 3-x: Functional safety fieldbuses - Additional specifications for CPF x

Please notify the secretary if you are aware of any keywords that might assist in classifying or identifying the standard or if the content of this standard

- i) has any issues related to 3rd party IPR, patent or copyright
- ii) affects other national standard(s)
- iii) requires additional national guidance or information

**WARNING: THIS IS A DRAFT AND MUST NOT BE REGARDED OR USED AS A BRITISH STANDARD.  
THIS DRAFT IS NOT CURRENT BEYOND 15 January 2014**

This draft is issued to allow comments from interested parties; all comments will be given consideration prior to publication. No acknowledgement will normally be sent. **See overleaf for information on the submission of comments.**

No copying is allowed, in any form, without prior written permission from BSI except as permitted under the Copyright, Designs and Patent Act 1988 or for circulation within a nominating organization for briefing purposes. Electronic circulation is limited to dissemination by e-mail within such an organization by committee members.

Further copies of this draft may be purchased from BSI Shop <http://shop.bsigroup.com> or from BSI Customer Services, Tel: + 44(0) 20 8996 9001 or email [cservices@bsigroup.com](mailto:cservices@bsigroup.com). British, International and foreign standards are also available from BSI Customer Services.

Information on the co-operating organizations represented on the committees referenced above may be obtained from <http://standardsdevelopment.bsigroup.com>

Responsible Committee Secretary: **Committee Service Centre (BSI)**  
Direct tel: **020 8996 7009**  
E-mail: **csc@bsigroup.com**

## Introduction

This draft standard is based on international discussions in which the UK has taken an active part. Your comments on this draft are welcome and will assist in the preparation of the consequent standard. There is a high probability that this text could be adopted by CENELEC as a reference document for harmonization or as a European Standard. Recipients of this draft are requested to comment on the text bearing in mind this possibility.

## UK Vote

Please indicate whether you consider the UK should submit a negative (with reasons) or positive vote on this draft.

## BSI Committee Responsibilities

Whether or not the standard is published in its original (international) form, or as a formal British Standard Implementation the BSI committee's responsibilities are to:

- aid enquirers to understand the text;
- present to the responsible international committee any enquiries on interpretation, or proposals for change, and keep UK interests informed;
- monitor related International and European developments and promulgate them in the UK.

## Submission of Comments

- The guidance given below is intended to ensure that all comments receive efficient and appropriate attention by the responsible BSI committee. **Annotated drafts are not acceptable and will be rejected.**
- All comments must be submitted, preferably electronically, to the Responsible Committee Secretary at the address given on the front cover. Comments should be compatible with version 6.0 or version 97 of Microsoft Word for Windows, if possible; otherwise comments in ASCII text format are acceptable. **Any comments not submitted electronically should still adhere to these format requirements.**
- All comments submitted should be presented as given in the example below. Further information on submitting comments and how to obtain a blank electronic version of a comment form are available from the BSI website at: <http://drafts.bsigroup.com/>

## Template for comments and secretariat observations

|                  |                               |
|------------------|-------------------------------|
| Date: xx/xx/20xx | Document: <b>ISO/DIS xxxx</b> |
|------------------|-------------------------------|

| 1  | 2                                          | (3)                           | 4               | 5                                                                                                                                  | (6)                                                                      | (7)                                                |
|----|--------------------------------------------|-------------------------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|----------------------------------------------------|
| MB | Clause No./ Subclause No./Annex (e.g. 3.1) | Paragraph/ Figure/ Table/Note | Type of comment | Comment (justification for change) by the MB                                                                                       | Proposed change by the MB                                                | Secretariat observations on each comment submitted |
|    | 3.1                                        | Definition 1                  | ed              | Definition is ambiguous and needs clarifying.                                                                                      | Amend to read '...so that the mains connector to which no connection...' |                                                    |
|    | 6.4                                        | Paragraph 2                   | te              | The use of the UV photometer as an alternative cannot be supported as serious problems have been encountered in its use in the UK. | Delete reference to UV photometer.                                       |                                                    |



**65C/748/CD**

**COMMITTEE DRAFT (CD)**

|                                                                                                                                                                      |  |                                                                                                                                                                                                                                                                                                    |                                                |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|
| <b>IEC/TC or SC:</b><br>SC65C                                                                                                                                        |  | Project number<br>IEC 61784-3-x Ed 1.0                                                                                                                                                                                                                                                             |                                                |
| Title of TC/SC:<br>Industrial networks                                                                                                                               |  | Date of circulation<br><b>2013-11-15</b>                                                                                                                                                                                                                                                           | Closing date for comments<br><b>2014-02-21</b> |
| Also of interest to the following committees<br>SC 65A, TC 44, TC 57, TC 66, ISO TC184/SC5                                                                           |  | Supersedes document<br>65C/712A/RR,                                                                                                                                                                                                                                                                |                                                |
| Proposed horizontal standard<br><input type="checkbox"/> Other TC/SCs are requested to indicate their interest, if any, in this CD to the TC/SC secretary            |  |                                                                                                                                                                                                                                                                                                    |                                                |
| Functions concerned:<br><input type="checkbox"/> Safety <input type="checkbox"/> EMC <input type="checkbox"/> Environment <input type="checkbox"/> Quality assurance |  |                                                                                                                                                                                                                                                                                                    |                                                |
| Secretary:<br>Valérie DEMASSIEUX                                                                                                                                     |  | THIS DOCUMENT IS STILL UNDER STUDY AND SUBJECT TO CHANGE. IT SHOULD NOT BE USED FOR REFERENCE PURPOSES.<br><br>RECIPIENTS OF THIS DOCUMENT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION. |                                                |

Title:

IEC 61784-3-x Ed 3.0: Industrial communication networks - Profiles - Part 3-x: Functional safety fieldbuses - Additional specifications for CPF x

(Titre) :

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

Introductory note

Changes from the previous edition have been highlighted in these drafts using either specific comments boxes, or yellow highlights over modified text.

NC comments will be addressed during the SC65C/WG12 meeting scheduled on March 24<sup>th</sup>-28<sup>th</sup>, 2014 in Hamburg (Germany). Corresponding meeting notice will be provided in due time by the convenor.

**Copyright © 2013 International Electrotechnical Commission, IEC.** All rights reserved. It is permitted to download this electronic file, to make a copy and to print out the content for the sole purpose of preparing National Committee positions. You may not copy or "mirror" the file or printed version of the document, or any part of it, for any other purpose without permission in writing from IEC.

## INCLUDED SUBPARTS

NOTE 1: The page numbers of each subpart are prefixed with the CPF number of the subpart to facilitate identification, and so that the numbering of each subpart can be independent of those that precede it.

NOTE 2: The Contents of each subpart begins on page xxx2, so that the page numbering will be unchanged when the final International Standard is issued with its IEC-Central-Office-provided cover sheet.

NOTE 3: Part 3-1 (Ed 2.0), Part 3-6 (Ed 2.0), Part 3-12 (Ed 1.0) and Part 3-14 (Ed 1.0) are not included since they are simply reconfirmed, as indicated in 65C/712A/RR.

IEC 61784-3-2 Ed3.0, Industrial communication networks - Profiles –  
Part 3-2: Functional safety fieldbuses - Additional specifications for CPF 2 ..... 2002

IEC 61784-3-3 Ed3.0, Industrial communication networks - Profiles –  
Part 3-3: Functional safety fieldbuses - Additional specifications for CPF 3 ..... 3002

IEC 61784-3-8 Ed2.0, Industrial communication networks - Profiles –  
Part 3-8: Functional safety fieldbuses - Additional specifications for CPF 8 ..... 8002

IEC 61784-3-13 Ed2.0, Industrial communication networks - Profiles –  
Part 3-13: Functional safety fieldbuses - Additional specifications for CPF 13 ..... 13002

IEC 61784-3-17 Ed1.0, Industrial communication networks - Profiles –  
Part 3-17 Functional safety fieldbuses - Additional specifications for CPF 17 ..... 17002

IEC 61784-3-18 Ed1.0 Amd.1, Industrial communication networks - Profiles –  
Part 3-18: Functional safety fieldbuses - Additional specifications for CPF 18 ..... 18002

# CONTENTS

|    |                                                                               |      |
|----|-------------------------------------------------------------------------------|------|
| 1  |                                                                               |      |
| 2  | FOREWORD.....                                                                 | 2012 |
| 3  | 0 Introduction .....                                                          | 2014 |
| 4  | 0.1 General .....                                                             | 2014 |
| 5  | 0.2 Patent declaration .....                                                  | 2016 |
| 6  | 1 Scope .....                                                                 | 2017 |
| 7  | 2 Normative references .....                                                  | 2017 |
| 8  | 3 Terms, definitions, symbols, abbreviated terms and conventions .....        | 2018 |
| 9  | 3.1 Terms and definitions .....                                               | 2018 |
| 10 | 3.1.1 Common terms and definitions .....                                      | 2019 |
| 11 | 3.1.2 CPF 2: Additional terms and definitions .....                           | 2022 |
| 12 | 3.2 Symbols and abbreviated terms.....                                        | 2023 |
| 13 | 3.2.1 Common symbols and abbreviated terms .....                              | 2023 |
| 14 | 3.2.2 CPF 2: Additional symbols and abbreviated terms .....                   | 2023 |
| 15 | 3.3 Conventions .....                                                         | 2024 |
| 16 | 4 Overview of FSCP 2/1 (CIP Safety™).....                                     | 2024 |
| 17 | 4.1 General .....                                                             | 2024 |
| 18 | 4.2 FSCP 2/1 .....                                                            | 2025 |
| 19 | 5 General .....                                                               | 2026 |
| 20 | 5.1 External documents providing specifications for the profile .....         | 2026 |
| 21 | 5.2 Safety functional requirements .....                                      | 2026 |
| 22 | 5.3 Safety measures .....                                                     | 2026 |
| 23 | 5.4 Safety communication layer structure .....                                | 2027 |
| 24 | 5.5 Relationships with FAL (and DLL, PhL) .....                               | 2028 |
| 25 | 5.5.1 General .....                                                           | 2028 |
| 26 | 5.5.2 Data types .....                                                        | 2028 |
| 27 | 6 Safety communication layer services .....                                   | 2028 |
| 28 | 6.1 Introduction .....                                                        | 2028 |
| 29 | 6.2 Connection object .....                                                   | 2028 |
| 30 | 6.2.1 General .....                                                           | 2028 |
| 31 | 6.2.2 Class attribute extensions .....                                        | 2028 |
| 32 | 6.2.3 Service extensions .....                                                | 2029 |
| 33 | 6.2.4 Explicit message response format for SafetyOpen and SafetyClose .....   | 2030 |
| 34 | 6.3 Connection Manager object .....                                           | 2030 |
| 35 | 6.3.1 General .....                                                           | 2030 |
| 36 | 6.3.2 ForwardOpen for safety .....                                            | 2031 |
| 37 | 6.3.3 Safety network segment .....                                            | 2033 |
| 38 | 6.3.4 Originator rules for calculating the connection parameter CRC .....     | 2036 |
| 39 | 6.3.5 SafetyOpen processing flowcharts .....                                  | 2036 |
| 40 | 6.3.6 Checks required by Multipoint producers with existing connections ..... | 2039 |
| 41 | 6.3.7 Electronic key usage for safety .....                                   | 2040 |
| 42 | 6.3.8 RPI vs. API in safety connections .....                                 | 2040 |
| 43 | 6.3.9 Application path construction for safety .....                          | 2040 |
| 44 | 6.3.10 Safety Validator connection types .....                                | 2041 |
| 45 | 6.3.11 Application reply data in a successful SafetyOpen response .....       | 2043 |
| 46 | 6.3.12 Unsuccessful SafetyOpen response .....                                 | 2045 |
| 47 | 6.3.13 ForwardClose for safety .....                                          |      |

|    |       |                                                                                  |      |
|----|-------|----------------------------------------------------------------------------------|------|
| 48 | 6.4   | Identity object.....                                                             | 2047 |
| 49 | 6.4.1 | General .....                                                                    | 2047 |
| 50 | 6.4.2 | Changes to common services .....                                                 | 2047 |
| 51 | 6.4.3 | Extensions for CP 16/3 devices .....                                             | 2048 |
| 52 | 6.5   | Link objects .....                                                               | 2048 |
| 53 | 6.5.1 | DeviceNet object changes .....                                                   | 2048 |
| 54 | 6.5.2 | TCP/IP Interface object changes .....                                            | 2049 |
| 55 | 6.5.3 | SERCOS III Link object .....                                                     | 2049 |
| 56 | 6.6   | Safety Supervisor object.....                                                    | 2050 |
| 57 | 6.6.1 | General .....                                                                    | 2050 |
| 58 | 6.6.2 | Safety Supervisor class attributes.....                                          | 2051 |
| 59 | 6.6.3 | Subclasses .....                                                                 | 2051 |
| 60 | 6.6.4 | Safety Supervisor instance attributes.....                                       | 2051 |
| 61 | 6.6.5 | Semantics .....                                                                  | 2054 |
| 62 | 6.6.6 | Subclasses .....                                                                 | 2061 |
| 63 | 6.6.7 | Safety Supervisor common services .....                                          | 2061 |
| 64 | 6.6.8 | Safety Supervisor behavior .....                                                 | 2072 |
| 65 | 6.7   | Safety Validator object .....                                                    | 2078 |
| 66 | 6.7.1 | General .....                                                                    | 2078 |
| 67 | 6.7.2 | Class attributes .....                                                           | 2078 |
| 68 | 6.7.3 | Instance attributes .....                                                        | 2079 |
| 69 | 6.7.4 | Class services .....                                                             | 2084 |
| 70 | 6.7.5 | Instance services.....                                                           | 2084 |
| 71 | 6.7.6 | Object behavior .....                                                            | 2085 |
| 72 | 6.8   | Connection Configuration Object .....                                            | 2088 |
| 73 | 6.8.1 | General .....                                                                    | 2088 |
| 74 | 6.8.2 | Class attribute extensions .....                                                 | 2088 |
| 75 | 6.8.3 | Instance attributes, additions and extensions. ....                              | 2088 |
| 76 | 6.8.4 | Instance attribute semantics extensions or restrictions for safety .....         | 2090 |
| 77 | 6.8.5 | Special Safety Related Parameters – (Attribute 13) .....                         | 2094 |
| 78 | 6.8.6 | Object-specific services .....                                                   | 2099 |
| 79 | 6.8.7 | Common service extensions for safety.....                                        | 2099 |
| 80 | 6.8.8 | Object behavior .....                                                            | 2101 |
| 81 | 7     | Safety communication layer protocol .....                                        | 2102 |
| 82 | 7.1   | Safety PDU format .....                                                          | 2102 |
| 83 | 7.1.1 | Safety PDU encoding .....                                                        | 2102 |
| 84 | 7.1.2 | Safety CRC .....                                                                 | 2114 |
| 85 | 7.2   | Communication protocol behavior.....                                             | 2115 |
| 86 | 7.2.1 | Sequence of safety checks .....                                                  | 2115 |
| 87 | 7.2.2 | Connection termination.....                                                      | 2115 |
| 88 | 7.2.3 | Cross checking error .....                                                       | 2115 |
| 89 | 7.3   | Time stamp operation.....                                                        | 2116 |
| 90 | 7.4   | Rollover counts in the EF .....                                                  | 2116 |
| 91 | 7.5   | Protocol sequence diagrams .....                                                 | 2117 |
| 92 | 7.5.1 | General .....                                                                    | 2117 |
| 93 | 7.5.2 | Normal safety transmission.....                                                  | 2117 |
| 94 | 7.5.3 | Lost, corrupted and delayed message transmission.....                            | 2118 |
| 95 | 7.5.4 | Lost, corrupted or delayed message transmission with production<br>repeated..... | 2118 |
| 96 |       |                                                                                  |      |

|     |        |                                                                         |      |
|-----|--------|-------------------------------------------------------------------------|------|
| 97  | 7.5.5  | Point-to-point ping .....                                               | 2122 |
| 98  | 7.5.6  | Multipoint ping on CP 2/3 Safety.....                                   | 2123 |
| 99  | 7.5.7  | Multipoint ping on CP 2/2 safety networks .....                         | 2124 |
| 100 | 7.5.8  | Multipoint ping – retry with success .....                              | 2125 |
| 101 | 7.5.9  | Multipoint ping – retry with timeout .....                              | 2126 |
| 102 | 7.6    | Safety protocol definition .....                                        | 2126 |
| 103 | 7.6.1  | General .....                                                           | 2126 |
| 104 | 7.6.2  | High level view of a safety device .....                                | 2126 |
| 105 | 7.6.3  | Safety Validator object .....                                           | 2127 |
| 106 | 7.6.4  | Relationship between SafetyValidatorServer and                          |      |
| 107 |        | SafetyValidatorClient .....                                             | 2127 |
| 108 | 7.6.5  | Extended Format time stamp rollover handling .....                      | 2128 |
| 109 | 7.6.6  | SafetyValidatorClient function definition .....                         | 2132 |
| 110 | 7.6.7  | SafetyValidatorServer function definition .....                         | 2140 |
| 111 | 7.7    | Safety message and protocol data specifications.....                    | 2153 |
| 112 | 7.7.1  | Mode octet .....                                                        | 2153 |
| 113 | 7.7.2  | Time Stamp Section .....                                                | 2153 |
| 114 | 7.7.3  | Time Coordination Message .....                                         | 2153 |
| 115 | 7.7.4  | Time correction message.....                                            | 2154 |
| 116 | 7.7.5  | Safety data production.....                                             | 2155 |
| 117 | 7.7.6  | Producer dynamic variables.....                                         | 2161 |
| 118 | 7.7.7  | Producer per consumer dynamic variables .....                           | 2163 |
| 119 | 7.7.8  | Consumer data variables .....                                           | 2164 |
| 120 | 7.7.9  | Consumer input static variables .....                                   | 2166 |
| 121 | 7.7.10 | Consumer dynamic variables .....                                        | 2166 |
| 122 | 8      | Safety communication layer management.....                              | 2168 |
| 123 | 8.1    | Overview .....                                                          | 2168 |
| 124 | 8.2    | Definition of the measures used during connection establishment .....   | 2169 |
| 125 | 8.3    | Originator-Target relationship validation .....                         | 2172 |
| 126 | 8.4    | Detection of mis-routed connection requests .....                       | 2173 |
| 127 | 8.5    | SafetyOpen processing .....                                             | 2173 |
| 128 | 8.6    | Ownership management .....                                              | 2173 |
| 129 | 8.7    | Bridging different physical layers .....                                | 2174 |
| 130 | 8.8    | Safety connection establishment .....                                   | 2175 |
| 131 | 8.8.1  | Overview .....                                                          | 2175 |
| 132 | 8.8.2  | Basic facts for connection establishment .....                          | 2176 |
| 133 | 8.8.3  | Configuring safety connections .....                                    | 2176 |
| 134 | 8.8.4  | Network time expectation multiplier .....                               | 2177 |
| 135 | 8.8.5  | Establishing connections .....                                          | 2179 |
| 136 | 8.8.6  | Recommendations for consumer number allocation .....                    | 2182 |
| 137 | 8.8.7  | Recommendations for connection establishment .....                      | 2183 |
| 138 | 8.8.8  | Ownership establishment.....                                            | 2183 |
| 139 | 8.8.9  | Ownership use cases .....                                               | 2184 |
| 140 | 8.8.10 | PID/CID usage and establishment .....                                   | 2186 |
| 141 | 8.8.11 | Proper PID/CID usage in multipoint and point-to-point connections ..... | 2187 |
| 142 | 8.8.12 | Network supported services.....                                         | 2189 |
| 143 | 8.8.13 | FSCP 2/1 safety device type.....                                        | 2190 |
| 144 | 8.9    | Safety configuration process .....                                      | 2193 |
| 145 | 8.9.1  | Introduction to safety configuration .....                              | 2193 |

