IEC 61784-3-3

Edition 4.0 2021-05

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

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

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

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

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

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

IEC 61784-3-3

Edition 4.0 2021-05

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

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

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

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

ICS 25.040.40; 35.100.05

ISBN 978-2-8322-9749-0

CONTENTS

FOREWORD 9
0 Introduction 11
0.1 General 11
0.2 Patent declaration 12
1 Scope 14
2 Normative references 14
3 Terms, definitions, symbols, abbreviated terms and conventions 16
3.1 Terms and definitions 16
3.1.1 Common terms and definitions 16
3.1.2 CPF 3: Additional terms and definitions 22
3.2 Symbols and abbreviated terms 27
3.2.1 Common symbols and abbreviated terms 27
3.2.2 CPF 3: Additional symbols and abbreviated terms 28
3.3 Conventions 29
4 Overview of FSCP 3/1 (PROFIsafe™) 29
5 General 32
5.1 External documents providing specifications for the profile 32
5.2 Safety functional requirements 32
5.3 Safety measures 32
5.4 Safety communication layer structure 33
5.4.1 Principle of FSCP 3/1 safety communications 33
5.4.2 CPF 3 communication structures 35
5.5 Relationships with FAL (and DLL, PhL) 37
5.5.1 Device model 37
5.5.2 Application and communication relationships 38
5.5.3 Data types 38
6 Safety communication layer services 39
6.1 F-Host driver services 39
6.2 F-Device driver services 43
6.3 Diagnosis 45
6.3.1 Safety alarm generation 45
6.3.2 F-(Sub)Module safety layer diagnosis 45
7 Safety communication layer protocol 46
7.1 Safety PDU format 46
7.1.1 Safety PDU structure 46
7.1.2 Safety IO data 47
7.1.3 Status and Control Byte 47
7.1.4 (Virtual) MonitoringNumber 49
7.1.5 (Virtual) MNR mechanism (F_CRC_Seed=0) 50
7.1.6 (Virtual) MNR mechanism (F_CRC_Seed=1) 50
7.1.7 CRC2 Signature (F_CRC_Seed=0) 52
7.1.8 CRC2 Signature (F_CRC_Seed=1) 53
7.1.9 Non-safety IO data 54
7.2 FSCP 3/1 behavior 54
7.2.1 General 54

7.2.2 F-Host driver state diagram 55
7.2.3 F-Device driver state diagram 58
7.2.4 F-Device driver restart 62
7.2.5 Sequence diagrams 62
7.2.6 Timing diagram for a MonitoringNumber reset 69
7.2.7 Monitoring of safety times 69
7.3 Reaction in the event of a malfunction 72
7.3.1 Corruption of safety data 72
7.3.2 Unintended repetition 72
7.3.3 Incorrect sequence 73
7.3.4 Loss 73
7.3.5 Unacceptable delay 73
7.3.6 Insertion 73
7.3.7 Masquerade 73
7.3.8 Addressing 73
7.3.9 Out-of-sequence 74
7.3.10 Loop-back 74
7.3.11 Network boundaries and router 74
7.4 F-Startup and parameter change at runtime 75
7.4.1 Standard startup procedure 75
8 Safety communication layer management 75
8.1 F-Parameter 75
8.1.1 Summary 75
8.1.2 F_Source/Destination_Address (Codename) 76
8.1.3 F_WD_Time (F-Watchdog time) 77
8.1.4 F_WD_Time_2 (secondary F-Watchdog time) 77
8.1.5 F_Prm_Flag1 (Parameters for the safety layer management) 77
8.1.6 F_Prm_Flag2 (Parameters for the safety layer management) 80
8.1.7 F_iPar_CRC (value of iPar_CRC across iParameters) 81
8.1.8 F_Par_CRC calculation (across F-Parameters) 81
8.1.9 Structure of the F-Parameter record data object 82
8.2 iParameter and iPar_CRC 82
8.3 Safety parameterization 83
8.3.1 Objectives 83
8.3.2 GSDL and GSDML safety extensions 84
8.3.3 Securing safety parameters and GSD data 86
8.4 Safety configuration 90
8.4.1 Order of IO data types 90
8.4.2 Securing the safety IO data description 90
8.4.3 DataItem data type section examples 91
8.5 Data type information usage 95
8.5.1 F-Host Channel driver 95
8.5.2 Rules for standard F-Host Channel drivers 96
8.5.3 Recommendations for the use of F-Host Channel drivers 97
8.6 Safety parameter assignment mechanisms 98
8.6.1 F-Parameter assignment 98
8.6.2 General iParameter assignment 98
8.6.3 System integration requirements for iParameterization tools 98
8.6.4 iPar-Server 100

9 System requirements 111
9.1 Indicators and switches 111
9.2 Installation guidelines 111
9.3 Safety function response time 111
9.3.1 Model 111
9.3.2 Calculation and optimization 113
9.3.3 Adjustment of watchdog times for FSCP 3/1 115
9.3.4 Engineering tool support 116
9.3.5 Retries (repetition of messages) 116
9.4 Duration of demands 117
9.5 Constraints for the calculation of system characteristics 117
9.5.1 Probabilistic considerations 117
9.5.2 Safety related assumptions 119
9.5.3 Non safety related constraints (availability) 120
9.6 Maintenance 120
9.6.1 F-(Sub)Module commissioning / replacement 120
9.6.2 Identification and maintenance functions 120
9.7 Safety manual 121
9.8 Wireless transmission channels 122
9.8.1 Black channel approach 122
9.8.2 Availability 122
9.8.3 Security measures 122
9.8.4 Stationary and mobile applications 122
9.9 Relationship between functional safety and security 123
9.10 Conformance classes 123
10 Assessment 125
10.1 Safety policy 125
10.2 Obligations 125
Annex A (informative) Additional information for functional safety communication profiles of CPF 3 126
A.1 Hash function calculation 126
A.2 Example values for MonitoringNumbers (MNR) 130
Annex B (informative) Information for assessment of the functional safety communication profiles of CPF 3 131
Annex C (normative) Optional features 132
C.1 Reaction on Device_Fault in F-Host 132
C.1.1 Situation 132
C.1.2 Documentation for the user 132
C.1.3 Optional extensions of F-Host driver Transition Table 132
C.1.4 Recommendation for the case without Extensions of F-Host driver Transitions 135
C.2 Optional extensions of F-Host driver to "Disable F-(Sub)Module" 135
C.3 Combination of "Disable F-(Sub)Module" and "reaction on Device_Fault" 139
C.4 FSCP 3/1 and PROFIenergy 141
C.4.1 Use of FSCP 3/1-Devices with PROFIenergy 141
C.4.2 Sequence in case of PROFIenergy power off on 141
C.5 Requirement multiple F-Hosts communicate with single F-(Sub)Module 141
C.6 FSCP 3/1 PiR 142
Bibliography 143

Figure 1 – Relationships of IEC 61784-3 with other standards (machinery) 11
Figure 2 – Relationships of IEC 61784-3 with other standards (process) 12
Figure 3 – Basic communication preconditions for FSCP 3/1 30
Figure 4 – Structure of an FSCP 3/1 safety PDU 30
Figure 5 – Safety communication on CPF 3 31
Figure 6 – Standard CPF 3 transmission system 34
Figure 7 – Safety layer architecture 35
Figure 8 – Basic communication layers 35
Figure 9 – Crossing network borders with routers 36
Figure 10 – Complete safety transmission paths 37
Figure 11 – IO Device model 38
Figure 12 – FSCP 3/1 communication structure 39
Figure 13 – F application interface of F-Host driver instances 40
Figure 14 – Motivation for "Channel-related Passivation" 41
Figure 15 – F-Device driver interfaces 43
Figure 16 – Safety PDU for CPF 3 47
Figure 17 – Status Byte 47
Figure 18 – Control Byte 48
Figure 19 – The Toggle Bit function 49
Figure 20 – MonitoringNumber integration 50
Figure 21 – F-Host driver CRC2 signature generation (F_CRC_Seed=0) 52
Figure 22 – Details of the CRC2 signature calculation (F_CRC_Seed=0) 53
Figure 23 – CRC2 signature calculation (F_CRC_Seed=1) 53
Figure 24 – Details of the CRC2 signature calculation (F_CRC_Seed=1) 54
Figure 25 – Safety layer communication relationship 54
Figure 26 – F-Host driver state diagram 55
Figure 27 – F-Device driver state diagram 59
Figure 28 – Interaction F-Host driver / F-Device driver during start-up 63
Figure 29 – Interaction F-Host driver / F-Device driver during F-Host power off > on 64
Figure 30 – Interaction F-Host driver / F-Device driver with delayed power on 65
Figure 31 – Interaction F-Host driver / F-Device driver during power off → on 66
Figure 32 – Interaction while F-Host driver recognizes CRC error 67
Figure 33 – Interaction while F-Device driver recognizes CRC error 68
Figure 34 – Impact of the MNR reset signal 69
Figure 35 – Monitoring the message transit time F-Host ↔ F-(Sub)Module 70
Figure 36 – Extended watchdog time on request 72
Figure 37 – Effect of F_WD_Time_2 77
Figure 38 – F_Prm_Flag1 78
Figure 39 – F_Check_iPar 78
Figure 40 – F_SIL 78
Figure 41 – F_CRC_Length 79
Figure 42 – F_CRC_Seed 79

Figure 43 – F_Prm_Flag2 80
Figure 44 – F_Passivation 80
Figure 45 – F_Block_ID 80
Figure 46 – F_Par_Version 81
Figure 47 – F-Parameter 82
Figure 48 – iParameter block 83
Figure 49 – F-Parameter extension within the GSDML specification 85
Figure 50 – F_Par_CRC signature including iPar_CRC 86
Figure 51 – F-Host Channel driver as "glue" between F-(Sub)Module and application program 96
Figure 52 – Layout example of an F-Host Channel driver 97
Figure 53 – F-Parameter assignment for F-(Sub)Modules 98
Figure 54 – System integration of CPD-Tools 99
Figure 55 – iPar-Server mechanism (commissioning) 100
Figure 56 – iPar-Server mechanism (for example F-(Sub)Module replacement) 102
Figure 57 – iPar-Server request coding ("status model") 103
Figure 58 – Coding of SR_Type 104
Figure 59 – iPar-Server request coding ("alarm model") 105
Figure 60 – iPar-Server state diagram 108
Figure 61 – Example safety function with a critical response time path 112
Figure 62 – Simplified typical response time model 112
Figure 63 – Frequency distributions of typical response times of the model 113
Figure 64 – Context of delay times and watchdog times 114
Figure 65 – Timing sections forming the FSCP 3/1 F_WD_Time 115
Figure 66 – Frequency distribution of response times with message retries 116
Figure 67 – Residual error probabilities for the 24-bit CRC polynomial 117
Figure 68 – Residual error probabilities for the 32-bit CRC polynomial 118
Figure 69 – Monitoring of corrupted messages 119
Figure A.1 – Typical "C" procedure of a cyclic redundancy check 126
Figure C.1 – F-Host driver application interface with feature Reaction on Device_Fault 132
Figure C.2 – F-Host driver application interface with feature Disable F-(Sub)Module 136
Figure C.3 – Timing diagram to use Disable F-(Sub)Module 136

Table 1 – Deployed measures to master errors 33
Table 2 – Data types for FSCP 3/1 38
Table 3 – F_MessageTrailer for FSCP 3/1 38
Table 4 – Safety layer diagnosis messages 45
Table 5 – Buffer entry on CRC2 error 46
Table 6 – MonitoringNumber of an F-Host driver SPDU 50
Table 7 – MonitoringNumber of an F-Device driver SPDU 50
Table 8 – MonitoringNumber of an F-Host driver SPDU 51
Table 9 – MonitoringNumber of an F-Device driver SPDU 51
Table 10 – Definition of terms used in F-Host driver state diagram 55

Table 11 – F-Host driver states and transitions 56
Table 12 – Definition of terms used in Figure 27 59
Table 13 – F-Device driver states and transitions 60
Table 14 – SIL monitor times 71
Table 15 – Safety network boundaries 75
Table 16 – Codename octet order 76
Table 17 – Allowed combinations of F_CRC_Seed and F_Passivation 79
Table 18 – GSDL keywords for F-Parameters and F-IO structures 84
Table 19 – Algorithm to build CRC0 87
Table 20 – GSD example in GSDL notation 88
Table 21 – GSD example in GSDML notation 89
Table 22 – Serialized octet stream for the examples 89
Table 23 – Order of IO data types 90
Table 24 – IO data structure items 91
Table 25 – DataItem section for F_IN_OUT_1 92
Table 26 – DATA_STRUCTURE_CRC for F_IN_OUT_1 92
Table 27 – DataItem section for F_IN_OUT_2 93
Table 28 – DATA_STRUCTURE_CRC for F_IN_OUT_2 93
Table 29 – DataItem section for F_IN_OUT_5 94
Table 30 – DATA_STRUCTURE_CRC for F_IN_OUT_5 94
Table 31 – DataItem section for F_IN_OUT_6 95
Table 32 – DATA_STRUCTURE_CRC for F_IN_OUT_6 95
Table 33 – Sample F-Host Channel drivers 96
Table 34 – Requirements for iParameterization 99
Table 35 – Specifier for the iPar-Server Request 104
Table 36 – Structure of the Read_RES_PDU ("read record") 106
Table 37 – Structure of the Write_REQ_PDU ("write record") 106
Table 38 – Structure of the Pull_RES_PDU ("Pull") 106
Table 39 – Structure of the Push_REQ_PDU ("Push") 107
Table 40 – iPar-Server states and transitions 109
Table 41 – iPar-Server management measures 110
Table 42 – Definition of terms in Figure 69 119
Table 43 – Information to be included in the safety manual 121
Table 44 – F-Host conformance class requirements 123
Table 45 – Main characteristics of protocol versions 124
Table 46 – F-Host driver / F-Device driver conformance matrix 124
Table A.1 – The table "Crctab24" for 24 bit CRC signature calculations 127
Table A.2 – The table "Crctab32" for 32 bit CRC signature calculations 128
Table A.3 – The table "Crctab16" for 16 bit CRC signature calculations 129
Table A.4 – Values of CN_incrNR_64 and MNR for F-Host PDU 130
Table C.1 – Definition of additional terms used in driver transitions 133
Table C.2 – F-Host driver transitions – added with reaction on Device_Fault 133
Table C.3 – Prevent unintentional restart by application measures 135

Table C.4 – F-Host driver transitions – with feature Disable F-(Sub)Module 137
Table C.5 – F-Host driver transitions – added with "reaction on Device_Fault" and "Disable F-(Sub)Module" 139

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES –

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

FOREWORD

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

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

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

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

- editorial changes regarding timeliness, transformation of comments in the chart into instructions;
- use abbreviations of PROFINET;
- information added about checks and safety manual for PROFIsafe Address Type 1 and 2;
- information added about PFDavg, support of automatic test, add diagnosis messages;

- explanation and specification of optional statemachines for reaction on device fault;
- new optional variable "OAD_Nec_C" for optional feature "Reaction of Device_Fault in F_Host";
- specification of the optional F-Host feature for "Disable F-(Sub)Module";
- specify requirements for FSCP 3/1 and PROFIenergy;
- specify requirement for multiple F-Hosts communicating with a single F-(Sub)Module; Update of the Safety Manual;
- diverse error corrections, fixes of typos, and reference updates;
- updated bibliography.

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

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

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

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

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

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

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

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

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

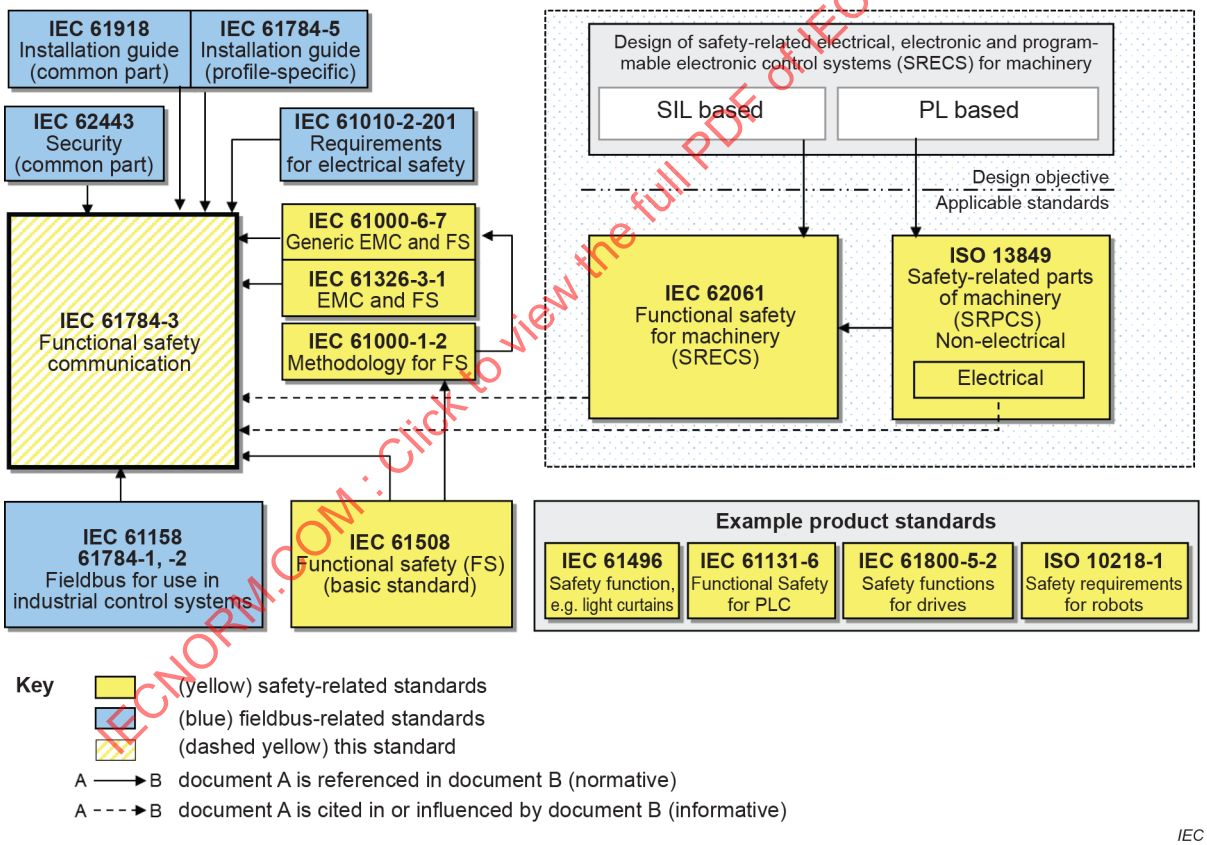
0 Introduction

0.1 General

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

IEC 61784-3 (all parts) explains the relevant principles for functional safety communications with reference to IEC 61508 (all parts) and specifies several safety communication layers (profiles and corresponding protocols) based on the communication profiles and protocol layers of IEC 61784-1, IEC 61784-2 and IEC 61158 (all parts). It does not cover electrical safety and intrinsic safety aspects. It also does not cover security aspects nor does it provide any requirements for security.

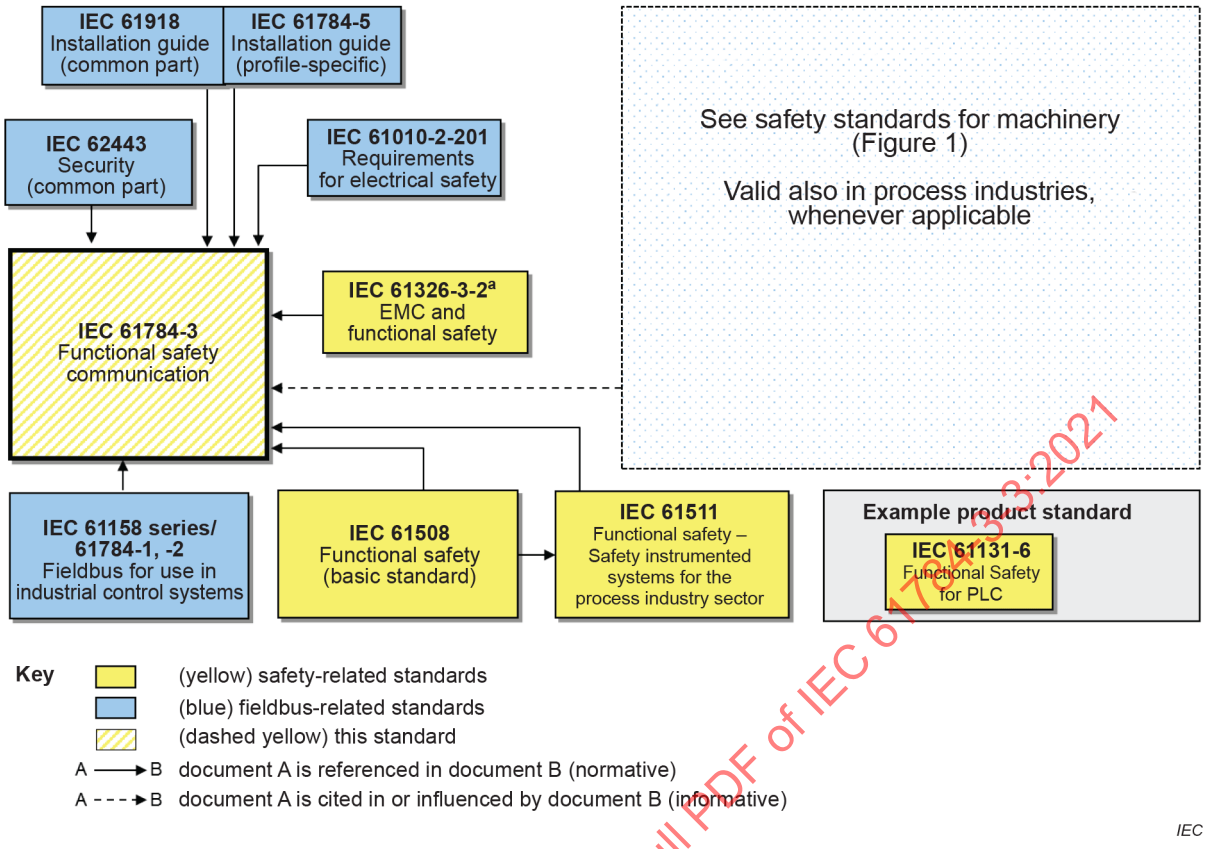
Figure 1 shows the relationships between IEC 61784-3 (all parts) and relevant safety and fieldbus standards in a machinery environment.



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

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

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



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

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

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

Safety communication layers specified in IEC 61784-3 (all parts) do this in such a way that a fieldbus can be used for applications requiring functional safety up to the Safety Integrity Level (SIL) specified by its corresponding functional safety communication profile.

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

IEC 61784-3 (all parts) describes:

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

0.2 Patent declaration

The International Electrotechnical Commission (IEC) draws attention to the fact that it is claimed that compliance with this document may involve the use of patents concerning the functional safety communication profiles for family 3. IEC takes no position concerning the evidence, validity, and scope of these patent rights.

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

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

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES –

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

1 Scope

This part of IEC 61784-3 (all parts) specifies a safety communication layer (services and protocol) based on CPF 3 of IEC 61784-1, IEC 61784-2 (CP 3/1, CP 3/2, CP 3/4, CP 3/5 and CP 3/6) and IEC 61158 Types 3 and 10. It identifies the principles for functional safety communications defined in IEC 61784-3 that are relevant for this safety communication layer. This safety communication layer is intended for implementation in safety devices only.

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

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

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

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

2 Normative references

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

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

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

IEC 61010-2-201:2017, *Safety requirements for electrical equipment for measurement, control and laboratory use – Part 2-201: Particular requirements for control equipment*

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

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

IEC 61158-5-3, *Industrial communication networks – Fieldbus specifications – Part 5-3: Application layer service definition –Type 3 elements*

IEC 61158-5-10, *Industrial communication networks – Fieldbus specifications – Part 5-10: Application layer service definition – Type 10 elements*

IEC 61158-6-3, *Industrial communication networks – Fieldbus specifications – Part 6-3: Application layer protocol specification – Type 3 elements*

IEC 61158-6-10, *Industrial communication networks – Fieldbus specifications – Part 6-10: Application layer protocol specification – Type 10 elements*

IEC 61326-3-1, *Electrical equipment for measurement, control and laboratory use – EMC requirements – Part 3-1: Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety) – General industrial applications*

IEC 61326-3-2, *Electrical equipment for measurement, control and laboratory use – EMC requirements – Part 3-2: Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety) – Industrial applications with specified electromagnetic environment*

IEC 61508 (all parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

IEC 61508-2, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*

IEC 61511 (all parts), *Functional safety – Safety instrumented systems for the process industry sector*

IEC 61784-1, *Industrial communication networks – Profiles – Part 1: Fieldbus profiles*

IEC 61784-2, *Industrial communication networks – Profiles – Part 2: Additional fieldbus profiles for real-time networks based on ISO/IEC/IEEE 8802-3*

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

IEC 61784-5-3, *Industrial communication networks – Profiles – Part 5-3: Installation of fieldbuses – Installation profiles for CPF 3*

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

IEC 62061, *Safety of machinery – Functional safety of safety-related control systems*

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

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

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

ISO 13849-2:2012, *Safety of machinery – Safety-related parts of control systems – Part 2: Validation*

3 Terms, definitions, symbols, abbreviated terms and conventions

3.1 Terms and definitions

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

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

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

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

3.1.1 Common terms and definitions

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

3.1.1.1
active network element
network element containing electrically and/or optically active components that allows extension of the network

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

[SOURCE: IEC 61918:2018, 3.1.2]

3.1.1.2
availability
probability for an automated system that for a given period of time there are no unsatisfactory system conditions such as loss of production

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

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

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

3.1.1.5
communication channel
logical connection between two end-points within a *communication system*

3.1.1.6
communication system
arrangement of hardware, software and propagation media to allow the transfer of *messages* (ISO/IEC 7498-1 application layer) from one application to another

3.1.1.7
connection
logical binding between two application objects within the same or different devices

3.1.1.8
Cyclic Redundancy Check
CRC
<value> redundant data derived from, and stored or transmitted together with, a block of data in order to detect data corruption

<method> procedure used to calculate the redundant data

Note 1 to entry: Terms "CRC code" and "CRC signature", and labels such as CRC1, CRC2, may also be used in this document to refer to the redundant data.

Note 2 to entry: See also [27],[28][2].

3.1.1.9
defined communication system
defined channel
fixed number or fixed maximum number of participants linked by a *fieldbus* based *communication system* with well-known and fixed properties, such as installation conditions, electromagnetic immunity, industrial *(active) network elements*, and where the *risk* of unauthorized access is reduced to a tolerated level according to the lifecycle model of IEC 62443 (all parts), using for example zones and conduits

3.1.1.10
DLPDU
DEPRECATED: frame
Data Link Protocol Data Unit

3.1.1.11
error
discrepancy between a computed, observed or measured value or condition and the true, specified or theoretically correct value or condition

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

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

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

3.1.1.12
explicit code
code for safety measure that is actually transmitted within the SPDU and is known to the sender and receiver

3.1.1.13
explicit data
data that is transmitted

Note 1 to entry: Explicit data is defined in contrast to implicit data.

2 Figures in square brackets refer to the bibliography.

3.1.1.14
failure
termination of the ability of a functional unit to perform a required function or operation of a functional unit in any way other than as required

Note 1 to entry: Failure may be due to an *error* (for example, problem with hardware/software design or message disruption).

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

3.1.1.15
fault
abnormal condition that may cause a reduction in, or loss of, the capability of a functional unit to perform a required function

Note 1 to entry: IEC 60050-191:1990, 191-05-01 defines "fault" as a state characterized by the inability to perform a required function, excluding the inability during preventive maintenance or other planned actions, or due to lack of external resources.

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

3.1.1.16
fieldbus
communication system based on serial data transfer and used in industrial automation or process control applications

3.1.1.17
fieldbus system
system using a *fieldbus* with connected devices

3.1.1.18
Frame Check Sequence
FCS
redundant data derived from a block of data within a DLPDU (frame), using a hash function, and stored or transmitted together with the block of data, in order to detect data corruption

Note 1 to entry: An FCS can be derived using for example a CRC or other hash function.

Note 2 to entry: See also [27], [28].

3.1.1.19
functional safety communication profile
FSCP
technology specification for the implementation of an SCL

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

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

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

3.1.1.21
hazard
potential source of harm

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

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

3.1.1.22
implicit code
code for safety measure that is not transmitted within the SPDU but is known to the sender and receiver

3.1.1.23
implicit data
additional data that is not transmitted but is known to the sender and receiver, and used in the encoding and decoding of the message/SPDU

Note 1 to entry: Implicit data is defined in contrast to explicit data.

[SOURCE: IEC 62280:2014, 3.1.25, modified – addition of ", and used in the encoding and decoding of the message/SPDU"]

3.1.1.24
master
communication entity able to initiate and schedule communication activities by other stations which may be masters or slaves

3.1.1.25
message
<information theory and communication theory> ordered sequence of characters (usually octets) intended to convey information

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

3.1.1.26
proof test
periodic test performed to detect dangerous hidden failures in a *safety-related system* so that, if necessary, a repair can restore the system to an "as new" condition or as close as practical to this condition

Note 1 to entry: A proof test is intended to confirm that the safety-related system is in a condition that assures the specified safety integrity.

[SOURCE: IEC 61508-4:2010, 3.8.5, modified by replacement of the four notes with another one]

3.1.1.27
performance level
PL
discrete level used to specify the ability of safety-related parts of control systems to perform a safety function under foreseeable conditions

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

3.1.1.28
protective extra-low-voltage
PELV
protective earth referenced electrical circuit in which the voltage cannot exceed the following:

NORMAL CONDITION and SINGLE FAULT CONDITION: The AC voltage levels are 30 V RMS 42,4 V peak and the DC voltage level is 60 V. For equipment intended for use in WET LOCATIONS, the AC voltage levels are 16 V RMS, 22,6 V peak and the DC voltage level is 35 V.

[SOURCE: IEC 61010-2-201:2017, 3.111, modified – deletion of "circuit" from term, and deletion of source]

3.1.1.29
redundancy
existence of more than one means for performing a required function or for representing information

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

3.1.1.30
residual error probability
RP
probability of an error undetected by the SCL safety measures

3.1.1.31
residual error rate
statistical rate at which the SCL safety measures fail to detect errors

3.1.1.32
risk
combination of the probability of occurrence of harm and the severity of that harm

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

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

3.1.1.33
safety communication channel
communication channel starting at the top of the SCL of the source and ending at the top of the SCL of the sink

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

3.1.1.34
safety communication layer
SCL
communication layer above the FAL that includes all necessary additional measures to ensure safe transmission of data in accordance with the requirements of IEC 61508

3.1.1.35
safety connection
connection that utilizes the safety protocol for communications transactions

3.1.1.36
safety data
data transmitted across a safety network using a safety protocol

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

3.1.1.37
safety device
device designed in accordance with IEC 61508 and which implements the functional safety communication profile

3.1.1.38
safety extra-low-voltage
SELV
non-protective earth referenced electrical circuit in which the voltage cannot exceed the following:

NORMAL CONDITION and SINGLE FAULT CONDITION: The AC voltage levels are 30 V RMS, 42,4 V peak and the DC voltage level is 60 V. For equipment intended for use in WET LOCATIONS, the AC voltage levels are 16 V RMS, 22,6 V peak and the DC voltage level is 35 V.

[SOURCE: IEC 61010-2-201:2017, 3.112, modified – deletion of "circuit" from term, and deletion of source]

3.1.1.39
safety function
function to be implemented by an E/E/PE safety-related system or other risk reduction measures, that is intended to achieve or maintain a safe state for the EUC, in respect of a specific hazardous event

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

3.1.1.40
safety function response time
SFRT
worst case elapsed time following an actuation of a safety sensor connected to a fieldbus, until the corresponding safe state of its safety actuator(s) is achieved in the presence of errors or failures in the safety function

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

3.1.1.41
safety integrity level
SIL
discrete level (one out of a possible four), corresponding to a range of safety integrity values, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest

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

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

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

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

3.1.1.42
safety measure
measure to control possible communication *errors* that is designed and implemented in compliance with the requirements of IEC 61508

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

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

3.1.1.43
safety PDU
SPDU
PDU transferred through the safety communication channel

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

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

Note 3 to entry: In terms of CP 3/4 to 3/6 it is the APDU Application Protocol Data Unit.

3.1.1.44
safety-related application
programs designed in accordance with IEC 61508 to meet the SIL requirements of the application

3.1.1.45
safety-related system
system performing *safety functions* according to IEC 61508

3.1.1.46
slave
communication entity able to receive messages and send them in response to another communication entity which may be a master or a slave, but not to initiate communication activities

3.1.1.47
spurious trip
trip caused by the safety system without a process demand

3.1.1.48
uniform distribution
probability distribution where all values from a finite set are equally likely to occur

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

3.1.2 CPF 3: Additional terms and definitions

3.1.2.1
Address Type
Address Type 1 if F_DestAdd is checked only
Address Type 2 if F_SourceAdd is checked together with the F_DestAdd

3.1.2.2
bit
Binary Digi**t**
encoded binary information without a technical unit

3.1.2.3
Codename
Identification of the safety communication relationship between safety communication peers.

Note 1 to entry: The Codename is used for the unique identification of the safety communication relationship.

Note 2 to entry: The Codename consists of F_Source_Address and F_Dest_Address.

Note 3 to entry: Instance of *connection authentication* as described in IEC 61784-3.

3.1.2.4
configuration
definition of the standard communication connections and communication parameters for bus entities of a particular application

Note 1 to entry: The configuration for safety communication comprises the definition of the safety connections and F-Parameters for safety-related bus entities of a particular safety-related application.

3.1.2.5
CPD-Tool
dedicated program in service computers connected to the fieldbus for the purpose of Configuration, Parameterization and Diagnosis of particular field devices

3.1.2.6
cycle
interval at which a list of instructions or an activity is repetitively and continuously executed

3.1.2.7
device access point
DAP
item used to address a modular IO device as an entity

Note 1 to entry: Usually this is called a head station.

3.1.2.8
device acknowledgment time
DAT
elapsed time in an IO-Device starting with the reception of a safety PDU with a new *MonitoringNumber* in the device access point until an appropriate response safety PDU has been generated and returned to the device access point

3.1.2.9
driver
software module used for abstracting the hardware with respect to the remaining application software

3.1.2.10
fail-safe
F
ability of a system that, by adequate technical or organizational measures, prevents from hazards either deterministically or by reducing the risk to a tolerable measure

Note 1 to entry: Equivalent to functional safety.

3.1.2.11
fail-safe values
FV
values which are issued instead of process values when the safety function is set to a fail-safe state

Note 1 to entry: In this document, the fail-safe values (FV) shall always be set to "0".

3.1.2.12
fail-safe state
operational mode of a safety function or final element (actuator) that by adequate technical measures prevents from hazards either deterministically or by reducing the risk to a tolerable measure

Note 1 to entry: Depending on a particular safety function, de-energizing is not the only possibility for a fail-safe state.

3.1.2.13
F-Host Channel driver
driver within F-Hosts according to the FSCP 3/1 specifications to represent F IO data in the F-Host application program

3.1.2.14
F-Device
The term F-Device used in previous versions of this profile is substituted by "F-Device driver"

3.1.2.15
F-Device driver
software administering safety PDUs within F-(Sub)Module according to the FSCP 3/1 specifications triggered by the F-Host driver for data exchange

3.1.2.16
F driver
software administering safety PDUs as F-Host driver or F-Device driver according to the FSCP 3/1 specifications

3.1.2.17
F-Host
data processing unit that is able to perform the FSCP 3/1 protocol and to service the black channel

Note 1 to entry: This is usually implemented in a PLC or an IPC with an adequate operating system.

3.1.2.18
F-Host driver
software administering safety PDUs within F-Hosts according to the FSCP 3/1 specifications

3.1.2.19
F-(Sub)Module
communication peer within a modular IO-Slave or IO-Device that is able to perform the CP 3/1 or CP 3/4 to CP 3/6 protocol

Note 1 to entry: The F-(Sub)Module is hosting the F-Device driver.

Note 2 to entry: This is usually a safety-related input or output module.

3.1.2.20
F-Slave
CP 3/1 or CP 3/2 communication peer that is able to perform the FSCP 3/1 protocol, usually triggered by the F-Host for data exchange

3.1.2.21
fault reaction
indication of a communication malfunction by setting the fault bits in the Status Byte and a corresponding automatic safe reaction within the components

Note 1 to entry:

Within F-Output: Shutting down the outputs, and/or automatic safe reaction of the actuator unit.

Within F-CPU: Corresponding application program reaction possible. F-IO data to be set to fail-safe values.

Within F-Input: On communication faults detected from F-Input:
Fault bits set in the Status Byte.
On communication faults detected from F-Host:
F-Input data to be set to fail-safe values.

3.1.2.22
function block
FB
self-contained program part possessing a specific functionality

3.1.2.23
host acknowledgment time
HAT
elapsed time in an F-Host starting with the reception of a safety PDU with a certain *MonitoringNumber* until an appropriate safety PDU with a changed *MonitoringNumber* has been generated and returned to the master/IO-Controller

3.1.2.24
IO-Controller
active communication entity able to initiate and schedule CP 3/4 to CP 3/6 communication activities by other entities which may be IO-Controllers or IO-Devices

Note 1 to entry: Within CP 3/1 this task is corresponding to a master class 1.

Note 2 to entry: The IO-Controller interface is called "FAL services of the IO controller" according to IEC 61158-5-10.

3.1.2.25
IO-Device
communication entity able to receive messages and send them in response to another CP 3/4 to CP 3/6 communication entity which may be an IO-Controller or other IO-Devices

Note 1 to entry: Within CP 3/1 this task is corresponding to a slave.

Note 2 to entry: The IO-Device interface is called "FAL services of the IO device" according to IEC 61158-5-10.

3.1.2.26
IO-Module
addressable sub input/output unit within a modular IO-Device

3.1.2.27
IO-Supervisor
engineering station enabled to read and write data from and to an IO-Device

Note 1 to entry: It is used for commissioning or diagnostics purposes. In contrast to an IO-Controller it does not take over an active role during the run-up of an IO-System. An IO-Supervisor is not part of the IO-System.

3.1.2.28
IO-System
IO-Controller and its associated IO-Devices

3.1.2.29
iParameter
individual or technology specific F-(Sub)Module parameters

Note 1 to entry: Typical iParameters are the protection zone coordinates of a laser scanner.

3.1.2.30
iPar-Server
standardised mechanism to store and retrieve individual or technology specific F-(Sub)Module parameters within the standard part of an F-Host or its controlled subsystem

3.1.2.31
master (class 1)
active CP 3/1 communication peer triggering slaves for data exchange

Note 1 to entry: The term "master" alone is used as a short form for "master class 1".

3.1.2.32
MonitoringNumber
MNR
means to ensure authenticity and the correct order of transmitted safety PDUs

Note 1 to entry: Instance of *sequence number* as described in IEC 61784-3.

Note 2 to entry: The MonitoringNumber is secured via the transmitted CRC signature.

3.1.2.33
process values
PV
input and output data (in a safety PDU) that are required to control an automated process

3.1.2.34
qualifier
additional qualifying bits within *process values* indicating the status of each individual input

3.1.2.35
Retentive Selection of the Codename
The Retentive Selection of the Codename is part or whole codename retentively stored in the F-(Sub)Module

3.1.2.36
shared IO
inputs and outputs in field devices that can be accessed by several controllers

Note 1 to entry: Even though CP 3/4 to CP 3/6 is permitting shared IO, it is not permitted with FSCP 3/1.

3.1.2.37
toggle bit
one bit of the Control and Status Byte to synchronize the (virtual) *MonitoringNumber* in both the F-Host driver and the F-Device driver

3.1.2.38
universal serial bus
USB
external bus standard

Note 1 to entry: USB is replacing serial and parallel computer ports and is used for fast direct connections between service computers and field devices.

3.1.2.39
V2-mode
FSCP 3/1 services and protocol according to this document

3.2 Symbols and abbreviated terms

3.2.1 Common symbols and abbreviated terms

BSC	Binary Symmetric Channel	
CP	Communication Profile	[IEC 61784-1/2]
CPF	Communication Profile Family	[IEC 61784-1/2]
CRC	Cyclic Redundancy Check	
DLL	Data Link Layer	
DLPDU	Data Link Protocol Data Unit	
EMC	Electromagnetic Compatibility	
EMI	Electromagnetic Interference	
EUC	Equipment Under Control	[IEC 61508-4:2010]
E/E/PE	Electrical/Electronic/Programmable Electronic	[IEC 61508-4:2010]
FAL	Fieldbus Application Layer	[IEC 61158-5 (all parts)]
FCS	Frame Check Sequence	
FIT	Failure In Time (equals 10^{-9} failure per hour)	
FS	Functional Safety	
FSCP	Functional Safety Communication Profile	
IACS	Industrial Automation and Control System	
MTBF	Mean Time Between Failures	
MTTF	Mean Time To Failure	
NSR	Non Safety Related	
PDU	Protocol Data Unit	[ISO/IEC 7498-1]
PELV	Protective Extra Low Voltage	[IEC 61010-2-201]
PFD	Average probability of dangerous Failure on Demand	[IEC 61508-4:2010]
PFH	Average frequency of dangerous failure [h^{-1}] per hour	[IEC 61508-4:2010]
PhL	Physical Layer	[ISO/IEC 7498-1]
PL	Performance Level	[ISO 13849-1]
PLC	Programmable Logic Controller	
RP	Residual Error Probability	
SCL	Safety Communication Layer	
SELV	Safety Extra Low Voltage	[IEC 61010-2-201]
SIL	Safety Integrity Level	[IEC 61508-4:2010]
SIS	Safety Instrumented Systems	
SL	Security Level	[IEC 62443 (all parts)]
SMS	Security Management System	[IEC 62443 (all parts)]
SPDU	Safety PDU	
SR	Safety Related	

3.2.2 CPF 3: Additional symbols and abbreviated terms

AES-CCMP	Advanced Encryption Standard – Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
AP	Application Process
API	Application Process Identifier
AR	Application Relationship
ASE	Application Service Element
ASIC	Application Specific Integrated Circuit
C	Coverage
CGP	Channel-granular Passivation
DR	Dynamic Reconfiguration
CP 3/1	Communication profile commonly known as PROFIBUS DP[3]
CP 3/2	Communication profile commonly known as PROFIBUS PA
CP 3/4 to CP 3/6	Communication profile commonly known as PROFINET
CPU	Central Processing Unit
CR	Communication Relationship
CRC_FP	16 bit CRC2 seed value of the F-Host (across F-Parameter = F_Par_CRC)
CRC_FP+	32 bit CRC value across F-Parameter
DAP	Device Access Point
DAT	Device Acknowledgment Time
DP	Decentralized Peripherals
F	Identifier for safety items (fail-safe, functional safe)
FB	Function Block
FV	Fail-safe Values
GSD	General Station Description (file associated with device)
GSDL	General Station Description Language (for CP 3/1 and CP 3/2 devices)
GSDML	General Station Description Markup Language (for CP 3/4 to CP 3/6 devices)
HAT	Host Acknowledgment Time
HD	Hamming Distance
IO	Input/Output
LED	Light Emitting Diode
LIV	Last Input-Value
LOV	Last Output-Value
MNR	MonitoringNumber
PA	Process Automation
Pe	Bit error probability
PN	PROFINET = CP 3/4 to 3/6
PiR	Parameterization in Run
PV	Process Values
SFRT	Safety Function Response Time
RADIUS	Remote Authentication Dial In User Service
S	*Standard*
TPF	Temporary Parameter File (XML File)
UML	Unified Modeling Language [43]

[3] For trade name declarations, see Clause 4.

USB	Universal Serial Bus	[48]
WCDT	Worst Case Delay Time	
WDTime	Watchdog Time	
XML	eXtensible Markup Language	[45], [46], [47]

3.3 Conventions

In this document, the abbreviation "F" is an indication for safety related items, technologies, systems, and units (fail-safe, functional safe).

In this document the default data that shall be used in case of unit failures or errors, are called fail-safe values (FV) and are set to "0".

In this document, reserved bit ("res") within the Status/Control Byte and the F-Parameters shall be set "0" and ignored by the receiver in order to avoid hassles with future versions of the FSCP 3/1 devices.

In this document, any CRC signature calculation resulting in a "0" value, will use the value "1" instead. Only exception see 8.1.8.

In this document the abbreviation "CP 3/4 to CP 3/6" comprises the three communication profiles CP 3/4, CP 3/5, and CP 3/6. CP 3/4 to CP 3/6 is commonly known as PROFINET.

This document uses UML2 notation for the drawing of the state charts and a condensed form for sequence charts [43]. The transition tables are depicted following the recommendations of IEC 62390.

4 Overview of FSCP 3/1 (PROFIsafe™)

Communication Profile Family 3 (commonly known as PROFIBUS™, PROFINET™[4]) defines communication profiles based on IEC 61158-2 Type 3, IEC 61158-5-3, IEC 61158-5-10, IEC 61158-6-3, and IEC 61158-6-10.

The basic profiles CP 3/1 and CP 3/2 are defined in IEC 61784-1; CP 3/4, CP 3/5 and CP 3/6 are defined in IEC 61784-2. The CPF 3 functional safety communication profile FSCP 3/1 (PROFIsafe™[4]) is based on the CPF 3 basic profiles in IEC 61784-1 and IEC 61784-2 and the safety communication layer specifications defined in this document.

FSCP 3/1 is based on the cyclic data exchange of a (bus) controller with its associated (field) devices using a one-to-one communication relationship (Figure 3). One controller can operate any mix of standard and safety devices connected to the network. Assigning safety tasks and standard tasks to different controllers also is possible. Any so-called acyclic communications between devices and controllers or supervisors such as programming devices are intended for configuration, parameterization, diagnosis, and maintenance purposes.

[4] PROFIBUS™, PROFINET™ and PROFIsafe™ are trade names of the non-profit organization PROFIBUS Nutzerorganisation e.V. (PNO). This information is given for the convenience of users of this document and does not constitute an endorsement by IEC of the trade name holder or any of its products. Compliance to this document does not require use of the registered logos for PROFIBUS™, PROFINET™ or PROFIsafe™. Use of the registered logos for PROFIBUS™, PROFINET™ or PROFIsafe™ requires permission of PNO and compliance with conditions for its use (such as testing and validation).

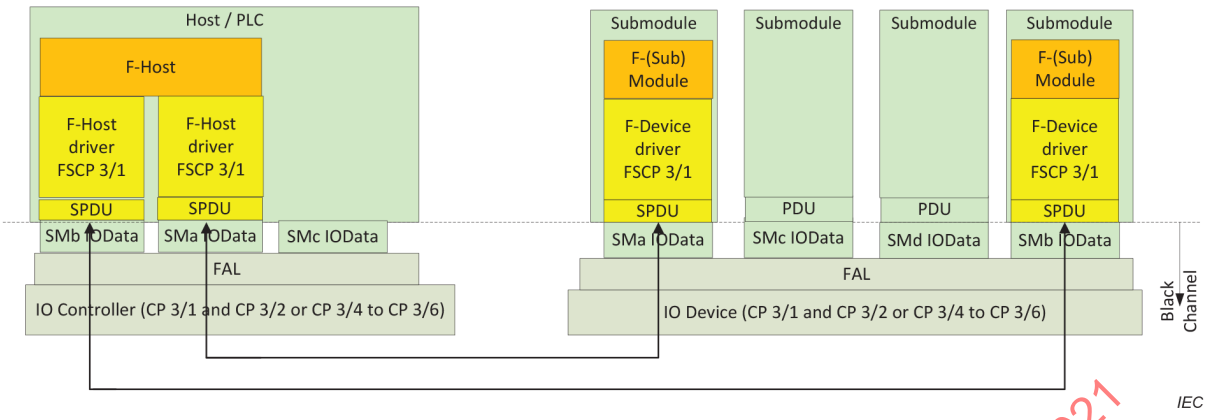


Figure 3 – Basic communication preconditions for FSCP 3/1

For the realization of FSCP 3/1, the following four measures have been chosen:

– (virtual) MonitoringNumber (MNR);
– watchdog time monitoring with acknowledgment;
– Codename per communication relationship (Codename is the basis for the MNR. The direction is differentiated via the one's complement of the MNR);
– cyclic redundancy checking for data integrity.

The MonitoringNumber uses a range that is large enough to secure any malfunction caused by message storing network elements. Every safety device returns a message with a safety PDU for acknowledgment even if there are no process data. A separate watchdog timer on both the sender and the receiver side is used for each one-to-one communication relationship. The Codename per communication relationship (and via additional measures the source-sink direction) is established for authentication reasons. The Codename is encoded within the calculated and transmitted CRC2 signature (Figure 4).

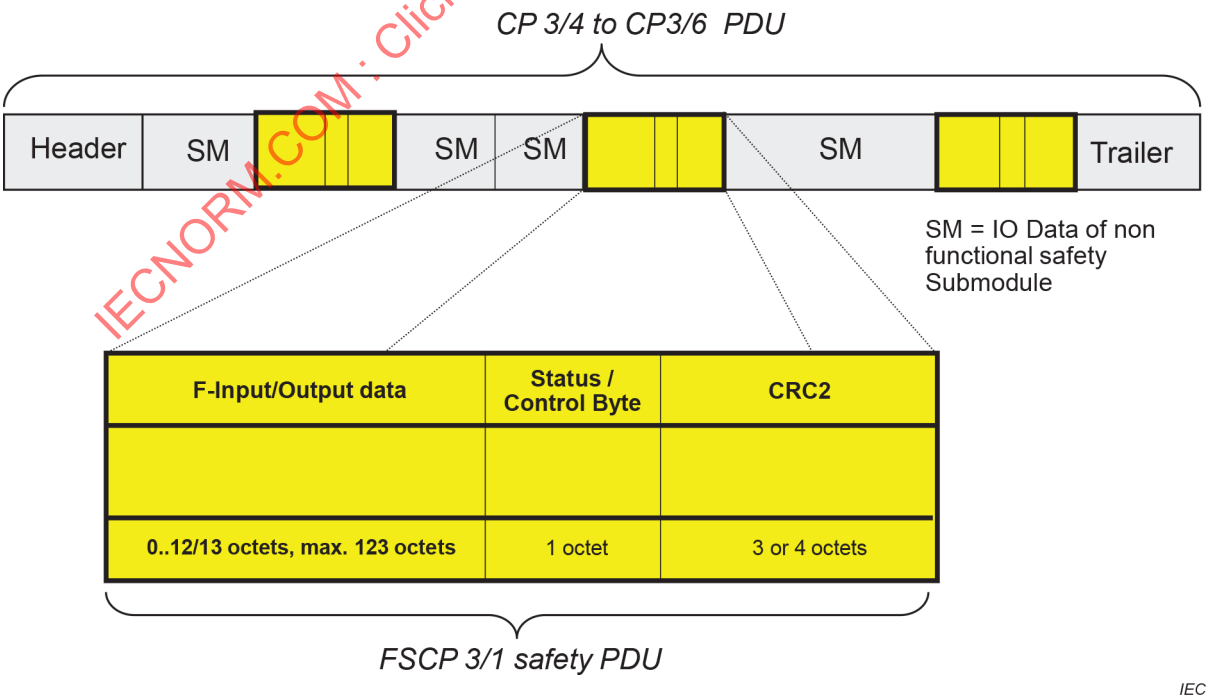


Figure 4 – Structure of an FSCP 3/1 safety PDU

FSCP 3/1 provides the so-called V2-mode. The V2-mode covers CPF3 such as programmable routing of messages and scientific findings on CRC properties.

Figure 5 provides an overview on FSCP 3/1 within the CPF 3 architectures.

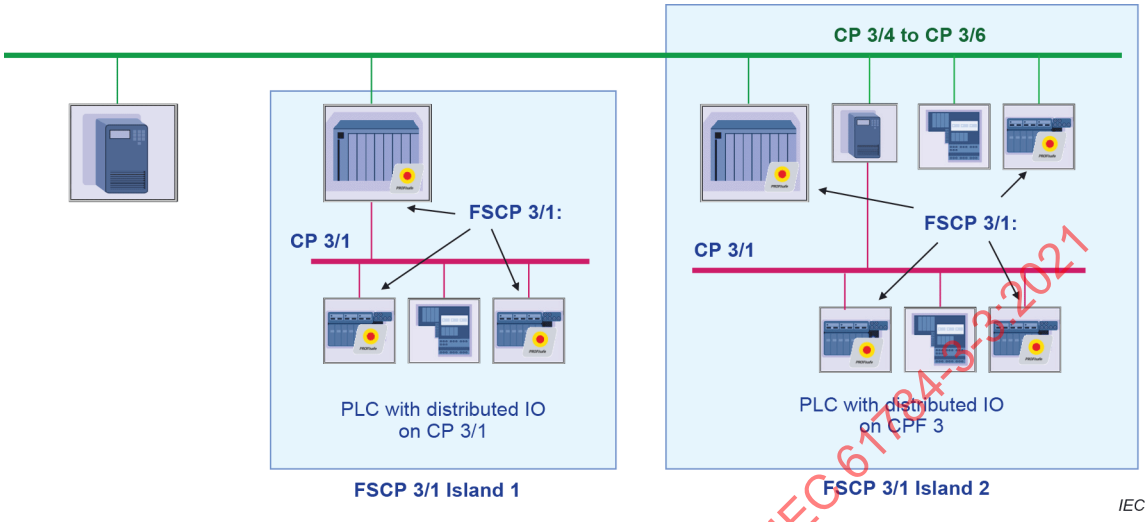


Figure 5 – Safety communication on CPF 3

While automation solutions with distributed IO gained widely acceptance through PROFIBUS (CP 3/1 and CP 3/2) and the industrial Ethernet based PROFINET (CP 3/4 to CP 3/6), safety applications were still relying on a second layer of conventional electrical techniques or special busses thus limiting the seamless engineering and interoperability. Additionally, modern safety devices such as laser scanners or drives with integrated safety could not be fostered as needed due to missing system support. It is the purpose of this document and related documents to provide the corresponding enabling technologies.

After this introduction, Subclause 5.1 holds additional references for the development of the FSCP 3/1 technology and 5.2 holds its functional requirements. The four safety measures of FSCP 3/1 are listed in 5.3. The network topologies within CP 3/4 to CP 3/6 and their crossovers to CP 3/1 and CP 3/2 are mentioned in 5.4. A brief introduction into the communication relationships and objects of the fieldbus standard is following in 5.5.

For safety and efficiency reasons the list of possible fieldbus data types is reduced to a concise set and described in 5.5.3. Subclauses 6.1 to 6.3 are unveiling the F-Host driver and F-Device driver services as well as the possible diagnosis messages of the safety layer.

Clause 7 starts with an overview on the safety PDU (7.1), continues with a description of the state machines for F-Host driver and F-Device driver and sequence diagrams in the Unified Modeling Language 2 format (7.2.2 to 7.2.5). Associated timing constraints are contained in 7.2.6 and 7.2.7. Following the format in IEC 61784-3:2021, Annex G, Subclause 7.3 illustrates the system reactions in the event of the possible malfunctions. Other system functions such as start-up of the safety layer are contained in 7.4. The layer management of safety devices focuses on safety communication specific F-Parameters (8.1) and on device specific individual iParameters (8.2). The requirements for handling and supply of the F-Parameters are described in 8.3. Subclause 8.4 deals with securing the data structures that are to be exchanged between the communicating partners and that represent the configuration of a device. Subclause 8.5 shows how the data structure information can be used to configure F-Host Channel drivers for more complex F-(Sub)Modules to save programming effort. The requirements for the system integration of iParameterization means and tools are listed in 8.6. The aspects of response times, installation guidelines, and duration of demands, maintenance, safety manual, wireless transmission, and F-Host conformance classes are covered in Clause 9. The reasoning for assessment is pointed out in 10.1 and the details in 10.2. An informative Annex A contains

examples for fast CRC signature calculations and a bibliography. Two additional FSCP 3/1 guidelines for electrical safety and assessment shall be observed ([36], [61]).

Annex C describes new optional features. Clause C.1 contains requirements for the "reaction on Device_Fault in F-Host" either as documentation or implemented in the state machine. Clause C.2 specifies the optional F-Host feature to "Disable F-(Sub)Module". Clause C.3 explains the use of PROFIenergy together with FSCP 3/1. Clause C.5 specifies the requirements on multiple F-Hosts communicate with single F-(Sub)Module. The Amendment "PROFIsafe Parameterization in Run" specifies the optional feature FSCP 3/1 Parameterization in Run, see [64].

5 General

5.1 External documents providing specifications for the profile

In addition to the normative references in Clause 2, the technology in this document meets the requirements of NE97 [44].

5.2 Safety functional requirements

The following requirements apply for the development of the FSCP 3/1 technology.

a) Safety communication and standard communication shall be independent. However, standard devices and safety devices shall be able to use the same communication channel.

b) Safety communication shall be suitable for Safety Integrity Level SIL3 (see IEC 61508) and PL e (see ISO 13849-1).

c) Safety communication shall use a single-channel communication system. Media Redundancy and/or System Redundancy may be used optionally for increased availability.

d) Implementation of the safety transmission protocol shall be restricted to the communication end devices (F-Host driver or F-Device driver).

e) There shall always be a 1:1 communication relationship between an F-Device driver and its F-Host driver.

f) The transmission duration times shall be monitored.

g) Environmental conditions shall be according to general automation requirements, mainly IEC 61326-3-1 or IEC 61326-3-2, if there are no particular product standards.

h) Transmission equipment such as controllers, ASICs, links, couplers, etc. shall remain unmodified (black channel). The safety functions shall be above OSI layer 7 (i.e. profile, no standard protocol changes or enhancements)

i) The safety communication shall not reduce the permitted number of devices. Restrictions may occur during mapping in case of CP 3/2 applications due to message limitations (see CP 3/2 in IEC 61784-1).

j) Safety communication shall be suitable for NE97 [44] and meet the requirements of IEC 61784-3:2021.

5.3 Safety measures

The safety measures mentioned in Table 1 for mastering possible transmission errors are one significant component of the FSCP 3/1 profile. The selection in Table 1 of the generic safety measures listed in IEC 61784-3:2021, 5.5 is required for FSCP 3/1.

The safety measures shall be processed and monitored within one safety unit.

Table 1 – Deployed measures to master errors

Communication error	Safety measures			
	(virtual) MonitoringNumber [a]	Timeout with receipt [b]	Codename for sender and receiver [c]	Data integrity check [d]
Corruption	–	–	–	X
Unintended repetition	–	X	–	–
Incorrect sequence	X	–	–	–
Loss	X	X	–	–
Unacceptable delay	–	X	–	–
Insertion	X	–	–	–
Masquerade	–	–	–	X
Addressing	X	–	X	–
Out-of-sequence	X	–	–	–
Loop-back of messages	X [e]	–	–	–

[a] Instance of "sequence number" of IEC 61784-3.

[b] Instance of "time expectation" (Timeout) and "feedback message" (Receipt) of IEC 61784-3.

[c] Instance of "connection authentication" of IEC 61784-3.

[d] Instance of "data integrity assurance" of IEC 61784-3, based on CRC signature.

[e] in mode F_CRC_Seed =0 via status bit 7, in mode F_CRC_Seed =1 via one's complement of MNR

In case of communication errors according to Table 1, defined fault reactions as specified in Table 11, Table 13 and 7.2.7.1 shall occur.

5.4 Safety communication layer structure

5.4.1 Principle of FSCP 3/1 safety communications

FSCP 3/1's way of safety communication is based on the experience made in the railway signaling technique as it has been laid down in earlier versions of IEC 62280.

On this basis, safety communication is performed by

- a standard transmission system (Figure 6), and
- an additional safety transmission protocol on top of this standard transmission system.

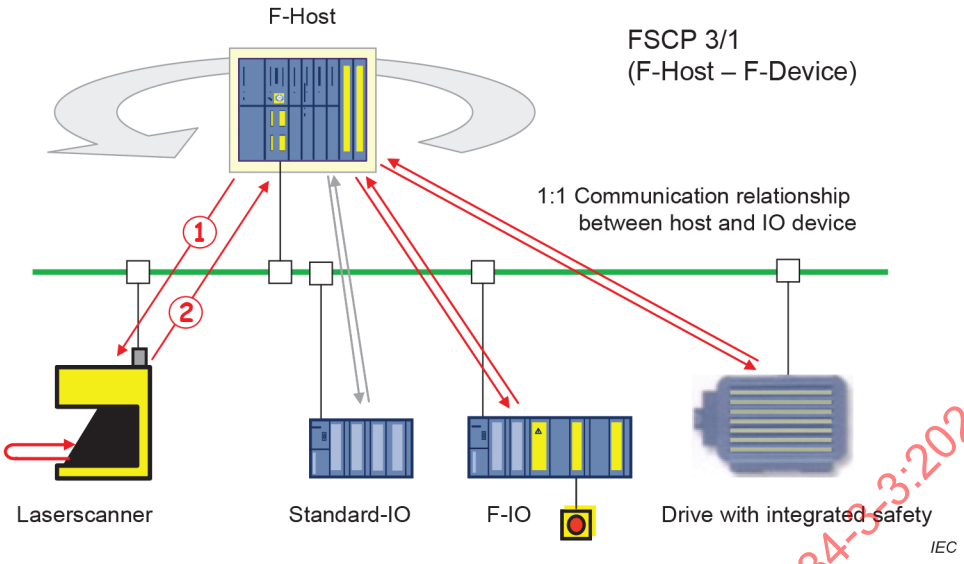


Figure 6 – Standard CPF 3 transmission system

The standard transmission system includes the entire hardware of the transmission system and the related protocol functions (i.e. OSI layers 1, 2 and 7 according to Figure 7).

Safety applications and standard applications are sharing the same standard CPF 3 communication systems at the same time. The safe transmission function comprises all measures to deterministically discover all possible faults / hazards that could be infiltrated by the standard transmission system or to keep the residual error rate under a certain limit. This includes

- Random malfunctions, for example due to electromagnetic interference on the transmission channel;
- Failures / faults of the standard hardware;
- Systematic malfunctions of components within the standard hardware and software.

This principle delimits the assessment effort to the "safe transmission functions". The "standard transmission system" (black channel) does not need any additional safety assessment.

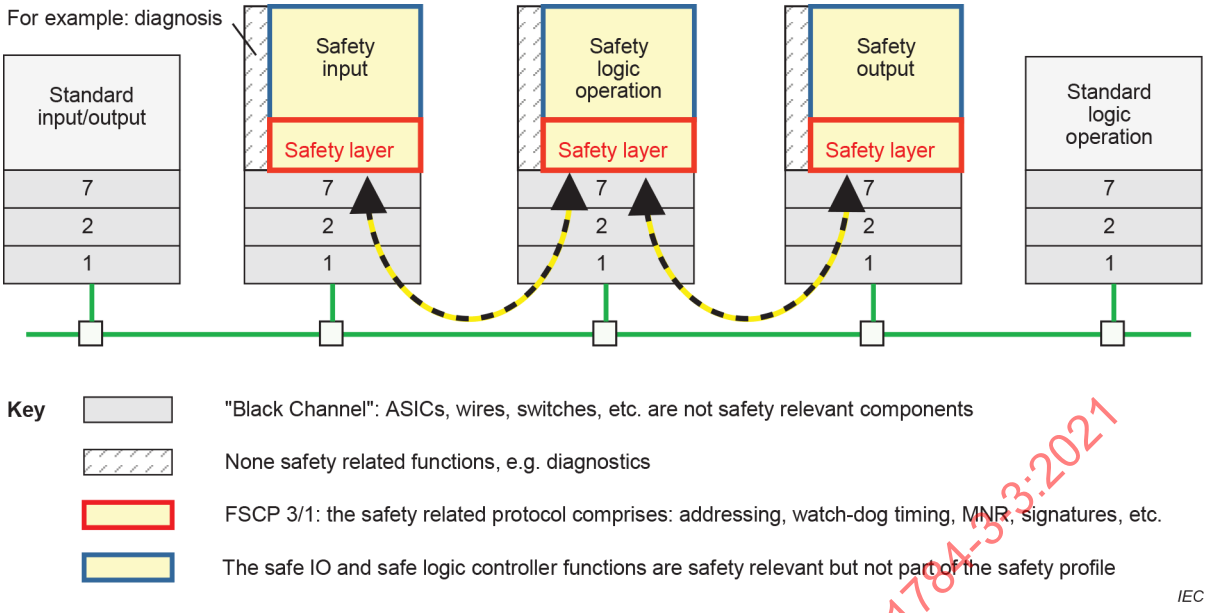


Figure 7 – Safety layer architecture

Transmission is performed via electrical, optical conductors or wireless. Permissible topologies and transmission features of the standard transmission system and the components of the "black channel" are described in 5.4.2.

5.4.2 CPF 3 communication structures

The basic communication layers of CP 3/4 to CP 3/6 are shown in Figure 8. While the cyclic transmitted buffered safety communication of FSCP 3/1 is using the real-time channel the other services are using acyclic queued communication.

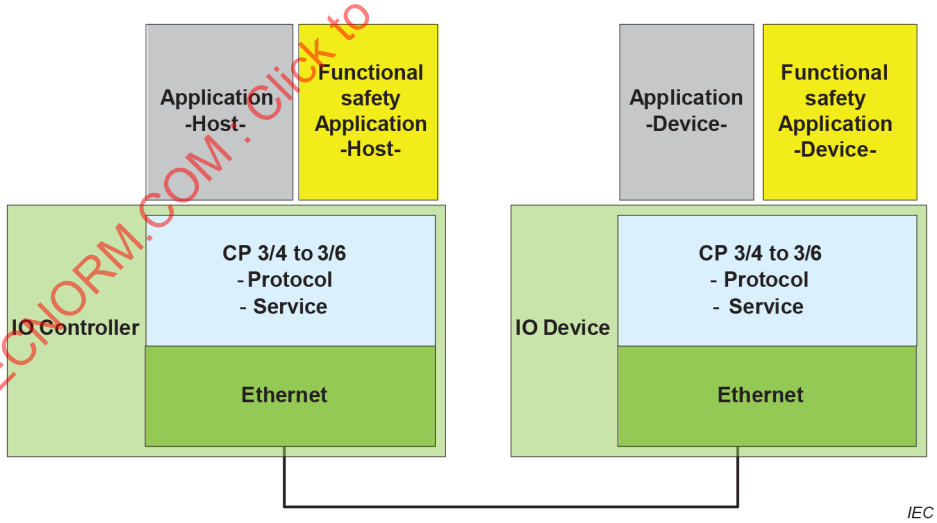


Figure 8 – Basic communication layers

Networks which belong to one CP 3/4 to CP 3/6

In systems with one particular IP-Address as the Real-Time protocol (RT or IRT) in layer 2 cannot pass beyond this IP-Address space. It is the (OSI layer 3) task of routers to redirect messages on an IP-Address level (see Figure 9). Thus routers are natural borders for CP 3/4 to CP 3/6 systems where RT_CLASS_UDP is not permitted or not supported.

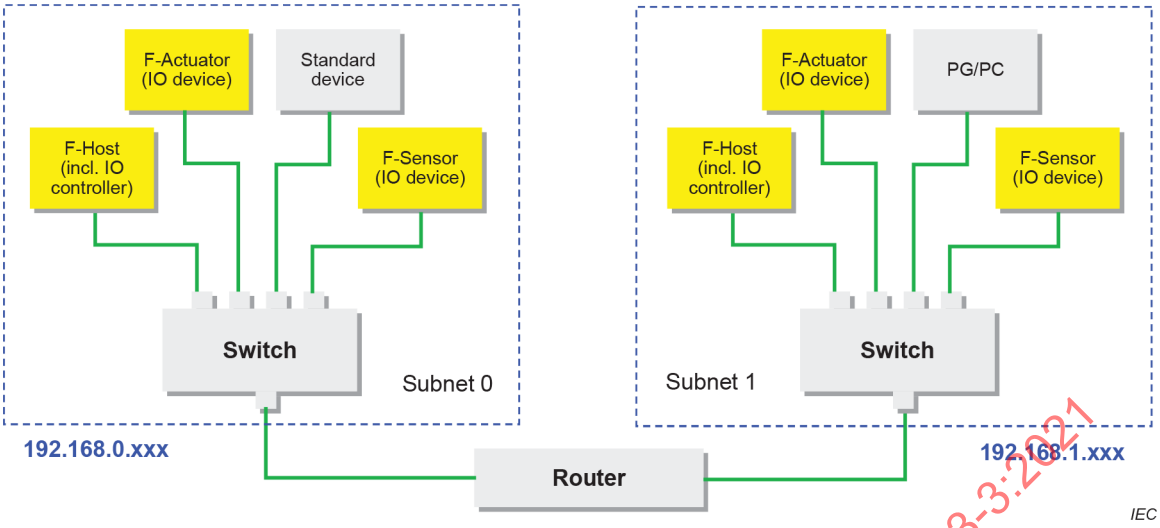


Figure 9 – Crossing network borders with routers

The following restrictions apply for FSCP 3/1.

- Wireless LAN permitted. However, uniqueness of Retentive Selection of the Codenames shall be guaranteed within a Subnet.
- Single port routers are not permitted (7.3.11).

If the cyclic transmitted buffered communication is crossing routers, the Codenames within the entire network shall be unambiguous and the Codename checks shall identify unambiguous relationships and via additional measures both transmission directions.

In contrast to the fieldbus system configuration, Figure 10 shows the possible network structure, i.e. how far the safety profile extents into the individual units. A standard remote IO, for example, can comprise an F-Module for the connection of an emergency stop pushbutton. Thus the whole FSCP 3/1 transmission path reaches from the F-Host driver across its backplane bus via CP 3/4 to CP 3/6 into the IO-Device and across a possible other backplane into the final F-Submodule. The safety layer is implemented within these far ends of communication.

Multi-controller or multi-master operation of F-Hosts is permitted. "Shared F-Inputs" are not permitted. A mix of F-Host and standard host is possible.

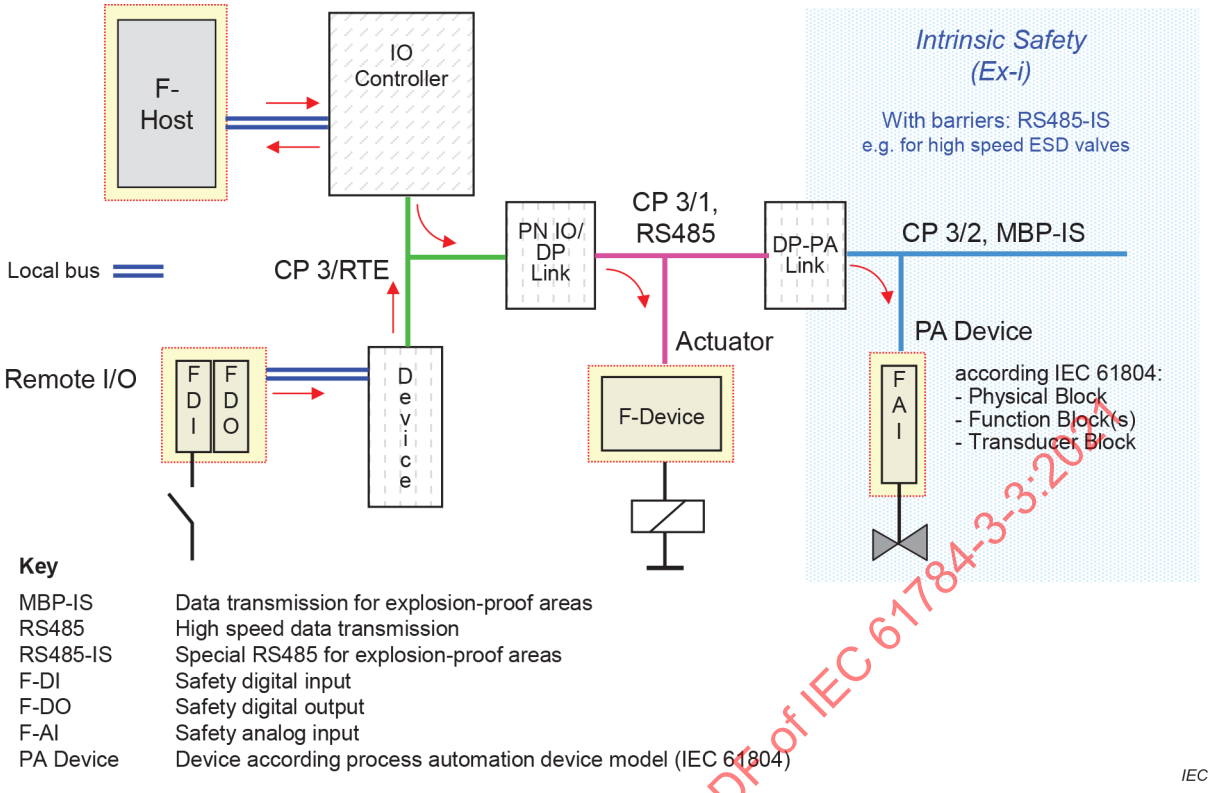


Figure 10 – Complete safety transmission paths

5.5 Relationships with FAL (and DLL, PhL)

5.5.1 Device model

The CP 3/4 to CP 3/6 as well as the CP 3/1 device model is assuming one or several application processes (AP) within the device. Figure 11 shows the internal structure of an application process for a modular field device. Optionally it could have several of these APs. The application process is subdivided into as many Modules as needed to represent the physical IOs of the device. In contrast to CP 3/1, CP 3/4 to CP 3/6 provides two hierarchical level more: the Submodules with channels.

Within the Submodule, application service elements (ASE) provide a set of standardized services for conveying requests and responses to and from application processes and their data objects such as IO data, Context (Parameterization), Diagnosis, Alarms, and Record Data.

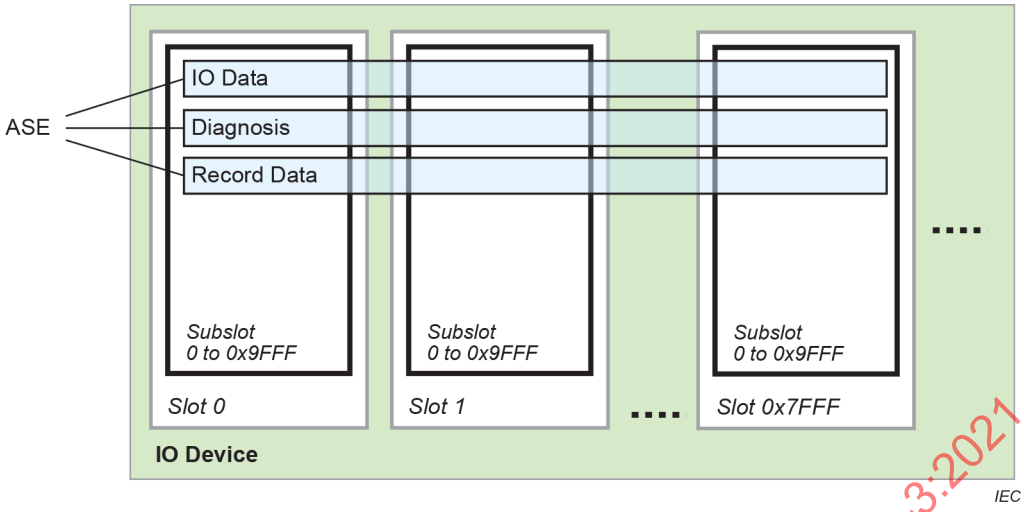


Figure 11 – IO Device model

The device manufacturer is responsible for the specification (GSD) of F-(Sub)Modules that can be plugged into Slots and Subslots.

5.5.2 Application and communication relationships

CP 3/4 to CP 3/6 in general permits shared input. Since FSCP 3/1 is based on 1:1 communication relationships, shared input cannot be used for functional safety.

5.5.3 Data types

CPF 3 uses the basic data types listed in IEC 61158-5-10. Table 2 shows a restricted number of data types for FSCP 3/1. Table 3 shows the specified F_Message Trailers.

Table 2 – Data types for FSCP 3/1

Data type name	Number of octets
Unsigned8 (use as bits)	1
Unsigned16 (use as bits) [a]	2
Unsigned32 (use as bits) [a]	4
Integer16	2
Integer32	4
Float32	4
Unsigned8 (use as bits) +Unsigned8 (use as bits)	2
Float32+Unsigned8 (use as bits)	5
[a] It is highly recommended to use multiple Unsigned8 instead.	

Table 3 – F_MessageTrailer for FSCP 3/1

F_MessageTrailer	Number of octets
F_MessageTrailer4Byte (F_CRC_Seed = 0)	4
F_MessageTrailer5Byte (F_CRC_Seed = 1)	5

NOTE Rationale for Unsigned8: As CPF 3 uses the octet sequence Big Endian the numbers of the channels are not according to the bit number of Unsigned16/32. In case of using BitDataItems the BitOffsets are not synchronous to the number of the channels. By using multiple Unsigned8 (used as bits) it can be avoided that the F-Modules with more than one octet booleans are represented differently in different F-Hosts.

Single bits shall be coded within Unsigned8 data type due to its higher efficiency in comparison to the data type Boolean.

See IEC 61158-5-10 for general information on data types and 8.4.2 for functional safety coding.

6 Safety communication layer services

6.1 F-Host driver services

Figure 12 shows that each F-Input and each F-Output requires a safety PDU management (F driver) in order to handle the FSCP 3/1 protocol. The corresponding F-Host operates with an instance of an F driver for each F-Input or F-Output respectively. Thus each and every 1:1 relationship between an instance of the F-Host driver and the corresponding partner F-Device driver is identified by a Codename (one of the F-Parameters).

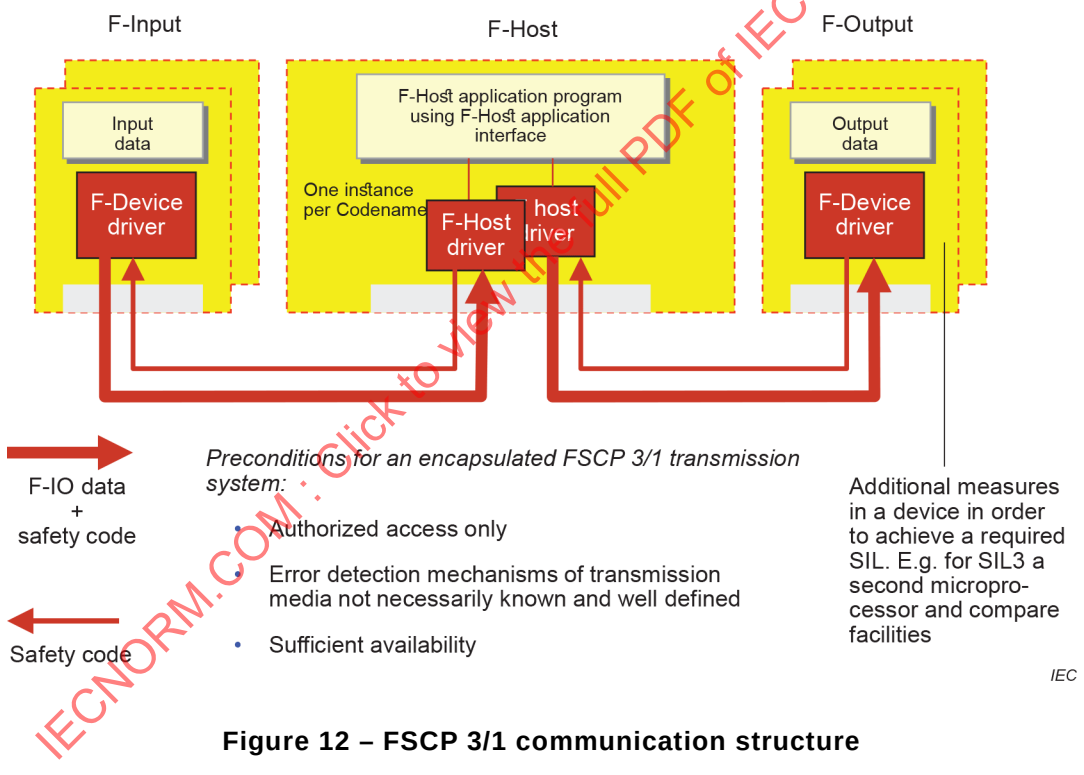


Figure 12 – FSCP 3/1 communication structure

The entire standard CPF 3 communication equipment between F drivers belongs to the black channel. The arrows in Figure 12 are indicating the cyclic transmitted buffered communication between the F drivers: the safety addenda (Status or Control Byte and CRC2) are transferred in addition to the F-Input data from the F-Input to the F-Host driver.

As an acknowledgment, the F-Input merely receives the safety addenda (safety code). Accordingly, the F-Output receives the safety addenda in addition to the F-Output data, and uses it for acknowledgment.

NOTE It is possible for F-(Sub)Modules to provide F-Input and F-Output data.

Safety PDU management and F-Parameterization are tasks of the F drivers within the F-Host and the F-(Sub)Modules. They provide also the measures to support the additional system features "Parameterization in Run" (PiR) according to [54] and "Channel-granular Passivation" based on [56].

The F application interface at the F-Host application program level is shown in Figure 13.

"Dynamic Reconfiguration" (DR) or "Maintenance of Fault Tolerant Systems" according to [54] are planned activities that shall be monitored by authorized personnel only. DR shall only be activated by an operator. It shall not be set/reset via the "F Application Program".

The design of corresponding safety-related parts of the F-Host shall exclude any unintended activation of the function "use_TO2" (see 7.2.7.2).