|     |        |                                                                  |      |
|-----|--------|------------------------------------------------------------------|------|
| 146 | 8.9.2  | Configuration goals .....                                        | 2193 |
| 147 | 8.9.3  | Configuration overview .....                                     | 2194 |
| 148 | 8.9.4  | User configuration guidelines .....                              | 2195 |
| 149 | 8.9.5  | Configuration process SIL3 justification .....                   | 2196 |
| 150 | 8.9.6  | Device functions for tool configuration .....                    | 2196 |
| 151 | 8.9.7  | Password security .....                                          | 2197 |
| 152 | 8.9.8  | SNCT interface services .....                                    | 2197 |
| 153 | 8.9.9  | Configuration lock .....                                         | 2197 |
| 154 | 8.9.10 | Effect of configuration lock on device behavior .....            | 2198 |
| 155 | 8.9.11 | Configuration ownership .....                                    | 2199 |
| 156 | 8.9.12 | Configuration mode .....                                         | 2199 |
| 157 | 8.9.13 | Measures used to ensure integrity of configuration process ..... | 2199 |
| 158 | 8.9.14 | Download process .....                                           | 2201 |
| 159 | 8.9.15 | Verification process .....                                       | 2204 |
| 160 | 8.9.16 | Verification process .....                                       | 2206 |
| 161 | 8.9.17 | Configuration error analysis .....                               | 2207 |
| 162 | 8.10   | Electronic Data Sheets extensions for safety .....               | 2211 |
| 163 | 8.10.1 | General rules for EDS based safety devices .....                 | 2211 |
| 164 | 8.10.2 | EDS extensions for safety .....                                  | 2211 |
| 165 | 8.11   | Requirements for CP 2/2 .....                                    | 2216 |
| 166 | 8.11.1 | EPI rules for safety messages that travel over CP 2/2 .....      | 2216 |
| 167 | 8.11.2 | Default safety I/O service .....                                 | 2216 |
| 168 | 8.11.3 | Duplicate IP detection .....                                     | 2216 |
| 169 | 8.11.4 | Priority for safety connections .....                            | 2217 |
| 170 | 8.12   | Requirements for CP 2/3 .....                                    | 2217 |
| 171 | 8.12.1 | Allocation of CP 2/3 identifiers .....                           | 2217 |
| 172 | 8.12.2 | Additional requirements .....                                    | 2219 |
| 173 | 8.13   | CP 16/3 requirements .....                                       | 2219 |
| 174 | 8.13.1 | General architecture for CPF 2 on CP 16/3 .....                  | 2219 |
| 175 | 8.13.2 | Baseline FSCP 2/1 on CP 16/3 device .....                        | 2220 |
| 176 | 8.13.3 | Supported objects and services in CP 16/3 devices .....          | 2220 |
| 177 | 8.13.4 | Transport layer requirements .....                               | 2221 |
| 178 | 8.13.5 | FSCP 2/1 and the CP 16/3 device model .....                      | 2223 |
| 179 | 8.13.6 | UNID assignment on CP 16/3 .....                                 | 2224 |
| 180 | 9      | System requirements .....                                        | 2226 |
| 181 | 9.1    | Indicators and switches .....                                    | 2226 |
| 182 | 9.1.1  | General indicator requirements .....                             | 2226 |
| 183 | 9.1.2  | LED indications for setting the device UNID .....                | 2226 |
| 184 | 9.1.3  | Module Status LED .....                                          | 2226 |
| 185 | 9.1.4  | Indicator warning .....                                          | 2227 |
| 186 | 9.1.5  | Network Status LED .....                                         | 2227 |
| 187 | 9.1.6  | Switches .....                                                   | 2228 |
| 188 | 9.2    | Installation guidelines .....                                    | 2230 |
| 189 | 9.3    | Safety function response time .....                              | 2230 |
| 190 | 9.3.1  | Overview .....                                                   | 2230 |
| 191 | 9.3.2  | Network time expectation .....                                   | 2231 |
| 192 | 9.3.3  | Equations for calculating network reaction times .....           | 2232 |
| 193 | 9.4    | Duration of demands .....                                        | 2234 |
| 194 | 9.5    | Constraints for calculation of system characteristics .....      | 2234 |

|     |                       |                                                                   |      |
|-----|-----------------------|-------------------------------------------------------------------|------|
| 195 | 9.5.1                 | Number of nodes .....                                             | 2234 |
| 196 | 9.5.2                 | Network PFH .....                                                 | 2234 |
| 197 | 9.5.3                 | Bit Error Rate (BER) .....                                        | 2236 |
| 198 | 9.6                   | Maintenance.....                                                  | 2237 |
| 199 | 9.7                   | Safety manual .....                                               | 2237 |
| 200 | 10                    | Assessment.....                                                   | 2237 |
| 201 | Annex A (informative) | Additional information for functional safety communication        |      |
| 202 |                       | profiles of CPF 2 .....                                           | 2238 |
| 203 | A.1                   | Hash function example code.....                                   | 2238 |
| 204 | A.2                   | .....                                                             | 2252 |
| 205 | Annex B (informative) | Information for assessment of the functional safety               |      |
| 206 |                       | communication profiles of CPF 2 .....                             | 2253 |
| 207 | Bibliography.....     |                                                                   | 2254 |
| 208 |                       |                                                                   |      |
| 209 | Table 1 –             | Communications errors and detection measures matrix.....          | 2027 |
| 210 | Table 2 –             | New class attributes .....                                        | 2029 |
| 211 | Table 3 –             | Service extensions .....                                          | 2030 |
| 212 | Table 4 –             | SafetyOpen and SafetyClose response format .....                  | 2030 |
| 213 | Table 5 –             | Safety network segment identifier.....                            | 2033 |
| 214 | Table 6 –             | Safety network segment definition .....                           | 2033 |
| 215 | Table 7 –             | Safety network segment router format .....                        | 2035 |
| 216 | Table 8 –             | Safety Network Segment Extended Format .....                      | 2035 |
| 217 | Table 9 –             | Multipoint producer parameter evaluation rules .....              | 2040 |
| 218 | Table 10 –            | ForwardOpen setting options for safety connections .....          | 2042 |
| 219 | Table 11 –            | Network connection parameters for safety connections .....        | 2043 |
| 220 | Table 12 –            | CP 2/3 Safety target application reply (size: 10 octets).....     | 2043 |
| 221 | Table 13 –            | EF CP 2/3 Safety target application reply (size: 14 octets) ..... | 2044 |
| 222 | Table 14 –            | SafetyOpen target application reply (size: 18 octets) .....       | 2044 |
| 223 | Table 15 –            | EF SafetyOpen target application reply (size: 22 octets).....     | 2044 |
| 224 | Table 16 –            | New and extended error codes for safety .....                     | 2045 |
| 225 | Table 17 –            | SafetyOpen error event guidance table.....                        | 2046 |
| 226 | Table 18 –            | Identity object common service changes .....                      | 2048 |
| 227 | Table 19 –            | Identity object extensions for CP 16/3 devices.....               | 2048 |
| 228 | Table 20 –            | New DeviceNet object instance attribute .....                     | 2048 |
| 229 | Table 21 –            | New TCP/IP Interface object instance attribute.....               | 2049 |
| 230 | Table 22 –            | SERCOS III Link object class attributes .....                     | 2049 |
| 231 | Table 23 –            | SERCOS III Link object instance attributes.....                   | 2050 |
| 232 | Table 24 –            | SERCOS III Link Object Common Services .....                      | 2050 |
| 233 | Table 25 –            | Safety Supervisor class attributes .....                          | 2051 |
| 234 | Table 26 –            | Safety Supervisor instance attributes .....                       | 2051 |
| 235 | Table 27 –            | Device status attribute state values .....                        | 2055 |
| 236 | Table 28 –            | Exception status attribute format .....                           | 2056 |
| 237 | Table 29 –            | Common exception detail attribute values .....                    | 2057 |
| 238 | Table 30 –            | Exception detail format summary.....                              |      |

|     |                                                                                          |      |
|-----|------------------------------------------------------------------------------------------|------|
| 239 | Table 31 – Summary of device behavior for various CFUNID values .....                    | 2059 |
| 240 | Table 32 – Safety Supervisor common services .....                                       | 2061 |
| 241 | Table 33 – Safety Supervisor object specific services .....                              | 2061 |
| 242 | Table 34 – Configure_Request message structure .....                                     | 2063 |
| 243 | Table 35 – Validate_Configuration message structure .....                                | 2064 |
| 244 | Table 36 – Validate_Configuration success message structure .....                        | 2064 |
| 245 | Table 37 – Validate_Configuration error code .....                                       | 2064 |
| 246 | Table 38 – Validate_Configuration extended codes .....                                   | 2064 |
| 247 | Table 39 – Set_Password message structure .....                                          | 2067 |
| 248 | Table 40 – Reset_Password message structure .....                                        | 2067 |
| 249 | Table 41 – Configuration_Lock/Unlock message structure .....                             | 2067 |
| 250 | Table 42 – Mode_Change message structure .....                                           | 2068 |
| 251 | Table 43 – Safety_Reset message structure .....                                          | 2068 |
| 252 | Table 44 – Safety Supervisor safety reset types .....                                    | 2069 |
| 253 | Table 45 – Attribute bit map parameter .....                                             | 2069 |
| 254 | Table 46 – Reset processing rules for reset types .....                                  | 2069 |
| 255 | Table 47 – Propose_TUNID service .....                                                   | 2070 |
| 256 | Table 48 – Apply_TUNID service .....                                                     | 2070 |
| 257 | Table 49 – Safety Supervisor events .....                                                | 2072 |
| 258 | Table 50 – State event matrix for Safety Supervisor .....                                | 2073 |
| 259 | Table 51 – Configuration owner control vs. device state .....                            | 2076 |
| 260 | Table 52 – State mapping of Safety Supervisor to Identity object .....                   | 2077 |
| 261 | Table 53 – Safety Supervisor object event mapping .....                                  | 2077 |
| 262 | Table 54 – Identity object event mapping .....                                           | 2078 |
| 263 | Table 55 – Safety Validator class attributes .....                                       | 2078 |
| 264 | Table 56 – Safety Validator instance attributes .....                                    | 2079 |
| 265 | Table 57 – Safety Validator state assignments .....                                      | 2081 |
| 266 | Table 58 – Safety Validator type, bit field assignments .....                            | 2081 |
| 267 | Table 59 – Multipoint producer SafetyOpen parameter evaluation rules .....               | 2083 |
| 268 | Table 60 – Safety Validator class services .....                                         | 2084 |
| 269 | Table 61 – Safety Validator instance services .....                                      | 2084 |
| 270 | Table 62 – Safety Validator Get_Attributes_All service data .....                        | 2085 |
| 271 | Table 63 – Safety Validator state event matrix .....                                     | 2087 |
| 272 | Table 64 – State mapping between Safety Supervisor and Safety Validator objects .....    | 2087 |
| 273 | Table 65 – Connection configuration object class attribute extensions .....              | 2088 |
| 274 | Table 66 – Connection Configuration Object instance attribute additions/extensions ..... | 2088 |
| 275 | Table 67 – Connection flag bit definitions .....                                         | 2090 |
| 276 | Table 68 – O-to-T connection parameters .....                                            | 2091 |
| 277 | Table 69 – T-to-O connection parameters .....                                            | 2092 |
| 278 | Table 70 – Data map formats .....                                                        | 2093 |
| 279 | Table 71 – Data map format 0 .....                                                       | 2094 |
| 280 | Table 72 – Data map format 1 .....                                                       | 2094 |
| 281 | Table 73 – Target device's SCCRC values .....                                            | 2096 |

|     |                                                                                  |             |
|-----|----------------------------------------------------------------------------------|-------------|
| 282 | Table 74 – Target device's SCTS values.....                                      | 2096        |
| 283 | Table 75 – Time correction connection parameters for multipoint connection ..... | 2097        |
| 284 | Table 76 – Format Type attribute meaning .....                                   | 2098        |
| 285 | Table 77 – Format Status attribute meaning.....                                  | 2099        |
| 286 | Table 78 – Connection Configuration Object-specific services .....               | 2099        |
| 287 | Table 79 – Get_Attributes_All Response service data (added attributes ) .....    | 2100        |
| 288 | Table 80 – Get_Attributes_All Response service data (added parameters ) .....    | 2100        |
| 289 | Table 81 – Set_Attributes_All Request service data (added attributes) .....      | 2100        |
| 290 | Table 82 – Set_Attributes_All Response service data (added parameters ).....     | 2101        |
| 291 | Table 83 – State Mapping between Safety Supervisor and the CCO objects .....     | 2101        |
| 292 | Table 84 – Connection sections and PDU formats.....                              | 2103        |
| 293 | Table 85 – Mode octet variables .....                                            | 2104        |
| 294 | Table 86 – Time Stamp variables.....                                             | 2107        |
| 295 | Table 87 – Time Coordination message variables .....                             | 2108        |
| 296 | Table 88 – Time Correction Message variables.....                                | 2110        |
| 297 | Table 89 – CRC polynomials used .....                                            | 2114        |
| 298 | Table 90 – Connection sections and message formats.....                          | 2115        |
| 299 | Table 91 – Data reception - Link triggered .....                                 | 2143        |
| 300 | Table 92 – Time_Correction reception - Link triggered .....                      | 2143        |
| 301 | Table 93 – Data reception - Application triggered.....                           | 2143        |
| 302 | Table 94 – Time_Correction reception - Application triggered .....               | 2143        |
| 303 | Table 95 – Consuming application – Safety data monitoring .....                  | 2144        |
| 304 | Table 96 – Producer connection status determination .....                        | 2155        |
| 305 | Table 97 – Consuming safety connection status .....                              | 2165        |
| 306 | Table 98 – Connection establishment errors and measures to detect errors.....    | 2169        |
| 307 | Table 99 – SNN Date/Time allocations.....                                        | 2169        |
| 308 | Table 100 – SNN legal range of time values .....                                 | 2170        |
| 309 | Table 101 – Safety connection parameters .....                                   | 2177        |
| 310 | Table 102 – SafetyOpen summary .....                                             | 2180        |
| 311 | Table 103 – Originator/Target service mapping.....                               | 2190        |
| 312 | Table 104 – Unsupported originator/target service types.....                     | 2191        |
| 313 | Table 105 – Configuration goals .....                                            | 2194        |
| 314 | Table 106 – Configuration owner control vs. device state.....                    | 2199        |
| 315 | Table 107 – Errors and detection measures .....                                  | 2208        |
| 316 | Table 108 – Object Class section keywords .....                                  | 2211        |
| 317 | <b>Table 109- Safety Classx entry format .....</b>                               | <b>2212</b> |
| 318 | Table 110 – Parameter class keywords.....                                        | 2213        |
| 319 | Table 111 – New Connection Manager section keywords for safety .....             | 2213        |
| 320 | Table 112 – Connection Manager field usage for safety .....                      | 2214        |
| 321 | Table 113 – Connection parameter field settings for safety .....                 | 2216        |
| 322 | Table 114 – CP 2/3 ID assignment rules .....                                     | 2217        |
| 323 | Table 115 – LED indications for setting UNID .....                               | 2226        |
| 324 | Table 116 – Module Status LED.....                                               | 2227        |

|     |                                                                                    |             |
|-----|------------------------------------------------------------------------------------|-------------|
| 325 | Table 117 – Network status LED states .....                                        | 2227        |
| 326 | Table 118 – Connection reaction time type – producing/consuming applications ..... | 2232        |
| 327 |                                                                                    |             |
| 328 | Figure 1 – Relationships of IEC 61784-3 with other standards (machinery) .....     | 2014        |
| 329 | Figure 2 – Relationships of IEC 61784-3 with other standards (process).....        | 2015        |
| 330 | Figure 3 – Relationship of Safety Validators .....                                 | 2025        |
| 331 | Figure 4 – Communication layers.....                                               | 2028        |
| 332 | Figure 5 – ForwardOpen with safety network segment .....                           | 2032        |
| 333 | Figure 6 – Safety network target format .....                                      | 2034        |
| 334 | Figure 7 – Target Processing SafetyOpen with no configuration data (Form 2         |             |
| 335 | SafetyOpen) .....                                                                  | 2037        |
| 336 | Figure 8 – Target Processing for SafetyOpen with configuration data (Form 1        |             |
| 337 | SafetyOpen) .....                                                                  | 2038        |
| 338 | Figure 9 – Originator logic to determine which format to use .....                 | 2039        |
| 339 | Figure 10 – Applying device configuration.....                                     | 2065        |
| 340 | Figure 11 – Configure and Validate processing flowcharts .....                     | 2066        |
| 341 | <b>Figure 12 – UNID handling during “Waiting for TUNID” .....</b>                  | <b>2071</b> |
| 342 | Figure 13 – Safety Supervisor state diagram.....                                   | 2072        |
| 343 | Figure 14 – Configuration, testing and locked relationships.....                   | 2076        |
| 344 | Figure 15 – Safety connection types .....                                          | 2082        |
| 345 | Figure 16 – Safety Validator state transition diagram .....                        | 2086        |
| 346 | Figure 17 – Logic for Auto-detecting format type.....                              | 2098        |
| 347 | Figure 18 – Connection Configuration Object state diagram.....                     | 2102        |
| 348 | Figure 19 – Connection Configuration Object data flow .....                        | 2102        |
| 349 | Figure 20 – Format of the mode octet .....                                         | 2104        |
| 350 | Figure 21 – 1 or 2 octet data section, Base Format .....                           | 2104        |
| 351 | Figure 22 – 1 or 2 octet data section, Extended Format .....                       | 2105        |
| 352 | Figure 23 – 3 to 250 octet data section format, Base Format .....                  | 2105        |
| 353 | Figure 24 – 3 to 250 octet data section format, Extended Format.....               | 2106        |
| 354 | Figure 25 – Time Stamp section format, Base Format.....                            | 2107        |
| 355 | Figure 26 – BF Time Coordination message encoding .....                            | 2108        |
| 356 | Figure 27 – EF Time Coordination message encoding .....                            | 2108        |
| 357 | Figure 28 – BF Time Correction message encoding .....                              | 2109        |
| 358 | Figure 29 – EF Time Correction message encoding .....                              | 2109        |
| 359 | Figure 30 – 1 or 2 octet point-to-point PDU encoding.....                          | 2111        |
| 360 | Figure 31 – 1 or 2 Octet multipoint PDU encoding.....                              | 2111        |
| 361 | Figure 32 – 1 or 2 Octet, multipoint, Format 2 safety connection format .....      | 2112        |
| 362 | Figure 33 – 3 to 250 Octet Point-to-point PDU encoding .....                       | 2112        |
| 363 | Figure 34 – 3 to 248 Octet Multipoint PDU encoding .....                           | 2113        |
| 364 | Figure 35 – 3 to 248 Octet, Multipoint, safety connection format .....             | 2113        |
| 365 | Figure 36 – CRC Calculation order for Extended Format messages .....               | 2114        |
| 366 | <b>Figure 37 – Time stamp sequence .....</b>                                       | <b>2116</b> |
| 367 | Figure 38 – Sequence diagram of a normal producer/consumer safety sequence.....    | 2117        |

|     |                                                                                         |      |
|-----|-----------------------------------------------------------------------------------------|------|
| 368 | Figure 39 – Sequence diagram of a normal producer/consumer safety sequence              |      |
| 369 | (production repeated) .....                                                             | 2118 |
| 370 | Figure 40 – Sequence diagram of a corrupted producer to consumer message .....          | 2119 |
| 371 | Figure 41 – Sequence diagram of a lost producer to consumer message .....               | 2119 |
| 372 | Figure 42 – Sequence diagram of a delayed message .....                                 | 2120 |
| 373 | Figure 43 – Sequence diagram of a corrupted producer to consumer message with           |      |
| 374 | production repeated .....                                                               | 2121 |
| 375 | Figure 44 – Sequence diagram of a connection terminated due to delays .....             | 2121 |
| 376 | Figure 45 – Sequence diagram of a failure of safety CRC check .....                     | 2122 |
| 377 | <b>Figure 46 – Sequence diagram of a point-to-point ping - normal response</b> .....    | 2122 |
| 378 | Figure 47 – Sequence diagram of a successful multipoint ping, CP 2/3 safety .....       | 2124 |
| 379 | Figure 48 – Sequence diagram of a successful multipoint ping, CP 2/2 safety .....       | 2125 |
| 380 | Figure 49 – Sequence diagram of a multipoint ping retry.....                            | 2125 |
| 381 | Figure 50 – Sequence diagram of a multipoint ping timeout .....                         | 2126 |
| 382 | Figure 51 – Safety device reference model entity relation diagram.....                  | 2127 |
| 383 | Figure 52 – Two devices interchanging safety data via a SafetyValidatorClient and a     |      |
| 384 | SafetyValidatorServer .....                                                             | 2128 |
| 385 | Figure 53 – Point-to-point, originating consumer. target producer .....                 | 2129 |
| 386 | Figure 54 – Point-to-point, originator producer, target consumer.....                   | 2130 |
| 387 | Figure 55 – Multi-point, originator consumer, target producer .....                     | 2131 |
| 388 | Figure 56 – Safety production data flow .....                                           | 2132 |
| 389 | Figure 57 – Consumer safety data monitoring .....                                       | 2141 |
| 390 | Figure 58 – SafetyValidatorServer - application triggered .....                         | 2142 |
| 391 | Figure 59 – Target ownership .....                                                      | 2172 |
| 392 | Figure 60 – SafetyOpen forms .....                                                      | 2173 |
| 393 | Figure 61 – Connection ownership state chart .....                                      | 2174 |
| 394 | Figure 62 – SafetyOpen UNID mapping .....                                               | 2174 |
| 395 | Figure 63 – Common CPF 2 application layer .....                                        | 2175 |
| 396 | Figure 64 – End-to-End routing example.....                                             | 2175 |
| 397 | Figure 65 – Sources for safety related connection parameters .....                      | 2178 |
| 398 | Figure 66 – Parameter mapping between originator and target .....                       | 2179 |
| 399 | Figure 67 – CP 2/3 Safety connection establishment in targets for Form 2a SafetyOpen... | 2181 |
| 400 | Figure 68 – General sequence to detect configuration is required .....                  | 2182 |
| 401 | Figure 69 – PID/CID exchanges for two originator scenarios.....                         | 2187 |
| 402 | Figure 70 – Seed generation for multipoint connections .....                            | 2188 |
| 403 | Figure 71 – PID/CID runtime handling.....                                               | 2189 |
| 404 | Figure 72 – Connection categories and supported services.....                           | 2191 |
| 405 | Figure 73 – Recommended connection types.....                                           | 2192 |
| 406 | Figure 74 – Logic-to-logic supported services .....                                     | 2192 |
| 407 | Figure 75 – Recommended connection types for logic to logic .....                       | 2193 |
| 408 | Figure 76 – Configuration data transfers .....                                          | 2194 |
| 409 | Figure 77 – Protection measures in safety devices .....                                 | 2196 |
| 410 | Figure 78 – Configuration, testing and locked relationships.....                        | 2198 |
| 411 | Figure 79 – Originator's configuration data .....                                       |      |

|     |                                                                                   |      |
|-----|-----------------------------------------------------------------------------------|------|
| 412 | Figure 80 – SNCT to device download process .....                                 | 2202 |
| 413 | Figure 81 – SNCT Downloads to originators that perform Form 1 configuration ..... | 2203 |
| 414 | Figure 82 – Protection from locking and ownership .....                           | 2205 |
| 415 | Figure 83 – Example of read back and comparison of original and printout .....    | 2205 |
| 416 | Figure 84 – Diverse display without full data read back .....                     | 2206 |
| 417 | Figure 85 – Verification process including all alternatives .....                 | 2207 |
| 418 | <b>Figure 86 – Baseline FSCP 2/1 on CP 16/3 device</b> .....                      | 2220 |
| 419 | Figure 87 – FSCP 2/1 Adaptation Layer and SMP interaction .....                   | 2222 |
| 420 | <b>Figure 88 – FSCP 2/1 Adaptation</b> .....                                      | 2223 |
| 421 | Figure 89 – CP 16/3 device model .....                                            | 2224 |
| 422 | Figure 90 – Adding a standard module to a modular device .....                    | 2225 |
| 423 | <b>Figure 91 – Safety device NodeID processing logic</b> .....                    | 2230 |
| 424 | Figure 92 – Safety function response time .....                                   | 2231 |
| 425 | Figure 93 – Safety function response time components .....                        | 2233 |
| 426 | Figure 94 – Network protocol reliability block diagram (RBD) .....                | 2234 |
| 427 | Figure 95 – Network PFH summary .....                                             | 2235 |
| 428 | Figure 96 – Extended Format PFH summary .....                                     | 2236 |
| 429 |                                                                                   |      |
| 430 |                                                                                   |      |
| 431 |                                                                                   |      |
| 432 |                                                                                   |      |

## INTERNATIONAL ELECTROTECHNICAL COMMISSION

**INDUSTRIAL COMMUNICATION NETWORKS –  
PROFILES –****Part 3-2: Functional safety fieldbuses –  
Additional specifications for CPF 2**

## FOREWORD

- 1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as “IEC Publication(s)”). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
  - 2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
  - 3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
  - 4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
  - 5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
  - 6) All users should ensure that they have the latest edition of this publication.
  - 7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
  - 8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
- International Standard IEC 61784-3-2 has been prepared by subcommittee 65C: Industrial networks, of IEC technical committee 65: Industrial process measurement, control and automation.

This third edition cancels and replaces the second edition published in 2010. This edition constitutes a technical revision. The main changes with respect to the previous edition are listed below (and highlighted in yellow in this document).

- Added detailed requirements for use of FSCP 2/1 in conjunction with CP 16/3 (see 4.1, 6.4.3, 6.5.3, 8.2, 8.13, and miscellaneous references when referencing CPF 2 networks)
- Defined object class section keywords for safety to EDS file definition in 8.10.2.1
- New sections on safety CRC overview in 7.1.2.1 and Rollover counts for EF format in 7.4
- Corrections to PFH calculations in 9.5.2
- Change from MACID to NodeID as general reference to network identifier
- Miscellaneous minor corrections made since the last publication

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

| FDIS         | Report on voting |
|--------------|------------------|
| 65C/XXX/FDIS | 65C/XXX/RVD      |

491  
492 Full information on the voting for the approval of this standard can be found in the report on  
493 voting indicated in the above table.

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

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

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

- 501 • reconfirmed,  
502 • withdrawn,  
503 • replaced by a revised edition, or  
504 • amended.

505

506 The National Committees are requested to note that for this publication the stability date  
507 is 20??.

508 THIS TEXT IS INCLUDED FOR THE INFORMATION OF THE NATIONAL COMMITTEES AND WILL BE  
509 DELETED AT THE PUBLICATION STAGE.

510

**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.**

511

512

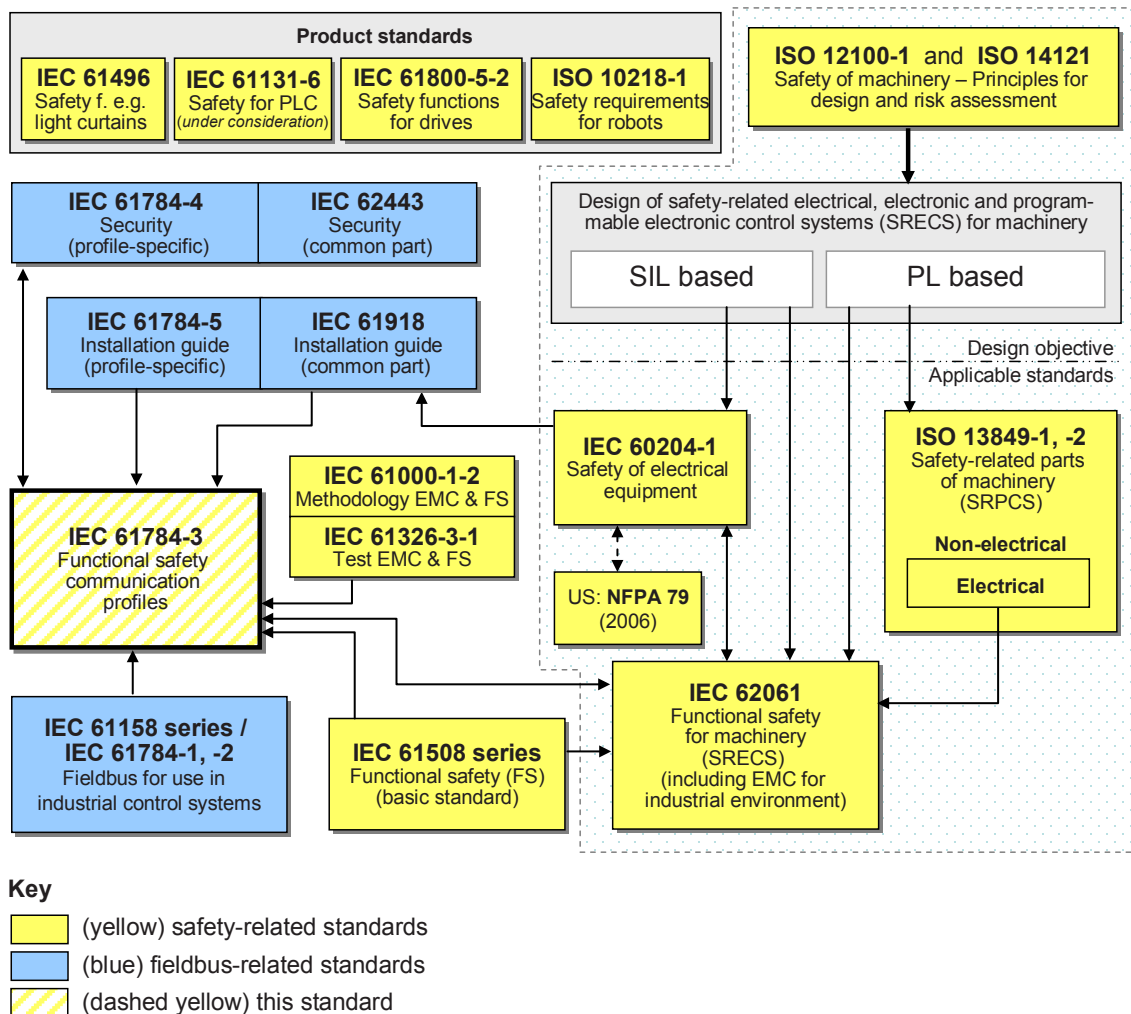
## 0 Introduction

### 0.1 General

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

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

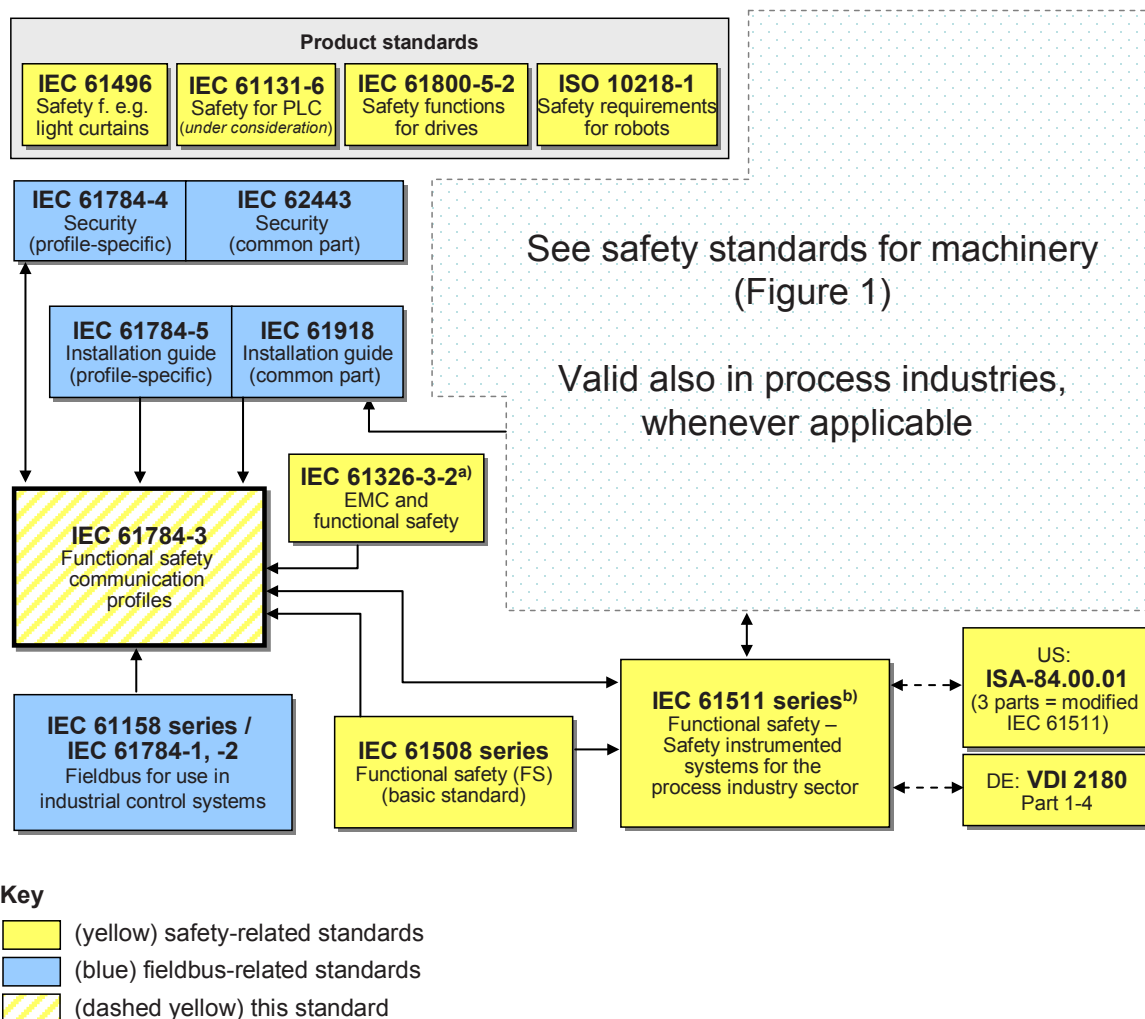
Figure 1 shows the relationships between this standard and relevant safety and fieldbus standards in a machinery environment.



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

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

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



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

<sup>b</sup> EN ratified.