The F-Host may set and reset "use_TO2" for all the F-(Sub)Modules thus affecting all F-(Sub)Modules simultaneously.

The F-Host shall extend the regular (primary) watchdog time (F_WD_Time) by a secondary watchdog time (F_WD_Time_2) once only (see Figure 18, Figure 26, Figure 27, 7.2.7.2, 8.1.1, 8.1.4).

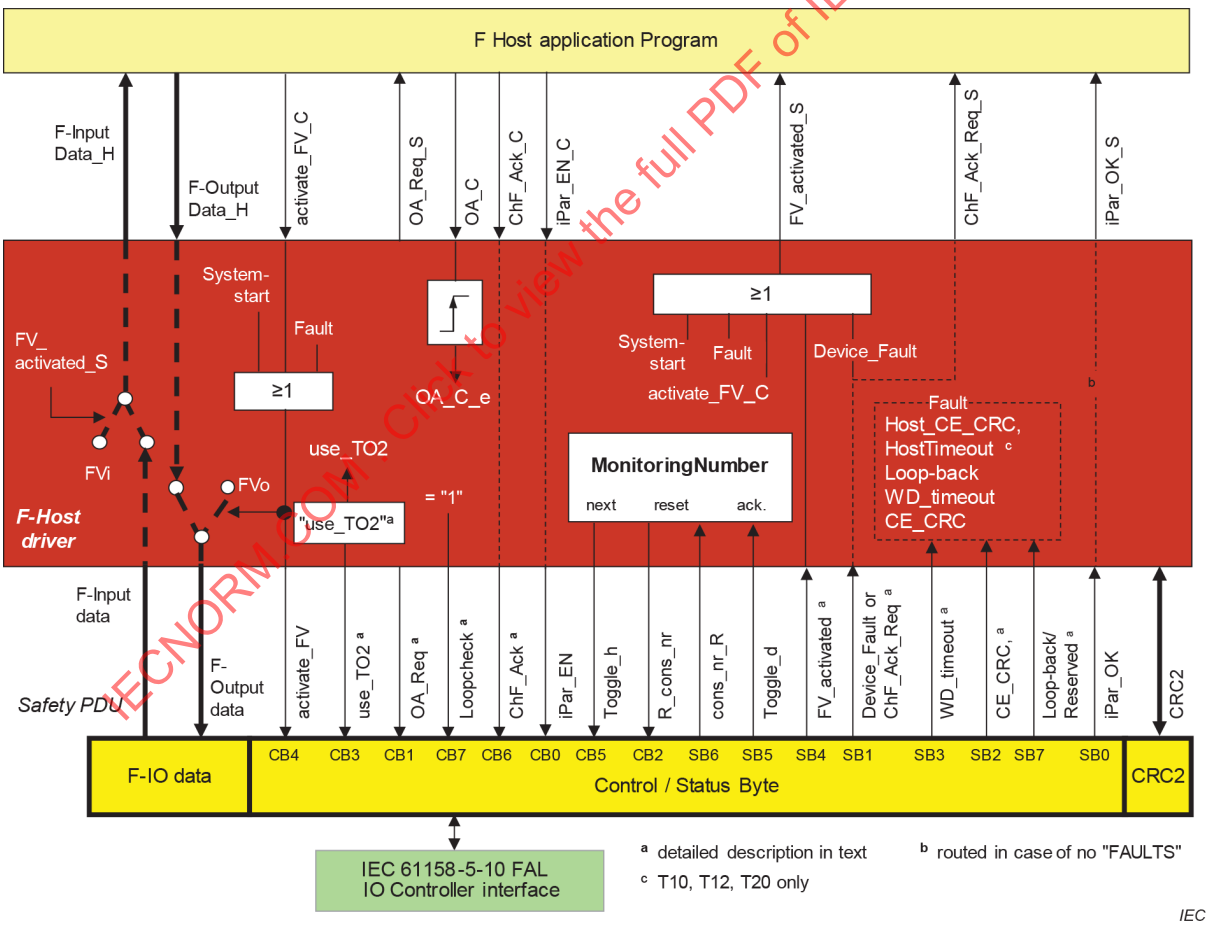


Figure 13 – F application interface of F-Host driver instances

The need for "Channel-granular Passivation" can be seen in 5.4.2 and Figure 10. The FSCP 3/1 transmission path reaches for example an F-(Sub)Module of a Remote IO. Usually, the F-Module provides several signal channels each for a safety sensor as shown in Figure 14. Each signal channel can be associated with an individual safety function. In case one channel fails, the F-Module will cause all associated safety functions to enter the fail-safe state. The option "Channel-granular Passivation" based on [56] allows for an individual fail-safe state only for that safety function, which is impacted by the failed signal channel.

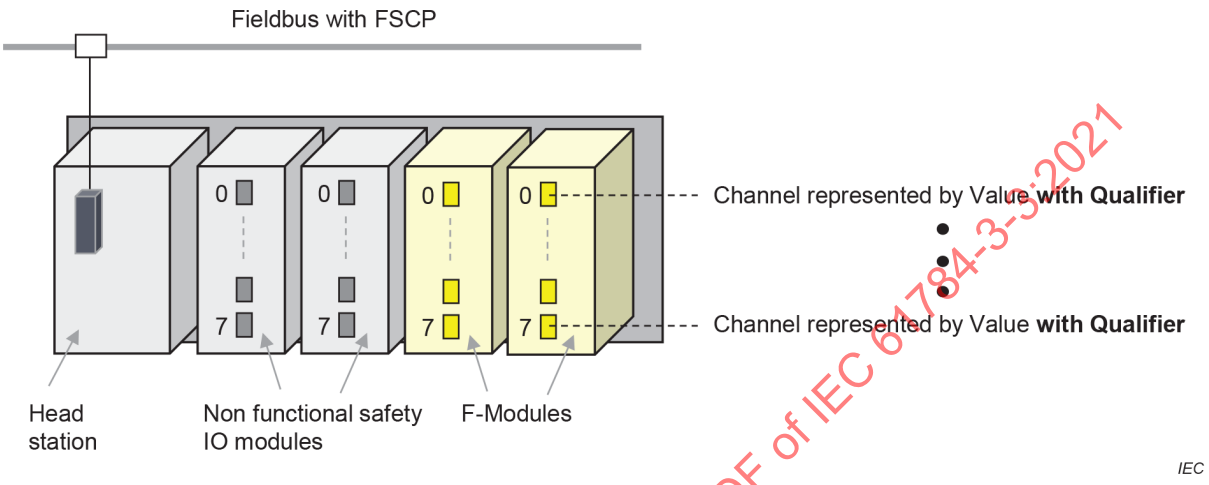


Figure 14 – Motivation for "Channel-related Passivation"

There are several variables available to the programmer to manipulate these safety processes according to the standards. The variables are carrying similar names – normally extended by an index "_C" (Control) or "_S" (Status) – like the corresponding bits within the Status and Control Bytes but may have some control logic in between within the F driver. See also 8.5.2 and Figure 52.

Implementation hints for the F-Host driver are collected in 8.5.3.

The following variables shall be available to the programmer of an F-Host application program in accordance with 9.10:

activate_FV_C Every F-Host application program that deals with a corresponding F-Host driver shall set/reset this variable (type: bit). With input devices (for example sensors) this variable set to "1" causes the F-Host driver to deliver fail-safe values ("0") to the F application program. With output devices (for example actuators) this variable set to "1" causes the F-Host driver to send fail-safe values ("0") to the F-Device driver and to set bit "activate_FV" of the Control Byte to "1". The safety concept of the output device defines the kind of information of "activate_FV" shall be used to achieve the safe state at the F-(Sub)Modules output.

FV_activated_S Every F-Host application program that deals with a corresponding F-Device driver shall evaluate this variable (type: bit). With input devices this variable indicates via "1" the F driver is delivering fail-safe values ("0") to the F-Host application program for each and every channel of the F-Module. See [56].

With output devices this variable indicates via "1" that each and every channel of the F-Module is set to fail-safe values "0" (default behavior) or an F-Output device specific value controlled by the "activate_FV" signal (= bit 4 of the Control Byte). See [56].

This variable (type: bit) represents the result of a logical "OR" of the signals: Faults, activate_FV_C, FV_activated (SB4), Device_Fault, and System start (implicit). ChF_Ack_Req does not influence *FV_activated_S*.

iPar_EN_C This variable if set to "1" shows the request of a parameterization assignment. Recommended usage of *iPar_EN_C* in case F_CRC_Seed =1 see Amendment "Amd 1 PiR" [64].

iPar_OK_S This variable if set to "1" indicates Parameter acknowledge by the F-(Sub)Module application. Recommended usage of *iPar_OK_S* in case of F_CRC_Seed =1 see Amendment "Amd 1 PiR" [64].

OA_C
(Operator Acknowledgment) Every F-Host application program shall set/reset this variable (type: bit). In changing this variable to "1" the application is able to resume a safety function after a fault reaction (safety function specific) via an F-Host application program.

OA_Req_S This variable (type: bit) indicates a request for acknowledgment prior to the resumption of a safety function. In case the F-Host driver or an F-Device driver detects a communication error or an F-(Sub)Module fault (Device_Fault = 1 and OAD_Nec_C = 1 and F_Passivation = 0), fail-safe values will be activated until an error or fault is cleared and an operator acknowledgment occurred. The F-Host driver then sets the variable OA_Req_S (="1") as soon as the fault/error has been eliminated and operator acknowledgment is possible. Once the acknowledgment occurred (OA_C = "1") the F-Host driver will reset the request variable OA_Req_S (= "0").

ChF_Ack_C
(Channel Operator Acknowledgment) F_Passivation =1 (see 8.1.6.2): Every F-Host application program shall set/reset this variable (type: bit). In changing this variable to "1" the application is able to resume a safety function after any cleared signal channel fault within an F-(Sub)Module via an F-Host application program. ChF_Ack (CB6) is set to "0" in case of stored faults (FAULTS and/or WD_timeout), otherwise takes over the value of ChF_Ack_C. The signal ChF_Ack_C can be omitted and represented by signal OA_C instead.

ChF_Ack_Req_S F_Passivation =1 (see 8.1.6.2): This variable (type: bit) indicates a request for acknowledgment if at least one of the input or output channels within an F-(Sub)Module had failed. The F-Device driver then sets the variable ChF_Ack_Req (= "1") as soon as the fault/error of at least one channel within the F-(Sub)Module has been eliminated. Once the acknowledgment occurred (ChF_Ack = "1") the F-Device driver will reset the request variable ChF_Ack_Req (= "0"). This signal can be logically ORed with *OA_Req_S* and presented as joint signal *OA_Req_S*. ChF_Ack_Req_S is set to "0" in case of stored faults (FAULTS and/or WD_timeout), otherwise takes over the value of ChF_Ack_Req.

Input values	PVi	Process input values (←F-Input_Data_D, see Figure 15)
	FVi	Fail-safe input values, used instead of PVi for F-Input_Data_D (Figure 15).
Output values	PVo	Process output values (→F-Output_Data_D)
	FVo	Fail-safe output values (=0), used instead of PVo for F-Output_Data_D.

6.2 F-Device driver services

Figure 15 illustrates details of the F-Device driver and how it is embedded between the CP 3/4 to CP 3/6 interface and the safety part of the specific device application. During the start-up phase and in working modus the non-safety part of the specific device application receives the F-Parameters and passes them down to the F-Device driver. The F driver itself, after checking some of the F-Parameters passes some F-Parameters up to the safety part of the specific F-Submodule application.

Usually the specific device application provides a time base (1 ms) to the F-Device driver in order to feed the watchdog timers.

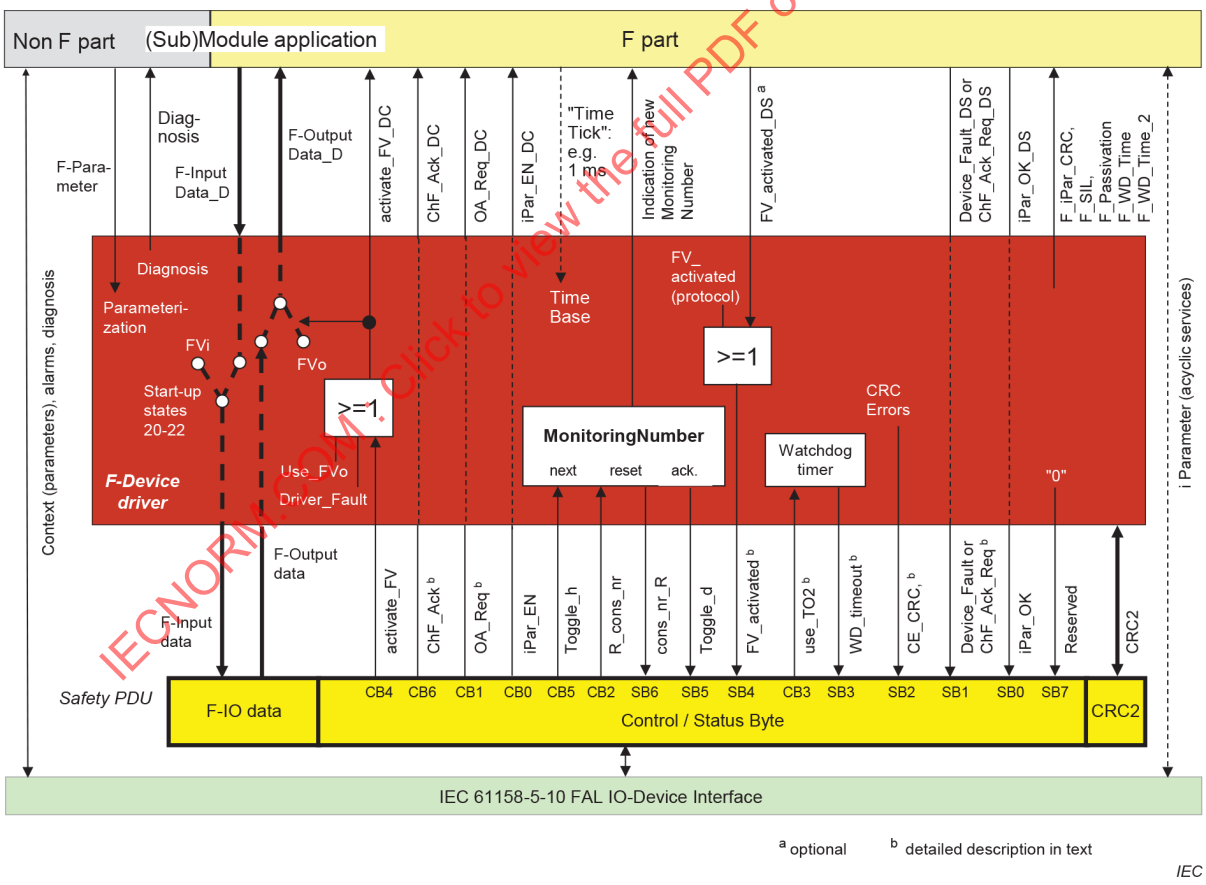


Figure 15 – F-Device driver interfaces

The F-Device driver mainly deals with safety PDUs that are received or transmitted via the cyclic transmitted buffered IO Data Communication Relationship of CP 3/4 to CP 3/6 (5.5.2). The F-IO data usually are passed through except during start-up (FVi instead) or in case of faults (FVo instead). The received safety PDUs are containing Control Bytes with Control Bits CB0 to CB6 (in case of F_CRC_Seed =0: CB7 also). Some of these signals are passed through to the application interface without interaction. An indication of a new MonitoringNumber is provided to facilitate the implementation of demands with sufficient duration (at least one FSCP 3/1 cycle = two different MonitoringNumbers).

In return safety PDUs are prepared for transmission. They are containing Status Bytes with Status Bits SB0 to SB6. One of these is passed through, the F driver is generating some of them, and some are coming from the application interface with F driver manipulation before the entry into the safety PDU. Driver_Fault is set in case of an internal fault of the F driver.

The MonitoringNumber is changed when "Toggle_h" is changing its state (0→1; 1→0). R_cons_nr = "1" will reset the MonitoringNumber. The MonitoringNumber being changed will change the state of "Toggle_d" (0→1; 1→0). CRC checking is executed with each received and sent safety PDU (CRC2).

The following variables are available to the specific device application. The variables are carrying similar names – normally extended by an index "DC" (device control) or "DS" (device status) – like the corresponding bits within the Status and Control Bytes.

activate_FV_DC	This safety-related variable indicates the F-Output data are fail-safe values (FV = 0). It can be used to force the outputs of an F-(Sub)Module to configured or built-in fail-safe values.
FV_activated_DS	For input devices this variable indicates via "1" the device application is delivering fail-safe values ("0") to the FSCP 3/1 driver for every input value. For output devices this variable indicates via "1" that each and every output channel is set to fail-safe values. For combined input and output devices this variable (type: bit) indicates via "1" the device application is delivering fail-safe values ("0") to the FSCP 3/1 driver for each and every input and output channel is set to fail-safe values.
OA_Req_DC	The F-(Sub)Module application shall use this non-safety-related variable to indicate locally the request for an operator acknowledgment (*OA_C* within F-Host) usually via a LED. Implementation is optional for F-(Sub)Modules.
Device_Fault_DS or *ChF_Ack_Req_DS*	F_Passivation =0 (see 8.1.6.2): Fault recognized by the specific device application; F_Passivation =1 (see 8.1.6.2): Fault recognized by any signal channel of an F-(Sub)Module via qualifier (see [56]) is cleared and can be acknowledged.
ChF_Ack_DC	F_Passivation =1 (see 8.1.6.2): The F-Host application program sets this variable to "1". This acknowledgment confirms that the signal channel fault has been cleared and personal has left the protection area.

6.3 Diagnosis

6.3.1 Safety alarm generation

Due to fast polling cycles of the F-Host application program, the speed of detecting modifications of the F- IO data and the CRC2 signature is satisfactory. In case of communication errors the system is able to react in time in a safe manner for example via the information in the Status Byte.

6.3.2 F-(Sub)Module safety layer diagnosis

In order to report diagnosis information of the FSCP 3/1 F-Device driver to a human machine interface device, the F-Device driver passes its information to the F-Submodule application which is using standard CP 3/4 to CP 3/6 mechanisms for propagation to the IO-Controller. Every standard diagnosis option of CP 3/4 to CP 3/6 is possible, preferably the Channel-Related-Diagnosis. There is an assigned range for FSCP 3/1 within the coding table of the field "ChannelErrorType" in IEC 61158-6-10.

Table 4 shows the different types of diagnosis information of the FSCP 3/1 protocol layer within F-(Sub)Modules.

Table 4 – Safety layer diagnosis messages

Hex	Number	Diagnosis Information	Mandatory
0x0040	64	Mismatch of safety destination address (F_Dest_Add), see 8.1.2	Yes
0x0041	65	Safety destination address not valid (F_Dest_Add), see 8.1.2	-
0x0042	66	Safety source address not valid or mismatch (F_Source_Add), see 8.1.2	-[a]
0x0043	67	Safety watchdog time value is 0 ms (F_WD_Time, F_WD_Time_2)	-
0x0044	68	Parameter "F_SIL" exceeds SIL from specific device application	-
0x0045	69	Parameter "F_CRC_Length" does not match the generated values	-
0x0046	70	Version of F-Parameter set incorrect	-
0x0047	71	Data inconsistent in received F-Parameter block (CRC1 error)	Yes
0x0048	72	Device specific or unspecified diagnosis information, see manual	-
0x0049	73	Save iParameter watchdog time exceeded	-
0x004A	74	Restore iParameter watchdog time exceeded	-
0x004B	75	Inconsistent iParameters (iParCRC error)	Yes[b]
0x004C	76	F_Block_ID not supported	-
0x004D	77	Transmission error: data inconsistent (CRC2 error)	Yes[c]
0x004E	78	Transmission error: timeout (F_WD_Time or F_WD_Time_2 elapsed)	Yes[c]
0x004F	79	Acknowledge required to enable the channel(s) – as channel error(s) is/are remedied.	See[d]
0x0050	80	Reserved: do not use numbers, do not evaluate numbers	-
0x0051	81	Reserved: do not use numbers, do not evaluate numbers	-
..	..	Reserved: do not use numbers, do not evaluate numbers	-
0x005F	96	Reserved: do not use numbers, do not evaluate numbers	-

[a] shall be used with Address Type 2

[b] mandatory if parameter in F_Block_ID: "F_iPar_CRC" = 1,

[c] mandatory for variant F_CRC_Seed = 1,

[d] used for variant F_Passivation = 1.

The column mandatory shows which diagnosis messages shall be sent in case of a corresponding error. If a non mandatory diagnosis message is implemented then it shall use the corresponding diagnosis number.

F-(Sub)Modules using the iPar-Server mechanism to store and retrieve iParameters within an F-Host or its controlled subsystem can report dedicated diagnosis information via vendor specific additional codings.

F-(Sub)Modules shall use these types within diagnosis messages, whenever applicable. However, diagnosis messages can carry summary information for several individual causes.

Transmission errors (codes 77 and 78) shall not lead to diagnosis message flooding, for example via waiting on correct FSCP 3/1 communication first prior to new entry to the Diagnosis ASE.

Transmission error: data inconsistent (CRC2 error) shall lead to an internal buffer entry according to Table 5 which can be read by a vendor specific tool.

Table 5 – Buffer entry on CRC2 error

Attribute name [a]	Length		Description
IMPLICIT 1	8 octets	Mandatory	In case F_CRC_Seed =0: MNR In case F_CRC_Seed =1: CN_incrNR_64 [1]
IMPLICIT 2	8 octets	Mandatory	In case F_CRC_Seed =0: F_Par_CRC In case F_CRC_Seed =1: CN_incrNR_64 [2]
CRC_Expected	4 octets	Mandatory	Expected CRC
CRC_Received	4 octets	Mandatory	Wrong CRC
VERSION	2 octet	Optional	Value = 1
Codename	4 octets	Optional	
…	…	Optional	manufacturer specific
[a] These Attribute names are examples, the real names are defined by the vendor.			

A device vendor should explain the mapping of the individual causes to a particular diagnosis message.

Further information can be retrieved from [40] and [58].

7 Safety communication layer protocol

7.1 Safety PDU format

7.1.1 Safety PDU structure

Figure 16 shows the structure of one single safety PDU that contains the safety input/output data and an additional safety code. A CP 3/4 to CP 3/6 message may contain several safety PDUs, for example in case of modular IO-Devices for each F-(Sub)Module its own safety PDU.

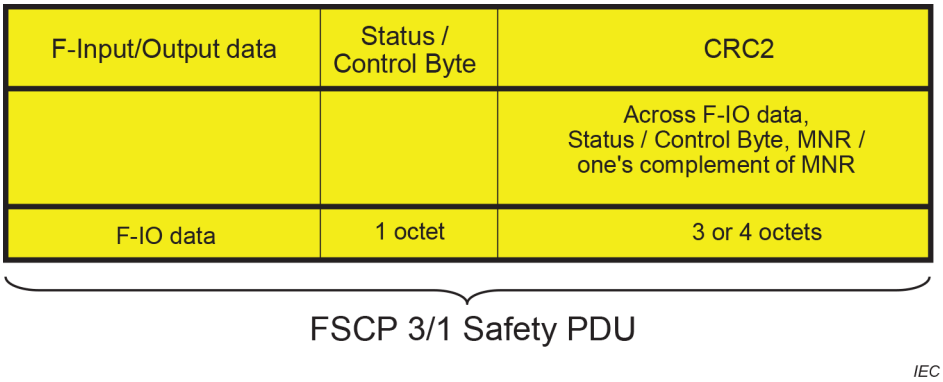


Figure 16 – Safety PDU for CPF 3

A Safety PDU contains F-IO data, the Status/Control Byte and 3 or 4 octets for the CRC2 code.

Subclauses 7.1.2 through 7.1.9 provide a detailed description of the elements of the safety PDU structure.

7.1.2 Safety IO data

The F-IO data of the F-IO peripherals are accommodated in this safety PDU section. The data type coding corresponds to the one of CP 3/4 to CP 3/6 and is defined system wide within IEC 61158-5-10. Subclause 8.5.2 recommends and specifies standardized data types and data structures for several families of safety devices such as remote IO, light curtains, laser scanners, drives, etc.

Besides the compact devices, there are *modular devices* with F and standard IO units and subaddresses (Figure 11). Their CP 3/4 to CP 3/6 head station (DAP), which is considered to be a part of the black channel, is used for agreeing the structure of a CP 3/4 to CP 3/6 message with several safety PDUs via the start-up parameterization. One safety PDU corresponds to one Submodule.

7.1.3 Status and Control Byte

Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
Res ("0")	Monitoring Number has been reset	Toggle Bit	Fail-safe values (FV) activated	Communi-cation fault: WD-timeout	Communi-cation fault: CRC	Fault in F-(Sub)Module or F-(Sub)Module channel fault cleared	F-(Sub)Module acknowledges iParameter assignment
-	cons_nr_R	Toggle_d	FV_activated	WD_timeout	CE_CRC	Device_Fault/ ChF_Ack_Req	iPar_OK

Figure 17 – Status Byte

The Status Byte shown in Figure 17 is contained in each safety PDU of a (Sub)Module transmitted from a device to its controller (Figure 16).

Bit 0 is set when the F-(Sub)Module acknowledges a Parameterization in Run. Signal name is "iPar_OK", see "Amd 1 PiR" [64].

Bit 1 at F_Passivation = 0 shall be set by the specific device technology firmware for at least two (2) changes of the MonitoringNumber, as long as an F-(Sub)Module is not able to guarantee the safety integrity of the process data to be transmitted. Signal name in this implementation case is "Device_Fault".

Bit 1 at F_Passivation = 1 shall be set by the specific device technology firmware if at least one of the channels of an F-(Sub)Module had been set to Fail-safe Values (FV) due to a signal channel fault and this fault is eliminated (cleared). Duration constraints for this signal are not necessary. A failure within the F-(Sub)Module (not within a single channel) shall cause each and every channel to switch to the fail-safe state and all qualifiers to bad. Signal name in this implementation case is "ChF_Ack_Req". See [56].

Bit 2 is set if the F-Device driver is recognizing an F communication fault, i.e. if the Monitoring-Number is incorrect (detected via CRC2 error) or the data integrity is violated (CRC error). This bit information enables the F-Host to count all erroneous messages within a defined time period T and to trigger a configured safe state of the system if the number exceeds a certain limit (maximum residual error rate). Signal name is "CE_CRC". See also 9.5.1.

Bit 3 is set if the F-Device driver is recognizing an F communication fault, i.e. if the watch dog time in the F-Device driver is exceeded. Signal name is "WD_timeout".

Bit 4 is set by the FSCP 3/1 protocol layer during start-up and in cases of any communication fault (Figure 15 and 7.2). In addition the F part of the specific device application can set this bit also. Signal name is "FV_activated".

Bit 5 is an F-Device driver based Toggle Bit indicating a trigger to change the virtual MonitoringNumber within the F-Host. Signal name is "Toggle_d".

Bit 6 is set when the F-Device driver has to reset its MNR. Signal name is "cons_nr_R" (from "consecutive number reset").

Bit 7 is reserved (res) for future FSCP 3/1 releases and thus, by default it shall be set to "0" to guarantee a defined state for future use and for the "Loop-back check" (see 3.3).

Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
Reserved or Loop-back check ("1")	Operator acknowledge after cleared channel fault	Toggle Bit	Fail-safe values (FV) to be activated	Use F_WD_Time_2 (secondary watchdog)	Reset Monitoring Number	Operator acknowledge requested (indication)	iParameter assignment enabled
Loopcheck	ChF_Ack	Toggle_h	activate_FV	Use_TO2	R_cons_nr	OA_Req	iPar_EN

Figure 18 – Control Byte

The Control Byte shown in Figure 18 is being sent with each safety PDU for a (Sub)Module from the IO-Controller to the device (Figure 16).

Bit 0 is set by the F application within an F-Host in case of a Parameterization in Run request. Signal name is "iPar_EN", see "Amd 1 PiR" [64].

Bit 1 is set by the F-Host driver corresponding to the variable "OA_Req_S". This signal is not safety related and should be used by the F-(Sub)Module to indicate locally the request for an operator acknowledgment (OA_C) usually *via a LED* (9.1). Signal name is "OA_Req".

Bit 2 is set when the F-Host detects a communication error, either by the Status Byte or by itself. As a consequence, the virtual MonitoringNumber within the F-Device driver will be reset (see "RESETxD" in 7.1.5 and 7.1.6). Bit 2 shall be reset again after an error has gone. The MNR then resumes. Signal name is "R_cons_nr" (from "Reset consecutive number").

Bit 3 is set when the F-Host driver gets informed via vendor specific internal input that an intended update process of the safety fieldbus components in case of "Dynamic Reconfiguration" or "maintenance of a fault tolerant system" is taking place. This informs the F-(Sub)Module to extend the watchdog time F_WD_Time once only by F_WD_Time_2 (see 6.1). Signal name is "Use_TO2".

Bit 4 can be set to force the outputs of an F-(Sub)Module to configured or built-in fail-safe values. See 6.1 for more details. Signal name is "activate_FV".

Bit 5 is the F-Host driver based Toggle Bit indicating a trigger to change the virtual MonitoringNumber within the F-Device driver. See 7.1.4 for more details. Signal name is "Toggle_h".

Bit 6 is set by the F application within an F-Host application program after clearance of at least one signal channel fault within an F-(Sub)Module indicated by Bit 1 (ChF_Ack_Req) of the Status Byte and personal has left the protection area. PV are activated. See [56]. Signal name is "ChF_Ack".

Bit 7 at F_CRC_Seed =0: is set to "1" for all F-(Sub)Modules with implementations according to FSCP 3/1 versions prior to this release (F_CRC_Seed =0). Since these F-(Sub)Modules will always return Status Bytes with Bit 7 = "0" a potential loop-back of messages can be detected by the F-Host driver if this Bit 7 returns "1". Signal name is "Loopcheck".

Bit 7 at F_CRC_Seed =1: is set to "0" for all F-(Sub)Modules with a GSD entry F_CRC_Seed =1 and reserved for future use.

7.1.4 (Virtual) MonitoringNumber

The recipient uses the MonitoringNumber (MNR) to monitor whether the sender of the SPDU and the communication channel are still alive. The MNR is used in an acknowledgment mechanism for monitoring the *propagation times* between sender and recipient.

FSCP 3/1 is not transmitting the MNR with each and every safety PDU. It uses a virtual MNR instead. It is called virtual due to the fact that it cannot be seen within the safety PDU. This approach uses MonitoringNumbers located within the F-Host driver and the F-Device driver and a Toggle Bit within the Status Byte and the Control Byte to change the appropriate MNR synchronously (Figure 19).

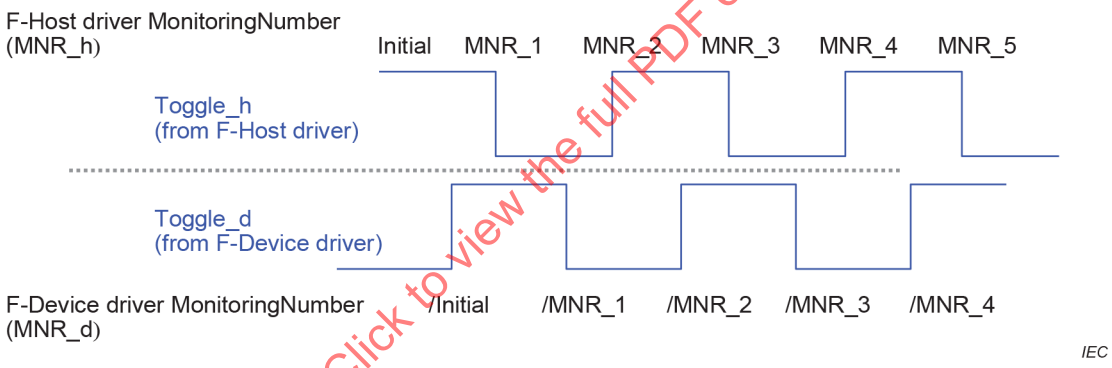


Figure 19 – The Toggle Bit function

The checking for correctness and for the synchronism of the two independent MNR is performed by including the MonitoringNumbers in the CRC2 calculation. CRC2 then is transmitted with each and every safety PDU (Figure 20).

The transmitted part of the (virtual) MonitoringNumber is reduced to a Toggle Bit, which indicates a change of the local MNR. The MNRs within F-Host driver and F-Device driver are changed at each edge of the Toggle-Bits (0→1, 1→0).

Figure 20 illustrates the mechanism for the MNR within the F-Device driver. The MNR is reset when the F-Host sends R_cons_nr = "1" within the Control Byte (see 7.1.3).

The mechanism for the MNR within the F-Host driver corresponds to the one in the F-Device driver. However, the MNR is reset whenever a fault occurs (internally or via Status Byte).

The name of this mechanism is "MNR" even though two different procedures selected by the F_CRC_Seed parameter are possible.

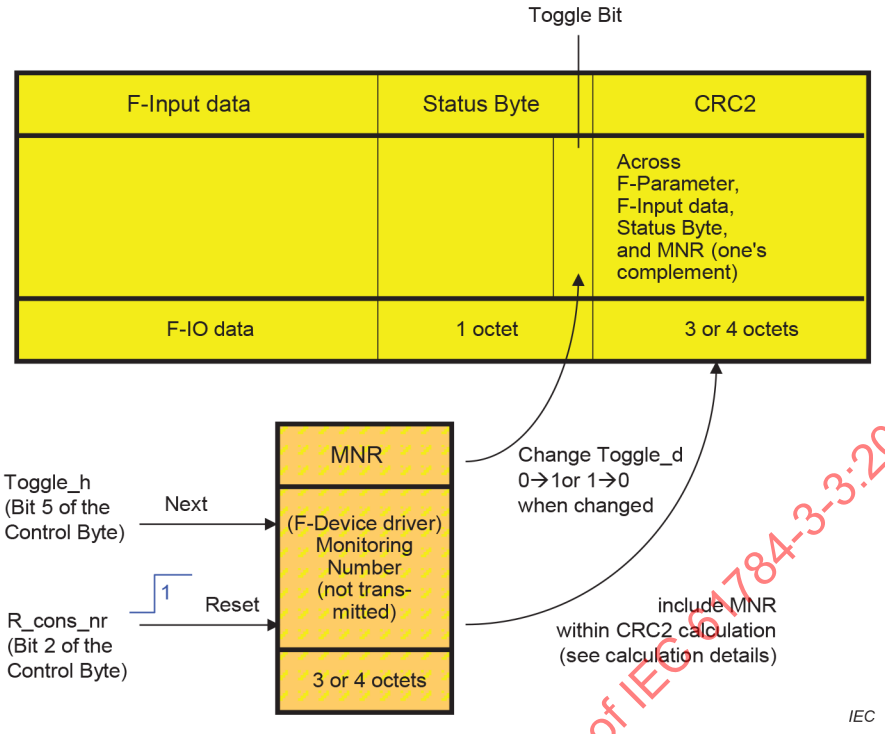


Figure 20 – MonitoringNumber integration

7.1.5 (Virtual) MNR mechanism (F_CRC_Seed=0)

FSCP 3/1 uses *24 bit counters* for the MonitoringNumber in this case. Thus, the Monitoring-Number counts in a cyclic mode from 1 to 0xFFFFFF, wrapping over back to 1 at the end (see Table 6 and Table 7). The counter value is represented by MNR.

Table 6 – MonitoringNumber of an F-Host driver SPDU

MACRO	ACTION (Pseudocode)
INITIALxH	old_MNR = 0xFFFFF0; MNR=0xFFFFF0;
RESETxH	R_cons_nr =1; MNR=0;
RUNxH	R_cons_nr =0; old_MNR = MNR; **if** MNR=0xFFFFFF **then** MNR=1 **else** MNR= MNR +1;

Table 7 – MonitoringNumber of an F-Device driver SPDU

MACRO	ACTION (Pseudocode)
INITIALxD	MNR=0xFFFFF0;
RESETxD	cons_nr_R =1; MNR=0;
RUNxD	cons_nr_R =0; **if** MNR=0xFFFFFF **then** MNR=1 **else** MNR= MNR +1;

7.1.6 (Virtual) MNR mechanism (F_CRC_Seed=1)

FSCP 3/1 provides an extended procedure that is activated if the GSD entry "F_CRC_Seed" =1 (see 8.1.5.2). It allows for the compatibility to IEC 61784-3:2021 Annex G, especially to the fault model of implicit transmission.

This procedure splits the use of MonitoringNumber into two phases. The first phase is characterized as system start (INITIALx) or in case of fault and as long as Bit 2 (R_cons_nr) in the Control Byte is set to "1" (RESETx). The second phase is characterized as cyclic communication. "CRC_FP+" is the 32 bit CRC signature (*0xF4ACFB13*) which includes the same F-Parameters as "CRC_FP" (see Table 8, Table 9, and 8.3.3.2).

Table 8 – MonitoringNumber of an F-Host driver SPDU

MACRO	ACTION (Pseudocode)
INITIALxH	old_MNR = CRC_FP+; MNR=CRC_FP+; CRC2 = CRC2 (calculated according 7.1.8) XOR Modifier; CN_incrNR_64 [1] = 0x5851F42D4C957F2D × Codename; SwapHL = shl (CN_incrNR_64 [1], 32) + shr (CN_incrNR_64 [1], 32); CN_incrNR_64 [2] = 0xAB16D2792302FE5A × (SwapHL + Modifier) +1;
RESETxH	R_cons_nr =1; MNR=CRC_FP+; CRC2 = CRC2 (calculated according 7.1.8) XOR Modifier; CN_incrNR_64 [1] = 0x5851F42D4C957F2D × Codename SwapHL = shl (CN_incrNR_64 [1], 32) + shr (CN_incrNR_64 [1], 32); CN_incrNR_64 [2] = 0xAB16D2792302FE5A × (SwapHL + Modifier) +1;
RUNxH	R_cons_nr =0; old_MNR = MNR; CN_incrNR_64 [0] = CN_incrNR_64 [1] + CN_incrNR_64 [2]; CN_incrNR_64 [2] = CN_incrNR_64 [1]; CN_incrNR_64 [1] = CN_incrNR_64 [0]; MNR= Most significant 32 Bit of CN_incrNR_64 [0];

Table 9 – MonitoringNumber of an F-Device driver SPDU

MACRO	ACTION (Pseudocode)
INITIALxD	MNR= one's complement of CRC_FP+; Modifier = received CRC2 XOR calculated CRC2 according 7.1.8; INI_SPDU=1; CN_incrNR_64 [1] = 0x5851F42D4C957F2D × Codename; SwapHL = shl (CN_incrNR_64 [1], 32) + shr (CN_incrNR_64 [1], 32); CN_incrNR_64 [2] = 0xAB16D2792302FE5A × (SwapHL + Modifier) +1
RESETxD	cons_nr_R =1; MNR= one's complement of CRC_FP+; Modifier = received CRC2 XOR calculated CRC2 according 7.1.8; CN_incrNR_64 [1] = 0x5851F42D4C957F2D × Codename; SwapHL = shl (CN_incrNR_64 [1], 32) + shr (CN_incrNR_64 [1], 32); CN_incrNR_64 [2] = 0xAB16D2792302FE5A × (SwapHL + Modifier) +1;

RUNxD	cons_nr_R =0;
	old_MNR = MNR;
	CN_incrNR_64 [0] = CN_incrNR_64 [1] + CN_incrNR_64 [2];
	CN_incrNR_64 [2] = CN_incrNR_64 [1];
	CN_incrNR_64 [1] = CN_incrNR_64 [0];
	MNR= "one's complement" of 32 most significant bit of CN_incrNR_64 [0];

The instruction shl (x,n) is a logical n bit left shift of the value x, the instruction shr (x,n) is a logical n bit right shift of the value x.

CN_incrNR_64 [0], CN_incrNR_64 [1], CN_incrNR_64 [2], and SwapHL are Unsigned64 variables. CRC_FP+, CRC2, and Modifier are Unsigned32 variables.

Modifier is an F-Host generated value for future use, which determines a new initialization. When the F-Device driver macros INITIALxD and/or RESETxD are executed multiple times, they cannot be expected to contain the same value. However, within this release, the value "0" is always used within the F-Host-macros INITIALxH and RESETxH.

An example of the first 5 values of the MonitoringNumbers is shown in Table A.4. The MonitoringNumber is an Unsigned32 value. The "one's complement" is used to differentiate between safety PDUs from the F-Host driver and safety PDUs from the F-Device driver in order to detect a Loop-back error.

For Codename, see 8.1.2.

7.1.7 CRC2 Signature (F_CRC_Seed=0)

In case of F_CRC_Seed = 0, the following applies: Once the F-Parameters (source-destination relationship or Codename, SIL, watchdog times, etc.) have been transferred to the F-Device driver, the identical parameters are employed in an identical procedure in the F-Host and in the F-(Sub)Module for producing a CRC_FP signature as a seed value for the calculation of CRC2 that is transferred cyclically. For information on how this CRC_FP is built, see 8.3.3.2. This CRC_FP signature, the F-IO data, the Status or Control Byte and the corresponding MNR are used for generating another 3 octet CRC2 signature within the F-Host (see Figure 21).

In the F-Device driver, the identical CRC2 signature is generated and the signatures are compared. The subsequent cyclic transfers require only a CRC2 signature comparison.

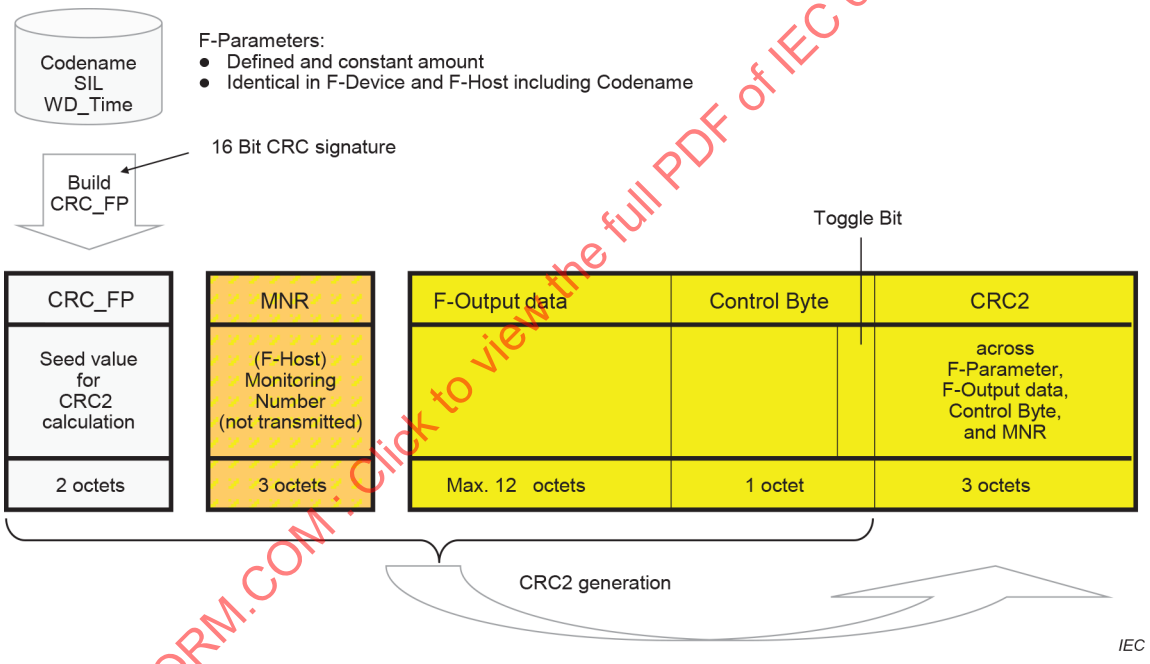


Figure 21 – F-Host driver CRC2 signature generation (F_CRC_Seed=0)

For better error detection even if there are identical CRC polynomials within the black channel and in the safety layer, the CRC2 signature calculation includes the octets of Figure 21 in reverse order (see Figure 22).

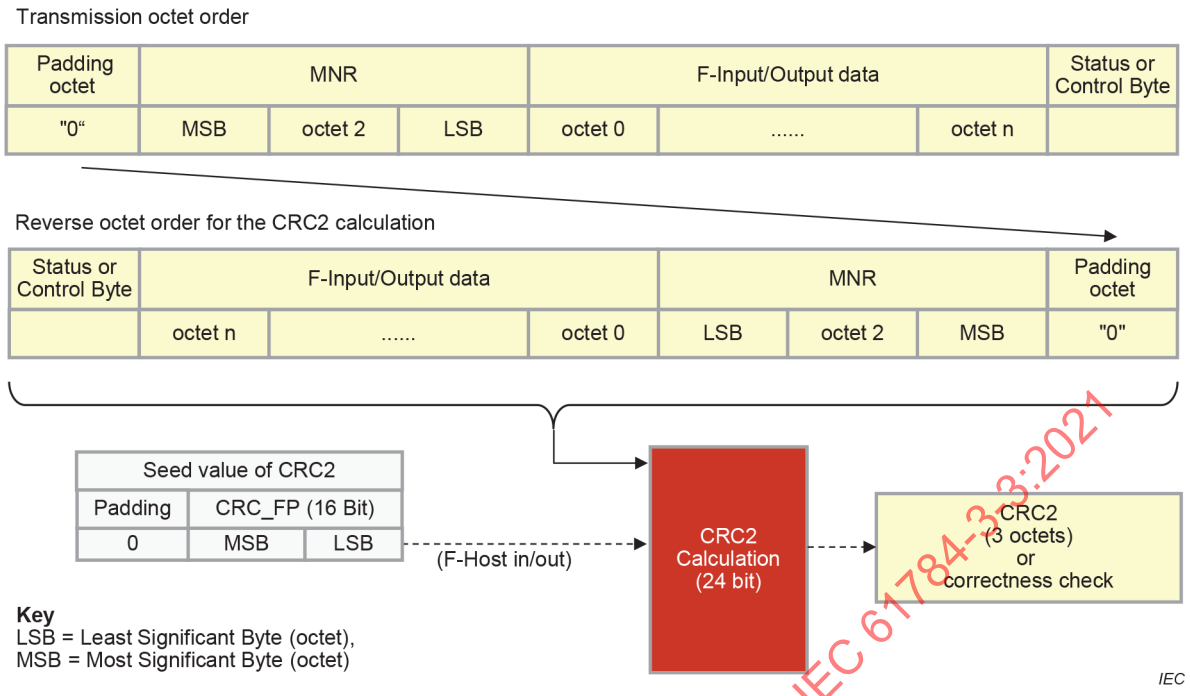


Figure 22 – Details of the CRC2 signature calculation (F_CRC_Seed=0)

The generator polynomial *0x5D6DCB* shall be used for the 24 bit CRC2 signature. In order to prevent a safety PDU from carrying "0" only, an exception is made in this particular case: CRC2 will be set "1" instead of "0" (see 3.3).

7.1.8 CRC2 Signature (F_CRC_Seed=1)

In case of F_CRC_Seed = 1, the first value of MNR is the CRC_FP+ of the F-Parameter, the following MNRs are a sequence based on the Codename.

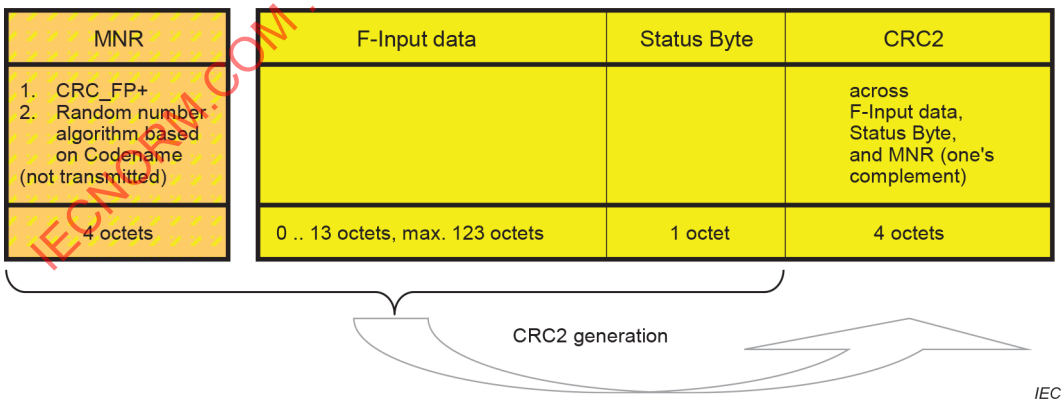


Figure 23 – CRC2 signature calculation (F_CRC_Seed=1)

The CRC2 signature calculation includes the octets in reverse order (see Figure 24).

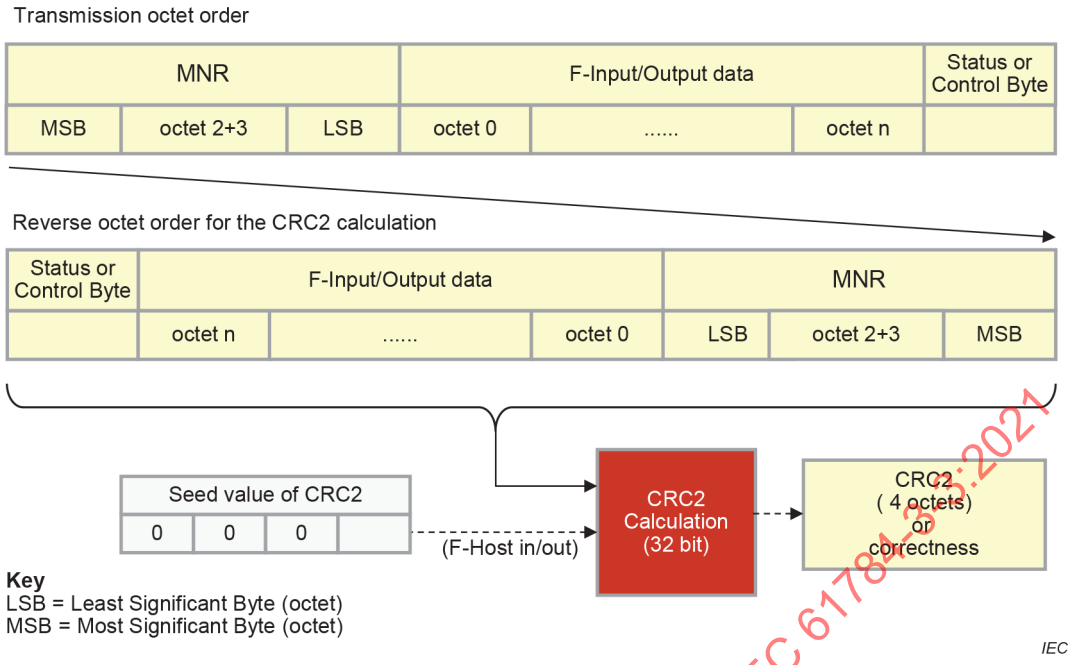


Figure 24 – Details of the CRC2 signature calculation (F_CRC_Seed=1)

The F-Host driver uses the same CRC2 signature calculation procedure in Figure 24 to check the correctness of the F-Device driver safety PDU including the Status Byte, F-Input data, and the one's complement of the MNR.

The generator polynomial *0xF4ACFB13* shall be used for the 32 bit CRC2 signature. In order to prevent a safety PDU from carrying "0" only, an exception is made in this particular case: CRC2 will be set "1" instead of "0" (see 3.3).

7.1.9 Non-safety IO data

Non-safety IO data cannot be appended to a safety PDU. If an F-Submodule needs or generates CP 3/4 to CP 3/6 data it is able to use the mechanism of Submodule modeling.

7.2 FSCP 3/1 behavior

7.2.1 General

The core of the safety layers within F-Host is the F-Host driver and in the F-(Sub)Module is the F-Device driver. This driver consists each of a finite state machine. Its modes of operation are defined by means of the state diagrams and sequence diagrams in 7.2.2 and 7.2.3. Figure 25 shows a simplified model of the safety communication. A special timing diagram in 7.2.6 is illustrating the consequences of a fault on the reset signal for the MNR. The monitoring of safety PDU transit times is described in 7.2.7.

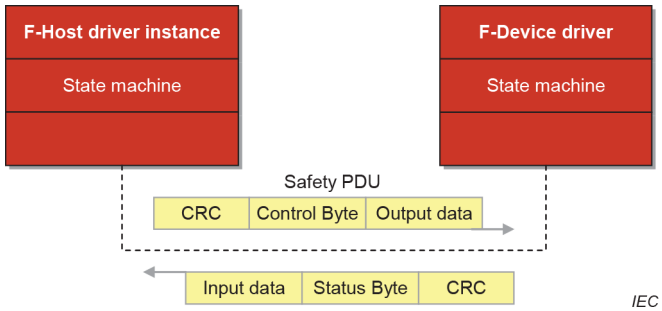


Figure 25 – Safety layer communication relationship

7.2.2 F-Host driver state diagram

Figure 26 shows the F-Host state diagram and Table 11 describes the F-Host states, transitions, and internal items. The diagrams are following the UML2 notation.

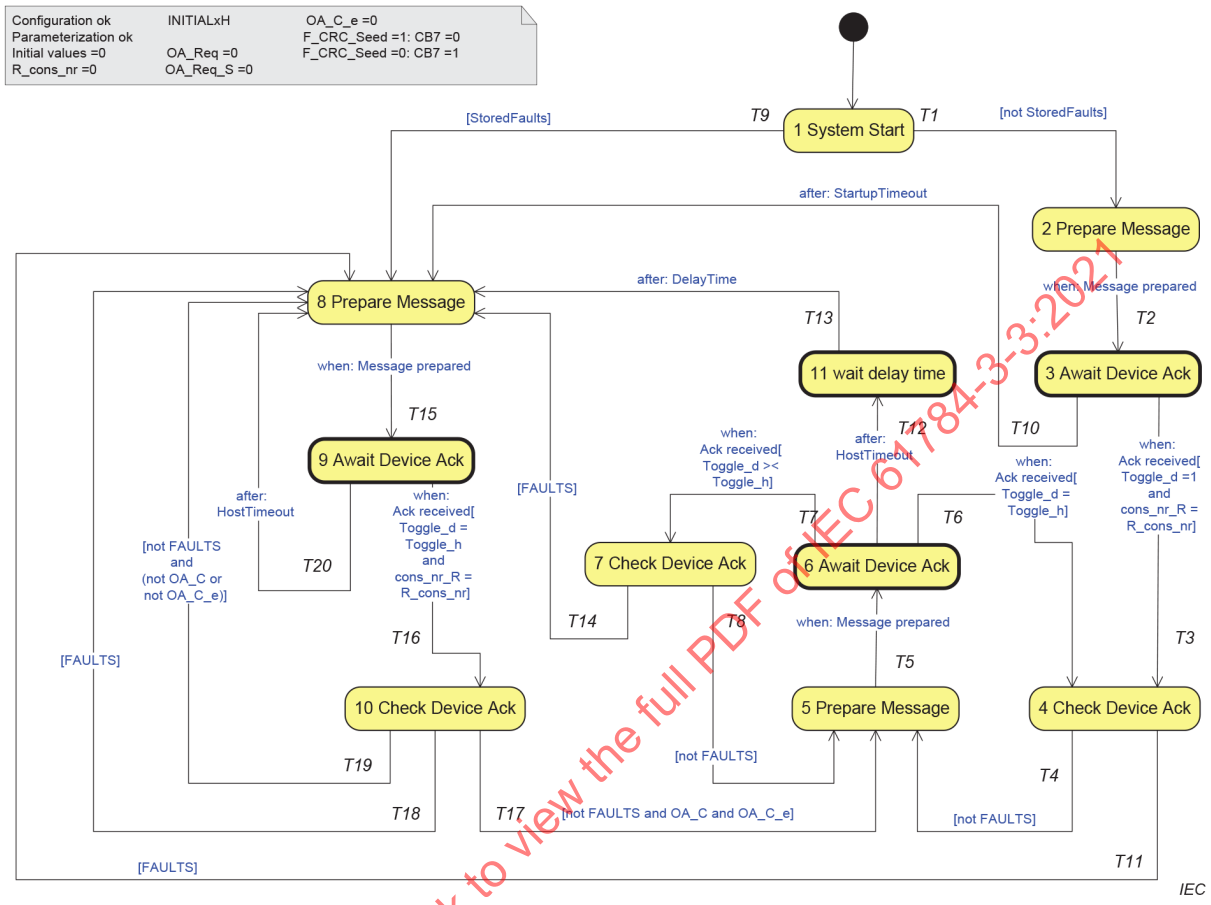


Figure 26 – F-Host driver state diagram

The terms used in Figure 26 are specified in Table 10.

Table 10 – Definition of terms used in F-Host driver state diagram

Term	Definition
Initial values	Any safety PDU values =0
StartupTimeout	F-Host vendor specific Timeout. Value between F_WD_Time and infinite.
HostTimeout	F-Host driver recognizes local timeout while awaiting an F-Device driver acknowledgment within F_WD_Time. This HostTimeout shall be extended once only by F_WD_Time_2 in case of "use_TO2" = 1 (F_WD_Time + F_WD_Time_2), similar to the F-Device driver (see 6.1, 8.1.4).
Host_CE_CRC	F-Host driver recognizes CRC fault while analyzing the received safety PDU
Device_Fault	F_Passivation =0 (see 8.1.6.2): F-(Sub)Module reported internal fault via F-Device driver to F-Host driver; Status Bit 1 =1.
CE_CRC	F-Device driver reported CRC fault to the F-Host driver; Status Bit 2 =1
OA_C_e	Auxiliary flag indicating a raising edge of the OA_C signal (0 → 1)
WD_timeout	F-Device driver reported timeout fault to the F-Host driver; Status Bit 3 =1
INITIALxH	Macro see 7.1.5 and 7.1.6
FAULTS	This variable is true (=1) if one of the following bit is set: - SB2 (CE_CRC) - SB3 (WD_timeout) - SB7 (Status Byte, Bit7), if F_CRC_Seed =0 - Host_CE_CRC

Term	Definition
StoredFaults	This variable is true (=1) if any of the FAULTS bit and/or HostTimeout had been stored at shut down
Ack received	Any new safety PDU received; ignore safety PDU with all values =0

The transitions are fired in case of an event for example receiving a message. In case of several possible transitions so-called guards [conditions] are defining which transition to fire.

The states 4, 7, and 10 (Check Device Ack) are so-called change states according to UML2 without an "external" event. The corresponding transitions are fired after an evaluation of internal values.

The diagram consists of activity and action states. Activity states are surrounded by bold lines, action states by thin lines. While activity states may be interruptable by new events, action states are not. Events within an action state such as timeouts, messages received, or operator acknowledgments are deferred until the next activity state is reached.

Table 11 – F-Host driver states and transitions

STATE NAME	STATE DESCRIPTION
1 System Start	Initial state of the F-Host driver instance upon power-on. If a system is designed to store faults, transition T9 shall be implemented. Otherwise the system is using transition T1 only.
2 Prepare Message	Preparation of a regular safety PDU for the F-Device driver
3 Await Device Ack	Safety Layer is waiting on next regular safety PDU from F-Device driver (Acknowledgment).
4 Check Device Ack	Check received safety PDU for a CRC2-error (Host_CE_CRC) including MNR and for potential F-Device driver detected faults within the Status Byte (WD_timeout, CE_CRC)
5 Prepare Message	Preparation of a regular safety PDU for the F-Device driver
6 Await Device Ack	Safety Layer is waiting on next regular safety PDU from F-Device driver (Acknowledgment)
7 Check Device Ack	Check received safety PDU for a CRC-error (Host_CE_CRC) including previous MNR (old_MNR) and for potential F-Device driver detected faults within the Status Byte (WD_timeout, CE_CRC)
8 Prepare Message	Preparation of a safety PDU for the F-Device driver (exception handling)
9 Await Device Ack	Safety Layer is waiting on next safety PDU from F-Device driver (Acknowledgment)
10 Check Device Ack	Check received safety PDU for a CRC2-error (Host_CE_CRC) including MNR and for potential F-Device driver detected faults within the Status Byte (WD_timeout, CE_CRC). Once a fault occurred, no automatic restart of a safety function is permitted unless an operator acknowledgment signal (OA_C) arrived.
11 wait delay time	This state to avoid the storage of a timeout fault in case of an occasional system shut-down which would cause a request for an operator acknowledge with the next power-on. A delay time of 0 ms is permitted.

TRAN-SITION	SOURCE STATE	TARGET STATE	ACTION
T1	1	2	use FV, activate_FV =1, FV_activated_S =1 Toggle_h =1
T2	2	3	send safety PDU
T3	3	4	(re)start host-timer
T4	4	5	RUNxH Toggle_h = not Toggle_h, **if** FV_activated =1 or activate_FV_C =1 or Device_Fault [b] =1 **then** use FVi, FV_activated_S =1 **else** use PVi, FV_activated_S =0 **if** activate_FV_C =1 or Device_Fault [b] =1 **then** use FVo, activate_FV =1

TRAN-SITION	SOURCE STATE	TARGET STATE	ACTION
			else use PVo, activate_FV =0 iPar_OK_S =iPar_OK
T5	5	6	send safety PDU
T6	6	4	restart host-timer
T7	6	7	-
T8	7	5	**if** FV_activated =1 or activate_FV_C =1 or Device_Fault [b] =1 **then** use FVi, FV_activated_S =1 **else** use PVi, FV_activated_S =0 **if** activate_FV_C =1 or Device_Fault [b] =1 **then** use FVo, activate_FV =1 **else** use PVo, activate_FV =0 iPar_OK_S =iPar_OK
T9 [a]	1	8	use FV, activate_FV =1, FV_activated_S =1, Toggle_h =1, RESETxH
T10	3	8	restart host-timer, store faults, use FV, activate_FV =1, FV_activated_S =1, Toggle_h = not Toggle_h, RESETxH
T11 [c]	4	8	store faults, use FV, activate_FV =1, FV_activated_S =1, Toggle_h = not Toggle_h, RESETxH
T12 [d]	6	11	use FV, activate_FV =1, FV_activated_S =1, RESETxH
T13	11	8	store faults, Toggle_h = not Toggle_h, restart host-timer
T14 [c]	7	8	restart host-timer, store faults, use FV, activate_FV =1, FV_activated_S =1, Toggle_h = not Toggle_h, RESETxH
T15	8	9	send safety PDU
T16	9	10	restart host-timer
T17	10	5	reset stored faults, OA_Req_S =0, OA_Req =0, OA_C_e =0, Toggle_h = not Toggle_h, RUNxH **if** FV_activated =1 or activate_FV_C =1 or Device_Fault [b] =1 **then** use FVi, FV_activated_S =1 **else** use PVi, FV_activated_S =0 **if** activate_FV_C =1 or Device_Fault [b] =1 **then** use FVo, activate_FV =1 **else** use PVo, activate_FV =0 iPar_OK_S =iPar_OK
T18	10	8	store faults, OA_Req =0, OA_Req_S =0, OA_C_e =0, use FV, activate_FV =1, FV_activated_S =1, Toggle_h = not Toggle_h, RESETxH
T19	10	8	OA_Req_S =1, OA_Req =1, if OA_C =0 then OA_C_e =1 use FV, activate_FV =1, FV_activated_S =1, Toggle_h = not Toggle_h, RUNxH

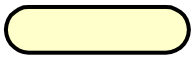
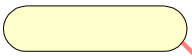
TRAN-SITION	SOURCE STATE	TARGET STATE	ACTION
T20	9	8	store faults, OA_Req =0, OA_Req_S =0, OA_C_e =0, use FV, activate_FV =1, FV_activated_S =1, Toggle_h = not Toggle_h, RESETxH restart host-timer

[a] See STATE DESCRIPTION of STATE 1. The statement "store faults" within the transitions can be omitted if T9 is not implemented.

[b] Device_Fault is not considered in the logic operation if F_Passivation =1.

[c] Transition T11 and T14 produce an diagnosis message "Host Diagnosis transmission errors (CRC)".

[d] Transition T12 produce a diagnosis message "Host Diagnosis transmission errors (Timeout)".

INTERNAL ITEMS	TYPE	DEFINITION
RESETxH	Macro	See 7.1.5 and 7.1.6
RUNxH	Macro	See 7.1.5 and 7.1.6
MNR	Variable	MNR is representing the local MonitoringNumber within the F-Host driver instance. It is not transmitted to its counterpart within the F-Device driver, but is synchronizing those via a Toggle Bit in the Control Byte. The actual MNR is incorporated in the CRC2 calculation and thus checked against transmission faults.
old_MNR	Variable	Previous value of the current local MNR. It is necessary to store this previous value of the MNR.
DelayTime	Timer	This delay time is to cover power off settling time within the whole system. It is within the host/system manufacturer's responsibility to define this parameter.
host-timer	Timer	This timer checks whether the next valid safety PDU from the F-Device driver did arrive in time. The host engineering tool is responsible to define this watchdog time. Value range is 0 to 65 535 ms.
OA_C_e	Flag	By means of this auxiliary variable (bit) it is ensured that the safe state will be left only after a signal change of OA_C from 0 → 1 (edge). Without this mechanism an operator could overrule safe states by permanently actuating the OA_C signal.
faults	Flags	Until an operator acknowledgment (OA_C), persistent storage of the FAULT bit (see Table 10) is required within the F-Host only (no F-(Sub)Module persistence).
	Activity State	Within these interruptable "activity" states the host waits for new inputs such as timeout or acknowledgment [29].
	Action State	Within these non-interruptable "action" states events like timeout, message received or operator acknowledgment are deferred until the next "activity" state [29].

7.2.3 F-Device driver state diagram

Figure 27 shows the F-Device driver state diagram and Table 13 describes the states, transitions, and internal items. The diagrams are following the UML2 notation.

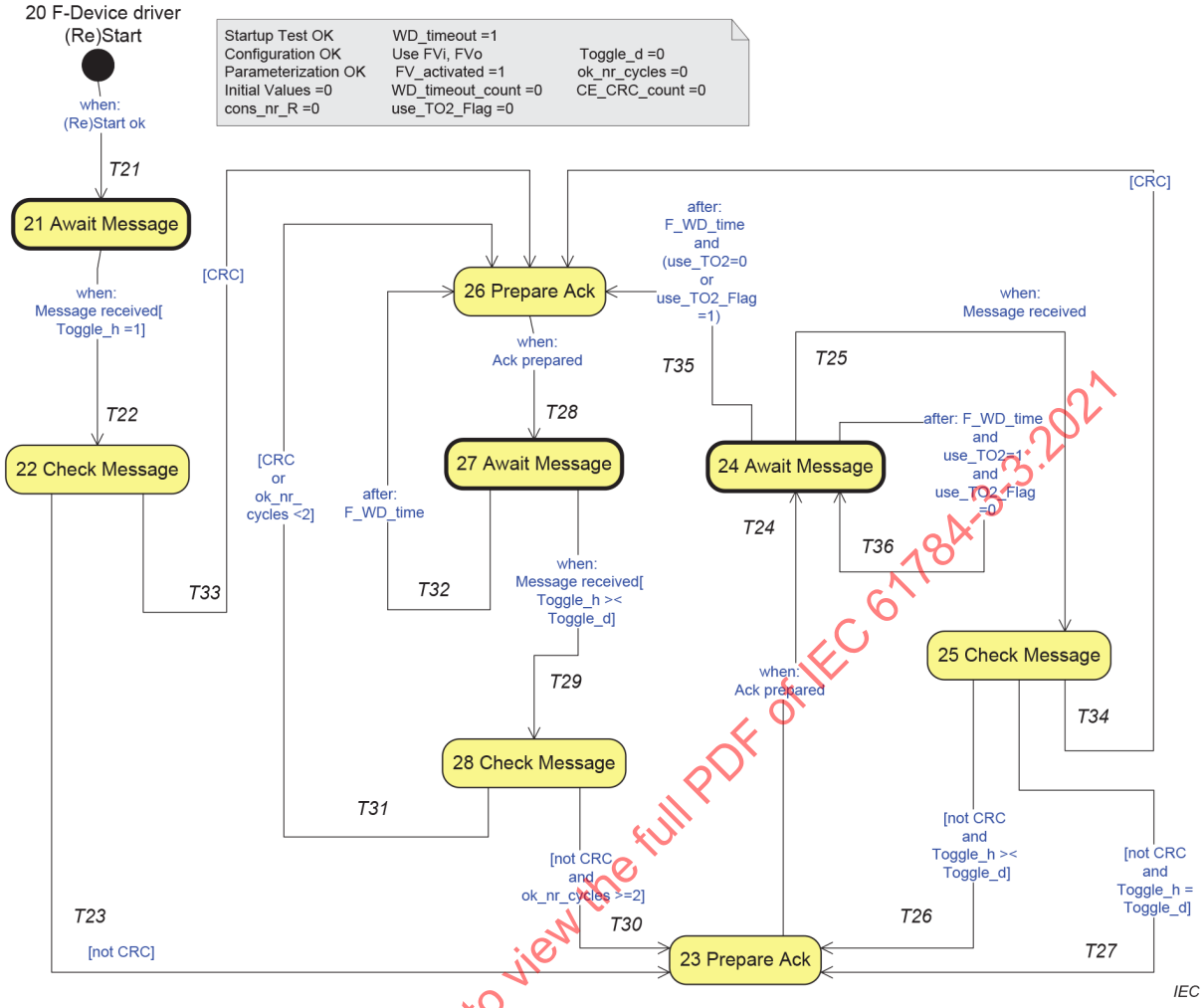


Figure 27 – F-Device driver state diagram

The terms used in Figure 27 are specified in Table 12.

Table 12 – Definition of terms used in Figure 27

Term	Definition
[Toggle_h = Toggle_d]	UML notation of a condition (guard) to fire the transition. In this case it means: Bit Toggle_h has not changed value ("not toggled")
[Toggle_h >< Toggle_d]	Bit Toggle_h has changed value ("toggled")
[CRC]	F-Device driver recognizes CRC fault (communication and/or MNR error)
F_WD_Time	Watchdog time defined by the F-Parameter "F_WD_Time"
use_TO2	CB3 within the Control Byte indicating usage of the secondary watchdog time F_WD_Time_2
use_TO2_Flag	Auxiliary flag
INI_SPDU	Auxiliary flag used for the first cycle to omit the CRC2 check
Ack	Acknowledgment safety PDU of the F-Device driver
Message received	Any new safety PDU received; ignore safety PDU with all values =0
INITIALxD	Macro see 7.1.5 and 7.1.6

Table 13 – F-Device driver states and transitions

STATE NAME	STATE DESCRIPTION
20 F-Device driver (Re)Start	Initial state of the F- (Sub)Module. Initial values of the input F-(Sub)Module are "0". Immediately after F-Parameterization F-Device shall set output fail-safe values.
21 Await Message	Safety Layer is waiting on next safety PDU from F-Host driver. At State "(Re)Start the F-Devcie shall react on the first valid SPDU from the F-Host driver within PROFIsafe timeout by response with a valid SPDU.
22 Check Message	**If** (F_CRC_Seed =0) **then** Check received safety PDU for CRC2-error **else** no Check (The content of CRC2 is evaluated in T22)
23 Prepare Ack	Preparation of regular safety PDU for the F-Host driver (Acknowledgment)
24 Await Message	Safety Layer is waiting on next regular safety PDU from F-Host driver
25 Check Message	**if** (F_CRC_Seed =0) **then** Check received safety PDU for CRC2-error **else** **if** (R_cons_nr =0) and (INI_SPDU=0) **then** Check received safety PDU for CRC2-error
26 Prepare Ack	Preparation of safety PDU for the F-Host (Acknowledgment with fault bits)
27 Await Message	Safety Layer is waiting on next safety PDU from F-Host (exception handling)
28 Check Message	**if** (R_cons_nr =0) **then** Check received safety PDU for CRC2-error

TRAN-SITION	SOURCE STATE	TARGET STATE	ACTION
T21	20	21	-
T22	21	22	**if** R_cons_nr =1 **then** RESETxD **else** INITIALxD
T23	22	23	use PVi, FVo, FV_activated =1, CE_CRC =0, WD_timeout =0, Toggle_d =Toggle_h, restart device-timer, ok_nr_cycles =ok_nr_cycles +1
T24	23	24	send safety PDU
T25	24	25	**if** Toggle_h >< Toggle_d **then** INI_SPDU=0 **if** R_cons_nr =1 **then** RESETxD **else** RUNxD
T26	25	23	restart device-timer Use PVi, Toggle_d = Toggle_h, if ok_nr_cycles <4 ok_nr_cycles =ok_nr_cycles +1 **if** ok_nr_cycles <4 **then** use FVo, FV_activated =1 **else** use PVo, FV_activated =0 **if** activate_FV =1 **then** use FVo **if** use_TO2 =0 **then** use_TO2_Flag =0

TRAN-SITION	SOURCE STATE	TARGET STATE	ACTION
T27	25	23	Use PVi, Toggle_d = Toggle_h, **if** ok_nr_cycles <4 **then** use FVo, FV_activated =1 **else** use PVo, FV_activated =0 **if** activate_FV =1 **then** use FVo
T28	26	27	Send safety PDU
T29	27	28	INI_SPDU=0 **if** R_cons_nr =1 **then** RESETxD **else** RUNxD
T30	28	23	use PVi, FVo, FV_activated =1, Toggle_d = Toggle_h, restart device-timer, ok_nr_cycles =ok_nr_cycles +1
T31	28	26	Toggle_d = Toggle_h, restart device-timer, **if** CRC **then** CE_CRC =1, CE_CRC_count =1, ok_nr_cycles =0, **else** ok_nr_cycles =ok_nr_cycles +1, **if** CE_CRC_count >0 **then** CE_CRC =1, CE_CRC_count = CE_CRC_count -1, **else** CE_CRC =0, **if** WD_timeout_count >0 **then** WD_timeout=1, WD_timeout_count = WD_timeout_count -1 **else** WD_timeout =0
T32	27	26	Use PVi, FVo, FV_activated =1, WD_timeout =1, WD_timeout_count =1, ok_nr_cycles =0, restart device timer, Toggle_d = Toggle_h
T33	22	26	Use PVi, FVo, FV_activated =1, CE_CRC =1, CE_CRC_count =1, WD_timeout =0, ok_nr_cycles =0, restart device-timer, Toggle_d = Toggle_h
T34	25	26	Use PVi, FVo, FV_activated =1, CE_CRC =1, CE_CRC_count =1, ok_nr_cycles =0, restart device-timer, Toggle_d = Toggle_h
T35	24	26	Use PVi, FVo, FV_activated =1, WD_timeout =1, WD_timeout_count =1, ok_nr_cycles =0, restart device timer, Toggle_d = Toggle_h
T36	24	24	restart device timer with F_WD_Time_2 use_TO2_Flag =1

INTERNAL ITEM	TYPE	DEFINITION
RESETxD	Macro	See 7.1.5 and 7.1.6
RUNxD	Macro	See 7.1.5 and 7.1.6
MNR	Variable	MNR is representing the real local MNR within the F-Device driver. It is not transmitted to its counterpart within the F-Host, but synchronized with those via a Toggle Bit within the Control Byte. That means it changes each time when the Toggle Bit within the Control Byte (Toggle_h) changes its state from 0 → 1 or from 1 → 0.
ok_nr_cycles	Counter	During start-up and after a fault, the F-Device driver shall set FVo and FV_activated =1 for at least 3 cycles. It is the task of this incremental counter to count these cycles from 0 to 3.
CE_CRC_count	Counter	This decremental counter is used to guarantee that the bit "CE_CRC" within the Status Byte is set at least for 1 cycle or for a maximum of 2 cycles. Value range is 0 to 1.
WD_timeout_count	Counter	This decremental counter is used to guarantee the bit "WD_timeout" within the Status Byte is set at least for 1 cycle or for a maximum of 2 cycles. Value range is 0 to 1.
device-timer	Timer	This timer checks whether the next valid safety PDU did arrive in time. The F-Parameter "F_WD_Time" is used to define this watchdog time. Value range is 0 to 65 535 ms.

7.2.4 F-Device driver restart

The following sequence shall initiate a restart of the F-Device driver to state 20 (according to Figure 27):

– Loss of the fieldbus connection (e.g. AR-Release) for at least F_WD_Timeout [a], and then

– Restart of the fieldbus connection (e.g. AR-Connect/ establish AR) and/or transmission of F-Parameters.

[a] The F-Device driver can react on loss of the fieldbus connection immediately or after F_WD_Timeout.

NOTE The check of this sequence and perform the F-Device driver restart is typically executed by the F-(Sub)module Application.

In case of F-Device driver restart to state 20 the F-Device driver shall check the F-Parameter regardless whether they are changed or not.

7.2.5 Sequence diagrams

Figure 28 to Figure 33 show the interaction messages of F-Host driver and F-Device driver during start-up phase. Three phases are covered: both partners during start-up, the F-Host temporarily switches power off or the F-(Sub)Module temporarily has power off while its partner is still operating. The figures are informing about the states and the corresponding transitions. Numbers within circles represent the states the respective F-Host driver and F-Device driver are passing through.

Figure 28 shows the regular start of safety PDU transmissions between F-Host driver and F-Device driver after power on. A possible sequence of MonitoringNumbers is shown in Table A.4.

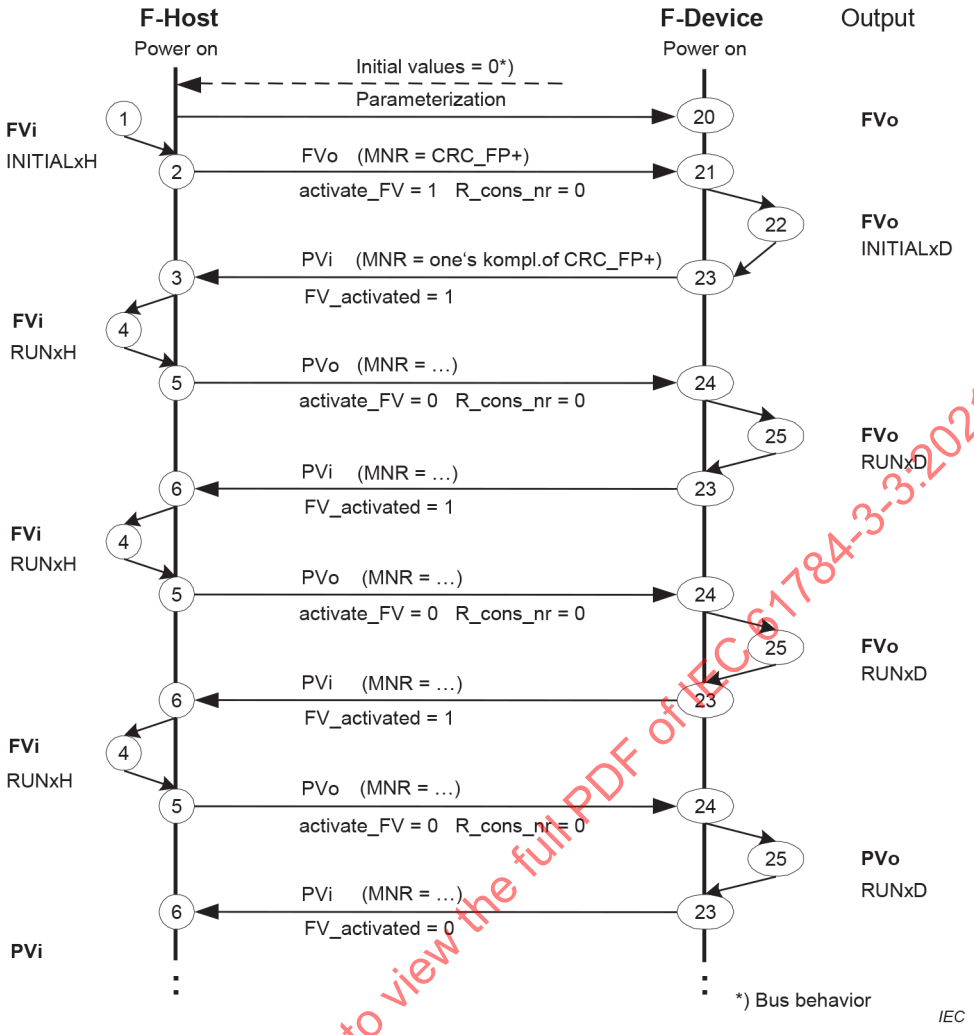


Figure 28 – Interaction F-Host driver / F-Device driver during start-up

Figure 29 shows an example with F-Parameter assignment in case the F-Device driver is already operating and the F-Host is switching from power off to power on.