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

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

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

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

This standard describes:

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

- 551 – individual description of functional safety profiles for several communication profile
- 552 families in IEC 61784-1 and IEC 61784-2;
- 553 – safety layer extensions to the communication service and protocols sections of the
- 554 IEC 61158 series.
- 555

## 556 0.2 Patent declaration

557 The International Electrotechnical Commission (IEC) draws attention to the fact that it is  
 558 claimed that compliance with this document may involve the use of patents concerning the  
 559 functional safety communication profiles for family 2 as follows, where the [xx] notation  
 560 indicates the holder of the patent rights:

|              |      |                                                                                                  |
|--------------|------|--------------------------------------------------------------------------------------------------|
| US 6,631,476 | [RA] | Safety network for industrial controller providing redundant connections on single media         |
| US 6,701,198 | [RA] | Safety network for industrial controller allowing initialization on standard networks            |
| US 6,721,900 | [RA] | Safety network for industrial controller having reduced bandwidth requirements                   |
| US 6,891,850 | [RA] | Network independent safety protocol for industrial controller                                    |
| US 6,915,444 | [RA] | Network independent safety protocol for industrial controller using data manipulation techniques |

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

562 The holder of these patent rights has assured the IEC that he/she is willing to negotiate  
 563 licences either free of charge or under reasonable and non-discriminatory terms and  
 564 conditions with applicants throughout the world. In this respect, the statement of the holder of  
 565 these patent rights is registered with IEC.

566 Information may be obtained from:

[RA] Rockwell Automation, Inc.  
 1201 S. Second Street  
 Milwaukee, WI 53204  
 USA  
 Attention: Intellectual Property Dept.

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

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

573

574

## INDUSTRIAL COMMUNICATION NETWORKS – PROFILES –

### Part 3-2: Functional safety fieldbuses – Additional specifications for CPF 2

#### 1 Scope

This part of the IEC 61784-3 series specifies a safety communication layer (services and protocol) based on CPF 2 of IEC 61784-1, IEC 61784-2 and IEC 61158 Type 2. 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<sup>1</sup> defines mechanisms for the transmission of safety-relevant messages among participants within a distributed network using fieldbus technology in accordance with the requirements of IEC 61508 series<sup>2</sup> for functional safety. These mechanisms may be used in various industrial applications such as process control, manufacturing automation and machinery.

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

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

#### 2 Normative references

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

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

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

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

IEC 61158-3-2, *Industrial communication networks – Fieldbus specifications – Part 3-2: Data-link layer service definition – Type 2 elements*

IEC 61158-3-19, *Industrial communication networks – Fieldbus specifications – Part 3-19: Data-link layer service definition – Type 19 elements*

IEC 61158-4-2, *Industrial communication networks – Fieldbus specifications – Part 4-2: Data-link layer protocol specification – Type 2 elements*

IEC 61158-4-19, *Industrial communication networks – Fieldbus specifications – Part 4-19: Data-link layer protocol specification – Type 19 elements*

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

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

- 617 IEC 61158-5-2, *Industrial communication networks – Fieldbus specifications – Part 5-2:*  
618 *Application layer service definition – Type 2 elements*
- 619 IEC 61158-5-19, *Industrial communication networks – Fieldbus specifications – Part 5-19:*  
620 *Application layer service definition – Type 19 elements*
- 621 IEC 61158-6-2, *Industrial communication networks – Fieldbus specifications – Part 6-2:*  
622 *Application layer protocol specification – Type 2 elements*
- 623 IEC 61158-6-19, *Industrial communication networks – Fieldbus specifications – Part 6-19:*  
624 *Application layer protocol specification – Type 19 elements*
- 625 IEC 61326-3-1, *Electrical equipment for measurement, control and laboratory use – EMC*  
626 *requirements – Part 3-1: Immunity requirements for safety-related systems and for equipment*  
627 *intended to perform safety related functions (functional safety) – General industrial*  
628 *applications*
- 629 IEC 61326-3-2, *Electrical equipment for measurement, control and laboratory use – EMC*  
630 *requirements – Part 3-2: Immunity requirements for safety-related systems and for equipment*  
631 *intended to perform safety related functions (functional safety) – Industrial applications with*  
632 *specified electromagnetic environment*
- 633 IEC 61508 (all parts), *Functional safety of electrical/electronic/programmable electronic*  
634 *safety-related systems*
- 635 IEC 61784-1, *Industrial communication networks – Profiles – Part 1: Fieldbus profiles*
- 636 IEC 61784-2, *Industrial communication networks – Profiles – Part 2: Additional fieldbus*  
637 *profiles for real-time networks based on ISO/IEC 8802-3*
- 638 IEC 61784-3:2010, *Industrial communication networks – Profiles – Part 3: Functional safety*  
639 *fieldbuses – General rules and profile definitions*
- 640 IEC 61784-5-2, *Industrial communication networks – Profiles – Part 5: Installation of*  
641 *fieldbuses – Installation profiles for CPF 2*
- 642 IEC 61918, *Industrial communication networks – Installation of communication networks in*  
643 *industrial premises*
- 644 IEC 62026-3, *Low-voltage switchgear and controlgear – Controller-device interfaces (CDIs) –*  
645 *Part 3: DeviceNet*
- 646 ISO 13849-1, *Safety of machinery – Safety-related parts of control systems – Part 1: General*  
647 *principles for design*
- 648 ISO 15745-2:2003, *Industrial automation systems and integration – Open systems application*  
649 *integration framework – Part 2: Reference description for ISO 11898-based control systems*
- 650 ISO 15745-3:2003, *Industrial automation systems and integration – Open systems application*  
651 *integration framework – Part 3: Reference description for IEC 61158-based control systems*
- 652 ISO 15745-4:2003, *Industrial automation systems and integration – Open systems application*  
653 *integration framework – Part 4: Reference description for Ethernet-based control systems*
- 654 **3 Terms, definitions, symbols, abbreviated terms and conventions**
- 655 **3.1 Terms and definitions**
- 656 For the purposes of this document, the following terms and definitions apply.

657 **3.1.1 Common terms and definitions**

658 **3.1.1.1**

659 **availability**

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

662 **3.1.1.2**

663 **black channel**

664 *communication channel* without available evidence of design or validation according to  
665 IEC 61508

666 **3.1.1.3**

667 **bridge**

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

669 **3.1.1.4**

670 **communication channel**

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

672 **3.1.1.5**

673 **communication system**

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

676 **3.1.1.6**

677 **connection**

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

679 **3.1.1.7**

680 **Cyclic Redundancy Check (CRC)**

681 <value> redundant data derived from, and stored or transmitted together with, a block of data  
682 in order to detect data corruption

683 <method> procedure used to calculate the redundant data

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

686 NOTE 2 See also [34], [35]<sup>3</sup>.

687 **3.1.1.8**

688 **error**

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

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

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

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

695 **3.1.1.9**

696 **failure**

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

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

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

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

<sup>3</sup> Figures in square brackets refer to the bibliography.

- 703 **3.1.1.10**  
 704 **fault**  
 705 abnormal condition that may cause a reduction in, or loss of, the capability of a functional unit  
 706 to perform a required function
- 707 NOTE IEC 191-05-01 defines “fault” as a state characterized by the inability to perform a required function,  
 708 excluding the inability during preventive maintenance or other planned actions, or due to lack of external  
 709 resources.
- 710 [IEC 61508-4:2010, modified], [ISO/IEC 2382-14.01.10, modified]
- 711 **3.1.1.11**  
 712 **fieldbus**  
 713 *communication system* based on serial data transfer and used in industrial automation or  
 714 process control applications
- 715 **3.1.1.12**  
 716 **frame**  
 717 denigrated synonym for DLPDU
- 718 **3.1.1.13**  
 719 **hash function**  
 720 (mathematical) function that maps values from a (possibly very) large set of values into a  
 721 (usually) smaller range of values
- 722 NOTE 1 Hash functions can be used to detect data corruption.
- 723 NOTE 2 Common hash functions include parity, checksum or CRC.
- 724 [IEC/TR 62210, modified]
- 725 **3.1.1.14**  
 726 **hazard**  
 727 state or set of conditions of a system that, together with other related conditions will inevitably  
 728 lead to harm to persons, property or environment
- 729 **3.1.1.15**  
 730 **master**  
 731 active communication entity able to initiate and schedule communication activities by other  
 732 stations which may be masters or slaves
- 733 **3.1.1.16**  
 734 **message**  
 735 ordered series of octets intended to convey information  
 736 [ISO/IEC 2382-16.02.01, modified]
- 737 **3.1.1.17**  
 738 **nuisance trip**  
 739 spurious trip with no harmful effect
- 740 NOTE Internal abnormal errors can be caused in communication systems such as wireless transmission, for  
 741 example by too many retries in the presence of interferences.
- 742 **3.1.1.18**  
 743 **performance level (PL)**  
 744 discrete level used to specify the ability of safety-related parts of control systems to perform a  
 745 safety function under foreseeable conditions  
 746 [ISO 13849-1]
- 747 **3.1.1.19**  
 748 **redundancy**  
 749 existence of means, in addition to the means which would be sufficient for a functional unit to  
 750 perform a required function or for data to represent information
- 751 NOTE The definition in IEC 61508-4 is the same, with additional example and notes.
- 752 [IEC 61508-4:2010, modified], [ISO/IEC 2382-14.01.12, modified]

**3.1.1.20****reliability**

probability that an automated system can perform a required function under given conditions for a given time interval ( $t_1, t_2$ )

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

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

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

NOTE 4 Reliability differs from availability.

[IEC 62059-11, modified]

**3.1.1.21****risk**

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

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

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

**3.1.1.22****safety communication layer (SCL)**

communication layer that includes all the necessary measures to ensure safe transmission of data in accordance with the requirements of IEC 61508

**3.1.1.23****safety connection**

connection that utilizes the safety protocol for communications transactions

**3.1.1.24****safety data**

data transmitted across a safety network using a safety protocol

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

**3.1.1.25****safety device**

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

**3.1.1.26****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]

**3.1.1.27****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, 5.2.4 and addressed by the functional safety communication profiles defined in this part.

**3.1.1.28****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

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

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

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

811 [IEC 61508-4:2010]

812 **3.1.1.29**  
813 **safety measure**

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

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

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

818 **3.1.1.30**  
819 **safety-related application**

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

822 **3.1.1.31**  
823 **safety-related system**

824 system performing *safety functions* according to IEC 61508

825 **3.1.1.32**  
826 **slave**

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

829 **3.1.1.33**  
830 **spurious trip**

831 trip caused by the safety system without a process demand

832 **3.1.1.34**  
833 **time stamp**

834 time information included in a *message*

835 **3.1.2 CPF 2: Additional terms and definitions**

836 **3.1.2.1**  
837 **base format**

838 format used for connection RPIs of less than 100 ms or for applications where dropped  
839 connections can be tolerated

840 **3.1.2.2**  
841 **extended format**

842 format used for connection RPIs of more than 100 ms or for applications where there is a  
843 need to avoid dropped connections

844 **3.1.2.3**  
845 **ping**

846 request for the consumer to acknowledge the reception of a message

847 **3.1.2.4**  
848 **ping response**

849 response to a ping

850 **3.1.2.5**  
851 **signature**

852 method of uniquely identifying a set of data

853 NOTE This could be by revision, checksum or some other method that is agreed upon by the originating and  
854 target devices.

855

856 **3.2 Symbols and abbreviated terms**857 **3.2.1 Common symbols and abbreviated terms**

|        |                                                                    |                    |
|--------|--------------------------------------------------------------------|--------------------|
| CP     | Communication Profile                                              | [IEC 61784-1]      |
| CPF    | Communication Profile Family                                       | [IEC 61784-1]      |
| CRC    | Cyclic Redundancy Check                                            |                    |
| DLL    | Data Link Layer                                                    | [ISO/IEC 7498-1]   |
| DLPDU  | Data Link Protocol Data Unit                                       |                    |
| EMC    | Electromagnetic Compatibility                                      |                    |
| EUC    | Equipment Under Control                                            | [IEC 61508-4:2010] |
| E/E/PE | Electrical/Electronic/Programmable Electronic                      | [IEC 61508-4:2010] |
| FAL    | Fieldbus Application Layer                                         | [IEC 61158-5]      |
| FS     | Functional Safety                                                  |                    |
| FSCP   | Functional Safety Communication Profile                            |                    |
| MTBF   | Mean Time Between Failures                                         |                    |
| MTTF   | Mean Time To Failure                                               |                    |
| PDU    | Protocol Data Unit                                                 | [ISO/IEC 7498-1]   |
| PFD    | Probability of dangerous Failure on Demand                         | [IEC 61508-6:2010] |
| PFH    | Average frequency of dangerous failure [h <sup>-1</sup> ] per hour | [IEC 61508-6:2010] |
| PhL    | Physical Layer                                                     | [ISO/IEC 7498-1]   |
| PL     | Performance Level                                                  | [ISO 13849-1]      |
| PLC    | Programmable Logic Controller                                      |                    |
| SCL    | Safety Communication Layer                                         |                    |
| SIL    | Safety Integrity Level                                             | [IEC 61508-4:2010] |

858

859 **3.2.2 CPF 2: Additional symbols and abbreviated terms**

|        |                                                                                              |
|--------|----------------------------------------------------------------------------------------------|
| AIRS   | Already In Requested Mode/State                                                              |
| BER    | Bit Error Rate                                                                               |
| BF     | Base Format                                                                                  |
| CCO    | Connection Configuration Object                                                              |
| CFUNID | Configuration UNID                                                                           |
| CNP    | Connection Point                                                                             |
| CID    | Consumer ID                                                                                  |
| CIP™ 4 | Common Industrial Protocol (application framework shared among CPF 2 communication profiles) |
| CPCRC  | Connection Parameter CRC                                                                     |
| CTM    | Connection Timeout Multiplier                                                                |
| EDS    | Electronic Data Sheet                                                                        |
| EF     | Extended Format                                                                              |
| EPI    | Expected Packet Interval                                                                     |
| LED    | Light Emitting Diode                                                                         |
| MACID  | Device physical address (CP 2/3)                                                             |
| MOD    | Module                                                                                       |

---

<sup>4</sup> For trade name declaration, see Clause 4.

|               |                                                                                                                                                                                                                                       |                 |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| <b>NodeID</b> | For CP 2/3 safety devices, this is the MACID of the device on the network. For CP 2/2 safety devices, this is the IP address of the device on the network. For CP 16/3 safety devices, this is the SDID of the device on the network. |                 |
| NV            | Non-Volatile                                                                                                                                                                                                                          |                 |
| NVS           | Non-Volatile Storage                                                                                                                                                                                                                  |                 |
| OCPUNID       | Output Connection Owner UNID                                                                                                                                                                                                          |                 |
| OSC           | Object State Conflict                                                                                                                                                                                                                 |                 |
| O-to-T        | Originator to Target                                                                                                                                                                                                                  |                 |
| OUNID         | Originator UNID                                                                                                                                                                                                                       |                 |
| PID           | Producer Identifier                                                                                                                                                                                                                   |                 |
| PS            | Power Supply                                                                                                                                                                                                                          |                 |
| Res.          | Reserved                                                                                                                                                                                                                              |                 |
| RPI           | Requested Packet Interval                                                                                                                                                                                                             |                 |
| SCCRC         | Safety Configuration Data CRC                                                                                                                                                                                                         |                 |
| SCID          | Safety Configuration Identified                                                                                                                                                                                                       |                 |
| SCTS          | Safety Configuration Time Stamp                                                                                                                                                                                                       |                 |
| SNCT          | Safety Network Configuration Tool                                                                                                                                                                                                     |                 |
| SNN           | Safety Network Number                                                                                                                                                                                                                 |                 |
| T-to-O        | Target to Originator                                                                                                                                                                                                                  |                 |
| TBD           | To Be Defined                                                                                                                                                                                                                         |                 |
| TNS           | TUNID Not Set                                                                                                                                                                                                                         |                 |
| TUNID         | Target UNID                                                                                                                                                                                                                           |                 |
| UML           | Universal Modeling Language                                                                                                                                                                                                           | [ISO/IEC 19501] |
| UNID          | Unique Network Identifier                                                                                                                                                                                                             |                 |

860

### 861 3.3 Conventions

862 The conventions used for the descriptions of objects services and protocols are described in  
863 IEC 61158-3-2, IEC 61158-4-2, IEC 61158-5-2, and IEC 61158-6-2.

864 As appropriate this part uses flow charts, UML Sequence Diagrams and “C” pseudo-code to  
865 describe concepts.

## 866 4 Overview of FSCP 2/1 (CIP Safety™)

### 867 4.1 General

868 Communication Profile Family 2 (commonly known as CIP™<sup>5</sup>) defines communication profiles  
869 based on IEC 61158-2 Type 2, IEC 61158-3-2, IEC 61158-4-2, IEC 61158-5-2, and  
870 IEC 61158-6-2.

871 Communication Profile Family 16 (commonly known as SERCOS™<sup>6</sup>) defines a communication  
872 profile CP 16/3 based on IEC 61158-3-19, IEC 61158-4-19, IEC 61158-5-19, and  
873 IEC 61158-6-19.

5 CIP™ (Common Industrial Protocol) and CIP Safety™ are trade names of the non-profit organization ODVA, Inc. This information is given for the convenience of users of this International Standard and does not constitute an endorsement by IEC of the trade name holder or any of its products. Compliance to this part does not require use of the trade names CIP™ or CIP Safety™. Use of the trade names CIP™ or CIP Safety™ requires permission of ODVA.

6 SERCOS is a trade name of Interests Group SERCOS interface e.V. This information is given for the convenience of users of this technical report and does not constitute an endorsement by IEC of the trademark holder or any of its products. Compliance does not require use of the trade name. Use of the trade name requires permission of the trade name holder.

The basic profiles CP 2/1, CP 2/2, CP 2/3 and CP 16/3 are defined in IEC 61784-1 and IEC 61784-2. The CPF 2 functional safety communication profile FSCP 2/1 (CIP Safety™<sup>5</sup>) is based on the CPF 2 basic profiles in IEC 61784-1 and IEC 61784-2, the CP 16/3 basic profile in IEC 61784-2, and the safety communication layer specifications defined in this part.

## 4.2 FSCP 2/1

FSCP 2/1 is based on the producer/consumer model of CPF 2. The pairing of producers and consumers is an important part of the relationship that provides the high integrity needed for safety-related applications.

The FSCP 2/1 safety communication layer is specified using a Safety Validator object. This object is responsible for managing the FSCP 2/1 safety connections and serves as the interface between the safety-related application objects and the link layer connections, as shown in Figure 3. The Safety Validator ensures the integrity of the safety data transfers.

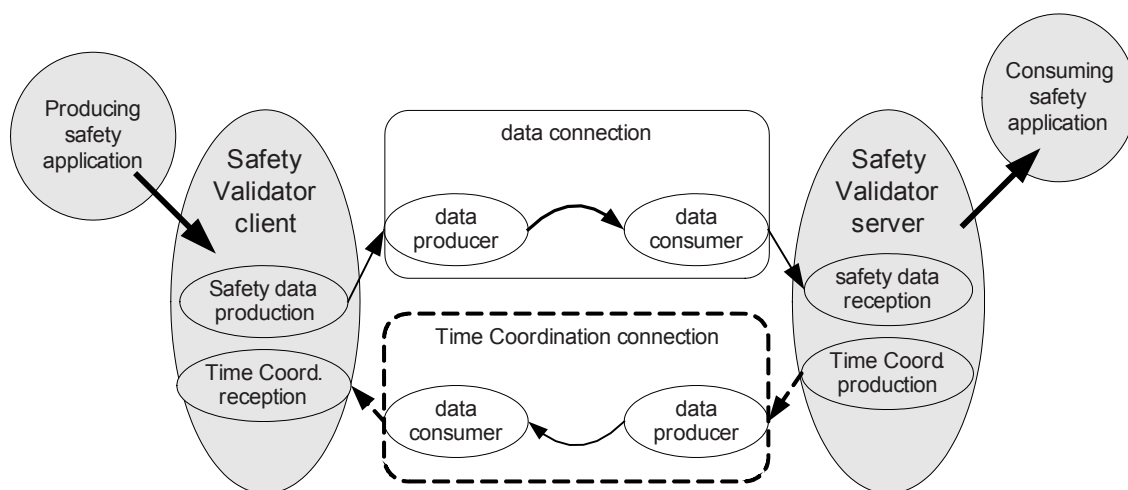


**Figure 3 – Relationship of Safety Validators**

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

- the producing safety-related application uses an instance of a client Safety Validator to produce safety data and ensure time coordination;
- the client uses a link data producer to transmit the data and a link consumer to receive time coordination messages;
- the consuming safety-related application uses a server Safety Validator to receive and check data;
- the server uses a link consumer to receive data and a link producer to transmit time coordination messages.

FSCP 2/1 utilizes the black channel concept. The link producers and consumers have no knowledge of the safety packet and implement no safety function. The responsibility for high-integrity transfer and checking of safety data lies within the Safety Validators.

FSCP 2/1 uses the following measures to ensure the integrity of safety messaging:

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

Messages are produced with a timestamp that allows the consumer to verify the age of data being sent. Identification is encoded into each safety-related message to ensure that the correct consumer is using the message. All safety-related messages use a unique CRC.

909 Safety-related data is sent redundantly. Diverse measures for producing safety-related  
910 messages are used to ensure that standard CPF 2 messages are not interpreted as safety  
911 messages.

## 912 **5 General**

### 913 **5.1 External documents providing specifications for the profile**

914 The following document is especially useful in understanding the design of FSCP 2/1  
915 protocols:

- 916 • GS-ET-26 [33]

### 917 **5.2 Safety functional requirements**

918 The following requirements shall apply to the development of devices that implement the  
919 FSCP 2/1 protocol. The same requirements were used in the development of FSCP 2/1.

- 920 • The FSCP 2/1 protocol is designed to support Safety Integrity Level 3 (SIL3) (see  
921 IEC 61508), and PLe/category 4 (see ISO 13849-1).
- 922 • The safety state for discrete data is the unenergized state (0). For analog values the  
923 unenergized state shall be defined by the safety-related application.
- 924 • The basic requirements for the development of the FSCP 2/1 protocol are in IEC 61784-3.
- 925 • FSCP 2/1 protocol is implemented using a black channel approach; there is no safety  
926 related dependency on the standard CPF 2 communication profiles.
- 927 • Implementations of FSCP 2/1 shall comply with IEC 61508.
- 928 • Environmental conditions shall be according to IEC 61131-2 for the basic levels and  
929 IEC 61326-3-1, IEC 61326-3-2 for the safety margin tests, unless there are specific  
930 product standards.
- 931 • Safety communication and standard communication shall be independent. However,  
932 standard devices and safety devices shall be able to use the same communication  
933 channel.
- 934 • Unless specified in this part, the CPF 2 requirements shall be unchanged for safety.

### 935 **5.3 Safety measures**

936 Table 1 contains the measures used to detect communication errors and the coverage  
937 provided by each measure as used.

938

**Table 1 – Communications errors and detection measures matrix**

| Communication errors                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Safety measures |                  |                  |                           |                  |                          |                                |                                            |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|------------------|------------------|---------------------------|------------------|--------------------------|--------------------------------|--------------------------------------------|
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Sequence number | Time stamp       | Time expectation | Connection authentication | Feedback message | Data integrity assurance | Redundancy with cross checking | Different data integrity assurance systems |
| Corruption                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                 |                  |                  |                           |                  | X                        | X                              |                                            |
| Unintended repetition                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                 | X                |                  |                           |                  | X <sup>a</sup>           | (X) <sup>e</sup>               |                                            |
| Incorrect sequence                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                 | X                |                  |                           |                  | X <sup>a</sup>           | (X) <sup>e</sup>               |                                            |
| Loss                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                 |                  | X <sup>c</sup>   |                           |                  | X <sup>a</sup>           | (X) <sup>e</sup>               |                                            |
| Unacceptable delay                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                 | (X) <sup>e</sup> | X                |                           |                  |                          |                                |                                            |
| Insertion                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                 | X <sup>d</sup>   |                  | X                         |                  | X <sup>a</sup>           | (X) <sup>e</sup>               |                                            |
| Masquerade                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                 | X <sup>d</sup>   |                  | X                         |                  | X <sup>b</sup>           | X <sup>f</sup>                 | X                                          |
| Addressing                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                 |                  |                  | X                         |                  | X <sup>b</sup>           |                                |                                            |
| <p><sup>a</sup> The safety related CRC provides additional protection for communication errors in messages.</p> <p><sup>b</sup> Encoding the unique identifier into the safety related CRC prevent masquerade and addressing errors.</p> <p><sup>c</sup> A message not received within the time expectation will be detected.</p> <p><sup>d</sup> Masquerade or inserted messages will not have the expected time stamp.</p> <p><sup>e</sup> Not claimed for FSCP 2/1.</p> <p><sup>f</sup> Masquerade will likely not have redundant data and will fail the cross-check.</p> |                 |                  |                  |                           |                  |                          |                                |                                            |

939

#### 940 5.4 Safety communication layer structure

941 The safety protocol is layered on top of the standard network protocol (the standard protocol  
 942 stack is a black channel). Figure 4 shows how the safety communication layer is related to the  
 943 existing CPF 2 layers.

944 The safety layers accept safety data from the safety-related application circuit. The safety  
 945 layers then formulate a safety message, transmit the safety message, receive and decode the  
 946 safety message. Once the safety message is decoded and verified, the data is presented to  
 947 the receiving safety-related application circuit.

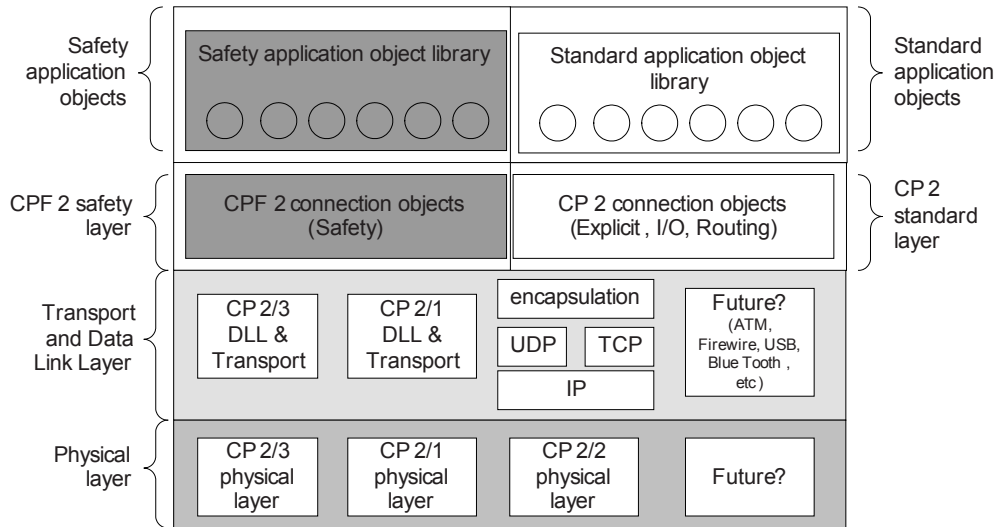


Figure 4 – Communication layers

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

### 5.5.1 General

This safety communication layer shall only be used in conjunction with CPF 2 communication profiles (CP 2/3 (DeviceNet™ 7), CP 2/2 (EtherNet/IP™ 8), and CP 16/3 (SERCOS III™ 9)). There are no requirements of CPF 2 communications profiles other than those defined in this part.

### 5.5.2 Data types

Profiles defined in this part support all the CPF 2 data types as defined in IEC 61158-5-2.

## 6 Safety communication layer services

### 6.1 Introduction

This subclause defines the extensions to existing CPF 2 objects and new objects for Safety. Safety connections use Class 0 connections for I/O messages. Standard Explicit message connections are used for the establishment of Safety I/O connections.

### 6.2 Connection object

#### 6.2.1 General

Several safety specific class attributes and services are defined to support safety. CP 2/3 Safety nodes which reside on FSCP 2/1 shall implement the SafetyOpen and SafetyClose services of the Connection object.

#### 6.2.2 Class attribute extensions

Table 2 defines the class attributes used by safety devices.

<sup>7</sup> DeviceNet™ is a trade name of the non-profit organization ODVA, Inc. This information is given for the convenience of users of this International Standard and does not constitute an endorsement by IEC of the trade name holder or any of its products. Compliance to this part does not require use of the trade name DeviceNet™. Use of the trade name DeviceNet™ requires permission of ODVA.

<sup>8</sup> EtherNet/IP™ is a trade name of ODVA, Inc. This information is given for the convenience of users of this International Standard and does not constitute an endorsement by IEC of the trade name holder or any of its products. Compliance to this part does not require use of the trade name EtherNet/IP™. Use of the trade name EtherNet/IP™ requires permission of ODVA.

<sup>9</sup> SERCOS and SERCOS interface are trade names of SERCOS International e.V. This information is given for the convenience of users of this International Standard and does not constitute an endorsement by IEC of the trademark holder or any of its products. Compliance to this profile does not require use of the trade name. Use of the trade name requires permission of the trade name holder.

971

Table 2 – New class attributes

| Attrib ID                                                                                                                                                                                                                                                                                                                                                          | Need in implementation | Access rule | N V | Name                                              | Date type  | Description of attribute                                                                    |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|-------------|-----|---------------------------------------------------|------------|---------------------------------------------------------------------------------------------|
| 8                                                                                                                                                                                                                                                                                                                                                                  | Optional               | Get         | V   | Connection request error count                    | UINT       | Diagnostic Counter that is a running count of SafetyOpen or SafetyClose faults <sup>a</sup> |
| 9                                                                                                                                                                                                                                                                                                                                                                  | Optional               | Get         | V   | Safety connection counters                        | STRUCT of: | Status counters                                                                             |
|                                                                                                                                                                                                                                                                                                                                                                    |                        |             |     | SafetyOpen request success count                  | UINT       | Count of successful SafetyOpen requests issued from this node to another target             |
|                                                                                                                                                                                                                                                                                                                                                                    |                        |             |     | SafetyOpen request failure count                  | UINT       | Count of unsuccessful SafetyOpen requests issued from this node to another target           |
|                                                                                                                                                                                                                                                                                                                                                                    |                        |             |     | SafetyClose request success count                 | UINT       | Count of successful SafetyClose requests issued from this node to another target            |
|                                                                                                                                                                                                                                                                                                                                                                    |                        |             |     | SafetyClose request failure count <sup>b</sup>    | UINT       | Count of unsuccessful SafetyClose requests issued from this node to another target          |
|                                                                                                                                                                                                                                                                                                                                                                    |                        |             |     | SafetyOpen indication success count               | UINT       | Count of successful SafetyOpen requests issued from an external originator to this node     |
|                                                                                                                                                                                                                                                                                                                                                                    |                        |             |     | SafetyOpen indication failure count <sup>b</sup>  | UINT       | Count of unsuccessful SafetyOpen requests issued from an external originator to this node   |
|                                                                                                                                                                                                                                                                                                                                                                    |                        |             |     | SafetyClose indication success count              | UINT       | Count of successful SafetyClose requests issued from an external originator to this node    |
|                                                                                                                                                                                                                                                                                                                                                                    |                        |             |     | SafetyClose indication failure count <sup>b</sup> | UINT       | Count of unsuccessful SafetyClose requests issued from an external originator to this node  |
| <sup>a</sup> Attribute 8 is the sum of the 4 failure counters in attribute 9. Having this single attribute represent connection errors can be used in monitoring software to efficiently monitor errors without polling the additional attribute 9 structures. Once attribute 8 is non-zero then the monitoring software can examine attribute 9 for more details. |                        |             |     |                                                   |            |                                                                                             |
| <sup>b</sup> Included in class attribute 8.                                                                                                                                                                                                                                                                                                                        |                        |             |     |                                                   |            |                                                                                             |

972

973 **6.2.3 Service extensions**

974 Table 3 defines services for use by CP 2/3 safety devices on FSCP 2/1. These services shall  
975 be supported by a target device on FSCP 2/1. The SafetyOpen and SafetyClose services,  
976 used in lieu of the ForwardOpen and ForwardClose services of the Connection Manager  
977 object, inherit the identical behavior from those Connection Manager services.

978

**Table 3 – Service extensions**

| Service code                                                                                                  | Need in implementation |          | Service name            | Description of service                                                                                        |
|---------------------------------------------------------------------------------------------------------------|------------------------|----------|-------------------------|---------------------------------------------------------------------------------------------------------------|
|                                                                                                               | Class                  | Instance |                         |                                                                                                               |
| 4D <sub>hex</sub>                                                                                             | Optional               | N/A      | Reset Counters          | This service resets class attributes 8 and 9 to zero                                                          |
| 4E <sub>hex</sub>                                                                                             | Required               | N/A      | SafetyClose             | Used to close a Safety I/O connection. See the ForwardClose service of the Connection Manager object 6.3.13   |
| 54 <sub>hex</sub>                                                                                             | Required               | N/A      | SafetyOpen <sup>a</sup> | Used to establish a safety I/O connection. See the ForwardOpen service of the Connection Manager object 6.3.2 |
| <sup>a</sup> The SafetyOpen service data shall contain a Safety Network Segment in the Connection_Path field. |                        |          |                         |                                                                                                               |

979

**980 6.2.4 Explicit message response format for SafetyOpen and SafetyClose**

981 The SafetyOpen and SafetyClose service responses have a common response format. This  
 982 format contains status information for both success and failure. If the service response is a  
 983 success, response data specific to each service is returned. If the service response is an  
 984 error, a successful FSCP 2/1 status indicated by the general error code FF<sub>hex</sub> is returned,  
 985 along with a variable amount of extended error information.

986 The response format for the SafetyOpen and SafetyClose object Specific services are defined  
 987 in Table 4:

988

**Table 4 – SafetyOpen and SafetyClose response format**

| Parameter name            | Data type      | Description of response parameter                                                        |
|---------------------------|----------------|------------------------------------------------------------------------------------------|
| Reserved                  | USINT          | Reserved                                                                                 |
| General status            | USINT          | One of the general status codes listed in IEC 61158-6-2 (status codes)                   |
| Size of additional status | USINT          | Number of 16 bit words in Additional status array                                        |
| Additional status         | ARRAY of UINT  | Additional status                                                                        |
| Response data             | ARRAY of OCTET | Response data from request or additional error data if general status indicated an error |

989

990 The Response Data and General/Additional Statuses for the SafetyOpen and SafetyClose  
 991 services shall match the Response Data and General/Additional Statuses for the  
 992 ForwardOpen and ForwardClose services of the Connection Manager object, respectively.

**993 6.3 Connection Manager object****994 6.3.1 General**

995 CP 2/2 and CP 16/3 safety devices shall use a ForwardOpen with a Safety Network Segment  
 996 to establish safety connections. This segment uniquely identifies the ForwardOpen service as  
 997 a safety ForwardOpen. Throughout this subclause, the term “SafetyOpen” shall refer to both  
 998 the ForwardOpen service of the Connection Manager object (when containing a Safety  
 999 Network Segment) and the SafetyOpen service of the Connection object.