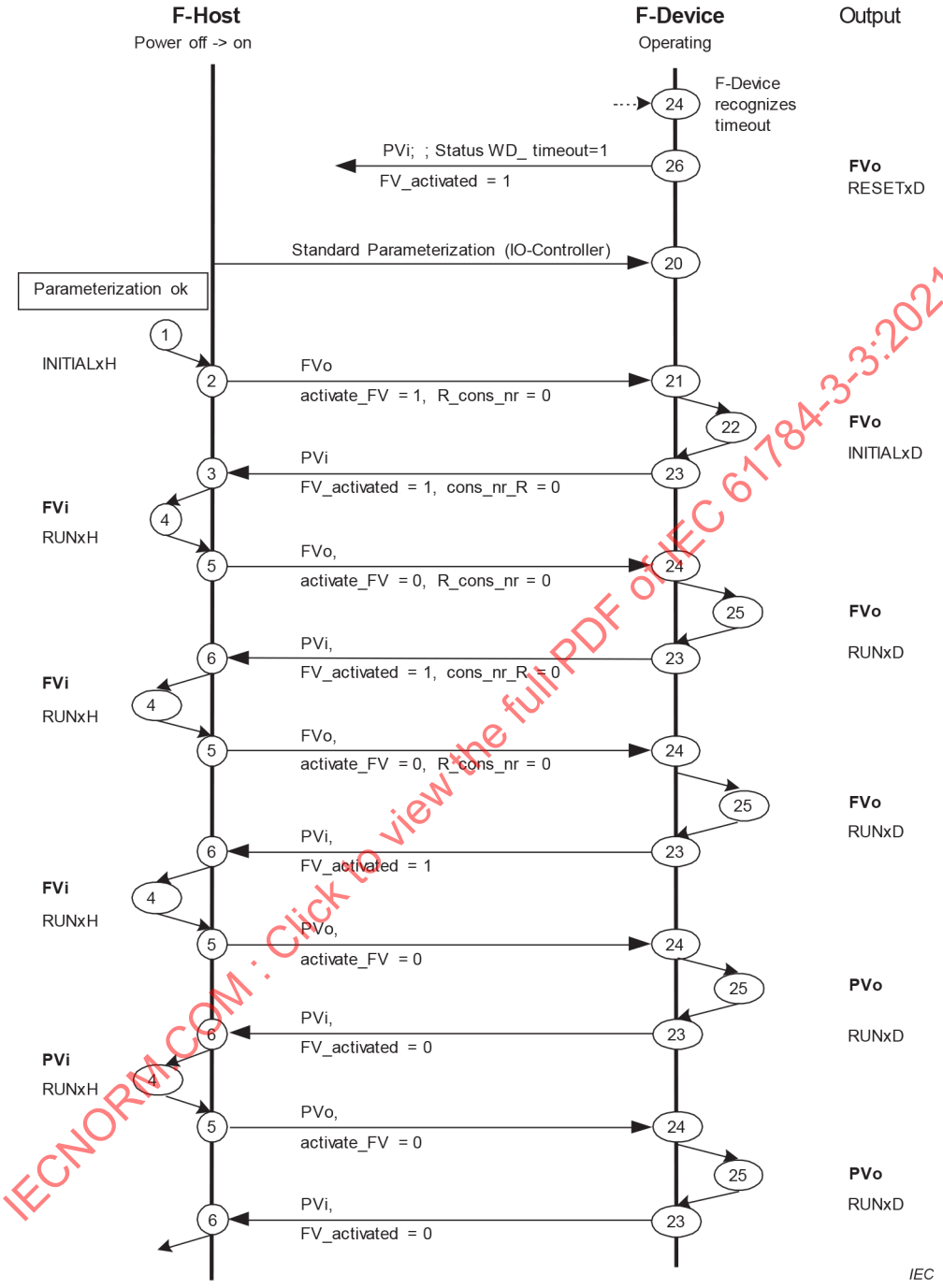


Figure 29 – Interaction F-Host driver / F-Device driver during F-Host power off > on

Figure 30 shows an example with F-Parameter assignment in case the F-Host driver is already operating and the F-(Sub)Module is switching power on after a delay.

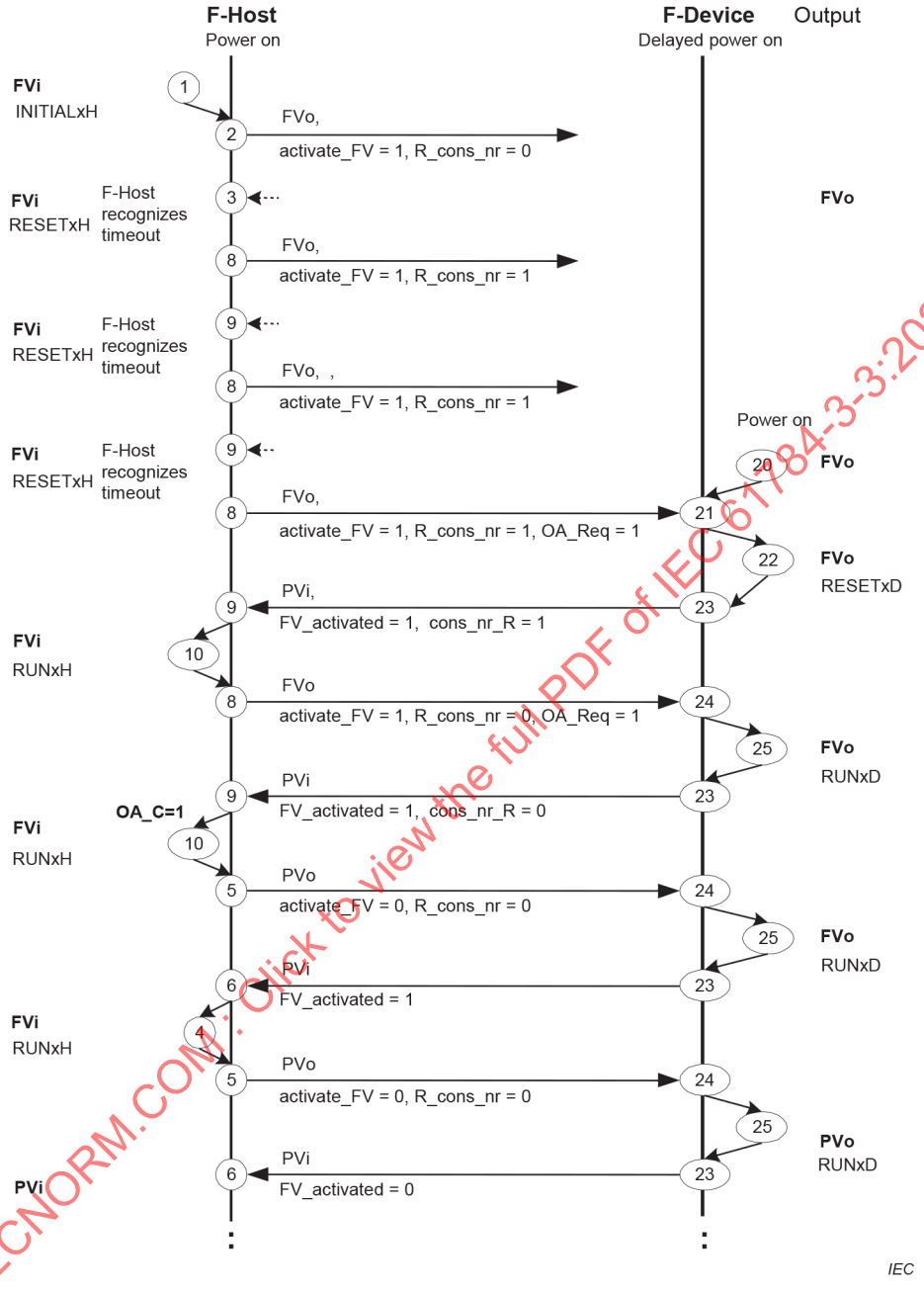


Figure 30 – Interaction F-Host driver / F-Device driver with delayed power on

Figure 31 corresponds to Figure 30. It shows the case when the F-Host is already operating and the F-(Sub)Module switches power off and after a delay switches power on again.

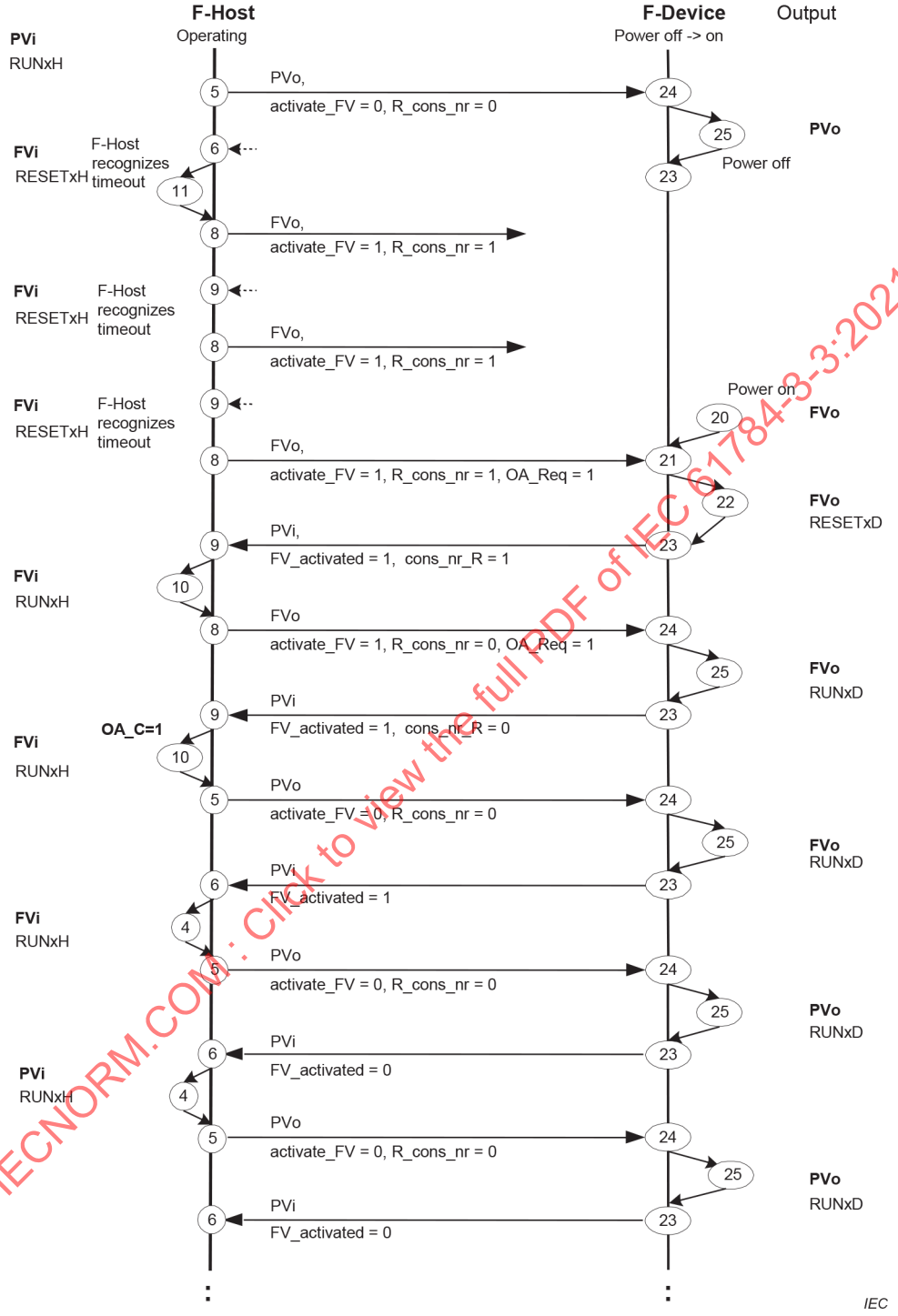


Figure 31 – Interaction F-Host driver / F-Device driver during power off → on

Figure 32 shows the interaction messages between F-Host driver and F-Device driver while CRC faults are detected on the F-Host driver side.

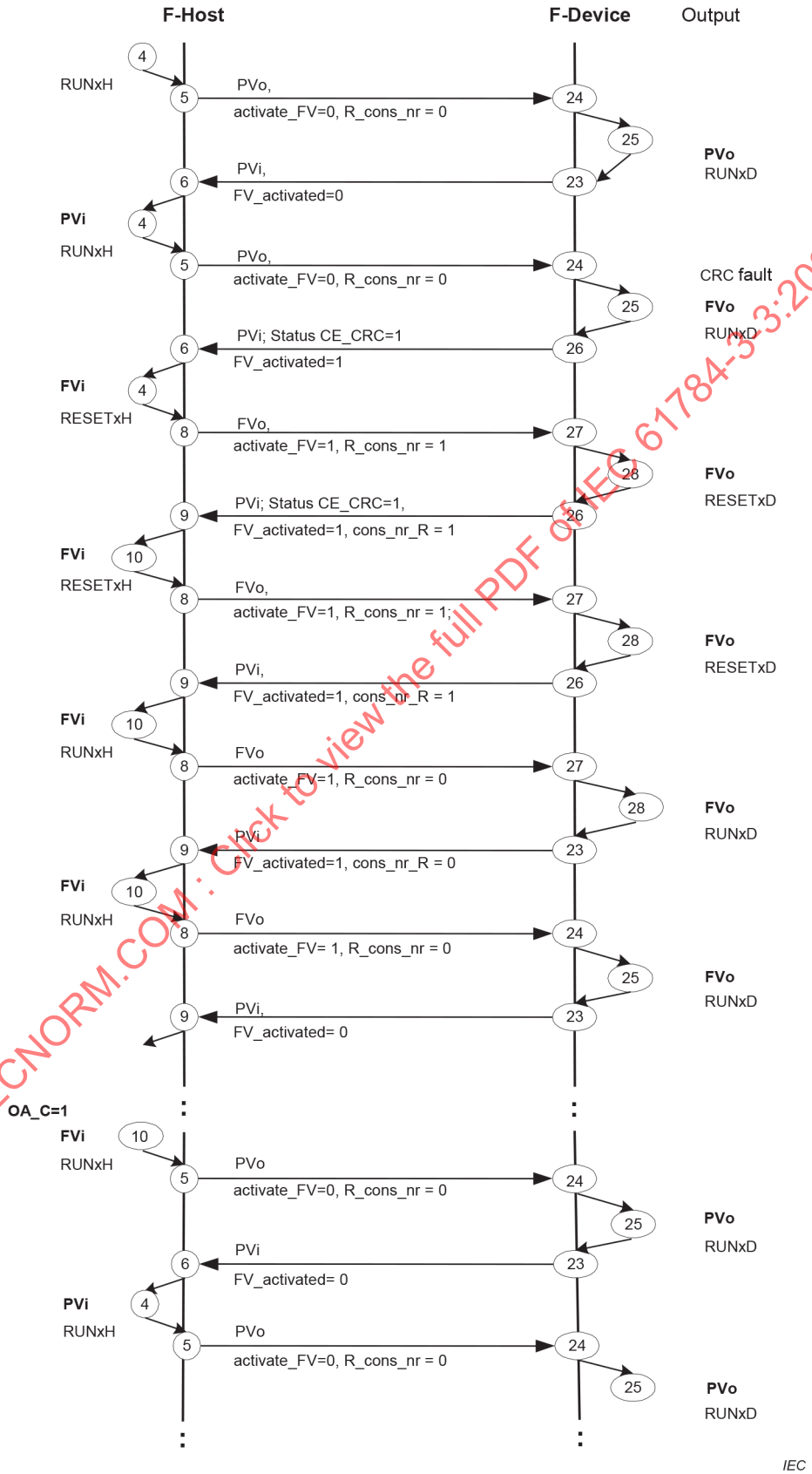


Figure 32 – Interaction while F-Host driver recognizes CRC error

Figure 33 shows the interaction messages between F-Host driver and F-Device driver while CRC faults are detected on the F-Device driver side.

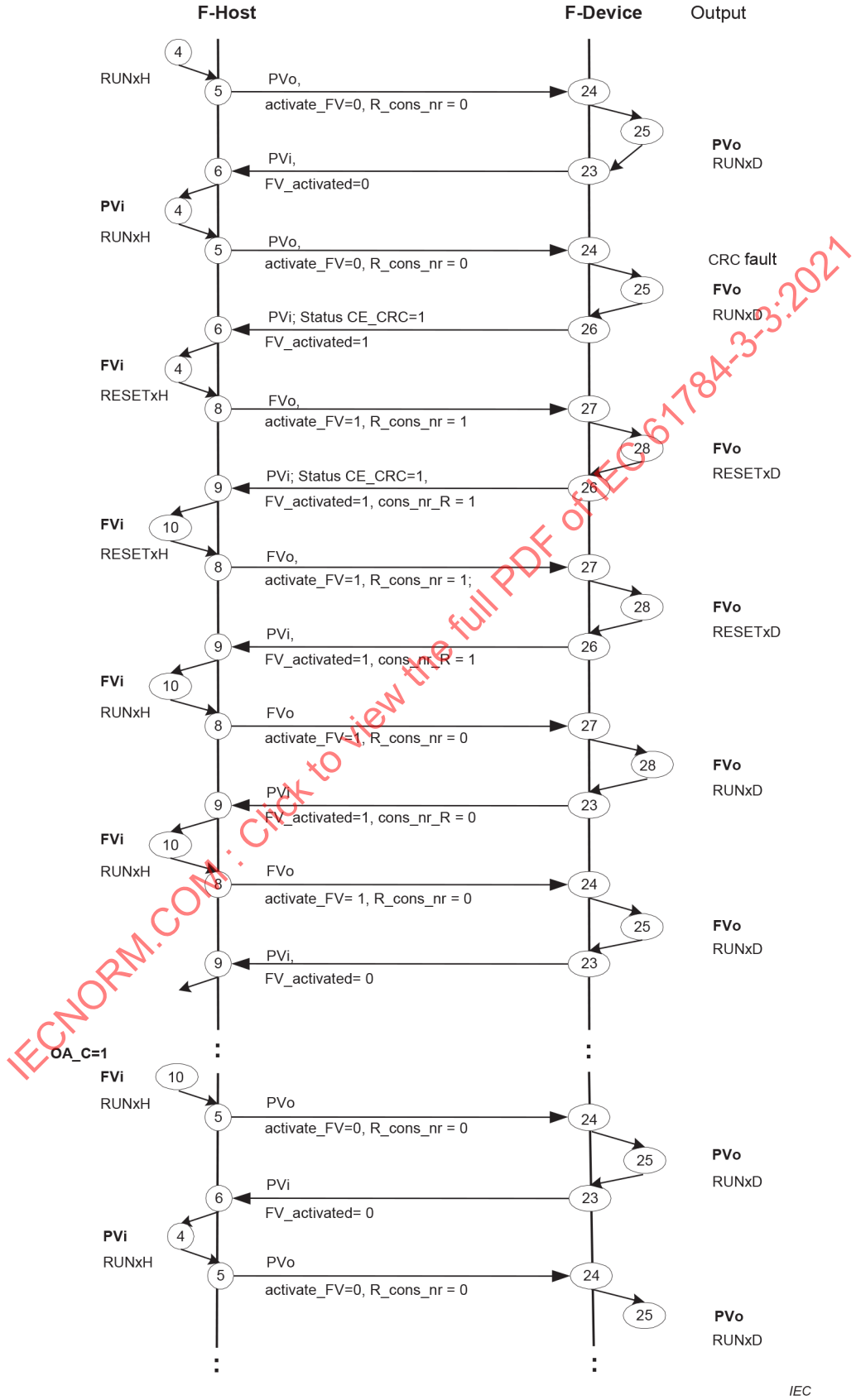


Figure 33 – Interaction while F-Device driver recognizes CRC error

7.2.6 Timing diagram for a MonitoringNumber reset

Figure 34 demonstrates the consequences of a communication fault on the MonitoringNumber and depending items.

After a fault, bit 2 ("R_cons_nr") and bit 4 ("activate_FV") of the Control Byte is set (=1). In consequence the MNR is reset and the output values of an F-Output-Device are set to "FVo".

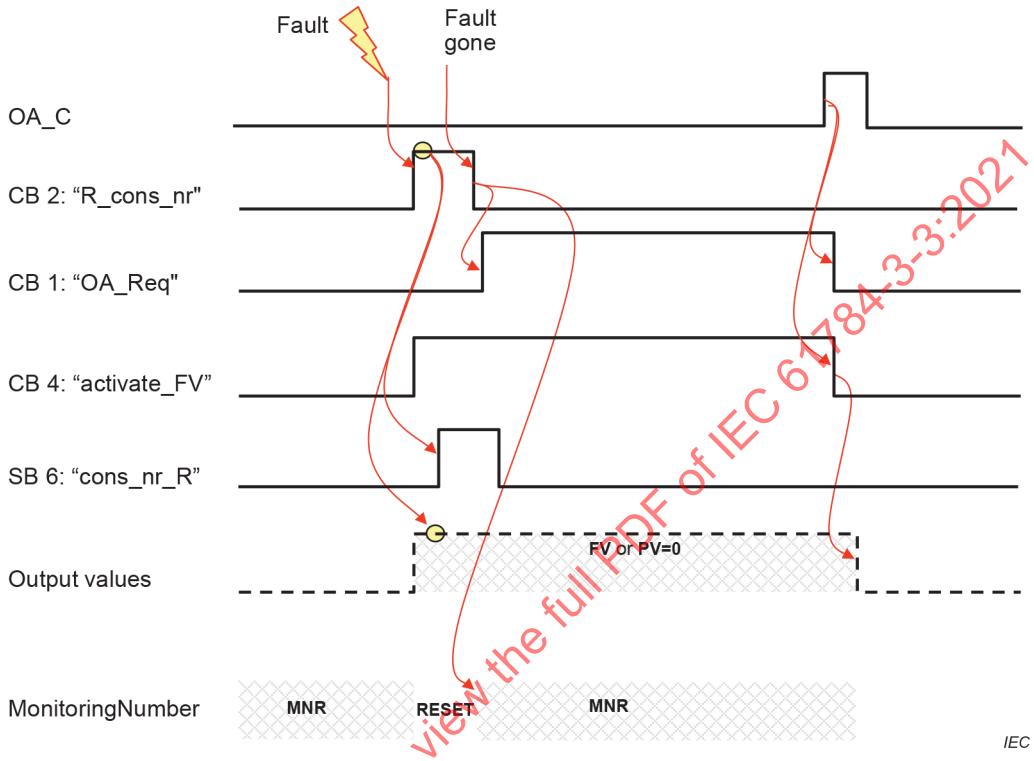


Figure 34 – Impact of the MNR reset signal

Right after the fault is gone the following actions take place:

- MNR reset resumes its default value (R_cons_nr =0);
- the MNR restarts.

Right after an Operator Acknowledgment (OA_C = 1) the following actions take place:

- request for an Operator Acknowledgment resumes its default value (OA_Req =0);
- request to activate fail-safe output state resumes its default value (activate_FV =0);
- process output values appear again after three message cycles.

7.2.7 Monitoring of safety times

7.2.7.1 Normal operation

Figure 35 demonstrates how the F drivers (at F-Host and F-(Sub)Module) are using the underlying CP 3/4 to CP 3/6 communications and how the monitoring times are defined. Meaning of the short arrows: in CP 3/4 to CP 3/6, the IO-Controller is able to update the F-Submodule and thus the safety PDU more frequently than a new safety PDU is generated by the F-Host driver within the F-Host driver cycle time and / or within the F-Device driver cycle time.

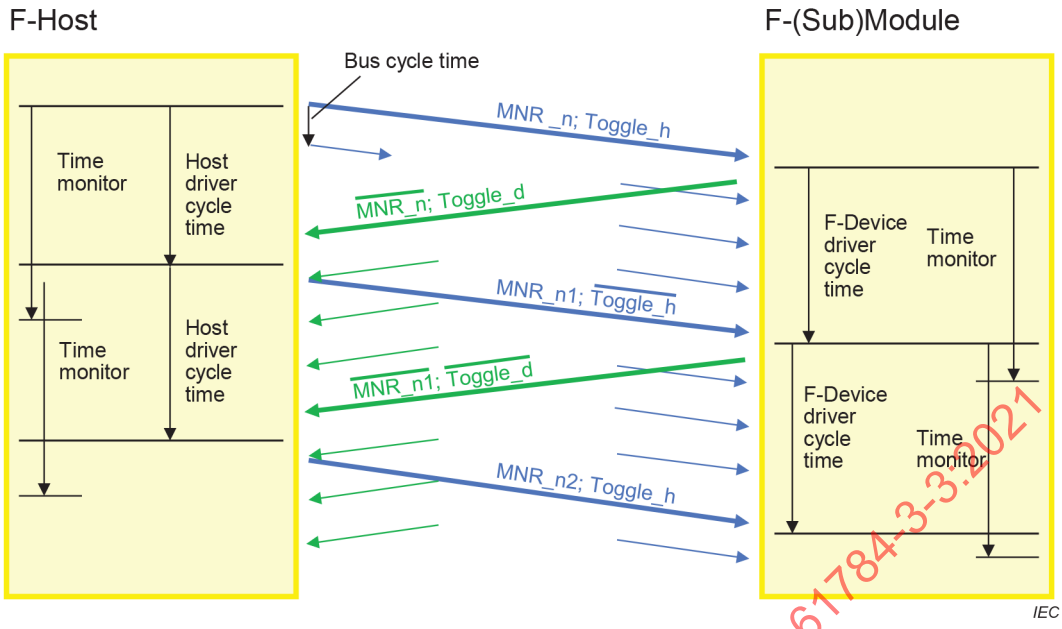


Figure 35 – Monitoring the message transit time F-Host ↔ F-(Sub)Module

Figure 35 shows the time monitoring within the F-Host and an F-(Sub)Module.

Other timing constraints are listed below:

Startup (Synchronization)	To synchronize after a system start, the F-Host driver starts with the virtual initial MNR (see 7.1.5 and 7.1.6).
F protocol cycle	An F-Device driver returns a safety PDU to the F-Host driver with the same but complement virtual MNR to acknowledge the reception of a safety PDU.
Time monitor (Watchdog)	The arrival of a new correct safety PDU at the F-Device driver within the watchdog time is being monitored. This verification can be performed as often as necessary, but at least once at the end of the monitoring time interval, see 9.3.3. When the watchdog time expires, the related recipient starts the fault reaction.
Monitoring the MNR	A new correct safety PDU is characterized by the fact that at least the Toggle_Bit and the virtual MNR is changed to the next virtual MNR and that either the entire rest of the safety PDU part is unchanged or has been changed faultlessly. This means that an incorrect change of the virtual MNR is recognized directly by CRC2. This will then lead to a fault reaction.
Safety PDU repetition	A complete safety PDU repetition in the case that a new correct safety PDU has not been received within the watchdog time interval is not supported.

SIL monitor

Every corrupted message related to one safety communication relationship detected in one of the states 4, 7, or 25 (CRC and virtual MNR fault) will be counted during a configurable SIL monitor time period (T). The fail-safe values are set whenever more than one such fault occurred, i.e. one detected corrupted message can be tolerated (*variant A*). Thus, the preallocation is "one corrupted message" at system startup. The cases, where the whole SPDU of the message = "0" (for example at start-up), shall not be counted.

In practice it can be shown that the counting actually always remains zero. This is the reason for an optimization of complexity resulting in *variant B*, where the SIL monitor time (T) is set to infinite. In this case, the simplified F-Host state chart of Figure 26 shall be taken into account where any detected corrupted safety PDU is not tolerated and always leads to a safe state.

Whenever such an unlikely event of a detected corrupted message should occur during the shift of production or operation, the responsible operator is assigned to play the role of the SIL-Monitor and can tolerate the indication and acknowledge it. In case of frequent indications more often than once per SIL Monitor time a check of the installation (for example electromagnetic interference), network traffic load, or transmission quality should be performed.

It is up to the F-Host manufacturer to implement variant A. However, a detailed realization is not specified here for the sake of individual adaptations to the particular system environments.

SIL Monitor time period (T)

The SIL monitor time period T is a constant value with the dimension hour (h) that results from the requested SIL and the configured CRC length (9.5.1). Table 14 specifies the SIL monitor times.

Table 14 – SIL monitor times

SIL	Time period (h) protocol LP	Time period (h) protocol XP
3	>100	>10
2	>10	>1

7.2.7.2 Extended watchdog time on request after user interaction

For use cases such as maintenance activities like 'Dynamic Reconfiguration' [54] or 'maintenance of fault tolerance systems' a certain time is required to update the affected devices. This update time usually is longer than the regular (primary) watchdog time (F_WD_Time) defined for a safety application. In order to avoid spurious trips, the F-Host driver can use once only per mentioned maintenance activity (see Figure 37) a secondary watchdog time (F_WD_Time_2) to extend the primary watchdog time for these cases as shown in Figure 36.

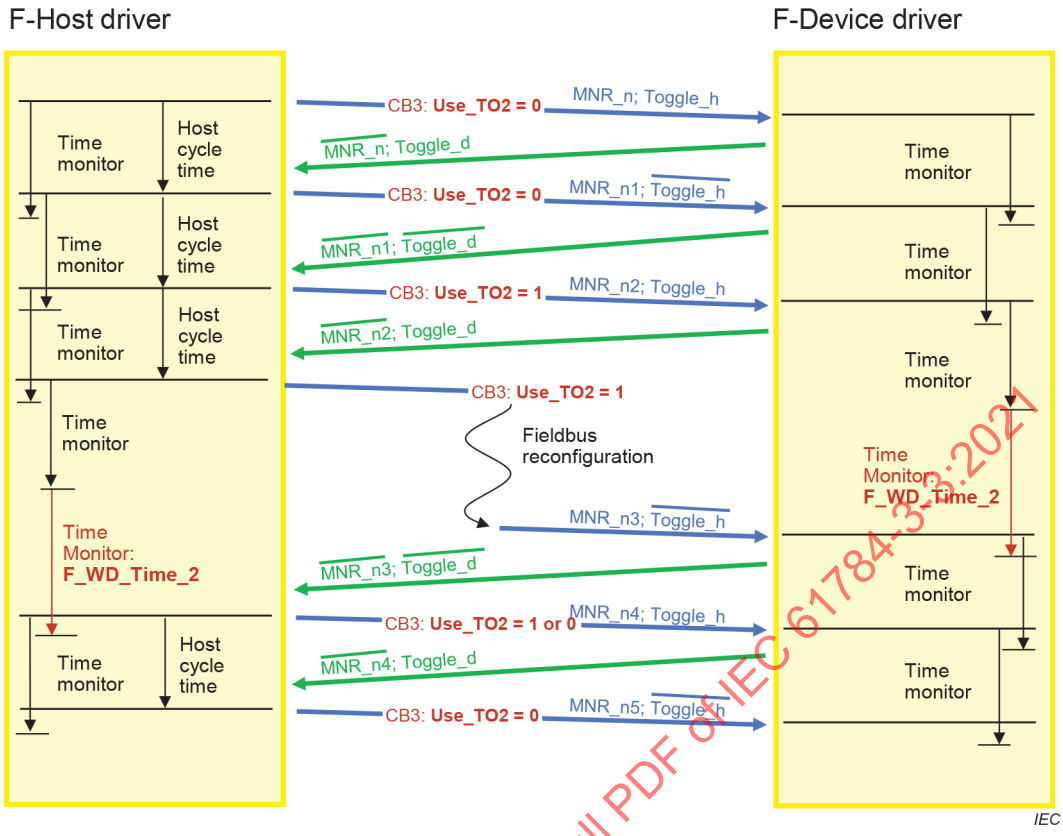


Figure 36 – Extended watchdog time on request

The F-Host shall set and reset Bit 3 (Use_TO2) of the Control Byte for all the F-Device driver thus affecting all F-Device drivers (see 6.1).

7.3 Reaction in the event of a malfunction

7.3.1 Corruption of safety data

Explanation: "The malfunction of a bus device or the transmission link perturbs safety PDUs."

NOTE "Explanation" references the corresponding malfunctions in the clause "communication errors" within IEC 61784-3:2021.

Remedial action: The CRC2 signature discovers a perturbation of the data between sender and recipient.

The CRC2 signature is generated across the F-Parameters respectively, the F-IO data, the virtual MNR, and the Control/Status Byte (see 7.1.7, 7.1.8, Figure 22, and Figure 24).

7.3.2 Unintended repetition

Explanation: "The malfunction of a bus device causes old and obsolete safety PDUs to be repeated at the incorrect time so that a recipient would dangerously be disturbed (for example guard door is reported closed although it has already been opened)."

Remedial action: Unintended repetition will be discovered by stringently changing and examining the MNR and/or watchdog time within the respective recipient as F-Host driver or F-Device driver.

7.3.3 Incorrect sequence

Explanation: "The malfunction of a bus device modifies the safety PDU sequence. Example: Prior to initiating the safe operational stop one wants to select the safely reduced velocity. The machine will be running instead of being stopped when these safety PDUs are confused."

Remedial action: Due to the stringently sequential expectation of the MNR, the recipient will discover any incorrect sequence.

7.3.4 Loss

Explanation: "The malfunction of a bus device deletes a safety PDU (for example request for "safe operational stop")."

Remedial action: Lost information will be discovered by stringently changing and examining the MNR and/or watchdog time within the respective recipient as F-Host driver or F-Device driver.

7.3.5 Unacceptable delay

Explanation: "1. The operational data exchange exceeds the capacity of the communication link. 2. A bus device causes an overload situation by simulating incorrect safety PDUs so that a service that belongs to the safety PDU is delayed or prevented."

Remedial action:

- Watchdog time in the respective recipient (as F-Host driver and/or F-Device driver) will detect an unacceptable delayed safety PDU.
- Change of Toggle bit within Control Byte and Status Byte in a SPDU with correct CRC2 causes a reset of the watchdog timer (see 7.1.3).

The watchdog time is defined in 9.3.3.

7.3.6 Insertion

Explanation: "The malfunction of a bus device inserts a safety PDU (for example deselection of the "safe operational stop")."

Remedial action: Due to the sequential expectation and "Codename initialization" of the MNR, the recipient will detect an inserted safety PDU.

7.3.7 Masquerade

Explanation: "The malfunction of a bus device causes safety PDUs, misrouted safety PDUs, and non-safety PDUs to be mixed up".

Remedial action: The recipient detects these "safety" PDUs from senders with incorrect authenticity via the CRC2 signature.

7.3.8 Addressing

Explanation: "The malfunction of a bus causes one or more misrouted safety PDUs".

Principle of safe connection authentication:

Detecting data from a different sender or for a different recipient is guaranteed by the fact that the respective sender F-Host or F-(Sub)Module that belongs to the F source-destination relationship (Codename) is the only one that generates exactly the matching CRC2 signature that is expected by the respective receiver as F-Host or F-(Sub)Module. At the same time, the recipient employs this CRC2 signature for implicitly checking the authenticity of the connection since Codename and direction are included in the CRC2 via MNR (see 7.1.7, 7.1.8, and 7.3.10).

A Retentive Selection of the Codename ("F_S/D_Address") in the individual devices can be achieved through one of the following methods:

– coding switch in the unit for the Codename;
– a one-time device parameterization by software that requires to be checked whether the correct device has been addressed. This shall be repeated when such a unit is replaced;
– by address mechanisms that are independent of CPF 3 addressing.

7.3.9 Out-of-sequence

Explanation: Central elements of CP 3/4 to CP 3/6 networks are switches, which are fairly complex active network components. They can have different faults. Messages may be sent to the incorrect destination or their data content can be perturbed. Furthermore a switch can send stored messages over and over again even when the sender already was shut down.

The following faults are detected / mastered:

– The F-Host fails or its safety PDUs does not reach the receiver. A switch transmits the messages of its revolving buffer without the correct MNR instead. The F-Device driver recognizes a MNR fault and sets Fail-safe Values (FV).
– A single message of the switch buffer is retransmitted and has a safety PDU with the correct MNR. This fault will be detected due to the MNR and the F driver switches to Fail-safe Values (FV).
– A switch transmits messages with safety PDUs out of its revolving buffer with the correct MNRs and this message sequence starts within the safety watchdog time. This fault will be detected due to the MNR and the switch back to process values needs an Operator Acknowledgment (OA_C = 1).

7.3.10 Loop-back

Explanation: "The programmable routing feature of a bus device reroutes unintentionally an F-Host message back to the F-Host, which expects a safety PDU of the same length".

Remedial action:

F_CRC_Seed =0: F-Host checks Loop-back via bit 7 of the Status Byte (Figure 17) and F-Output-Device driver detects Loop-back via timeout;

F_CRC_Seed =1: CRC2 signature calculation from F-Host and to F-Host uses different MNR algorithms (one's complement).

7.3.11 Network boundaries and router

Explanation: "1. The operational data exchange exceeds the capacity of the communication link. 2. A bus device causes an overload situation by simulating incorrect messages so that a service that belongs to the incorporated safety PDU is delayed or prevented."

For CP 3/4 to CP 3/6 networks with routers, Figure 9 and the corresponding explanations apply. Such a system with subnetworks connected via routers is assumed for the following considerations. They demonstrate that a single error will not misdirect a safety PDU to the incorrect F-Device driver and will not cause it to switch to a dangerous state.

The router connects two or more subnets over layer 3 levels. Every F-Host and IO-Device hosting F-Submodules can be configured to "use router" together with an appropriate router address. The router manages IP addresses of the connected subnets. Table 15 contains a list of fault types and the constraints for router operation to achieve sufficient safety.

Table 15 – Safety network boundaries

Fault type	Consequences	Detection and Mastering
Router holds the incorrect address of an IO Device hosting F-Submodules s	Router receives message for that particular F-Submodule. Result: Target not found.	Timeout detected by F-Device driver checking the SPDU
Two IO-Devices hosting F-Submodules with identical addresses and Submodule structure. One in subnet 0, the other one in subnet 1 Constraint: 2-Port-Router as shown in Figure 9	1) IO Device hosting F-Submodules of subnet 0 correct in subnet 0 2) IO Device hosting F-Submodules of subnet 0 not reachable in subnet 1 3) IO Device hosting F-Submodules of subnet 1 not reachable in subnet 0 4) IO Device hosting F-Submodules of subnet 1 correct in subnet 1	By standard CP 3/4 to CP 3/6

7.4 F-Startup and parameter change at runtime

7.4.1 Standard startup procedure

The startup of the F-Device driver is subsequent to the startup defined for CP 3/4 to CP 3/6. The F-Host driver and the F-Device driver are starting at their own whenever the CP 3/4 to CP 3/6 communication is established. The previously executed supply of the safety layers with their special F-Parameters is embedded in the Application Relation establishment and startup parameterization process ("Context") of CP 3/4 to CP 3/6. Any repetition of the F-Parameter supply with identical values at runtime (activate_FV_DC=0) shall be ignored; deviating values shall be either rejected or result in a safe state. If F-Submodules are plugged or pulled, then the CP 3/4 to CP 3/6 re-parameterization process applies.

See IEC 61158-5-10, and IEC 61158-6-10 for information on the startup sequences of an IO-Controller and its IO-Devices.

8 Safety communication layer management

8.1 F-Parameter

8.1.1 Summary

The parameter values of the CP 3/4 to CP 3/6 devices on the black channel are assigned according to the standard CP 3/4 to CP 3/6, i.e. via GSD files based on the GSD description languages (see [35] and [38]). The F-Parameters additionally required for the safety layer can be loaded via several alternative parameterization options.

Unintended change of "F-Parameter in use" during operation of a FSCP 3/1 communication shall be detected or prevented by the generic safety measures defined by the vendor.

"F-Parameter in use" are the values of F-Parameter which are used for the operating CPF 3 communication. That means F-(Sub)Module driver is in one of the states 23 to 28).

Summary of the F-Parameters:

- F_S/D_Address "Codename" between sender and recipient
- F_WD_Time Watchdog time in the F driver
- F_WD_Time_2 Optional secondary watchdog time in F-(Sub)Modules designed for "Dynamic Reconfiguration" or "maintenance of fault tolerant systems" or "Parameterization in Run". The engineering tool calculates and sets the value (with reserves for upcoming "DR" sessions) during commissioning (7.2.7.2)
- F_Prm_Flag1 + 2 Parameter octets containing several parameters for the profile management
  - F_Check_SeqNr V2-mode: ignore
  - F_Check_iPar Manufacturer specific use within homogeneous systems
  - F_SIL configured SIL
  - F_CRC_Length CRC2 signature length
  - F_CRC_Seed Use of different rules for CRC seed value and MNR for the CRC2 signature calculation (see Figure 42)
  - F_Passivation F-(Sub)Module or Channel-granular Passivation [56]
  - F_Block_ID Parameter block type identification
  - F_Par_Version Version No. of F-Parameters/FSCP 3/1 operational mode
- F_iPar_CRC Value of the iParameter CRC signature calculation, at least manually transferred from a CPD-Tool to the engineering tool
- F_Par_CRC CRC signature calculation across the F-Parameters to secure the transfer from the F-Engineering to the F-Device driver

8.1.2 F_Source/Destination_Address (Codename)

The Retentive Selection of the Codenames (stored in the F-(Sub)Module) of the safety communication relationships shall be unambiguous within the borders of one subnet according to IETF RFC 917. Subnets are connected to each other via (2-port) routers, which are natural borders for CP 3/4 to CP 3/6 where RT_CLASS_UDP is not permitted or not supported (5.4.2). Locally, each F-(Sub)Module holds the configured source-destination relationship of the safety communication link with its partner ("F_Source/Destination_Address" or short "F_S/D_Address"). It is a part of the F-Parameter set, and, consequently, the F-Device driver compares the F_S/D_Address parameters with the Retentive Selection of the Codename. The F_S/D_Address parameters are logic address designations that can be assigned *freely* but *unambiguously*. Typically, they are depicted from the F-Host driver (as source) and F-Device driver (as destination) during the configuration by engineering (7.3.7). The addresses *0* and *0xFFFF* shall be *excluded*.

The parameter consists of two parts: "F_Source_Add" and "F_Dest_Add", each of data type Unsigned16. Table 16 specifies the octet order of the Codename (F_Source/Destination_-Address).

Table 16 – Codename octet order

Codename			
MSB	octet	octet	LSB
F_Source_Address		**F_Dest_Address**	
MSB	LSB	MSB	LSB

8.1.3 F_WD_Time (F-Watchdog time)

Locally, each F-Device driver and its counterpart the F-Host driver maintains a configured F watchdog time for each source-destination relationship. The F driver starts this timer whenever it sends a safety PDU with a new MNR.

This F_WD_Time parameter is encoded as follows: Unsigned16. Time base: *1 ms*. The value range is 1 to 65 535.

See 9.3.3 for details on how these watchdog times fit into the whole definition of safety function response times (SFRT) and how they can be determined.

A manufacturer of an F-(Sub)Module assigns the maximum device acknowledgment time (DAT) to the default value of the parameter F_WD_Time in the GSD file. An engineering tool will then be able to propose the necessary F_WD_Time for this 1:1 communication relationship between F-Host driver and F-Device driver.

NOTE An engineering tool will then be able to calculate the safety function reaction times provided that all the other values are available. See 9.3.2.

8.1.4 F_WD_Time_2 (secondary F-Watchdog time)

This F-Parameter can be used optionally to extend the regular F-WD_Time by one extra time F_WD_Time_2 via Bit 3 of the Control Byte as demonstrated in Figure 37 (MNR "n5"). This extra time is required for the configuration update of Host and/or Devices, e.g. the switch over time of the two AR of an ARset.

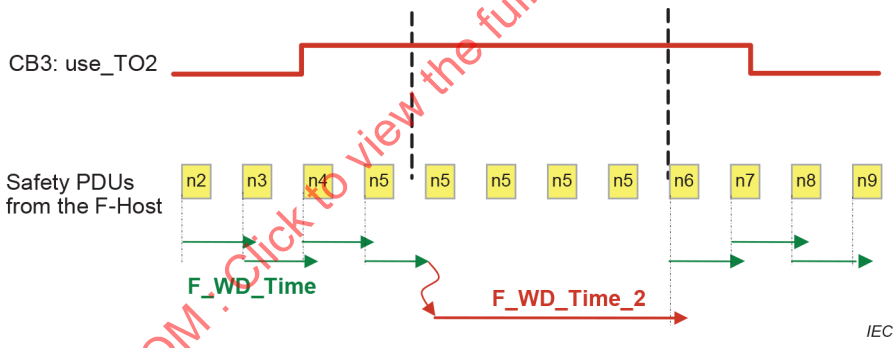


Figure 37 – Effect of F_WD_Time_2

The F_WD_Time_2 parameter is encoded as follows: Unsigned16. Time base: *1 ms*. The value range is 1 to 65 535. CB3 = 1 ("use_TO2") is an indicator for the F-Device driver to enable the F_WD_Time_2 once only. The normal F_WD_Time will be started immediately after the reception of the next safety PDU with a new MNR. Prior to a restart of F_WD_Time_2, the F-Host shall reset CB3.

8.1.5 F_Prm_Flag1 (Parameters for the safety layer management)

8.1.5.1 Structure of F_Prm_Flag1

Subclauses 8.1.5.2 to 8.1.5.5 are describing the details of the F_Prm_Flag1 parameter octet. It has the structure as in Figure 38:

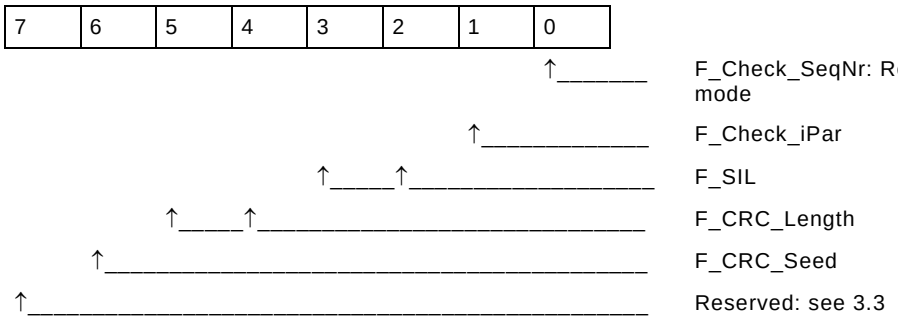


Figure 38 – F_Prm_Flag1

8.1.5.2 F_Check_SeqNr

This parameter is reserved as legacy from V1 mode, ignore in V2-mode.

8.1.5.3 F_Check_iPar

This vendor specific parameter shall always be set to "0" for normal use. It is reserved for manufacturer specific use in homogeneous systems. It is not related to the iPar-Server mechanism.

It is encoded as follows: Bit 1 of the parameter octet "F_Prm_Flag1" (see Figure 39).

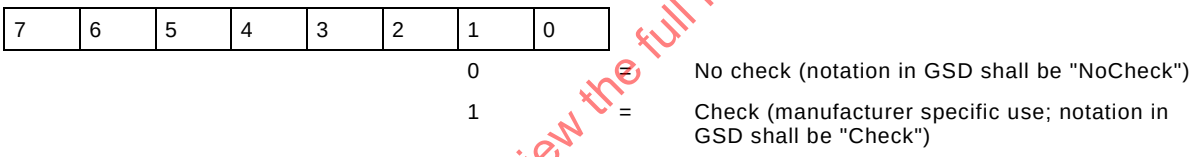


Figure 39 – F_Check_iPar

8.1.5.4 F_SIL (SIL stage)

The different safety functions using safety communication may require different safety integrity levels (SIL 1 to SIL 3). The F-(Sub)Modules are able to compare their own assigned SIL with the configured SIL (F_SIL). If it is higher than the SIL of the connected F-(Sub)Module, the "device failure" Status Bit is set and a safe state reaction is triggered. There are four different stages: SIL 1 to SIL 3, NoSIL (see Figure 40).

It is encoded as follows: Bits 2 and 3 of the parameter octet "F_Prm_Flag1".

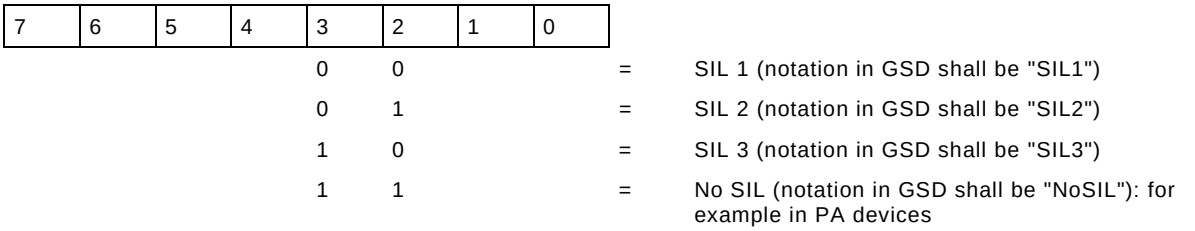


Figure 40 – F_SIL

8.1.5.5 F_CRC_Length (length of the CRC2 signature)

Depending on the parameter F_CRC_Seed, a CRC2 signature of 3 or 4 octets is required (see Figure 41). This parameter transfers the expected length of the CRC2 signature in the safety PDU to the F-Device driver during startup.

It is encoded as follows: Bits 4 and 5 of the parameter octet "F_Prm_Flag1".

7	6	5	4	3	2	1	0		
		0	0					=	3 octet CRC2 signature; notation in GSD shall be "3-Byte-CRC")
		0	1					=	Legacy: This parameter assignment shall not be used for new developments
		1	0					=	4 octet CRC2 signature; notation in GSD shall be "4-Byte-CRC")
		1	1					=	Reserved

Figure 41 – F_CRC_Length

8.1.5.6 F_CRC_Seed (Seed value for CRC2)

With F_CRC_Seed =0, the F-Device driver shall use CRC_FP (16 bit) as seed value and a counter as MNR for inclusion in the CRC2 signature calculation (see 7.1.5 and 7.1.7) according to previous protocol versions.

With F_CRC_Seed =1, the F-Device driver shall use a "1" as seed value, the CRC-FP+, and the virtual MonitoringNumber based on Codename for inclusion in the CRC2 signature calculation (see 7.1.6 and 7.1.8).

The engineering tool of an F-Host adjusts the F-Host driver according to this entry. The parameter is distributed to the F-Device driver during startup.

It is encoded as follows (see Figure 42): Bit 6 of the parameter octet "F_Prm_Flag1".

7	6	5	4	3	2	1	0		
	0							=	CRC-FP as seed value and counter (notation in GSD is "CRC-Seed16")
	1							=	"1" as seed value and CRC-FP+/MNR (notation in GSD is "CRC-Seed24/32"

Figure 42 – F_CRC_Seed

Table 17 shows the allowed combinations of F_CRC_Seed and F_Passivation.

Table 17 – Allowed combinations of F_CRC_Seed and F_Passivation

F_CRC_Seed	F_Passivation	
0	1	Not allowed
1	0 / 1	allowed

8.1.6 F_Prm_Flag2 (Parameters for the safety layer management)

8.1.6.1 Structure of F_Prm_Flag2

Subclauses 8.1.6.3 and 8.1.6.4 are describing the details of the F_Prm_Flag2 parameter octet. It has the structure as shown in Figure 43.

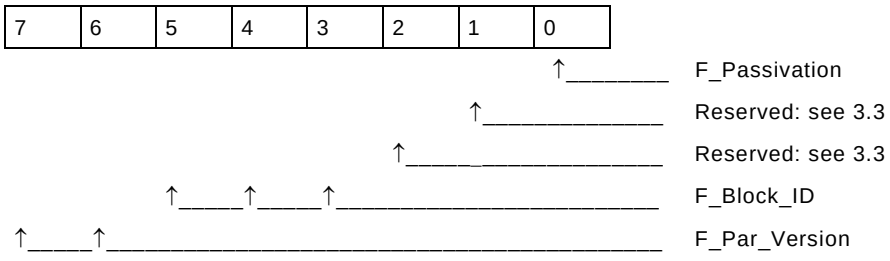


Figure 43 – F_Prm_Flag2

8.1.6.2 F_Passivation

Subclause 6.1 and Figure 14 describe the concept of Channel-granular Passivation (CGP) in contrast to the complete F-(Sub)Module passivation. An F-Host engineering tool will set this parameter to "0" if an F-Host does not support CGP (see Figure 44). An F-(Sub)Module supporting CGP shall check this parameter "F_Passivation". An F-(Sub)Module not supporting CGP shall react in case F_Passivation =1 with "Version of F-Parameter set incorrect".

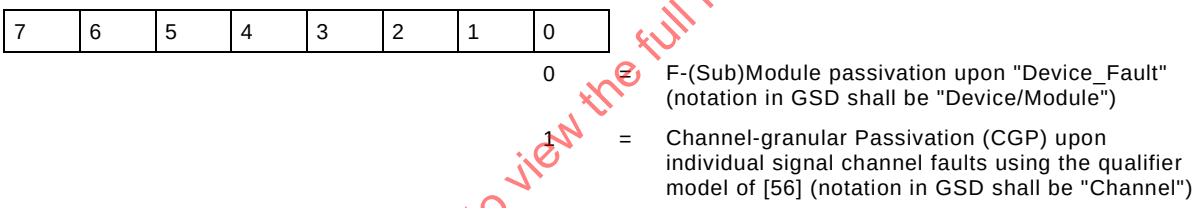


Figure 44 – F_Passivation

8.1.6.3 F_Block_ID (type identification of parameters)

In order to distinct parameters for future FSCP 3/1 modes, parameter type identification "F_Block_ID" is encoded in the following manner: Bits 3, 4 and 5 of the parameter octet "F_Prm_Flag2" (see Figure 45). It is mandatory for the safety layer to check the F_Block_ID.

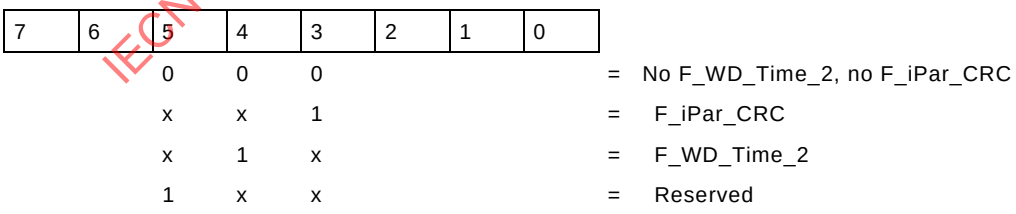


Figure 45 – F_Block_ID

8.1.6.4 F_Par_Version (version number of the F-Parameter set)

The purpose of this version counter is to identify releases of an operational mode inside the F-Device driver. The F-Device driver shall respond with a specific diagnosis message in case the requested version of the safety layer does not match the implemented version (see 6.3.2 and Figure 46). Validity checking of F-Parameters shall be done by the F-Device driver.

7	6	5	4	3	2	1	0		
0	0							=	Legacy V1-mode, which shall not be used for new implementations (notation in GSD shall be "V1-mode")
0	1							=	Valid for V2-mode (notation in GSD shall be "V2-mode")
1	0							=	Reserved
1	1							=	Reserved

Figure 46 – F_Par_Version

8.1.7 F_iPar_CRC (value of iPar_CRC across iParameters)

The CPD-Tool of a particular F-(Sub)Module is calculating a CRC signature (iPar_CRC) across all iParameters after a successful parameterization and commissioning session. Whenever the calculation results in a "0", the value shall be set to "1". The recommended CRC seed value for this calculation is "1". The value in *hexadecimal* format shall be transferred at least manually to the engineering tool and assigned to the "F_iPar_CRC" entry field.

This parameter is transmitted to the F-(Sub)Module during start-up and serves for an iParameter consistency check within the F-(Sub)Module prior to a start of regular safe operation. This parameter shall be set to "0" while in "FSCP test mode" (8.6.4.5) of an F-(Sub)Module. In this case the F-(Sub)Module will omit the consistency check. Whenever the F-(Sub)Module discovers a discrepancy between the locally calculated iPar_CRC signature and the value of F_iPar_CRC it shall set Fail-safe Values (FV).

This parameter is optional. Bit 3 of the F-parameter "F_Prm_Flag2" indicates its presence. It is encoded as: Unsigned32

8.1.8 F_Par_CRC calculation (across F-Parameters)

The engineering tool is generating this CRC signature across the F-Parameters. The seed value for this CRC signature is "0". Exception to general rule: In case of calculation result "0" and F-Parameter F_CRC_Seed =0, the CRC signature remains "0". See 8.3.3.2 for details on the order of the F-Parameters that shall be used for generating this CRC signature. The 16-bit CRC generator polynomial is used (*0x4EAB*).

It is encoded as: Unsigned16.

8.1.9 Structure of the F-Parameter record data object

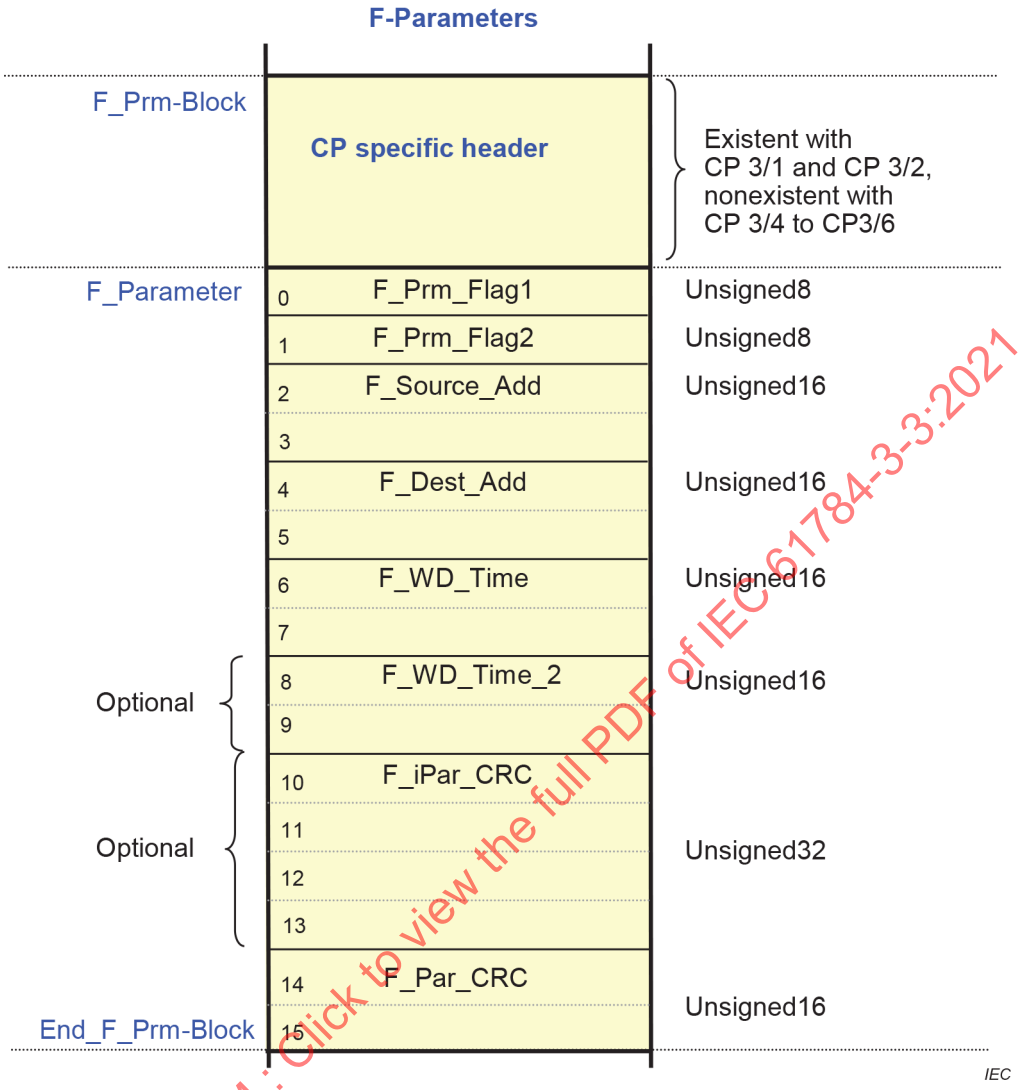


Figure 47 – F-Parameter

The Figure 47 shows the structure of the F-Parameter block for the F-(Sub)Modules. The octet ordering is according to CPF 3. For CP 3/4 to CP 3/6 the F-Parameter block is assigned to the F-Submodule via the subslot number.

8.2 iParameter and iPar_CRC

F-(Sub)Modules are increasingly provided with smart functions that require extensive individual parameter values to be assigned. These safety-related parameters are called iParameters. These F-(Sub)Modules may need additional parameters which are not provided by the Master / IO Controller. In particular in the event of a device replacement it is expedient to load these parameters directly via the bus on the standard path. These parameter records usually exceed the range of parameterization data based on GSD (several laser scanners with approximately 1 kB per protection zone may lead to an overall quantity of up to *90 kB* and more) and so this FSCP 3/1 specification provides additional mechanisms.

Figure 48 shows a proposal for the structuring of large amounts of iParameters for up- and download purposes. The absolute upper limit for iParameters is 2^{22}-1 octets; the lower limit is 4 octets. Thus, segmentation is required with CP 3/1 whenever the total exceeds 240 octets as shown in Figure 48. No segmentation is required with CP 3/4 to CP 3/6.

The CRC signature ("iPar_CRC") shall be calculated across the iParameters (Figure 48) using any appropriate CRC polynomial and filled into the 4 octet iPar_CRC in hexadecimal format and displayed on the CPD-Tool. Whenever the calculation results in a "0", the value shall be set to "1". The recommended CRC seed value for this calculation is "1". Inclusion of the iPar_CRC value in the iParameters as shown in Figure 48 is optional. No safety proof of sufficient residual error rate is required when using FSCP 3/1's 32 bit CRC polynomial.

The F_Source/Destination relationship (Codename) allows checking of delivery to the configured recipient. Inclusion in the iParameters as shown in Figure 48 is optional.

Identification and maintenance functions (I&M) are mandatory for all the CPF 3 devices. They provide codes identifying the type and release of a particular (Sub)Module. Including such information in the iParameter set can be used to check the validity of a replacement device with its own I&M functions. Inclusion in the iParameters as shown in Figure 48 is optional. Device manufacturers can use their own codings.

The length of the iParameter block can be helpful to efficiently organize the up- and download processes within the devices. Inclusion in the iParameters as shown in Figure 48 is optional.

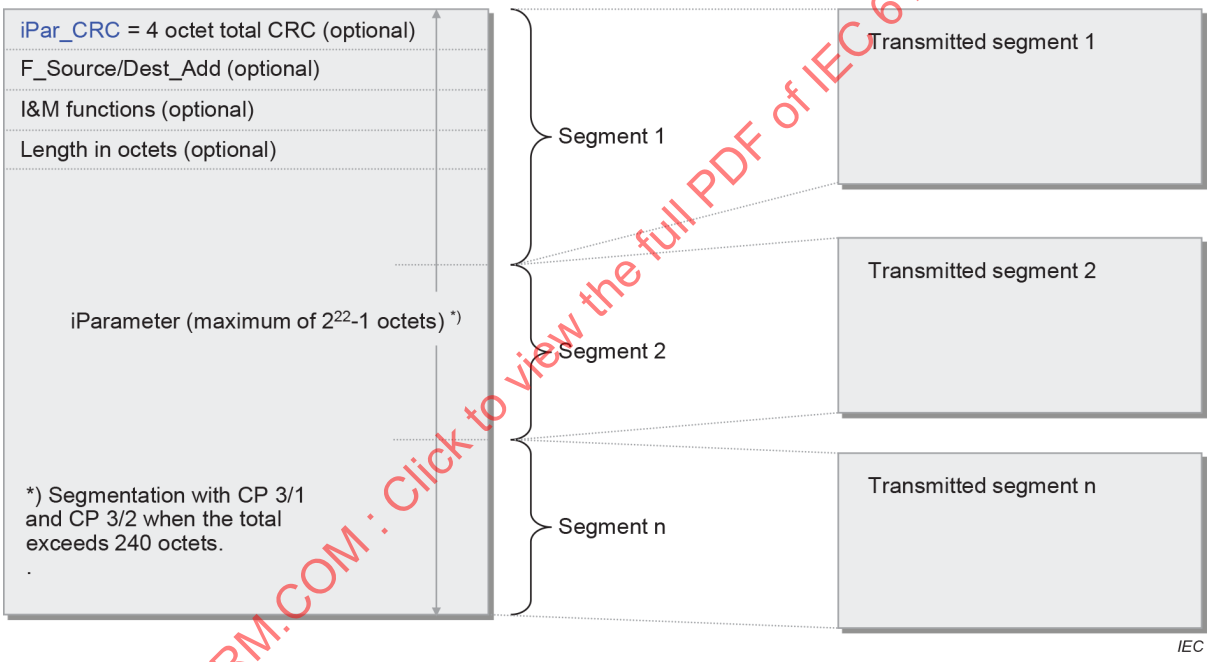


Figure 48 – iParameter block

See 8.6 for details on how to work with several iParameter segments.

8.3 Safety parameterization

8.3.1 Objectives

FSCP 3/1 provides scaled methods for F and iParameter supply of F-(Sub)Modules due to the different handlings of field devices within the manufacturing and the process industries. One major objective is to keep a small defined set of F-Parameters (communication level) stable across all F-(Sub)Modules and provide interfaces for iParameterization in order to minimize the dependency between system and device manufacturer and thus draw a clear line of responsibilities.

The F-(Sub)Module vendor takes responsibility for the integrity (Data integrity, Authenticity and Timeliness) of the iParameter.

For any amount of iParameters a standardized Proxy-FB, the "iPar-Server" is specified in this document. The F-Host system manufacturer takes responsibility for the iPar-Server and provides this feature either within the standard function block library or as a built-in function. The iPar-Server concept is specified in 8.6.4.

The small set of identical F-Parameters through all the different F-(Sub)Modules is passed over to an engineering tool via GSD and thus provides a constant and uncomplex application interface.

After the adjustment of the F-Parameters after network configuration, an F-Parameter record is compiled and stored within the F-Host and Master/IO-Controller for start-up of the automation system.

The F-Parameter "F_IO_StructureDescCRC" is used to ensure correct usage of the F-IO data structure and data types by the F application program and thus is not transferred to the F-(Sub)Module during start-up.

8.3.2 GSDL and GSDML safety extensions

8.3.2.1 CP 3/1 and CP 3/2: GSDL extensions

FSCP 3/1 uses the CP 3 defined structure of devices. CP 3/1 or CP 3/2 devices are structured using modules placed into slots. All parameters are defined for and assigned to Modules. The General Station Description Language (GSDL) specification [35] for IEC 61158 type 3 therefore defines keywords to structure and identify the F-Parameter block information of F-Modules shown in Figure 47. The possible F-Parameter value selections are contained in a General Station Description (GSD) file associated with a Slave which hosts F-Modules is designed for. The following keywords in Table 18 are defined.

Table 18 – GSDL keywords for F-Parameters and F-IO structures

GSDL Keyword	Description
F_Ext_Module_Prm_Data_Len	The parameter associated with this keyword indicates the total length of the F_Prm-Block shown in Figure 47.
F_Ext_Module_Prm_Data_Const (offset)	With the help of the parameter associated with this keyword a fixed value can be entered into one of the 4 header octets of the F_Prm-Block shown in Figure 47. The position of an octet is indicated by an offset 0...3
F_Ext_Module_Prm_Data_Const (0)	Indicates the F_Prm_Block length including the F_iPar_CRC, e.g. 0x12
F_Ext_Module_Prm_Data_Const (1)	Identification of the F_Prm-Block = 5 (fix)
F_Ext_Module_Prm_Data_Const (2)	Slot of the F-Module
F_Ext_Module_Prm_Data_Const (3)	Reserved. Shall be set "0".
F_Ext_Module_Prm_Data_Ref (offset)	With the help of the parameter associated with this keyword a user selectable value at configuration time can be entered into one of the octets 0 to 13 of the F_Prm-Block shown in Figure 47. The position of an octet is indicated by an offset 4 to 16. The parameter is pointing to an ExtUserPrmData range definition within other parts of the GSD file
F_ParamDescCRC	The parameter associated with this keyword secures the safety-related parts of the F-Parameter descriptions within the GSD file See 8.3.3.3 for details on how to determine this CRC0 signature.
F_IO_StructureDescCRC	The parameter associated with this keyword secures the description of the F-IO data structure (cyclically transferred process values). See [35] and 8.4.2 for details on how to determine this F_IO_StructureDescCRC signature

GSDL Keyword	Description
F_IO_StructureDescVersion	The parameter associated with this keyword indicates the version of an F-IO data structure description. A value of 1 indicates a 16-bit F_IO_StructureDescCRC signature while a value of 2 indicates a 32-bit F_IO_StructureDescCRC signature. If this attribute is not present, a value of 1 is assumed

Structured parameterization is recommended. See 8.6.4.6 for further GSDL extensions.

8.3.2.2 CP 3/4 to CP 3/6: GSDML extensions

FSCP 3/1 uses the CP 3 defined structure of devices. CP 3/4 to CP 3/6 devices are structured using Modules und Submodules placed into Slots and Subslots. All parameters are defined for and assigned to Submodules. The F-Parameters of a particular F-(Sub)Module are defined with the help of its GSD file. The description is provided using the General Station Description Markup Language (GSDML) for IEC 61158 type 10 based on XML (see [38].

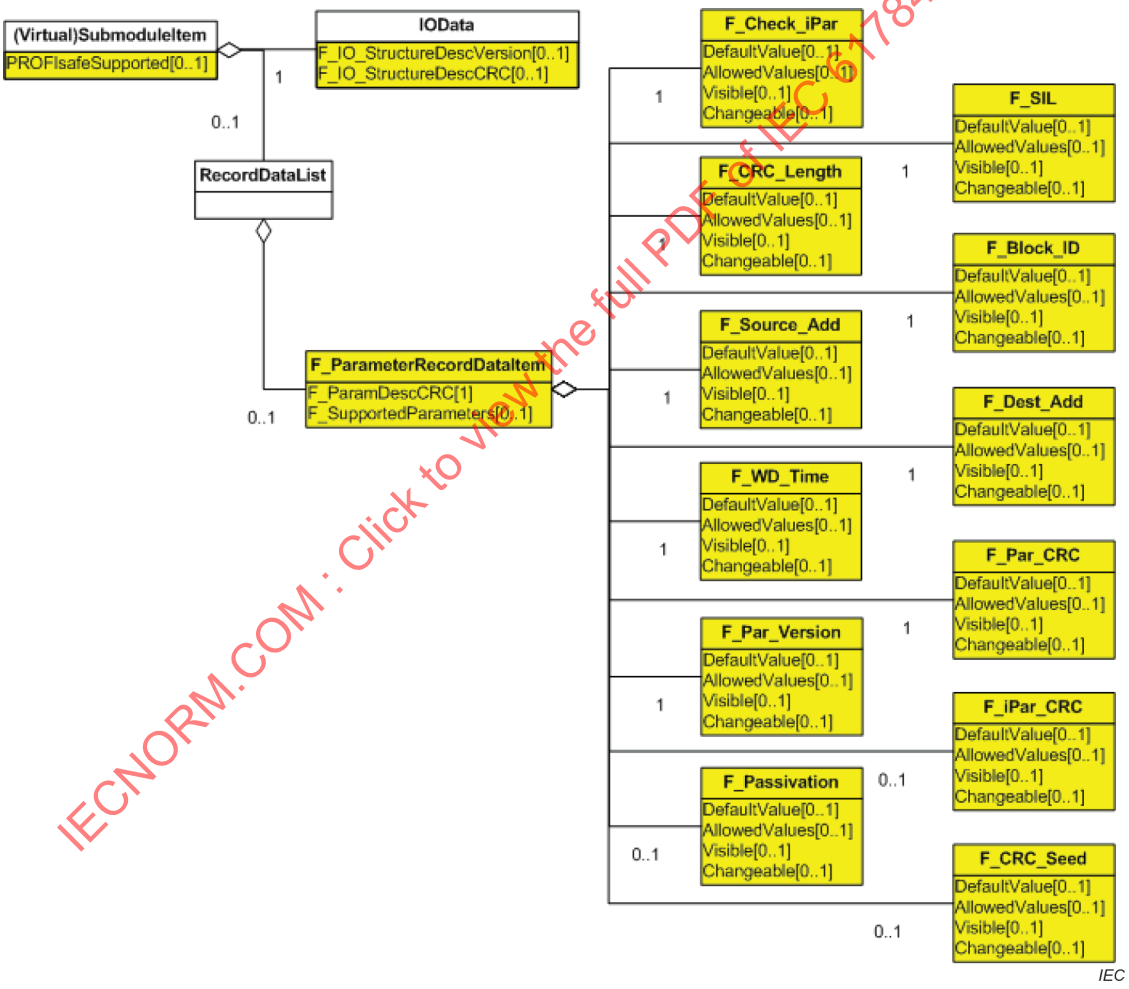


Figure 49 – F-Parameter extension within the GSDML specification

Figure 49 shows the extensions within the GSDML. The element "(Virtual)SubmoduleItem" provides the following attributes:

- "F_ParamDescCRC": This is the CRC signature (CRC0) of the F-Parameter description according to Figure 49.
- "F_SupportedParameters": Direct indication of the supported optional F-Parameters in the F-Parameter record (decoded information of "F_Block_ID"). For details see [38].

The "F_IO_StructureDescCRC" in element "IOData" secures the formats of the F-Input and F-Output data. The "F_IO_StructureDescVersion" indicates the version of an F-IO data structure description (see 8.3.3).

In GSDML, the F-Parameters F_CRC_Seed and F_Passivation are optional. They shall be present either both or none. Their presence indicates support of FSCP 3/1 protocol according to this document. To prevent engineering tools from stopping by the new F-Parameters, insert attribute RequiredSchemaVersion= "V2.32" (recommended V2.34/V2.35) to the description of the F-Submodule.

In case of backward compatibility to previous FSCP 3/1 protocol versions, an F-Submodule shall be described a second time in the GSD file without F_CRC_Seed and F_Passivation, and with F_CRC_Length=3-Byte-CRC instead of 4-Byte-CRC.

F-Submodules supporting both settings of F_Passivation also require separate sets of descriptions in the GSD file due to the different IO data layouts with or without qualifiers.

8.3.3 Securing safety parameters and GSD data

8.3.3.1 General

It is vital for the safety of the system to secure the safety parameters of the safety layer (F-Parameters) and for the F-(Sub)Module (iParameters) as well as the chosen safety IO data structures. This is done via CRC signatures, persistent storage within the F-(Sub)Module and in the F-Host and periodical comparison of CRC signatures.

In order to prevent the engineering tool from using perturbed device description data (GSD) the safety relevant parts of it are secured via CRC signature also.

8.3.3.2 F_Par_CRC and iPar_CRC across safety parameters

Figure 21 is only showing the CRC1 signature across the F-Parameters that shall be involved in the CRC2 signature generating process. However, optionally there can be involved more CRC signatures as follows in 8.3.3.2.

In order to secure the F-Parameters, the engineering tool of the F-Host is generating the *F_Par_CRC* signature as described in 8.1.7. The CRC polynomial that shall be used is *0x4EAB*. The CRC signature is built across all F-Parameters in the octet order of Figure 47 excluding the optional F_iPar_CRC. Whenever bit 3 of the F-Parameter "F_Block_ID" is set to "1" the F_iPar_CRC signature shall be included at the beginning of the calculation as shown in Figure 50.

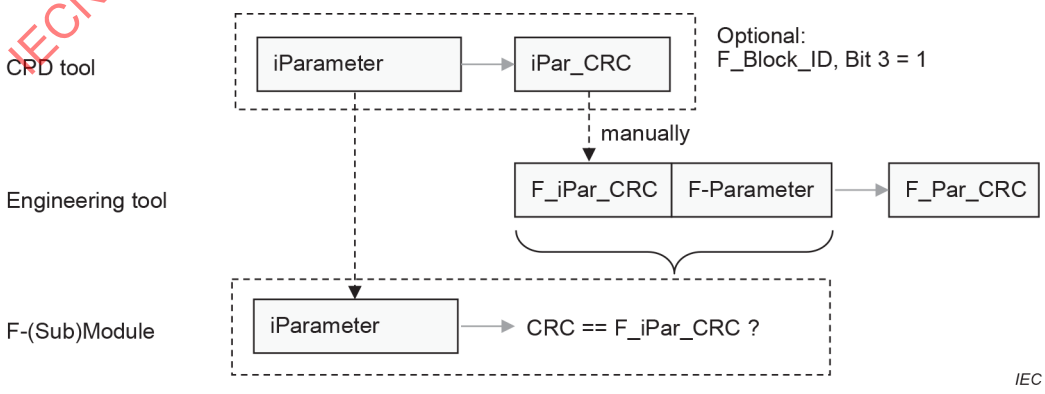


Figure 50 – F_Par_CRC signature including iPar_CRC

This procedure shall also be used for the calculation of CRC_FP (see 7.1.7) and CRC_FP+ (see 7.1.6).

8.3.3.3 CRC0 across GSD data

In order to make sure that safety relevant parameters of the F-(Sub)Module will not change unnoticed during lifetime of a storage media and can be read safely into the engineering tool they all are CRC protected. The parameter "F_ParamDescCRC" contains a 2-octet CRC signature (CRC0) generated with the help of the same 16-bit CRC polynomial (0x4EAB) that is used all over FSCP 3/1. Table 19 describes the serialization and calculation algorithm.

Table 19 – Algorithm to build CRC0

1	Sort the F-Parameters in ascending order by octet offset bit offset (as they appear in the F-Parameter record shown in Figure 47).
2	For each listed visible F-Parameter serialize: a) The F-Parameter name b) One octet for the data type (0 = Bit/BitArea, 1 = Unsigned8, 2 = Unsigned16, 3 = Unsigned32). c) One octet for the bit offset within the octet (0-7 for data type Bit/BitArea, 0 for the other data types). d) The default value. e) The allowed value(s).
3	There are two ways of serialization of the allowed values: in form of a value range or an enumeration. a) A value range contains only values. It is serialized as a minimum value and a maximum value. If there is only one allowed value, this value is used for both the minimum and the maximum value. This form is used for F-Parameters consisting only of numerical values (e.g. F_Source_Add), and it is also used for F-Parameters having standardized names in addition to their numerical value, when there exists only one allowed value. b) An enumeration comprises pairs of a name and its associated value, sorted by increasing value. This form is used for F-Parameters having standardized names in addition to their numerical value (e.g. F_SIL), when there exists more than one allowed value.
4	The following rules shall be considered for strings and numerical values while serializing: a) Strings (names) are serialized character by character using their ASCII code. Neither a string length nor a terminating zero character is serialized. b) Numerical values are serialized in little-endian octet order (least significant octet first). Values of type Bit/BitArea, Unsigned8, and Unsigned16 are serialized as 16-bit unsigned integer, while values of type Unsigned32 are serialized as 32-bit unsigned integer.
5	Calculate the 2 byte CRC across the octet stream using the CRC polynomial *0x4EAB*.

In case of a GSD file for an F-Slave (CP 3/1 or CP 3/2) the following GSDL annotation rules apply for the CRC0 signature calculation (see the example in Table 20 and Table 22):

- If an F-Parameter out of the set F_Check_SeqNr, F_Check_iPar, F_CRC_Length, F_CRC_Seed, F_Passivation, F_Block_ID is omitted in the GSD, a fixed value of zero is assumed and it shall not be included into the calculation of CRC0.
- The F_Ext_User_Prm_Data_Const keywords shall be ignored.
- In case the F-Parameters are described in a block structure form (see keywords Prm_Block_Structure_supp / ..._req), the F_Ext_User_Prm_Data_Ref keywords shall be ignored that point into the block header.
- The F_Ext_User_Prm_Data_Ref points to the ExtUserPrmData where the F-Parameter name, the data type, the default value and the permitted numerical values can be found.
- For F-Parameters with standardized names in addition to their numerical values, the Prm_Text_Ref points to the PrmText with these name definitions. The PrmTxt shall contain texts for all of the permitted values. Additional texts for unspecified values shall be ignored by engineering/configuration tools.

Table 20 – GSD example in GSDL notation

Declaration	Referenced PrmData	Referenced PrmText
F_Ext_User_Prm_Data_Ref(4) = 1	ExtUserPrmData = 1 "F_SIL" BitArea(2-3) 2 0-2 Prm_Text_Ref = 1 EndExtUserPrmData	PrmText = 1 Text(0) = "SIL1" Text(1) = "SIL2" Text(2) = "SIL3" Text(3) = "NoSIL" EndPrmText
F_Ext_User_Prm_Data_Ref(4) = 2	ExtUserPrmData = 2 "F_CRC_Length" BitArea(4-5) 2 2-2 Prm_Text_Ref = 2 EndExtUserPrmData	PrmText = 2 Text(0) = "3-Byte-CRC" Text(1) = "2-Byte-CRC" Text(2) = "4-Byte-CRC" EndPrmText
F_Ext_User_Prm_Data_Ref(4) = 3	ExtUserPrmData = 3 "F_CRC_Seed" Bit(6) 1 1-1 Prm_Text_Ref = 3 EndExtUserPrmData	PrmText = 3 Text(0) = "CRC-Seed16" Text(1) = "CRC-Seed24/32" EndPrmText
F_Ext_User_Prm_Data_Ref(5) = 4	ExtUserPrmData = 4 "F_Passivation" Bit(0) 0 0-0 Prm_Text_Ref = 4 EndExtUserPrmData	PrmText = 4 Text(0) = "Device/Module" Text(1) = "Channel" EndPrmText
F_Ext_User_Prm_Data_Ref(5) = 5	ExtUserPrmData = 5 "F_Block_ID" BitArea(3-5) 0 0-0 EndExtUserPrmData	
F_Ext_User_Prm_Data_Ref(5) = 6	ExtUserPrmData = 6 "F_Par_Version" BitArea(6-7) 1 1-1 Prm_Text_Ref = 5 EndExtUserPrmData	PrmText = 5 Text(0) = "V1-mode" Text(1) = "V2-mode" EndPrmText
F_Ext_User_Prm_Data_Ref(6) = 7	ExtUserPrmData = 7 "F_Source_Add" Unsigned16 1 1-65534 EndExtUserPrmData	
F_Ext_User_Prm_Data_Ref(8) = 8	ExtUserPrmData = 8 "F_Dest_Add" Unsigned16 1 1-65534 EndExtUserPrmData	
F_Ext_User_Prm_Data_Ref(10) = 9	ExtUserPrmData = 9 "F_WD_Time" Unsigned16 500 10-2000 EndExtUserPrmData	
F_Ext_User_Prm_Data_Ref(12) = 10	ExtUserPrmData = 10 "F_Par_CRC" Unsigned16 21211 0-65535 EndExtUserPrmData	

For sample GSD files for F-Slaves (CP 3/1 or CP 3/2), contact the fieldbus organizations in Annex B.