1000 **6.3.2 ForwardOpen for safety**1001 **6.3.2.1 ForwardOpen for safety contents**

1002 The contents of the ForwardOpen service of the Connection Manager object, including the  
 1003 safety network segment, are outlined in Figure 5 below. The proper settings for the various  
 1004 parameters in the ForwardOpen are given in Figure 5.

| Parameter Name                       |                             | Data Type / Size | Target Destination and Semantics                                                                                                                                                  |
|--------------------------------------|-----------------------------|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Priority/Time_tick                   |                             | OCTET            | Connection manager servicing request                                                                                                                                              |
| Time-out_ticks                       |                             | USINT            | Connection manager servicing request                                                                                                                                              |
| O-to-T Network Connection ID         |                             | UDINT            | Consuming connection instance:: CIP consumed connection ID                                                                                                                        |
| T-to-O Network Connection ID         |                             | UDINT            | Producing connection instance:: CIP producing connection ID                                                                                                                       |
| Connection Serial Number             |                             | UINT             | Value: Unique (to originator) 16-bit number.<br>Destination: Connection manager servicing request                                                                                 |
| Originator Vendor ID                 |                             | UINT             | Connection manager servicing request                                                                                                                                              |
| Originator Serial Number             |                             | UDINT            | Connection manager servicing request                                                                                                                                              |
| Connection Timeout Multiplier        |                             | USINT            | Producing and consuming connection instance: Timeout Multiplier                                                                                                                   |
| Reserved                             |                             | 3 OCTETS         |                                                                                                                                                                                   |
| O-to-T RPI                           |                             | UDINT            | Consuming connection instance: EPR                                                                                                                                                |
| O-to-T Network Connection Parameters | Redundant Owner             | WORD             | Value: 0 (Safety Connections do not support redundancy); Destination: Connection Manager                                                                                          |
|                                      | Connection Type             |                  | Value: Point-to-point;<br>Destination: Connection Manager                                                                                                                         |
|                                      | Priority                    |                  | Value: High Priority;<br>Destination: Connection Manager                                                                                                                          |
|                                      | Fixed/Variable              |                  | Value: Fixed;<br>Destination: Connection Manager                                                                                                                                  |
|                                      | Connection Size (in octets) |                  | Value: Size of safety PDU including the Mode Octet, Actual, Complement, and Time stamp sections<br>Destination: Consuming connection instance: Consumed connection size attribute |
| T-to-O RPI                           |                             | UDINT            | Producing connection instance: EPR                                                                                                                                                |
| T to O Network Connection Parameters | Redundant Owner             | WORD             | Value: 0 (Safety connections do not support redundancy); Destination: Connection Manager                                                                                          |
|                                      | Connection Type             |                  | Value: Point-to-point;<br>Destination: Connection Manager                                                                                                                         |
|                                      | Priority                    |                  | Value: High Priority;<br>Destination: Connection Manager                                                                                                                          |
|                                      | Fixed/Variable              |                  | Value: Fixed;<br>Destination: Connection Manager                                                                                                                                  |
|                                      | Connection Size (in octets) |                  | Value: Size of safety PDU including the Mode Octet, Actual, Complement, and Time stamp sections.<br>Destination: Producing Connection Instance: Produced connection size          |
| Transport Type/Trigger               |                             | SWORD            | Value: Safety single or multipoint.<br>Destination: Validator instance.<br>Trigger always set to Application.<br>Client/Server: depending on direction                            |
| Connection_Path_Size                 |                             | USINT            | Number of 16 bit words in the Connection_Path field – destination is Connection Manager                                                                                           |

| Parameter Name                 |                                 | Data Type / Size                  | Target Destination and Semantics                                                                                                                                            |
|--------------------------------|---------------------------------|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                |                                 |                                   | servicing request.<br>NOTE Value included in CRC calculation does not include the words used for Network/Port segments.                                                     |
| Connection_Path (Padded EPATH) |                                 |                                   |                                                                                                                                                                             |
|                                | Path                            | Variable                          | Consumed by intermediate bridge connection manager(s). Each Router Format-safety Network Segment immediately follows the (CPF 2 - to-CPF 2) bridge for which it is intended |
|                                | Logical Segment: Electronic Key | Vendor ID                         | Value: Electronic Key of required target. Servicing Connection Manager or Connection object                                                                                 |
|                                |                                 | Prod Type                         |                                                                                                                                                                             |
|                                |                                 | Prod Code                         |                                                                                                                                                                             |
|                                |                                 | Compatible/ Major Rev             |                                                                                                                                                                             |
|                                |                                 | Minor Rev                         |                                                                                                                                                                             |
|                                | Application Path 1              | Logical Segment: Class            | Refer to IEC 61158-6-2 for rules on setting/parsing these paths                                                                                                             |
|                                |                                 | Logical Segment: Instance         |                                                                                                                                                                             |
|                                | Application Path 2              | Logical Segment: Connection Point | Refer to IEC 61158-6-2 for rules on setting/parsing these paths                                                                                                             |
|                                | Application Path 3              | Logical Segment: Connection Point | Refer to IEC 61158-6-2 for rules on setting/parsing these paths                                                                                                             |
|                                | Config Data                     | Data Segment: Simple Data         | Configuration data to apply to the Safety-related application object identified by Config Path                                                                              |
|                                | Network Segment:                | Safety Segment Name               | Safety Network Segment                                                                                                                                                      |
|                                |                                 | Segment Size                      | Target format size = 54 octets                                                                                                                                              |
|                                |                                 | Segment Format                    | Target format = 0                                                                                                                                                           |
|                                |                                 | Network Safety Data               | Safety Network Segment data                                                                                                                                                 |

Key

-  = Connection/Safety Validator fields covered by Connection Parameters CRC
-  = Configuration Data Segment covered by SCCV

**Figure 5 – ForwardOpen with safety network segment**

### 6.3.2.2 ForwardOpen for safety for Extended Format

Safety Originators that support the Extended Format may connect to Targets with RPI's of 100 ms or less with either the Extended Format (EF) or the Base Format (BF).

Safety Originators that connect with a CP 2/2 target, a CP 16/3 target, or a CP 2/3 target with a CP 2/2 hop or CP 16/3 hop within the path and have an RPI of greater than 100 ms shall use the Extended Format.

A variety of methods may be used to assure this. EDS files and configuration software can pre-configure the choice, or the originator can use a dynamic algorithm to make the determinations.

The mechanism used by the originator to indicate to a target that the Extended Format is being requested will be with a new Safety Network Segment Format as defined in 6.3.3.

### 6.3.3 Safety network segment

#### 6.3.3.1 Common format

The Safety Connection Parameters Segment Type has been added to the CPF 2 Network Segment definition as segment type 10<sub>hex</sub> (resulting in a segment value of 50<sub>hex</sub>). The updated Network Segment definition is defined in Table 5.

**Table 5 – Safety network segment identifier**

| Network segment type | Network segment name |
|----------------------|----------------------|
| 50 <sub>hex</sub>    | Safety segment       |

The format of the Safety Network Segment is defined in Table 6. This segment type is in the range of Network Segment types, which contains a data size field. The Safety Segment Format parameter, the first parameter in the data area, indicates which data follows.

**Table 6 – Safety network segment definition**

| Octet offset | Field name                    | Data type      | description                                                                                                               |
|--------------|-------------------------------|----------------|---------------------------------------------------------------------------------------------------------------------------|
| 0            | Segment Type                  | SWORD          | Indicates Safety Network Segment (50 <sub>hex</sub> )                                                                     |
| 1            | Network Segment data length   | SWORD          | Length of segment data to follow (in words)                                                                               |
| 2            | Safety Network Segment format | USINT          | Indicates type of Safety Network Segment<br>0 = Target format<br>1 = Router format<br>2 = EF format<br>3 – 255 = Reserved |
| 3 - n        | Safety Network Segment data   | ARRAY of OCTET | Safety Network Segment data, defined by segment format                                                                    |

#### 6.3.3.2 Safety network segment: target format (00<sub>hex</sub>)

The target format is directed at the target of the connection. The value of the Network Segment Data Length parameter shall be 27 (1b<sub>hex</sub>) which corresponds to 27 WORDS. Figure 6 defines the safety network target format.

| Field name                                    | Data type            | Description                                                                                                                                                                                                                                                |
|-----------------------------------------------|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Reserved                                      | SWORD                | Pad                                                                                                                                                                                                                                                        |
| Configuration CRC (SCCRC)                     | UDINT                | CRC-S4 of target Config Data Segment. A value of 0 is an indicator that SCID check can be skipped                                                                                                                                                          |
| Configuration Time Stamp (SCTS)               | DATE_AND_TIME        | Time and Date stamp of the configuration. A value of 0 is an indicator that SCID check can be skipped. 6 octet value (Date: 2 octets, Time: 4 octets)                                                                                                      |
| Time Correction EPI                           | UDINT                | Not used: 0<br>When used: Time Correction Connection Instance:: EPI                                                                                                                                                                                        |
| Time Correction Network Connection Parameters | WORD                 | Network Connection Parameters for the Time Correction connection. This field uses the same definition as the Network Connection Parameter within the Connection Manager object.<br>When not used: 0 (Null).<br>When used: Fixed, High Priority, Multipoint |
| Target_UNID (TUNID)                           | STRUCT of: 10 OCTETS | UNID of the target device. This value is a 10 octet value consisting of the Safety Network Id (6 octets) and the Node Address (4 octet address)                                                                                                            |
| Originator UNID (OUNID)                       | STRUCT of: 10 OCTETS | UNID of the Originator device. This value is a 10 octet value consisting of the Safety Network Id (6 octets) and the Node Address (4 octet address)                                                                                                        |
| Ping_Interval_EPI_Multiplier                  | UINT                 | Number that defines the Ping_Count_Interval for the connection. Valid range of values is given in 7.7.5.10                                                                                                                                                 |
| Time_Coord_Msg_Min_Multiplier                 | UINT                 | For Producing Connection Instance. Valid range is 0 to 7 813                                                                                                                                                                                               |
| Network_Time_Expectation_Multiplier           | UINT                 | For Consuming Connection Instance. Valid range is 1 to 45 313                                                                                                                                                                                              |
| Timeout_Multiplier                            | USINT                | Used by producer and consumer to timeout connections. Valid range 1 to 4                                                                                                                                                                                   |
| Max_Consumer_Number                           | USINT                | Value: 1 (Point-to-point), 2-15(Multipoint)                                                                                                                                                                                                                |
| Connection Parameters CRC (CPCRC)             | UDINT                | CRC-S4 of target connection parameters in this request                                                                                                                                                                                                     |
| Time Correction Connection ID                 | UDINT                | Not Used: FFFFFFFF <sub>hex</sub><br>When used: Time Correction Connection Instance:: Connection ID                                                                                                                                                        |

Key

 = Safety Segment fields covered by Connection Parameters CRC

**Figure 6 – Safety network target format**

### 6.3.3.3 Safety network segment: router format (01<sub>hex</sub>)

The router format is directed at an intermediate router along the connection path when that router needs to know this is a Safety ForwardOpen. Currently, only CP 2/3 routers need this network segment directed to them. The Network Segment is applied to the subnet from which the connection request originated. Router Format Safety Network Segments only appear in the Path portion of the Connection\_Path of a Safety ForwardOpen. The total segment length is 6 words. The safety network segment router format is defined in Table 7.

1042

**Table 7 – Safety network segment router format**

| Field name                                    | Data type | Description                                                                                                                                                                                                                                           |
|-----------------------------------------------|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Reserved                                      | SWORD     | Reserved, value = 0                                                                                                                                                                                                                                   |
| Time Correction Connection ID                 | UDINT     | Not Used: FFFFFFFF <sub>hex</sub><br>When used: Time Correction connection instance:: Connection ID                                                                                                                                                   |
| Time Correction EPI                           | UDINT     | Not used: 0<br>When used: Time Correction connection instance:: EPI                                                                                                                                                                                   |
| Time Correction Network Connection Parameters | WORD      | Network Connection Parameters for the Time Correction connection. This field uses the same definition as the Network Connection Parameter within the Connection Manager object.<br>Not used: 0 (Null).<br>When used: Fixed, High Priority, Multipoint |

1043

**1044 6.3.3.4 Safety network segment: Extended Format (0x02)**

1045 The Extended Format is directed at the target of the connection and shown in Table 8.

1046 All EF safety connections shall be established using the **Extended Format** safety network  
 1047 segment in a Forward Open (CP 2/2 **or CP 16/3**) or a SafetyOpen (CP 2/3).

1048

**Table 8 – Safety Network Segment Extended Format**

| Field Name                                    | Data Type                        | Description                                                                                                                                                                                                                                                |
|-----------------------------------------------|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Reserved                                      | octet                            | Pad                                                                                                                                                                                                                                                        |
| Configuration CRC (SCCRC)                     | UDINT                            | CRC-S32 of target Config Data Segment.<br>A value of 0 is an indicator that SCID check can be skipped                                                                                                                                                      |
| Configuration TimeStamp (SCTS)                | DATE_AND_TIME                    | Time and Date stamp of the configuration. A value of 0 is an indicator that SCID check can be skipped. 6 octet value (Date: 2 octets, Time: 4 octets)                                                                                                      |
| Time Correction EPI                           | UDINT                            | Not used: 0<br>When used: Time Correction Connection Instance:: EPI                                                                                                                                                                                        |
| Time Correction Network Connection Parameters | WORD                             | Network Connection Parameters for the Time Correction connection. This field uses the same definition as the Network Connection Parameter within the Connection Manager object.<br>When not used: 0 (Null).<br>When used: Fixed, High Priority, Multipoint |
| Target_UNID (TUNID)                           | STRUCT of:<br>UINT<br>10: octets | UNID of the target device. This value is a 10 octet value consisting of the Safety Network Id (6 octets) and the Node Address (4 octet address)                                                                                                            |
| Originator UNID (OUNID)                       | STRUCT of:<br>UINT<br>10: octets | UNID of the Originator device. This value is a 10 octet value consisting of the Safety Network Id (6 octets) and the Node Address (4 octet address)                                                                                                        |
| Ping_Interval_EPI_Multiplier                  | UINT                             | Number that defines the Ping_Count_Interval for the connection. Valid range of values is given in 7.7.5.10                                                                                                                                                 |
| Time_Coord_Msg_Min_Multiplier                 | UINT                             | For Producing Connection Instance. Valid range is 0 to 7 813                                                                                                                                                                                               |
| Network_Time_Expectation_Multiplier           | UINT                             | For Consuming Connection Instance. Valid range is <b>1 to 45 313</b>                                                                                                                                                                                       |
| Timeout_Multiplier                            | USINT                            | Used by producer and consumer to timeout connections. Valid range of 1 to 255 for HiAvailabilityFormat                                                                                                                                                     |
| Max_Consumer_Number                           | USINT                            | Value: 1 (Point to point), 2-15(Multipoint)                                                                                                                                                                                                                |

| Field Name                                                                                                                             | Data Type | Description                                                                                                                                                                                                                                                                |
|----------------------------------------------------------------------------------------------------------------------------------------|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Max_Fault_Number                                                                                                                       | UINT      | Used by both producers and consumers to determine how many erroneous packets can be dropped before a connection shall be closed.<br><b>Valid range is 0 to 255<sup>b</sup></b><br>Default = 5.<br>A value of 0 indicates connections shall be closed on any detected error |
| Connection Parameters CRC (CPCRC)                                                                                                      | UDINT     | CRC-S32 of target connection parameters in this request                                                                                                                                                                                                                    |
| Time Correction Connection ID <sup>a</sup>                                                                                             | UDINT     | Not Used: 0xFFFFFFFF<br>When used: Time Correction Connection Instance:: Connection ID                                                                                                                                                                                     |
| Initial Time Stamp <sup>a</sup>                                                                                                        | UINT      | Used by Consumer to initialize Last_Time_Stamp_for_Rollover.<br>Consuming Originator sets to 0xFFFF                                                                                                                                                                        |
| Initial Rollover Value <sup>a</sup>                                                                                                    | UINT      | Used by Consumer to initialize TS_Rollover_Count.<br>Consuming Originator sets to 0xFFFF                                                                                                                                                                                   |
| <sup>a</sup> These fields are NOT included in the CPCRC.<br><sup>b</sup> See 8.8.3 for originator configuration rules and restrictions |           |                                                                                                                                                                                                                                                                            |

1049

#### 1050 6.3.4 Originator rules for calculating the connection parameter CRC

1051 The Connection Parameter CRC (CPCRC) is only calculated when a connection is initially  
1052 configured or when that connection configuration is changed. This value remains static in the  
1053 originator otherwise.

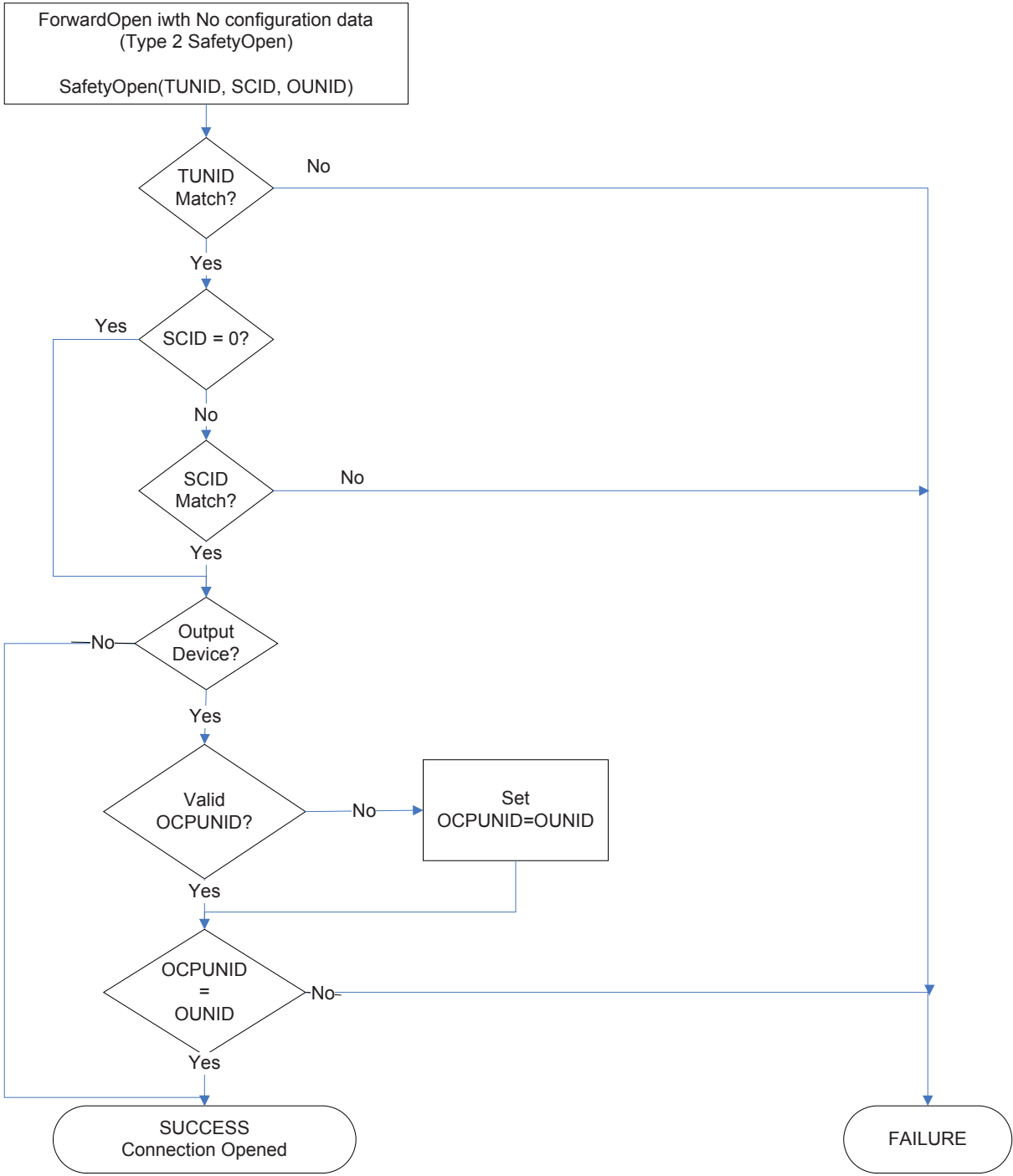
1054 The connection path size in the SafetyOpen changes value depending on whether an  
1055 originator is sending configuration data or not. Since this field is included in the CPCRC  
1056 calculation, originators need to calculate and maintain two values when they support the  
1057 SafetyOpen configuration function. One value is used when configuring a device while  
1058 opening the connection and the other value is used when just opening the connection (no  
1059 configuration data is included).