In case of a GSD file for an IO Device able to host F-Submodules (CP 3/4 to CP 3/6) the following GSDML annotation rules apply for the CRC0 signature calculation (see the example in Table 21 and Table 22):

- Some F-Parameters have standardized names with associated numerical values. In the GSDML notation only these names shall be used in the attributes "DefaultValue" and "AllowedValues". The associated numerical values can be found in 8.1.
- If an F-Parameter out of the set F_Check_iPar, F_CRC_Length, F_Block_ID is set to invisible in the GSD, a fixed value of zero is assumed and it shall not be included into the calculation of CRC0.
- If an F-Parameter (or parts of its definition) is merely omitted from the GSD file, default values from the corresponding GSDML schema shall be used. Visible parameters shall always be included in the CRC0 calculation, regardless of whether their values are explicitly specified in a GSD file or supplemented from the schema.

- F_Check_SeqNr does not exist in the GSDML definition and thus shall not be included in the CRC0 calculation.
- F_Par_Version always shall be included in the CRC0 calculation although it has a fixed value of "1".
- The order of F-Parameters in element "F_ParameterRecordDataItem" corresponds with the order in the F-Parameter record, except for F_iPar_CRC.

Table 21 – GSD example in GSDML notation

```
<F_ParameterRecordDataItem Index="1" F_ParamDescCRC="56313">
    <F_Check_iPar/>
    <F_SIL DefaultValue="SIL3" AllowedValues="SIL1 SIL2 SIL3"/>
    <F_CRC_Length DefaultValue="4-Byte-CRC" AllowedValues="4-Byte-CRC" Visible="true"/>
    <F_CRC_Seed/>
  <F_Passivation DefaultValue="Device/Module" AllowedValues="Device/Module"/>
    <F_Block_ID DefaultValue="0" AllowedValues="0" Changeable="false"/>
    <F_Par_Version/>
    <F_Source_Add/>
    <F_Dest_Add/>
    <F_WD_Time DefaultValue="500" AllowedValues="10..2000"/>
    <F_Par_CRC DefaultValue="21211"/>
</F_ParameterRecordDataItem
```

For sample GSD files for IO Device able to host F-Submodules (CP 3/4 to CP 3/6) contact the fieldbus organizations in Annex B.

Table 22 – Serialized octet stream for the examples

GSD content	Serialized octet stream for CRC0 calculation
"F_SIL" Type=BitArea, Offset=2 Default=2 (SIL3) "SIL1", 0 (enumeration) "SIL2", 1 "SIL3", 2	0x46, 0x5F, 0x53, 0x49, 0x4C, 0x00, 0x02, 0x02, 0x00, 0x53, 0x49, 0x4C, 0x31, 0x00, 0x00, 0x53, 0x49, 0x4C, 0x32, 0x01, 0x00, 0x53, 0x49, 0x4C, 0x33, 0x02, 0x00,
"F_CRC_Length" Type=BitArea, Offset=4 Default=2 (4-Byte-CRC) Min=2, Max=2 (range)	0x46, 0x5F, 0x43, 0x52, 0x43, 0x5F, 0x4C, 0x65, 0x6E, 0x67, 0x74, 0x68, 0x00, 0x04, 0x02, 0x00, 0x02, 0x00, 0x02, 0x00,
"F_CRC_Seed" Type=Bit, Offset=6 Default=1 (CRC_Seed24/32) Min=1, Max=1 (range)	0x46, 0x5F, 0x43, 0x52, 0x43, 0x5F, 0x53, 0x65, 0x65, 0x64, 0x00, 0x06, 0x01, 0x00, 0x01, 0x00, 0x01, 0x00,
"F_Passivation" Type=Bit, Offset=0 Default=0 (Device/Module) Min=0, Max=0 (range)	0x46, 0x5F, 0x50, 0x61, 0x73, 0x73, 0x69, 0x76, 0x61, 0x74, 0x69, 0x6F, 0x6E, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
"F_Block_ID" Type=BitArea, Offset=3 Default=0 Min=0, Max=0	0x46, 0x5F, 0x42, 0x6C, 0x6F, 0x63, 0x6B, 0x5F, 0x49, 0x44, 0x00, 0x03, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
"F_Par_Version" Type=BitArea, Offset=6 Default=1 (V2-mode) Min=1, Max=1	0x46, 0x5F, 0x50, 0x61, 0x72, 0x5F, 0x56, 0x65, 0x72, 0x73, 0x69, 0x6F, 0x6E, 0x00, 0x06, 0x01, 0x00, 0x01, 0x00, 0x01, 0x00,

GSD content	Serialized octet stream for CRC0 calculation
"F_Source_Add" Type=Unsigned16 Default=1 Min=1, Max=65534	0x46, 0x5F, 0x53, 0x6F, 0x75, 0x72, 0x63, 0x65, 0x5F, 0x41, 0x64, 0x64, 0x02, 0x00, 0x01, 0x00, 0x01, 0x00, 0xFE, 0xFF,
"F_Dest_Add" Type=Unsigned16 Default=1 Min=1, Max=65534	0x46, 0x5F, 0x44, 0x65, 0x73, 0x74, 0x5F, 0x41, 0x64, 0x64, 0x02, 0x00, 0x01, 0x00, 0x01, 0x00, 0xFE, 0xFF,
"F_WD_Time" Type=Unsigned16 Default=500 Min=10, Max=2000	0x46, 0x5F, 0x57, 0x44, 0x5F, 0x54, 0x69, 0x6D, 0x65, 0x02, 0x00, 0xF4, 0x01, 0x0A, 0x00, 0xD0, 0x07,
"F_Par_CRC" Type=Unsigned16 Default=21211 Min=0, Max=65535	0x46, 0x5F, 0x50, 0x61, 0x72, 0x5F, 0x43, 0x52, 0x43, 0x02, 0x00, 0xDB, 0x52, 0x00, 0x00, 0xFF, 0xFF

The resulting CRC0 signature 56313 (decimal) or 0xDBF9 (hexadecimal) shall be entered into the F_ParamDescCRC attribute.

Interpretation of the GSD file: Whenever the engineering tool recognizes F-Keywords, special F-Configuration software (usually safety assessed) inside the engineering tool may be launched to handle F-Parameters in a safety-related way.

8.4 Safety configuration

8.4.1 Order of IO data types

The IO Data of the SPDU shall be sorted according to Table 23:

Table 23 – Order of IO data types

Order	IO Data type name	
1	Float32+Unsigned8 (use as bits)	[=PA data type "composite"]
2	Unsigned8 (use as bits) + Unsigned8 (use as bits)	[=PA data type]
3	Unsigned8 (use as bits)	[=DI, DO]
4	Integer16	[=AI, AO]
5	Integer32	
6	Float32	

If a data type is not present the others shift up.

8.4.2 Securing the safety IO data description

The F-IO data structure is described in the "IOData" section of the GSD file. One attribute is the "F_IO_StructureDescCRC". This CRC is built across the attributes in Table 24 in the listed order (Version 2). The 32 bit CRC polynomial (*0xF4ACFB13*) shall be used to calculate the signature. Permitted data types for FSCP 3/1 are listed in 5.5.3. The previous version 1 of the IO data structure item set did not comprise the attribute VERSION and the data types Integer32 and Unsigned8+Unsigned8. Thus, no keyword F_IO_StructureDescVersion in a particular GSD file indicates the data types Integer32 and Unsigned8+Unsigned8 are not available, the F_IO_StructureDescCRC signature shall be calculated using the 16 bit CRC polynomial (*0x4EAB*), and the length of the CRC signature is 2 octets.

All octets of "COUNT_PS_INPUT_BYTES_BOOL_MAX" without the one with the highest address count as "8" bool in COUNT_PS_INPUT_CHANNELS_BOOL_MAX. All octets of "COUNT_PS_OUTPUT_BYTES_BOOL" without the one with the highest address count as "8" bool in COUNT_PS_OUTPUT_CHANNELS_BOOL. Only the one octet with the highest address may count with less than 8 bool if the channels with the highest bit address are unused.

In case some boolean channels are not used by the F-Submodule, the F-Submodule shall set the value to 0 (FVi, FVo) for these channels.

The parameter "F_IO_StructureDescCRC" is not transmitted to the F-Submodule at start-up time. The Host engineering tool shall check F_IO_StructureDescCRC to ensure correct representation in F-Host.

Table 24 – IO data structure items

Attribute name	Length	Description
F_IO_StructureDescVERSION	1 octet	Indicates a particular set of IO data structure items. This attribute is available for Version 2 or higher.
IN_ADDRESS_RANGE	2 octets	Length in octets of the whole IOData Input section (including F_MessageTrailer)
COUNT_PS_INPUT_BYTES_COMPOSITE	2 octets	Input: Length of all "Float32+Unsigned8" DataItems (5 × number of)
COUNT_PS_INPUT_BYTES_U8_U8	2 octets	Input: Length of all "Unsigned8+Unsigned8" DataItems (2 × number of)
COUNT_PS_INPUT_CHANNELS_BOOL_MAX	2 octets	Input: Number of all bool channels ("used as bits") in maximum mode (for example 1oo1 mode)
COUNT_PS_INPUT_BYTES_BOOL_MAX	2 octets	Input: Length of all bool DataItems (in octets) in maximum mode (for example 1oo1 mode)
COUNT_PS_INPUT_CHANNELS_INT	2 octets	Input: Number of all Integer16 DataItems
COUNT_PS_INPUT_CHANNELS_DINT	2 octets	Input: Number of all Integer32 DataItems
COUNT_PS_INPUT_CHANNELS_REAL	2 octets	Input: Number of all Float32 DataItems
OUT_ADDRESS_RANGE	2 octets	Length in octets of the whole IOData Output section (including F_MessageTrailer)
COUNT_PS_OUTPUT_BYTES_COMPOSITE	2 octets	Output: Length of all "Float32+Unsigned8" DataItems (5 × number of)
COUNT_PS_OUTPUT_BYTES_U8_U8	2 octets	Output: Length of all "Unsigned8+Unsigned8" DataItems (2 × number of)
COUNT_PS_OUTPUT_CHANNELS_BOOL	2 octets	Output: Number of all bool channels ("used as bits")
COUNT_PS_OUTPUT_BYTES_BOOL	2 octets	Output: Length of all Bool DataItems (in octets)
COUNT_PS_OUTPUT_CHANNELS_INT	2 octets	Output: Number of all Integer16 DataItems
COUNT_PS_OUTPUT_CHANNELS_DINT	2 octets	Output: Number of all Integer32 DataItems
COUNT_PS_OUTPUT_CHANNELS_REAL	2 octets	Output: Number of all Float32 DataItems

8.4.3 DataItem data type section examples

8.4.3.1 Approach

Subclauses 8.4.3.2 to 8.4.3.5 contain example DataItem sections according to some F-Host Channel driver types in 8.5.2 using the attributes described in Table 24. These example DataItem sections refer to F_CRC_Seed = 1.

Permitted data types for FSCP 3/1 are listed in 5.5.3.

NOTE F_Passivation =1 ("Channel") is only used in conjunction with [56], which contains additional examples

8.4.3.2 F_IN_OUT_1

Input: 32 bit Boolean
Output: 32 bit Boolean

The coding of the DataItem section for the F_IN_OUT_1 F-Host Channel driver example is shown in Table 25 and Table 26. Table 24 contains a description of the variables.

Table 25 – DataItem section for F_IN_OUT_1

```
<IOData>
        <Input Consistency="All items consistency">
                <DataItem DataType="Unsigned8" UseAsBits="true", TextId="Inputs" />
                <DataItem DataType="Unsigned8" UseAsBits="true", TextId="Inputs" />
                <DataItem DataType="Unsigned8" UseAsBits="true", TextId="Inputs" />
                <DataItem DataType="Unsigned8" UseAsBits="true", TextId="Inputs" />
                <DataItem DataType="F_MessageTrailer5Byte" TextId="Safety" />
        </Input>
        <Output Consistency="All items consistency">
                <DataItem DataType="Unsigned8" UseAsBits="true", TextId="Outputs" />
                <DataItem DataType="Unsigned8" UseAsBits="true", TextId="Outputs" />
                <DataItem DataType="Unsigned8" UseAsBits="true", TextId="Outputs" />
                <DataItem DataType="Unsigned8" UseAsBits="true", TextId="Outputs" />
                <DataItem DataType="F_MessageTrailer5Byte" TextId="Safety" />
        </Output>
</IOData>
```

Table 26 – DATA_STRUCTURE_CRC for F_IN_OUT_1

VERSION	02
IN_ADDRESS_RANGE	09
COUNT_PS_INPUT_BYTES_COMPOSITE	00
COUNT_PS_INPUT_BYTES_U8_U8	00
COUNT_PS_INPUT_CHANNELS_BOOL_MAX	32
COUNT_PS_INPUT_BYTES_BOOL_MAX	04
COUNT_PS_INPUT_CHANNELS_INT	00
COUNT_PS_INPUT_CHANNELS_DINT	00
COUNT_PS_INPUT_CHANNELS_REAL	00
OUT_ADDRESS_RANGE	09
COUNT_PS_OUTPUT_BYTES_COMPOSITE	00
COUNT_PS_OUTPUT_BYTES_U8_U8	00
COUNT_PS_OUTPUT_CHANNELS_BOOL	32
COUNT_PS_OUTPUT_BYTES_BOOL	04
COUNT_PS_OUTPUT_CHANNELS_ INT	00
COUNT_PS_OUTPUT_CHANNELS_DINT	00
COUNT_PS_OUTPUT_CHANNELS_ REAL	00
F_IO_StructureDescCRC	0x278AB2E8

8.4.3.3 F_IN_OUT_2

Input: 16 bit Boolean, 16 bit Integer; Output: 16 bit Boolean, 16 bit Integer. The coding for the F_IN_OUT_2 F-Host Channel driver example is shown in Table 27 and Table 28.

Table 27 – DataItem section for F_IN_OUT_2

```
<IOData>
        <Input Consistency="All items consistency">
                <DataItem DataType="Unsigned8" UseAsBits="true", TextId="Inputs" />
                <DataItem DataType="Unsigned8" UseAsBits="true", TextId="Inputs" />
                <DataItem DataType="Integer16" UseAsBits="false", TextId="AI channel" />
                <DataItem DataType="F_MessageTrailer5Byte", TextId="Safety" />
        </Input>
        <Output Consistency="All items consistency">
                <DataItem DataType="Unsigned8" UseAsBits="true" TextId="Outputs" />
                <DataItem DataType="Unsigned8" UseAsBits="true", TextId="Outputs" />
                <DataItem DataType="Integer16" UseAsBits="false", TextId="AO channel" />
                <DataItem DataType="F_MessageTrailer5Byte", TextId="Safety" />

        /Output>
</IOData>
```

Table 28 – DATA_STRUCTURE_CRC for F_IN_OUT_2

VERSION	02
IN_ADDRESS_RANGE	09
COUNT_PS_INPUT_BYTES_COMPOSITE	00
COUNT_PS_INPUT_BYTES_U8_U8	00
COUNT_PS_INPUT_CHANNELS_BOOL_MAX	16
COUNT_PS_INPUT_BYTES_BOOL_MAX	02
COUNT_PS_INPUT_CHANNELS_INT	01
COUNT_PS_INPUT_CHANNELS_DINT	00
COUNT_PS_INPUT_CHANNELS_REAL	00
OUT_ADDRESS_RANGE	09
COUNT_PS_OUTPUT_BYTES_COMPOSITE	00
COUNT_PS_OUTPUT_BYTES_U8_U8	00
COUNT_PS_OUTPUT_CHANNELS_BOOL	16
COUNT_PS_OUTPUT_BYTES_BOOL	02
COUNT_PS_OUTPUT_CHANNELS_ INT	01
COUNT_PS_OUTPUT_CHANNELS_DINT	00
COUNT_PS_OUTPUT_CHANNELS_ REAL	00
F_IO_StructureDescCRC	0x3B1CA2F0

8.4.3.4 F_IN_OUT_5

Input: Composite (Float32+Unsigned8). The coding for the F_IN_OUT_5 F-Host Channel driver example is shown in Table 29 and Table 30.

Table 29 – DataItem section for F_IN_OUT_5

```
<IOData>
        <Input Consistency="All items consistency">
                <DataItem DataType="Float32+Unsigned8" TextId="AI channel" />
                <DataItem DataType="F_MessageTrailer5Byte" TextId="Safety" />
        </Input>
        <Output Consistency="All items consistency">
                <DataItem DataType="F_MessageTrailer5Byte" TextId="Safety" />
        </Output>
</IOData>
```

Table 30 – DATA_STRUCTURE_CRC for F_IN_OUT_5

VERSION	02
IN_ADDRESS_RANGE	10
COUNT_PS_INPUT_BYTES_COMPOSITE	05
COUNT_PS_INPUT_CHANNELS_BOOL_MAX	00
COUNT_PS_INPUT_BYTES_BOOL_MAX	00
COUNT_PS_INPUT_CHANNELS_INT	00
COUNT_PS_INPUT_CHANNELS_DINT	00
COUNT_PS_INPUT_CHANNELS_REAL	00
OUT_ADDRESS_RANGE	05
COUNT_PS_OUTPUT_BYTES_COMPOSITE	00
COUNT_PS_OUTPUT_CHANNELS_BOOL	00
COUNT_PS_OUTPUT_BYTES_BOOL	00
COUNT_PS_OUTPUT_CHANNELS_ INT	00
COUNT_PS_OUTPUT_CHANNELS_DINT	00
COUNT_PS_OUTPUT_CHANNELS_ REAL	00
F_IO_StructureDescCRC	0xDD243507

8.4.3.5 F_IN_OUT_6

Input:
Readback (Float32 + Unsigned8),
Checkback (Unsigned8 + Unsigned8 + Unsigned8)

Output:
Setpoint (Float32 + Unsigned8)

The coding of the DataItem section for the F_IN_OUT_6 F-Host Channel driver example is shown in Table 31 and Table 32. Table 24 contains a description of the variables.

Table 31 – DataItem section for F_IN_OUT_6

```
<IOData>
        <Input Consistency="All items consistency">
                <DataItem DataType="Float32+Unsigned8" TextId="AI channel" />
                <DataItem DataType="Unsigned8" UseAsBits=" true " TextId="Status1" />
                <DataItem DataType="Unsigned8" UseAsBits=" true " TextId="Status2" />
                <DataItem DataType="Unsigned8" UseAsBits=" true " TextId="Status3" />
                <DataItem DataType="F_MessageTrailer5Byte" TextId="Safety" />
        </Input>
        <Output Consistency="All items consistency">
                <DataItem DataType="Float32+Unsigned8" TextId="AO channel" />
                <DataItem DataType="F_MessageTrailer5Byte" TextId="Safety" />
        </Output>
</IOData>
```

Table 32 – DATA_STRUCTURE_CRC for F_IN_OUT_6

VERSION	02
IN_ADDRESS_RANGE	13
COUNT_PS_INPUT_BYTES_COMPOSITE	05
COUNT_PS_INPUT_CHANNELS_BOOL_MAX	24
COUNT_PS_INPUT_BYTES_BOOL_MAX	03
COUNT_PS_INPUT_CHANNELS_INT	00
COUNT_PS_INPUT_CHANNELS_DINT	00
COUNT_PS_INPUT_CHANNELS_REAL	00
OUT_ADDRESS_RANGE	10
COUNT_PS_OUTPUT_BYTES_COMPOSITE	05
COUNT_PS_OUTPUT_CHANNELS_BOOL	00
COUNT_PS_OUTPUT_BYTES_BOOL	00
COUNT_PS_OUTPUT_CHANNELS_ INT	00
COUNT_PS_OUTPUT_CHANNELS_DINT	00
COUNT_PS_OUTPUT_CHANNELS REAL	00
F_IO_StructureDescCRC	0x8B927FCC

8.5 Data type information usage

8.5.1 F-Host Channel driver

The F-IO data cyclically transferred in SPDUs between an F-Device driver and an F-Host driver need to be controlled by an application program.

Usually, a programmer expects discrete logically addressable input or output variables (for example in case of the "ladder logic" programming language) that correspond directly to a so-called process image.

In case of more complex F-(Sub)Modules the programmer expects appropriate Function Blocks ("F-Host Channel driver") within tool libraries that can be embedded into the customer program.

Figure 51 illustrates such a programmer's view on "F-Host Channel driver" function blocks.

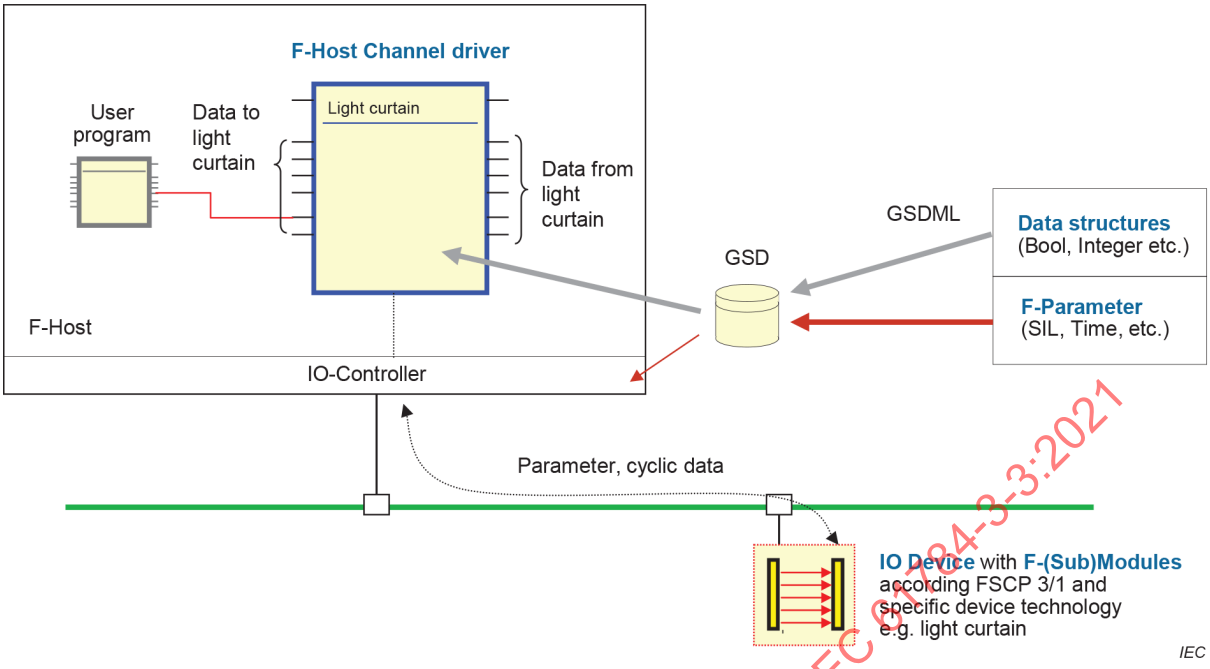


Figure 51 – F-Host Channel driver as "glue" between F-(Sub)Module and application program

8.5.2 Rules for standard F-Host Channel drivers

General system support from all kinds of F-Host types can be achieved by following a set of rules for the design of the F IO data structures:

- The F IO data structure shall be described in the IODataSection of the GSD file. See detailed description in 8.3.2.
- A composed data structure shall have the order according 8.4.1.

Table 33 contains a liast of sample F-Host Channel drivers. The drivers represent different F-Input and F-Output data structures according to the associated safety PDUs. The permitted data types for FSCP 3/1 are listed in 5.5.3. Thus, 32 Boolean values shall be mapped into data type 4 × Unsigned8 and 1 × 8 bit into the data type 1 × Unsigned8. See 8.4.3 for details.

Table 33 – Sample F-Host Channel drivers

F-Host Channel driver configuration[a]	F-Input (from device)	F-Output (to device)	Remarks
F_IN_OUT_1	32 Boolean,	32 Boolean,	for example light curtains
F_IN_OUT_2	16 Boolean, 1 Integer16	16 Boolean, 1 Integer16	for example laser scanners
F_IN_OUT_5	1 Float32, Unsigned8 (8 bit "Qualifier")		for example pressure transmitter
F_IN_OUT_6	"Readback": 1 Float32, 8 bit "Checkback": 24 bit	"Setpoint": 1 Float32, 8 bit	for example pneumatic valve

[a] The numbering does not necessarily mean different drivers. It can be one driver parameterized via GSD information.

Constraints:

- unused bits shall be set to "0";
- status and fault indications (qualifier) of an F-(Sub)Module can be defined according [56].

8.5.3 Recommendations for the use of F-Host Channel drivers

Figure 52 shows a layout example of an F-Host Channel driver for a F-(Sub)Module.

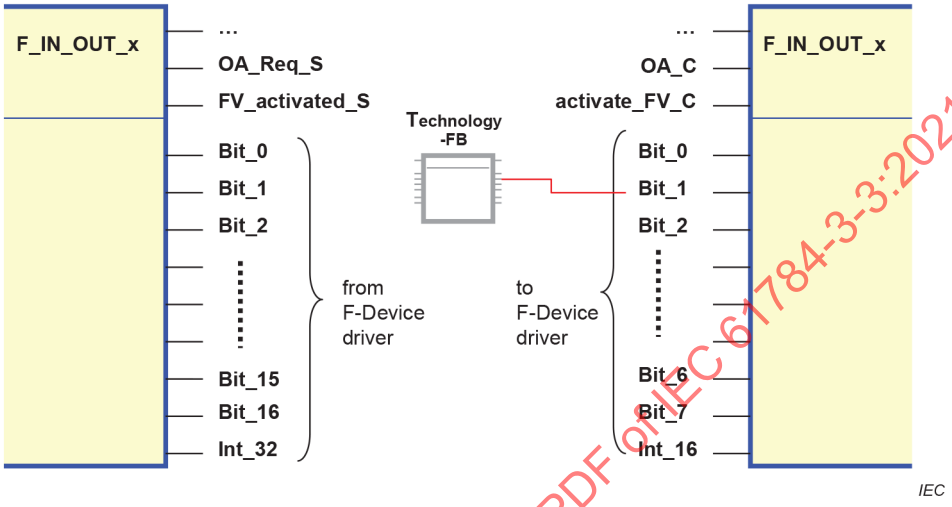


Figure 52 – Layout example of an F-Host Channel driver

The terms used in Figure 52 and the driver behaviors are specified below:

OA_C	Operator Acknowledgment (for resumption after fault)
OA_Req_S	When fault (Timeout or CRC2) detected and removed
FV_activated_S	Fail-safe values activated by F-Device driver
activate_FV_C	Fail-safe values to be activated within F-(Sub)Module
Fixed behavior of F-Host Channel driver	Fail-safe values set to "0"

In addition to the F-(Sub)Module specific data structures there are some more FSCP 3/1 signals that are available to the programmer. See 7.1.3 "Status and Control Byte" and 6.1 for detailed information on the above-mentioned signals.

For performance reasons the F-Host Channel driver may be split into two function blocks, one for inputs and one for outputs (Figure 52).

There is a fixed behavior of the F-Host Channel drivers in respect to fail-safe values: whether the data structure consists of bit (Unsigned8), Integer16, Float32 or Float32 + Unsigned8, every value is set to "0".

If actuators cannot agree to FV = "0", other values may be implemented either hard-coded or via iParameters. Application programs may activate these device specific fail-safe values via bit 4 within the Control Byte (see 7.1.3).

If sensors cannot agree to FV = "0", additional application program logic may turn them into individual values using the "activate_ FV_C" input of the F-Host Channel driver.

8.6 Safety parameter assignment mechanisms

8.6.1 F-Parameter assignment

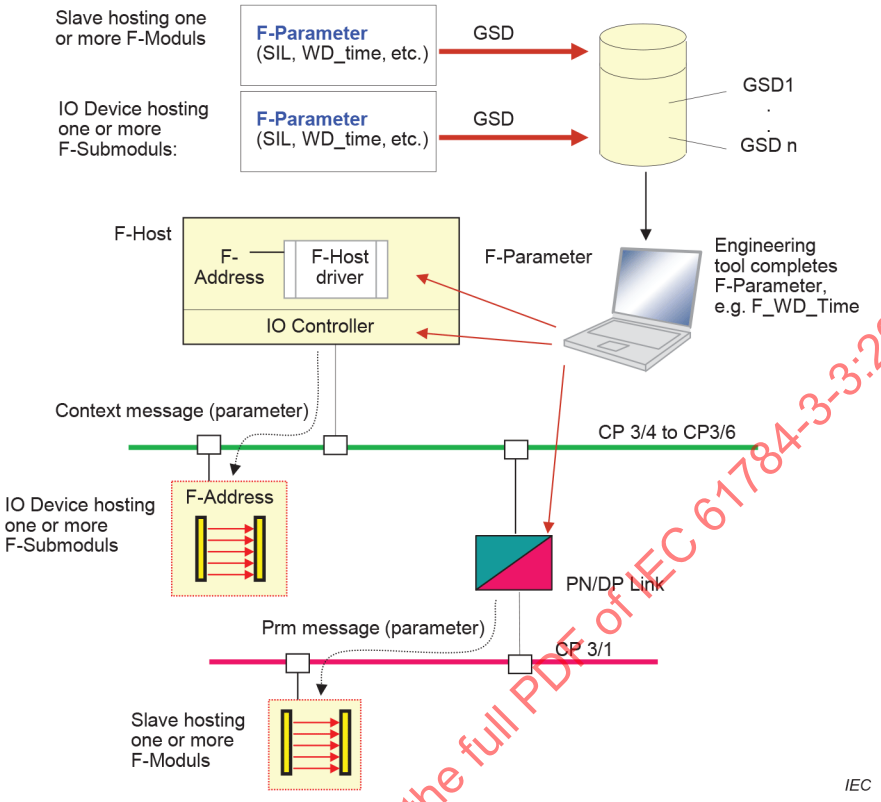


Figure 53 – F-Parameter assignment for F-(Sub)Modules

Simple F-(Sub)Modules without iParameters can be supplied via the standard connection establishment and start-up parameterization path. See IEC 61158-5-10, IEC 61158-6-10. The total amount of F-Parameters hereby cannot exceed the upper limit for CP 3/1 of 234 octets (Figure 53).

8.6.2 General iParameter assignment

For complex F-(Sub)Modules with iParameters a (safety) decision shall be made whether an automatic start-up assignment is favored over a separate assignment from a dedicated CPD-Tool for the particular F-(Sub)Module as requested in IEC 62061. In each case the F-Host shall deblock the assignment only, if there is no hazardous process state. Principally, three ways are possible that can complement each other:

- iParameter value assignment through a dedicated CPD-Tool using DeviceAccess (Engineering tool/PC).
- iParameter value assignment via iPar Server in an F-Host and an appropriate iParameter data set;
- iParameter as part of the Start-up parameter.

8.6.3 System integration requirements for iParameterization tools

Table 34 contains a list of requirements to be fulfilled for iParameterization procedures.

Table 34 – Requirements for iParameterization

No.	System requirement	Scope
R1	CPD-Tool to be designed for compatible personal computers or laptops and operating systems WINDOWS	CPD-Tool
R2	Several CPD-Tools or instances of CPD-Tools should be able to run concurrently	Host-Engineering
R3	Authorization (roles and access rights) should be supported by Host-Engineering- and CPD-Tool	Host-Engineering- and CPD-Tool
R4	Download of iParameters to the IO Device hosting F-Submodules: octet stream of iParameters should be defined such that it can be stored within the IO-Controller and transferred to the F-(Sub)Module upon start-up parameterization.	Host mandatory support of iPar Server
R5	Printout: It should be possible to "remote control" the individual CPD-Tools from the Host-Engineering-Tool for batch printing or to deliver the printout in a standardized format (for example HTML) to the Host-Engineering-Tool	Support of TCI
R6	Download of iParameters: It should be possible to use the dedicated CPD-Tools from the Host-Engineering-Tool for "iParameterization" " by two possibilities: a) The iParameter are specified in GSD. The iParameter are transferred from the Host engineering to the CPD with the help of TPF. The CPD Tool calculates the iPar_CRC. This iPar_CRC can be transferred manually to the F-Parameter. The F-Host engineering and the CPD Tool need the TCI conformance class 2 (i.e. the TPF shall be generated/interpreted) b) The iParameter are known and parameterized by the CPD Tool only and transferred to the F-Submodule by the CPD Tool. The CPD Tool calculates the iPar_CRC. This iPar_CRC can be transferred manually to the F-Parameter. The F-Host engineering and the CPD Tool need the TCI conformance class 2 (i.e. provide and use communication server)	Support of TCI class 3
R7	The submission of symbol names is possible with the GSD file of CP 3/4 to CP 3/6 by using the TPF which shows the path to the GSD in the F-Host engineering.	Support of TCI class 2
R8	In order to achieve independence from the underlying black channel, the same securing principle for the transmission of iParameter data shall be used as for the SPDUs described in Figure 24 and the associated clause, i.e. calculation of the iPar CRC32 shall be in reverse octet order (the initial value shall not be zero). A manufacturer can use his own method to secure the iParameters as long as the criteria are fulfilled (iPar-Server, CPD-Tool)	Calculation of iPar-CRC

Figure 54 illustrates the system aspects of the CPD-Tool-Integration.

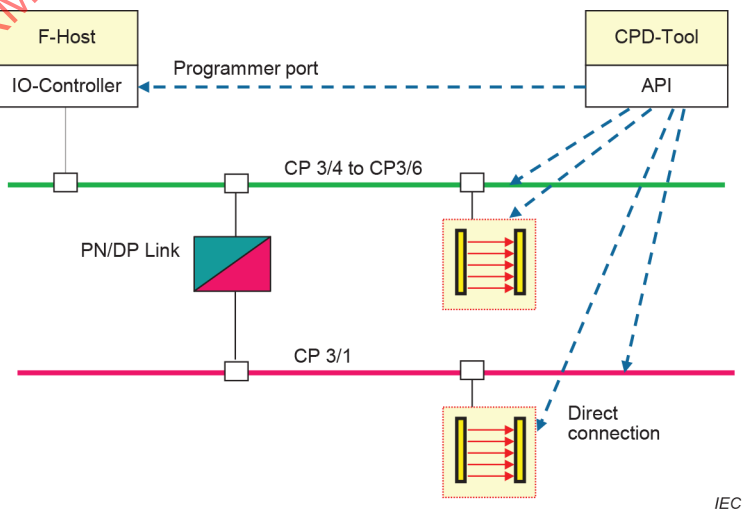


Figure 54 – System integration of CPD-Tools

The CPD-Tool may be either connected to:

- the IO Device hosting F-Submodules directly (for example USB, RS232);
- the Ethernet or to the CP 3/4 to CP 3/6

The CPD-Tool can use TCI.

The Engineering System of the F-Host / IO-Controller shall support TCI Conformance Class C2 for CP 3/4 to CP 3/6. See [63].

NOTE 1 TCI is mainly used so send iParameters edited in the Engineering System to the vendor specific CPD Tool. The CPD Tool uses a vendor specific algorithm to calculate the iPar_CRC value. The user has to key this value in the Engineering System for the F_iPar_CRC by hand.

NOTE 2 Instead of the Conformance Class C3 the vendor-specific, IP-based communication between CPD Tool and the "CP 3/4 to CP 3/6 Device" could be used. See Chapter 5.10. of the document "Implementation Guideline Tool Calling Interface Version 1.1".

8.6.4 iPar-Server

8.6.4.1 General description and constraints

The iPar-Server concept is a specialized form of the more general Proxy-FB concept. It is the responsibility of F-Host manufacturers to provide this feature as stated in Table 44, be it realized within the non-safety part of an F-Host as the parameterization master or within a controlled subsystem such as a non-safety PLC or an industrial computer on the same network. [55] supersedes the non-safety-related part of the following specification.

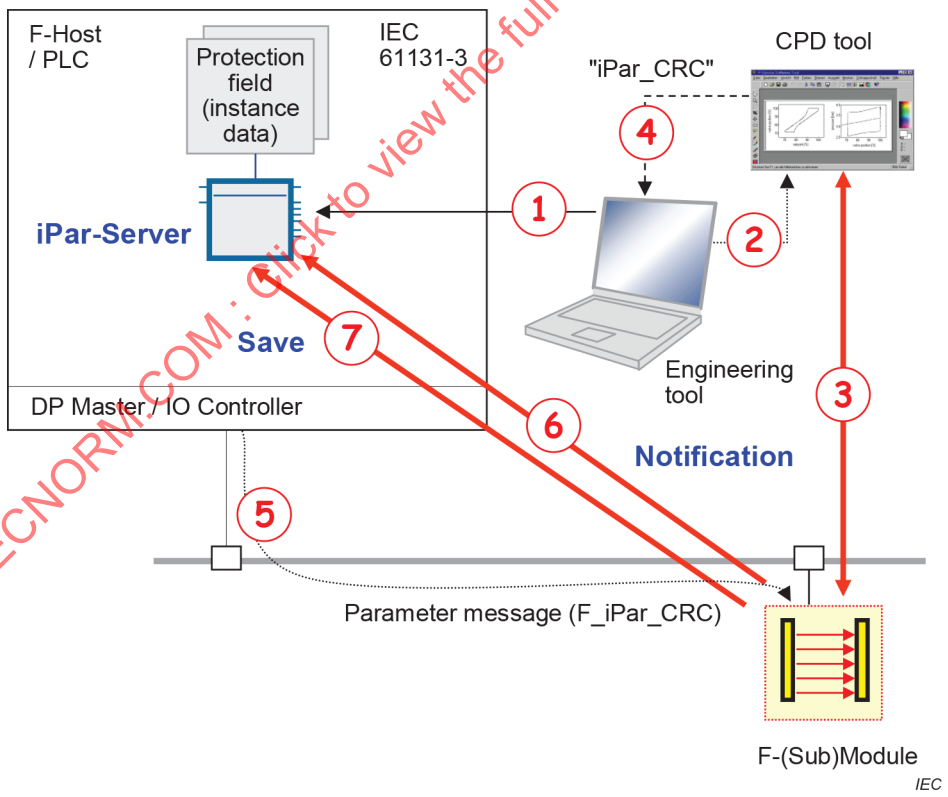


Figure 55 – iPar-Server mechanism (commissioning)

Figure 55 demonstrates the basic procedure of the iPar-Server mechanism via an example. Together with the network configuration and F-Parameterization of an F-(Sub)Module, an associated iPar-Server function is instantiated (step 1).

The F-(Sub)Module is able to go in the data exchange mode using a safe state (FV). An associated CPD-Tool can be launched via an appropriate interface (step 2) from the engineering tool propagating at least the node address of the configured device.

Parameterization, commissioning, test, etc. can be executed with the help of the CPD-Tool (step 3).

After finalization, the iPar_CRC signature is being calculated and displayed in hexadecimal form for at least copying and pasting of this value into the "F_iPar_CRC" entry field of the configuration part of the engineering tool (step 4).

A restart of the F-(Sub)Module is necessary to transfer the "F_iPar_CRC" parameter into the F-(Sub)Module (step 5).

After final verification and release the F-(Sub)Module is enabled to initiate an upload notification (step 6) to its iPar-Server instance. It thereby uses the diagnosis means of CPF 3 (8.6.4.2 and [39]).

The iPar-Server is polling the diagnosis information to interpret the request (R) and to establish the upload process (step 7) which stores the iParameters as instance data within the iPar-Server host.

Figure 56 shows the second part of the iPar-Server mechanism. In case of the replacement of a defect F-(Sub)Module (step 1) the F-(Sub)Module receives its F-Parameters including the "F_iPar_CRC" (step 2) at start-up.

As iParameters normally are missing in a replacement or non-remanent F-(Sub)Module it initiates a download notification (step 3) to its iPar-Server instance. It thereby uses the diagnosis means of CPF 3 (8.6.4.2 and [39]).

The iPar-Server is polling the diagnosis information to interpret the request (R) and to establish the download process (step 4). Through this transfer the F-(Sub)Module is enabled to provide the original functionality without further engineering or CPD-Tools.

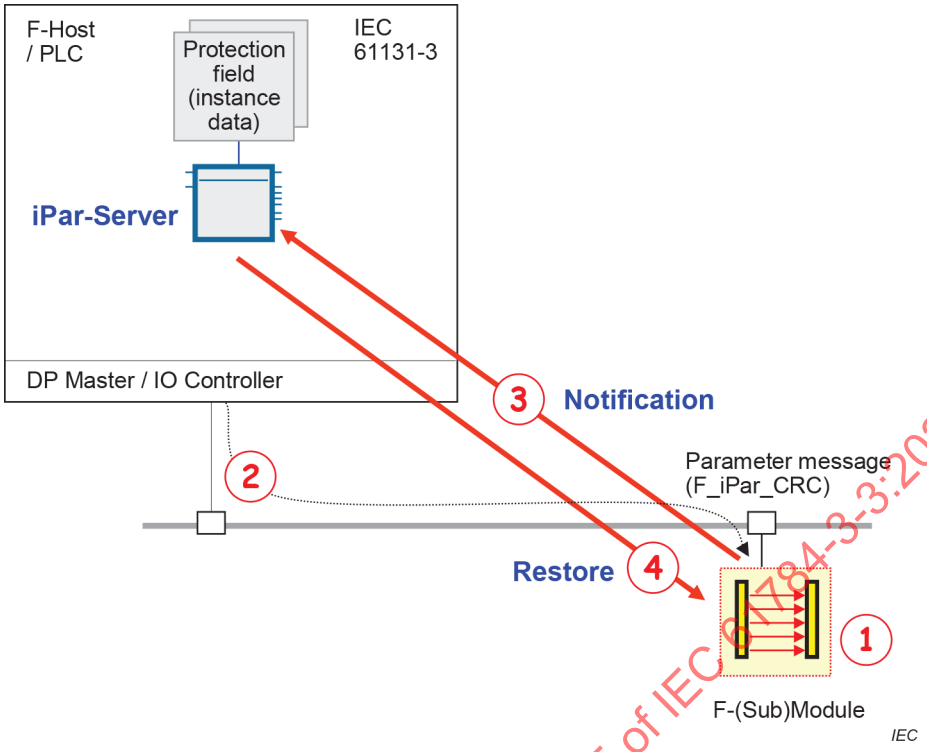


Figure 56 – iPar-Server mechanism (for example F-(Sub)Module replacement)

The following constraints have been identified for the iPar-Server mechanism.

- Each iPar-Server instance shall support a minimum of 2^{15}-1 octets of iParameters per Codename.
- The iParameters are stored as one fixed block of data as shown in Figure 48.
- The iPar-Server is not safety-related. It can be implemented or launched within a standard host or within the standard part of an F-Host (Figure 56).
- It is the responsibility of the F-(Sub)Module manufacturer that the downloaded iParameter set matches for example the correct type and version of the replacement device.
- An F-(Sub)Module only shall initiate an iPar-Server-Request when the black channel guarantees delivery of the notification.
- One repetition is permitted whenever a "Restore" attempt failed. The associated safety function remains in safe state (FV).
- "Restore" shall only be executed upon start-up of the PLC-system and/or F-(Sub)Module.

8.6.4.2 Notification

8.6.4.2.1 Case CP3/1 or CP3/2

The only standard mechanism for an F-Slave/F-Module to notify the iPar-Server on CPF 3 type networks is via a diagnosis message. However, in contrast to the standard diagnosis context the iPar-Server notification does not need information propagation to any visualization tool for maintenance interaction. Out of several different types on CP 3/1 and CP 3/2, specified in IEC 61158-5-3, the coding relates to the "Status Model" [40]. In order to avoid conflicts with already existing types a new status type "iPar-Server Request" (type = 7) has been defined within a previously reserved range.

NOTE The "Update Alarm" (type = 6) has not been chosen as this type normally leads to a display of the alarm information and follows another semantic. It is an objective of FSCP 3/1 to specify codings for the two diagnosis message types for CP 3/1, CP 3/2, and CP 3/4 to CP 3/6 as close as possible such that an F-Module inside a remote IO does not have to know its deployment.

Figure 57 shows the iPar-Server request coding for CP 3/1 and CP 3/2.

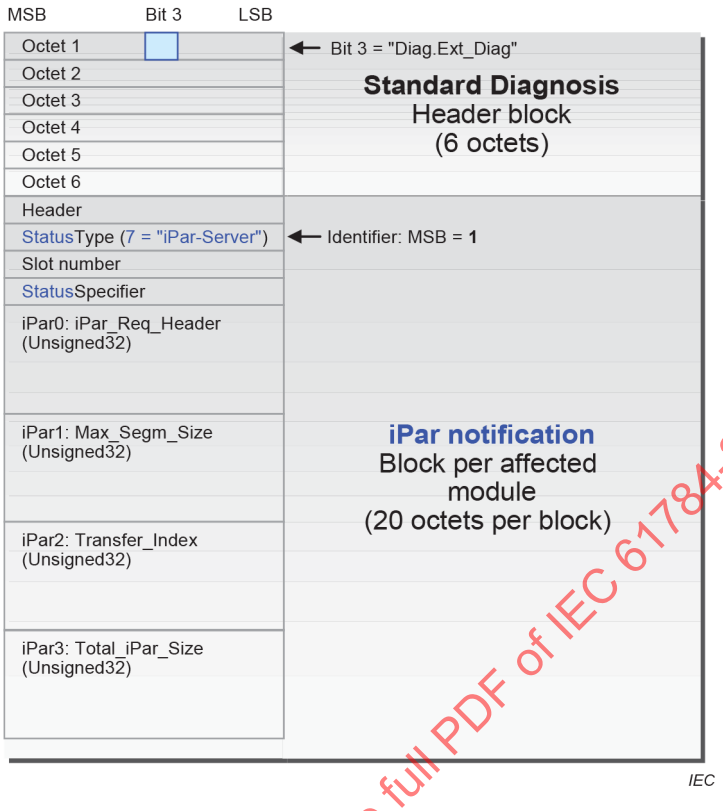


Figure 57 – iPar-Server request coding ("status model")

Each coding of the "iPar-Server Request" starts with the six mandatory octets of the standard diagnosis block. The "Diag.ext.diag" flag (bit 3 of the first octet) shall not be impacted as no LED indicator shall be light up if no defect is to be reported. The next four octets are following the standard coding as described in IEC 61158-5-3 and in Figure 57. Status type is the new "iPar-Server Request" (7). The Status specifier shall be set "0". The body of the "iPar-Server Request" contains the specifiers as defined in Table 35.

An F-Module within a remote IO always uses the coding of Figure 57 or an appropriate subset, whenever it can be deployed in a CP 3/1 remote IO. A remote IO shall only cast one notification at a time and thus save or restore iParameters F-Module by F-Module. Design hints for cases of diagnosis congestion (e.g. "Diag.Ext_Diag_Overflow") can be found in [40].

NOTE The coding of the information transfer between a module and its head station is not standardized.

It is the task of the headstation of a remote IO to transform the iPar-Server request coding into the appropriate format of the actual communication profile (Figure 57 or Figure 59).

Table 35 – Specifier for the iPar-Server Request

iPar specifier	Name	Octet 3	Octet 2	Octet 1	Octet 0	Definition
iPar0	iPar_Req_Header	SR_Version	Reserved	N_Count	SR_Type	Type of iPar-Server request (Unsigned32)
iPar1	Max_Segm_Size	0x00	0x00	0x00	0 to 234	Maximum permitted net size of a segment in octets (Unsigned32)
iPar2	Transfer_Index	0x00	0x00	0x00	0 to 254 (255)	Index for the read/write record transfer (Unsigned32)
iPar3	Total_iPar_Size					Total length of iParameter octets (Unsigned32)

Reserved: See 3.3.

The parameter "Max_Segm_Size" may be larger than 234 octets with CP 3/4 to CP 3/6. It can comprise up to 2^{22}-1 octets due to FSCP 3/1 restrictions.

A "Transfer_Index" of 255 may conflict with other services such as a CALL of I&M functions.

The parameter "Transfer_Index" may be larger than 255 with CP 3/4 to CP 3/6. It can go up to 65 535.

A replacement device will possibly not know the correct size of iParameter of its predecessor. In this case the notification for Restore may contain "Total_iPar_Size =0", which means the iPar-Server will download the complete iParameter data set.

N_Count is a sequence counter for notifications (for CP 3/1 and CP 3/2 only), counting from 1 to 15 and over again.

The parameter "SR_Version" shall be set to 0x01. The parameter "N_Count" shall start with "1" and be changed with each notification (only in case of CP 3/1 and CP 3/2) until the value 15 and continued with "1" all over again. The parameter "SR_Type" shall be coded as shown in Figure 58.

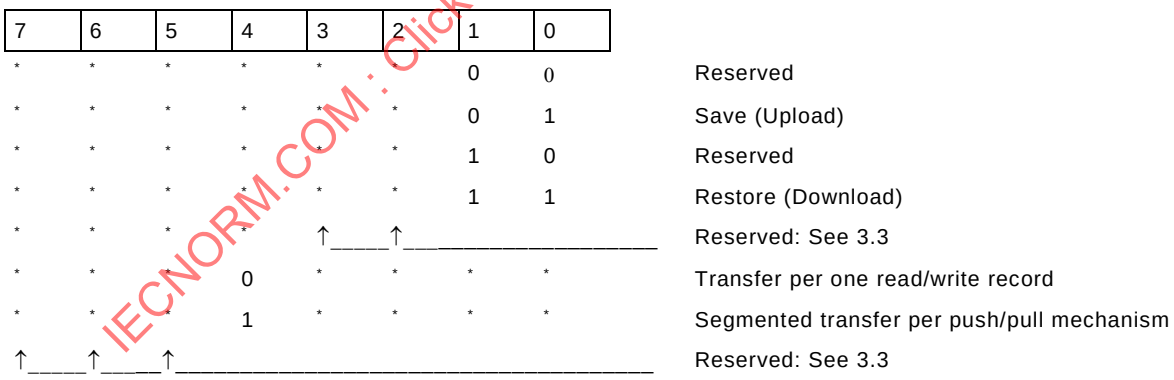


Figure 58 – Coding of SR_Type

A possible realization of the counterpart within for example the non-safety part of an F-Host is specified in [39] and called RDIAG communication function block.

8.6.4.2.2 Case CP3/4 to CP3/6

The coding on CP 3/4 to CP 3/6 for the iPar-Server relates to the "Alarm Model" and on the standard "Upload&Retrieval" alarm defined in IEC 61158-5-10 and IEC 61158-6-10. Figure 59 shows the iPar-Server request coding for CP 3/4 to CP 3/6.

After sending an iPar-Server request the (Sub)Module is waiting 2^{18} ms (approximately 4,4 minutes) for the "Save" or "Restore" service to be executed completely. After the expiration of this time, it launches an appropriate diagnosis message according to 6.3.2.

In case of an iPar-Server request for the "Restore" service and no stored iParameters, the iPar-Server shall send a record of length "0".

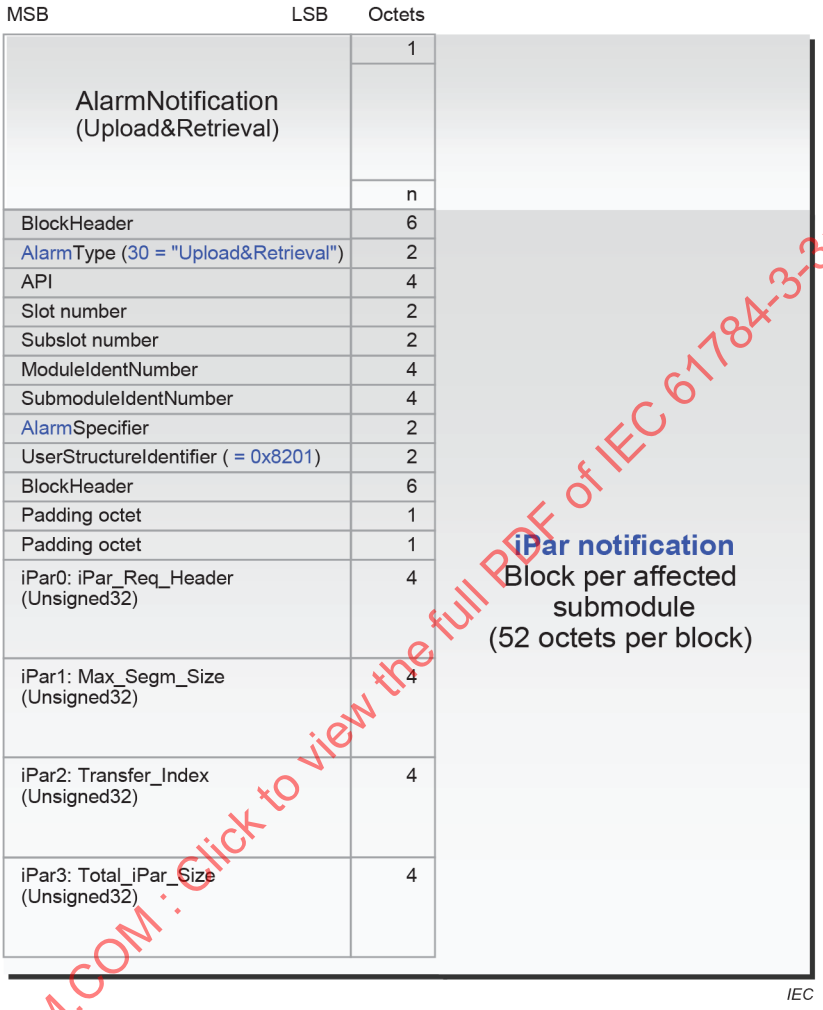


Figure 59 – iPar-Server request coding ("alarm model")

8.6.4.3 Services

The iPar-Server is a small program that is invoked at each main cycle for example within the non-safety-related part of an F-Host. It polls the diagnosis information of the particular F-Submodules, looking for any of the two kinds of requests "Save" and "Restore". In order to execute these requests it uses the standard "read record" and "write record" acyclic services as defined in IEC 61158-5-3. For small amounts of iParameters an ordinary unsegmented version per single "read record" and "write record" is sufficient (Table 36 and Table 37). A possible realization of these two functions based on IEC 61131-3 programming languages is specified in [39] and called RDREC and WRREC communication function blocks. It is highly recommended for F-Host systems to provide these function blocks within the library for its non-safety related part.

Table 36 – Structure of the Read_RES_PDU ("read record")

Structure of the Read_RES_PDU	Size	Coding	Notes	
Function_Num	1 octet	0x5E	Indicates "read", fix	Header
Slot_Number	1 octet	0 to 255	Location of module	
Index	1 octet	0 to 254	"Transfer_Index"	
Length of net data	1 octet	0 to 240	Length of iPar segment	
iParameter (segment)	n octets	-	n = 240 maximum per record	Data
NOTE Corresponding structures for CP 3/4 to CP 3/6 can be found in [39].				

Table 37 – Structure of the Write_REQ_PDU ("write record")

Structure of the Write_REQ_PDU	Size	Coding	Notes	
Function_Num	1 octet	0x5F	Indicates "write", fix	Header
Slot_Number	1 octet	0 to 255	Location of module	
Index	1 octet	0 to 254	"Transfer_Index"	
Length of net data	1 octet	0 to 240	Length of iParameter segment	
iParameter	n octets	-	n = 240 maximum	Data

For amounts of iParameters exceeding the record or buffer limit of a particular F-Slave/ F-Module an extended version of the "read record" and "write record" acyclic services can be used, specified in IEC 61158-5-3 as the so-called "Pull" and "Push" services (Table 38 and Table 39).

Table 38 – Structure of the Pull_RES_PDU ("Pull")

Structure of the Pull_RES_PDU	Size	Coding	Notes	
Function_Num	1 octet	0x5E	Indicates "Read", fix	Header
Slot_Number	1 octet	0 to 255	Location of module	
Index	1 octet	0 to 254 (255)	"Transfer_Index" [a]	
Length of net data	1 octet	0 to 240	Length of iPar segment + Load Region header	
Extended_Function_Num	1 octet	0x02	Indicates "Pull"	Load Region
Options	1 octet	Unsigned8	Flow control, see 6.2.17.2 in IEC 61158-5-3	
Sequence_Number	4 octets	Unsigned32	...of current iPar segment	
iParameter (segment)	n octets	Octet String	n = 234 maximum per record	Data

[a] A "Transfer_Index" of 255 complies in this case with IEC 61158-5-3. However, access conflicts with other services such as a CALL of I&M functions shall be considered in the design and implementation phase. All other indices can be used for the "Pull" and "Push" services.

Table 39 – Structure of the Push_REQ_PDU ("Push")

Structure of the Push_REQ_PDU	Size	Coding	Notes	
Function_Num	1 octet	0x5F	Indicates "Write", fix	Header
Slot_Number	1 octet	0 to 255	Location of module	
Index	1 octet	0 to 254 (255)	"Transfer_Index" [a]	
Length of net data	1 octet	0 to 240	Length of iPar segment + Load Region header	
Extended_Function_Num	1 octet	0x01	Indicates "Push"	Load Region
Options	1 octet	Unsigned8	Flow control, see 6.2.17.2 in IEC 61158-5-3	
Sequence_Number	4 octets	Unsigned32	...of current iPar segment	
iParameter (segment)	n octets	Octet String	n = 234 maximum per record	Data

[a] A "Transfer_Index" of 255 complies in this case with IEC 61158-5-3. However, access conflicts with other services such as a CALL of I&M functions shall be considered in the design and implementation phase. All other indices can be used for the "Pull" and "Push" services.

An F-Host or an associated non-safety system can provide the iPar-Server mechanism totally hidden for the user or as a set of library functions to be configured for a particular project.

An example for a standard parameter server is the "Upload&Retrieval" mechanism of CP 3/4 to CP 3/6 as defined in IEC 61158-5-10, IEC 61158-6-10, and IEC 61784-2.

An F-(Sub)Module within an IO Device always uses an appropriate coding, whenever it can be deployed in a CP 3/1 or CP 3/4 to CP 3/6 IO device.

The indices of records for "Save" (= upload) or "Restore" (= retrieval, download) services can differ. It also is possible for a "Restore" service to read a smaller amount of data than previously had been saved. This saved data can contain check information such as device type, data length, CRC signature, etc. in addition to the iParameter. A download of a short record with the check information allows for verifying data integrity and up-to-dateness without stressing the performance.

8.6.4.4 iPar Server State Machine

Figure 60 shows the iPar-Server state diagram and Table 40 describes the iPar-Server states, transitions, and internal items. See 7.2.2 on general information about UML2 notation.

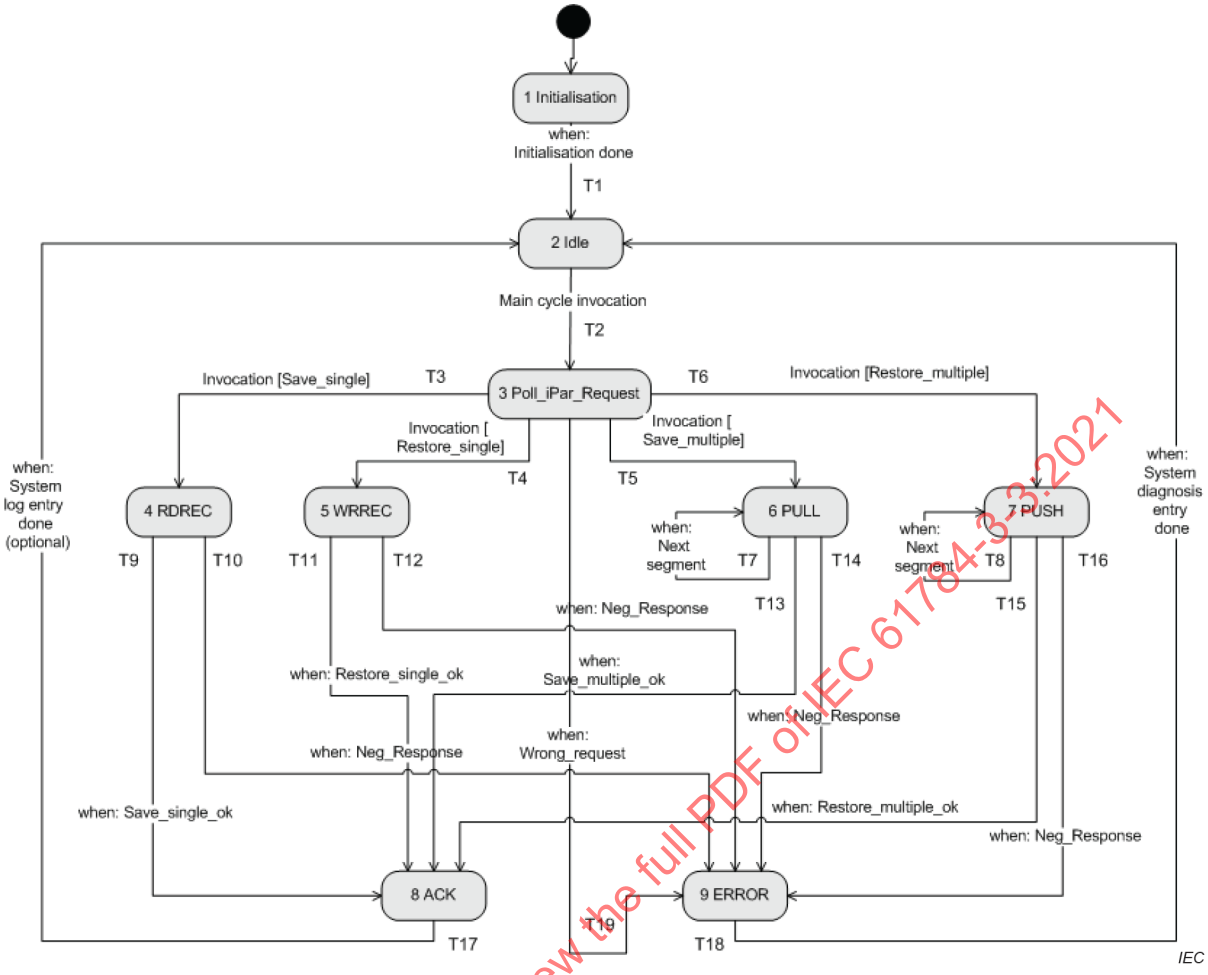


Figure 60 – iPar-Server state diagram

The terms used in Figure 60 are specified below:

Save_single	iPar-Server request to save (upload) an iParameter block per one single record (RDREC)
Restore_single	iPar-Server request to restore (download) an iParameter block per one single record (WRREC)
Save_multiple	iPar-Server request to save (upload) a larger iParameter block per multiple records (PULL)
Restore_multiple	iPar-Server request to restore (download) a larger iParameter block per multiple records (PUSH)
System log entry	Any successful save and restore action can be recorded in an iPar-Server log file (optional)
System diagnosis entry	Any unsuccessful save and restore action shall be reported via system diagnosis means
Neg_Response	Whenever a system function such as RDREC, WRREC, PULL, or PUSH aborts with an error, the iPar-Server shall create a system diagnosis entry
Incorrect_request	Whenever the iPar-Server discovers an incorrect request type or no reaction of any of the called system functions, it shall abort the action and create a system diagnosis entry

Table 40 – iPar-Server states and transitions

STATE NAME	STATE DESCRIPTION
1 Initialization	Cold start state; initialize outputs if defined
2 Idle	Idle state, no actions
3 Poll_iPar_Request	Upon main cycle invocation or similar activity in a controlled subsystem, the iPar-Server request within the body of the diagnosis information is interpreted and the corresponding system service shall be launched. In case of errors the ERROR state shall be entered
4 RDREC	Within this state the system function RDREC according [39] or a similar function shall be invoked that executes a read function according to the CP 3/1 or CP 3/2 in IEC 61158-5-3
5 WRREC	Within this state the system function WRREC according [39] or a similar function shall be invoked that executes a write function according to the CP 3/1 or CP 3/2 in IEC 61158-5-3
6 PULL	Within this state the system function PULL shall be invoked that executes a multiple read function via the "Extended_Function_Num" =0x02 according to the CP 3/1 or CP 3/2 in IEC 61158-5-3
7 PUSH	Within this state the system function PUSH shall be invoked that executes a multiple write function via the "Extended_Function_Num" =0x01 according to the CP 3/1 or CP 3/2 in IEC 61158-5-3
8 ACK	Within this state any successful save and restore action can be recorded in a "system iPar-Server log file" (optional)
9 ERROR	Whenever a system function such as RDREC, WRREC, PULL, or PUSH aborts with an error, or in case of an erroneous request, the iPar-Server shall create within this state a system diagnosis entry

TRAN-SITION	SOURCE STATE	TARGET STATE	ACTION
T1	1	2	-
T2	2	3	Main cycle invocation (or similar event in a controlled subsystem)
T3	3	4	Invocation of the RDREC function for the upload of a single iParameter block
T4	3	5	Invocation of the WRREC function for the download of a single iParameter block
T5	3	6	Invocation of the POLL function for the multiple upload of a segmented larger iParameter block
T6	3	7	Invocation of the PUSH function for the multiple download of a segmented larger iParameter block
T7	6	6	Start reading the next segment
T8	7	7	Start writing the next segment
T9	4	8	Start entry of a successful RDREC execution in the system log file (optional)
T10	4	9	Start system diagnosis entry
T11	5	8	Start entry of a successful WRREC execution in the system log file (optional)
T12	5	9	Start system diagnosis entry
T13	6	8	Start entry of a successful POLL execution in the system log file (optional)
T14	6	9	Start system diagnosis entry
T15	7	8	Start entry of a successful PUSH execution in the system log file (optional)
T16	7	9	Start system diagnosis entry
T17	8	2	Go to sleep (idle)
T18	9	2	Go to sleep (idle)
T19	3	9	Start system diagnosis entry

8.6.4.5 iPar-Server management

The iPar-Server management measures to ensure authenticity, validity and data integrity of the iParameters are listed in Table 41. It is the responsibility of the F-(Sub)Module to provide the safety measures for the save and restore mechanisms. The iPar-Server is just storing the iParameters as a stream of octets and can be a standard parameter server for non-safety-related devices also.

Table 41 – iPar-Server management measures

Item / phase	Clauses	Description
F_S/D_Address	8.1.2 7.3.7 9.1	The usage of the F_Source/Destination_Address or short F_S/D_Address is a precondition to ensure authenticity of the saved and restored iParameters. It is not necessary to include the F_S/D_Address in the iPar_CRC calculation or in the iParameter block. The correct delivery of the F_iPar_CRC is already secured by the F_S/D_Address so that an erroneously delivered iParameter block can be detected by comparing its iPar_CRC with the F_iPar_CRC. In case the F_S/D_Address is defined via a coding switch the replacement device shall be adjusted to the original F_S/D_Address prior to a restart. In case the F_S/D_Address is assigned via a CPD-Tool, it is the responsibility of the device manufacturer to provide the means for the adjustment of the original F_S/D_Address prior to a restart
Start-up	8.1.7 8.6.3 9.1	After start-up the F-(Sub)Module receives the F-Parameters to establish a CPF 3 communication (cyclic data exchange). The preset value of F_iPar_CRC is "0" thus guaranteeing the device is in a safe state and is sending FV (fail-safe values). The (green) LED is blinking with 2 Hz
Commissioning	-	In this phase the device can be configured and parameterized with the help of a CPD-Tool being directly connected or using acyclic communication services such as MS2. It is the responsibility of the device and the corresponding CPD-Tool manufacturer to ensure safely parameterization across these standard communication channels and to define the safety of the device while in FSCP test mode
iPar_CRC / F_iPar_CRC	8.2 8.3.3.2	The usage of the iPar_CRC and its diversely transmitted counterpart F_iPar_CRC is a precondition to ensure data integrity of the saved and restored iParameters. In case the calculated iPar_CRC signature in the CPD-Tool results in a "0" it shall be set to "1". This also applies for the iPar_CRC signature calculation within the F-(Sub)Module prior to a comparison with the F_iPar_CRC value which stems from the start-up parameterization
Manual propagation	8.1.7	The iPar_CRC is calculated within the CPD-Tool and shall be displayed in hexadecimal format. The user then can transfer this value manually into the "F_iPar_CRC" entry field of the engineering tool. This transfer can be done automatically if proven sufficiently safe
I&M functions	8.2	The validity of a particular iParameter set (block) for a device replacing a defect one can be checked for example via the identification and maintenance functions (I&M) "order number", "HW release", and "SW release". It is the responsibility of the device manufacturer to choose the right information for ensuring the validity
Verification	-	Usually the iParameter assignment phase is finalized by a particular test and verification step followed by a device "disconnect" and "reconnect" action, which causes a start-up and the transmission of the correct F_iPar_CRC
iPar-Server	-	An F-(Sub)Module shall only launch an iPar-Server request after successful start-up parameterization (F-Parameters)
LED indication	9.1	As long as the F-(Sub)Module did not accomplish to save its iParameters or while in FSCP test mode it shall indicate this state via the LED indicators described in 9.1. The blinking frequency in this case shall be 2 Hz

8.6.4.6 iParameter size in GSD

An F-(Sub)Module can indicate the maximum size of its iParameters via the keyword entry "Max_iParameter_Size" in its GSD file ("Max_iParameterSize" in GSDML). See [35] and [38] for details.

9 System requirements

9.1 Indicators and switches

In case of a fault that can be associated with a particular F-(Sub)Module the F-Host sets Control Bit 1 "Operator Acknowledgment requested" within the Control Byte (=1). This bit can be used to inform the user about three actions to start:

- checking of the equipment and if necessary its repair or replacement;
- verification of the safety function;
- Operator Acknowledgment (OA_C).

With compact IO-Devices hosting a virtual F-Submodule it is highly recommended to use an indicator LED (for example existing bicolor bus LED) that is blinking with 0,5 Hz in green mode (= bus communication ok but OA_C requested). With modular devices hosting physical F-Submodules a usually available "safe operation" LED at each module should be used that is blinking with 0,5 Hz in green mode (= safety communication ok but OA_C required). Implementation is *optional* for IO-Devices.

While in *FSCP test mode* or as long as the F-(Sub)Module did not accomplish to save its iParameters the indicator LED or "safe operation" LED shall indicate this state by blinking with 2 Hz in green mode.

Subclauses 7.3.7 and 8.1.2 provide information on how to enter the F_S/D_Address of F-(Sub)Module via switches.

9.2 Installation guidelines

The installation guidelines of IEC 61918 and the CPF 3 specific amendments in IEC 61784-5-3 shall apply. Additional information can be retrieved from [36].

9.3 Safety function response time

9.3.1 Model

A safety function may consist of several sensors such as a light curtain and E-Stop buttons, a F-Host application program within an F-Host, and an actuator such as a motor (Figure 61).

Each sensor has its own signal path and thus a particular typical response time (see blue dotted line in Figure 61).

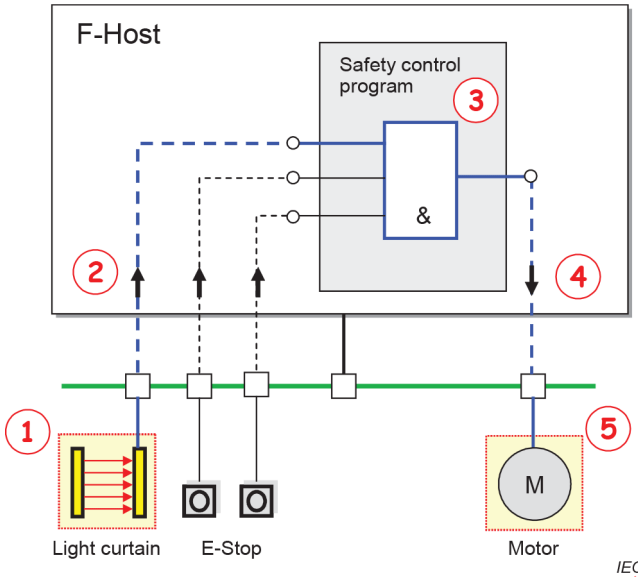


Figure 61 – Example safety function with a critical response time path

This typical response time consists of several individual time values including the bus transfer times as shown in the simplified typical response time model of Figure 62. An example is used to show the principle, which can be adopted for the internal response time model of a complex device.

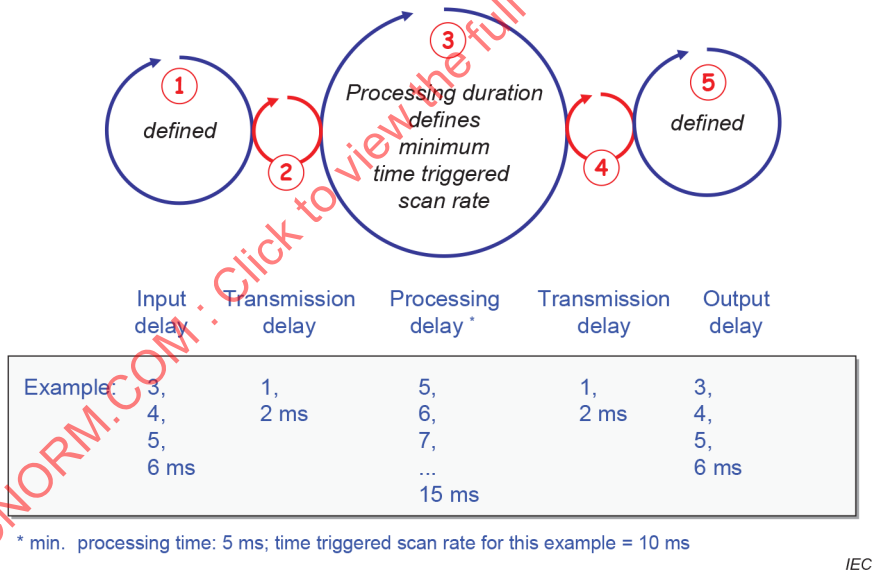


Figure 62 – Simplified typical response time model

The example represents a signal path consisting of a sensor F-(Sub)Module, the bus transfer to the F-Host, the F-Host's processing, another bus transfer F-(Sub)Module to the output device, and the output F-(Sub)Module (final element).

Any of these elements have minimum (= processing) and maximum delay times (= processing + waiting). The actual delay may be any time (or time interval) in between these values.

In this model the F-Host is supposed to be a combined controller for standard and safety programs. The safety program is executed within a separate time triggered program level and may need a processing time of 5 ms. Trigger time in this case is each other 10 ms. This results in a processing delay of minimal 5 ms and a maximum of 15 ms. In total, the minimum delay for this safety function is 13 ms and the maximum delay is 31 ms.

Figure 63 shows the frequency distributions of typical response times of the model for a time trigger of 10 ms, 20 ms and 30 ms.

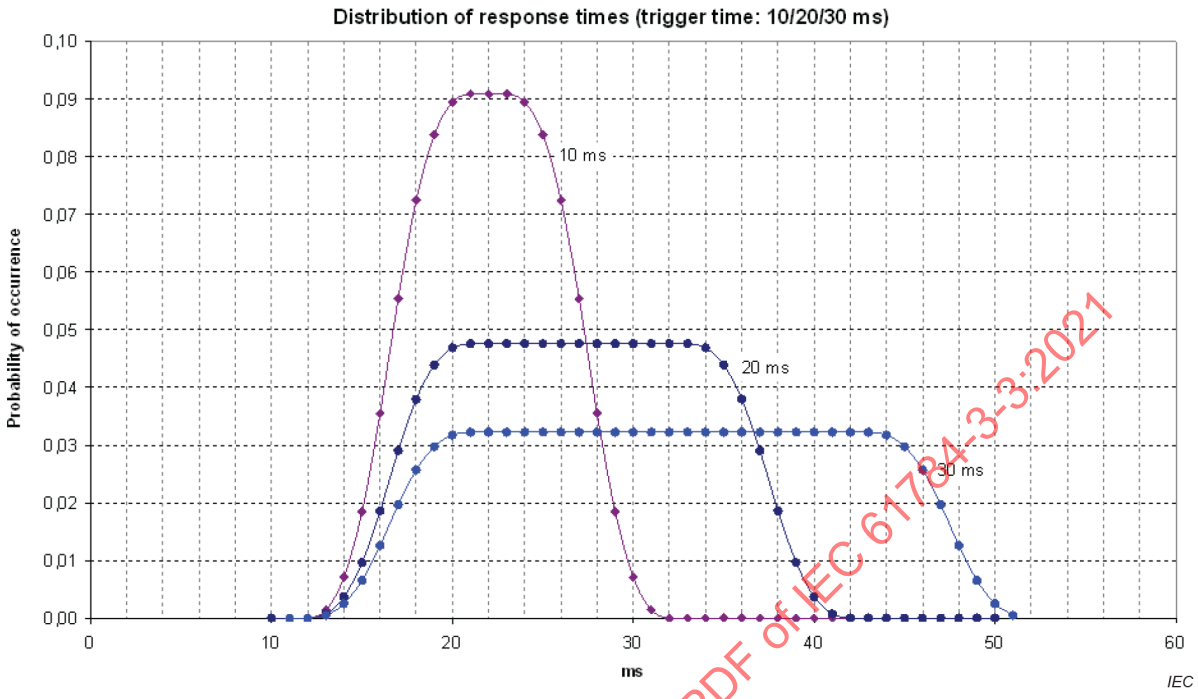


Figure 63 – Frequency distributions of typical response times of the model

9.3.2 Calculation and optimization

The model for typical response times in 9.3.1 is used to define the safety function response time. Each of the cycles in the model can vary between a best case and a worst case delay time ($WCDT_i$). Every cycle has for safety reasons its superposed watchdog timer ($WDTime_i$), which takes the necessary actions to activate the safe state whenever a failure or error occurs within that particular entity.

Figure 64 illustrates the context of the worst case delay times and the watchdog times.

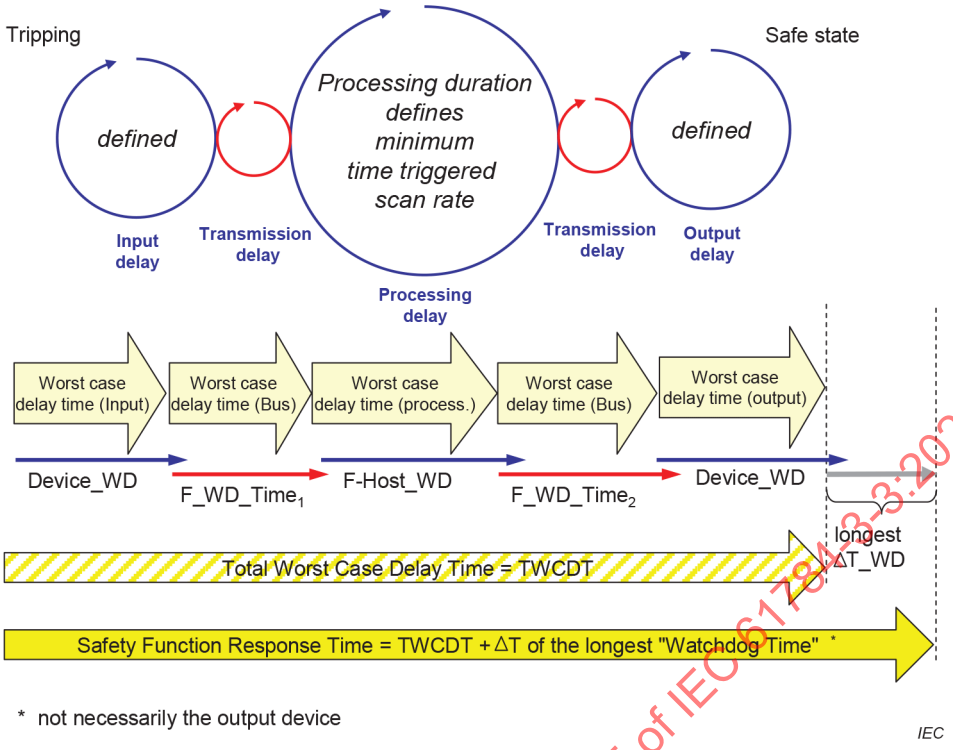


Figure 64 – Context of delay times and watchdog times

In order to calculate the safety function response time one error or failure shall be assumed in that entity of the signal path, which contributes the maximum difference time between its worst case delay time and its watchdog time (WDTime). The corresponding Formula (1) is shown below:

$$SFRT = \sum_{i=1}^{n} WCDT_i + \max_{i=1,2,...n}\left(WDTime_i - WCDT_i\right) \quad (1)$$

where

SFRT Safety function response time

TD Transmission delay

$WCDT_i$ Worst case delay time of entity i

$WDTime_i$ The WDTime spans the time frame starting with the reception of a safety PDU with a new MNR and ending with the reaction on the expiration of the F_WD_Time. Following the particular expressions for the entities i:

– Input: $OFDT_{Input}$

– TD_1: $F\_WD\_Time_1 + WCDT_{TD1} + Tcy_{F\text{-}Host}$

– F-Host: $OFDT_{F\text{-}Host}$

– TD_2: $F\_WD\_Time_2 + WCDT_{TD2} + DAT_{Output}$

– Output: $OFDT_{Output}$

OFDT One fault delay time of an entity, i.e. worst case delay time in case of a fault within the entity

$Tcy_{F\text{-}Host}$ F-Host cycle time

System manufacturers shall provide their individual adapted calculation method if necessary.

9.3.3 Adjustment of watchdog times for FSCP 3/1

The F-Parameter F_WD_Time determines the watchdog time for a FSCP 3/1 1:1 communication relationship (8.1.3). Figure 65 illustrates that the minimum watchdog time is composed of four timing sections (DAT – Bus – HAT – Bus).