1060 Also, the path size shall be “pre-adjusted” to remove the path entries that get stripped off by  
1061 routers as the Safety ForwardOpen traverses each sub-net. The requirement is that the  
1062 originator is responsible for calculating the CPCRC value based on what the SafetyOpen or  
1063 ForwardOpen will be when the target receives it so that the target can perform a simple  
1064 calculation in all cases.

#### 1065 6.3.5 SafetyOpen processing flowcharts

1066 The following flowcharts outline the required behavior of a target upon receipt of a  
1067 SafetyOpen:

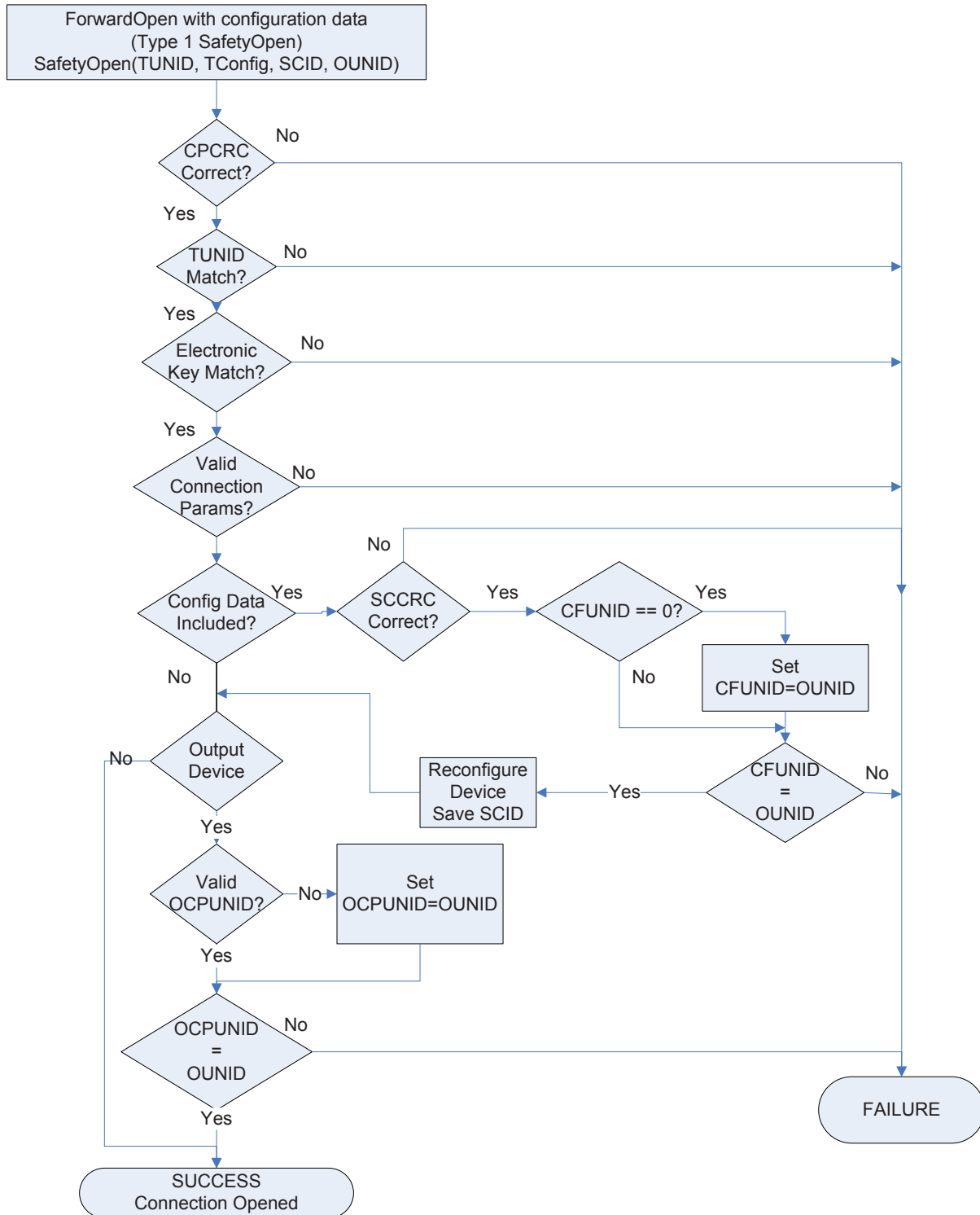
- 1068 a) Verify the Connection Parameter CRC. As depicted in Figure 6, the connection  
1069 parameter CRC covers the SafetyOpen fields that will be used by the target.  
1070 Routers along the path shall not modify these fields;
- 1071 b) The target checks that the electronic key segment matches (see 6.3.7);
- 1072 c) Depending on the type of safety connection, the logic is defined in Figure 7 or  
1073 Figure 8 shall be followed.



Key:

|                                         |                                                |
|-----------------------------------------|------------------------------------------------|
| UNID = Unique Network Identifier        | TUNID = Target's Unique Network Identifier     |
| SCID = Target's Safety Configuration ID | OUNID = Originator's Unique Network Identifier |
| OCF = Output Connection Point           | OCPUNID = Output Connection Owning UNID        |
| CFUNID = Configuration Owning UNID      |                                                |

Figure 7 – Target Processing SafetyOpen with no configuration data (Form 2 SafetyOpen)



Key:

UNID = Unique Network Identifier  
CPCRC = Connection Parameter CRC  
SCCRC= CRC portion of the SCID  
OCPUNID = Output Connection Owning UNID

TUNID = Target's Unique Network Identifier  
SCID = Target's Safety Configuration ID  
OUNID = Originator's Unique Network Identifier  
CFUNID = Configuration Owning UNID

**Figure 8 – Target Processing for SafetyOpen with configuration data  
(Form 1 SafetyOpen)**

Safety Originators that do not support any other means to determine which format to connect with can implement the logic shown in Figure 9 to dynamically determine the format.

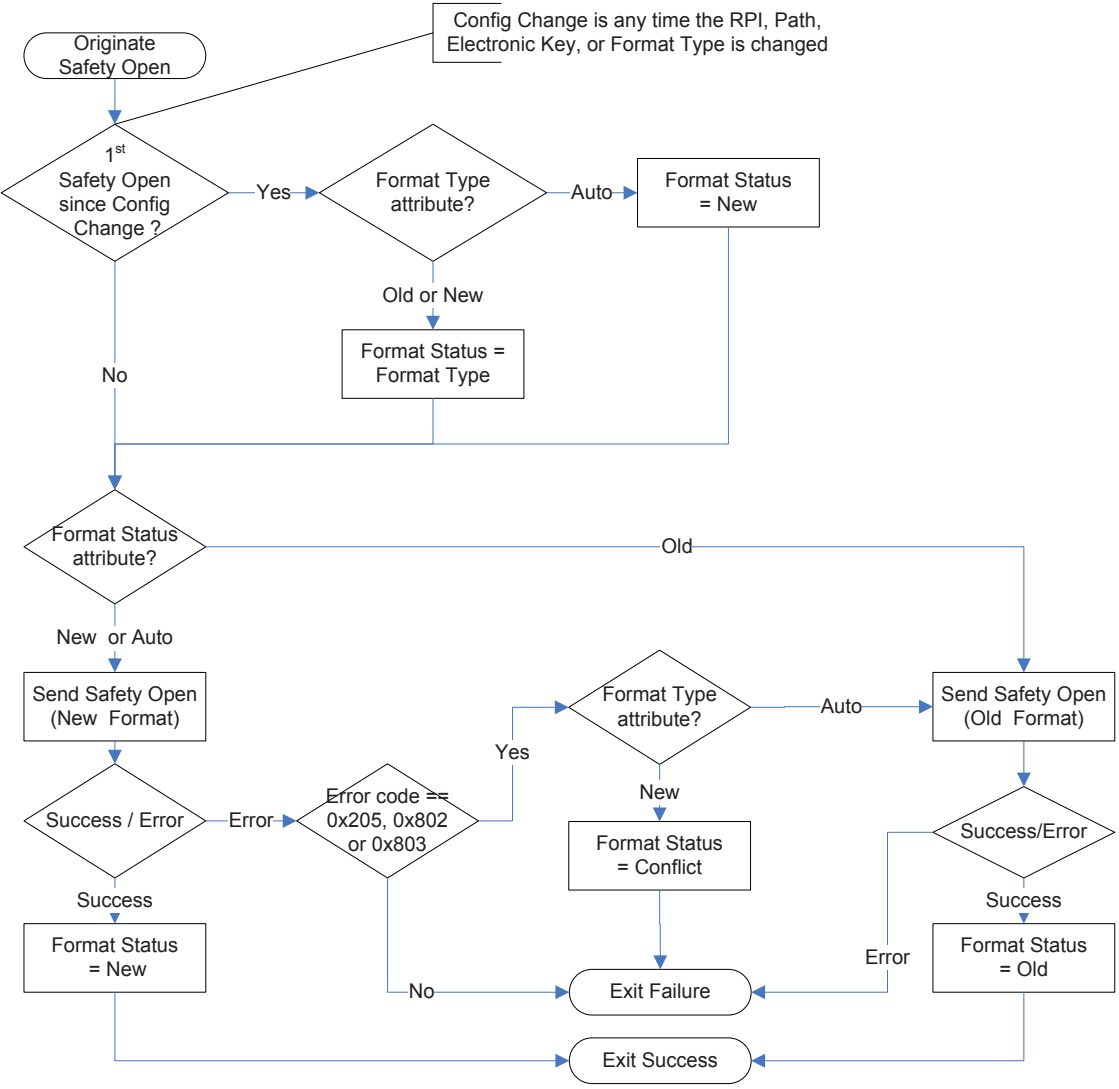


Figure 9 – Originator logic to determine which format to use

6.3.6 Checks required by Multipoint producers with existing connections

There is a distinct possibility that the safety parameters used in a ForwardOpen or SafetyOpen from various consuming originators will not always be the same. A consistent set of rules shall be used for how a Multipoint producing target evaluates these parameters when they conflict with other already established consuming connections. Table 9 defines the multipoint producer parameter evaluation rules.

1092

**Table 9 – Multipoint producer parameter evaluation rules**

| Safety parameter                                                                                                                          | Producer evaluation rule if connection exists          | Error response <sup>a</sup><br>(if appropriate) |                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------|-------------------------------------------------|--------------------------------------------|
|                                                                                                                                           |                                                        | General                                         | Extended                                   |
| Ping_Interval EPI Multiplier                                                                                                              | Shall match existing P.I.E.M.                          | 01 <sub>hex</sub><br>00 <sub>hex</sub>          | 0801 <sub>hex</sub><br>0012 <sub>hex</sub> |
| Time Coord Msg Min Multiplier                                                                                                             | Accept any (all can be different)                      | N/A                                             |                                            |
| Network Time Expectation Multiplier                                                                                                       | Accept any (all can be different)                      | N/A                                             |                                            |
| Timeout_Multiplier                                                                                                                        | Accept any (all can be different)                      | N/A                                             |                                            |
| Max_Consumer_Number                                                                                                                       | Shall match existing<br>Max_Consumer_Number            | 00 <sub>hex</sub><br>01 <sub>hex</sub>          | 0801 <sub>hex</sub><br>002A <sub>hex</sub> |
| T-to-O RPI, O-to-T RPI, and Time<br>Correction RPI                                                                                        | Shall match existing connection<br>RPIs                | 01 <sub>hex</sub>                               | 0111 <sub>hex</sub>                        |
| Network Segment Type                                                                                                                      | Shall match existing connection<br>format <sup>b</sup> | 0x01                                            | 0x803                                      |
| Max_Fault_Number                                                                                                                          | Accept any (all can be different)                      | N/A                                             |                                            |
| <sup>a</sup> At the option of the device developer, another connection could also be opened rather than return an error response.         |                                                        |                                                 |                                            |
| <sup>b</sup> Subsequent connection requests on an existing multi-point connection shall all be the same format as the existing connection |                                                        |                                                 |                                            |

1093

### 1094 6.3.7 Electronic key usage for safety

1095 Safety originators and targets shall meet the following requirements for use of the Electronic  
1096 Key segment within a SafetyOpen.

1097 The Electronic Key segment shall be present in all SafetyOpen or Safety ForwardOpen  
1098 service requests.

1099 The Electronic Key shall always be processed by Target devices with integrity (cannot be  
1100 confirmed externally).

1101 The compatibility bit and behavior in the Electronic Key shall be supported as defined by  
1102 safety originators and targets. Wildcards (fields set to 0) for individual fields within the  
1103 Electronic Key shall not be supported.

### 1104 6.3.8 RPI vs. API in safety connections

1105 Safety devices do not have the ability to negotiate the RPI value. Safety Targets either accept  
1106 the requested RPI because it can be supported, or it rejects it completely. The tolerance  
1107 around an acceptable RPI request shall be  $\pm 128 \mu s$ .

1108 The T-to-O API, O-to-T API, and Time Correction API in a success response shall always be  
1109 the same value received in the SafetyOpen.

### 1110 6.3.9 Application path construction for safety

1111 IEC 61158-6-2 defines a method to construct an application path in a SafetyOpen for 3  
1112 references: one for configuration, one for consumed data and one for produced data.

1113 The possible path types are identified as follows:

1114 A. - [Class] [Assembly] [Instance] [Configuration-instance]

1115 B. - [Class] [Assembly] [Instance] [Producer-instance]

1116 C. - [Class] [Assembly] [Instance] [Consumer-instance]

1117 D. - [Class] [Assembly] [Instance] [Device-defined NULL instance]]

1118 E. - [CNP] [Consumer CNP]

1119 F. - [CNP] [Producer CNP]

1120 G. - [CNP] [Device-defined NULL CNP]

1121 When all 3 paths referenced the same class, they are often formatted in a compressed format:  
1122 (CNP stands for Connection Point).

1123 [Class] [Class #] [Instance] [Instance #] [CNP] [Consumer CNP] [CNP] [Producer CNP]

1124 Since all three paths shall reference the same class, a NULL instance value shall be reserved  
1125 in that class (by the device developers) to use the compressed form for safety. The NULL  
1126 value will be used for the portion of the path that references the Time Coordination connection  
1127 and configuration connection (in non-configuring originators). If a common class reference is  
1128 not practical, the long form shall be used.

1129 The following rules apply to SafetyOpen path construction:

- 1130 • all devices shall support the long form at a minimum;
- 1131 • a Null path or Null connection point shall be used to represent the Time Coordination  
1132 connection;
- 1133 • a Null path or Null connection point shall be used for the configuration path when no  
1134 configuration data can ever be sent on the connection;
- 1135 • on any connections, which can accept a Form 1 SafetyOpen, Originators shall always  
1136 send a valid configuration path even if no configuration data is present (i.e. Form 2a).

1137 The “Null” path or connection point used shall be one of the module’s choosing. The method  
1138 of making this selection in an EDS file will be via the Data Path field in the Connection  
1139 Manager section. Devices configured by configuration applet also shall provide this path.

1140 Safety device designers can choose the path format to specify in their EDS files from the  
1141 following options. The possible three-path combinations for Form 1, 2a SafetyOpen on  
1142 connections, which will accept configuration are:

- 1143 • [A, D, B] for the input connection;
- 1144 • [A, G, F] compressed format for input connections;
- 1145 • [A, C, D] for the output connection;
- 1146 • [A, E, G] compressed format for output connections.

1147 The possible three-path combinations for Form 2a, 2b SafetyOpen on connections, which will  
1148 not accept configuration data are:

- 1149 • [D, D, B] for the input connection;
- 1150 • [D, G, F] compressed format for input connections;
- 1151 • [D, C, D] for the output connection;
- 1152 • [D, E, G] compressed format for output connections.

### 1153 6.3.10 Safety Validator connection types

1154 The Safety Validator function, depending on the safety connection type provided in the  
1155 SafetyOpen, will always require between 2-3 connection resources. The SafetyOpen contains  
1156 the connection information to allow a target to set up these connections appropriately. This  
1157 subclause will show how the connection types are determined by how the SafetyOpen shall be  
1158 filled out.

1159 One basic assumption is that connections for Time Coordination and Time Correction  
1160 messages do not require a path entry since they have an implied path to the Safety Validator  
1161 object coordinating the safety connection. The various connection scenarios are described in  
1162 the Validator object in 6.7.

1163 The Safety Validator function can determine which connection resources will be required by  
 1164 looking at the parameter in the SafetyOpen. The various SafetyOpen parameters as well as  
 1165 the key parameters that the safety function will need to determine the types of connections  
 1166 are defined in Table 10. Connection object instances may not be available due to target  
 1167 identifier capacity or limitations; there may be no unallocated connection identifiers. Or the  
 1168 device may not have the processing throughput to handle the additional connection; etc.  
 1169 Safety Connection objects requires resources similar to standard I/O connections.