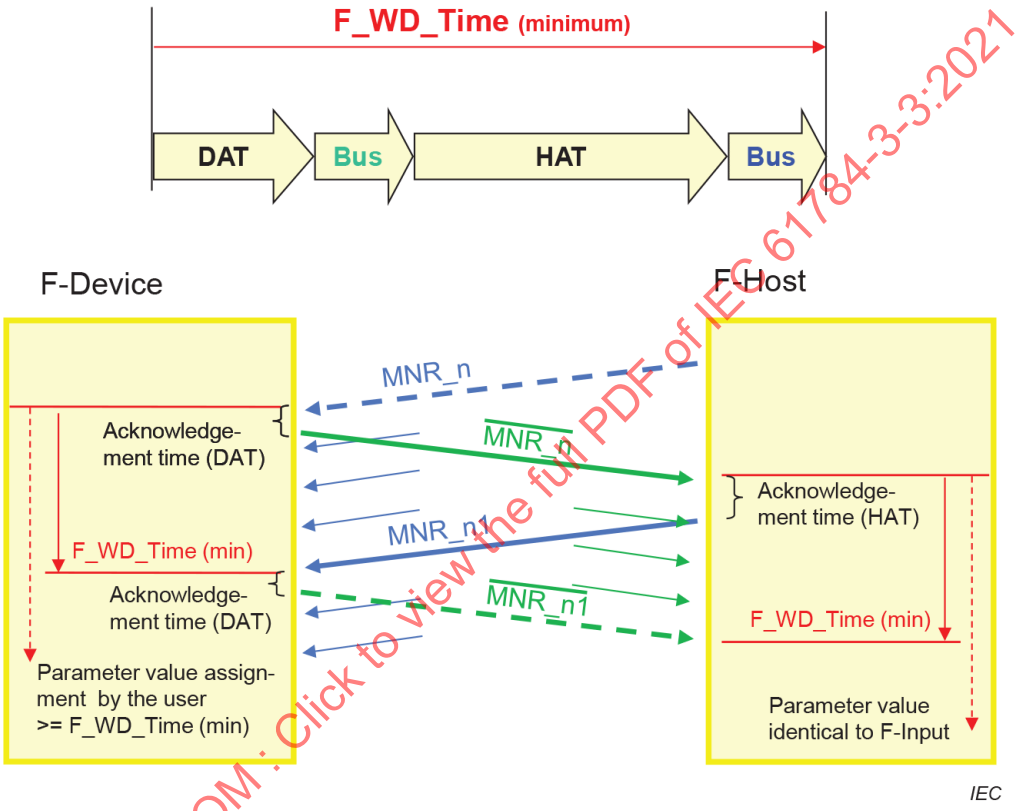


Figure 65 – Timing sections forming the FSCP 3/1 F_WD_Time

Whenever the F driver (6.2) recognizes a safety PDU (FSCP 3/1 frame) with a new MNR it restarts the watchdog timer. It then processes the FSCP 3/1 protocol while taking the *currently available process values* and prepares a new safety PDU. The elapsed time for this operation is called "DAT = Device Acknowledgment Time".

NOTE DAT includes internal transfer times across the backplane bus.

The transfer of the new safety PDU to the F-Host characterizes the next timing section (Bus). As soon as the F driver in the F-Host received the new safety PDU it restarts its watchdog timer and processes the FSCP 3/1 protocol. It generates a safety PDU with the next MNR. The elapsed time for this operation is called "HAT = Host Acknowledgment Time". The transfer of the safety PDU to the F-Device driver characterizes the last timing section (Bus).

Constraints:

- The Formula (1) in 9.3.2 is valid in case the timings for DAT, HAT, and bus transmissions can be guaranteed. The primary F-Parameter F_WD_Time shall be assigned a value that is slightly greater than the sum of DAT, HAT, and two times the bus transmission time.

- It is **highly recommended** for the difference between the assigned parameter value F_WD_Time and the sum (DAT, HAT, and bus transmission delays) to not exceed 30 %.

System manufacturers can adjust this rule to their individual needs.

According to 8.1.3, the value to be assigned to F_WD_Time in the example of Figure 62 (Time trigger = 10 ms) would be 2 × bus transmission (2 × 2 ms) plus DAT of the device (6 ms) and the F-Host (15 ms): F_WD_Time = 4 ms + 6 ms + 15 ms = 25 ms. An adjustment of a shorter watchdog time will not affect the safety of a system. It may cause spurious trips and thus affect its availability.

The fact that a device can extend the bus transfer times in the event of a diagnosis message shall also be taken into account in reserving the necessary time allowance within the watchdog timer adjustments. Additional communication partners or shared media users have minor influence on the response times. Other influences are described in 9.3.5.

9.3.4 Engineering tool support

Engineering tools should provide means to already estimate safety function response times during the planning phase to support dimensioning of distances in the mechanical design and during the commissioning phase to support the assignment of watchdog parameters.

9.3.5 Retries (repetition of messages)

In case of extreme electromagnetic interference or devices that are not conform to the fieldbus standards in stressing the data communication lines with unacceptable electrical noise, fieldbus systems tend to use retry mechanisms to increase the availability. It is good engineering practice during the commissioning phase to check each connection to all of the devices – non-safety or safety – for its number of retries and, if necessary, to take appropriate measures such as correct application of the installation guidelines or usage of conformance tested devices (Clause 10). This will not only help to increase the availability but also provide short reaction times without spurious trips (Figure 66).

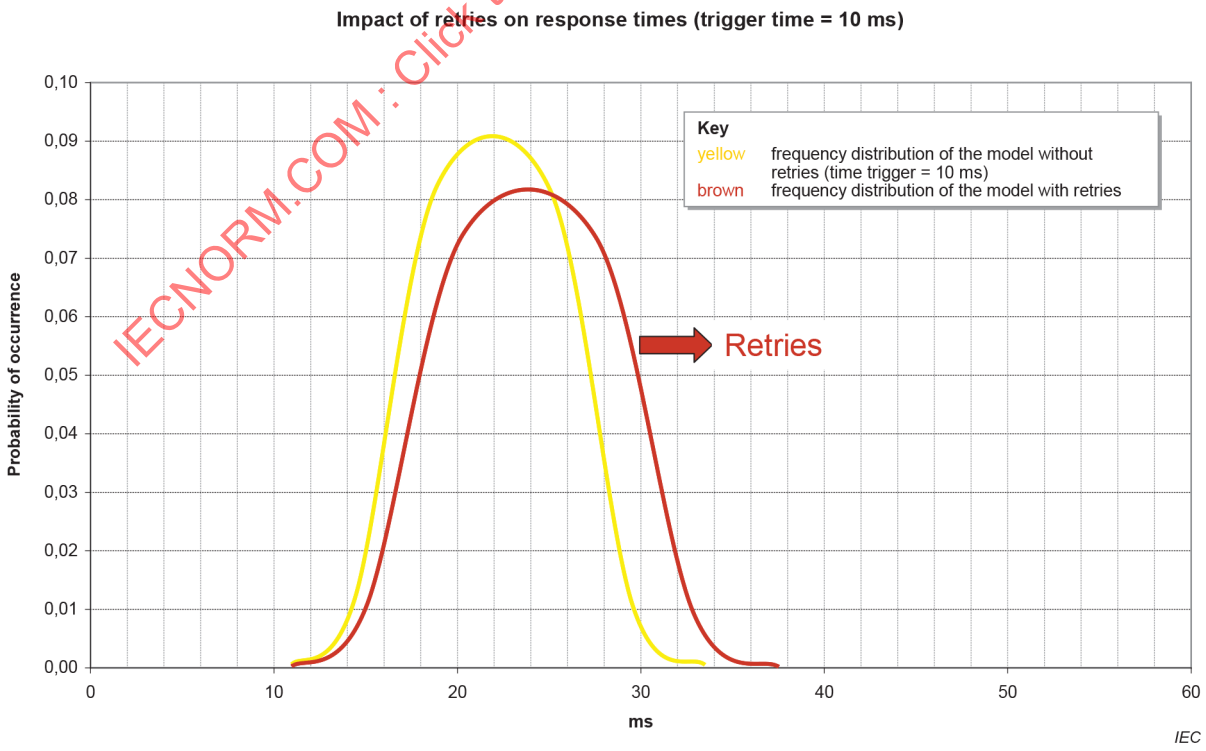


Figure 66 – Frequency distribution of response times with message retries

9.4 Duration of demands

The "demands for a safe reaction" usually are coming from for example light curtains, safety shut-off mats, 2-hand controls, emergency stops and alike. Those signals

- shall be present as long as or longer than the Process Safety Time or the FSCP 3/1 timeout (F_WD_Time) respectively;
- may be present shorter than the Process Safety Time or the FSCP 3/1 timeout (F_WD_Time) respectively. In this case a safety reaction is possible. Example: a fly cruising through a light curtain.

Within the F_WD_Time, safety PDUs with the same MNR and different process values can be received due to permuted messages in the black channel.

9.5 Constraints for the calculation of system characteristics

9.5.1 Probabilistic considerations

The data integrity checking mechanism of the FSCP 3/1 is independent from the mechanisms of the underlying communication system, which then is called a "black channel". Thus it can be used for backplane communication channels also.

According to IEC 62280, the "properness" of the used CRC generator polynomials shall be proven. This requires calculation of the residual error probability as a function of the bit error probability for a given polynomial, here for the 24-bit version (*0x5D6DCB*), as well as for the 32-bit version (*0xF4ACFB13*).

Figure 67 shows the diagrams of residual error probabilities for the 24-bit CRC generator polynomial. The calculated diagrams are for data lengths including the CRC signature.

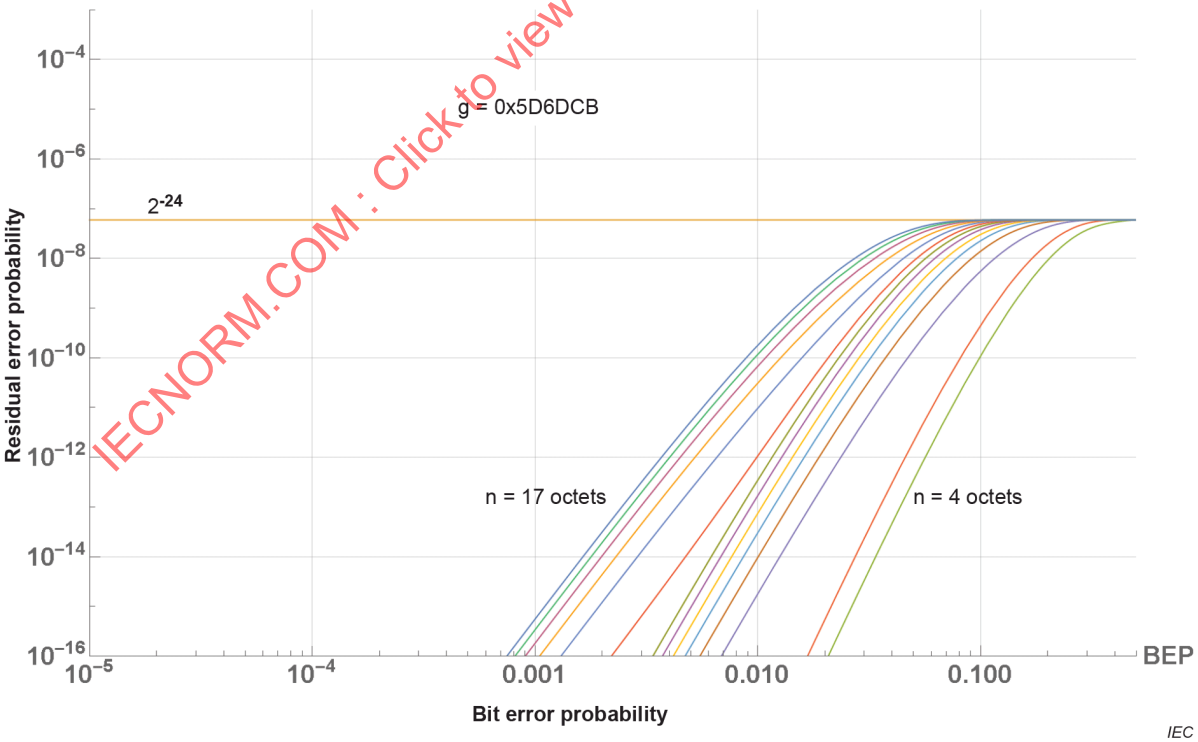


Figure 67 – Residual error probabilities for the 24-bit CRC polynomial

A polynomial will be assessed "proper" if there is no significant "humpback" curve with increasing bit error probability, i.e. if it rises monotonic for example.

Figure 68 shows diagrams for the 32-bit CRC generator polynomial.

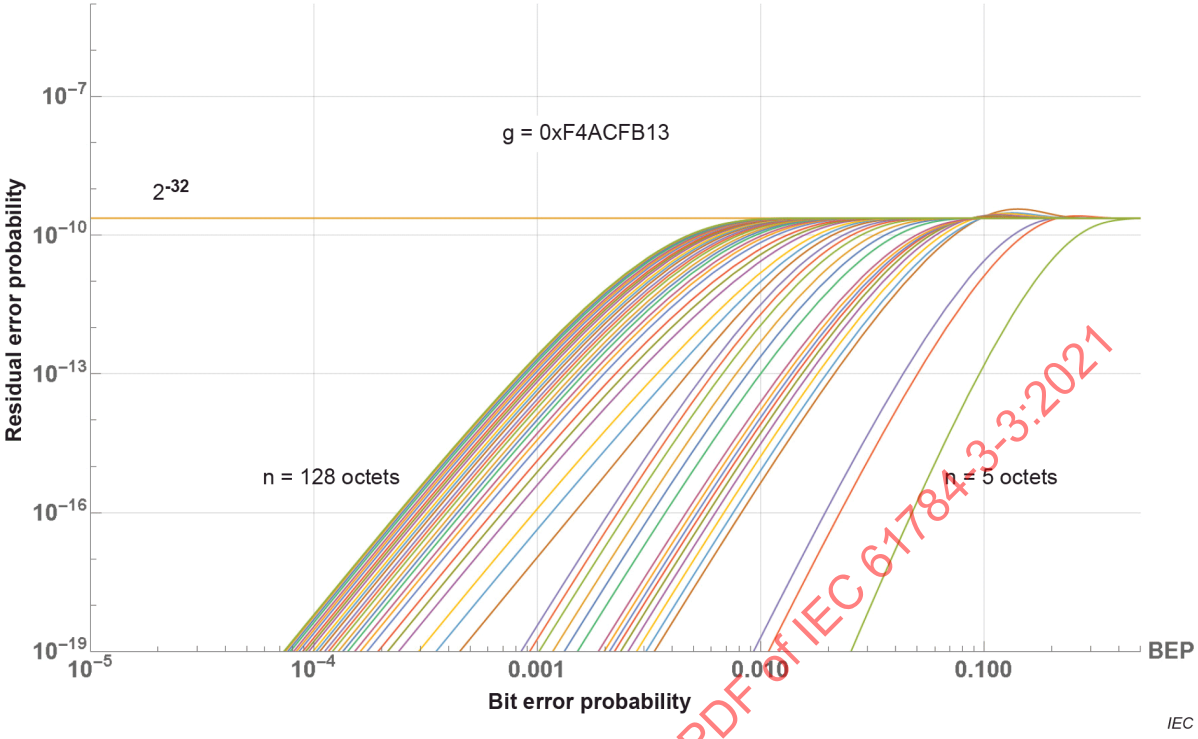


Figure 68 – Residual error probabilities for the 32-bit CRC polynomial

The terms used in Figure 67 and Figure 68 are specified below:

g = generator polynomial

n = length of data (including the CRC signature)

Summarizing reflections about any perturbing influences lead directly to Figure 69. The combination of the bus failure and error causes provides a (fictive) frequency of corrupted messages on the transmission system. The standard error detecting mechanisms of Black channel (1st Filter) detects every fault up to a certain level, thus only special bit patterns are reaching the safety layer mechanism. For the frequency of undetected corrupted messages the worst-case value of c = 1/T is taken, since the overall frequency of corrupted safety PDUs on the bus is continuously monitored.

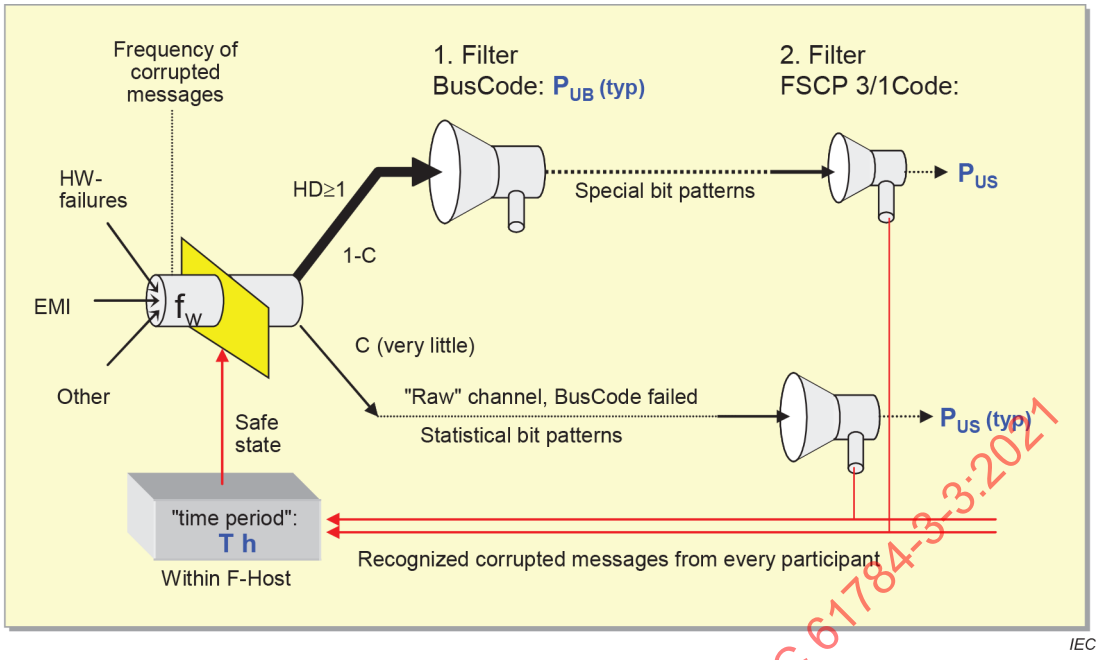


Figure 69 – Monitoring of corrupted messages

The terms used in Figure 69 are specified in Table 42:

Table 42 – Definition of terms in Figure 69

Term	Definition
fw	frequency of corrupted messages
EMI	electromagnetic interference
HD	hamming distance
c	frequency of occurrence
T	measurement period in hours (see 7.2.7)

If the safety mechanisms within the standard CP 3/1 and CP 3/4 to CP 3/6 IO layers are failing (very little probability), then corrupted messages with statistical bit patterns are reaching the safety layer mechanism.

This FSCP 3/1 protocol allows simple monitoring of every corrupted safety PDU within the F-Host driver and via the Status Byte within the acknowledgment safety PDU of an F-Device driver.

9.5.2 Safety related assumptions

The boundary conditions and assumptions for safety assessments and calculations of residual error rates are listed here.

Generally:

- All devices provide electrical safety SELV/PELV and a CPF 3 conformance test report
- Safety devices shall comply with the increased test levels and durations, as well as corresponding performance criteria specified in IEC 61326-3-1 or the generic standard IEC 61000-6-7. IEC 61326-3-2 may be used as an exception, if the intended application exactly matches the specific scope and pre-conditions of IEC 61326-3-2.

FSCP 3/1 protocol (V2-mode):

- Number of retries per channel type (see 9.3.5):
  No restrictions
- Number of safety-related message sinks per safety function:
  No restrictions
- Black Channel CRC polynomials:
  No restrictions
- Active buffering network elements:
  No restrictions; any switch permitted (see 7.3.9 and 5.4.2)
- Safety islands:
  Single port routers are not permitted as borders for a safety island (see 7.3.11)
- Octet-wise splitting of safety PDU:
  No restrictions
- Size of F-I/O data within one SPDU
  F_CRC_Seed =0: ≤ 12 octets
  F_CRC_Seed =1: ≤ 123 octets
- SIL-Monitor observation time:
  F_CRC_Seed =0: 100 h
  F_CRC_Seed =1: 10 h

9.5.3 Non safety related constraints (availability)

- Cyclic data exchange of SPDUs within a defined time period (sign of life)
- Guaranteed delivery of entire safety PDUs at the F driver

Generally:

  – CP 3/1: No spurs (branch lines)
  – Ethernet-Switches shall be suitable for standard industrial environment as defined for example in IEC 61010-2-201.

Standard and safety devices may share the same 24V power supply.

9.6 Maintenance

9.6.1 F-(Sub)Module commissioning / replacement

F-Modules can be replaced while the system is running. Restart of the corresponding safety function is only permitted, if there is no hazardous process state, and after an Operator Acknowledgment (OA_C).

9.6.2 Identification and maintenance functions

9.6.2.1 Overview

Identification and maintenance functions (I&M) define a set of parameters in a Slave or IO Device (hosting F-(Sub)Module) to identify device types and individual devices via a CPF 3 network and to support its maintenance.

9.6.2.2 Case CP 3/1 and CP 3/2

F-Slaves shall implement the mandatory set of I&M functions [37]. Additionally, F-Slaves shall fill the field IM4 (signature) with a signature that indicates the safety configuration and parameterization state of the F-Slave if this signature is not otherwise incorporated in the overall F-Host project signature. External write access to IM4 shall be denied.

9.6.2.3 Case CP 3/4 to CP 3/6

F-Submodules shall implement the mandatory set of I&M functions. Additionally, F-Submodules shall fill the field IM4 (signature) with a signature that indicates the safety configuration and parameterization state of the F-Submodule if this signature is not otherwise incorporated in the overall F-Host project signature (e.g. as by the F_iPar_CRC). External write access to IM4 shall be denied.

The function "Reset to factory settings" of CP 3/4 to CP 3/6 shall not reset the iParameters including the access password and IM4 to default values.

9.7 Safety manual

According to IEC 61508-2, F-Host and F-(Sub)Module suppliers shall provide a safety manual. In case of FSCP 3/1, the instructions, information and parameters of Table 43 shall be included.

Table 43 – Information to be included in the safety manual

	Item	Instruction and/or parameter	Remark
1	Safety handling	Instructions on how to configure, parameterize, commission, test, and lock this device safely in accordance with IEC 61508	See 9.1 (LED) , 7.3.7 and 8.1.2 Codename ("F_S/D_Address")
2	PFH, respectively PFDavg (LP, XP)	Implementations according to FSCP 3/1 provide a communication PFH, respectively PFDavg, less than 1% of the target SIL of the overall safety function.	Assumptions, see 9.5.2
3	F-Host manual: Network components	Constraints on switches, router, and other network components	See 7.3.11, 9.5.2, and 9.5.3
4	Commissioning	Usage of the check list in IEC 61784-5-3 on for example proper addressing, retry checking, or signal quality. Where appropriate explain measures to get unique Codenames per Subnet. (e.g. uniqueness of the Retentive Selection of the Codename). See also 8.1.2	See also [51] and 9.10
5	FSCP 3/1 Address check in the F-(Sub)Module	For the particular F-(Sub)Module it shall be declared, whether the F-Source address part of the Codename is included in the Codename check, and which range for the Codename is permitted (for example 1 to 1023). **Use naming:** **FSCP 3/1 Address Type 1:** F-(Sub)Module which checks as Retentive Selection of the Codename the "destination address" only. **FSCP 3/1 Address Type 2:** F-(Sub)Module which checks as Retentive Selection of the Codename the retentive "source and destination address".	
6	F-Host manual: Automatic reintegration (restart)	(Operation automatic restart); Automatic restart in safety for machinery is only allowed depending on the safety requirements specification of the particular machinery.	
7	Reaction on Device_Fault	Documentation how the F-(Sub)Modules uses Device_Fault and if the F-Host application program has to prevent an unintentional restart. See C.1.4	

	Item	Instruction and/or parameter	Remark
8	iParameter	Verification of safety functions of F-(Sub)Modules supporting the FSCP test mode shall include a check for F_iPar_CRC > "0".	See 8.6.4.5, 8.1.7
9	Response time	Parameter values for DAT, WCDT, WDTime	See 9.3.2 and 9.3.3
10	F-Host manual: SIL monitor	Information for operators, similar to: "In case a request for manual Operator Acknowledgment caused by an associated diagnosis message (e.g. number 77 in table 3) has been perceived more than once within 100 hours it is highly recommended to call in the responsible service technician". Information for operators and service technicians: "This suggests a massive disturbance of the data transmission within the fieldbus system. Causes for this incident can be changes in the installation, corrosion of bus cable shields with connectors, and extreme electromagnetic interferences. Compliance with installation guidelines [53] should be checked, or an EMC expert (see Annex B for further guidance) should be called in".	See 7.2.7.1.
11	F-Host manual: Security	Instructions on how to establish an adequate level of security defining security zones with security gates.	See 9.9
12	Parameterization in Run	See Amendment FSCP 3/1 PiR	See [64]
13	PROFIenergy	In case of usage of PROFIenergy together with FSCP 3/1 see Clause C.4	

9.8 Wireless transmission channels

9.8.1 Black channel approach

CP 3/3 and CP 3/4 defines the usage of Wireless transmission channels. These are classified to be part of the black channel and thus do not need to be assessed for safety as FSCP 3/1 is approved for a bit error probability of 10^{-2}.

9.8.2 Availability

One of the major challenges with wireless transmission is a sufficient availability. The user shall establish appropriate measures to ensure sufficient availability wherever roaming overtimes or communication blackouts due to reflexions or interferences, or other causes for spurious trips are possible. Spurious trips may lead to switching off or removal of safety equipment (foreseeable misuse).

9.8.3 Security measures

Before any deployment of a safety application with FSCP 3/1 and wireless components an assessment for dangerous threats such as eavesdropping or data manipulation shall be executed, see 9.9.

9.8.4 Stationary and mobile applications

Two kinds of safety applications shall be considered: the "stationary" safety applications that are characterized by well-defined locations and movements and "mobile" safety applications.

There are no constraints and special assessments for stationary applications such as revolving emptying and filling systems.

Mobile deployment of wireless components has additional challenges. In particular the unambiguous allocation of safety functions to the hazardous final elements (for example robots, see ISO 10218-1 [22]) shall be assured.

9.9 Relationship between functional safety and security

Security shall be considered for safety-related applications that include functional safety communication systems, however, FSCP 3/1 does not cover security aspects nor does it provide any requirements for security. Security of industrial automation and control systems (IACS) is addressed in IEC 62443 (all parts) and in [36].

9.10 Conformance classes

Manufacturers of F-(Sub)Modules rely on some features their counterparts (F-Host) shall support as a minimum besides the conformance to the FSCP 3/1 protocol. The required features are listed in Table 44.

Table 44 – F-Host conformance class requirements

	Item	Factory Automation	Process Automation	Note
1a	GSD-Support - CP3/1 and CP3/2	V5.04 of [35];	ditto	Regarding F-Parameters only
1b	GSD-Support - CP3/4 to CP3/6	V2.33 of [38] or later versions	V2.34	Regarding F-Parameters only
2	Support of Channel-granular Passivation	Mandatory for F-Host (XP), see Table 46	ditto	–
3	"F_CRC_Seed" (see 8.1.5.2) supported	Mandatory for F-Host (XP) see Table 46	ditto	Previous "CRC1" corresponds to "CRC_FP" and shall be supported
4	Loop-back check via Bit 7 in Status/Control Byte	Mandatory for F-Host (LP) and (XP), see Table 46	ditto	Necessary for support of legacy F-(Sub)Modules
5a	CP 3/1 Communication function blocks according IEC 61131-3	Minimum communication function block set is: RDREC, WRREC, RDIAG, RALRM [39]	ditto	–
5b	CP 3/4 to 3/6 Communication function blocks according IEC 61131-3	Minimum communication function block set is: RDREC, WRREC, RALRM [39]	ditto	–
6	iPar-Server	System manufacturers shall provide the "iPar-Server" services with at least 2^{15} octets	Ditto	–
7	Quantities (bit) of F-I/O data	Up to 64 bit (Bool) coded as Unsigned8, V2.6MU1 Up to 96 bit.	Ditto	–
8	Quantities of F-I/O data (octets)	F_CRC_Seed =0: up to12 octets F_CRC_Seed = 1: up to13 octets minimum; maximum of 123 octets permitted	Ditto	Sizes of supported minimum data structures as shown for example in Figure 4 , Figure 16, Figure 20, and Figure 23.
9	Data types	Unsigned8, -16, -32, Integer16, -32	all FSCP 3/1 data types: See Table 2	FSCP 3/1 rules for F Host Channel drivers shall be observed
10	F-Host driver interface	All signals	All signals	–

	Item	Factory Automation	Process Automation	Note
11	Diagnosis	Highly recommended: safety layer error messages (6.3.2)	Highly recommended: safety layer error messages (6.3.2)	Recommended literature: see [40] and [58]
12	Read and write record service	mandatory	mandatory	According CP 3/1, CP 3/2, and CP 3/4 to CP 3/6
13	Slave hosting F-Modules MS2 access	Recommended	optional	According CP 3/1, CP 3/2 Small CPUs could be possibly not able to carry high traffic through load
14	IO Device hosting F-Submodules Device access	Recommended	optional	According CP 3/4 to CP 3/6
15	SIL claim	3 (within special application areas such as CNC: minimum 2)	3	–
16	Tool-Integration, Parameterization	Tool interface that meets the requirements of Table 34	According to [49] or via tool interface that meets the requirements of Table 34	–
17	F_WD_Time_2	Optional for F-Host (XP)	Recommended for F-Host (XP)	See 8.1.4

The expanded protocol functions in this document require conformance considerations between two F-Host driver protocol versions (LP and XP) and F-Device driver according to IEC 61784-3-3:2010 and Edition IEC 61784-3-3:2016.

Table 45 shows the main characteristics of the protocol versions.

Table 45 – Main characteristics of protocol versions

Protocol type	Characteristics
Loop-back extension (LP)	- IEC 61784-3-3:2010 - F_CRC_Seed =0 - Check Loop-back Bit 7
Expanded protocol (XP)	- IEC 61784-3-3:2016 - F_CRC_Seed = 1

Table 46 specifies the requirements for the two F-Device driver versions.

Table 46 – F-Host driver / F-Device driver conformance matrix

F-Host driver	F-Device driver	
	according previous editions of this document	**according to this document**
according to this document	**Loop-back extension (LP)** - No change for F-(Sub)Module and GSD	**Expanded protocol (XP)** - New GSD file - Qualifier for F-I/O data, see [56]

10 Assessment

10.1 Safety policy

In order to prevent and protect the manufacturers and vendors of FSCP 3/1 devices from possibly misleading understandings or wrong expectations and gross negligence actions regarding safety-related developments and applications the following shall be observed and explained in each training, seminar, workshop and consultancy.

- Any device automatically will not be applicable for safety-related applications just by using fieldbus communication and a safety communication layer.
- In order to enable a product for safety-related applications, appropriate development processes according to safety standards shall be observed (see IEC 61508 (all parts), IEC 61511 (all parts), IEC 60204-1, IEC 62061, ISO 13849-2) and/or an assessment from a competent assessment body shall be achieved.
- The manufacturer of a safety product is responsible for the correct implementation of the safety communication layer technology, the correctness and completeness of the product documentation and information.
- Additional important information about actual corrigendums through concluded change requests shall be considered for implementation and assessment. This information can be obtained from the organizations listed in Annex B.

The complete information is also available in [52].

10.2 Obligations

As a rule, the international safety standards are accepted (ratified) globally. However, since safety technology in automation is relevant to occupational safety and the concomitant insurance risks in a country, recognition of the rules pointed out here is still a sovereign right. The national "Authorities" decide on the recognition of assessment reports.

NOTE Examples of such "Authorities" are the IFA (Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung / Institute for Occupational Safety and Health of the German Social Accident Insurance) in Germany, HSE (Health and Safety Executive) in UK, FM (Factory Mutual / Property Insurance and Risk Management Organization), UL (Underwriters Laboratories Inc. / Product Safety Testing and Certification Organization) in USA, or the INRS (Institut National de Recherche et de Sécurité) in France.

For FSCP 3/1 the rules on assessments within IEC 61784-3 apply. Additional information can be retrieved from [61].

Annex A
(informative)

Additional information for functional safety communication profiles of CPF 3

A.1 Hash function calculation

The procedure in Figure A.1 detects 99,999 994 % of all errors that result from data modifications. It also discovers sequential errors because the signature check takes into account the sequence of the words.

For the 24-bit CRC signature, the value *0x5D6DCB* is used as the generator polynomial. The number of data bits may be odd or even. The value that is generated after the last octet corresponds to the transferred CRC signature.

```
void crc24_calc(unsigned char x, unsigned long *r)
 int i;
 for (i = 1; i <= 8; i++)
  if ((bool)(*r & 0x800000) != (bool)(x & 0x80))
    *r = (*r << 1) ^ 0x5D6DCB;          /* XOR = 1 => Shift and process polynomial */
    else
    *r = *r << 1;                      /* XOR = 0 => pure shift */
  x = x << 1;
 /* for */
```

Figure A.1 – Typical "C" procedure of a cyclic redundancy check

The runtime-optimized variant for the calculation of the CRC signature requires slightly more memory space. The corresponding function (A.1) in "C" programming language for the 24 bit CRC signature calculations with the help of lookup tables is shown below:

```
r = crctab24 [((r >> 16) ^ *q++) & 0xff] ^ (r << 8)        (A.1)
```

where

- r represents the 24 bit CRC signature result
- q represents the pointer to the actual octet value that needs CRC calculation. After reading the value this pointer shall be incremented for the next octet via q++.
- the seed values of r can be "0" (see 8.1.8), "1" (see 8.1.5.6, 8.1.7, 8.2) or "CRC_FP" = F_Par_CRC (see 8.1.5.6).

For this calculation, Table A.1 is used.

Table A.1 – The table "Crctab24" for 24 bit CRC signature calculations

CRC24 lookup table (0 to 255)							
000000	5D6DCB	BADB96	E7B65D	28DAE7	75B72C	920171	CF6CBA
51B5CE	0CD805	EB6E58	B60393	796F29	2402E2	C3B4BF	9ED974
A36B9C	FE0657	19B00A	44DDC1	8BB17B	D6DCB0	316AED	6C0726
F2DE52	AFB399	4805C4	15680F	DA04B5	87697E	60DF23	3DB2E8
1BBAF3	46D738	A16165	FC0CAE	336014	6E0DDF	89BB82	D4D649
4A0F3D	1762F6	F0D4AB	ADB960	62D5DA	3FB811	D80E4C	856387
B8D16F	E5BCA4	020AF9	5F6732	900B88	CD6643	2AD01E	77BDD5
E964A1	B4096A	53BF37	0ED2FC	C1BE46	9CD38D	7B65D0	26081B
3775E6	6A182D	8DAE70	D0C3BB	1FAF01	42C2CA	A57497	F8195C
66C028	3BADE3	DC1BBE	817675	4E1ACF	137704	F4C159	A9AC92
941E7A	C973B1	2EC5EC	73A827	BCC49D	E1A956	061F0B	5B72C0
C5ABB4	98C67F	7F7022	221DE9	ED7153	B01C98	57AAC5	0AC70E
2CCF15	71A2DE	961483	CB7948	0415F2	597839	BECE64	E3A3AF
7D7ADB	201710	C7A14D	9ACC86	55A03C	08CDF7	EF7BAA	B21661
8FA489	D2C942	357F1F	6812D4	A77E6E	FA13A5	1DA5F8	40C833
DE1147	837C8C	64CAD1	39A71A	F6CBA0	ABA66B	4C1036	117DFD
6EEBCC	338607	D4305A	895D91	46312B	1B5CE0	FCEABD	A18776
3F5E02	6233C9	858594	D8E85F	1784E5	4AE92E	AD5F73	F032B8
CD8050	90ED9B	775BC6	2A360D	E55AB7	B8377C	5F8121	02ECEA
9C359E	C15855	26EE08	7B83C3	B4EF79	E982B2	0E34EF	535924
75513F	283CF4	CF8AA9	92E762	5D8BD8	00E613	E7504E	BA3D85
24E4F1	79893A	9E3F67	C352AC	0C3E16	5153DD	B6E580	EB884B
D63AA3	8B5768	6CE135	318CFE	FEE044	A38D8F	443BD2	195619
878F6D	DAE2A6	3D54FB	603930	AF558A	F23841	158E1C	48E3D7
599E2A	04F3E1	E345BC	BE2877	7144CD	2C2906	CB9F5B	96F290
082BE4	55462F	B2F072	EF9DB9	20F103	7D9CC8	9A2A95	C7475E
FAF5B6	A7987D	402E20	1D43EB	D22F51	8F429A	68F4C7	35990C
AB4078	F62DB3	119BEE	4CF625	839A9F	DEF754	394109	642CC2
4224D9	1F4912	F8FF4F	A59284	6AFE3E	3793F5	D025A8	8D4863
139117	4EFCDC	A94A81	F4274A	3B4BF0	66263B	819066	DCFDAD
E14F45	BC228E	5B94D3	06F918	C995A2	94F869	734E34	2E23FF
B0FA8B	ED9740	0A211D	574CD6	98206C	C54DA7	22FBFA	7F9631

This table contains 24 bit values for each value (0 to 255) of the argument a in the function crctab24 [a]. The table should be used in ascending order from top left (0) to bottom right (255).

The corresponding function (A.2) in "C" programming language for the 32 bit CRC signature calculations with the help of lookup tables is shown below:

$$r = \text{crctab32}\ [((r >> 24)\ \hat{}\ *q{+}{+})\ \&\ 0xff]\ \hat{}\ (r << 8) \quad (A.2)$$

For this calculation, Table A.2 is used.

Table A.2 – The table "Crctab32" for 32 bit CRC signature calculations

CRC32 lookup table (0 to 255)							
00000000	F4ACFB13	1DF50D35	E959F626	3BEA1A6A	CF46E179	261F175F	D2B3EC4C
77D434D4	8378CFC7	6A2139E1	9E8DC2F2	4C3E2EBE	B892D5AD	51CB238B	A567D898
EFA869A8	1B0492BB	F25D649D	06F19F8E	D44273C2	20EE88D1	C9B77EF7	3D1B85E4
987C5D7C	6CD0A66F	85895049	7125AB5A	A3964716	573ABC05	BE634A23	4ACFB130
2BFC2843	DF50D350	36092576	C2A5DE65	10163229	E4BAC93A	0DE33F1C	F94FC40F
5C281C97	A884E784	41DD11A2	B571EAB1	67C206FD	936EFDEE	7A370BC8	8E9BF0DB
C45441EB	30F8BAF8	D9A14CDE	2D0DB7CD	FFBE5B81	0B12A092	E24B56B4	16E7ADA7
B380753F	472C8E2C	AE75780A	5AD98319	886A6F55	7CC69446	959F6260	61339973
57F85086	A354AB95	4A0D5DB3	BEA1A6A0	6C124AEC	98BEB1FF	71E747D9	854BBCCA
202C6452	D4809F41	3DD96967	C9759274	1BC67E38	EF6A852B	0633730D	F29F881E
B850392E	4CFCC23D	A5A5341B	5109CF08	83BA2344	7716D857	9E4F2E71	6AE3D562
CF840DFA	3B28F6E9	D27100CF	26DDFBDC	F46E1790	00C2EC83	E99B1AA5	1D37E1B6
7C0478C5	88A883D6	61F175F0	955D8EE3	47EE62AF	B34299BC	5A1B6F9A	AEB79489
0BD04C11	FF7CB702	16254124	E289BA37	303A567B	C496AD68	2DCF5B4E	D963A05D
93AC116D	6700EA7E	8E591C58	7AF5E74B	A8460B07	5CEAF014	B5B30632	411FFD21
E47825B9	10D4DEAA	F98D288C	0D21D39F	DF923FD3	2B3EC4C0	C26732E6	36CBC9F5
AFF0A10C	5B5C5A1F	B205AC39	46A9572A	941ABB66	60B64075	89EFB653	7D434D40
D82495D8	2C886ECB	C5D198ED	317D63FE	E3CE8FB2	176274A1	FE3B8287	0A977994
4058C8A4	B4F433B7	5DADC591	A9013E82	7BB2D2CE	8F1E29DD	6647DFFB	92EB24E8
378CFC70	C3200763	2A79F145	DED50A56	0C66E61A	F8CA1D09	1193EB2F	E53F103C
840C894F	70A0725C	99F9847A	6D557F69	BFE69325	4B4A6836	A2139E10	56BF6503
F3D8BD9B	07744688	EE2DB0AE	1A814BBD	C832A7F1	3C9E5CE2	D5C7AAC4	216B51D7
6BA4E0E7	9F081BF4	7651EDD2	82FD16C1	504EFA8D	A4E2019E	4DBBF7B8	B9170CAB
1C70D433	E8DC2F20	0185D906	F5292215	279ACE59	D336354A	3A6FC36C	CEC3387F
F808F18A	0CA40A99	E5FDFCBF	115107AC	C3E2EBE0	374E10F3	DE17E6D5	2ABB1DC6
8FDCC55E	7B703E4D	9229C86B	66853378	B436DF34	409A2427	A9C3D201	5D6F2912
17A09822	E30C6331	0A559517	FEF96E04	2C4A8248	D8E6795B	31BF8F7D	C513746E
6074ACF6	94D857E5	7D81A1C3	892D5AD0	5B9EB69C	AF324D8F	466BBBA9	B2C740BA
D3F4D9C9	275822DA	CE01D4FC	3AAD2FEF	E81EC3A3	1CB238B0	F5EBCE96	01473585
A420ED1D	508C160E	B9D5E028	4D791B3B	9FCAF777	6B660C64	823FFA42	76930151
3C5CB061	C8F04B72	21A9BD54	D5054647	07B6AA0B	F31A5118	1A43A73E	EEEF5C2D
4B8884B5	BF247FA6	567D8980	A2D17293	70629EDF	84CE65CC	6D9793EA	993B68F9

This table contains 32 bit values in hexadecimal representation for each value (0 to 255) of the argument a in the function crctab32 [a]. The table should be used in ascending order from top left (0) to bottom right (255).

The corresponding function (A.3) in "C" programming language for the F_Par_CRC (16 bit) signature calculation (see 8.1.8) with the help of lookup tables is shown below:

$$r = \text{crctab16}\ [((r >> 8)\ \hat{}\ *q{+}{+})\ \&\ 0xff]\ \hat{}\ (r << 8) \qquad \text{(A.3)}$$

For this calculation, Table A.3 is used.

Table A.3 – The table "Crctab16" for 16 bit CRC signature calculations

CRC16 lookup table (0 to 255)							
0000	4EAB	9D56	D3FD	7407	3AAC	E951	A7FA
E80E	A6A5	7558	3BF3	9C09	D2A2	015F	4FF4
9EB7	D01C	03E1	4D4A	EAB0	A41B	77E6	394D
76B9	3812	EBEF	A544	02BE	4C15	9FE8	D143
73C5	3D6E	EE93	A038	07C2	4969	9A94	D43F
9BCB	D560	069D	4836	EFCC	A167	729A	3C31
ED72	A3D9	7024	3E8F	9975	D7DE	0423	4A88
057C	4BD7	982A	D681	717B	3FD0	EC2D	A286
E78A	A921	7ADC	3477	938D	DD26	0EDB	4070
0F84	412F	92D2	DC79	7B83	3528	E6D5	A87E
793D	3796	E46B	AAC0	0D3A	4391	906C	DEC7
9133	DF98	0C65	42CE	E534	AB9F	7862	36C9
944F	DAE4	0919	47B2	E048	AEE3	7D1E	33B5
7C41	32EA	E117	AFBC	0846	46ED	9510	DBBB
0AF8	4453	97AE	D905	7EFF	3054	E3A9	AD02
E2F6	AC5D	7FA0	310B	96F1	D85A	0BA7	450C
81BF	CF14	1CE9	5242	F5B8	BB13	68EE	2645
69B1	271A	F4E7	BA4C	1DB6	531D	80E0	CE4B
1F08	51A3	825E	CCF5	6B0F	25A4	F659	B8F2
F706	B9AD	6A50	24FB	8301	CDAA	1E57	50FC
F27A	BCD1	6F2C	2187	867D	C8D6	1B2B	5580
1A74	54DF	8722	C989	6E73	20D8	F325	BD8E
6CCD	2266	F19B	BF30	18CA	5661	859C	CB37
84C3	CA68	1995	573E	F0C4	BE6F	6D92	2339
6635	289E	FB63	B5C8	1232	5C99	8F64	C1CF
8E3B	C090	136D	5DC6	FA3C	B497	676A	29C1
F882	B629	65D4	2B7F	8C85	C22E	11D3	5F78
108C	5E27	8DDA	C371	648B	2A20	F9DD	B776
15F0	5B5B	88A6	C60D	61F7	2F5C	FCA1	B20A
FDFE	B355	60A8	2E03	89F9	C752	14AF	5A04
8B47	C5EC	1611	58BA	FF40	B1EB	6216	2CBD
6349	2DE2	FE1F	B0B4	174E	59E5	8A18	C4B3

This table contains 16 bit values in hexadecimal representation for each value (0 to 255) of the argument a in the function crctab16 [a]. The table should be used in ascending order from top left (0) to bottom right (255).

A.2 Example values for MonitoringNumbers (MNR)

Table A.4 shows the first four MNR values for two different Codename examples (see 7.1.5 and 7.1.6). The value for the variable Modifier is assumed to be "0".

Table A.4 – Values of CN_incrNR_64 and MNR for F-Host PDU

Codename 0x010001			Codename 0x010002		
Nr	CN_incrNR_64 [0]	MNR	Nr	CN_incrNR_64 [0]	MNR
0	-	CRC_FP+	0	-	CRC_FP+
1	0xCACFA720FA43BF62	0xCACFA720	1	0x444B59A4D64ABABB	0x444B59A4
2	0x174EE7E3C6063E8F	0x174EE7E3	2	0xE91C8E94EEA2B915	0xE91C8E94
3	0xE21E8F04C049FDF1	0xE21E8F04	3	0x2D67E839C4ED73D0	0x2D67E839
4	0xF96D76E886503C80	0xF96D76E8	4	0x168476CEB3902CE5	0x168476CE

Annex B
(informative)

Information for assessment of the functional safety communication profiles of CPF 3

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

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

NOTE For IEC 61784-3-3, the relevant fieldbus organization is PROFIBUS Nutzerorganisation e.V. (PNO), see www.profibus.com.

Annex C
(normative)

Optional features

C.1 Reaction on Device_Fault in F-Host

C.1.1 Situation

The behavior of the F-Host driver State-Machine FSCP 3/1 version 2.4 and 2.6 (see 6.1): As soon the F-Host driver recognizes, that the bit Device_Fault of the Status Byte changes to TRUE, it activates fail-safe values and FV_activated_S becomes TRUE. As soon the bit Device_Fault in the Status Byte changes from TRUE to FALSE, the F-Host driver interfaces (F_Input_Data and F_Output_Data) use process values and FV_activated_S becomes FALSE.

C.1.2 Documentation for the user

In order to allow the user to choose or implement the appropriate reaction on the "Device_Fault", the required reaction of the F-Host application has to be documented in the safety manual of the F-(Sub)Module.

C.1.3 Optional extensions of F-Host driver Transition Table

If the reaction on Device_Fault is implemented in the F-Host diver, it shall be implemented as follows. All additions for the feature "Reaction on Device_Fault in F-Host" are stated in the in the application interface and the F-Host driver transitions. All additions for this feature are written in blue. See Figure C.1, Table C.1, and Table C.2. Table C.5 shows both additions – for the feature "Reaction on Device_Fault in F-Host" and the feature "Disable F-(Sub)Module".

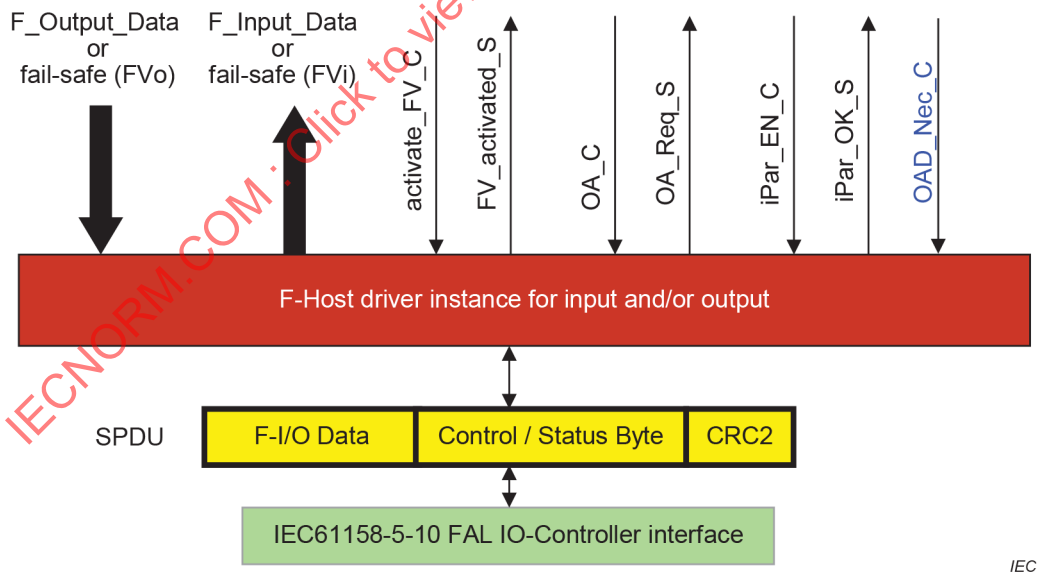


Figure C.1 – F-Host driver application interface with feature Reaction on Device_Fault

F-Host driver services:

OAD_Nec_C OperatorAcknowledgeDevicefault_Necessary: If this optional variable (type: bit) is set to "1" – in case of F_Passivation =0, the F-Host driver needs OA_C to resume a safety function after a Device_Fault gone. Default Value=1.

The F-Host driver state diagram according Figure 26 applies.

Table C.1 – Definition of additional terms used in driver transitions

Term	Definition
Device_Fault_e	Flag to store positive edge of Device_Fault in case for OAD_Nec_C =1

Table C.2 – F-Host driver transitions – added with reaction on Device_Fault

TRAN-SITION	SOURCE STATE	TARGET STATE	ACTION
T1	1	2	use FV, activate_FV =1, FV_activated_S =1 Toggle_h =1
T2	2	3	send safety PDU
T3	3	4	restart host-timer
T4	4	5	Toggle_h = not Toggle_h RUNxH **if** Device_Fault =1 and OAD_Nec_C =1 **then** Device_Fault_e=1, OA_Req_S =0, OA_Req =0, OA_C_e =0, **if** Device_Fault =0 and OA_C and OA_C_e =1 **then** Device_Fault_e=0, OA_Req_S =0, OA_Req =0, OA_C_e =0, **if** FV_activated =1 or activate_FV_C =1 or Device_Fault =1 or Device_Fault_e =1 **then** use FVi, FV_activated_S =1 **else** use PVi, FV_activated_S =0 **if** activate_FV_C =1 or Device_Fault =1 or Device_Fault_e =1 **then** use FVo, activate_FV =1 **else** use PVo, activate_FV =0 iPar_OK_S =iPar_OK **if** Device_Fault_e =1 and Device_Fault =0 **then** OA_Req_S =1, OA_Req =1 **if** OA_C =0 **then** OA_C_e =1
T5	5	6	send safety PDU
T6	6	4	restart host-timer
T7	6	7	-
T8	7	5	**if** Device_Fault =1 and OAD_Nec_C =1 **then** Device_Fault_e=1 **if** (FV_activated =1 or activate_FV_C =1 or Device_Fault =1 or Device_Fault_e =1) **then** use FVi, FV_activated_S =1 **else** use PVi, FV_activated_S =0 **if** activate_FV_C =1 or Device_Fault [b] =1 or Device_Fault_e =1 **then** use FVo, activate_FV =1 **else** use PVo, activate_FV =0 iPar_OK_S =iPar_OK
T9[a]	1	8	use FV, activate_FV =1, FV_activated_S =1, Toggle_h =1, RESETxH

TRAN-SITION	SOURCE STATE	TARGET STATE	ACTION
T10	3	8	restart host-timer, store faults, use FV, activate_FV =1, FV_activated_S =1, Toggle_h = not Toggle_h, RESETxH
T11	4	8	store faults, use FV, activate_FV =1, FV_activated_S =1, Toggle_h = not Toggle_h, RESETxH
T12	6	11	use FV, activate_FV =1, FV_activated_S =1, RESETxH
T13	11	8	store faults, Toggle_h = not Toggle_h, restart host-timer
T14	7	8	restart host-timer, store faults, use FV, activate_FV =1, FV_activated_S =1, Toggle_h = not Toggle_h, RESETxH
T15	8	9	send safety PDU
T16	9	10	restart host-timer
T17	10	5	reset stored faults, OA_Req_S =0, OA_Req =0, OA_C_e =0, Toggle_h = not Toggle_h, RUNxH **if** Device_Fault =1 and OAD_Nec_C =1 **then** Device_Fault_e=1 **if** Device_Fault =0 **then** Device_Fault_e=0 if FV_activated =1 or activate_FV_C =1 or Device_Fault [b] =1 or Device_Fault_e =1 then use FVi, FV_activated_S =1 else use PVi, FV_activated_S =0 if activate_FV_C =1 or Device_Fault [b] =1 or Device_Fault_e =1 then use FVo, activate_FV =1 else use PVo, activate_FV =0 iPar_OK_S =iPar_OK
T18	10	8	store faults, OA_Req =0, OA_Req_S =0, OA_C_e =0, use FV, activate_FV =1, FV_activated_S =1, Toggle_h = not Toggle_h, RESETxH
T19	10	8	OA_Req_S =1, OA_Req =1, if OA_C =0 then OA_C_e =1 use FV, activate_FV =1, FV_activated_S =1, Toggle_h = not Toggle_h, RUNxH
T20	9	8	store faults, OA_Req =0, OA_Req_S =0, OA_C_e =0, use FV, activate_FV =1, FV_activated_S =1, Toggle_h = not Toggle_h, RESETxH restart host-timer

[a] See STATE DESCRIPTION of STATE 1. The statement "store faults" within the transitions can be omitted if T9 is not implemented.

[b] Device_Fault is not considered in the logic operation if F_Passivation =1.

[c] Transition T11 and T14 produce a diagnosis message "Host Diagnosis transmission errors (CRC)".

[d] Transition T10 and T12 produce a diagnosis message "Host Diagnosis transmission errors (Timeout)".

C.1.4 Recommendation for the case without Extensions of F-Host driver Transitions

C.1.4.1 Required behavior in relation to F-Device driver and application

There are F-(Sub)Modules that tolerate the behavior of F-Host driver according C.1.1. E.g. F-(Sub)Modules that leave the status "Device_Fault" TRUE only by manual interaction at the F-(Sub)Module (supply voltage off / on or similar).

But there are also F-(Sub)Modules where additional means are necessary to prevent an automatic switch over from fail-safe values to process values by the F-Host driver in case the "Device_Fault" switches from TRUE to FALSE. This is necessary, if the F-(Sub)Module is used in applications that don't allow an automatic restart.

C.1.4.2 Prevent unintentional restart by application measures

The required reaction (additional means) has to be implemented in the safety PLC program on the F-Host side. The two possiple reactions are shown in Table C.3.

Table C.3 – Prevent unintentional restart by application measures

Variant A: Reaction on the Bit "Device_Fault" of the Status Byte by enforcing Fail-safe values
As soon the bit "Device_Fault" of the Status Byte becomes TRUE store this positive edge in the safety PLC program, activate fail-safe values, and set the interface signal "activate_FV_C" to TRUE. Not before the user has given the acknowledgement using an acknowledgement input, the restart of the safety function is allowed: the interface signal "activate_FV_C" is set to FALSE in the safety PLC program. The precondition for the acknowledgement is, that the "Device_Fault" has changed back from TRUE to FALSE.
Variant B: Reaction on the interface signal "FV_activated_S" by opening the emergency stop chain
The alternative to the reaction on the bit "Device_Fault" is the reaction on the interface signal "FV_activated_S" in the safety PLC program on the F-Host side. If the "FV_activated_S" becomes TRUE, then emergency stop chain has to be opened. Precondition: The emergency stop chain is protected against restart (e.g. using an PLCopen function block "SF_EmergencyStop"). Implementation in the safety PLC program: Negate "FV_activated_S" and build an AND-condition with the other emergency stop switches (normally closed).

C.2 Optional extensions of F-Host driver to "Disable F-(Sub)Module"

Applications such as Energy efficiency and tool change require an F-Host driver state extension, give the user the ability to disable and enable a FSCP 3/1 connection to an F-Device driver while the F-Host driver is running.

NOTE Applications using F_CRC_Seed =1 which restart FSCP communication more often than once per SIL Monitor time require the change of the Modifier value (see 7.1.6) with every restart of the F communication.

In principle this features requires an application where an automatic restart is allowed. That means that the environment of the IO Device (hosting F-(Sub)Modules) for the automatic restart (after deactivation and activation) is secured by other measures.

The F-Host driver gets the additional interface signals Disable_C and Disable_S. With the signal Disable_C the application switches the channels of the F-(Sub)Module to FV. With the signal Disable_S the application gets the acknowledge that the F-Host driver accepts an IO Device (hosting F-(Sub)Modules) switch of (produce timeout) as intentional procedure.

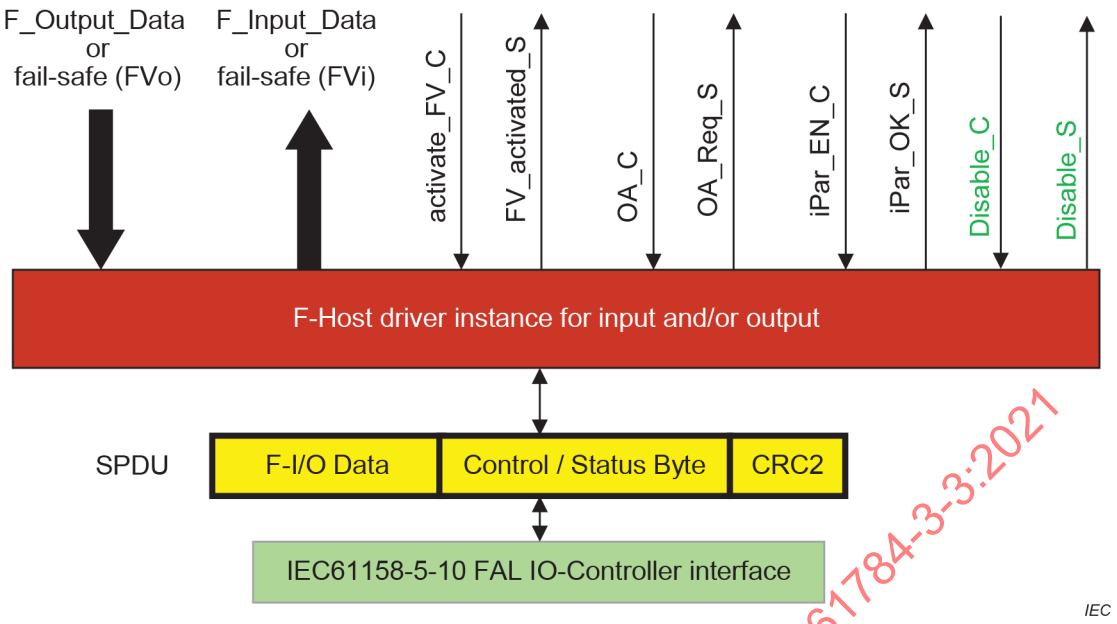


Figure C.2 – F-Host driver application interface with feature Disable F-(Sub)Module

The Figure C.3 shows the states "F-(Sub)Module in F-Host useable" and timing of power off and power on for the F-(Sub)Module and the control signals to be used and the status signals to be monitored by the F-Host application program.

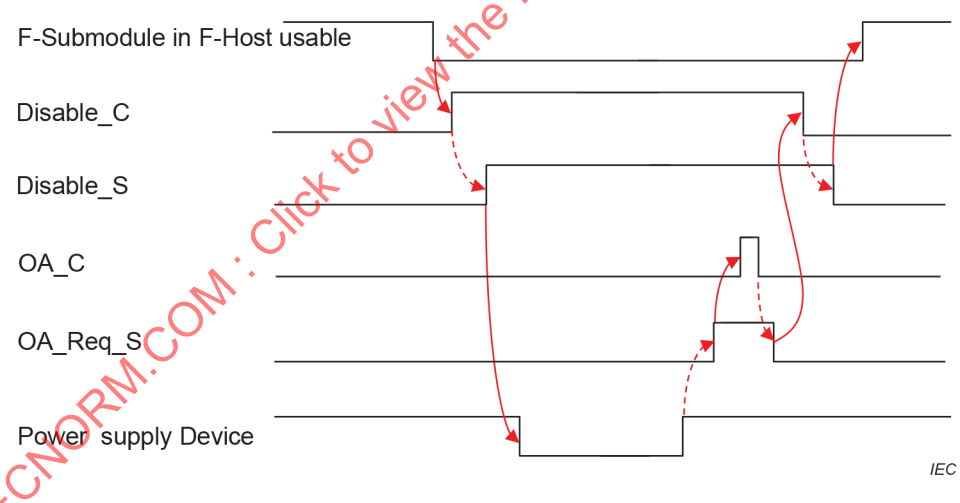


Figure C.3 – Timing diagram to use Disable F-(Sub)Module

The line arrows are actions of the F_Application and the dashed arrows are executed by the F-Host driver.

The F-Host driver state diagram is identical to the state diagram shown in 7.2.2 F-Host driver state diagram.

F-Host driver transitions shall be extended according the green instructions Table C.4 (See variable Disable_C and Disable_S). Table C.5 shows both additions – for the feature "Reaction on Device_Fault in F-Host" and the feature "Disable F-(Sub)Module".

The F-Host driver state diagram according Figure 26 applies.

Table C.4 – F-Host driver transitions – with feature Disable F-(Sub)Module

TRAN-SITION	SOURCE STATE	TARGET STATE	ACTION
T1	1	2	use FV, activate_FV =1, FV_activated_S =1 Toggle_h =1
T2	2	3	send safety PDU
T3	3	4	(re)start host-timer
T4	4	5	Toggle_h = not Toggle_h, RUNxH **if** Disable_C =1 **then** Disable_S =1 **else** Disable_S =0 **if** FV_activated =1 or activate_FV_C =1 or Device_Fault =1 or Disable_S =1 **then** use FVi, FV_activated_S =1 **else** use PVi, FV_activated_S =0 **if** activate_FV_C =1 or Device_Fault =1 or Disable_S =1 **then** use FVo, activate_FV =1 **else** use PVo, activate_FV =0 iPar_OK_S =iPar_OK
T5	5	6	send safety PDU
T6	6	4	restart host-timer
T7	6	7	-
T8	7	5	**if** Disable_C =1 **then** Disable_S =1 **else** Disable_S =0 **if** FV_activated =1 or activate_FV_C =1 or Device_Fault =1 or Disable_S =1 **then** use FVi, FV_activated_S =1 **else** use PVi, FV_activated_S =0 **if** activate_FV_C =1 or Device_Fault [b] =1 or Disable_S =1 **then** use FVo, activate_FV =1 **else** use PVo, activate_FV =0 iPar_OK_S =iPar_OK
T9[a]	1	8	use FV, activate_FV =1, FV_activated_S =1, Toggle_h =1, RESETxH
T10	3	8	restart host-timer, store faults, use FV, activate_FV =1, FV_activated_S =1, Toggle_h = not Toggle_h, RESETxH
T11[c]	4	8	store faults, use FV, activate_FV =1, FV_activated_S =1, Toggle_h = not Toggle_h, RESETxH
T12[d]	6	11	use FV, activate_FV =1, FV_activated_S =1, RESETxH
T13	11	8	store faults, Toggle_h = not Toggle_h, restart host-timer,
T14[c]	7	8	restart host-timer, store faults, use FV, activate_FV =1, FV_activated_S =1, Toggle_h = not Toggle_h, RESETxH
T15	8	9	send safety PDU
T16	9	10	restart host-timer

TRAN-SITION	SOURCE STATE	TARGET STATE	ACTION
T17	10	5	reset stored faults, OA_Req_S =0, OA_Req =0, OA_C_e =0, Toggle_h = not Toggle_h, RUNxH **if** Disable_C =1 **then** Disable_S =1 **else** Disable_S =0 **if** (FV_activated =1 or activate_FV_C =1 or Device_Fault [b] =1 or Disable_S =1) **then** use FVi, FV_activated_S =1 **else** use PVi, FV_activated_S =0 **if** activate_FV_C =1 or Device_Fault [b] =1 or Disable_S =1 **then** use FVo, activate_FV =1 **else** use PVo, activate_FV =0 iPar_OK_S =iPar_OK
T18	10	8	store faults, OA_Req =0, OA_Req_S =0, OA_C_e =0, use FV, activate_FV =1, FV_activated_S =1, Toggle_h = not Toggle_h, RESETxH
T19	10	8	OA_Req_S =1, OA_Req =1, **if** OA_C =0 **then** OA_C_e =1 use FV, activate_FV =1, FV_activated_S =1, Toggle_h = not Toggle_h, RUNxH
T20	9	8	store faults, OA_Req =0, OA_Req_S =0, OA_C_e =0, use FV, activate_FV =1, FV_activated_S =1, Toggle_h = not Toggle_h, RESETxH restart host-timer

[a] See STATE DESCRIPTION of STATE 1. The statement "store faults" within the transitions can be omitted if T9 is not implemented.

[b] Device_Fault is not considered in the logic operation if F_Passivation =1.

[c] if Disable_S =0 then Transition T11 and T14 produce a diagnosis message "Host Diagnosis transmission errors (CRC)".

[d] if Disable_S =0 then Transition T12 produce a diagnosis message "Host Diagnosis transmission errors (Timeout)".

C.3 Combination of "Disable F-(Sub)Module" and "reaction on Device_Fault"

The combinations of Table C.1 and Table C.2 are shown in Table C.5.

Table C.5 – F-Host driver transitions – added with "reaction on Device_Fault" and "Disable F-(Sub)Module"

TRAN-SITION	SOURCE STATE	TARGET STATE	ACTION
T1	1	2	use FV, activate_FV =1, FV_activated_S =1 Toggle_h =1
T2	2	3	send safety PDU
T3	3	4	(re)start host-timer
T4	4	5	Toggle_h = not Toggle_h RUNxH **if** Device_Fault =1 and OAD_Nec_C =1 **then** Device_Fault_e=1, OA_Req_S =0, OA_Req =0, OA_C_e =0, **if** Device_Fault =0 and OA_C and OA_C_e =1 **then** Device_Fault_e=0, OA_Req_S =0, OA_Req =0, OA_C_e =0, if Disable_C =1 **then** Disable_S =1 **else** Disable_S =0 **if** FV_activated =1 or activate_FV_C =1 or Device_Fault =1 or Device_Fault_e =1 or Disable_S =1 **then** use FVi, FV_activated_S =1 **else** use PVi, FV_activated_S =0 **if** (activate_FV_C =1 or Device_Fault =1 or Device_Fault_e =1 or Disable_S =1) **then** use FVo, activate_FV =1 **else** use PVo, activate_FV =0 iPar_OK_S =iPar_OK **if** Device_Fault_e =1 and Device_Fault =0 **then** OA_Req_S =1, OA_Req =1 **if** OA_C =0 **then** OA_C_e =1
T5	5	6	send safety PDU
T6	6	4	restart host-timer
T7	6	7	-
T8	7	5	**if** Device_Fault =1 and OAD_Nec_C =1 **then** Device_Fault_e=1 if Disable_C =1 **then** Disable_S =1 **else** Disable_S =0 **if** FV_activated =1 or activate_FV_C =1 or Device_Fault =1 or Device_Fault_e =1 or Disable_S =1 **then** use FVi, FV_activated_S =1 **else** use PVi, FV_activated_S =0 **if** (activate_FV_C =1 or Device_Fault [b] =1 or Device_Fault_e =1 or Disable_S =1) **then** use FVo, activate_FV =1 **else** use PVo, activate_FV =0 iPar_OK_S =iPar_OK
T9[a]	1	8	use FV, activate_FV =1, FV_activated_S =1, Toggle_h =1, RESETxH
T10	3	8	restart host-timer, store faults, use FV, activate_FV =1, FV_activated_S =1, Toggle_h = not Toggle_h, RESETxH

TRAN-SITION	SOURCE STATE	TARGET STATE	ACTION
T11	4	8	store faults, use FV, activate_FV =1, FV_activated_S =1, Toggle_h = not Toggle_h, RESETxH
T12	6	11	use FV, activate_FV =1, FV_activated_S =1, RESETxH
T13	11	8	store faults, Toggle_h = not Toggle_h, restart host-timer
T14	7	8	restart host-timer, store faults, use FV, activate_FV =1, FV_activated_S =1, Toggle_h = not Toggle_h, RESETxH
T15	8	9	send safety PDU
T16	9	10	restart host-timer
T17	10	5	reset stored faults, OA_Req_S =0, OA_Req =0, OA_C_e =0, Toggle_h = not Toggle_h, RUNxH **if** Device_Fault =1 and OAD_Nec_C =1 **then** Device_Fault_e=1 **if** Device_Fault =0 **then** Device_Fault_e=0 if Disable_C =1 **then** Disable_S =1 **else** Disable_S =0 **if** (FV_activated =1 or activate_FV_C =1 or Device_Fault [b] =1 or Device_Fault_e =1 or Disable_S =1) **then** use FVi, FV_activated_S =1 **else** use PVi, FV_activated_S =0 **if** (activate_FV_C =1 or Device_Fault [b] =1 or Device_Fault_e =1 or Disable_S =1) **then** use FVo, activate_FV =1 **else** use PVo, activate_FV =0 iPar_OK_S =iPar_OK
T18	10	8	store faults, OA_Req =0, OA_Req_S =0, OA_C_e =0, use FV, activate_FV =1, FV_activated_S =1, Toggle_h = not Toggle_h, RESETxH
T19	10	8	OA_Req_S =1, OA_Req =1, **if** OA_C =0 **then** OA_C_e =1 use FV, activate_FV =1, FV_activated_S =1, Toggle_h = not Toggle_h, RUNxH
T20	9	8	store faults, OA_Req =0, OA_Req_S =0, OA_C_e =0, use FV, activate_FV =1, FV_activated_S =1, Toggle_h = not Toggle_h, RESETxH restart host-timer

[a] See STATE DESCRIPTION of STATE 1. The statement "store faults" within the transitions can be omitted if T9 is not implemented.

[b] Device_Fault is not considered in the logic operation if F_Passivation =1.

[c] if Disable_S =0 then Transition T11 and T14 produce a diagnosis message "Host Diagnosis transmission errors (CRC)".

[d] if Disable_S =0 then Transition T10 and T12 produce a diagnosis message "Host Diagnosis transmission errors (Timeout)".

C.4 FSCP 3/1 and PROFIenergy

C.4.1 Use of FSCP 3/1-Devices with PROFIenergy

In case of Power-Down of FSCP 3/1-Devices caused by PROFIenergy the following rule have to be respected:

In case of use IO Device hosting F-Submodules with PROFIenergy the Safety function shall be designed in a way that no manual acknowledge is requested. E.g. laser scanner controls the whole area. These types of safety functions can be used together with PROFIenergy.

NOTE If a manual acknowledge would be requested in case of (re-) start the safety function, this frequent manual acknowledge may lead to a foreseeable misuse.

C.4.2 Sequence in case of PROFIenergy power off on

(Sequence allows an automatic safe restart)

1. Application program switch safety function in "safe state"

2. Sequence for power switch off

Application program shall disable IO Device hosting F-Submodules with the help of F-Host driver control signal Disable_C =1 (see Clause C.2). By acknowledge of F-Host application with status signal Disable_S =1, start PROFIenergy power off.

3. Sequence for power switch on

Start PROFIenergy power on. Activate IO Device hosting F-Submodules by F-Host driver control signal Disable_C =0. By acknowledge with F-Host driver status signal Disable_S =0, restart safety function.

C.5 Requirement multiple F-Hosts communicate with single F-(Sub)Module

The Requirement "Multiple F-Hosts communicate alternating for e.g. one minute with the same F- (Sub)Module" contradicts the FSCP 3/1-Requirement the Retentive Selection of the Codename at the F-Device driver shall be unique in a Subnet of reachable F-Hosts and F-(Sub)Module, see 3.1.2.3.

Adverse reaction:

One F-Host is connected physically with the F-(Sub)Module, but another F-Host (with its F-Host driver instance) – which is not connected physically but by communication – controls the F-(Sub)Module.

Example: Two robots with F-Host functionality aim to use one gripper with F-(Sub)Module functionality consequently. The usage of the gripper with F-(Sub)Module functionality includes the physical attachment of the gripper, the fieldbus connection via CP 3 and logical control using FSCP 3/1 communication. If the gripper with F-(Sub)Module is physically attached to robot_1 with F-Host_1, the robot_2 with F-Host_2 shall not have the logical control of this gripper with F-(Sub)Module using FSCP 3/1 communication although a CP 3 communication from robot_1 and robot_2 to the (Sub)Module is available as it is a fieldbus.

The adverse reaction shall be prevented by the safety application.

Rules in case "Multiple use of one Codename" or "Acceptance of multiple Codenames":

a) Within an area of all reachable F-Device drivers one Codename can be used only by one F-Host at the same time. At the same time means from F-Device driver start until F-Device driver power off.

b) All F-Host drivers which use the same Retentive Selection of the Codename to communicate alternating with the same F-Device driver are highly recommended to add safety mechanisms, which guarantee that only this F-Host driver instances is communicating with the F-Device driver where the IO Device hosting this F-Submodule is connected physically.

C.6 FSCP 3/1 PiR

Parameterization in Run see Amendment PROFIsafe PiR in [64].

Bibliography

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

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

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

[3] IEC 60870-5-1, *Telecontrol equipment and systems – Part 5: Transmission protocols – Section One: Transmission frame formats*

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

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

[6] IEC 61158 (all parts), *Industrial communication networks – Fieldbus specifications*

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

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

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

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

[11] IEC 61508-6:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3*

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

[13] IEC 61158-4-3, *Industrial communication networks – Fieldbus specifications – Part 4-3: Data-link layer protocol specification – Type 3 elements*

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

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

[16] IEC 61784-5 (all parts), *Industrial communication networks – Profiles – Part 5: Installation of fieldbuses*

5 Withdrawn.

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

[18] IEC 61804 (all parts), *Function blocks (FB) for process control and electronic device description language (EDDL)*

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

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

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

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

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

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

[25] IEEE 802.11, *IEEE Standard for Information technology – Telecommunications and information exchange between system – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications*

[26] IEEE 802.15.1-2005, *IEEE Standard for Information technology –Local and metropolitan area networks – Specific requirements – Part 15.1a: Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications for Wireless Personal Area Networks (WPAN)*

[27] ANDREW S. TANENBAUM, DAVID J. WETHERALL, *Computer Networks*, 5th Edition, Prentice Hall, N.J., ISBN-10: 01321269580, ISBN-13: 978-0132126953

[28] W. WESLEY PETERSON, EDWARD J. WELDON, *Error-Correcting Codes*, 2nd Edition 1981, MIT-Press, ISBN 0-262-16-039-0

[29] BRUCE P. DOUGLASS, *Doing Hard Time: Developing Real-Time Systems with UML, Objects, Frameworks, and Patterns*, 2011, Addison-Wesley, ISBN-13: 978-0321774934

[30] DIETER CONRADS, *Datenkommunikation*, 3rd Edition 1996, Vieweg, ISBN-13: 978-0321774934

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

[32] GUY E. CASTAGNOLI, STEFAN BRÄUER, and MARTIN HERRMANN, *Optimization of Cyclic Redundancy-Check Codes with 24 and 32 Parity Bits*, June 1993, IEEE Transactions On Communications, Volume 41, No. 6

[33] SCHILLER F and MATTES T: *An Efficient Method to Evaluate CRC-Polynomials for Safety-Critical Industrial Communication*, Journal of Applied Computer Science, Vol. 14, No 1, pp. 57-80, Technical University Press, Łódź,Poland, 2006

[34] SCHILLER F and MATTES T: *Analysis of CRC-polynomials for Safety-critical Communication by Deterministic and Stochastic Automata*, 6th IFAC Symposium on Fault Detection, Supervision and Safety for Technical Processes, SAFEPROCESS 2006, pp. 1003-1008, Beijing, China, 2006

[35] PROFIBUS Guideline: *Specification for PROFIBUS Device Description and Device Integration, Volume 1: GSD*, V5.1, July 2008. Order-No. 2.122

[36] PROFIBUS Guideline: *PROFIsafe – Environmental Requirements*, V2.6, June 2015. Order-No. 2.232

[37] Profile Guidelines, Part 1: *Identification & Maintenance Functions*, V2.1, May 2016. Order-No. 3.502

[38] PROFIBUS Guideline: *GSDML Specification for PROFINET*, Version 2.34, May 2017. Order-No. 2.352

[39] PROFIBUS Guideline: *Communication Function Blocks on PROFIBUS DP and PROFINET IO*, V2.0, November 2005. Order-No. 2.182

[40] PROFIBUS Profile Guideline, Part 3: *Diagnosis, Alarms, and Time Stamping*, V1.0, June 2004. Order-No. 3.522

[41] PROFINET *Cabling and Interconnection Technology*, Version 4.00, May 2017. Order-No. 2.252

[42] OPC Foundation, < www.opcfoundation.org > [viewed 2020-12-22]

[43] Object Management Group, *Unified Modeling Language: Superstructure*, Version 2.0; Formal/05-07-04; available at < www.omg.com > [viewed 2020-12-22]

[44] NAMUR, *NE97 – Fieldbus for safety-related uses*, 2003; available at < www.namur.de > [viewed 2020-12-22]

[45] REC-xml-20081126, *Extensible Markup Language (XML) 1.0 (Fifth Edition)* – W3C Recommendation 26 November 2008,
available at < www.w3.org/TR/2008/REC-xml-20081126 > [viewed 2020-12-22]

[46] REC-xmlschema-1-20041028, *XML Schema Part 1: Structures (Second Edition)* – W3C Recommendation 28 October 2004,
available at < www.w3.org/TR/2004/REC-xmlschema-1-20041028 > [viewed 2020-12-22]

[47] REC-xmlschema-2-20041028, *XML Schema Part 2: Datatypes (Second Edition)* – W3C Recommendation 28 October 2004,
available at < www.w3.org/TR/2004/REC-xmlschema-2-20041028 > [viewed 2020-12-22]

[48] USB Implementers Forum, Inc, *Universal Serial Bus Revision 2.0 specification*,
available at < http://www.usb.org/developers/docs > [viewed 2020-12-22]

[49] PROFIBUS Specification: Amendment *PA-Devices on PROFIsafe*, V1.01, March 2009; Order-No. 3.042

[50] PROFIBUS Guideline: *Cabling and Assembly*, V1.14, May 2015. Order No. 8.022

[51] PROFIBUS Guideline: *Commissioning*, V1.0.9, May 2015. Order No. 8.032

[52] PROFIBUS Guideline: *PROFIsafe Policy*, V1.5, July 2011. Order No. 2.282

[53] PI Specification: *Amendment PROFIdrive on PROFIsafe*, V3.1.0, February 2019. Order-No. 3.272

[54] Common profile for *PROFINET: Dynamic Reconfiguration,* V1.11, February 2017. Order-No. 7.112

[55] PROFIBUS Profile Guideline, Part 4: *iPar-Server*, V1.0.1, July 2011. Order-No. 3.532

[56] PI Specification: Remote IO for Factory Automation, V1.10, August 2018. Order-No. 3.242

[57] Common profile for *PROFINET:* System Redundancy, V1.11, February 2017. Order-No. 7.122

[58] Guideline for PROFINET: Diagnosis for PROFINET, V1.3, March 2017. Order-No. 7.142

[59] ISO 15745-3, *Industrial automation systems and integration – Open systems application integration framework – Part 3: Reference description for IEC 61158-based control systems*

[60] ISO 15745-4, *Industrial automation systems and integration – Open systems application integration framework – Part 4: Reference description for Ethernet-based control systems*

[61] PROFIBUS Guideline: *PROFIsafe – Test Specification related to PROFIsafe V2.6, V2.3* February 2018. Order-No. 2.242

[62] IEC TR 62390, *Common automation device – Profile guideline*

[63] PI Specification: Tool Calling Interface Specification for PROFIBUS and PROFINET Version 1.1 October 2008 Order No: 2.602

[64] PI Specification: *Amendment PROFIsafe PiR*, November 2019. Order-No. 3.202

SOMMAIRE

AVANT-PROPOS 155
0 Introduction 157
0.1 Généralités 157
0.2 Déclaration de brevets 159
1 Domaine d'application 160
2 Références normatives 160
3 Termes, définitions, symboles, abréviations et conventions 162
3.1 Termes et définitions 162
3.1.1 Termes et définitions communs 162
3.1.2 CPF 3: Termes et définitions supplémentaires 169
3.2 Symboles et abréviations 174
3.2.1 Symboles et abréviations communs 174
3.2.2 CPF 3: Symboles et abréviations supplémentaires 175
3.3 Conventions 176
4 Présentation générale de FSCP 3/1 (PROFIsafe™) 176
5 Généralités 179
5.1 Documents externes de spécifications applicables au profil 179
5.2 Exigences fonctionnelles de sécurité 179
5.3 Mesures de sécurité 180
5.4 Structure de la couche de communication de sécurité 181
5.4.1 Principe des communications de sécurité FSCP 3/1 181
5.4.2 Structures de communication CPF 3 182
5.5 Relations avec la FAL (et DLL, PhL) 184
5.5.1 Modèle d'appareil 184
5.5.2 Relations d'application et de communication 185
5.5.3 Types de données 185
6 Services de la couche de communication de sécurité 186
6.1 Services du pilote de l'hôte F 186
6.2 Services du pilote de l'appareil F 190
6.3 Diagnostic 192
6.3.1 Génération d'alarme de sécurité 192
6.3.2 Diagnostic de la couche de sécurité du (Sous-)Module F 192
7 Protocole de couche de communication de sécurité 194
7.1 Format PDU de sécurité 194
7.1.1 Structure PDU de sécurité 194
7.1.2 Données d'entrée-sortie de sécurité 195
7.1.3 Octet d'état et de contrôle 195
7.1.4 MonitoringNumber (virtuel) 197
7.1.5 Mécanisme du MNR (virtuel) (F_CRC_Seed=0) 198
7.1.6 Mécanisme du MNR (virtuel) (F_CRC_Seed=1) 198
7.1.7 Signature CRC2 (F_CRC_Seed=0) 200
7.1.8 Signature CRC2 (F_CRC_Seed=1) 201
7.1.9 Données d'entrée-sortie autres que de sécurité 202
7.2 Comportement FSCP 3/1 202
7.2.1 Généralités 202

7.2.2 Diagramme d'états du pilote de l'hôte F 203
7.2.3 Diagramme d'états du pilote de l'appareil F 208
7.2.4 Redémarrage du pilote de l'appareil F 211
7.2.5 Diagrammes séquentiels 212
7.2.6 Chronogramme de réinitialisation d'un MonitoringNumber 218
7.2.7 Surveillance des temps de sécurité 219
7.3 Réaction en cas de dysfonctionnement 221
7.3.1 Corruption des données de sécurité 221
7.3.2 Répétition non prévue 222
7.3.3 Séquence incorrecte 222
7.3.4 Perte 222
7.3.5 Retard inacceptable 222
7.3.6 Insertion 222
7.3.7 Déguisement 222
7.3.8 Adressage 223
7.3.9 Hors séquence 223
7.3.10 Bouclage 223
7.3.11 Limites du réseau et routeur 224
7.4 Démarrage F et modification des paramètres lors de l'exécution 224
7.4.1 Procédure de démarrage normalisée 224
8 Gestion de la couche de communication de sécurité 225
8.1 Paramètre F 225
8.1.1 Récapitulatif 225
8.1.2 F_Source/Destination_Address (Nom de code) 226
8.1.3 F_WD_Time (temps de fonctionnement du chien de garde F) 226
8.1.4 F_WD_Time_2 (temps de fonctionnement du chien de garde F secondaire) 226
8.1.5 F_Prm_Flag1 (Paramètres de gestion de la couche de sécurité) 227
8.1.6 F_Prm_Flag2 (Paramètres de gestion de la couche de sécurité) 229
8.1.7 F_iPar_CRC (valeur d'iPar_CRC dans les iParamètres) 230
8.1.8 Calcul de F_Par_CRC (dans les paramètres F) 231
8.1.9 Structure de l'objet de données d'enregistrement du paramètre F 231
8.2 iParamètre et iPar_CRC 232
8.3 Paramétrage de sécurité 233
8.3.1 Objectifs 233
8.3.2 Extensions de sécurité GSDL et GSDML 234
8.3.3 Protection des paramètres de sécurité et des données GSD 236
8.4 Configuration de la sécurité 240
8.4.1 Ordre des types de données d'entrée-sortie 240
8.4.2 Protection de la description des données d'entrée-sortie de sécurité 241
8.4.3 Exemples de sections de type de données DataItem 242
8.5 Utilisation des informations de type de données 246
8.5.1 Pilote de canal de l'hôte F 246
8.5.2 Règles pour les pilotes de canal de l'hôte F normalisés 247
8.5.3 Recommandations relatives à l'utilisation des pilotes de canal de l'hôte F 248
8.6 Mécanismes d'attribution de paramètres de sécurité 250
8.6.1 Attribution du paramètre F 250
8.6.2 Attribution générale d'iParamètres 250

8.6.3 Exigences d'intégration système des outils d'iParamétrage 250
8.6.4 Serveur d'iParamètres 252
9 Exigences système 263
9.1 Voyants et commutateurs 263
9.2 Lignes directrices d'installation 264
9.3 Temps de réponse de la fonction de sécurité 264
9.3.1 Modèle 264
9.3.2 Calcul et optimisation 266
9.3.3 Ajustement des temps de fonctionnement du chien de garde pour FSCP 3/1 268
9.3.4 Prise en charge de l'outil de développement 269
9.3.5 Relances (répétition des messages) 269
9.4 Durée des sollicitations 270
9.5 Contraintes liées au calcul des caractéristiques des systèmes 270
9.5.1 Considérations probabilistes 270
9.5.2 Hypothèses relatives à la sécurité 273
9.5.3 Contraintes non relatives à la sécurité (disponibilité) 273
9.6 Maintenance 273
9.6.1 Mise en service/remplacement du (Sous-)Module F 273
9.6.2 Fonctions d'identification et de maintenance 274
9.7 Manuel de sécurité 274
9.8 Canaux de transmission sans fil 276
9.8.1 Approche du canal noir 276
9.8.2 Disponibilité 276
9.8.3 Mesures de sécurité 276
9.8.4 Applications fixes et mobiles 276
9.9 Relation entre sécurité fonctionnelle et sûreté 276
9.10 Classes de conformité 276
10 Evaluation 278
10.1 Politique de sécurité 278
10.2 Obligations 279
Annexe A (informative) Informations supplémentaires pour les profils de communication de sécurité fonctionnelle de la CPF 3 280
A.1 Calcul de la fonction de hachage 280
A.2 Exemples de valeurs pour les MonitoringNumbers (MNR) 284
Annexe B (informative) Informations pour l'évaluation des profils de communication de sécurité fonctionnelle de la CPF 3 285
Annexe C (normative) Fonctions facultatives 286
C.1 Réaction à Device_Fault dans l'hôte F 286
C.1.1 Situation 286
C.1.2 Documentation destinée à l'utilisateur 286
C.1.3 Extensions facultatives du tableau de transitions du pilote de l'hôte F 286
C.1.4 Recommandation concernant le cas sans extensions des transitions de pilote de l'hôte F 289
C.2 Extensions facultatives du pilote de l'hôte F pour "Désactiver le (Sous-)Module F" 290
C.3 Combinaison de "Désactiver le (Sous-)Module F" et de "réaction à Device_Fault" 293
C.4 FSCP 3/1 et PROFIenergy 295
C.4.1 Utilisation d'appareils FSCP 3/1 avec PROFIenergy 295

C.4.2 Séquence en cas d'activation de la mise hors tension par PROFIenergy 295
C.5 Exigence "Plusieurs hôtes F communiquent avec un (Sous-)Module F unique" 296
C.6 PiR FSCP 3/1 296
Bibliographie 297

Figure 1 – Relations entre l'IEC 61784-3 et d'autres normes (machines) 157
Figure 2 – Relations entre l'IEC 61784-3 et d'autres normes (processus) 158
Figure 3 – Conditions préalables de communication de base pour le protocole FSCP 3/1 177
Figure 4 – Structure d'un PDU de sécurité FSCP 3/1 178
Figure 5 – Communication de sécurité avec CPF 3 178
Figure 6 – Système de transmission CPF 3 normalisé 181
Figure 7 – Architecture de la couche de sécurité 182
Figure 8 – Couches de communication de base 182
Figure 9 – Croisement des limites du réseau avec les routeurs 183
Figure 10 – Voies de transmission de sécurité complètes 184
Figure 11 – Modèle d'appareil entrée-sortie 185
Figure 12 – Structure de communication FSCP 3/1 186
Figure 13 – Interface d'application F des instances du pilote de l'hôte F 187
Figure 14 – Motivation pour l'option "Passivation relative aux canaux" 188
Figure 15 – Interfaces du pilote de l'appareil F 191
Figure 16 – PDU de sécurité pour CPF 3 194
Figure 17 – Octet d'état 195
Figure 18 – Octet de contrôle 196
Figure 19 – Fonction du bit de bascule 197
Figure 20 – Intégration du MonitoringNumber 198
Figure 21 – Génération de signature CRC2 du pilote de l'hôte F (F_CRC_Seed=0) 200
Figure 22 – Détails du calcul de la signature CRC2 (F_CRC_Seed=0) 201
Figure 23 – Calcul de signature CRC2 (F_CRC_Seed=1) 201
Figure 24 – Détails du calcul de la signature CRC2 (F_CRC_Seed=1) 202
Figure 25 – Relation de communication de la couche de sécurité 203
Figure 26 – Diagramme d'états du pilote de l'hôte F 203
Figure 27 – Diagramme d'états du pilote de l'appareil F 208
Figure 28 – Interaction du pilote de l'hôte F et du pilote de l'appareil F pendant le démarrage 212
Figure 29 – Interaction du pilote de l'hôte F et du pilote de l'appareil F pendant la mise hors tension > sous tension de l'hôte F 213
Figure 30 – Interaction du pilote de l'hôte F et du pilote de l'appareil F pendant un report de mise sous tension 214
Figure 31 – Interaction du pilote de l'hôte F et du pilote de l'appareil F pendant la mise hors tension → sous tension 215
Figure 32 – Interaction lorsque le pilote de l'hôte F reconnaît une erreur CRC 216
Figure 33 – Interaction lorsque le pilote de l'appareil F reconnaît une erreur CRC 217
Figure 34 – Impact du signal de réinitialisation du MNR 218

Figure 35 – Surveillance de la durée d'acheminement du message hôte F ↔ (Sous-)Module F 219
Figure 36 – Temps de fonctionnement étendu du chien de garde à la demande 221
Figure 37 – Effet de F_WD_Time_2 227
Figure 38 – F_Prm_Flag1 227
Figure 39 – F_Check_iPar 228
Figure 40 – F_SIL 228
Figure 41 – F_CRC_Length 228
Figure 42 – F_CRC_Seed 229
Figure 43 – F_Prm_Flag2 229
Figure 44 – F_Passivation 230
Figure 45 – F_Block_ID 230
Figure 46 – F_Par_Version 230
Figure 47 – Paramètre F 231
Figure 48 – Bloc iParamètre 233
Figure 49 – Extension du paramètre F dans la spécification GSDML 235
Figure 50 – Signature F_Par_CRC incluant iPar_CRC 236
Figure 51 – Pilote de canal de l'hôte F en tant que "colle" entre le (Sous-)Module F et le programme d'application 247
Figure 52 – Exemple de présentation d'un pilote de canal de l'hôte F 248
Figure 53 – Attribution du paramètre F pour (Sous-)Modules F 250
Figure 54 – Intégration système des outils CPD 252
Figure 55 –Mécanisme de serveur d'iParamètres (mise en service) 253
Figure 56 – Mécanisme du serveur d'iParamètres (remplacement du (Sous-)Module F, par exemple) 254
Figure 57 – Codage de la demande de serveur d'iParamètres ("modèle d'état") 255
Figure 58 – Codage de SR_Type 257
Figure 59 – Codage de la demande de serveur d'iParamètres ("modèle d'alarme") 257
Figure 60 – Diagramme d'états du serveur d'iParamètres 260
Figure 61 – Exemple de fonction de sécurité avec chemin de temps de réponse critique 264
Figure 62 – Modèle simplifié de temps de réponse classique 265
Figure 63 – Distributions de fréquence des temps de réponse classiques du modèle 266
Figure 64 – Contexte de délais et de temps de fonctionnement du chien de garde 267
Figure 65 – Sections de temporisation formant le F_WD_Time de FSCP 3/1 268
Figure 66 – Distribution de fréquence des temps de réponse avec relances de message 270
Figure 67 – Probabilités d'erreurs résiduelles du polynôme CRC 24 bits 271
Figure 68 – Probabilités d'erreurs résiduelles du polynôme CRC 32 bits 271
Figure 69 – Surveillance des messages corrompus 272
Figure A.1 – Procédure "C" classique de contrôle de redondance cyclique 280
Figure C.1 – Interface d'application du pilote de l'hôte F avec la fonction Réaction à Device_Fault 286
Figure C.2 – Interface d'application du pilote de l'hôte F avec la fonction Désactiver le (Sous-)Module F 290
Figure C.3 – Diagramme de temporisation pour utiliser Désactiver le (Sous-)Module F 291

Tableau 1 – Mesures déployées pour maîtriser les erreurs 180
Tableau 2 – Types de données pour FSCP 3/1 185
Tableau 3 – F_MessageTrailer pour FSCP 3/1 185
Tableau 4 – Messages de diagnostic de la couche de sécurité 193
Tableau 5 – Entrée de mémoire tampon sur erreur CRC2 194
Tableau 6 – MonitoringNumber du SPDU d'un pilote de l'hôte F 198
Tableau 7 – MonitoringNumber du SPDU d'un pilote de l'appareil F 198
Tableau 8 – MonitoringNumber du SPDU d'un pilote de l'hôte F 199
Tableau 9 – MonitoringNumber du SPDU d'un pilote de l'appareil F 199
Tableau 10 – Définition des termes utilisés dans le diagramme d'états du pilote de l'hôte F 204
Tableau 11 – Etats et transitions du pilote de l'hôte F 205
Tableau 12 – Définition des termes utilisés dans la Figure 27 208
Tableau 13 – Etats et transitions du pilote de l'appareil F 209
Tableau 14 – Temps de l'appareil de surveillance SIL 220
Tableau 15 – Limites du réseau de sécurité 224
Tableau 16 – Ordre des octets de nom de code 226
Tableau 17 – Combinaisons admises de F_CRC_Seed et de F_Passivation 229
Tableau 18 – Mots clés GSDL des paramètres F et des structures d'entrée-sortie F 234
Tableau 19 – Algorithme de génération de CRC0 237
Tableau 20 – Exemple de GSD dans la notation GSDL 238
Tableau 21 – Exemple de GSD dans la notation GSDML 239
Tableau 22 – Flux d'octets sérialisé pour les exemples 240
Tableau 23 – Ordre des types de données d'entrée-sortie 241
Tableau 24 – Eléments de structure de données d'entrée-sortie 242
Tableau 25 – Section DataItem de F_IN_OUT_1 243
Tableau 26 – DATA_STRUCTURE_CRC de F_IN_OUT_1 243
Tableau 27 – Section DataItem de F_IN_OUT_2 244
Tableau 28 – DATA_STRUCTURE_CRC de F_IN_OUT_2 244
Tableau 29 – Section DataItem de F_IN_OUT_5 245
Tableau 30 – DATA_STRUCTURE_CRC de F_IN_OUT_5 245
Tableau 31 – Section DataItem de F_IN_OUT_6 246
Tableau 32 – DATA_STRUCTURE_CRC de F_IN_OUT_6 246
Tableau 33 – Modèles de pilotes de canal de l'hôte F 248
Tableau 34 – Exigences pour l'iParamétrage 251
Tableau 35 – Spécificateur de la demande de serveur d'iParamètres 256
Tableau 36 – Structure de Read_RES_PDU ("read record") 258
Tableau 37 – Structure de Write_REQ_PDU ("write record") 258
Tableau 38 – Structure de Pull_RES_PDU ("Pull") 259
Tableau 39 – Structure de Push_REQ_PDU ("Push") 259
Tableau 40 – Etats et transitions du serveur d'iParamètres 261
Tableau 41 – Mesures de gestion du serveur d'iParamètres 262

Tableau 42 – Définition des termes utilisés dans la Figure 69 272
Tableau 43 – Informations à inclure dans le manuel de sécurité 274
Tableau 44 – Exigences de classe de conformité de l'hôte F 277
Tableau 45 – Principales caractéristiques des versions de protocole 278
Tableau 46 – Matrice de conformité du pilote de l'hôte F/du pilote de l'appareil F 278
Tableau A.1 – Tableau "Crctab24" de calculs de la signature CRC 24 bits 281
Tableau A.2 – Tableau "Crctab32" de calculs de la signature CRC 32 bits 282
Tableau A.3 – Tableau "Crctab16" de calculs de la signature CRC 16 bits 283
Tableau A.4 – Valeurs de CN_incrNR_64 et de MNR pour le PDU de l'hôte F 284
Tableau C.1 – Définition de termes supplémentaires utilisés dans les transitions de pilote 287
Tableau C.2 – Transitions de pilote de l'hôte F – ajoutées avec la réaction à Device_Fault 287
Tableau C.3 – Empêcher un redémarrage involontaire par des mesures d'application 289
Tableau C.4 – Transitions du pilote de l'hôte F – avec la fonction Désactiver le (Sous-)Module F 291
Tableau C.5 – Transitions du pilote de l'hôte F – ajoutées avec "réaction à Device_Fault" et "Désactiver le (Sous-)Module F" 293

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

RÉSEAUX DE COMMUNICATION INDUSTRIELS – PROFILS –

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

AVANT-PROPOS

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

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

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

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

- modifications rédactionnelles concernant l'opportunité, transformation des commentaires dans le diagramme en instructions;

- utilisation des abréviations de PROFINET;
- informations supplémentaires concernant les contrôles et le manuel de sécurité pour les types d'adresses PROFIsafe 1 et 2;
- informations supplémentaires concernant PFDavg, prise en charge de l'essai automatique, ajout de messages de diagnostic;
- explication et spécification de diagrammes d'états facultatifs concernant la réaction en cas d'anomalie de l'appareil;
- nouvelle variable facultative "OAD_Nec_C" pour la fonction facultative "Réaction à Device_Fault dans F_Host";
- spécification de la fonction facultative de l'hôte F pour "Désactiver le (Sous-)Module F";
- spécification des exigences concernant FSCP 3/1 et PROFIenergy;
- spécification des exigences concernant la communication de plusieurs hôtes F avec un (Sous-)Module F unique; mise à jour du manuel de sécurité;
- corrections d'erreurs diverses, de fautes de frappe, et mises à jour des références;
- mise à jour de la bibliographie.

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

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

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

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

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

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

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

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

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

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

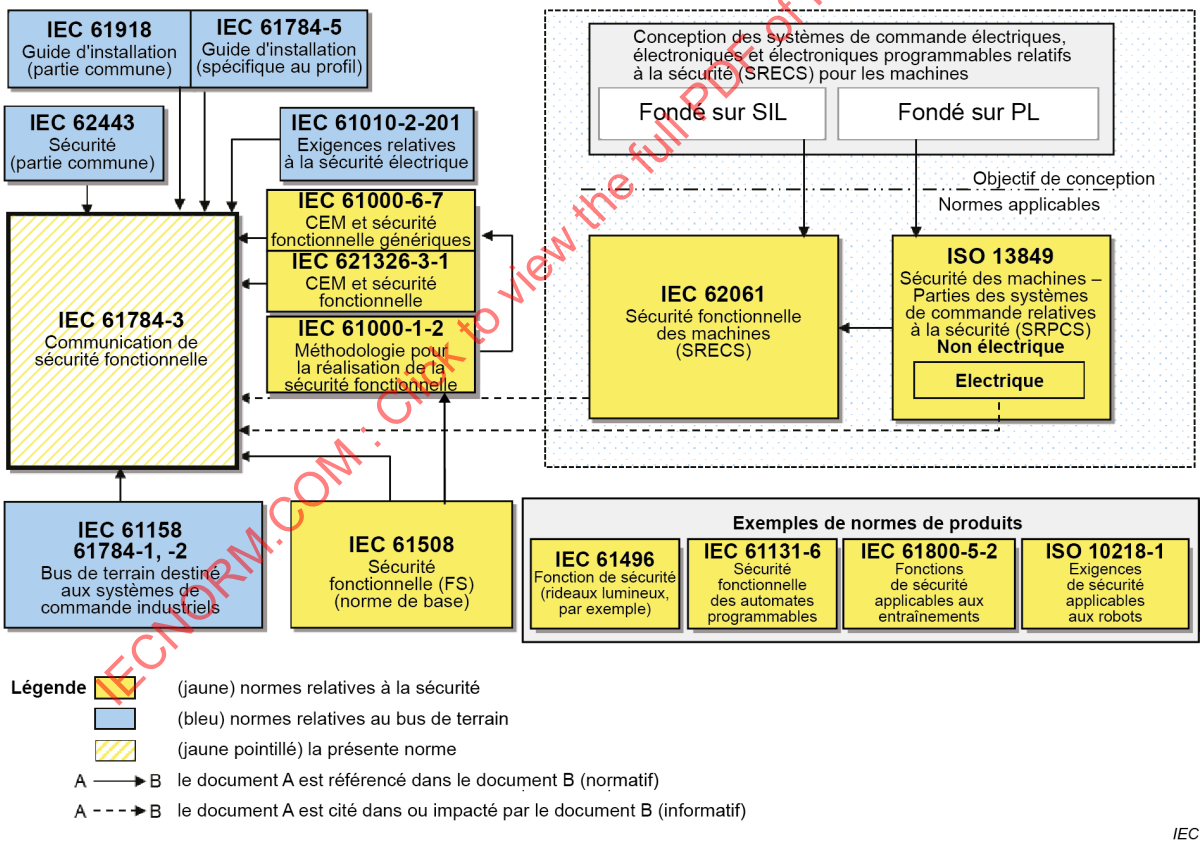
0 Introduction

0.1 Généralités

L'IEC 61158 (toutes les parties), relative aux bus de terrain, ainsi que ses normes associées IEC 61784-1 et IEC 61784-2, définissent un ensemble de protocoles de communication qui assurent la commande répartie d'applications automatisées. La technologie de bus de terrain est désormais reconnue et bien éprouvée. Les améliorations des bus de terrain se poursuivent; elles couvrent des applications pour des domaines comme les applications en temps réel relatives à la sécurité.

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

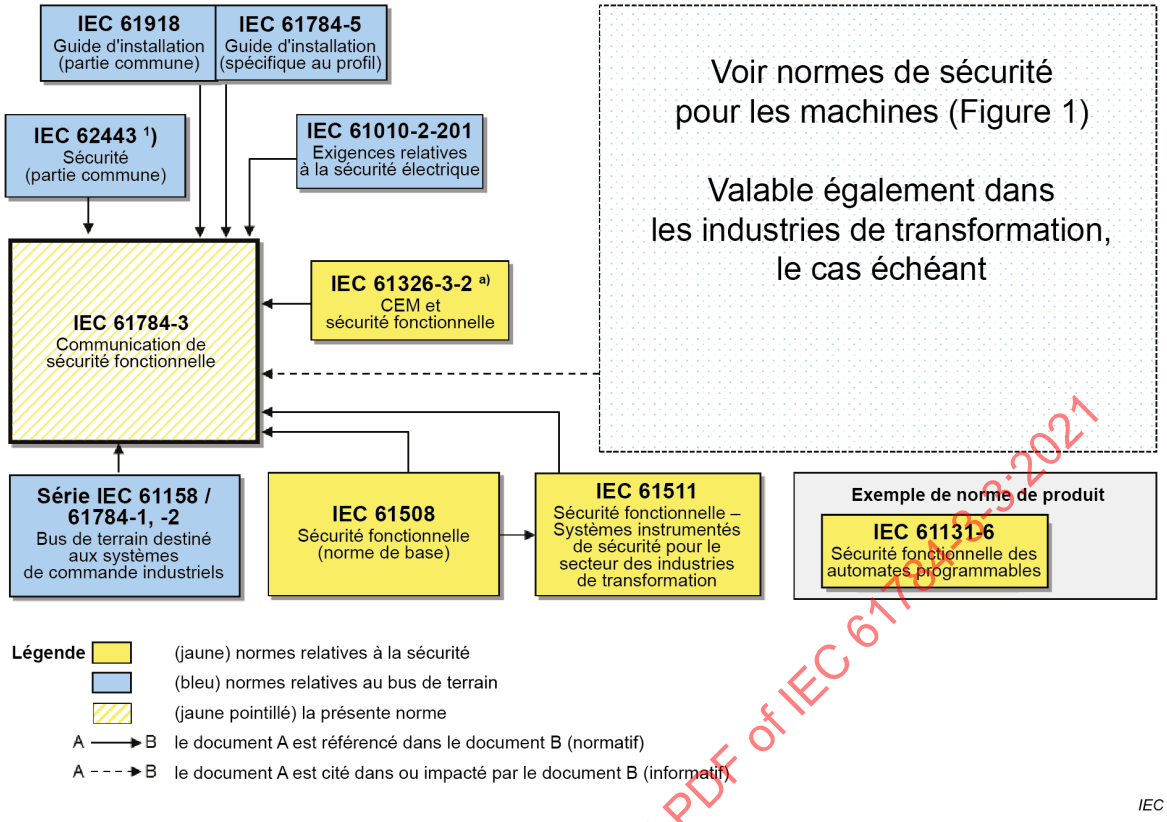
La Figure 1 représente les relations entre l'IEC 61784-3 (toutes les parties) et les normes pertinentes relatives à la sécurité et aux bus de terrain dans un environnement de machines.



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

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

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



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

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

Les couches de communication de sécurité mises en œuvre dans le cadre de systèmes relatifs à la sécurité conformément à l'IEC 61508 (toutes les parties) assurent la confiance nécessaire à accorder à la transmission de messages (informations) entre plusieurs participants sur un bus de terrain dans un système relatif à la sécurité ou une fiabilité suffisante dans le comportement de sécurité en cas d'erreurs ou de défaillances du bus de terrain.

Les couches de communication de sécurité spécifiées dans l'IEC 61784-3 (toutes les parties) permettent de s'assurer qu'un bus de terrain peut être utilisé dans des applications qui nécessitent une sécurité fonctionnelle jusqu'au niveau d'intégrité de sécurité (SIL) spécifié par son profil de communication de sécurité fonctionnelle correspondant.

La revendication du SIL qui en résulte pour un système dépend de la mise en œuvre du profil de communication de sécurité fonctionnelle (FSCP) retenu au sein du système (la mise en œuvre du profil de communication de sécurité fonctionnelle dans un appareil normal ne suffit pas à le qualifier d'appareil de sécurité).

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

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

0.2 Déclaration de brevets

La Commission Electrotechnique Internationale (IEC) attire l'attention sur le fait qu'il est déclaré que la conformité avec les dispositions du présent document peut impliquer l'utilisation de brevets intéressant les profils de communication de sécurité fonctionnelle pour la famille 3. L'IEC ne prend pas position quant à la preuve, à la validité et à la portée de ces droits de propriété.

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

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

RÉSEAUX DE COMMUNICATION INDUSTRIELS – PROFILS –

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

1 Domaine d'application

La présente partie de l'IEC 61784-3 (toutes les parties) spécifie une couche de communication de sécurité (services et protocole) qui repose sur la CPF 3 de l'IEC 61784-1 et les Types 3 et 10 de l'IEC 61784-2 (CP 3/1, CP 3/2, CP 3/4, CP 3/5 et CP 3/6) et de l'IEC 61158. Elle identifie les principes applicables aux communications de sécurité fonctionnelle définies dans l'IEC 61784-3, qui correspondent à cette couche de communication de sécurité. Cette couche de communication de sécurité est destinée à être mise en œuvre uniquement sur les appareils de sécurité.

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

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

Le présent document fournit des lignes directrices aux développeurs, ainsi qu'aux évaluateurs d'appareils et de systèmes conformes.

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

2 Références normatives

Les documents suivants sont cités dans le texte de sorte qu'ils constituent, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

IEC 60204-1, *Sécurité des machines – Equipement électrique des machines – Partie 1: Exigences générales*

IEC 61000-6-7, *Compatibilité électromagnétique (CEM) – Partie 6-7: Normes génériques – Exigences d'immunité pour les équipements visant à exercer des fonctions dans un système lié à la sécurité (sécurité fonctionnelle) dans des sites industriels*

IEC 61010-2-201:2017, *Règles de sécurité pour appareils électriques de mesurage, de régulation et de laboratoire – Partie 2-201: Exigences particulières relatives aux équipements de commande*

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

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

IEC 61158-5-3, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 5-3: Définition des services de la couche application – Eléments de type 3*

IEC 61158-5-10, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 5-10: Définition des services de la couche application – Eléments de type 10*

IEC 61158-6-3, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 6-3: Spécification du protocole de couche application – Eléments de type 3*

IEC 61158-6-10, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 6-10: Spécification du protocole de couche application – Eléments de type 10*

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

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

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

IEC 61508-2, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 2: Exigences pour les systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité*

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

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

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

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

IEC 61784-5-3, *Réseaux de communication industriels – Profils – Partie 5-3: Installation des bus de terrain – Profils d'installation pour CPF 3*

IEC 61918:2018, *Réseaux de communication industriels – Installation de réseaux de communication dans des locaux industriels*

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

IEC 62280:2014, *Applications ferroviaires – Systèmes de signalisation, de télécommunication et de traitement – Communication de sécurité dans les systèmes de transmission*

IEC 62443 (toutes les parties), *Réseaux industriels de communication – Sécurité dans les réseaux et les systèmes*

ISO 13849-1:2015, *Sécurité des machines - Parties des systèmes de commande relatives à la sécurité - Partie 1: Principes généraux de conception*

ISO 13849-2:2012, *Sécurité des machines - Parties des systèmes de commande relatives à la sécurité - Partie 2: Validation*

3 Termes, définitions, symboles, abréviations et conventions

3.1 Termes et définitions

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

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

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

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

3.1.1 Termes et définitions communs

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

3.1.1.1
élément de réseau actif
élément de réseau contenant des composants actifs du point de vue électrique et/ou optique et permettant d'étendre le réseau

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

[SOURCE: IEC 61918:2018, 3.1.2]

3.1.1.2
disponibilité
probabilité, pour un système automatisé, qu'il ne se produise pas de condition opérationnelle non satisfaisante, par exemple la perte de production, pendant une période donnée

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

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

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

3.1.1.5
canal de communication
connexion logique entre deux points limites d'un *système de communication*

3.1.1.6
système de communication
ensemble de matériels, de logiciels et de supports de propagation qui permet la transmission de *messages* (ISO/IEC 7498-1, couche d'application) d'une application à une autre

3.1.1.7
connexion
liaison logique entre deux objets d'application au sein du même appareil ou d'appareils différents

3.1.1.8
contrôle de redondance cyclique
CRC
<valeur> donnée redondante déduite, et enregistrée ou transmise simultanément, d'un bloc de données afin de détecter toute corruption des données

<méthode> procédure utilisée pour calculer les données redondantes

Note 1 à l'article: Les termes "code CRC" et "signature CRC", ainsi que les étiquettes comme CRC1, CRC2, peuvent également être utilisés dans le présent document pour se référer aux données redondantes.

Note 2 à l'article: Voir également [27],[28][2].

3.1.1.9
système de communication défini
canal défini
nombre fixe ou nombre maximal fixe d'éléments reliés par un *système de communication* à *bus de terrain*, dont les propriétés sont connues et fixées, par exemple les conditions d'installation, l'immunité électromagnétique, les *éléments (actifs) de réseau* industriel, et où le *risque* d'accès non autorisé est réduit à un niveau toléré conformément au modèle de cycle de vie de l'IEC 62443 (toutes les parties), en utilisant par exemple des zones et des conduits

3.1.1.10
DLPDU
DÉCONSEILLÉ: trame
unité de données de protocole de liaison de données

Note 1 à l'article: L'abréviation "DLPDU" est dérivée du terme anglais développé correspondant "data link protocol data unit".

3.1.1.11
erreur
écart ou discordance entre une valeur ou une condition calculée, observée ou mesurée et la valeur ou la condition vraie, prescrite ou théoriquement correcte

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

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

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

3.1.1.12
code explicite
code de mesure de sécurité réellement transmis dans le SPDU et connu de l'émetteur et du destinataire

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

3.1.1.13
données explicites
données qui sont transmises

Note 1 à l'article: Les données explicites sont définies par opposition aux données implicites.

3.1.1.14
défaillance
cessation de l'aptitude d'une unité fonctionnelle à accomplir une fonction requise ou à fonctionner comme prévu

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

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

3.1.1.15
anomalie
condition anormale qui peut entraîner une réduction de capacité ou la perte de capacité d'une unité fonctionnelle à accomplir une fonction requise

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

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

3.1.1.16
bus de terrain
système de communication fondé sur le transfert de données en série et utilisé dans des applications d'automatisation industrielle ou de commande de processus

3.1.1.17
système de bus de terrain
système qui utilise un *bus de terrain* avec des appareils reliés

3.1.1.18
séquence de contrôle de trame
FCS
données redondantes issues d'un bloc de données d'une DLPDU (trame), qui utilisent une fonction de hachage et enregistrées ou transmises avec le bloc de données, afin de déterminer l'altération des données

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

Note 2 à l'article: Voir également [27], [28].

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

3.1.1.19
profil de communication de sécurité fonctionnelle
FSCP
spécification de technologie pour la mise en œuvre d'une SCL

Note 1 à l'article: L'abréviation "FSCP" est dérivée du terme anglais développé correspondant "functional safety communication profile".

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

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

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

3.1.1.21
danger
source potentielle de dommage

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

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

3.1.1.22
code implicite
code de mesure de sécurité qui n'est pas transmis dans le SPDU, mais qui est connu de l'émetteur et du destinataire

3.1.1.23
données implicites
données additionnelles qui ne sont pas transmises, mais sont connues de l'émetteur et du récepteur, et qui sont utilisées pour le codage et le décodage du message/SPDU

Note 1 à l'article: Les données implicites sont définies par opposition aux données explicites.

[SOURCE: IEC 62280:2014, 3.1.25, modifié – ajout de ", et qui sont utilisées pour le codage et le décodage du message/SPDU"]

3.1.1.24
maître
entité de communication capable d'initier et de programmer des activités de communication effectuées par d'autres stations qui peuvent être des maîtres ou des esclaves

3.1.1.25
message
<théorie de l'information et théorie des communications> suite ordonnée de caractères (généralement des octets) destinée à communiquer des informations

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

3.1.1.26
essai périodique
essai périodique destiné à détecter les défaillances dangereuses cachées d'un *système relatif à la sécurité* de telle sorte que, si nécessaire, une réparation puisse rétablir le système dans une condition "comme neuf" ou dans une condition aussi proche que possible de celle-ci

Note 1 à l'article: Un essai périodique est destiné à confirmer que l'état du système relatif à la sécurité assure l'intégrité de sécurité spécifiée.

[SOURCE: IEC 61508-4:2010, 3.8.5, modifié par remplacement des quatre notes par une autre note]

3.1.1.27
niveau de performance
PL
niveau discret d'aptitude de parties relatives à la sécurité à réaliser une fonction de sécurité dans des conditions prévisibles

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

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

3.1.1.28
très basse tension de protection
TBTP
circuit électrique relié à la terre de protection dont la tension ne peut pas dépasser les valeurs suivantes:

CONDITION NORMALE et CONDITION DE PREMIER DEFAUT: Les niveaux de tension alternative sont de 30 V efficace, de 42,4 V crête et le niveau de tension continue est de 60 V. Pour un équipement destiné à être utilisé dans des EMPLACEMENTS HUMIDES, les niveaux de tension alternative sont de 16 V efficace, de 22,6 V crête et le niveau de tension continue est de 35 V.

[SOURCE: IEC 61010-2-201:2017, 3.111, modifié – suppression de "circuit à" du terme et suppression de la source]

3.1.1.29
redondance
existence de plusieurs moyens pour accomplir une fonction requise ou pour représenter des informations

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

3.1.1.30
probabilité d'erreurs résiduelles
RP
probabilité de non-détection d'une erreur par les mesures de sécurité SCL

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

3.1.1.31
taux d'erreurs résiduelles
taux statistique de défaut de détection d'erreurs par les mesures de sécurité SCL

3.1.1.32
risque
combinaison de la probabilité d'un dommage et de sa gravité

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

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

3.1.1.33
canal de communication de sécurité
canal de communication qui commence au sommet de la SCL de la source et qui se termine au sommet de la SCL du collecteur

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

3.1.1.34
couche de communication de sécurité
SCL
couche de communication située au-dessus de la FAL qui comprend toutes les mesures supplémentaires nécessaires qui permettent d'assurer la transmission de données en toute sécurité conformément aux exigences de l'IEC 61508

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

3.1.1.35
connexion de sécurité
connexion qui utilise le protocole de sécurité pour des transactions de communications

3.1.1.36
données de sécurité
données transmises par un réseau de sécurité qui utilise un protocole de sécurité

Note 1 à l'article: La couche de communication de sécurité n'assure pas la sécurité des données proprement dites, mais uniquement la transmission en toute sécurité de ces dernières.

3.1.1.37
appareil de sécurité
appareil conçu conformément à l'IEC 61508 et qui met en œuvre le profil de communication de sécurité fonctionnelle

3.1.1.38
très basse tension de sécurité
TBTS
circuit électrique non relié à la terre de protection dont la tension ne peut pas dépasser les valeurs suivantes:

CONDITION NORMALE et CONDITION DE PREMIER DEFAUT: Les niveaux de tension alternative sont de 30 V efficace, de 42,4 V crête et le niveau de tension continue est de 60 V. Pour un équipement destiné à être utilisé dans des EMPLACEMENTS HUMIDES, les niveaux de tension alternative sont de 16 V efficace, de 22,6 V crête et le niveau de tension continue est de 35 V.

[SOURCE: IEC 61010-2-201:2017, 3.112, modifié – suppression de "circuit à" du terme et suppression de la source]

3.1.1.39
fonction de sécurité
fonction à réaliser par un système E/E/PE relatif à la sécurité ou par un dispositif externe de réduction de risque, prévue pour assurer ou maintenir un état de sécurité de l'EUC par rapport à un événement dangereux spécifique

[SOURCE: IEC 61508-4:2010, 3.5.1, modifié – références et exemple supprimés]

3.1.1.40
temps de réponse de la fonction de sécurité
SFRT
temps écoulé dans le cas le plus défavorable à la suite de l'activation d'un capteur de sécurité relié à un bus de terrain, avant d'atteindre l'état de sécurité correspondant de ses actionneurs de sécurité, du fait d'erreurs ou de défaillances dans la fonction de sécurité

Note 1 à l'article: Ce concept, introduit dans l'IEC 61784-3:2021, 5.2.4, est traité par les profils de communication de sécurité fonctionnelle définis dans le présent document.

Note 2 à l'article: L'abréviation "SFRT" est dérivée du terme anglais développé correspondant "safety function response time".

3.1.1.41
niveau d'intégrité de sécurité
SIL
niveau discret (parmi quatre possibles) correspondant à une gamme de valeurs d'intégrité de sécurité où le niveau 4 d'intégrité de sécurité possède le plus haut degré d'intégrité et le niveau 1 possède le plus bas

Note 1 à l'article: Les objectifs chiffrés de défaillance (voir l'IEC 61508-4:2010, 3.5.17) pour les quatre niveaux d'intégrité de sécurité sont indiqués dans les Tableaux 2 et 3 de l'IEC 61508-1:2010.

Note 2 à l'article: Les niveaux d'intégrité de sécurité sont utilisés pour spécifier les exigences concernant l'intégrité de sécurité des fonctions de sécurité à allouer aux systèmes E/E/PE relatifs à la sécurité.

Note 3 à l'article: Un niveau d'intégrité de sécurité (SIL) ne constitue pas une propriété d'un système, sous-système, élément ou composant. L'interprétation correcte de l'expression "système relatif à la sécurité à SIL*n*" (où *n* est 1, 2, 3 ou 4) signifie que le système est potentiellement capable de prendre en charge les fonctions de sécurité avec un niveau d'intégrité de sécurité jusqu'à *n*.

Note 4 à l'article: L'abréviation "SIL" est dérivée du terme anglais développé correspondant "safety integrity level".

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

3.1.1.42
mesure de sécurité
mesure qui permet de contrôler les *erreurs* de communication éventuelles, qui est conçue et mise en œuvre conformément aux exigences de l'IEC 61508

Note 1 à l'article: Dans la pratique, plusieurs mesures de sécurité sont combinées pour atteindre le niveau d'intégrité de sécurité exigé.

Note 2 à l'article: Les *erreurs* de communication et les mesures de sécurité associées sont décrites dans l'IEC 61784-3:2021, 5.3 et 5.4.

3.1.1.43
PDU de sécurité
SPDU
PDU transféré par le biais du canal de communication de sécurité

Note 1 à l'article: Le SPDU peut comporter plusieurs exemplaires des données de sécurité qui utilisent des structures de codage et des fonctions de hachage différentes, associées à des parties explicites de protections supplémentaires, par exemple une clé, un nombre de séquences ou un mécanisme de datation.

Note 2 à l'article: Les SCL redondantes peuvent fournir deux versions différentes du SPDU en vue de son insertion dans des champs séparés de la trame de bus de terrain.

Note 3 à l'article: En ce qui concerne CP 3/4 à 3/6, il s'agit de l'unité de données de protocole d'application (APDU).

Note 4 à l'article: L'abréviation "SPDU" est dérivée du terme anglais développé correspondant "safety PDU".

3.1.1.44
application relative à la sécurité
programmes conçus conformément à l'IEC 61508 pour satisfaire aux exigences SIL de l'application

3.1.1.45
système relatif à la sécurité
système qui exécute les *fonctions de sécurité* conformément à l'IEC 61508

3.1.1.46
esclave
entité de communication capable de recevoir des messages et de les envoyer en réponse à une autre entité de communication qui peut être maître ou esclave, mais pas d'initier des activités de communication

3.1.1.47
déclenchement parasite
déclenchement provoqué par le système de sécurité sans injonction du processus

3.1.1.48
répartition uniforme
loi de probabilité où toutes les valeurs d'un ensemble fini sont susceptibles de se produire

Note 1 à l'article: Pour un champ de longueur de bit i, la probabilité d'occurrence d'une valeur particulière de champ est égale à 2^{-i} étant donné que la somme de toutes les probabilités d'occurrence est égale à 1.

3.1.2 CPF 3: Termes et définitions supplémentaires

3.1.2.1
type d'adresse
type d'adresse 1 si F_DestAdd est vérifié uniquement
type d'adresse 2 si F_SourceAdd est vérifié avec F_DestAdd

3.1.2.2
bit
chiffre binaire
informations binaires codées sans unité technique

3.1.2.3
nom de code
Codename
identification de la relation de communication de sécurité entre homologues de communication de sécurité.

Note 1 à l'article: Le nom de code est utilisé pour l'identification unique de la relation de communication de sécurité.

Note 2 à l'article: Le nom de code est constitué de F_Source_Address et de F_Dest_Address

Note 3 à l'article: Instance d'*authentification de connexion* décrite dans l'IEC 61784-3.

3.1.2.4
configuration
définition des connexions et paramètres de communication normalisés des entités de bus d'une application particulière

Note 1 à l'article: La configuration d'une communication de sécurité comprend la définition des connexions de sécurité et des paramètres F des entités de bus relatives à la sécurité d'une application relative à la sécurité particulière.

3.1.2.5
outil CPD
dans les ordinateurs de service connectés au bus de terrain, programme dédié aux besoins de la configuration, du paramétrage et du diagnostic d'appareils de terrain particuliers

3.1.2.6
cycle
intervalle d'exécution répétitive et continue d'une liste d'instructions ou d'une activité

3.1.2.7
point d'accès à l'appareil
DAP
élément qui permet d'adresser un appareil d'entrée-sortie modulaire comme une entité

Note 1 à l'article: En règle générale, il s'agit d'une station de tête.

Note 2 à l'article: L'abréviation "DAP" est dérivée du terme anglais développé correspondant "device access point".

3.1.2.8
temps d'acquittement de l'appareil
DAT
dans un appareil d'entrée-sortie, temps écoulé entre la réception d'un PDU de sécurité avec un nouveau *MonitoringNumber* dans le point d'accès à l'appareil et la génération, puis le renvoi au point d'accès à l'appareil, d'une réponse appropriée de PDU de sécurité

Note 1 à l'article: L'abréviation "DAT" est dérivée du terme anglais développé correspondant "device acknowledgment time".

3.1.2.9
pilote
module logiciel qui permet d'analyser le matériel en fonction de l'application logicielle restante

3.1.2.10
à sécurité intrinsèque (Failsafe)
F
aptitude d'un système qui, par des mesures techniques ou organisationnelles pertinentes, protège contre les dangers de manière déterministe ou en réduisant le risque à un niveau tolérable

Note 1 à l'article: Equivalent à sécurité fonctionnelle.

3.1.2.11
valeurs Failsafe
valeurs à sécurité intrinsèque
FV
valeurs qui remplacent des valeurs de processus lorsque la fonction de sécurité est définie sur un état de sécurité intrinsèque

Note 1 à l'article: Dans le présent document, les valeurs Failsafe (FV) doivent toujours être définies sur "0".

Note 2 à l'article: L'abréviation "FV" est dérivée du terme anglais développé correspondant "fail-safe values".

3.1.2.12
état de sécurité intrinsèque
mode opérationnel d'une fonction de sécurité ou d'un élément final (actionneur) qui, après des mesures techniques pertinentes, protège contre les dangers de manière déterministe ou en réduisant le risque à un niveau tolérable

Note 1 à l'article: Selon la fonction de sécurité particulière, la mise hors tension peut ne pas être la seule possibilité qui caractérise un état de sécurité intrinsèque.

3.1.2.13
pilote de canal de l'hôte F
pilote à l'intérieur des hôtes F conformément aux spécifications FSCP 3/1 qui permet de représenter les données d'entrée-sortie F dans le programme d'application de l'hôte F

3.1.2.14
appareil F
le terme appareil F utilisé dans les versions précédentes de ce profil est remplacé par "pilote de l'appareil F"

3.1.2.15
pilote de l'appareil F
logiciel qui assure la gestion des PDU de sécurité à l'intérieur du (Sous-)Module F conformément aux spécifications FSCP 3/1, déclenché par le pilote de l'hôte F pour l'échange de données

3.1.2.16
pilote F
logiciel qui assure la gestion des PDU de sécurité en tant que pilote de l'hôte F ou pilote de l'appareil F conformément aux spécifications FSCP 3/1

3.1.2.17
hôte F
unité de traitement de données capable d'exécuter le protocole FSCP 3/1 et d'entretenir le canal noir

Note 1 à l'article: En règle générale, il est mis en œuvre dans un PLC ou un IPC équipé d'un système d'exploitation adéquat.

3.1.2.18
pilote de l'hôte F
logiciel qui assure la gestion des PDU de sécurité à l'intérieur des hôtes F conformément aux spécifications FSCP 3/1

3.1.2.19
(Sous-)Module F
homologue de communication à l'intérieur d'un appareil d'entrée-sortie ou d'un esclave d'entrée-sortie modulaire capable d'exécuter le protocole CP 3/1 ou CP 3/4 à CP 3/6.

Note 1 à l'article: Le (Sous-)Module F héberge le pilote de l'appareil F.

Note 2 à l'article: Il s'agit en général d'un module d'entrée ou de sortie relatif à la sécurité.

3.1.2.20
esclave F
homologue de communication CP 3/1 ou CP 3/2 capable d'exécuter le protocole FSCP 3/1, en principe déclenché par l'hôte F pour l'échange de données

3.1.2.21
réaction aux anomalies
indication d'un dysfonctionnement de communication en définissant les bits erronés dans les octets d'état et une réaction sécurisée automatique correspondante à l'intérieur des composants

Note 1 à l'article:

Dans une sortie F: Arrêt des sorties et/ou réaction sécurisée automatique de l'actionneur.

Dans le CPU F: Réaction possible du programme d'application correspondant. Attribuer des valeurs Failsafe aux données d'entrée-sortie F.

Dans une entrée F: Lors de la communication, anomalies détectées à partir de l'entrée F:
Bits erronés définis dans l'octet d'état.
Lors de la communication, anomalies détectées à partir de l'hôte F:
Attribuer des valeurs Failsafe aux données d'entrée F.

3.1.2.22
bloc de fonctions
FB
partie intégrée d'un programme qui permet de traiter une fonctionnalité spécifique

Note 1 à l'article: L'abréviation "FB" est dérivée du terme anglais développé correspondant "function block".

3.1.2.23
temps d'acquittement de l'hôte
HAT
dans un hôte F, temps écoulé entre la réception d'un PDU de sécurité avec un certain *MonitoringNumber* et la génération, puis le renvoi au maître/contrôleur d'entrée-sortie, d'un PDU de sécurité approprié avec un *MonitoringNumber* modifié

Note 1 à l'article: L'abréviation "HAT" est dérivée du terme anglais développé correspondant "host acknowledgment time".

3.1.2.24
contrôleur d'entrée-sortie
entité de communication active qui permet à d'autres entités (qui peuvent être des contrôleurs ou appareils d'entrée-sortie, par exemple) d'initier et de planifier des activités de communication CP 3/4 à CP 3/6

Note 1 à l'article: Dans CP 3/1, cette tâche correspond à une classe maître 1.

Note 2 à l'article: L'interface du contrôleur d'entrée-sortie est appelée "Services FAL du contrôleur d'entrée-sortie" conformément à l'IEC 61158-5-10.

3.1.2.25
appareil d'entrée-sortie
entité de communication qui permet de recevoir des messages et de les envoyer en réponse à une autre entité de communication CP 3/4 à CP 3/6 (qui peut être un contrôleur d'entrée-sortie ou d'autres appareils d'entrée-sortie, par exemple)

Note 1 à l'article: Dans CP 3/1, cette tâche correspond à un esclave.

Note 2 à l'article: L'interface de l'appareil d'entrée-sortie est appelée "Services FAL de l'appareil d'entrée-sortie" conformément à l'IEC 61158-5-10.

3.1.2.26
module d'entrée-sortie
sous-unité adressable d'entrée-sortie à l'intérieur d'un appareil d'entrée-sortie modulaire

3.1.2.27
superviseur d'entrée-sortie
station d'ingénierie qui permet de lire et d'écrire des données sur un appareil d'entrée-sortie

Note 1 à l'article: Il est utilisé pour la mise en service et le diagnostic. A l'inverse d'un contrôleur d'entrée-sortie, il ne remplit pas un rôle actif lors de l'amorçage d'un système d'entrée-sortie. Un superviseur d'entrée-sortie ne fait pas partie intégrante du système d'entrée-sortie.

3.1.2.28
système d'entrée-sortie
contrôleur d'entrée-sortie et ses appareils d'entrée-sortie associés

3.1.2.29
iParamètre
paramètres de (Sous-)Module F individuels ou spécifiques à la technologie

Note 1 à l'article: Les coordonnées de la zone de protection d'un lecteur laser sont des iParamètres classiques.

3.1.2.30
serveur d'iParamètres
mécanisme normalisé qui permet de stocker et d'extraire des paramètres de (Sous-)Module F individuels ou spécifiques à la technologie dans la partie normalisée d'un hôte F ou de son sous-système contrôlé

3.1.2.31
maître (de classe 1)
homologue de communication CP 3/1 actif qui déclenche des esclaves pour l'échange de données

Note 1 à l'article: Le terme "maître" est utilisé seul comme forme abrégée de "maître de classe 1".

3.1.2.32
MonitoringNumber
MNR
moyen qui permet d'assurer l'authenticité et l'ordre correct des PDU de sécurité transmis

Note 1 à l'article: Instance de *nombre de séquences* décrite dans l'IEC 61784-3.

Note 2 à l'article: Le MonitoringNumber est protégé par la signature de CRC transmise.

3.1.2.33
valeurs de processus
PV
données d'entrée et de sortie (d'un PDU de sécurité) nécessaires au contrôle d'un processus automatisé

Note 1 à l'article: L'abréviation "PV" est dérivée du terme anglais développé correspondant "process values".

3.1.2.34
qualificatif
bits de qualification supplémentaires dans les *valeurs de processus* qui indiquent l'état de chaque entrée individuelle

3.1.2.35
nom de code soigneusement sélectionné
un nom de code soigneusement sélectionné constitue tout ou partie d'un nom de code soigneusement stocké dans le (Sous-)Module F

3.1.2.36
entrée-sortie partagée
entrées et sorties dans les appareils de terrain auxquelles plusieurs contrôleurs peuvent accéder

Note 1 à l'article: Même si CP 3/4 à CP 3/6 admet l'entrée-sortie partagée, celle-ci n'est pas admise avec FSCP 3/1.

3.1.2.37
bit de bascule
bit de l'octet de contrôle et d'état qui permet de synchroniser le *MonitoringNumber* (virtuel) dans le pilote de l'hôte F et le pilote de l'appareil F

3.1.2.38
bus de série universel
USB
norme de bus externe

Note 1 à l'article: USB remplace les ports série et parallèle. Il permet d'assurer une connexion directe et rapide entre les ordinateurs de service et les appareils de terrain.

Note 2 à l'article: L'abréviation "USB" est dérivée du terme anglais développé correspondant "universal serial bus".

3.1.2.39
mode V2
services et protocole FSCP 3/1 conformément au présent document

3.2 Symboles et abréviations

3.2.1 Symboles et abréviations communs

BSC	Binary Symmetric Channel (Canal symétrique binaire)	
CP	Communication Profile (Profil de communication)	[IEC 61784-1/2]
CPF	Communication Profile Family (Famille de profils de communication)	[IEC 61784-1/2]
CRC	Contrôle de redondance cyclique	
DLL	Data Link Layer (Couche de liaison de données)	
DLPDU	Data Link Protocol Data Unit (Unité de données de protocole de liaison de données)	
CEM	Compatibilité électromagnétique	
EMI	Electromagnetic Interference (Brouillage électromagnétique)	
EUC	Equipment Under Control (Equipement commandé)	[IEC 61508-4:2010]
E/E/PE	Electrical/Electronic/Programmable Electronic (Electrique/électronique/électronique programmable)	[IEC 61508-4:2010]
FAL	Fieldbus Application Layer (Couche application de bus de terrain)	[IEC 61158-5 (toutes les parties)]
FCS	Frame Check Sequence (Séquence de contrôle de trame)	
FIT	Failure In Time (Défaillance dans le temps) (équivaut à 10^{-9} défaillance par heure)	
FS	Functional Safety (Sécurité fonctionnelle)	
FSCP	Functional Safety Communication Profile (Profil de communication de sécurité fonctionnelle)	
IACS	Industrial Automation and Control System (Automatisation industrielle et système de commande)	
MTBF	Mean Time Between Failures (Durée moyenne de bon fonctionnement)	
MTTF	Mean Time To Failure (Durée moyenne de fonctionnement avant défaillance)	
NSR	Non Safety Related (Non relatif à la sécurité)	
PDU	Protocol Data Unit (Unité de données de protocole)	[ISO/IEC 7498-1]
TBTP	Très basse tension de protection	[IEC 61010-2-201]
PFD	Average probability of dangerous Failure on Demand (Probabilité moyenne de défaillance dangereuse sur sollicitation)	[IEC 61508-4:2010]
PFH	Fréquence moyenne de défaillance dangereuse [h^{-1}] par heure	[IEC 61508-4:2010]
PhL	Physical Layer (Couche physique)	[ISO/IEC 7498-1]
PL	Performance Level (Niveau de performance)	[ISO 13849-1]
PLC	Programmable Logic Controller (Automate programmable)	
RP	Residual Error Probability (Probabilité d'erreurs résiduelles)	
SCL	Safety Communication Layer (Couche de communication de sécurité)	
TBTS	Très basse tension de sécurité	[IEC 61010-2-201]
SIL	Safety Integrity Level (Niveau d'intégrité de sécurité)	[IEC 61508-4:2010]
SIS	Safety Instrumented Systems (Systèmes de sécurité instrumentés)	

SL	Security Level (Niveau de sécurité)	[IEC 62443 (toutes les parties)]
SMS	Security Management System (Système de gestion de sécurité)	[IEC 62443 (toutes les parties)]
SPDU	Safety PDU (PDU de sécurité)	
SR	Safety Related (Relatif à la sécurité)	

3.2.2 CPF 3: Symboles et abréviations supplémentaires

AES-CCMP	Advanced Encryption Standard – Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (Norme de chiffrement avancé – Protocole de code d'authentification de message en mode compteur avec chaînage de blocs chiffrés)
AP	Application Process (Processus d'application)
API	Application Process Identifier (Identifiant de processus d'application)
AR	Application Relationship (Relation d'application)
ASE	Application Service Element (Elément de service d'application)
ASIC	Application Specific Integrated Circuit (Circuit intégré à application spécifique)
C	Couverture
CGP	Channel-granular Passivation (Passivation granulaire des canaux)
DR	Dynamic Reconfiguration (Reconfiguration dynamique)
CP 3/1	Profil de communication communément appelé PROFIBUS DP[3]
CP 3/2	Profil de communication communément appelé PROFIBUS PA
CP 3/4 à CP 3/6	Profil de communication communément appelé PROFINET
CPU	Central Processing Unit (Unité centrale)
CR	Communication Relationship (Relation de communication)
CRC_FP	Valeur de départ CRC2 à 16 bits de l'hôte F (du paramètre F = F_Par_CRC)
CRC_FP+	Valeur CRC à 32 bits du paramètre F
DAP	Device Access Point (Point d'accès à l'appareil)
DAT	Device Acknowledgement Time (Temps d'acquittement de l'appareil)
DP	Decentralized Peripherals (Périphériques décentralisés)
F	Identifiant des éléments sécurisés (à sécurité intrinsèque, sécurité fonctionnelle)
FB	Function Block (Bloc de fonctions)
FV	Fail-safe Values (Valeurs Failsafe)
GSD	General Station Description (Description générale de station) (fichier associé à l'appareil)
GSDL	General Station Description Language (Langage de description générale de station) (pour les appareils CP 3/1 et CP 3/2)
GSDML	General Station Description Markup Language (Langage de balisage de description générale de station) (pour les appareils CP 3/4 à CP 3/6)
HAT	Host Acknowledgement Time (Temps d'acquittement de l'hôte)
HD	Hamming Distance (Distance de Hamming)
E-S	Entrée-sortie
LED	Light Emitting Diode (Diode électroluminescente)
LIV	Last Input-Value (Dernière valeur d'entrée)
LOV	Last Output-Value (Dernière valeur de sortie)
MNR	MonitoringNumber
PA	Process Automation (Automatisme industriel)
Pe	Probabilité d'erreurs sur les éléments binaires

[3] Pour les déclarations d'appellation commerciale, voir Article 4.

PN	PROFINET = CP 3/4 à 3/6	
PiR	Parameterization in Run (Paramétrage en cours)	
PV	Process Values (Valeurs de processus)	
SFRT	Safety Function Response Time (Temps de réponse de la fonction de sécurité)	
RADIUS	Remote Authentication Dial In User Service (Service d'usager commuté à authentification distante)	
S	*Standard*	
TPF	Temporary Parameter File (Fichier de paramètres temporaires) (fichier XML)	
UML	Unified Modeling Language (Langage de modélisation unifié)	[43]
USB	Universal Serial Bus (Bus de série universel)	[48]
WCDT	Worst Case Delay Time (Délai du cas le plus défavorable)	
WDTime	Watchdog Time (Temps de fonctionnement du chien de garde)	
XML	eXtensible Markup Language (Langage de balisage extensible)	[45], [46], [47]

3.3 Conventions

Dans le présent document, l'abréviation "F" se rapporte aux éléments, technologies, systèmes et unités relatifs à la sécurité (à sécurité intrinsèque, sécurité fonctionnelle).

Dans le présent document, les données par défaut qui doivent être utilisées en cas de défaillance du système ou d'erreurs sont appelées valeurs Failsafe (FV) et leur valeur est nulle (0).

Dans le présent document, le bit réservé ("res") dans l'octet d'état/de contrôle et les paramètres F doivent être définis sur "0" et ignorés par le récepteur de manière à éviter toute contrariété avec les versions futures des appareils FSCP 3/1.

Dans le présent document, le calcul de la signature CRC qui a pour résultat une valeur 0 utilise la valeur 1 à la place. La seule exception est donnée en 8.1.8.

Dans le présent document, l'abréviation "CP 3/4 à CP 3/6" comprend les trois profils de communication CP 3/4, CP 3/5 et CP 3/6. CP 3/4 à CP 3/6 est communément appelé PROFINET.

Le présent document utilise la notation UML2 pour le tracé des diagrammes d'états et une forme condensée de diagrammes séquentiels [43]. Les tableaux de transition sont présentés conformément aux recommandations de l'IEC 62390.

4 Présentation générale de FSCP 3/1 (PROFIsafe™)

La Famille de profils de communication 3 (souvent appelée PROFIBUS™, PROFINET™[4]) définit les profils de communication qui reposent sur l'IEC 61158-2 Type 3, l'IEC 61158-5-3, l'IEC 61158-5-10, l'IEC 61158-6-3, et l'IEC 61158-6-10.

[4] PROFIBUS™, PROFINET™ et PROFIsafe™ sont des appellations commerciales de l'organisme à but non lucratif PROFIBUS Nutzerorganisation e.V. (PNO). Cette information est donnée à l'intention des utilisateurs du présent document et ne signifie nullement que l'IEC approuve ou recommande le détenteur de la marque ou de l'un de ses produits. La conformité au présent document n'exige pas l'emploi des logos déposés pour PROFIBUS™, PROFINET™ ou PROFIsafe™. L'emploi des logos déposés pour PROFIBUS™, PROFINET™ ou PROFIsafe™ exige l'autorisation de PNO et la conformité aux conditions d'utilisation (essais et validation).

Les profils de base CP 3/1 et CP 3/2 sont définis dans l'IEC 61784-1; CP 3/4, CP 3/5 et CP 3/6 sont définis dans l'IEC 61784-2. Le profil de communication de sécurité fonctionnelle CPF 3 FSCP 3/1 (PROFIsafe™[4]) repose sur les profils de base CPF 3 définis dans l'IEC 61784-1 et l'IEC 61784-2, ainsi que sur les spécifications de la couche de communication de sécurité définies dans le présent document.

Le FSCP 3/1 repose sur l'échange de données cycliques d'un contrôleur (de bus) avec ses appareils (de terrain) associés au moyen d'une relation de communication un-un (Figure 3). Un contrôleur peut utiliser toute combinaison d'appareils normalisés et de sécurité reliés au réseau. Il est également possible d'affecter des tâches de sécurité et normales à différents contrôleurs. Les communications dites acycliques entre les appareils et les contrôleurs ou les superviseurs tels que les appareils de programmation sont prévues à des fins de configuration, paramétrage, diagnostic et maintenance.

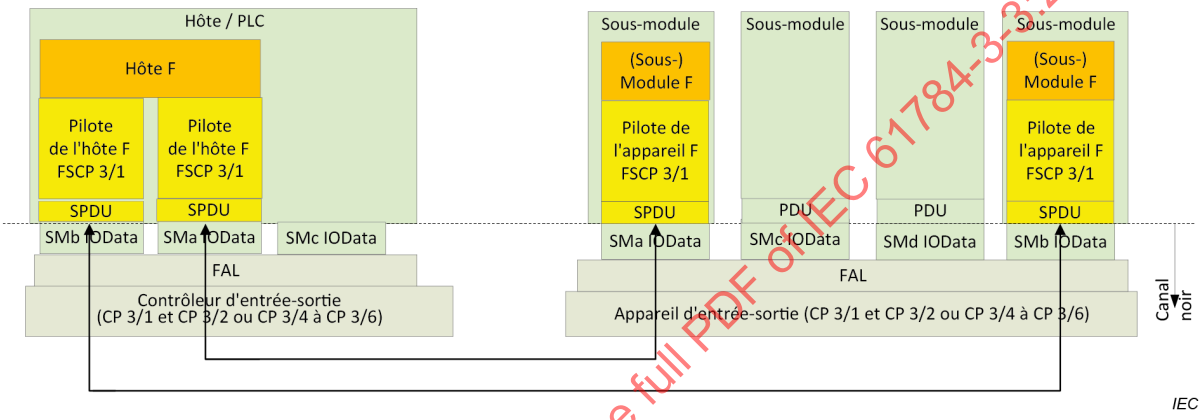


Figure 3 – Conditions préalables de communication de base pour le protocole FSCP 3/1

Les quatre mesures suivantes ont été retenues pour réaliser le protocole FSCP 3/1:

- MonitoringNumber (MNR) (virtuel);
- contrôle du temps de fonctionnement du chien de garde avec acquittement;
- nom de code par relation de communication (le nom de code constitue la base du MNR. La direction est différenciée par l'élément complémentaire unique du MNR);
- contrôle de redondance cyclique pour l'intégrité des données.

Le MonitoringNumber utilise une plage suffisamment grande pour sécuriser tout dysfonctionnement provoqué par les éléments de réseau de stockage des messages. Chaque appareil de sécurité renvoie un message qui contient un PDU de sécurité pour acquittement, y compris en l'absence de données de processus. Un temporisateur séparé placé à la fois du côté émetteur et récepteur est utilisé pour chaque relation de communication un-un. Le nom de code par relation de communication (et par des mesures supplémentaires de la direction source-collecteur) est établi pour des raisons d'authentification. Son codage est constitué la signature CRC2 calculée et transmise (voir Figure 4).

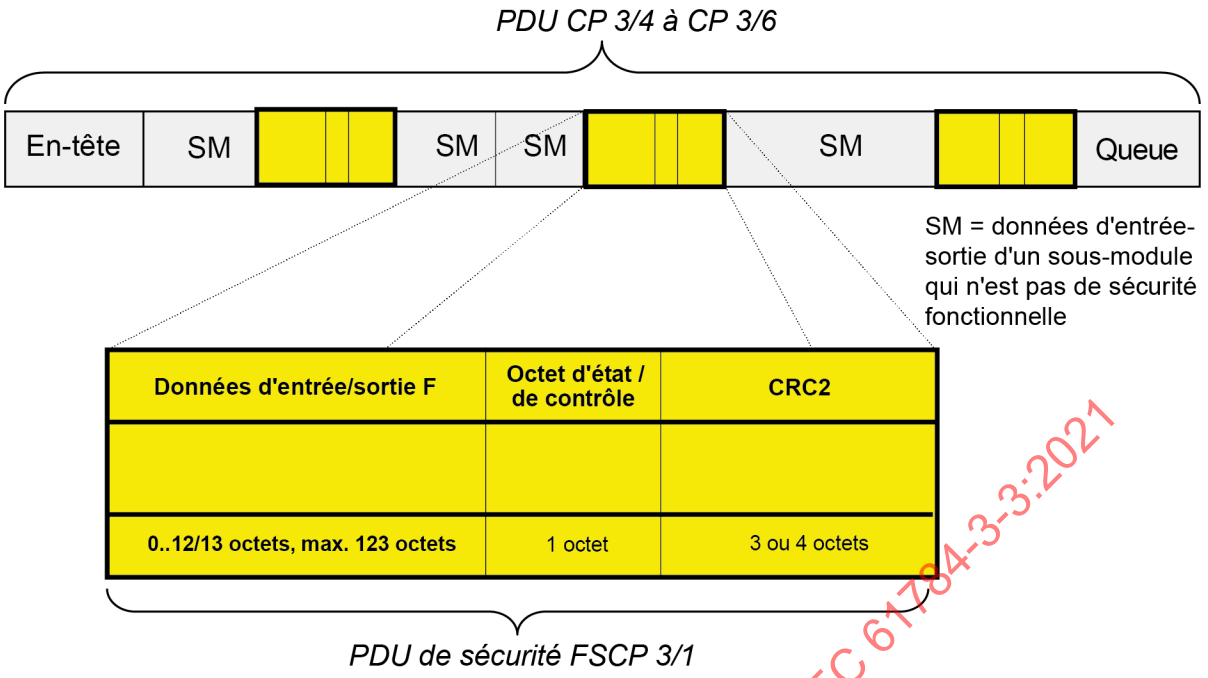


Figure 4 – Structure d'un PDU de sécurité FSCP 3/1

Le protocole FSCP 3/1 fournit le mode appelé V2. Le mode V2 couvre la CPF3, notamment l'acheminement programmable des messages et des constatations scientifiques concernant les propriétés CRC.

La Figure 5 représente FSCP 3/1 dans le cadre d'architectures CPF 3.

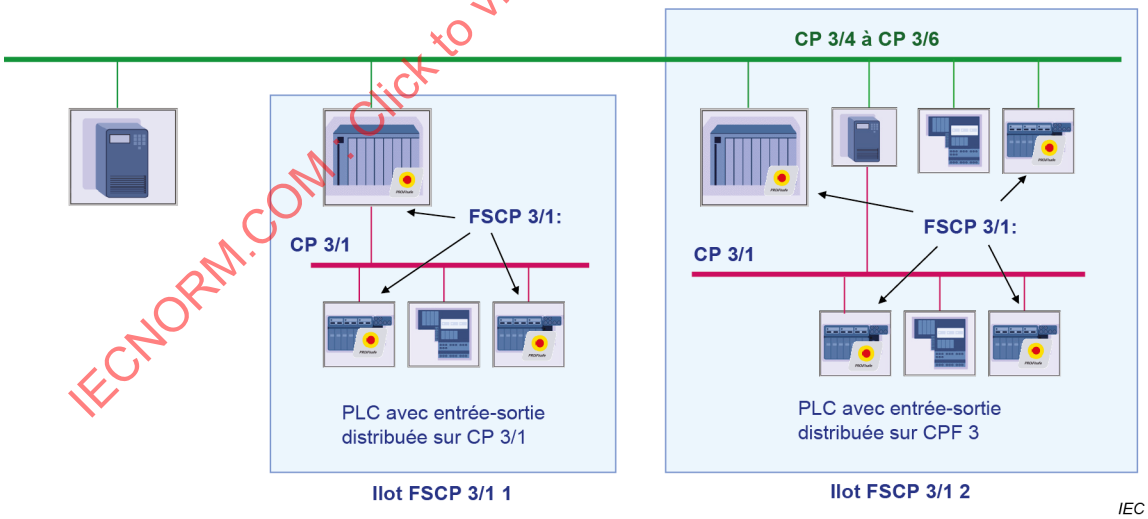


Figure 5 – Communication de sécurité avec CPF 3

Tandis que les solutions d'automatisation à entrée-sortie distribuée ont largement fait l'unanimité à l'aide de PROFIBUS (CP 3/1 et CP 3/2) et PROFINET fondé sur Ethernet pour les réseaux industriels (CP 3/4 à CP 3/6), les applications de sécurité reposent toujours sur une deuxième couche de techniques électriques conventionnelles ou de bus spéciaux, ce qui limite l'ingénierie et l'interopérabilité continues. De plus, il n'a pas été possible d'encourager comme nécessaire l'utilisation d'appareils de sécurité modernes (les lecteurs laser ou les appareils à sécurité intrinsèque, par exemple) compte tenu du manque de prise en charge du système. Le présent document et les documents connexes ont pour objet de fournir les technologies génériques correspondantes.

Après cette introduction, le 5.1 et le 5.2 reprennent respectivement des références supplémentaires pour le développement de la technologie FSCP 3/1 et ses exigences fonctionnelles. Les quatre mesures de sécurité de FSCP 3/1 figurent en 5.3. Les topologies de réseau de CP 3/4 à CP 3/6 et leurs mappings avec CP 3/1 et CP 3/2 sont mentionnés en 5.4. Une brève introduction des relations de communication et des objets de la norme relative au bus de terrain est ensuite présentée en 5.5.

Pour des raisons de sécurité et d'efficacité, la liste des types de données de bus de terrain possibles est limitée à un ensemble concis présenté en 5.5.3. Les paragraphes 6.1 à 6.3 dévoilent les services du pilote de l'hôte F et du pilote de l'appareil F, ainsi que les messages de diagnostic possibles de la couche de sécurité.

L'Article 7 commence par une présentation du PDU de sécurité (7.1) et se poursuit par une description des diagrammes d'états du pilote de l'hôte F et du pilote de l'appareil F et des diagrammes séquentiels au format UML 2 (7.2.2 à 7.2.5). Les contraintes de temporisation associées sont présentées en 7.2.6 et 7.2.7. Conformément au format de l'Annexe G de l'IEC 61784-3:2021, le 7.3 présente les réactions du système en cas d'éventuels dysfonctionnements. D'autres fonctions du système (le démarrage de la couche de sécurité, par exemple) sont présentées en 7.4. La gestion de la couche des appareils de sécurité se concentre sur les paramètres F spécifiques à la communication de sécurité (8.1) et sur les iParamètres individuels spécifiques à l'appareil (8.2). Les exigences de traitement et de fourniture des paramètres F sont présentées en 8.3. Le 8.4 traite de la sécurisation des structures de données échangées entre les partenaires qui communiquent et entrant dans la configuration d'un appareil. Le 8.5 explique comment les informations de structure de données peuvent être utilisées pour configurer les pilotes de canal de l'hôte F de (Sous-)Modules F plus complexes afin de limiter les efforts de programmation. Les exigences d'intégration système des moyens et outils d'iParamétrage figurent en 8.6. Les aspects liés aux temps de réponse, aux lignes directrices d'installation, à la durée des sollicitations, à la maintenance, au manuel de sécurité, à la transmission sans fil et aux classes de conformité de l'hôte F sont présentés à l'Article 9. Le raisonnement d'évaluation est présenté en 10.1 et les détails en 10.2. Une Annexe A informative contient des exemples de calculs de signature CRC rapides et une bibliographie. Deux lignes directrices FSCP 3/1 supplémentaires relatives à la sécurité électrique et à l'évaluation doivent être respectées ([36], [61]).

L'Annexe C décrit de nouvelles fonctions facultatives. L'Article C.1 contient les exigences relatives à la "Réaction à Device_Fault dans l'hôte F", soit sous forme de documentation, soit mises en œuvre dans le diagramme d'états. L'Article C.2 spécifie la fonction facultative de l'hôte F pour "Désactiver le (Sous-)Module F". L'Article C.3 explique l'utilisation de PROFIenergy avec FSCP 3/1. L'Article C.5 spécifie les exigences applicables à plusieurs hôtes F qui communiquent avec un (Sous-)Module F unique. La modification "Paramétrage de PROFIsafe en cours" spécifie la fonction facultative "Paramétrage FSCP 3/1 en cours" (voir [64]).

5 Généralités

5.1 Documents externes de spécifications applicables au profil

Outre les références normatives de l'Article 2, la technologie présentée dans le présent document satisfait aux exigences du document NE97 [44].

5.2 Exigences fonctionnelles de sécurité

Les exigences suivantes s'appliquent au développement de la technologie FSCP 3/1.

a) La communication de sécurité et la communication normale doivent être indépendantes. Toutefois, les appareils normalisés et les appareils de sécurité doivent être en mesure d'utiliser le même canal de communication.

b) La communication de sécurité doit être conforme au niveau d'intégrité de sécurité SIL3 (voir l'IEC 61508) et au niveau PL e (voir l'ISO 13849-1).

c) La communication de sécurité doit utiliser un système de communication à un seul canal. La redondance du support et/ou la redondance du système peut éventuellement être utilisée pour augmenter la disponibilité.

d) La mise en œuvre du protocole de transmission de sécurité doit être limitée aux éléments finaux de communication (pilote de l'hôte F ou pilote de l'appareil F).

e) La relation de communication entre un pilote de l'appareil F et le pilote de son hôte F doit toujours être de type 1:1.

f) Les durées de transmission doivent être surveillées.

g) Les conditions environnementales doivent être conformes aux exigences générales d'automatisation (principalement l'IEC 61326-3-1 ou l'IEC 61326-3-2 en l'absence de normes de produits particulières).

h) Les équipements de transmission (les contrôleurs, les ASIC, les liaisons, les coupleurs, etc.) ne doivent pas être modifiés (canal noir). Les fonctions de sécurité doivent être au-dessus de la couche OSI 7 (c'est-à-dire le profil, et pas de modifications ni d'améliorations apportées au protocole normalisé)

i) La communication de sécurité ne doit pas réduire le nombre d'appareils admis. Des restrictions peuvent apparaître pendant le mapping, dans le cas des applications CP 3/2, en raison des limitations de messages (voir CP 3/2 dans l'IEC 61784-1).

j) La communication de sécurité doit être conforme à NE97 [44] et satisfaire aux exigences de l'IEC 61784-3:2021.

5.3 Mesures de sécurité

Les mesures de sécurité mentionnées dans le Tableau 1 pour la maîtrise des erreurs de transmission possibles constituent un composant significatif du profil FSCP 3/1. La sélection dans le Tableau 1 des mesures de sécurité génériques qui figurent en 5.5 de l'IEC 61784-3:2021 est exigée pour FSCP 3/1.

Les mesures de sécurité doivent être traitées et surveillées dans une unité de sécurité.

Tableau 1 – Mesures déployées pour maîtriser les erreurs

Erreur de communication	Mesures de sécurité			
	MonitoringNumber (virtuel) [a]	Temporisation avec réception [b]	Nom de code de l'émetteur et du récepteur [c]	Contrôle d'intégrité des données [d]
Corruption	–	–	–	X
Répétition non prévue	–	X	–	–
Séquence incorrecte	X	–	–	–
Perte	X	X	–	–
Retard inacceptable	–	X	–	–
Insertion	X	–	–	–
Déguisement	–	–	–	X
Adressage	X	–	X	–
Hors séquence	X	–	–	–
Bouclage des messages	X [e]	–	–	–

[a] Instance de "numéro de séquence" de l'IEC 61784-3.

[b] Instance de "délai" (Temporisation) et de "message de réaction" (Réception) de l'IEC 61784-3.

[c] Instance d'"authentification de connexion" de l'IEC 61784-3.

[d] Instance d'"assurance d'intégrité des données" de l'IEC 61784-3.

[e] En mode F_CRC_seed =0 par le bit d'état 7, en mode F_CRC_seed =1 par l'élément complémentaire unique du MNR

En cas d'erreurs de communication conformément au Tableau 1, des réactions aux anomalies définies, spécifiées dans le Tableau 11, le Tableau 13 et en 7.2.7.1, doivent se produire.

5.4 Structure de la couche de communication de sécurité

5.4.1 Principe des communications de sécurité FSCP 3/1

La communication de sécurité FSCP 3/1 repose sur l'expérience en matière de technique de signalisation ferroviaire, présentée dans les versions antérieures de l'IEC 62280.

Sur cette base, la communication de sécurité est assurée par

- un système de transmission normalisé (Figure 6), et
- un protocole de transmission de sécurité supplémentaire qui vient à l'appui de ce système de transmission normalisé.

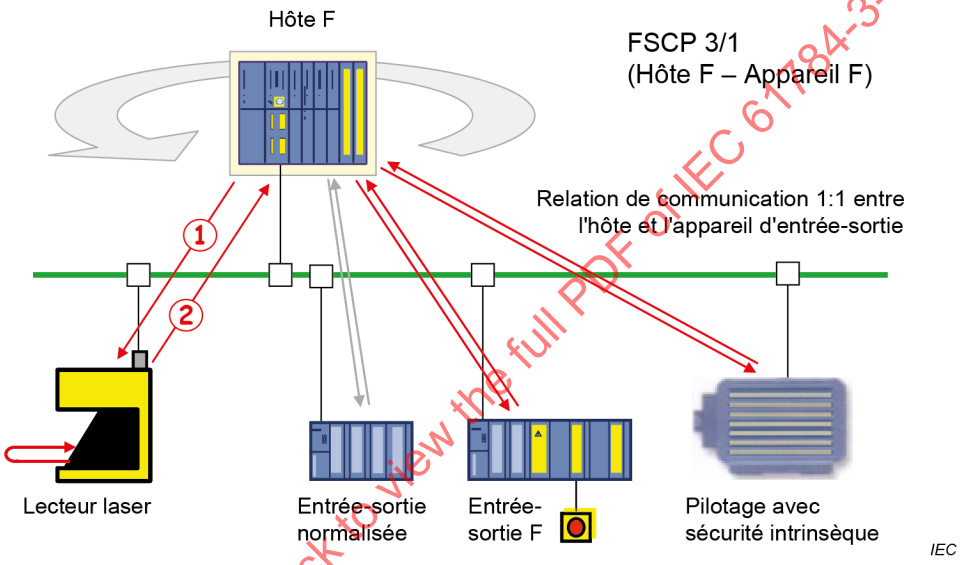


Figure 6 – Système de transmission CPF 3 normalisé

Le système de transmission normalisé est composé de l'ensemble du matériel de transmission et des fonctions de protocoles associées (c'est-à-dire les couches OSI 1, 2 et 7 selon la Figure 7).

Les applications de sécurité et les applications normalisées partagent simultanément les mêmes systèmes de communication CPF 3 normalisés. La fonction de transmission sécurisée comprend toutes les mesures de détection déterministe de toutes les anomalies/tous les dangers potentiels que le système de transmission normalisé est susceptible d'infiltrer, ou de maintien du taux d'erreurs résiduelles sous une certaine limite. Il s'agit

- de dysfonctionnements aléatoires (en raison, par exemple, de l'impact du brouillage électromagnétique sur le canal de transmission);
- des défaillances/d'anomalies du matériel normalisé;
- de dysfonctionnements systématiques des composants dans le matériel et le logiciel normalisés.

Ce principe permet de limiter l'effort d'évaluation aux "fonctions de transmission sécurisée". Il n'est pas nécessaire de procéder à une évaluation de sécurité supplémentaire du "système de transmission normalisé" (canal noir).