1170 **Table 10 – ForwardOpen setting options for safety connections**

| O-to-T connection type | T-to-O connection type | Transport type/ trigger      | App path 1                            | App path 2 <sup>a</sup>   | App path 3 <sup>a</sup>  | Max consumer number | Safety Validator connection type | Key decision factors                       | Target role                                                                                                 |
|------------------------|------------------------|------------------------------|---------------------------------------|---------------------------|--------------------------|---------------------|----------------------------------|--------------------------------------------|-------------------------------------------------------------------------------------------------------------|
| Point-to-point         | Point-to-point         | Application, Class 0, Client | Vendor defined Null Path <sup>b</sup> | Vendor defined Null Path  | Safety Input App. object | 1                   | Point-to-point Producer (Input)  | 2-point-to-point + Client                  | Producing connection: Safety data<br>Consumer connection: Coordination                                      |
| Point-to-point         | Point-to-point         | Application, Class 0, Server | Vendor defined Null Path              | Safety Output App. object | Vendor defined Null Path | 1                   | Point-to-point Consumer (Output) | 2- point-to-point + Server                 | Consuming connection: Safety data<br>Producing connection: coordination                                     |
| Point-to-point         | Multipoint             | Application, Class 0, Client | Vendor defined Null Path              | Vendor defined Null Path  | Safety Input App. object | 2-15                | Multipoint Producer CP 2/3       | 2 – Multipoint + 1 point-to-point + Client | Producing connection: Safety data<br>Producing connection: Correction<br>Consuming connection: coordination |
| Point-to-point         | Multipoint             | Application, Class 0, Client | Vendor defined Null Path              | Vendor defined Null Path  | Safety input app. object | 2-15                | Multipoint Producer CP 2/2       | 1 – Multipoint + 1 point-to-point + Client | Producing connection: Safety data + correction<br>Consuming connection: coordination                        |
| Multipoint             | Point-to-point         | Application, Class 0, Server | Vendor defined Null Path              | Safety output app. object | Vendor defined Null Path | 2-15                | Multipoint Consumer CP 2/3       | 2 – Multipoint + 1 point-to-point + Server | Consuming connection: Safety data<br>Consuming connection: Correction<br>Producing connection: coordination |
| Multipoint             | Point-to-point         | Application, Class 0, Server | Vendor defined Null Path              | Safety output app. object | Vendor defined Null Path | 2-15                | Multipoint Consumer CP 2/2       | 1 – Multipoint + 1 point-to-point + Server | Consuming connection: Safety Data + correction<br>Producing connection: coordination                        |

<sup>a</sup> Input and Output with respect to the network.

<sup>b</sup> Devices configurable via EDS shall define an application Null Path in the EDS file.

Table 11 defines which network connection parameters to use for all three connections associated with each safety connection type.

**Table 11 – Network connection parameters for safety connections**

| Target type             | Network connection parameter | Proper parameter value | Description                         |
|-------------------------|------------------------------|------------------------|-------------------------------------|
| Point-to-point producer | O-to-T                       | 4406 <sub>hex</sub>    | Point-to-point high priority, fixed |
|                         | T-to-O                       | 4408 <sub>hex</sub>    | Point-to-point high priority, fixed |
|                         | Time Correction              | 0000 <sub>hex</sub>    | Not used                            |
| Point-to-point producer | O-to-T                       | 4408 <sub>hex</sub>    | Point-to-point high priority, fixed |
|                         | T-to-O                       | 4406 <sub>hex</sub>    | Point-to-point high priority, fixed |
|                         | Time Correction              | 0000 <sub>hex</sub>    | Not used                            |
| Multipoint producer     | O-to-T                       | 4406 <sub>hex</sub>    | Point-to-point high priority, fixed |
|                         | T-to-O                       | 240E <sub>hex</sub>    | Multipoint high priority, fixed     |
|                         | Time Correction              | 2406 <sub>hex</sub>    | Multipoint high priority, fixed     |

Successful SafetyOpen responses shall return the connection identifiers used, as well as the Consumer\_Number assigned to the originator (always FFFF<sub>hex</sub> for point-to-point connections).

### 6.3.11 Application reply data in a successful SafetyOpen response

The format for a SafetyOpen response for Success is the same as the Forward\_Open\_Reply as defined in IEC 61158-6-2. The data return is defined in Table 12.

The target of a SafetyOpen shall return the data defined in Table 12 through Table 15 in the Application Reply field of the SafetyOpen response. The consumer number and PID reply data is only of significance when the originator is the consumer.

**Table 12 – CP 2/3 Safety target application reply (size: 10 octets)**

| Parameter name                  | Data type  | Description                                                                                                |
|---------------------------------|------------|------------------------------------------------------------------------------------------------------------|
| Consumer_Number                 | UINT       |                                                                                                            |
| PID/CID                         | STRUCT of: | Target Identifier used to generate a PID or CID seed value                                                 |
| Target Vendor Id                | UINT       | Target's Vendor Id                                                                                         |
| Target Device Serial Number     | UDINT      | Target's Device Serial Number                                                                              |
| Target Connection Serial Number | UINT       | Connection Serial Number Target assigned to the connection. The Safety Validator instance Id shall be used |

When the Target of a connection is using the Extended Format on CP 2/2 or CP 16/3 links, it shall use the 14 octet EF SafetyOpen Target Application reply defined in Table 13.

1188

**Table 13 – EF CP 2/3 Safety target application reply (size: 14 octets)**

| Parameter Name <sup>a</sup>                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Data Type  | Description                                                                                                 |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|-------------------------------------------------------------------------------------------------------------|
| Consumer_Number                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | UINT       |                                                                                                             |
| PID/CID                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | STRUCT of: | Target Identifier used to generate a PID or CID seed value                                                  |
| Target Vendor Id                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | UINT       | Target's Vendor Id                                                                                          |
| Target Device Serial Number                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | UDINT      | Target's Device Serial Number                                                                               |
| Target Connection Serial Number                                                                                                                                                                                                                                                                                                                                                                                                                                                             | UINT       | Connection Serial Number Target assigned to the connection. The Safety Validator instance Id should be used |
| Initial Time Stamp <sup>b</sup>                                                                                                                                                                                                                                                                                                                                                                                                                                                             | UINT       | Used by Consumer to initialize Last_Time_Stamp_for_Rollover                                                 |
| Initial Rollover Value <sup>b</sup>                                                                                                                                                                                                                                                                                                                                                                                                                                                         | UINT       | Used by Consumer to initialize TS_Rollover_Count                                                            |
| <p><sup>a</sup> These fields are always present in the Application Reply field. When a CP 2/3 Safety target receives a SafetyOpen that is not multipoint (thus no Time Correction connection is established) the Time_Correction_Connection_ID parameter shall be set to FFFF<sub>hex</sub>. If the target is not a multipoint producer, the consumer number is set to FFFF<sub>hex</sub>.</p> <p><sup>b</sup> Consuming targets should echo back the values received in the SafetyOpen</p> |            |                                                                                                             |

1189

1190

1191

**Table 14 – SafetyOpen target application reply (size: 18 octets)**

| Parameter name <sup>a</sup>                                                                                                                                                                                                                                                                                                                                                                    | Data type  | Description                                                                                                                         |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|-------------------------------------------------------------------------------------------------------------------------------------|
| Consumer_Number                                                                                                                                                                                                                                                                                                                                                                                | UINT       |                                                                                                                                     |
| PID/CID                                                                                                                                                                                                                                                                                                                                                                                        | STRUCT of: | Target Identifier used to generate a PID or CID seed value                                                                          |
| Target Vendor Id                                                                                                                                                                                                                                                                                                                                                                               | UINT       | Target's Vendor Id                                                                                                                  |
| Target Device Serial Number                                                                                                                                                                                                                                                                                                                                                                    | UDINT      | Target's Device Serial Number                                                                                                       |
| Target Connection Serial Number                                                                                                                                                                                                                                                                                                                                                                | UINT       | Connection Serial Number Target assigned to the connection. The Safety Validator instance Id shall be used                          |
| Time_Correction_Connection_ID                                                                                                                                                                                                                                                                                                                                                                  | UDINT      | Connection ID selected by the Target for the Time Correction connection. If chosen by the originator, then the value is echoed back |
| Time_Correction_API                                                                                                                                                                                                                                                                                                                                                                            | UDINT      | Returns same value received in the Request packet                                                                                   |
| <p><sup>a</sup> These fields are always present in the Application Reply field. When a CP 2/3 Safety target receives a SafetyOpen that is not multipoint (thus no Time Correction connection is established) the Time_Correction_Connection_ID parameter shall be set to FFFF<sub>hex</sub>. If the target is not a multipoint producer, the consumer number is set to FFFF<sub>hex</sub>.</p> |            |                                                                                                                                     |

1192

1193 When the Target of a connection is using the Extended Format on CP 2/3, it shall use the 22  
 1194 octet EF SafetyOpen Target Application reply defined in Table 15.

1195

**Table 15 – EF SafetyOpen target application reply (size: 22 octets)**

| Parameter Name <sup>a</sup> | Data Type | Description |
|-----------------------------|-----------|-------------|
|-----------------------------|-----------|-------------|

| Parameter Name <sup>a</sup>                                                                                                                                                                                                                                                                                                                                                                                                                        | Data Type  | Description                                                                                                                         |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|-------------------------------------------------------------------------------------------------------------------------------------|
| Consumer_Number                                                                                                                                                                                                                                                                                                                                                                                                                                    | UINT       |                                                                                                                                     |
| PID/CID                                                                                                                                                                                                                                                                                                                                                                                                                                            | STRUCT of: | Target Identifier used to generate a PID or CID seed value                                                                          |
| Target Vendor Id                                                                                                                                                                                                                                                                                                                                                                                                                                   | UINT       | Target's Vendor Id                                                                                                                  |
| Target Device Serial Number                                                                                                                                                                                                                                                                                                                                                                                                                        | UDINT      | Target's Device Serial Number                                                                                                       |
| Target Connection Serial Number                                                                                                                                                                                                                                                                                                                                                                                                                    | UINT       | Connection Serial Number Target assigned to the connection. The Safety Validator instance Id should be used                         |
| Time_Correction_Connection_ID                                                                                                                                                                                                                                                                                                                                                                                                                      | UDINT      | Connection ID selected by the Target for the Time Correction connection. If chosen by the originator, then the value is echoed back |
| Time_Correction_API                                                                                                                                                                                                                                                                                                                                                                                                                                | UDINT      | Returns same value received in the Request packet                                                                                   |
| Initial Time Stamp <sup>b</sup>                                                                                                                                                                                                                                                                                                                                                                                                                    | UINT       | Used by Consumer to initialize Last_Time_Stamp_for_Rollover                                                                         |
| Initial Rollover Value <sup>b</sup>                                                                                                                                                                                                                                                                                                                                                                                                                | UINT       | Used by Consumer to initialize TS_Rollover_Count                                                                                    |
| <sup>a</sup> These fields are always present in the Application Reply field. When a CP 2/3 target receives a SafetyOpen that is not multipoint (thus no Time Correction connection is established) the Time_Correction_Connection_ID parameter shall be set to 0xFFFF. If the target is not a multipoint producer, the consumer number is set to 0xFFFF.<br><sup>b</sup> Consuming targets should echo back the values received in the SafetyOpen. |            |                                                                                                                                     |

1196

1197 **6.3.12 Unsuccessful SafetyOpen response**

1198 The SafetyOpen has some special error cases that do not map to the existing set of error  
1199 codes, and extends the definition of existing error codes.

1200 Table 16 defines new extended error codes for safety and shows the extended definition of  
1201 existing error codes.

1202

**Table 16 – New and extended error codes for safety**

| General status    | Extended status     | Explanation                                                                                         |
|-------------------|---------------------|-----------------------------------------------------------------------------------------------------|
| 01 <sub>hex</sub> | 0105 <sub>hex</sub> | Ownership conflict or OUNID mismatch. The configuration is already owned by another originator      |
| 01 <sub>hex</sub> | 0106 <sub>hex</sub> | Ownership conflict or OUNID mismatch. The output connection was already owned by another originator |
| 01 <sub>hex</sub> | 0205 <sub>hex</sub> | Parameter Error in Unconnected Send service or<br>Parameter Error in SafetyOpen or SafetyClose      |
| 01 <sub>hex</sub> | 801 <sub>hex</sub>  | Incompatible Multipoint RPI. An existing connection has been established at a different RPI         |
| 01 <sub>hex</sub> | 802 <sub>hex</sub>  | Invalid Safety Connection size                                                                      |
| 01 <sub>hex</sub> | 803 <sub>hex</sub>  | Invalid Safety Connection format                                                                    |
| 01 <sub>hex</sub> | 804 <sub>hex</sub>  | Invalid Time Correction Connection Parameters                                                       |
| 01 <sub>hex</sub> | 805 <sub>hex</sub>  | Invalid Ping Interval EPI Multiplier                                                                |
| 01 <sub>hex</sub> | 806 <sub>hex</sub>  | Time Coordination Msg Min Multiplier                                                                |
| 01 <sub>hex</sub> | 807 <sub>hex</sub>  | Network Time Expectation Multiplier                                                                 |
| 01 <sub>hex</sub> | 808 <sub>hex</sub>  | Timeout Multiplier                                                                                  |
| 01 <sub>hex</sub> | 809 <sub>hex</sub>  | Invalid Max Consumer Number                                                                         |

| General status    | Extended status    | Explanation                                                                                            |
|-------------------|--------------------|--------------------------------------------------------------------------------------------------------|
| 01 <sub>hex</sub> | 80A <sub>hex</sub> | Invalid CPCRC                                                                                          |
| 01 <sub>hex</sub> | 80B <sub>hex</sub> | Time Correction Connection Id invalid                                                                  |
| 01 <sub>hex</sub> | 80C <sub>hex</sub> | SCID Mismatch. The SCID was non-zero and did not match the value in the target                         |
| 01 <sub>hex</sub> | 80D <sub>hex</sub> | TUNID not set. Device is out-of-box and TUNID has not been set, so connections are not allowed         |
| 01 <sub>hex</sub> | 80E <sub>hex</sub> | TUNID Mismatch. The TUNID provided does not match. The message was likely routed to this node in error |
| 01 <sub>hex</sub> | 80F <sub>hex</sub> | Configuration operation not allowed                                                                    |

1203

1204 Event/Error Matrix Table 17 provides guidance for which error codes to use for possible errors  
 1205 detected in processing a SafetyOpen. This is not intended to be an exhaustive list.

1206

**Table 17 – SafetyOpen error event guidance table**

| Event                                                                                                               | Error type                                                             | General status    | Extended status     |
|---------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------|-------------------|---------------------|
| The target device received a SafetyOpen request in states of Safety Supervisor object other than Idle and Executing | Configuration operation not allowed                                    | 01 <sub>hex</sub> | 080F <sub>hex</sub> |
|                                                                                                                     | Device not configured                                                  | 01 <sub>hex</sub> | 110 <sub>hex</sub>  |
| Safety Connection Type (name) Invalid                                                                               | Safety parameter error – Invalid Connection Type                       | 01 <sub>hex</sub> | 315 <sub>hex</sub>  |
| Safety Connection Size Invalid                                                                                      | Safety parameter error – Invalid Safety Connection Size                | 01 <sub>hex</sub> | 0802 <sub>hex</sub> |
| Safety Connection Format Invalid                                                                                    | Safety parameter error – Invalid Safety Connection Format              | 01 <sub>hex</sub> | 0803 <sub>hex</sub> |
| Time Correction Connection Parameters Invalid                                                                       | Safety parameter error – Invalid Time Correction Connection Parameters | 01 <sub>hex</sub> | 0804 <sub>hex</sub> |
| Ping Interval EPI Multiplier was out of the range                                                                   | Safety parameter error – Invalid Ping Interval EPI Multiplier          | 01 <sub>hex</sub> | 0805 <sub>hex</sub> |
| Time Coordination Message Min Multiplier was out of the range                                                       | Safety parameter error – Time Coordination Msg Min Multiplier          | 01 <sub>hex</sub> | 0806 <sub>hex</sub> |
| Time Expectation Multiplier was out of the range                                                                    | Safety parameter error – Time Expectation Multiplier                   | 01 <sub>hex</sub> | 0807 <sub>hex</sub> |
| Timeout Multiplier was out of the range                                                                             | Safety parameter error – Timeout Multiplier                            | 01 <sub>hex</sub> | 0808 <sub>hex</sub> |
| Max Consumer Number not within the limits in Multipoint Producer                                                    | Safety parameter error – Invalid Max Consumer Number                   | 01 <sub>hex</sub> | 0809 <sub>hex</sub> |
| CPCRC value in SafetyOpen and calculated CPCRC value                                                                | Safety parameter error – Invalid CPCRC                                 | 01 <sub>hex</sub> | 080A <sub>hex</sub> |
| Time Correction Connection Id Invalid                                                                               | Safety parameter error – Time Correction Connection Id invalid         | 01 <sub>hex</sub> | 080B <sub>hex</sub> |

| Event                                                                            | Error type                                                                  | General status    | Extended status     |
|----------------------------------------------------------------------------------|-----------------------------------------------------------------------------|-------------------|---------------------|
| RPI requested is incompatible with previously established multipoint connections | Incompatible multipoint RPI                                                 | 01 <sub>hex</sub> | 801 <sub>hex</sub>  |
| O-to-T RPI, T-to-O RPI, or Time Correction RPI is not supported                  | RPI not supported                                                           | 01 <sub>hex</sub> | 0111 <sub>hex</sub> |
| All Safety Validator Instances are being used                                    | Connection Manager or connection object cannot support any more connections | 01 <sub>hex</sub> | 0113 <sub>hex</sub> |

1207

1208 **6.3.13 ForwardClose for safety**

1209 There are no additional behaviors defined for the ForwardClose service when used to close a  
 1210 Safety connection. In the following Safety Requirements, the term “SafetyClose” refers to both  
 1211 the ForwardClose of the Connection Manager object and the SafetyClose of the Connection  
 1212 object.

1213 The SafetyClose Service shall be used to close connections with a Safety Targets (and in the  
 1214 case of a ForwardClose all other nodes in the connection path).

1215 The SafetyClose request shall remove a connection from all the nodes participating in the  
 1216 original connection.

1217 The SafetyClose request shall cause all resources in all nodes participating in the connection  
 1218 to be deallocated, including connection IDs, bandwidth, and internal memory buffers.

1219 Targets receiving the SafetyClose service request shall close the connection who's Originator  
 1220 Vendor ID, Connection Serial Number, and Originator Serial Number parameters match.  
 1221 Additional information provided by this service (ie, Connection Path) shall be ignored by the  
 1222 target.

1223 A SafetyClose Success reply shall be returned after the connection has been deleted at the  
 1224 target.

1225 When a SafetyClose success reply is received, the originator and each intermediate node  
 1226 along the path, closes the connection and releases resources associated with that  
 1227 connection. But the originator shall also close the connection if no response is received within  
 1228 a vendor selected wait period.

1229 **6.4 Identity object**1230 **6.4.1 General**

1231 Class Code: 01hex

1232 This subclause describes changes to the Identity object to support safety.

1233 All CPF 2 safety devices shall replace the Identity object state behavior with the behavior  
 1234 defined in the Safety Supervisor object.

1235 **6.4.2 Changes to common services**

1236 Table 18 defines the services of the Identity object that require updates.