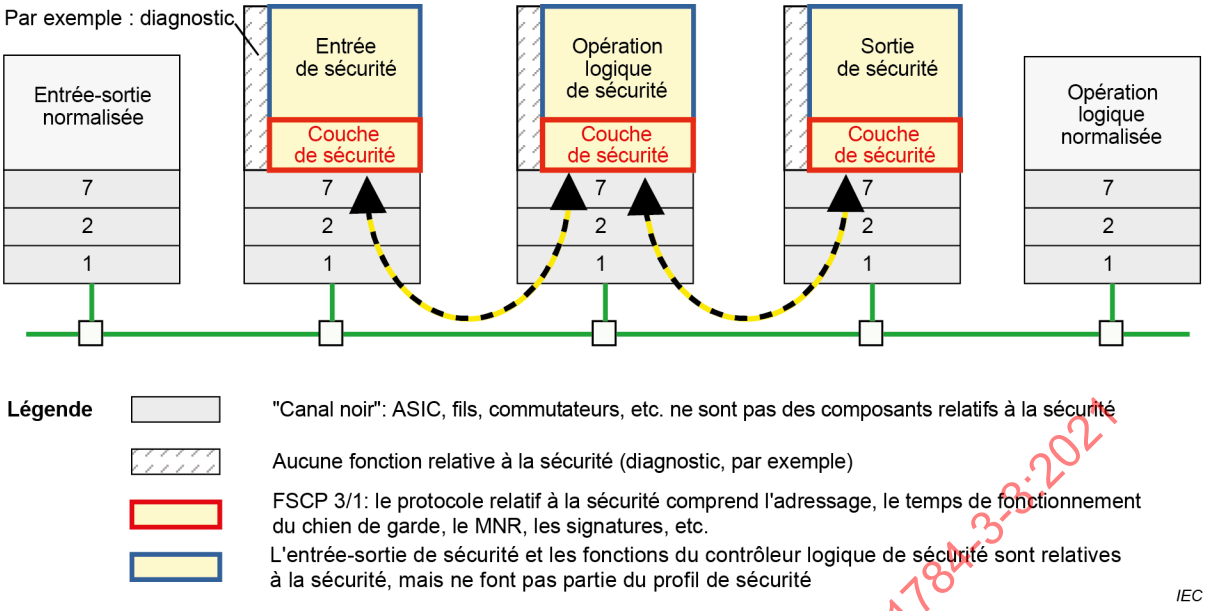


Figure 7 – Architecture de la couche de sécurité

La transmission s'effectue par le biais de conducteurs électriques, optiques ou sans fil. Les topologies et fonctions de transmission admissibles du système de transmission normalisé et les composants du "canal noir" sont présentés en 5.4.2.

5.4.2 Structures de communication CPF 3

Les couches de communication de base de CP 3/4 à CP 3/6 sont représentées à la Figure 8. Alors que la communication de sécurité à transmission cyclique en mémoire tampon de FSCP 3/1 utilise le canal en temps réel, les autres services utilisent la communication acyclique à file d'attente.

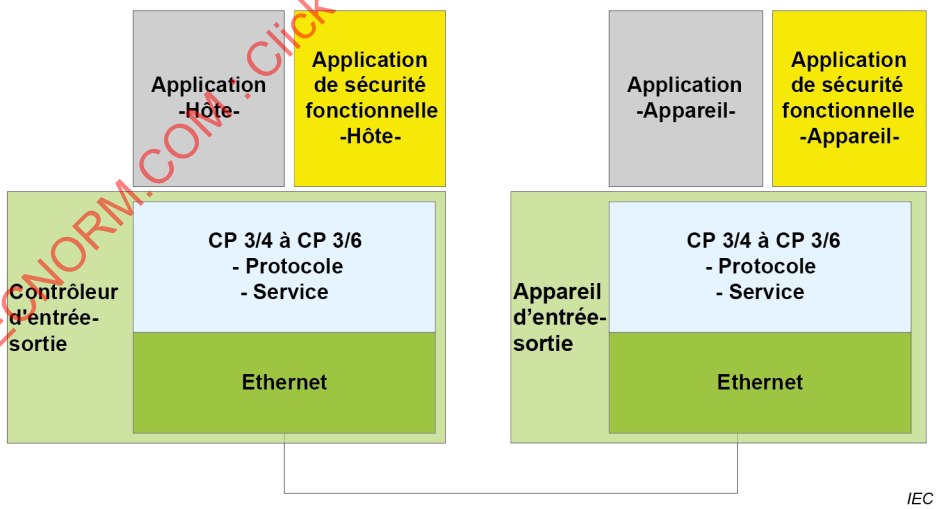


Figure 8 – Couches de communication de base

Réseaux qui appartiennent à un CP 3/4 à CP 3/6

Dans les systèmes qui portent une adresse IP particulière, car le protocole en temps réel (RT ou IRT) de la couche 2 ne peut pas aller au-delà de cet espace d'adresse IP. Il revient aux routeurs (couche OSI 3) de réacheminer les messages vers un niveau d'adresse IP (voir Figure 9). Par conséquent, les routeurs sont les limites naturelles des systèmes CP 3/4 à CP 3/6 où RT_CLASS_UDP n'est ni admis ni pris en charge.

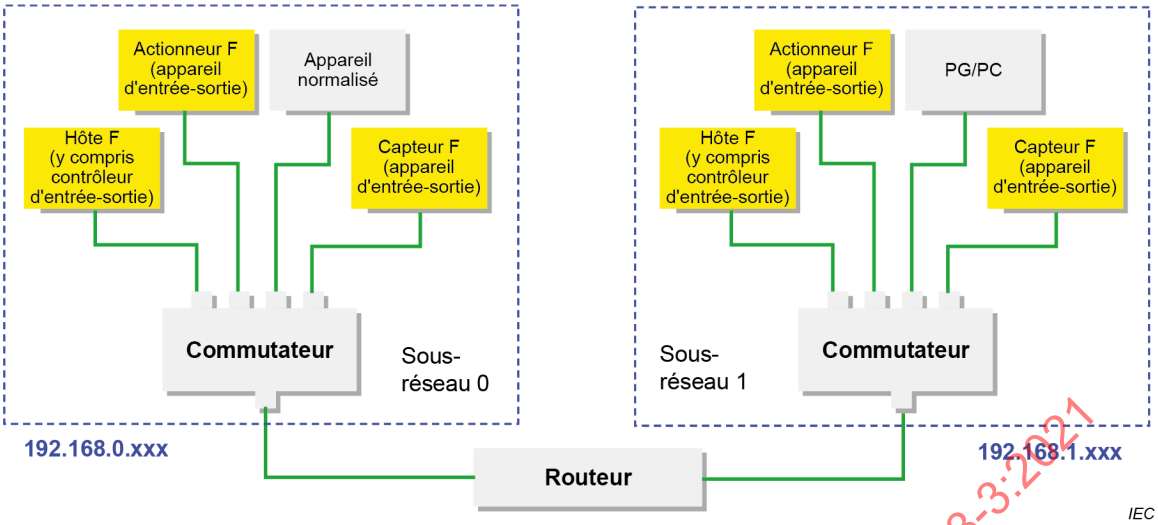


Figure 9 – Croisement des limites du réseau avec les routeurs

Les restrictions suivantes s'appliquent à FSCP 3/1.

- Réseau local sans fil admis. Toutefois, le caractère unique des noms de code soigneusement sélectionnés doit être assuré à l'intérieur d'un sous-réseau.
- Les routeurs à un seul port ne sont pas admis (7.3.11).

Lorsque la communication à transmission cyclique en mémoire tampon croise les routeurs, les noms de codes internes à l'ensemble du réseau doivent être exempts de toute ambiguïté et les vérifications de nom de code doivent identifier les relations non ambiguës et par des mesures supplémentaires les deux directions de transmission.

A l'inverse de la configuration d'un système de bus de terrain, la Figure 10 représente la structure de réseau possible, c'est-à-dire la mesure dans laquelle le profil de sécurité s'étend dans les unités individuelles. Par exemple, une entrée-sortie distante normalisée peut contenir un module F qui permet de connecter un bouton d'arrêt d'urgence. Par conséquent, l'ensemble du canal de transmission FSCP 3/1 passe dans l'appareil d'entrée-sortie par le bus de fond de panier du pilote de l'hôte F par CP 3/4 à CP 3/6, puis dans le Sous-module F final par l'intermédiaire d'un autre fond de panier possible. La couche de sécurité est mise en œuvre à l'intérieur de ces extrémités de communication.

Un fonctionnement à plusieurs contrôleurs ou plusieurs maîtres des hôtes F est admis. Les "entrées F partagées" ne sont pas admises. Un mélange de l'hôte F et de l'hôte normalisé est possible.

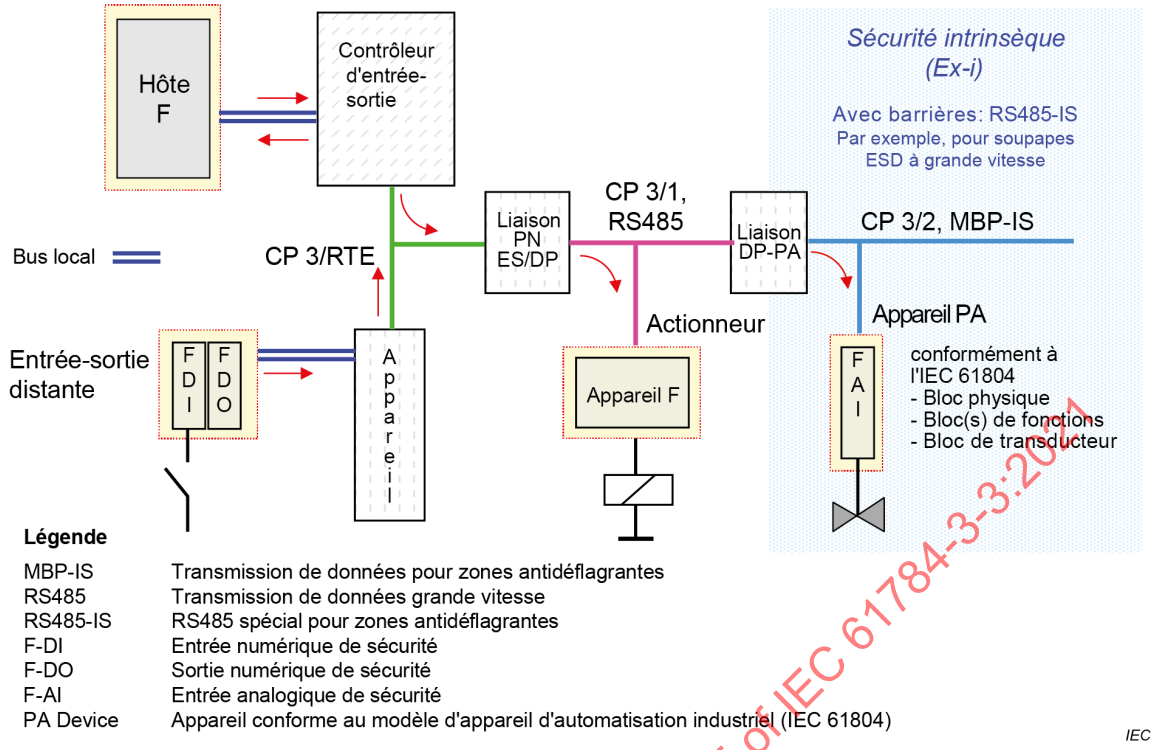


Figure 10 – Voies de transmission de sécurité complètes

5.5 Relations avec la FAL (et DLL, PhL)

5.5.1 Modèle d'appareil

Le CP 3/4 à CP 3/6, ainsi que le modèle d'appareil CP 3/1, prend pour hypothèse la présence d'un ou de plusieurs processus d'application (AP) dans l'appareil. La Figure 11 représente la structure interne d'un processus d'application pour un appareil de terrain modulaire. Eventuellement, elle peut comporter plusieurs de ces processus d'application. Le processus d'application est divisé en autant de Modules que nécessaire afin de représenter les entrées-sorties physiques de l'appareil. A l'inverse de CP 3/1, CP 3/4 à CP 3/6 offre deux niveaux hiérarchiques supplémentaires: les Sous-modules avec canaux.

Dans les Sous-modules, les éléments de service d'application (ASE) offrent un ensemble de services normalisés qui permet d'acheminer les demandes et les réponses entre les processus d'application ainsi que leurs objets de données (données d'entrée-sortie, Contexte (Paramétrage), Diagnostic, Alarmes et Données d'enregistrement, par exemple).

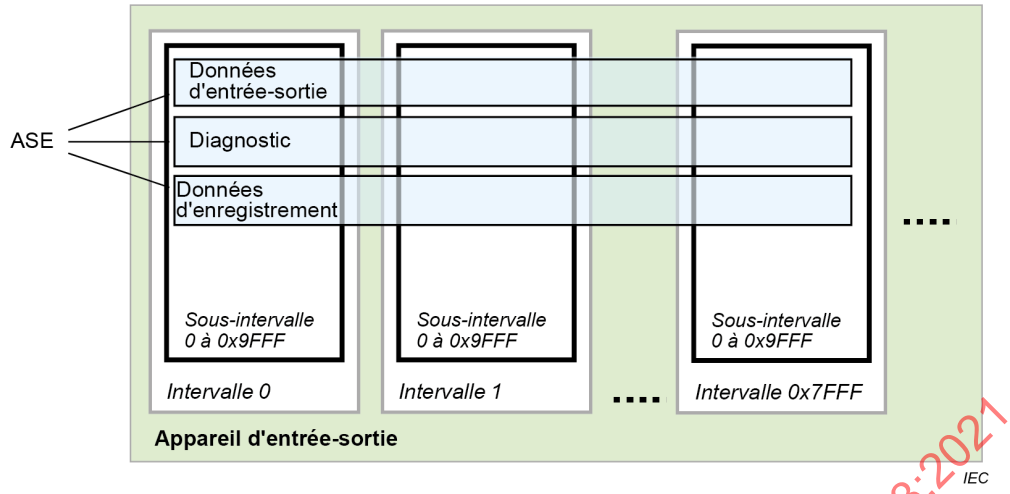


Figure 11 – Modèle d'appareil entrée-sortie

Le fabricant de l'appareil est chargé de la spécification (GSD) des (Sous-)Modules F qui peuvent être insérés dans des intervalles et des sous-intervalles.

5.5.2 Relations d'application et de communication

CP 3/4 à CP 3/6 admet en général une entrée partagée. Etant donné que FSCP 3/1 repose sur des relations de communication 1:1, l'entrée partagée ne peut pas être utilisée pour la sécurité fonctionnelle.

5.5.3 Types de données

CPF 3 utilise les types de données de base qui figurent dans l'IEC 61158-5-10. Le Tableau 2 présente un nombre limité de types de données pour FSCP 3/1. Le Tableau 3 présente les queues F_Message spécifiées.

Tableau 2 – Types de données pour FSCP 3/1

Nom du type de données	Nombre d'octets
Unsigned8 (utilisé comme bits)	1
Unsigned16 (utilisé comme bits) [a]	2
Unsigned32 (utilisé comme bits) [a]	4
Integer16	2
Integer32	4
Float32	4
Unsigned8 (utilisé comme bits) + Unsigned8 (utilisé comme bits)	2
Float32+Unsigned8 (utilisé comme bits)	5
[a] Il est fortement recommandé d'utiliser plusieurs Unsigned8 à la place.	

Tableau 3 – F_MessageTrailer pour FSCP 3/1

F_MessageTrailer	Nombre d'octets
F_MessageTrailer4Byte (F_CRC_Seed = 0)	4
F_MessageTrailer5Byte (F_CRC_Seed = 1)	5

NOTE Justification de Unsigned8: Etant donné que CPF 3 utilise la séquence d'octets en mode gros-boutiste, les numéros des canaux ne dépendent pas du numéro de bit de Unsigned16/32. En cas d'utilisation de BitDataItems, les BitOffsets ne sont pas synchrones aux numéros des canaux. Une représentation différente des Modules F avec plusieurs octets booléens dans différents hôtes F peut être évitée par l'utilisation de plusieurs Unsigned8 (utilisés comme bits).

Les bits uniques doivent être codés dans un type de données Unsigned8, en raison de sa plus grande efficacité par rapport au type de données booléen.

Voir l'IEC 61158-5-10 pour obtenir des informations générales relatives aux types de données et 8.4.2 pour le codage de sécurité fonctionnelle.

6 Services de la couche de communication de sécurité

6.1 Services du pilote de l'hôte F

La Figure 12 indique que chaque entrée F et chaque sortie F impliquent une gestion de PDU de sécurité (pilote F) afin de traiter le protocole FSCP 3/1. L'hôte F correspondant fonctionne avec une instance d'un pilote F pour chaque entrée ou sortie F, respectivement. Par conséquent, toutes les relations de type 1:1 entre une instance du pilote de l'hôte F et le pilote de l'appareil F partenaire correspondant sont identifiées par un Codename (l'un des paramètres F).

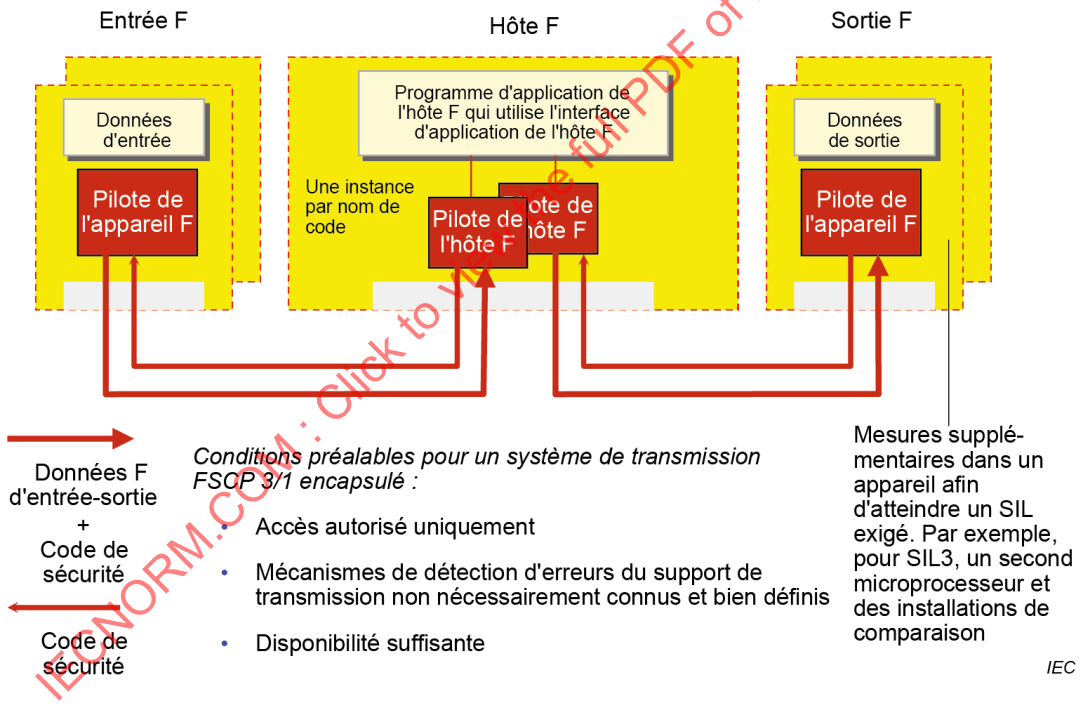


Figure 12 – Structure de communication FSCP 3/1

L'ensemble de l'équipement de communication CPF 3 normalisé entre les pilotes F appartient au canal noir. Les flèches dans la Figure 12 indiquent la communication à transmission cyclique en mémoire tampon entre les pilotes F: les suppléments de sécurité (Octet d'état ou de contrôle et CRC2) sont transférés, en plus des données de l'entrée F, de l'entrée F vers le pilote de l'hôte F.

A titre d'acquittement, l'entrée F reçoit simplement le supplément de sécurité (code de sécurité). En conséquence, la sortie F reçoit le supplément de sécurité accompagné des données de la sortie F, et l'utilise pour l'acquittement.

NOTE Il est possible que les (Sous-)Modules F fournissent des données de l'entrée et de la sortie F.

La gestion de PDU de sécurité et le paramétrage F sont des tâches des pilotes F à l'intérieur de l'hôte F et des (Sous-)Modules F. Ces tâches fournissent également les mesures qui viennent à l'appui des fonctions système supplémentaires "Paramétrage en cours" (PiR) selon [54] et "Passivation granulaire des canaux" fondée sur [56].

L'interface d'application F au niveau du programme d'application de l'hôte F est représentée à la Figure 13.

"Reconfiguration dynamique" (DR) ou "Maintenance des systèmes de tolérance aux anomalies" selon [54] sont des activités planifiées qui doivent être contrôlées par du personnel autorisé uniquement. DR doit être activée uniquement par un opérateur. Elle ne doit pas être définie/réinitialisée par le "Programme d'application F".

La conception des parties relatives à la sécurité correspondantes de l'hôte F doit exclure toute activation involontaire de la caractéristique "use_TO2" (voir 7.2.7.2).

L'hôte F peut définir et réinitialiser "use_TO2" pour tous les (Sous-)Modules F, affectant ainsi simultanément tous les (Sous-)Modules F.

L'hôte F doit prolonger une seule fois le temps de fonctionnement du chien de garde (principal) régulier (F_WD_Time) par un temps de fonctionnement de chien de garde secondaire (F_WD_Time_2) (voir Figure 18, Figure 26, Figure 27, 7.2.7.2, 8.1.1 et 8.1.4).

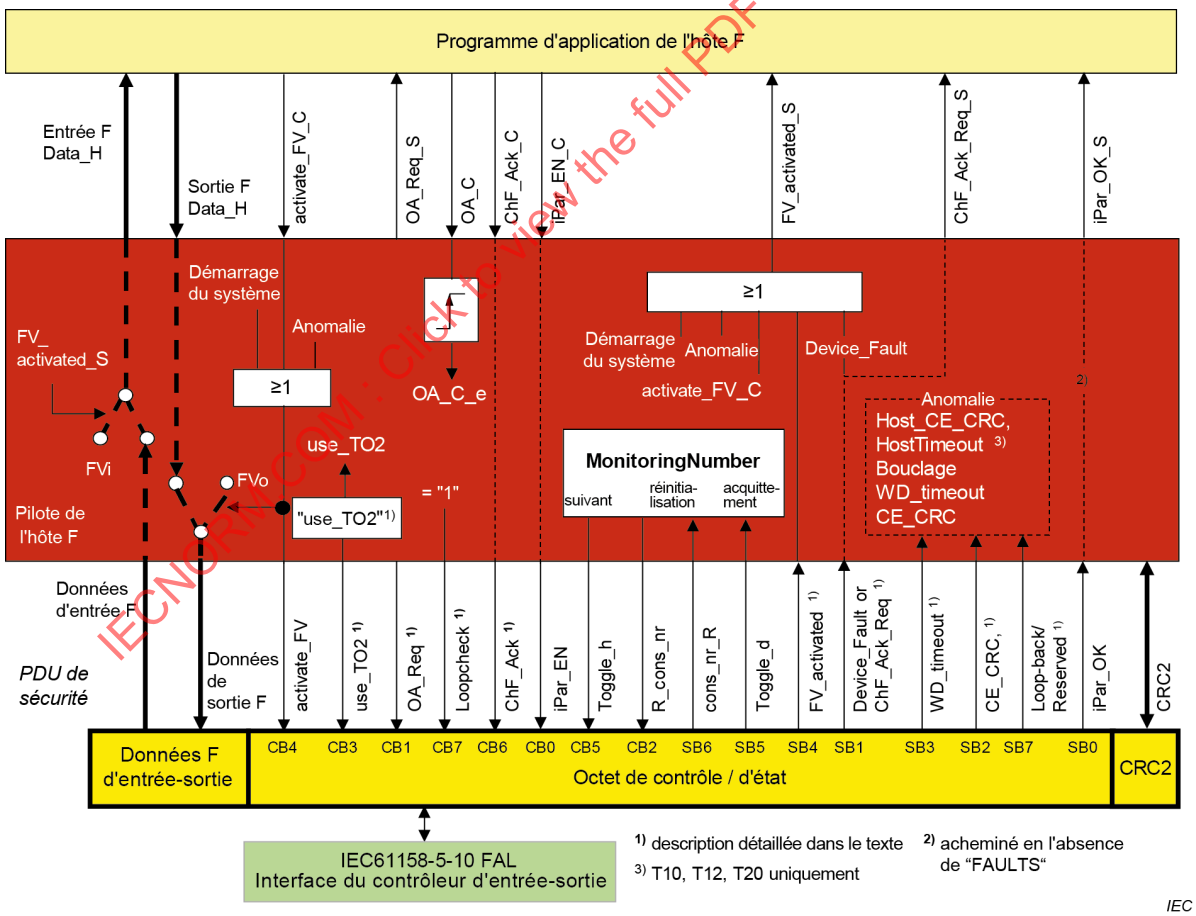


Figure 13 – Interface d'application F des instances du pilote de l'hôte F

La nécessité d'une "Passivation granulaire des canaux" peut être constatée en 5.4.2 et à la Figure 10. Le canal de transmission FSCP 3/1 atteint par exemple un (Sous-)Module F d'un appareil d'entrée-sortie distant. Habituellement, le module F fournit plusieurs canaux de signalisation, avec un canal pour chaque capteur de sécurité, comme représenté à la Figure 14. Chaque canal de signalisation peut être associé à une fonction de sécurité individuelle. En cas de défaillance d'un canal, le module F entraîne l'état de sécurité intrinsèque de toutes les fonctions de sécurité associées. L'option "Passivation granulaire des canaux" fondée sur [56] permet un état de sécurité intrinsèque individuel uniquement pour la fonction de sécurité soumise à l'influence du canal de signalisation défaillant.

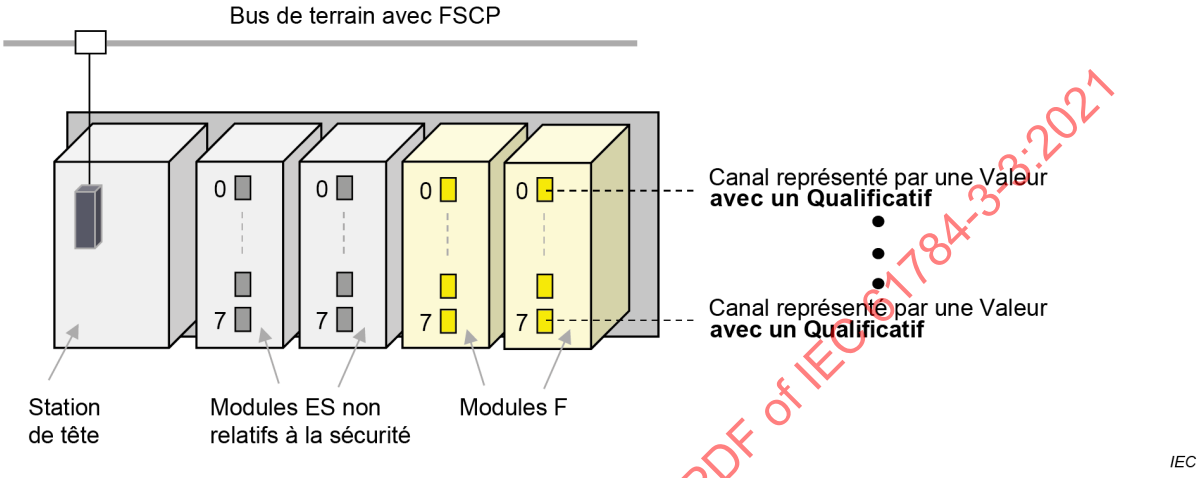


Figure 14 – Motivation pour l'option "Passivation relative aux canaux"

Le programmeur dispose de plusieurs variables pour manipuler ces processus de sécurité conformément aux normes. Ces variables portent des noms similaires (en principe suivis d'une extension "_C" (Control) ou "_S" (Status)), comme le bit correspondant dans les octets d'état et de contrôle, mais peuvent faire l'objet d'une certaine logique de commande à l'intérieur du pilote F. Voir également 8.5.2 et Figure 52.

Les indications de mise en œuvre pour le pilote de l'hôte F sont collectées en 8.5.3.

Le programmeur d'un programme d'application de l'hôte F doit disposer des variables suivantes conformément au 9.10:

activate_FV_C Chaque programme d'application de l'hôte F qui gère un pilote de l'hôte F correspondant doit définir/réinitialiser cette variable (type: bit). Si la valeur "1" est attribuée à cette variable des appareils d'entrée (des capteurs, par exemple), le pilote de l'hôte F fournit des valeurs Failsafe ("0") au programme d'application F. Si la valeur "1" est attribuée à cette variable des appareils de sortie (des actionneurs, par exemple), le pilote de l'hôte F envoie des valeurs Failsafe ("0") au pilote de l'appareil F et attribue la valeur "1" au bit "activate_FV" de l'octet de contrôle. Le concept de sécurité de l'appareil de sortie définit le type d'informations de "activate_FV" qui doivent être utilisées pour atteindre l'état de sécurité à la sortie des (Sous-)Modules F.

FV_activated_S — Chaque programme d'application de l'hôte F qui gère un pilote de l'appareil F correspondant doit évaluer cette variable (type: bit). Si la valeur "1" est attribuée à cette variable dans les appareils d'entrée, le pilote F fournit des valeurs Failsafe ("0") au programme d'application de l'hôte F pour tous les canaux du module F. Voir [56].

Si la valeur "1" est attribuée à cette variable dans les appareils de sortie, des valeurs Failsafe "0" (comportement par défaut) ou une valeur spécifique à l'appareil de sortie F contrôlé par le signal "activate_FV" (= bit 4 de l'octet de contrôle) sont attribuées à tous les canaux du module F. Voir [56].

Cette variable (type: bit) représente le résultat d'un "OR" logique des signaux: Faults, activate_FV_C, FV_activated (SB4), Device_Fault, et System start (implicite). ChF_Ack_Req n'influence pas *FV_activated_S.*

iPar_EN_C — Définie sur "1", cette variable indique la demande d'une attribution de paramètres. Utilisation recommandée de *iPar_EN_C* si F_CRC_Seed =1; voir la modification "Amd 1 PiR" [64].

iPar_OK_S — Définie sur "1", cette variable indique l'acquittement du paramètre par l'application du (Sous-)Module F. Utilisation recommandée de *iPar_OK_S* si F_CRC_Seed =1; voir la modification "Amd 1 PiR" [64].

OA_C
(Acquittement de l'opérateur) — Chaque programme d'application de l'hôte F doit définir/réinitialiser cette variable (type: bit). Si l'application attribue la valeur "1" à cette variable, elle est en mesure de reprendre la fonction de sécurité après une réaction aux anomalies (spécifique à la fonction de sécurité) à l'aide d'un programme d'application de l'hôte F.

OA_Req_S — Cette variable (type: bit) indique une demande d'acquittement avant la reprise d'une fonction de sécurité. Si le pilote de l'hôte F ou un pilote de l'appareil F détecte une erreur de communication ou une anomalie du (Sous-)Module F (Device_Fault = 1 et OAD_Nec_C = 1 et F_Passivation = 0), les valeurs Failsafe sont activées jusqu'à la suppression de l'erreur ou de l'anomalie et un acquittement de l'opérateur. Ensuite, le pilote de l'hôte F définit la variable OA_Req_S (="1") dès que l'anomalie/l'erreur a été résolue et que l'acquittement de l'opérateur est possible. Après l'acquittement (OA_C = "1"), le pilote de l'hôte F réinitialise la variable de demande OA_Req_S (= "0").

ChF_Ack_C
(Acquittement de l'opérateur de canal) — F_Passivation =1 (voir 8.1.6.2): Chaque programme d'application de l'hôte F doit définir/réinitialiser cette variable (type: bit). Si l'application attribue la valeur "1" à cette variable, elle est en mesure de reprendre une fonction de sécurité après la correction de toute anomalie de canal de signalisation d'un (Sous-)Module F à l'aide d'un programme d'application de l'hôte F. ChF_Ack (CB6) est défini sur "0" en cas d'anomalies stockées (FAULTS et/ou WD_timeout), ou prend la valeur de ChF_Ack_C sinon. Le signal ChF_Ack_C peut être omis et représenté par le signal OA_C à la place.

ChF_Ack_Req_S F_Passivation =1 (voir 8.1.6.2): Cette variable (type: bit) signale une demande d'acquittement en cas de défaillance d'au moins un des canaux d'entrée ou de sortie d'un (Sous-)Module F. Le pilote de l'appareil F définit alors la variable ChF_Ack_Req (= "1") dès l'élimination de l'anomalie/erreur d'au moins un canal du (Sous-)Module F. Après l'acquittement (ChF_Ack = "1"), le pilote de l'appareil F réinitialise la variable de demande ChF_Ack_Req (= "0"). Ce signal peut fait l'objet d'une relation OR logique avec *OA_Req_S* et être présenté comme signal joint *OA_Req_S*. ChF_Ack_Req_S est défini sur "0" en cas d'anomalies stockées (FAULTS et/ou WD_timeout), ou prend la valeur de ChF_Ack_Req sinon.

Valeurs d'entrée PVi Valeurs d'entrée de processus (←F-Input_Data_D, voir Figure 15)
FVi Valeurs d'entrée Failsafe, utilisées à la place de PVi pour F-Input_Data_D (Figure 15).

Valeurs de sortie PVo Valeurs de sortie de processus (→F-Output_Data_D)
FVo Valeurs de sortie Failsafe (=0), utilisées à la place de PVo pour F-Output_Data_D.

6.2 Services du pilote de l'appareil F

La Figure 15 représente les caractéristiques du pilote de l'appareil F et son imbrication entre l'interface CP 3/4 à CP 3/6 et la partie relative à la sécurité de l'application de l'appareil spécifique. Au cours de la phase de démarrage et en mode de fonctionnement, la partie non relative à la sécurité de l'application de l'appareil spécifique reçoit les paramètres F et les transmet au pilote de l'appareil F. Le pilote F lui-même, après vérification de certains des paramètres F, transmet des paramètres F à la partie relative à la sécurité de l'application du Sous-module F spécifique.

En règle générale, l'application de l'appareil spécifique offre une base de temps (1 ms) au pilote de l'appareil F afin d'alimenter les temporisateurs.

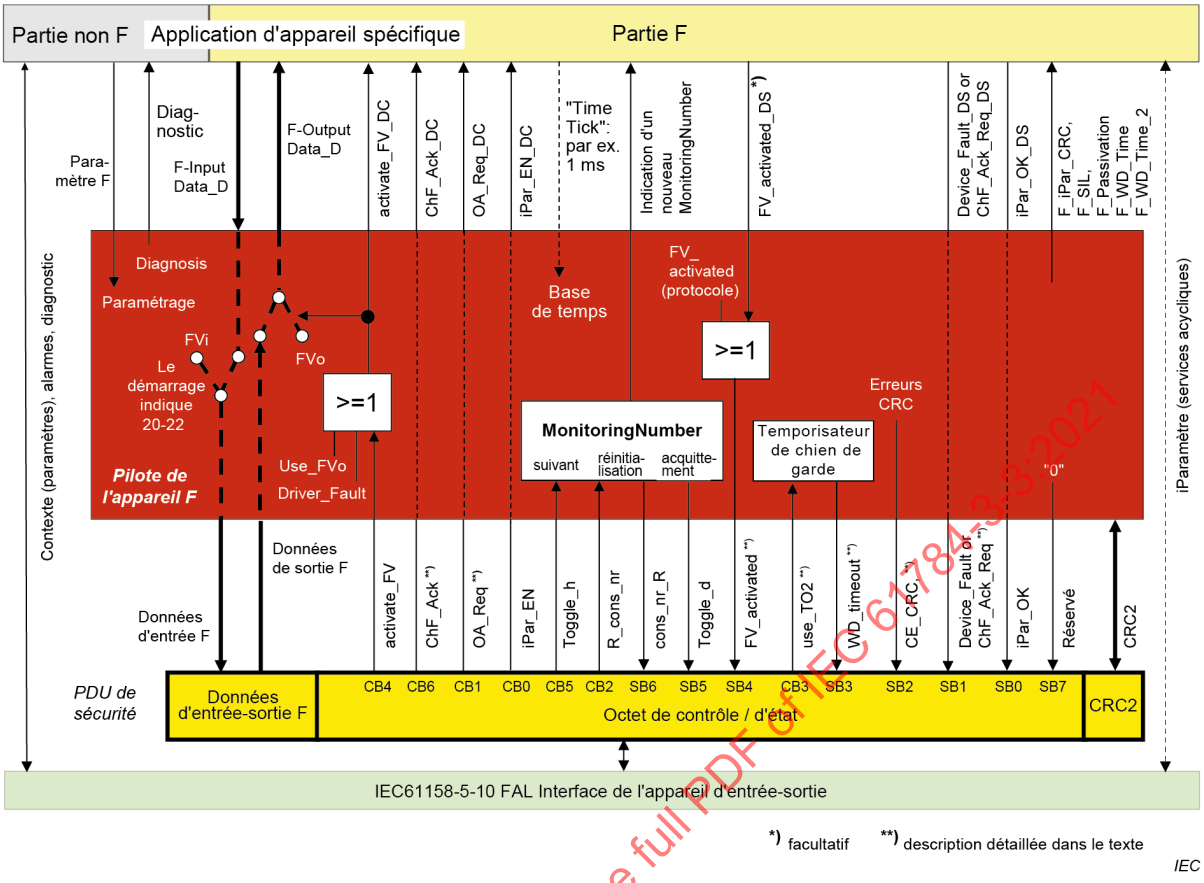


Figure 15 – Interfaces du pilote de l'appareil F

Le pilote de l'appareil F traite principalement les PDU de sécurité reçus ou transmis par l'intermédiaire de la relation de communication des données d'entrée-sortie à transmission cyclique en mémoire tampon de CP 3/4 à CP 3/6 (5.5.2). En général, les données d'entrée-sortie F sont transmises, sauf pendant le démarrage (auquel cas, FVi est transmis) ou en cas d'anomalies (auquel cas, FVo est transmis). Les PDU de sécurité reçus contiennent des octets de contrôle avec les bits de contrôle CB0 à CB6 (dans le cas où F_CRC_SEED =0: CB7 également). Certains de ces signaux sont transmis à l'interface d'application sans interaction. Un nouveau MonitoringNumber est indiqué afin de faciliter la mise en œuvre des sollicitations avec une durée suffisante (au moins un cycle FSCP 3/1 = deux MonitoringNumbers différents).

En retour, les PDU de sécurité sont préparés pour la transmission. Ils contiennent des octets d'état avec les bits d'état SB0 à SB6. L'un d'eux est transmis, le pilote F en générant certains, d'autres provenant de l'interface d'application avec manipulation du pilote F avant d'entrer dans le PDU de sécurité. Une valeur est attribuée à Driver_Fault en cas d'anomalie interne du pilote F.

Le MonitoringNumber est modifié lorsque l'état de "Toggle_h" change (0→1; 1→0). Le MonitoringNumber est réinitialisé lorsque R_cons_nr = "1". Le MonitoringNumber en cours de modification change l'état de "Toggle_d" (0→1; 1→0). Le contrôle CRC est exécuté avec chaque PDU de sécurité reçu et envoyé (CRC2).

L'application de l'appareil spécifique dispose des variables suivantes. Les variables portent des noms similaires (en principe suivis d'une extension "DC" (contrôle de l'appareil) ou "DS" (état de l'appareil), comme les bits correspondants dans les octets d'état et de contrôle.

activate_FV_DC	Cette variable relative à la sécurité indique que les données de sortie F sont des valeurs Failsafe (FV = 0). Elle peut être utilisée pour forcer les sorties d'un (Sous-)Module F à être des valeurs Failsafe configurées ou intégrées.
FV_activated_DS	Si la valeur "1" est attribuée à cette variable dans les appareils d'entrée, l'application de l'appareil fournit des valeurs Failsafe (0) au pilote FSCP 3/1 pour chaque valeur d'entrée. Si la valeur "1" est attribuée à cette variable dans les appareils de sortie, des valeurs Failsafe sont attribuées à tous les canaux de sortie. Pour les appareils d'entrée et de sortie combinés, cette variable (type: bit) signale au moyen de la valeur "1" que l'application de l'appareil fournit des valeurs Failsafe (0) au pilote FSCP 3/1 pour tous les canaux d'entrée et de sortie, et que des valeurs Failsafe sont attribuées à chaque canal d'entrée et de sortie.
OA_Req_DC	L'application du (Sous-)Module F doit utiliser cette variable non relative à la sécurité pour indiquer localement la demande d'un acquittement de l'opérateur (*OA_C* dans l'hôte F), en général par l'intermédiaire d'une LED. La mise en œuvre est facultative pour les (Sous-)Modules F.
Device_Fault_DS ou *ChF_Ack_Req_DS*	F_Passivation =0 (voir 8.1.6.2): Anomalie reconnue par l'application de l'appareil spécifique. F_Passivation =1 (voir 8.1.6.2): L'anomalie reconnue par tout canal de signalisation d'un (Sous-)Module F au moyen du qualificatif (voir [56]) est corrigée et peut être acquittée.
ChF_Ack_DC	F_Passivation =1 (voir 8.1.6.2): Le programme d'application de l'hôte F attribue la valeur "1" à cette variable. Cet acquittement confirme la correction de l'anomalie du ou des canaux de signalisation et l'évacuation de la zone de protection par le personnel.

6.3 Diagnostic

6.3.1 Génération d'alarme de sécurité

Compte tenu de la rapidité des cycles d'interrogation du programme d'application de l'hôte F, la vitesse de détection des modifications des données d'entrée-sortie F et de la signature CRC2 est satisfaisante. En cas d'erreurs de communication, le système est en mesure de réagir à temps de manière sécurisée (à l'aide des informations de l'octet d'état, par exemple).

6.3.2 Diagnostic de la couche de sécurité du (Sous-)Module F

Afin de consigner les informations de diagnostic du pilote de l'appareil F FSCP 3/1 dans une interface homme/machine, le pilote de l'appareil F les transmet à l'application du Sous-module F qui utilise des mécanismes CP 3/4 à CP 3/6 normalisés pour leur propagation au contrôleur d'entrée-sortie. Chaque option de diagnostic normalisé de CP 3/4 à CP 3/6 est possible, de préférence le diagnostic relatif au canal (Channel-Related-Diagnosis). La table de codage du champ "ChannelErrorType" définie dans l'IEC 61158-6-10 contient une plage attribuée pour FSCP 3/1.

Le Tableau 4 présente les différents types d'informations de diagnostic de la couche de protocole FSCP 3/1 des (Sous-)Modules F.

Tableau 4 – Messages de diagnostic de la couche de sécurité

Hex	Numéro	Informations de diagnostic	Obligatoire
0x0040	64	Défaut d'adaptation de l'adresse de destination de sécurité (F_Dest_Add), voir 8.1.2	Oui
0x0041	65	Adresse de destination de sécurité non valide (F_Dest_Add), voir 8.1.2	-
0x0042	66	Adresse source de sécurité non valide ou défaut d'adaptation (F_Source_Add), voir 8.1.2	-[a]
0x0043	67	La valeur du temps de fonctionnement du chien de garde de sécurité est de 0 ms (F_WD_Time, F_WD_Time_2)	-
0x0044	68	Le paramètre "F_SIL" dépasse le niveau d'intégrité de sécurité (SIL) de l'application de l'appareil spécifique	-
0x0045	69	Le paramètre "F_CRC_Length" ne correspond pas aux valeurs générées	-
0x0046	70	La version de l'ensemble de paramètres F est incorrecte	-
0x0047	71	Données incohérentes dans le bloc de paramètres F reçu (erreur CRC1)	Oui
0x0048	72	Informations de diagnostic spécifique à l'appareil ou non spécifié, voir le manuel	-
0x0049	73	Temps de fonctionnement du chien de garde iParamètre de sauvegarde dépassé	-
0x004A	74	Temps de fonctionnement du chien de garde iParamètre de restauration dépassé	-
0x004B	75	iParamètres incohérents (erreur iParCRC)	Oui[b]
0x004C	76	F_Block_ID non pris en charge	-
0x004D	77	Erreur de transmission: données incohérentes (erreur CRC2)	Oui[c]
0x004E	78	Erreur de transmission: temporisation (F_WD_Time ou F_WD_Time_2 écoulé)	Oui[c]
0x004F	79	Acquittement exigé pour activer le canal ou les canaux – lorsque l'erreur ou les erreurs de canal sont corrigées	Voir[d]
0x0050	80	Réservé: ne pas utiliser les numéros, ne pas évaluer les numéros	-
0x0051	81	Réservé: ne pas utiliser les numéros, ne pas évaluer les numéros	-
..	..	Réservé: ne pas utiliser les numéros, ne pas évaluer les numéros	-
0x005F	96	Réservé: ne pas utiliser les numéros, ne pas évaluer les numéros	-

[a] doit être utilisé avec le type d'adresse 2

[b] obligatoire si le paramètre dans F_Block_ID: "F_iPar_CRC" = 1,

[c] obligatoire pour la variante F_CRC_Seed = 1,

[d] utilisé pour la variante F_Passivation = 1.

La colonne obligatoire indique quels messages de diagnostic doivent être envoyés en cas d'erreur correspondante. Si un message de diagnostic non obligatoire est mis en œuvre, il doit utiliser le numéro de diagnostic correspondant.

Les (Sous-)Modules F qui s'appuient sur le mécanisme de serveur d'iParamètres pour stocker et extraire des iParamètres dans un hôte F ou son sous-système contrôlé peuvent consigner des informations de diagnostic dédiées à l'aide de codages supplémentaires spécifiques au fournisseur.

Les (Sous-)Modules F doivent le cas échéant utiliser ces types dans les messages de diagnostic. Toutefois, les messages de diagnostic peuvent contenir des informations récapitulatives pour plusieurs causes individuelles.

Les erreurs de transmission (codes 77 et 78) ne doivent pas engendrer l'engorgement de messages de diagnostic, par exemple lors de l'attente en premier lieu d'une communication FSCP 3/1 correcte avant une nouvelle entrée dans les ASE de diagnostic.

Erreur de transmission: les données incohérentes (erreur CRC2) doivent conduire à une entrée dans la mémoire tampon interne selon le Tableau 5, qui peut être lue par un outil spécifique au fournisseur.

Tableau 5 – Entrée de mémoire tampon sur erreur CRC2

Nom de l'attribut [a]	Longueur		Description
IMPLICIT 1	8 octets	Obligatoire	Si F_CRC_Seed =0: MNR Si F_CRC_Seed =1: CN_incrNR_64 [1]
IMPLICIT 2	8 octets	Obligatoire	Si F_CRC_Seed =0: F_Par_CRC Si F_CRC_Seed =1: CN_incrNR_64 [2]
CRC_Expected	4 octets	Obligatoire	CRC prévu
CRC_Received	4 octets	Obligatoire	CRC erroné
VERSION	2 octets	Facultatif	Valeur = 1
Codename	4 octets	Facultatif	
...	...	Facultatif	spécifique au fabricant
[a] Ces noms d'attributs sont des exemples, les noms réels sont définis par le fournisseur.			

Il convient que le fournisseur d'un appareil explique le mapping des causes individuelles avec un message de diagnostic particulier.

Des informations supplémentaires peuvent être obtenues dans [40] et [58].

7 Protocole de couche de communication de sécurité

7.1 Format PDU de sécurité

7.1.1 Structure PDU de sécurité

Figure 16 représente la structure d'un PDU de sécurité unique qui contient les données d'entrée-sortie de sécurité et un code de sécurité supplémentaire. Un message CP 3/4 à CP 3/6 peut contenir plusieurs PDU de sécurité (dans le cas d'appareils d'entrée-sortie modulaires, pour chaque (Sous-)Module F, son propre PDU de sécurité, par exemple).

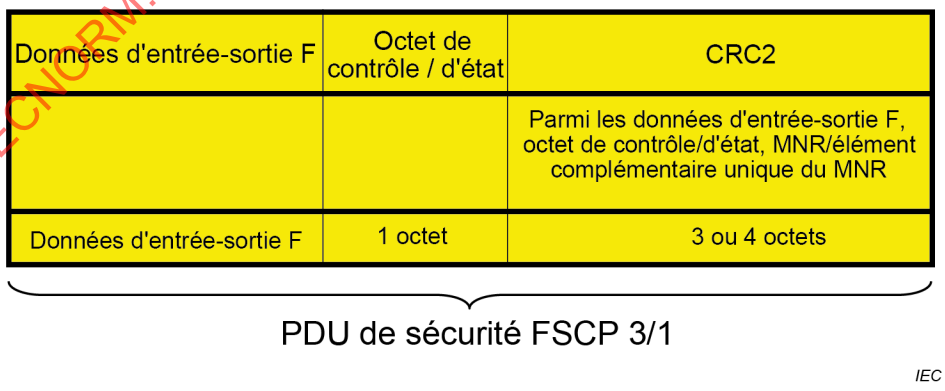


Figure 16 – PDU de sécurité pour CPF 3

Un PDU de sécurité contient les données d'entrée-sortie F, l'octet d'état/de contrôle et 3 ou 4 octets pour le code CRC2.

Les paragraphes 7.1.2 à 7.1.9 donnent une description détaillée des éléments de la structure du PDU de sécurité.

7.1.2 Données d'entrée-sortie de sécurité

Les données d'entrée-sortie F des périphériques d'entrée-sortie F sont présentées dans cette section du PDU de sécurité. Le codage de type de données correspond à celui de CP 3/4 à CP 3/6 et est défini dans l'ensemble du système dans l'IEC 61158-5-10. Le 8.5.2 recommande et spécifie les types et structures de données normalisés pour plusieurs familles d'appareils de sécurité tels que les appareils d'entrée-sortie distants, rideaux de lumière, lecteurs laser, entraînements, etc.

Outre les appareils compacts, il existe des *appareils modulaires* avec des unités d'entrée-sortie et des sous-adresses F et normalisées (Figure 11). Leur station de tête CP 3/4 à CP 3/6 (DAP), considérée comme faisant partie intégrante du canal noir, permet de convenir de la structure d'un message CP 3/4 à CP 3/6 avec plusieurs PDU de sécurité au moyen du paramétrage de démarrage. Un PDU de sécurité correspond à un Sous-module.

7.1.3 Octet d'état et de contrôle

Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
Res ("0")	Monitoring Number a été réinitialisé	Bit de bascule	Valeurs Failsafe (FV) activées	Anomalie de communication: WD-timeout	Anomalie de communication: CRC	Anomalie du (Sous-)Module F ou anomalie du canal du (Sous-)Module F corrigée	Le (Sous-)Module F acquitte l'attribution d'iParamètres
-	cons_nr_R	Toggle_d	FV_activated	WD_timeout	CE_CRC	Device_Fault/ ChF_Ack_Req	iPar_OK

Figure 17 – Octet d'état

L'octet d'état représenté à la Figure 17 est présent dans chaque PDU de sécurité d'un (Sous-)Module transmis d'un appareil à son contrôleur (Figure 16).

Le bit 0 est défini lorsque le (Sous-)Module F acquitte un Paramétrage en cours. Le nom de signal est "iPar_OK"; voir "Amd 1 PiR" [64].

Le bit 1 avec F_Passivation = 0 doit être défini par le microprogramme technologique spécifique de l'appareil pour au moins deux (2) changements du MonitoringNumber, tant qu'un (Sous-)Module F n'est pas capable d'assurer la sécurité des données de processus à transmettre. Le nom de signal dans ce cas de mise en œuvre est "Device_Fault".

Le bit 1 avec F_Passivation = 1 doit être défini par le microprogramme technologique spécifique de l'appareil si au moins un des canaux d'un (Sous-)Module F est défini sur des valeurs Failsafe (FV) du fait de l'anomalie d'un canal de signalisation et si cette anomalie est éliminée (corrigée). Les contraintes de durée pour ce signal ne sont pas nécessaires. Une défaillance du (Sous-)Module F (et non d'un seul canal) doit entraîner la commutation de tous les canaux sur l'état de sécurité intrinsèque et de tous les qualificatifs sur l'état "erreur". Le nom de signal dans ce cas de mise en œuvre est "ChF_Ack_Req". Voir [56].

Le bit 2 est défini si le pilote de l'appareil F reconnaît une anomalie de communication F, c'est-à-dire si le MonitoringNumber est incorrect (détecté par une erreur CRC2) ou en cas de transgression de l'intégrité des données (erreur CRC). Ces informations binaires permettent à l'hôte F de dénombrer tous les messages erronés dans une période T définie et de déclencher un état de sécurité configuré du système si ce nombre dépasse une certaine limite (taux d'erreurs résiduelles maximal). Le nom de signal est "CE_CRC". Voir également 9.5.1.

Le bit 3 est défini si le pilote de l'appareil F reconnaît une anomalie de communication F, c'est-à-dire si le temps de fonctionnement du chien de garde du pilote de l'appareil F est dépassé. Le nom de signal est "WD_timeout".

Le bit 4 est défini par la couche de protocole FSCP 3/1 au démarrage et en cas d'anomalie de communication (Figure 15 et 7.2). De plus, la partie F de l'application d'appareil spécifique peut également définir ce bit. Le nom de signal est "FV_activated".

Le bit 5 est un bit de bascule fondé sur le pilote de l'appareil F qui indique le déclenchement de changement du MonitoringNumber virtuel dans l'hôte F. Le nom de signal est "Toggle_d".

Le bit 6 est défini lorsque le pilote de l'appareil F a réinitialisé son MNR. Le nom de signal est "cons_nr_R" (de "consecutive number reset", nombre de réinitialisations consécutives).

Le bit 7 est réservé (res) aux versions ultérieures de FSCP 3/1 et ainsi, par défaut, il doit être défini sur "0" afin d'assurer un état défini pour une utilisation future et pour la "Vérification de bouclage" (voir 3.3).

Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
Réservé ou vérification de bouclage ("1")	Acquittement de l'opérateur après correction de l'anomalie de canal	Bit de bascule	Valeurs Failsafe (FV) à activer	Utilisation de F_WD_Time_2 (chien de garde secondaire)	Réinitialisation de Monitoring Number	Acquittement de l'opérateur demandé (indication)	Attribution d'iParamètre activée
Loopcheck	ChF_Ack	Toggle_h	activate_FV	Use_TO2	R_cons_nr	OA_Req	iPar_EN

Figure 18 – Octet de contrôle

L'octet de contrôle représenté à la Figure 18 est transmis du contrôleur d'entrée-sortie à l'appareil avec chaque PDU de sécurité pour un (Sous-)Module (Figure 16).

Le bit 0 est défini par l'application F dans un hôte F en cas de demande de Paramétrage en cours. Le nom de signal est "iPar_EN"; voir "Amd 1 PiR" [64].

Le bit 1 est défini par le pilote de l'hôte F qui correspond à la variable "OA_Req_S". Il ne s'agit pas d'un signal de sécurité, et il convient que le (Sous-)Module F l'utilise pour indiquer localement la demande d'acquittement d'un opérateur (OA_C), en général par l'intermédiaire d'une LED (9.1). Le nom de signal est "OA_Req".

Le bit 2 est défini lorsque l'hôte F détecte une erreur de communication, soit par l'octet d'état soit par lui-même. En conséquence, le MonitoringNumber virtuel du pilote de l'appareil F est réinitialisé (voir "RESETxD" en 7.1.5 et 7.1.6). Le bit 2 doit être réinitialisé après une erreur. Par la suite, le MNR reprend. Le nom de signal est "R_cons_nr" (de "Reset consecutive number", nombre de réinitialisations consécutives).

Le bit 3 est défini lorsque le pilote de l'hôte F est informé, par l'entrée interne spécifique au fournisseur, d'un processus de mise à jour prévu des composants de bus de terrain de sécurité en cas de "Reconfiguration dynamique" ou de "maintenance d'un système de tolérance aux anomalies". Ceci indique au (Sous-)Module F de prolonger le temps de fonctionnement du chien de garde F_WD_Time une seule fois par F_WD_Time_2 (voir 6.1). Le nom de signal est "Use_TO2".

Le bit 4 peut être utilisé pour forcer les sorties d'un (Sous-)Module F à être des valeurs Failsafe configurées ou intégrées. Voir 6.1 pour plus de détails. Le nom de signal est "activate_FV".

Le bit 5 est un bit de bascule fondé sur le pilote de l'hôte F qui indique le déclenchement de changement du MonitoringNumber virtuel dans le pilote de l'appareil F. Voir 7.1.4 pour plus de détails. Le nom de signal est "Toggle_h".

Le bit 6 est défini par l'application F dans un programme d'application de l'hôte F après correction d'au moins une anomalie de canal de signalisation d'un (Sous-)Module F indiquée par le bit 1 (ChF_Ack_Req) de l'octet d'état et après l'évacuation de la zone de protection par le personnel. Les PV sont activées. Voir [56]. Le nom de signal est "ChF_Ack".

Le bit 7 avec F_CRC_Seed =0: est défini sur "1" pour tous les (Sous-)Modules F dont les mises en œuvre sont conformes aux versions FSCP 3/1 antérieures à cette version (F_CRC_Seed =0). Dans la mesure où ces (Sous)Modules F renvoient toujours les octets d'état avec Bit 7 = "0", un bouclage potentiel de messages peut être détecté par le pilote de l'hôte F si ce Bit 7 renvoie "1". Le nom de signal est "Loopcheck".

Le bit 7 avec F_CRC_Seed =1: est défini sur "0" pour tous les (Sous)Modules F avec une entrée GSD F_CRC_Seed =1 et réservés pour une utilisation future.

7.1.4 MonitoringNumber (virtuel)

Le destinataire utilise le MonitoringNumber (MNR) pour s'assurer que l'émetteur du SPDU et le canal de communication sont toujours actifs. Le MNR est utilisé dans un mécanisme d'acquittement pour surveiller les *temps de propagation* entre l'émetteur et le destinataire.

FSCP 3/1 ne transmet pas le MNR avec tous les PDU de sécurité. Il utilise un MNR virtuel à la place. Il est dit "virtuel" car il ne peut être observé dans le PDU de sécurité. Cette approche s'appuie sur des MonitoringNumbers situés dans le pilote de l'hôte F et le pilote de l'appareil F, un bit de bascule de l'octet d'état et de l'octet de contrôle changeant le MNR approprié de manière synchrone (Figure 19).

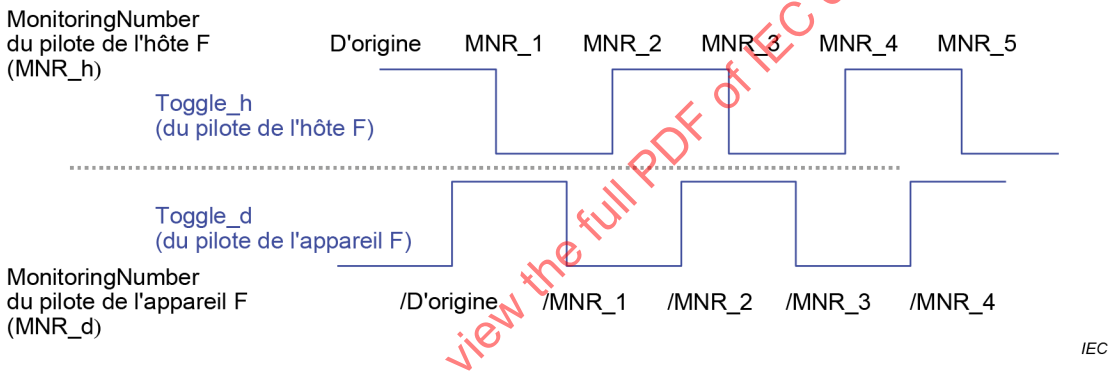


Figure 19 – Fonction du bit de bascule

L'exactitude et la synchronisation des deux MNR indépendants sont vérifiées en intégrant les MonitoringNumbers dans le calcul CRC2. CRC2 est ensuite transmis avec tous les PDU de sécurité (Figure 20).

La partie transmise du MonitoringNumber (virtuel) est réduite à un bit de bascule, qui indique un changement du MNR local. Les MNR internes au pilote de l'hôte F et au pilote de l'appareil F sont modifiés à chaque extrémité des bits de bascule (0→1, 1→0).

La Figure 20 représente le mécanisme du MRN dans le pilote de l'appareil F. Le MNR est réinitialisé lorsque l'hôte F envoie R_cons_nr = "1" dans l'octet de contrôle (voir 7.1.3).

Le mécanisme du MNR dans le pilote de l'hôte F correspond à celui du pilote de l'appareil F. Toutefois, le MNR est réinitialisé chaque fois qu'une anomalie se produit (en interne ou par l'octet d'état).

Le nom de ce mécanisme est "MNR" bien que deux procédures différentes sélectionnées par le paramètre F_CRC_Seed soient possibles.

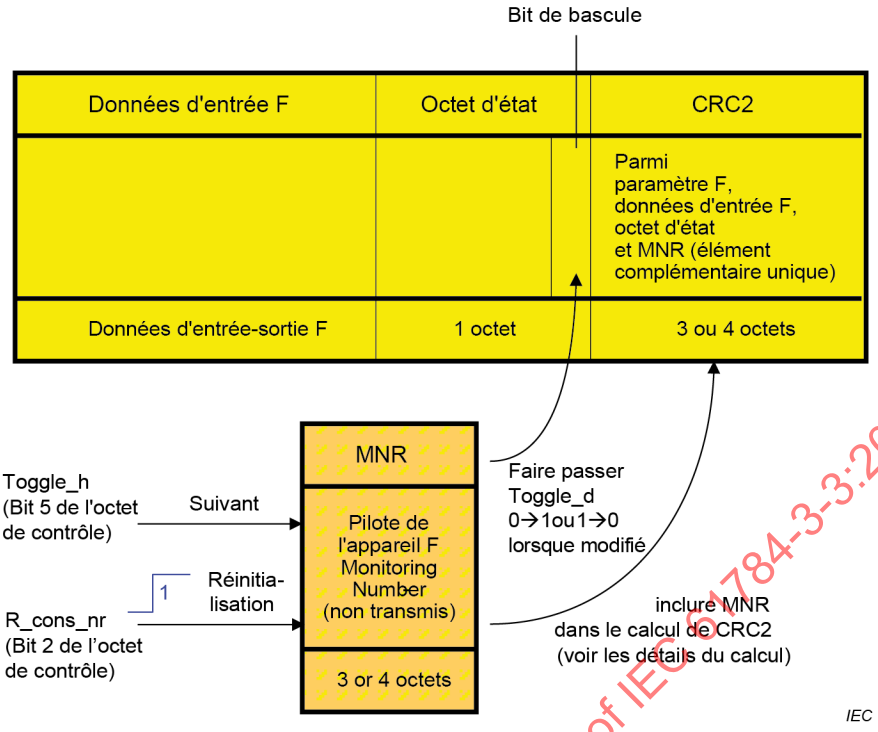


Figure 20 – Intégration du MonitoringNumber

7.1.5 Mécanisme du MNR (virtuel) (F_CRC_Seed=0)

FSCP 3/1 utilise dans ce cas des *compteurs 24 bits* pour le MonitoringNumber. Ainsi, dans un mode cyclique, le MonitoringNumber part de 1 à 0xFFFFFF, revenant à 1 à la fin (voir Tableau 6 et Tableau 7). La valeur de compteur est représentée par MNR.

Tableau 6 – MonitoringNumber du SPDU d'un pilote de l'hôte F

MACRO	ACTION (Pseudo code)
INITIALxH	old_MNR = 0xFFFFF0; MNR=0xFFFFF0;
RESETxH	R_cons_nr=1; MNR=0;
RUNxH	R_cons_nr =0, old_MNR = MNR; **if** MNR=0xFFFFFF **then** MNR=1 **else** MNR= MNR +1;

Tableau 7 – MonitoringNumber du SPDU d'un pilote de l'appareil F

MACRO	ACTION (Pseudo code)
INITIALxD	MNR=0xFFFFF0;
RESETxD	cons_nr_R =1; MNR=0;
RUNxD	cons_nr_R =0 **if** MNR=0xFFFFFF **then** MNR=1 **else** MNR= MNR +1;

7.1.6 Mécanisme du MNR (virtuel) (F_CRC_Seed=1)

FSCP 3/1 fournit une procédure étendue activée si l'entrée GSD "F_CRC_Seed" = 1 (voir 8.1.5.2). Il permet la compatibilité avec l'Annexe G de l'IEC 61784-3:2021, plus particulièrement avec le modèle par défaut d'une transmission implicite.

Cette procédure répartit l'utilisation de MonitoringNumber en deux phases. La première phase est caractérisée comme démarrage du système (INITIALx) ou en cas d'anomalie et tant que le bit 2 (R_cons_nr) dans l'octet de contrôle est défini sur "1" (RESETx). La deuxième phase est caractérisée comme communication cyclique. "CRC_FP+" est la signature CRC 32 bits (*0xF4ACFB13*) qui inclut les mêmes paramètres F que "CRC_FP" (voir Tableau 8, Tableau 9 et 8.3.3.2).

Tableau 8 – MonitoringNumber du SPDU d'un pilote de l'hôte F

MACRO	ACTION (Pseudo code)
INITIALxH	old_MNR = CRC_FP+; MNR=CRC_FP+; CRC2 = CRC2 (calculated according 7.1.8) XOR Modifier; CN_incrNR_64 [1] = 0x5851F42D4C957F2D × Codename; SwapHL = shl (CN_incrNR_64 [1], 32) + shr (CN_incrNR_64 [1], 32); CN_incrNR_64 [2] = 0xAB16D2792302FE5A × (SwapHL + Modifier) +1;
RESETxH	R_cons_nr =1; MNR=CRC_FP+; CRC2 = CRC2 (calculated according 7.1.8) XOR Modifier; CN_incrNR_64 [1] = 0x5851F42D4C957F2D × Codename SwapHL = shl (CN_incrNR_64 [1], 32) + shr (CN_incrNR_64 [1], 32); CN_incrNR_64 [2] = 0xAB16D2792302FE5A × (SwapHL + Modifier) +1;
RUNxH	R_cons_nr =0; old_MNR = MNR; CN_incrNR_64 [0] = CN_incrNR_64 [1] + CN_incrNR_64 [2]; CN_incrNR_64 [2] = CN_incrNR_64 [1]; CN_incrNR_64 [1] = CN_incrNR_64 [0]; MNR= Most significant 32 Bit of CN_incrNR_64 [0];

Tableau 9 – MonitoringNumber du SPDU d'un pilote de l'appareil F

MACRO	ACTION (Pseudo code)
INITIALxD	MNR= one's complement of CRC_FP+; Modifier = received CRC2 XOR calculated CRC2 according 7.1.8; INI_SPDU=1; CN_incrNR_64 [1] = 0x5851F42D4C957F2D × Codename; SwapHL = shl (CN_incrNR_64 [1], 32) + shr (CN_incrNR_64 [1], 32); CN_incrNR_64 [2] = 0xAB16D2792302FE5A × (SwapHL + Modifier) +1
RESETxD	cons_nr_R =1; MNR= one's complement of CRC_FP+; Modifier = received CRC2 XOR calculated CRC2 according 7.1.8; CN_incrNR_64 [1] = 0x5851F42D4C957F2D × Codename; SwapHL = shl (CN_incrNR_64 [1], 32) + shr (CN_incrNR_64 [1], 32); CN_incrNR_64 [2] = 0xAB16D2792302FE5A × (SwapHL + Modifier) +1;

RUNxD	cons_nr_R =0;
	old_MNR = MNR;
	CN_incrNR_64 [0] = CN_incrNR_64 [1] + CN_incrNR_64 [2];
	CN_incrNR_64 [2] = CN_incrNR_64 [1];
	CN_incrNR_64 [1] = CN_incrNR_64 [0];
	MNR= "one's complement" of 32 most significant bit of CN_incrNR_64 [0];

L'instruction shl (x,n) est un décalage à gauche de la valeur x du bit n logique, l'instruction shr (x,n) est un décalage à droite de la valeur x du bit n logique.

CN_incrNR_64 [0], CN_incrNR_64 [1], CN_incrNR_64 [2], et SwapHL sont des variables Unsigned64. CRC_FP+, CRC2, et Modifier sont des variables Unsigned32.

Modifier est une valeur générée par l'hôte F pour utilisation ultérieure, qui détermine une nouvelle initialisation. Lorsque les macros du pilote de l'appareil F, INITIALxD et/ou RESETxD, sont exécutées plusieurs fois, elles ne peuvent pas être censées comporter la même valeur. Cependant, dans la présente édition, la valeur "0" est toujours utilisée dans les macros de l'hôte F, INITIALxH et RESETxH.

Un exemple des 5 premières valeurs des MonitoringNumbers est présenté dans le Tableau A.4. Le MonitoringNumber est une valeur Unsigned32. L'élément complémentaire unique ("one's complement") sert à différencier les PDU de sécurité du pilote de l'hôte F des PDU de sécurité du pilote de l'appareil F afin de détecter une erreur de bouclage.

Pour le nom de code, voir 8.1.2.

7.1.7 Signature CRC2 (F_CRC_Seed=0)

Dans le cas où F_CRC_Seed = 0, les principes suivants s'appliquent: lorsque les paramètres F (relation source-destination ou nom de code, SIL, temps de fonctionnement du chien de garde, etc.) ont été transmis au pilote de l'appareil F, les paramètres identiques sont utilisés dans une procédure identique dans l'hôte F et le (Sous-)Module F pour produire une signature CRC_FP en tant que valeur de départ pour le calcul de CRC2 à transfert cyclique. Pour plus d'informations relatives à la conception de ce CRC_FP, voir 8.3.3.2. Cette signature CRC_FP, les données d'entrée-sortie F, l'octet d'état ou de contrôle et le MNR correspondant sont utilisés pour générer une autre signature CRC2 à 3 octets dans l'hôte F (voir Figure 21).

Dans le pilote de l'appareil F, la signature CRC2 identique est générée et les signatures sont comparées. Les transferts cycliques ultérieurs n'exigent qu'une comparaison de signature CRC2.

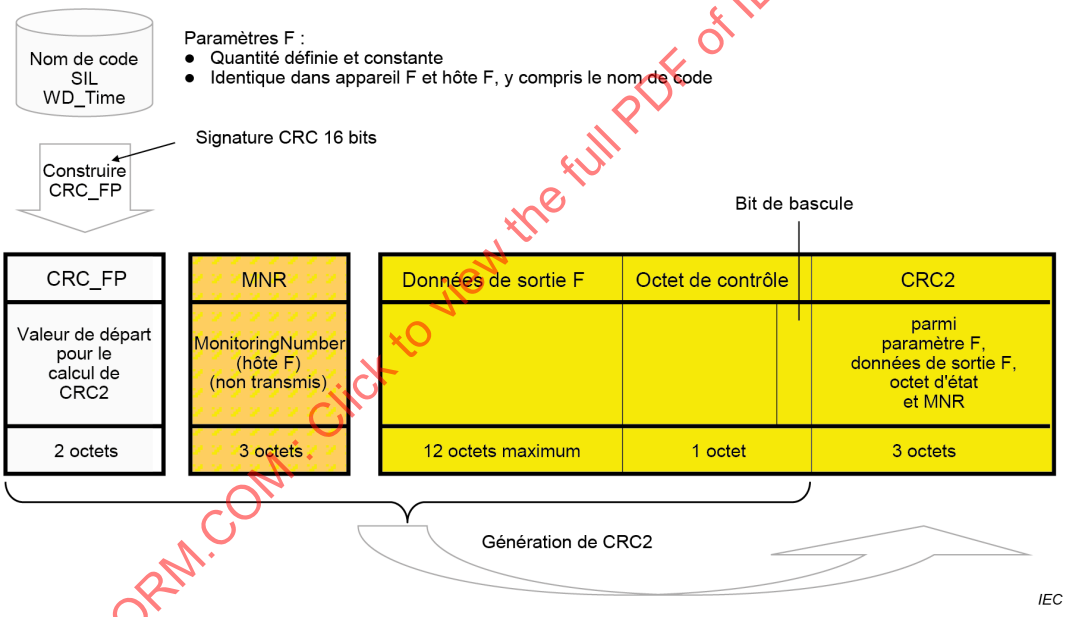


Figure 21 – Génération de signature CRC2 du pilote de l'hôte F (F_CRC_Seed=0)

Pour faciliter la détection des erreurs, même en présence de polynômes CRC identiques à l'intérieur du canal noir et de la couche de sécurité, le calcul de la signature CRC2 intègre les octets de la Figure 21 dans l'ordre inverse (voir Figure 22).

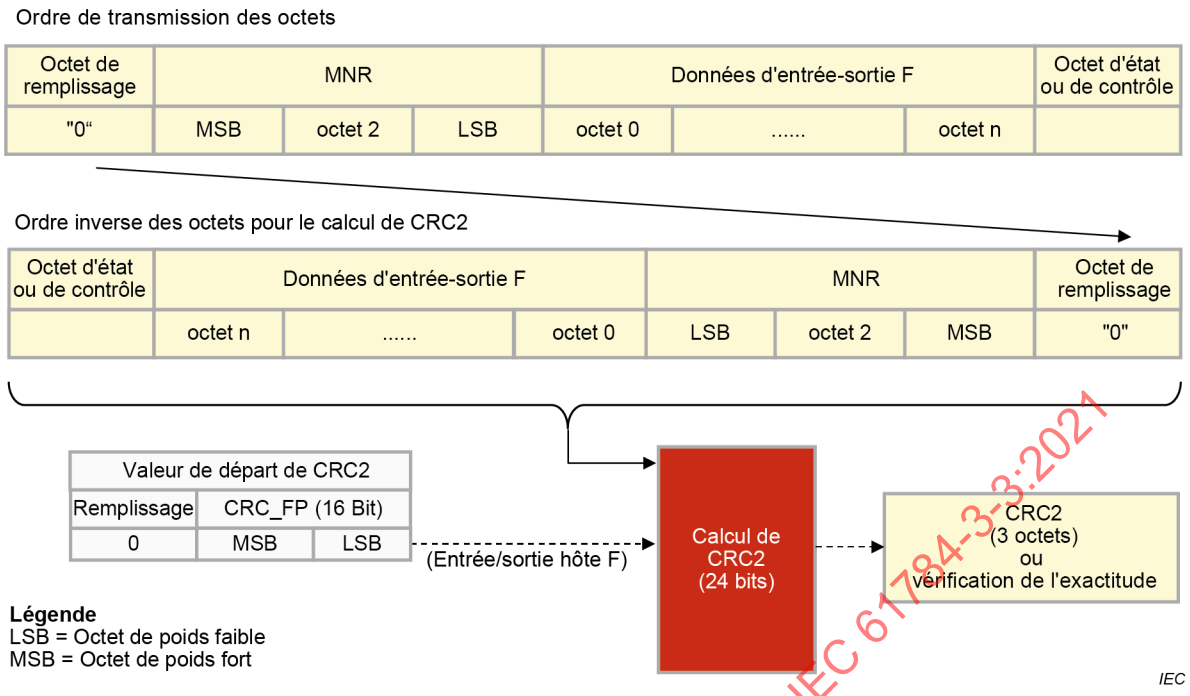


Figure 22 – Détails du calcul de la signature CRC2 (F_CRC_Seed=0)

Le polynôme générateur *0x5D6DCB* doit être utilisé pour la signature CRC2 24 bits. Pour éviter qu'un PDU de sécurité ne porte qu'un 0, une exception est faite dans ce cas particulier: la valeur "1" est attribuée à CRC2 au lieu de la valeur "0" (voir 3.3).

7.1.8 Signature CRC2 (F_CRC_Seed=1)

Dans le cas où F_CRC_Seed = 1, la première valeur de MNR est le CRC_FP+ du paramètre F, les MNR suivants constituant une séquence fondée sur le nom de code.

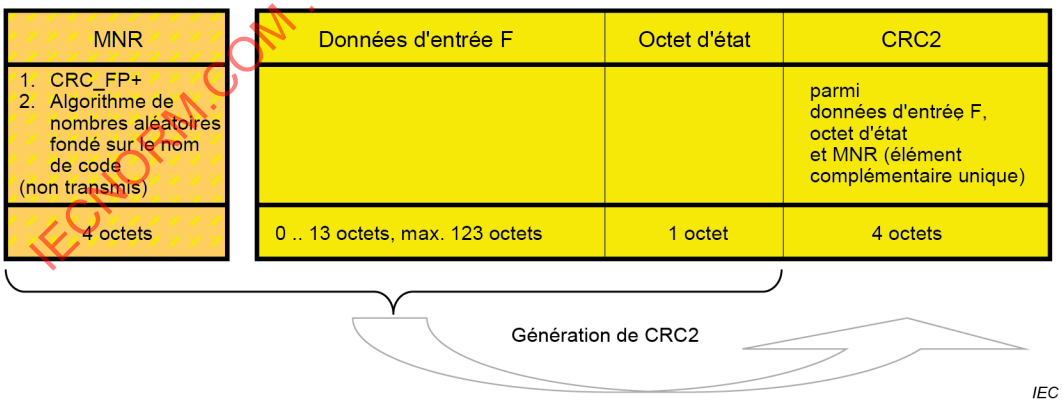


Figure 23 – Calcul de signature CRC2 (F_CRC_Seed=1)

Le calcul de la signature CRC2 inclut les octets dans l'ordre inverse (voir Figure 24).

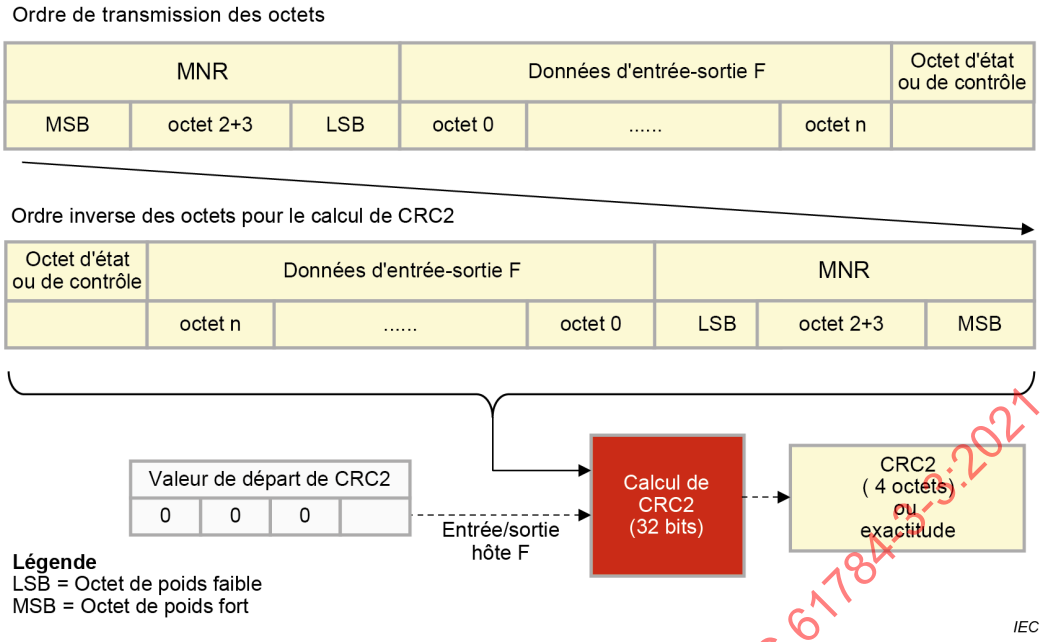


Figure 24 – Détails du calcul de la signature CRC2 (F_CRC_Seed=1)

Le pilote de l'hôte F utilise la même procédure de calcul de signature CRC2 représentée à la Figure 24 pour vérifier l'exactitude du PDU de sécurité du pilote de l'appareil F, y compris l'octet d'état, les données d'entrée F et l'élément complémentaire unique du MNR.

Le polynôme générateur *0xF4ACFB13* doit être utilisé pour la signature CRC2 32 bits. Pour éviter qu'un PDU de sécurité ne porte qu'un 0, une exception est faite dans ce cas particulier: la valeur "1" est attribuée à CRC2 au lieu de la valeur "0" (voir 3.3).

7.1.9 Données d'entrée-sortie autres que de sécurité

Des données d'entrée-sortie autres que de sécurité ne peuvent pas être ajoutées à un PDU de sécurité. Si un sous-module F a besoin de données CP 3/4 à CP 3/6 ou en génère, il est capable d'utiliser le mécanisme de modélisation de Sous-module.

7.2 Comportement FSCP 3/1

7.2.1 Généralités

Le cœur des couches de sécurité est le pilote de l'hôte F dans l'hôte F et le pilote de l'appareil F dans le (Sous-)Module F. Chacun de ces pilotes repose sur un diagramme d'états finis. Ses modes de fonctionnement sont définis au moyen des diagrammes d'états et des diagrammes séquentiels définis en 7.2.2 et 7.2.3. La Figure 25 représente un modèle simplifié de la communication de sécurité. Un chronogramme particulier présenté en 7.2.6 représente les conséquences d'une anomalie du signal de réinitialisation du MNR. La surveillance des temps de passage du PDU de sécurité est décrite en 7.2.7.

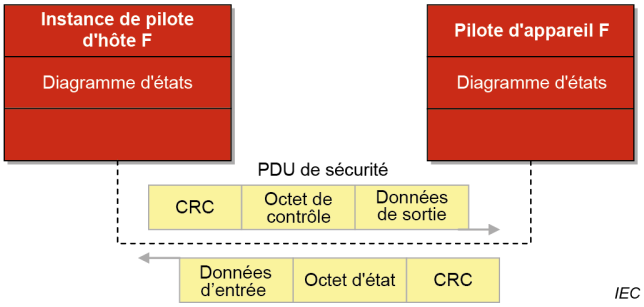


Figure 25 – Relation de communication de la couche de sécurité

7.2.2 Diagramme d'états du pilote de l'hôte F

La Figure 26 représente le diagramme d'états de l'hôte F, et le Tableau 11 décrit les états, les transitions et les éléments internes de l'hôte F. Les diagrammes suivent la notation UML2.

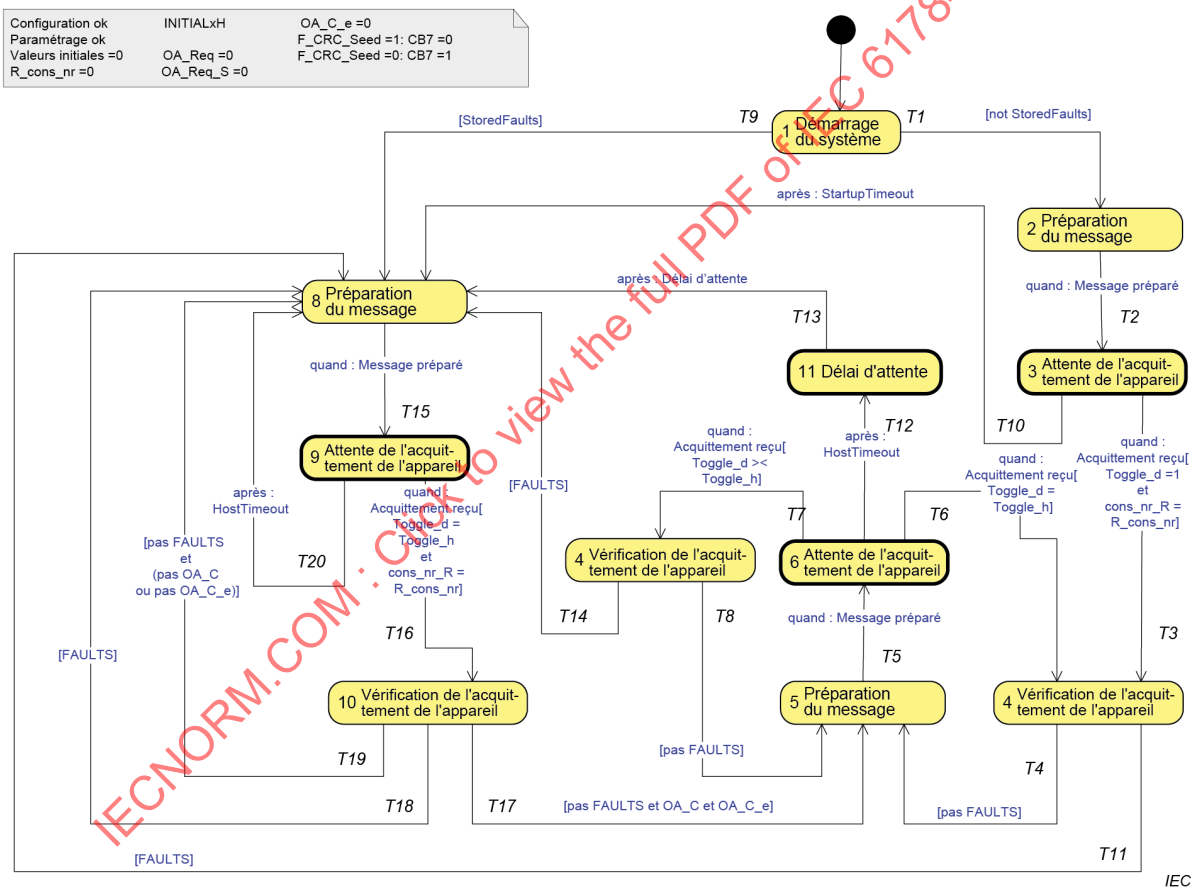


Figure 26 – Diagramme d'états du pilote de l'hôte F

Les termes utilisés dans la Figure 26 sont spécifiés dans le Tableau 10.

Tableau 10 – Définition des termes utilisés dans le diagramme d'états du pilote de l'hôte F

Terme	Définition
Initial values (Valeurs initiales)	Valeurs du PDU de sécurité =0
StartupTimeout	Temporisation spécifique au fournisseur de l'hôte F. Valeur comprise entre F_WD_Time et l'infini.
HostTimeout	Le pilote de l'hôte F reconnaît une temporisation locale lorsqu'il attend un acquittement du pilote de l'appareil F dans F_WD_Time. Cette HostTimeout doit être étendue une seule fois par F_WD_Time_2 dans le cas où "use_TO2" = 1 (F_WD_Time + F_WD_Time_2), similaire au pilote de l'appareil F (voir 6.1, 8.1.4).
Host_CE_CRC	Le pilote de l'hôte F reconnaît une anomalie CRC lors de l'analyse du PDU de sécurité reçu.
Device_Fault	F_Passivation =0 (voir 8.1.6.2): Le (Sous-)Module F a signalé une anomalie interne au pilote de l'hôte F par l'intermédiaire du pilote de l'appareil F; bit d'état 1 =1.
CE_CRC	Le pilote de l'appareil F a signalé une anomalie CRC au pilote de l'hôte F; bit d'état 2 =1.
OA_C_e	Drapeau auxiliaire qui indique un front montant du signal OA_C (0 → 1)
WD_timeout	Le pilote de l'appareil F a signalé une anomalie de temporisation au pilote de l'hôte F; bit d'état 3 =1.
INITIALxH	Macro voir 7.1.5 et 7.1.6
FAULTS	Cette variable est vraie (=1) si l'un des bits suivants est défini: - SB2 (CE_CRC) - SB3 (WD_timeout) - SB7 (Status Byte, Bit7), si F_CRC_Seed =0 - Host_CE_CRC
StoredFaults	Cette variable est vraie (=1) si l'un des bits FAULTS et/ou HostTimeout avait été stocké au moment de l'arrêt.
Ack received (Acquittement reçu)	Tout nouveau PDU de sécurité reçu; ignorer le PDU de sécurité avec toutes les valeurs =0.

Les transitions sont supprimées si un événement se produit (la réception d'un message, par exemple). Si plusieurs transitions sont possibles, les protections [conditions] définissent la transition à supprimer.

Les états 4, 7 et 10 (vérification de l'acquittement de l'appareil) sont appelés états de changement conformément à UML2 sans événement "externe". Les transitions correspondantes sont supprimées après évaluation des valeurs internes.

Le diagramme est composé d'états d'activité et d'action. Les états d'activité sont encadrés par des lignes en gras, et les états d'action par des lignes minces. Les états d'activité peuvent être interrompus par de nouveaux événements, ce qui n'est pas le cas des états d'action. Les événements qui composent un état d'action (les délais, les messages reçus ou les acquittements de l'opérateur, par exemple) sont différés jusqu'à l'état d'activité suivant.

Tableau 11 – Etats et transitions du pilote de l'hôte F

NOM D'ÉTAT	DESCRIPTION DE L'ÉTAT
1 System Start (Démarrage du système)	Etat initial de l'instance du pilote de l'hôte F lors de la mise sous tension. S'il est prévu qu'un système stocke les anomalies, la transition T9 doit être mise en œuvre. Sinon, le système utilise la transition T1 uniquement.
2 Prepare Message (Préparation du message)	Préparation d'un PDU de sécurité régulier pour le pilote de l'appareil F.
3 Await Device Ack (Attente de l'acquittement de l'appareil)	La couche de sécurité attend le PDU de sécurité régulier suivant en provenance du pilote de l'appareil F (Acquittement).
4 Check Device Ack (Vérification de l'acquittement de l'appareil)	Vérification du PDU de sécurité reçu pour une erreur CRC2 (Host_CE_CRC) qui comprend le MNR, et pour les potentielles anomalies du pilote de l'appareil F détectées dans l'octet d'état (WD_timeout, CE_CRC).
5 Prepare Message (Préparation du message)	Préparation d'un PDU de sécurité régulier pour le pilote de l'appareil F.
6 Await Device Ack (Attente de l'acquittement de l'appareil)	La couche de sécurité attend le PDU de sécurité régulier suivant en provenance du pilote de l'appareil F (Acquittement).
7 Check Device Ack (Vérification de l'acquittement de l'appareil)	Vérification du PDU de sécurité reçu pour une erreur CRC (Host_CE_CRC) qui comprend l'ancien MNR (old_MNR), et pour les potentielles anomalies du pilote de l'appareil F détectées dans l'octet d'état (WD_timeout, CE_CRC).
8 Prepare Message (Préparation du message)	Préparation d'un PDU de sécurité pour le pilote de l'appareil F (traitement des exceptions).
9 Await Device Ack (Attente de l'acquittement de l'appareil)	La couche de sécurité attend le PDU de sécurité suivant en provenance du pilote de l'appareil F (Acquittement).
10 Check Device Ack (Vérification de l'acquittement de l'appareil)	Vérification du PDU de sécurité reçu pour une erreur CRC2 (Host_CE_CRC) qui comprend le MNR, et pour les potentielles anomalies du pilote de l'appareil F détectées dans l'octet d'état (WD_timeout, CE_CRC). Lorsqu'une l'anomalie est survenue, aucun redémarrage automatique d'une fonction de sécurité n'est admis tant qu'un signal d'acquittement de l'opérateur (OA_C) n'est pas arrivé.
11 Wait delay time (Délai d'attente)	Cet état permet d'éviter le stockage d'une anomalie de temporisation en cas d'arrêt occasionnel du système, ce qui engendrerait une demande d'acquittement de l'opérateur à la prochaine mise sous tension. Un délai d'attente de 0 ms est admis.

TRANSITION	ÉTAT SOURCE	ÉTAT CIBLE	ACTION
T1	1	2	use FV, activate_FV =1, FV_activated_S =1 Toggle_h =1
T2	2	3	send safety PDU
T3	3	4	(re)start host-timer
T4	4	5	RUNxH Toggle_h = not Toggle_h, **if** FV_activated =1 or activate_FV_C =1 or Device_Fault [b] =1 **then** use FVi, FV_activated_S =1 **else** use PVi, FV_activated_S =0 **if** activate_FV_C =1 or Device_Fault [b] =1 **then** use FVo, activate_FV =1 **else** use PVo, activate_FV =0 iPar_OK_S =iPar_OK

TRANSITION	ÉTAT SOURCE	ÉTAT CIBLE	ACTION
T5	5	6	send safety PDU
T6	6	4	restart host-timer
T7	6	7	-
T8	7	5	**if** FV_activated =1 or activate_FV_C =1 or Device_Fault [b] =1 **then** use FVi, FV_activated_S =1 **else** use PVi, FV_activated_S =0 **if** activate_FV_C =1 or Device_Fault [b] =1 **then** use FVo, activate_FV =1 **else** use PVo, activate_FV =0 iPar_OK_S =iPar_OK
T9 [a]	1	8	use FV, activate_FV =1, FV_activated_S =1, Toggle_h =1, RESETxH
T10	3	8	restart host-timer, store faults, use FV, activate_FV =1, FV_activated_S =1, Toggle_h = not Toggle_h, RESETxH
T11 [c]	4	8	store faults, use FV, activate_FV =1, FV_activated_S =1, Toggle_h = not Toggle_h, RESETxH
T12 [d]	6	11	use FV, activate_FV =1, FV_activated_S =1, RESETxH
T13	11	8	store faults, Toggle_h = not Toggle_h, restart host-timer
T14 [c]	7	8	restart host-timer, store faults, use FV, activate_FV =1, FV_activated_S =1, Toggle_h = not Toggle_h, RESETxH
T15	8	9	send safety PDU
T16	9	10	restart host-timer
T17	10	5	reset stored faults, OA_Req_S =0, OA_Req =0, OA_C_e =0, Toggle_h = not Toggle_h, RUNxH **if** FV_activated =1 or activate_FV_C =1 or Device_Fault [b] =1 **then** use FVi, FV_activated_S =1 **else** use PVi, FV_activated_S =0 **if** activate_FV_C =1 or Device_Fault [b] =1 **then** use FVo, activate_FV =1 **else** use PVo, activate_FV =0 iPar_OK_S =iPar_OK
T18	10	8	store faults, OA_Req =0, OA_Req_S =0, OA_C_e =0, use FV, activate_FV =1, FV_activated_S =1, Toggle_h = not Toggle_h, RESETxH
T19	10	8	OA_Req_S =1, OA_Req =1, if OA_C =0 then OA_C_e =1 use FV, activate_FV =1, FV_activated_S =1, Toggle_h = not Toggle_h, RUNxH

TRANSITION	ÉTAT SOURCE	ÉTAT CIBLE	ACTION
T20	9	8	store faults, OA_Req =0, OA_Req_S =0, OA_C_e =0, use FV, activate_FV =1, FV_activated_S =1, Toggle_h = not Toggle_h, RESETxH restart host-timer

[a] Voir STATE DESCRIPTION de STATE 1. L'énoncé "store faults" (stocker les anomalies) dans les transitions peut être omis si T9 n'est pas mise en œuvre.

[b] Device_Fault n'est pas pris en considération dans l'opération logique si F_Passivation = 1.

[c] Les transitions T11 et T14 produisent un message de diagnostic "Erreurs de transmission du diagnostic de l'hôte (CRC)".

[d] La transition T12 produit un message de diagnostic "Erreurs de transmission du diagnostic de l'hôte (temporisation)".

ÉLÉMENTS INTERNES	TYPE	DÉFINITION
RESETxH	Macro	Voir 7.1.5 et 7.1.6
RUNxH	Macro	Voir 7.1.5 et 7.1.6
MNR	Variable	MNR représente le MonitoringNumber local dans l'instance du pilote de l'hôte F. Il n'est pas transmis à son homologue du pilote de l'appareil F, mais synchronise en revanche ces homologues par l'intermédiaire d'un bit de bascule de l'octet de contrôle. Le MNR réel est intégré dans le calcul de CRC2 et ainsi vérifié par rapport aux anomalies de transmission.
old_MNR	Variable	Valeur précédente du MNR local actuel. Il est nécessaire de stocker cette valeur précédente du MNR.
DelayTime	Temporisateur	Ce délai d'attente permet de couvrir le temps de stabilisation à la mise hors tension de l'ensemble du système. Le fabricant de l'hôte/du système est chargé de définir ce paramètre.
host-timer	Temporisateur	Ce temporisateur permet de vérifier si le PDU de sécurité valide suivant en provenance du pilote de l'appareil F est arrivé à temps. L'outil de développement de l'hôte est chargé de définir ce temps de fonctionnement du chien de garde. La plage de valeurs est comprise entre 0 et 65 535 ms.
OA_C_e	Drapeau	Au moyen de cette variable (bit) auxiliaire, l'état de sécurité est maintenu tant qu'un signal de changement OA_C de 0 → 1 (front) n'a pas été reçu. Sans l'aide de ce mécanisme, un opérateur peut annuler des états de sécurité en activant définitivement le signal OA_C.
faults	Drapeaux	Tant qu'un acquittement de l'opérateur (OA_C) n'a pas été reçu, un stockage permanent du bit FAULT (voir Tableau 10) est exigé dans l'hôte F uniquement (pas dans le (Sous-)Module F).
	Etat d'activité	Dans ces états d'"activité" qu'il est possible d'interrompre, l'hôte attend de nouvelles entrées (une temporisation ou un acquittement, par exemple) [29].
	Etat d'action	Dans ces états d'"action" qu'il est impossible d'interrompre, les événements (temporisation, message reçu ou acquittement de l'opérateur, par exemple) sont différés jusqu'à l'état d'"activité" suivant [29].

7.2.3 Diagramme d'états du pilote de l'appareil F

La Figure 27 représente le diagramme d'états du pilote de l'appareil F, et le Tableau 13 décrit les états, les transitions et les éléments internes. Les diagrammes suivent la notation UML2.

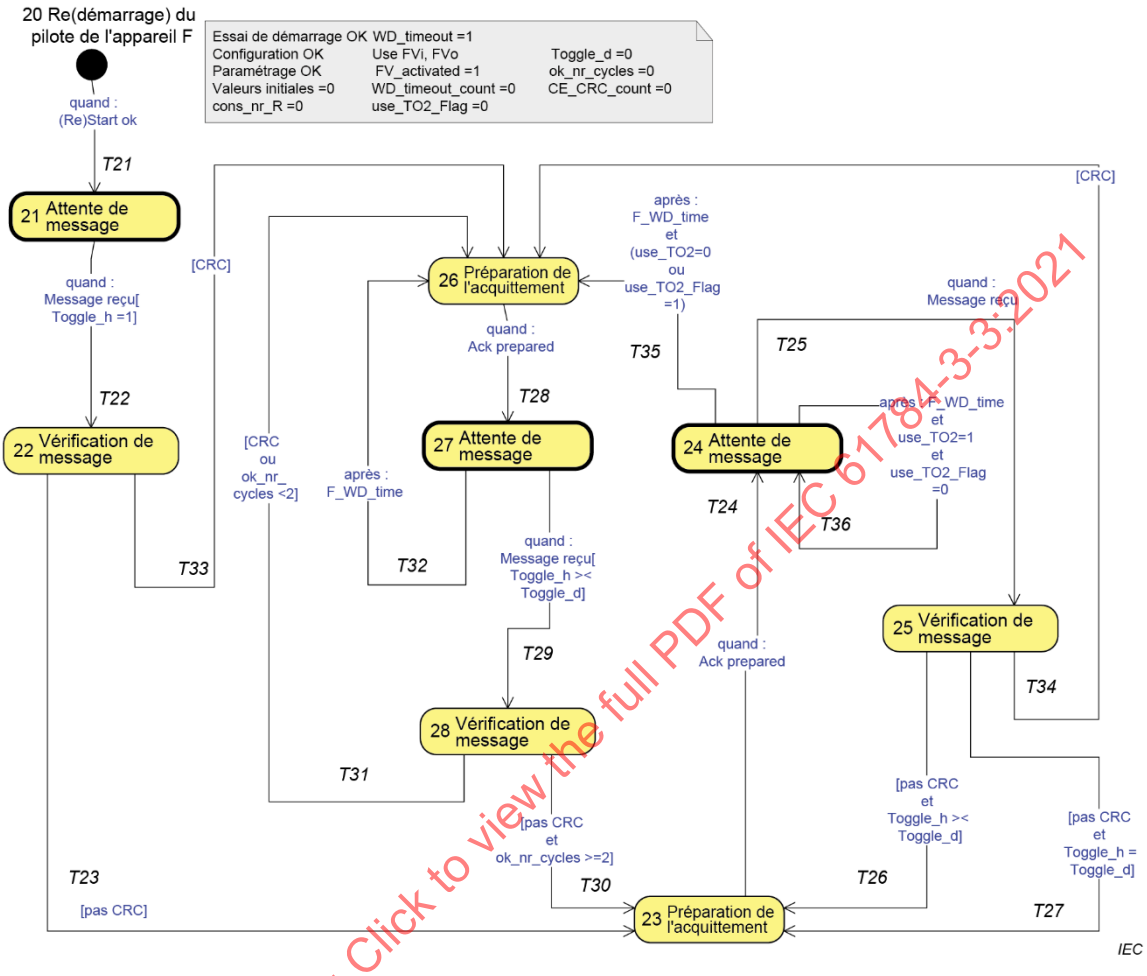


Figure 27 – Diagramme d'états du pilote de l'appareil F

Les termes utilisés dans la Figure 27 sont spécifiés dans le Tableau 12.

Tableau 12 – Définition des termes utilisés dans la Figure 27

Terme	Définition
[Toggle_h = Toggle_d]	Notation UML d'une condition (protection) pour supprimer la transition. Dans ce cas, elle signifie: La valeur du bit Toggle_h n'a pas changé ("pas de bascule")
[Toggle_h >< Toggle_d]	La valeur du bit Toggle_h a changé ("bascule")
[CRC]	Le pilote de l'appareil F reconnaît l'anomalie CRC (erreur de communication et/ou de MNR)
F_WD_Time	Temps de fonctionnement du chien de garde défini par le paramètre F "F_WD_Time"
use_TO2	CB3 de l'octet de contrôle qui indique l'utilisation du temps de fonctionnement du chien de garde secondaire F_WD_Time_2
use_TO2_Flag	Drapeau auxiliaire
INI_SPDU	Drapeau auxiliaire utilisé pour le premier cycle omettant le contrôle CRC2
Ack (Acquittement)	Acquittement du PDU de sécurité du pilote de l'appareil F
Message received (Message reçu)	Tout nouveau PDU de sécurité reçu; ignorer le PDU de sécurité avec toutes les valeurs =0.
INITIALxD	Macro voir 7.1.5 et 7.1.6

Tableau 13 – Etats et transitions du pilote de l'appareil F

NOM D'ÉTAT	DESCRIPTION DE L'ÉTAT
20 F-Device driver (Re)Start ((Re)démarrage du pilote de l'appareil F)	Etat initial du (Sous-)Module F. Les valeurs initiales du (Sous-)Module F d'entrée sont "0". Immédiatement après le paramétrage F, les valeurs Failsafe de sortie doivent être définies par l'appareil F.
21 Await Message (Attente de message)	La couche de sécurité attend le PDU de sécurité suivant en provenance du pilote de l'hôte F. A l'état "(Re)Start", l'appareil F doit réagir au premier SPDU valide en provenance du pilote de l'hôte F dans le délai de temporisation PROFIsafe en répondant avec un SPDU valide.
22 Check Message (Vérification de message)	**Si** (F_CRC_Seed =0) **alors** Vérification du PDU de sécurité reçu pour une erreur CRC2 **sinon** Pas de vérification (Le contenu de CRC2 est évalué en T22)
23 Prepare Ack (Préparation de l'acquittement)	Préparation d'un PDU de sécurité régulier pour le pilote de l'hôte F (Acquittement).
24 Await Message (Attente de message)	La couche de sécurité attend le PDU de sécurité régulier suivant en provenance du pilote de l'hôte F.
25 Check Message (Vérification de message)	**Si** (F_CRC_Seed =0) **alors** Vérification du PDU de sécurité reçu pour une erreur CRC2 **sinon** **si** (R_cons_nr =0) et (INI_SPDU=0) **alors** Vérification du PDU de sécurité reçu pour une erreur CRC2
26 Prepare Ack (Préparation de l'acquittement)	Préparation d'un PDU de sécurité pour l'hôte F (Acquittement avec bits erronés).
27 Await Message (Attente de message)	La couche de sécurité attend le PDU de sécurité suivant en provenance de l'hôte F (traitement des exceptions).
28 Check Message (Vérification de message)	**Si** (R_cons_nr =0) **alors** Vérification du PDU de sécurité reçu pour une erreur CRC2

TRANSITION	ÉTAT SOURCE	ÉTAT CIBLE	ACTION
T21	20	21	-
T22	21	22	**if** R_cons_nr =1 **then** RESETxD **else** INITIALxD
T23	22	23	use PVi, FVo, FV_activated =1, CE_CRC =0, WD_timeout =0, Toggle_d =Toggle_h, restart device-timer, ok_nr_cycles =ok_nr_cycles +1
T24	23	24	send safety PDU
T25	24	25	**if** Toggle_h >< Toggle_d **then** INI_SPDU=0 **if** R_cons_nr =1 **then** RESETxD **else** RUNxD

TRANSITION	ÉTAT SOURCE	ÉTAT CIBLE	ACTION
T26	25	23	restart device-timer Use PVi, Toggle_d = Toggle_h, if ok_nr_cycles <4 ok_nr_cycles =ok_nr_cycles +1 **if** ok_nr_cycles <4 **then** use FVo, FV_activated =1 **else** use PVo, FV_activated =0 **if** activate_FV =1 **then** use FVo **if** use_TO2 =0 **then** use_TO2_Flag =0
T27	25	23	Use PVi, Toggle_d = Toggle_h, **if** ok_nr_cycles <4 **then** use FVo, FV_activated =1 **else** use PVo, FV_activated =0 **if** activate_FV =1 **then** use FVo
T28	26	27	Send safety PDU
T29	27	28	INI_SPDU=0 **if** R_cons_nr =1 **then** RESETxD **else** RUNxD
T30	28	23	use PVi, FVo, FV_activated =1, Toggle_d = Toggle_h, restart device-timer, ok_nr_cycles =ok_nr_cycles +1
T31	28	26	Toggle_d = Toggle_h, restart device-timer, **if** CRC **then** CE_CRC =1, CE_CRC_count =1, ok_nr_cycles =0, **else** ok_nr_cycles =ok_nr_cycles +1, **if** CE_CRC_count >0 **then** CE_CRC =1, CE_CRC_count = CE_CRC_count -1, **else** CE_CRC =0, **if** WD_timeout_count >0 **then** WD_timeout =1, WD_timeout_count = WD_timeout_count -1 **else** WD_timeout =0
T32	27	26	Use PVi, FVo, FV_activated =1, WD_timeout =1, WD_timeout_count =1, ok_nr_cycles =0, restart device timer, Toggle_d = Toggle_h
T33	22	26	Use PVi, FVo, FV_activated =1, CE_CRC =1, CE_CRC_count =1, WD_timeout =0, ok_nr_cycles =0, restart device-timer, Toggle_d = Toggle_h

TRANSITION	ÉTAT SOURCE	ÉTAT CIBLE	ACTION
T34	25	26	Use PVi, FVo, FV_activated =1, CE_CRC =1, CE_CRC_count =1, ok_nr_cycles =0, restart device-timer, Toggle_d = Toggle_h
T35	24	26	Use PVi, FVo, FV_activated =1, WD_timeout =1, WD_timeout_count =1, ok_nr_cycles =0, restart device timer, Toggle_d = Toggle_h
T36	24	24	restart device timer with F_WD_Time_2 use_TO2_Flag =1

ÉLÉMENTS INTERNES	TYPE	DÉFINITION
RESETxD	Macro	Voir 7.1.5 et 7.1.6
RUNxD	Macro	Voir 7.1.5 et 7.1.6
MNR	Variable	MNR représente le MNR local réel dans le pilote de l'appareil F. Il n'est pas transmis à son homologue de l'hôte F, mais synchronisé en revanche avec ces homologues par l'intermédiaire d'un bit de bascule de l'octet de contrôle. Cela signifie qu'il change chaque fois que l'état du bit de bascule de l'octet de contrôle (Toggle_h) change de 0 → 1 ou de 1 → 0.
ok_nr_cycles	Compteur	Lors du démarrage et après une anomalie, le pilote de l'appareil F doit définir FVo et FV_activated =1 pendant au moins 3 cycles. Ce compteur incrémentiel est chargé de compter ces cycles de 0 à 3.
CE_CRC_count	Compteur	Ce compteur décrémentiel permet de s'assurer que le bit "CE_CRC" de l'octet d'état est défini pour au moins 1 cycle ou 2 cycles au maximum. La plage de valeurs est comprise entre 0 et 1.
WD_timeout_count	Compteur	Ce compteur décrémentiel permet de s'assurer que le bit "WD_timeout" de l'octet d'état est défini pour au moins 1 cycle ou 2 cycles au maximum. La plage de valeurs est comprise entre 0 et 1.
device-timer	Temporisateur	Ce temporisateur permet de vérifier si le PDU de sécurité valide suivant est arrivé à temps. Le paramètre F " F_WD_Time" permet de définir ce temps de fonctionnement du chien de garde. La plage de valeurs est comprise entre 0 et 65 535 ms.

7.2.4 Redémarrage du pilote de l'appareil F

La séquence suivante doit initier un redémarrage du pilote de l'appareil F à l'état 20 (conformément à la Figure 27):

– perte de la connexion au bus de terrain (AR-Release, par exemple) pendant au moins F_WD_Timeout [a]; puis

– redémarrage de la connexion au bus de terrain (AR-Connect/ établir AR, par exemple) et/ou transmission des Paramètres F.

[a] En cas de perte de la connexion du bus de terrain, le pilote de l'appareil F peut réagir immédiatement ou après F_WD_Timeout.

NOTE La vérification de cette séquence et le redémarrage du pilote de l'appareil F sont généralement exécutés par l'application du (Sous-)Module F.

Si le pilote de l'appareil F redémarre à l'état 20, le pilote de l'appareil F doit vérifier les paramètres F, qu'ils aient été modifiés ou non.

7.2.5 Diagrammes séquentiels

Les messages d'interaction du pilote de l'hôte F et du pilote de l'appareil F pendant la phase de démarrage sont représentés de la Figure 28 à la Figure 33. Trois phases sont représentées: les deux partenaires lors du démarrage, l'hôte F commutant temporairement la mise hors tension ou le (Sous-)Module F étant temporairement mis hors tension pendant le fonctionnement de son partenaire. Les figures donnent des informations sur les états et les transitions correspondantes. Les numéros placés dans des cercles représentent les états que traversent respectivement le pilote de l'hôte F et le pilote de l'appareil F.

La Figure 28 représente le début régulier des transmissions de PDU de sécurité entre le pilote de l'hôte F et le pilote de l'appareil F après mise sous tension. Une séquence possible des MonitoringNumbers est présentée dans le Tableau A.4.

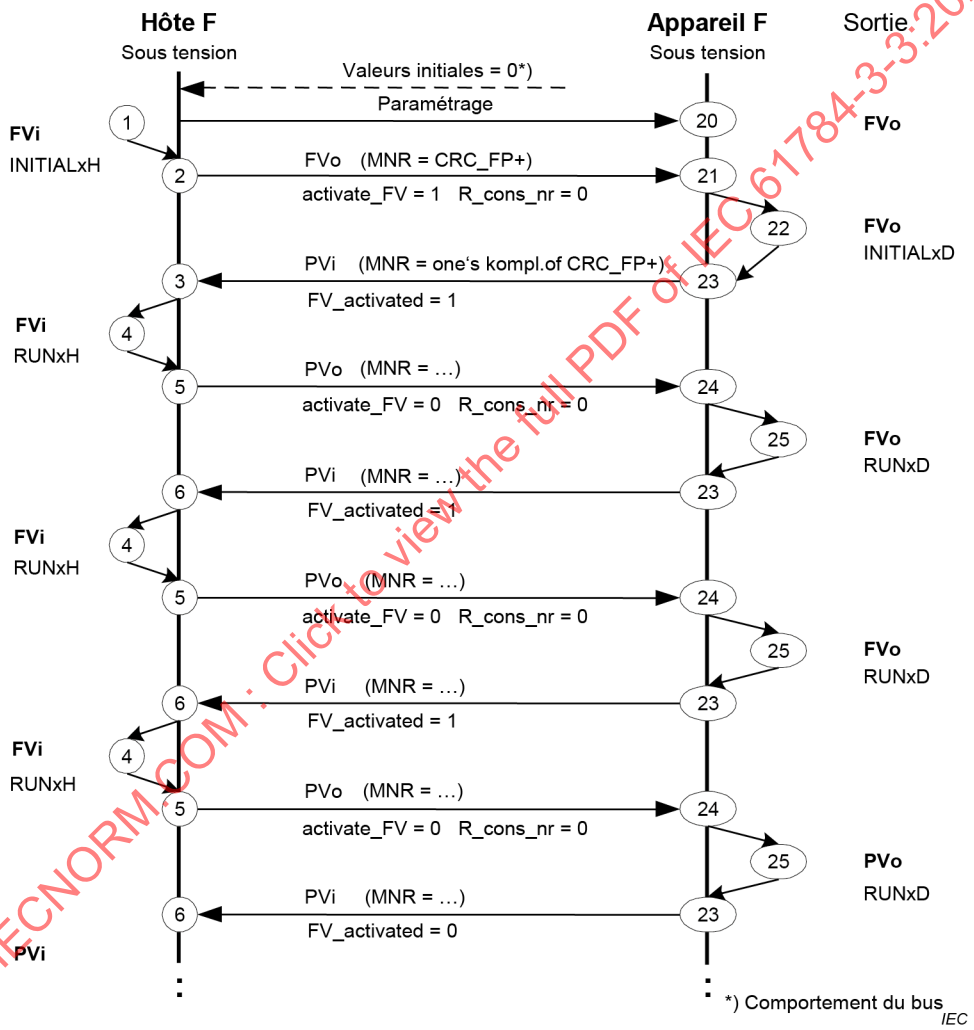


Figure 28 – Interaction du pilote de l'hôte F et du pilote de l'appareil F pendant le démarrage

La Figure 29 représente un exemple d'attribution de paramètre F dans le cas où le pilote de l'appareil F fonctionne déjà et où l'hôte F passe de la mise hors tension à la mise sous tension.

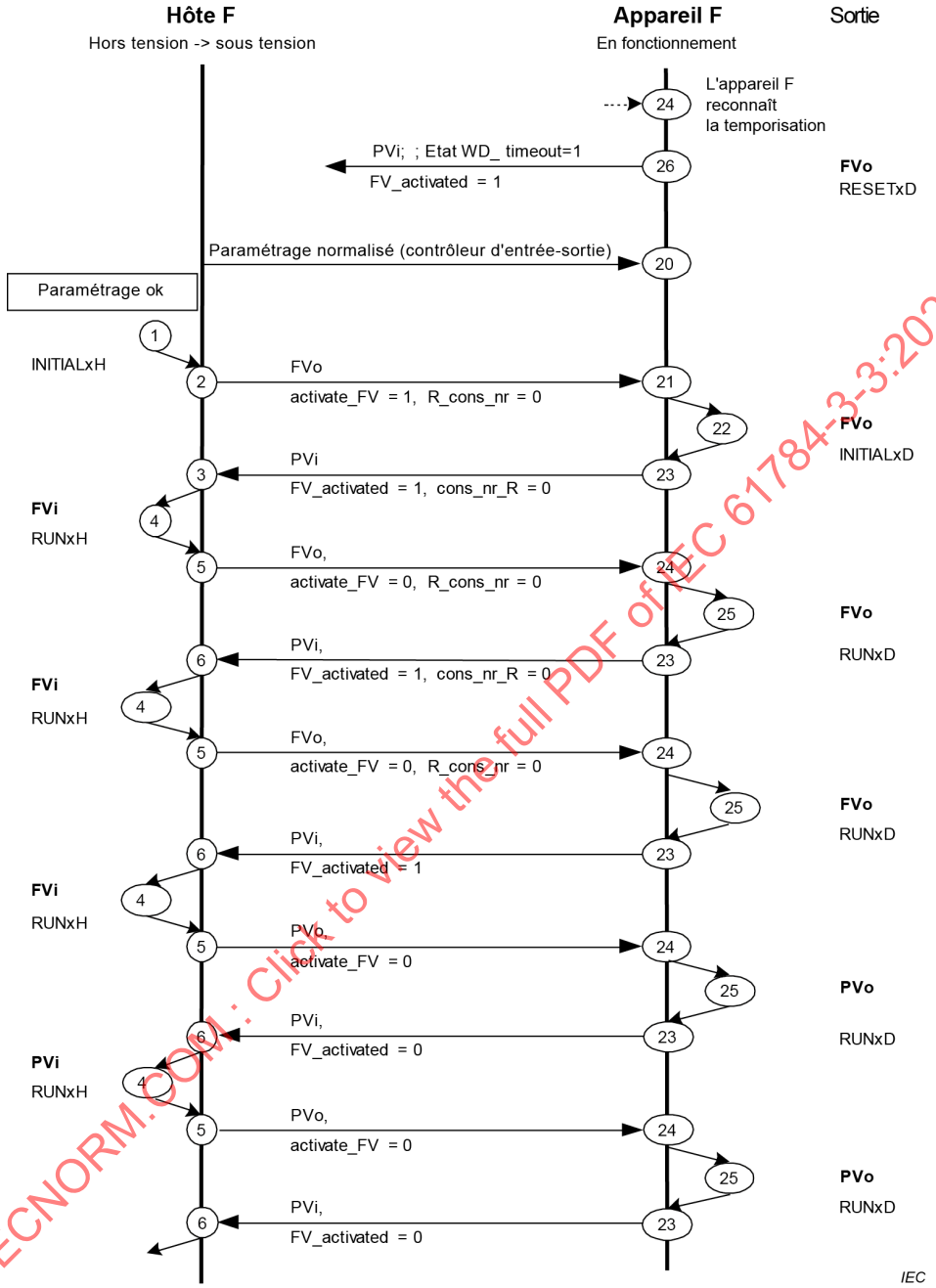


Figure 29 – Interaction du pilote de l'hôte F et du pilote de l'appareil F pendant la mise hors tension > sous tension de l'hôte F

La Figure 30 représente un exemple d'attribution de paramètre F dans le cas où le pilote de l'hôte F fonctionne déjà et où le (Sous-)Module F commute la mise sous tension après un report.

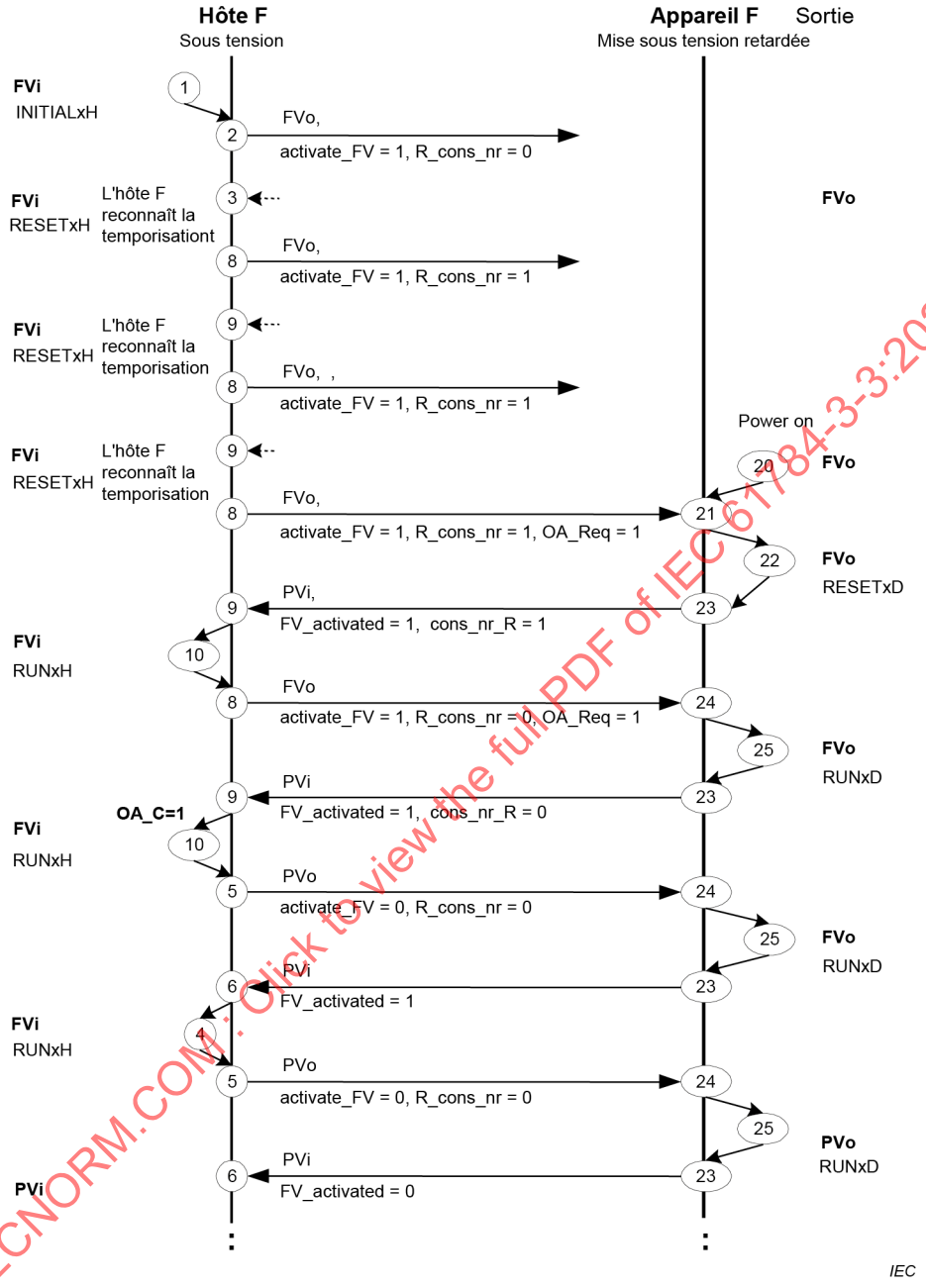


Figure 30 – Interaction du pilote de l'hôte F et du pilote de l'appareil F pendant un report de mise sous tension

La Figure 31 correspond à la Figure 30. Elle représente le cas où l'hôte F fonctionne déjà et où le (Sous-)Module F commute la mise hors tension, puis, après un report, commute à nouveau la mise sous tension.

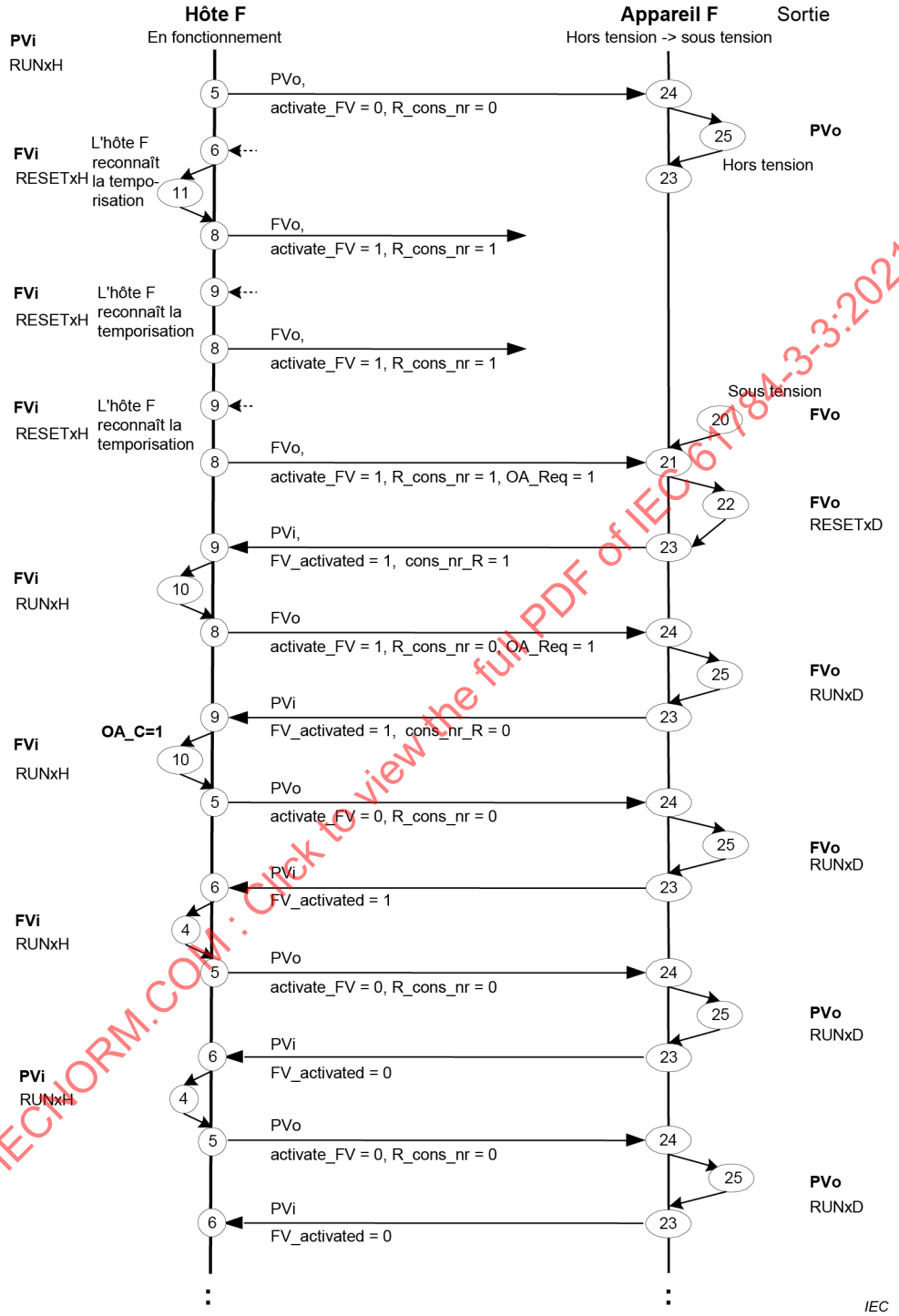


Figure 31 – Interaction du pilote de l'hôte F et du pilote de l'appareil F pendant la mise hors tension → sous tension

La Figure 32 représente les messages d'interaction entre le pilote de l'hôte F et le pilote de l'appareil F lorsque des anomalies CRC sont détectées du côté du pilote de l'hôte F.

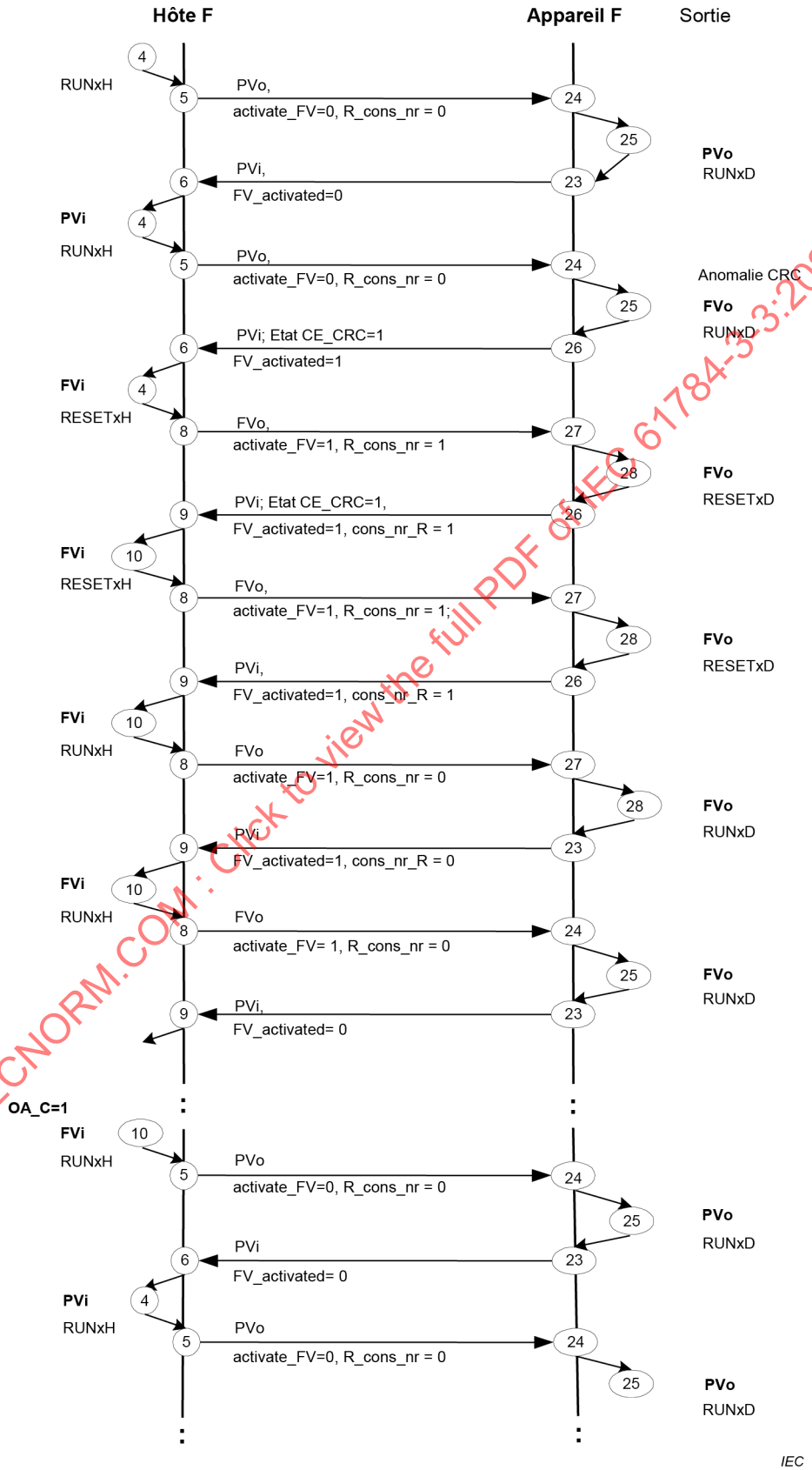


Figure 32 – Interaction lorsque le pilote de l'hôte F reconnaît une erreur CRC

La Figure 33 représente les messages d'interaction entre le pilote de l'hôte F et le pilote de l'appareil F lorsque des anomalies CRC sont détectées du côté du pilote de l'appareil F.

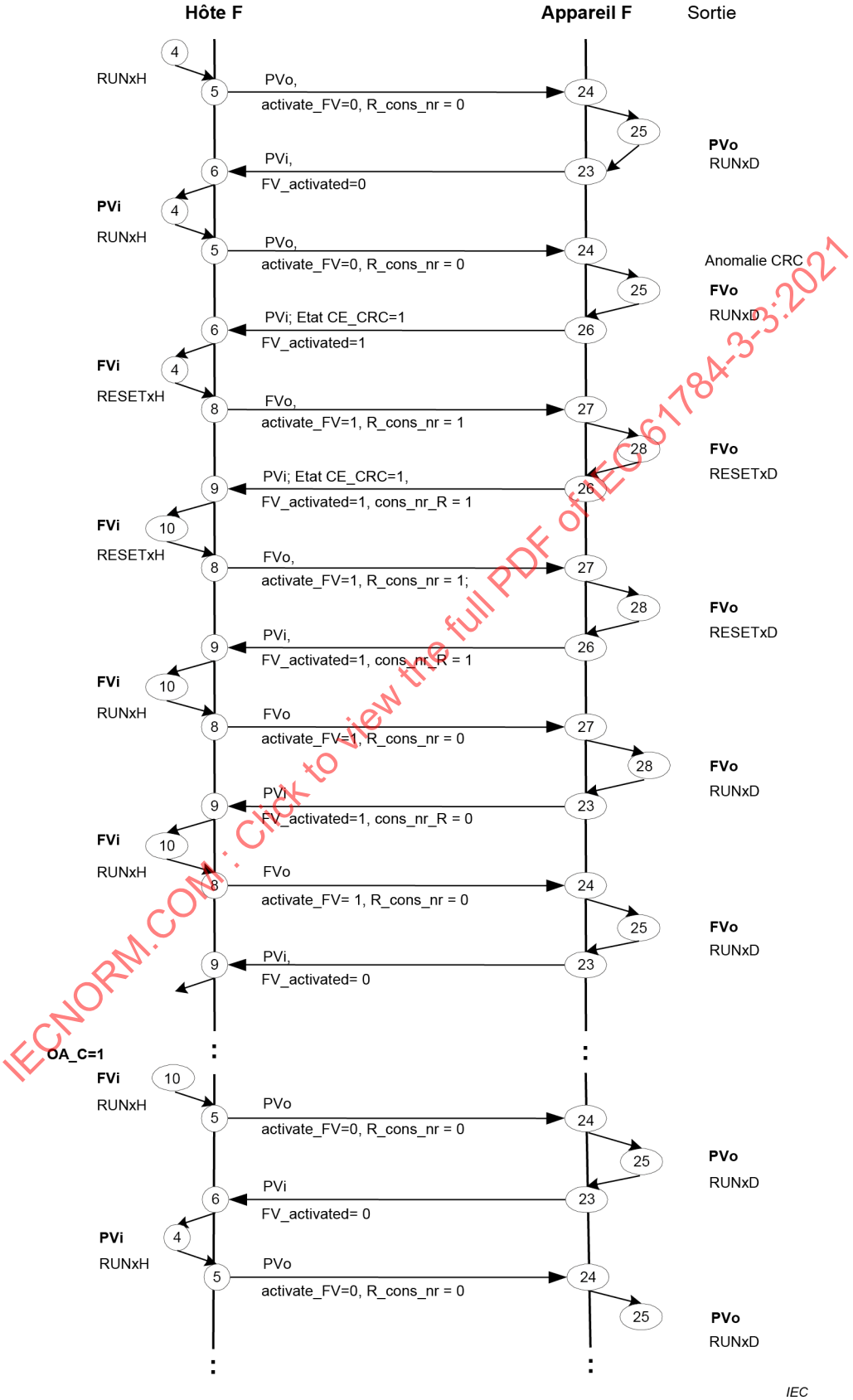


Figure 33 – Interaction lorsque le pilote de l'appareil F reconnaît une erreur CRC

7.2.6 Chronogramme de réinitialisation d'un MonitoringNumber

La Figure 34 représente les conséquences d'une anomalie de communication sur le MonitoringNumber et les éléments dépendants.

Après une anomalie, le bit 2 ("R_cons_nr") et le bit 4 ("activate_FV") de l'octet de contrôle sont définis (=1). Par conséquent, le MNR est réinitialisé et les valeurs de sortie d'un appareil de sortie F sont définies sur "FVo".

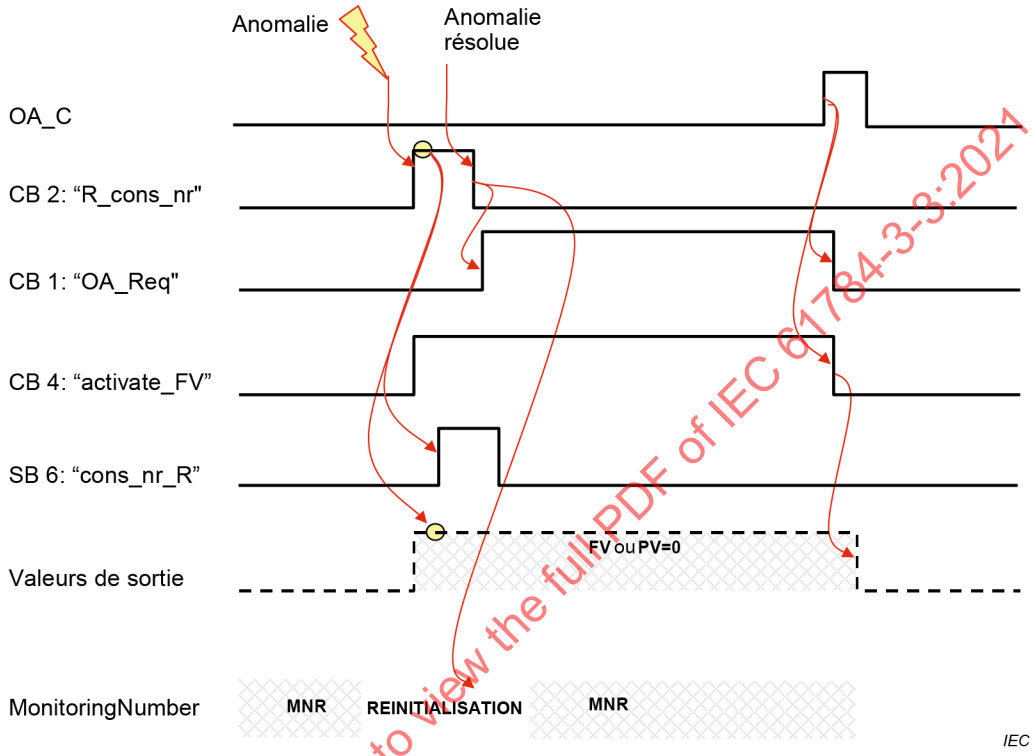


Figure 34 – Impact du signal de réinitialisation du MNR

Immédiatement après la résolution de l'anomalie, les actions ci-dessous se déroulent:

- la réinitialisation du MNR reprend sa valeur par défaut (R_cons_nr =0);
- le MNR redémarre.

Immédiatement après un acquittement de l'opérateur (OA_C = 1), les actions ci-dessous se déroulent:

- la demande d'un acquittement de l'opérateur reprend sa valeur par défaut (OA_Req =0);
- la demande d'activation d'un état de sortie de sécurité intrinsèque reprend sa valeur par défaut (activate_FV =0);
- les valeurs de sortie du processus apparaissent de nouveau après trois cycles de message.

7.2.7 Surveillance des temps de sécurité

7.2.7.1 Fonctionnement normal

La Figure 35 explique comment les pilotes F (de l'hôte F et du-(Sous-)Module F) utilisent les communications CP 3/4 à CP 3/6 sous-jacentes et la manière dont les temps de surveillance sont définis. Signification des flèches courtes: dans CP 3/4 à CP 3/6, le contrôleur d'entrée-sortie est capable de mettre à jour le Sous-module F et, par conséquent, le PDU de sécurité plus fréquemment que le pilote de l'hôte F ne génère un nouveau PDU de sécurité dans la durée de cycle du pilote de l'hôte F et/ou la durée de cycle du pilote de l'appareil F.

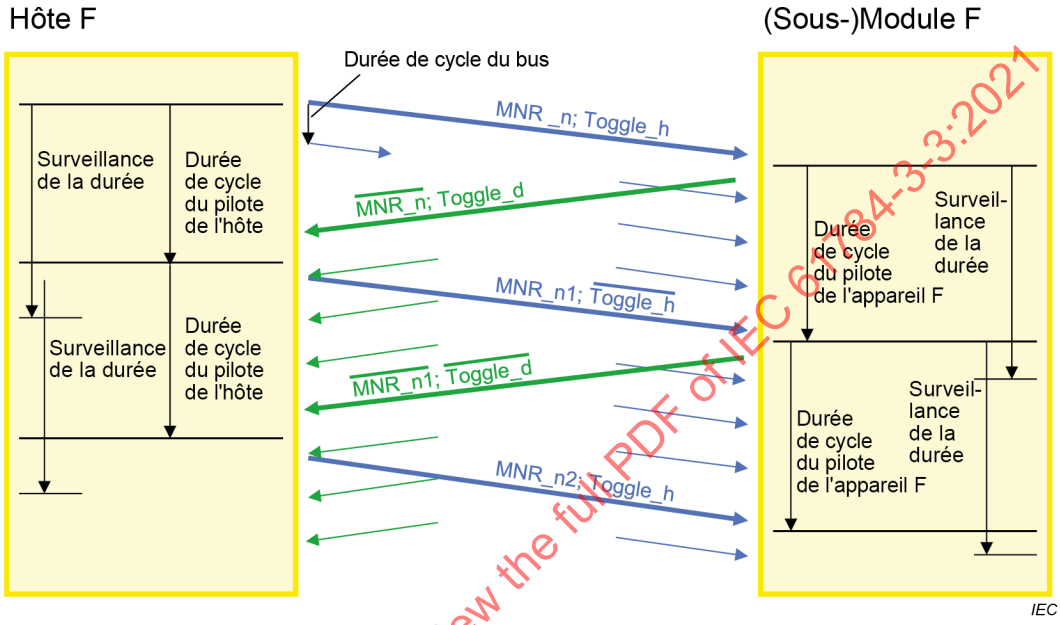


Figure 35 – Surveillance de la durée d'acheminement du message hôte F ↔ (Sous-)Module F

La Figure 35 représente le contrôle du temps dans l'hôte F et un (Sous-)Module F.

D'autres contraintes de temporisation sont présentées ci-dessous:

Démarrage (Synchronisation)	Pour procéder à une synchronisation après le démarrage d'un système, le pilote de l'hôte F démarre avec le MNR virtuel initial (voir 7.1.5 et 7.1.6).
Cycle de protocole F	Un pilote de l'appareil F renvoie un PDU de sécurité au pilote de l'hôte F avec le même MNR virtuel, mais complémentaire, afin d'acquitter la réception d'un PDU de sécurité.
Surveillance du temps de fonctionnement (Chien de garde)	L'arrivée d'un nouveau PDU de sécurité correct dans le pilote de l'appareil F dans le temps de fonctionnement du chien de garde est surveillée. Cette vérification peut être réalisée aussi souvent que nécessaire, mais au moins une fois à l'issue de l'intervalle de temps de surveillance (voir 9.3.3). A l'expiration du temps de fonctionnement du chien de garde, le destinataire associé initie la réaction aux anomalies.

Surveillance du MNR

Un nouveau PDU de sécurité correct se caractérise par le fait que le Toggle_Bit et le MNR virtuel au moins passent au MNR virtuel suivant et que tout le reste du PDU de sécurité n'a pas été modifié ou ne l'a pas été de manière erronée. Cela signifie qu'un changement incorrect du MNR virtuel est reconnu directement par CRC2. Cela se traduit alors par une réaction aux anomalies.

Répétition des PDU de sécurité

La répétition d'un PDU de sécurité complet n'est pas prise en charge si un nouveau PDU de sécurité correct n'a pas été reçu dans l'intervalle du temps de fonctionnement du chien de garde.

Appareil de surveillance SIL

Chaque message corrompu relatif à une relation de communication de sécurité détecté dans l'un des états 4, 7 ou 25 (CRC et anomalie du MRN virtuel) est compté pendant une période de temps de l'appareil de surveillance SIL configurable (T). Les valeurs Failsafe sont définies lorsque plusieurs anomalies de ce type se produisent. En d'autres termes, un message corrompu détecté peut être toléré (*variante A*). Ainsi, la préaffectation correspond à "un message corrompu" au démarrage du système. Les cas dans lesquels l'ensemble du SPDU du message = "0" (au démarrage, par exemple) ne doivent pas être comptés.

En réalité, il peut être démontré que le comptage reste effectivement toujours nul. Cela explique la nécessité d'optimiser la complexité donnant la *variante B*, où la période de temps (T) de l'appareil de surveillance SIL est infinie. Dans ce cas, le diagramme d'états simplifié de l'hôte F de la Figure 26 doit être pris en compte lorsque les PDU de sécurité corrompus détectés ne sont pas tolérés et donnent toujours lieu à un état de sécurité.

Chaque fois qu'un message corrompu est détecté de manière inattendue pendant la production ou l'exploitation, l'opérateur responsable joue le rôle d'appareil de surveillance SIL et peut tolérer et acquitter l'indication. Dans le cas d'indications fréquentes à plus d'une reprise par temps de l'appareil de surveillance SIL, il convient d'effectuer une vérification de l'installation (par exemple, brouillage électromagnétique), du volume de trafic de réseau ou de la qualité de transmission.

Il revient au fabricant de l'hôte F de mettre en œuvre la variante A. Toutefois, une réalisation détaillée n'est pas présentée ici afin de permettre des adaptations individuelles aux environnements système particuliers.

Période de temps de l'appareil de surveillance SIL (T)

La période de temps T de l'appareil de surveillance SIL est une valeur constante qui intègre la dimension horaire (h) qui résulte du SIL demandé et de la longueur CRC configurée (9.5.1). Le Tableau 14 spécifie les temps de l'appareil de surveillance SIL.

Tableau 14 – Temps de l'appareil de surveillance SIL

SIL	Période de temps (h) protocole LP	Période de temps (h) protocole XP
3	> 100	> 10
2	> 10	> 1

7.2.7.2 Temps de fonctionnement étendu du chien de garde à la demande après interaction de l'utilisateur

Pour les cas d'utilisation tels que les activités de maintenance comme la "Reconfiguration dynamique" [54] ou la "maintenance des systèmes de tolérance aux anomalies", un certain temps est nécessaire à la mise à jour des appareils concernés. En règle générale, ce temps de mise à jour est plus long que le temps de fonctionnement du chien de garde (principal) régulier (F_WD_Time) défini pour une application de sécurité. Afin d'éviter des déclenchements parasites, le pilote de l'hôte F peut utiliser uniquement une seule fois par activité de maintenance mentionnée (voir Figure 37) un temps de fonctionnement du chien de garde secondaire (F_WD_Time_2) pour étendre le temps de fonctionnement du chien de garde principal de ces cas représentés à la Figure 36.

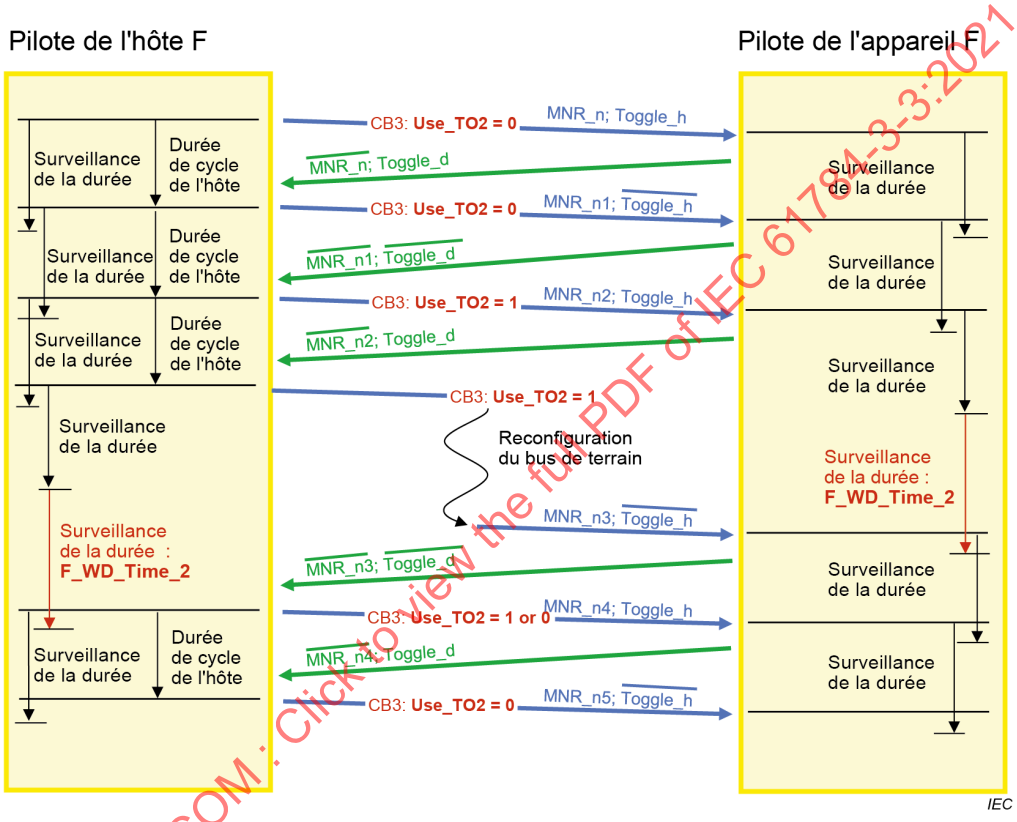


Figure 36 – Temps de fonctionnement étendu du chien de garde à la demande

L'hôte F doit définir et réinitialiser le bit 3 (Use_TO2) de l'octet de contrôle pour tous les pilotes de l'appareil F, affectant ainsi tous ces pilotes (voir 6.1).

7.3 Réaction en cas de dysfonctionnement

7.3.1 Corruption des données de sécurité

Explication: "Le dysfonctionnement d'un appareil de bus ou de la liaison de transmission perturbe les PDU de sécurité."

NOTE "Explication" fait référence aux dysfonctionnements correspondants dans l'article "erreurs de communication" de l'IEC 61784-3:2021.

Solution palliative: La signature CRC2 reconnaît une perturbation des données entre l'émetteur et le destinataire.

La signature CRC2 est générée par l'intermédiaire des paramètres F respectivement, des données d'entrée-sortie F, du MNR virtuel et de l'octet de contrôle/d'état (voir 7.1.7, 7.1.8, Figure 22 et Figure 24).

7.3.2 Répétition non prévue

Explication: "Le dysfonctionnement d'un appareil de bus génère d'anciens PDU de sécurité obsolètes répétés au moment inopportun, ce qui risque de gêner dangereusement le destinataire (l'appareil de sûreté est signalé comme étant fermé alors qu'il a déjà été ouvert, par exemple)."

Solution palliative: Les répétitions non prévues sont découvertes par une modification et un examen rigoureux du MNR et/ou du temps de fonctionnement du chien de garde du destinataire respectif (pilote de l'hôte F ou pilote de l'appareil F).

7.3.3 Séquence incorrecte

Explication: "Le dysfonctionnement d'un appareil de bus modifie la séquence du PDU de sécurité. Exemple: Avant de procéder à l'arrêt technique de sécurité, l'opérateur souhaite sélectionner la vitesse limitée de sécurité. Si ces PDU de sécurité ne sont pas clairs, la machine fonctionne au lieu de s'arrêter."

Solution palliative: En raison d'une attente d'un MNR rigoureusement séquentiel, le destinataire reconnaît une séquence incorrecte.

7.3.4 Perte

Explication: "Le dysfonctionnement d'un appareil de bus supprime un PDU de sécurité (demande d' "arrêt technique de sécurité", par exemple)."

Solution palliative: Les informations perdues seront découvertes par une modification et un examen rigoureux du MNR et/ou du temps de fonctionnement du chien de garde du destinataire respectif (pilote de l'hôte F ou pilote de l'appareil F).

7.3.5 Retard inacceptable

Explication: "1. Le volume d'échange de données opérationnelles dépasse la capacité de la liaison de communication. 2. Un appareil de bus provoque une situation de surcharge en simulant des PDU de sécurité incorrects, causant le retard ou l'empêchement d'un service appartenant au PDU de sécurité."

Solution palliative:

- le temps de fonctionnement du chien de garde du destinataire respectif (pilote de l'hôte F et/ou de l'appareil F) détecte le retard inacceptable d'un PDU de sécurité;
- le changement du bit de bascule de l'octet de contrôle et de l'octet d'état d'un SPDU avec le CRC2 correct entraîne une réinitialisation du temporisateur (voir 7.1.3).

Le temps de fonctionnement du chien de garde est défini en 9.3.3.

7.3.6 Insertion

Explication: "Le dysfonctionnement d'un appareil de bus insère un PDU de sécurité (désélection de l'"arrêt technique de sécurité", par exemple)."

Solution palliative: En raison de l'attente séquentielle et de l'"initialisation du nom de code" du MNR, le destinataire détecte un PDU de sécurité inséré.

7.3.7 Déguisement

Explication: "Le dysfonctionnement d'un appareil de bus provoque le mélange des PDU de sécurité, des PDU de sécurité mal acheminés et des PDU qui ne sont pas de sécurité."

Solution palliative: Le destinataire détecte ces PDU "de sécurité" des émetteurs avec une authenticité incorrecte par l'intermédiaire de la signature CRC2.

7.3.8 Adressage

Explication: "Le dysfonctionnement d'un bus provoque le mauvais acheminement d'un ou de plusieurs PDU de sécurité."

Principe d'authentification de connexion sécurisée:

La détection des données en provenance d'un autre émetteur ou destinées à un autre destinataire est assurée par le fait que l'émetteur respectif (l'hôte F ou le (Sous-)Module F) qui appartient à la relation source-destination F (nom de code) est le seul qui génère exactement la signature CRC2 correspondante attendue par le destinataire respectif (l'hôte F ou le (Sous-)Module F). Simultanément, le destinataire utilise cette signature CRC2 pour vérifier implicitement l'authenticité de la connexion étant donné que le nom de code et la direction sont inclus dans le CRC2 par le MRN (voir 7.1.7, 7.1.8 et 7.3.10).

Le nom de code ("F_S/D_Address") peut être soigneusement sélectionné dans les appareils individuels selon l'une des méthodes suivantes:

– codage du commutateur dans l'unité qui correspond au nom de code;
– un paramétrage unique d'appareil par un logiciel qui exige une vérification si le bon appareil a été adressé. L'opération doit être répétée lorsque cette unité est remplacée;
– mécanismes d'adressage indépendants de l'adressage CPF 3.

7.3.9 Hors séquence

Explication: Les commutateurs sont les éléments centraux des réseaux CP 3/4 à CP 3/6 et sont des composants de réseau actifs particulièrement complexes. Ils peuvent faire l'objet de différentes anomalies. Les messages peuvent être envoyés à la mauvaise destination ou leur contenu peut être perturbé. De plus, un commutateur peut envoyer perpétuellement des messages stockés, même lorsque l'émetteur a déjà été arrêté.

Les anomalies suivantes sont détectées/maîtrisées:

– l'hôte F est défaillant ou ses PDU de sécurité n'atteignent pas le récepteur. Un commutateur transmet les messages de sa mémoire tampon tournante sans le bon MNR. Le pilote de l'appareil F reconnaît une anomalie MNR et définit des valeurs Failsafe (FV);
– un seul message de la mémoire tampon de commutation est retransmis et comporte un PDU de sécurité avec le bon MNR. Cette anomalie est détectée à cause du MNR, et le pilote F commute vers des valeurs Failsafe (FV);
– un commutateur transmet les messages avec des PDU de sécurité depuis sa mémoire tampon tournante avec les bons MNR, la séquence de ce message commençant dans le temps de fonctionnement du chien de garde de sécurité. Cette anomalie est détectée à cause du MNR, et le retour aux valeurs de processus nécessite un acquittement de l'opérateur (OA_C = 1).

7.3.10 Bouclage

Explication: "La fonction d'acheminement programmable d'un appareil de bus réachemine de manière involontaire un message de l'hôte F vers ce même hôte, qui attend un PDU de sécurité de même longueur."

Solution palliative:

F_CRC_Seed =0: L'hôte F vérifie le bouclage par le bit 7 de l'octet d'état (voir Figure 17) et le pilote de l'appareil de sortie F détecte le bouclage par la temporisation;

F_CRC_Seed =1: Le calcul de la signature CRC2 de et vers l'hôte F utilise différents algorithmes MNR (élément complémentaire unique).

7.3.11 Limites du réseau et routeur

Explication: "1. Le volume d'échange de données opérationnelles dépasse la capacité de la liaison de communication. 2. Un appareil de bus provoque une situation de surcharge en simulant des messages incorrects, causant le retard ou l'empêchement d'un service appartenant au PDU de sécurité intrinsèque."

Pour les réseaux CP 3/4 à CP 3/6 équipés de routeurs, la Figure 9 et les explications correspondantes s'appliquent. Prendre pour hypothèse un système de ce type composé de sous-réseaux connectés par des routeurs pour les considérations ci-dessous. Ces considérations démontrent qu'une seule erreur n'est pas à l'origine de la transmission inappropriée d'un PDU de sécurité vers le mauvais pilote de l'appareil F, ni de son passage à un état dangereux.

Le routeur connecte deux sous-réseaux ou plus sur des niveaux de couche 3. Chaque hôte F et appareil d'entrée-sortie qui héberge des Sous-modules F peut être configuré pour "utiliser le routeur" avec une adresse de routeur appropriée. Le routeur gère les adresses IP des sous-réseaux connectés. Le Tableau 15 contient une liste des types d'anomalies et des contraintes liées à une opération de routeur pour obtenir un niveau de sécurité suffisant.

Tableau 15 – Limites du réseau de sécurité

Type d'anomalie	Conséquences	Détection et maîtrise
Le routeur ne détient pas la bonne adresse d'un appareil d'entrée-sortie qui héberge des Sous-modules F	Le routeur reçoit un message pour ce Sous-module F particulier. Résultat: cible introuvable.	Temporisation détectée par le pilote de l'appareil F lors de la vérification du SPDU
Deux appareils d'entrée-sortie qui hébergent des Sous-modules F avec des adresses et une structure de Sous-module identiques. L'un dans le sous-réseau 0, l'autre dans le sous-réseau 1 Contrainte: routeur à 2 ports (voir Figure 9)	1) Appareil d'entrée-sortie qui héberge des Sous-modules F du sous-réseau 0 correct dans le sous-réseau 0 2) Impossible d'atteindre l'appareil d'entrée-sortie qui héberge des Sous-modules F du sous-réseau 0 dans le sous-réseau 1 3) Impossible d'atteindre l'appareil d'entrée-sortie qui héberge des Sous-modules F du sous-réseau 1 dans le sous-réseau 0 4) Appareil d'entrée-sortie qui héberge des Sous-modules F du sous-réseau 1 correct dans le sous-réseau 1	Par CP 3/4 à CP 3/6 normalisé

7.4 Démarrage F et modification des paramètres lors de l'exécution

7.4.1 Procédure de démarrage normalisée

Le démarrage du pilote de l'appareil F est postérieur au démarrage défini pour CP 3/4 à CP 3/6. Le pilote de l'hôte F et le pilote de l'appareil F commencent d'eux-mêmes à chaque établissement de la communication CP 3/4 à CP 3/6. Les éléments déjà exécutés des couches de sécurité et leurs paramètres F spéciaux sont intégrés dans le processus d'établissement de la relation d'application et de paramétrage du démarrage ("Contexte") de CP 3/4 à CP 3/6. Toutes les répétitions des éléments du paramètre F qui portent des valeurs identiques lors de l'exécution (activate_FV_DC=0) doivent être ignorées et les valeurs qui s'écartent doivent être rejetées ou doivent générer un état de sécurité. Si les Sous-modules F sont branchés ou débranchés, alors le processus de reparamétrage CP 3/4 à CP 3/6 s'applique.

Voir l'IEC 61158-5-10 et l'IEC 61158-6-10 pour des informations relatives aux séquences de démarrage d'un contrôleur d'entrée-sortie et de ses appareils d'entrée-sortie.

8 Gestion de la couche de communication de sécurité

8.1 Paramètre F

8.1.1 Récapitulatif

Les valeurs de paramètre des appareils CP 3/4 à CP 3/6 sur le canal noir sont attribuées conformément au profil CP 3/4 à CP 3/6 normalisé, c'est-à-dire à l'aide de fichiers GSD qui reposent sur les langages de description GSD (voir [35] et [38]). De plus, les paramètres F exigés pour la couche de sécurité peuvent être chargés selon plusieurs options de paramétrage alternatives.

Tout changement involontaire du "Paramètre F en cours d'utilisation" pendant une communication FSCP 3/1 doit être détecté ou empêché par les mesures de sécurité génériques définies par le fournisseur.

"Paramètre F en cours d'utilisation" correspond aux valeurs de paramètre F utilisées pour la communication CPF 3. Cela signifie que le pilote du (Sous-)Module F est dans l'un des états 23 à 28.

Récapitulatif des paramètres F:

- F_S/D_Address — "Nom de code" entre l'émetteur et le destinataire
- F_WD_Time — Temps de fonctionnement du chien de garde dans le pilote F
- F_WD_Time_2 — Temps de fonctionnement du chien de garde secondaire dans les (Sous-)Modules F conçus pour la "Reconfiguration dynamique", la "maintenance des systèmes de tolérance aux anomalies" ou le "Paramétrage en cours". L'outil de développement calcule et définit la valeur (avec des réserves pour les sessions "DR" futures) lors de la mise en service (7.2.7.2)
- F_Prm_Flag1 + 2 — Octets du paramètre qui contiennent plusieurs paramètres de gestion de profil
  - F_Check_SeqNr — V2-mode: ignorer
  - F_Check_iPar — Utilisation spécifique au fabricant dans des systèmes homogènes
  - F_SIL — SIL configuré
  - F_CRC_Length — Longueur de signature CRC2
  - F_CRC_Seed — Utilisation de différentes règles pour la valeur de départ CRC et le MNR pour le calcul de la signature CRC2 (voir Figure 42)
  - F_Passivation — (Sous-)Module F ou Passivation granulaire des canaux [56]
  - F_Block_ID — Identification du type de blocage de paramètre
  - F_Par_Version — Numéro de version des paramètres F/du mode opérationnel FSCP 3/1
- F_iPar_CRC — Valeur du calcul de la signature CRC d'iParamètres, au moins manuellement transférée d'un outil CPD vers l'outil de développement
- F_Par_CRC — Calcul de la signature CRC des paramètres F afin de sécuriser le transfert entre l'hôte F et le pilote de l'appareil F

8.1.2 F_Source/Destination_Address (Nom de code)

Les noms de code soigneusement sélectionnés (stockés dans le (Sous-)Module F) des relations de communication de sécurité doivent être univoques dans les limites d'un sous-réseau, conformément à l'IETF RFC 917. Les sous-réseaux sont interconnectés par l'intermédiaire de routeurs (à 2 ports), qui sont les limites naturelles de CP 3/4 à CP 3/6, où RT_CLASS_UDP n'est pas admis ou pas pris en charge (5.4.2). En local, chaque (Sous-)Module F contient la relation source-destination configurée de la liaison de communication de sécurité avec son partenaire ("F_Source/Destination_Address" ou "F_S/D_Address" abrégée). La relation fait partie intégrante de l'ensemble de paramètres F et, par conséquent, le pilote de l'appareil F compare les paramètres F_S/D_Address aux noms de code soigneusement sélectionnés. Les paramètres F_S/D_Address sont des désignations d'adresse logique qui peuvent être attribuées *librement*, mais de manière *univoque*. En règle générale, elles sont représentées à partir du pilote de l'hôte F (comme source) et du pilote de l'appareil F (comme destination) pendant la configuration de développement (7.3.7). Les adresses *0* et *0xFFFF* doivent être *exclues*.

Le paramètre est composé de deux parties: "F_Source_Add" et "F_Dest_Add", chacune appartenant au type de données Unsigned16. Tableau 16 spécifie l'ordre des octets du nom de code (F_Source/Destination_Address).

Tableau 16 – Ordre des octets de nom de code

Nom de code			
Octet de poids fort	octet	octet	Octet de poids faible
F_Source_Address		**F_Dest_Address**	
Octet de poids fort	Octet de poids faible	Octet de poids fort	Octet de poids faible

8.1.3 F_WD_Time (temps de fonctionnement du chien de garde F)

En local, chaque pilote de l'appareil F et son homologue, le pilote de l'hôte F, gèrent un temps de fonctionnement du chien de garde F configuré pour chaque relation source-destination. Le pilote F démarre ce temporisateur à chaque envoi d'un PDU de sécurité avec un nouveau MNR.

Ce paramètre F_WD_Time est codé comme suit: Unsigned16. Base de temps: *1 ms*. La plage de valeurs est comprise entre 1 et 65 535.

Voir 9.3.3 pour plus d'informations sur la manière dont ces temps de fonctionnement du chien de garde s'intègrent dans l'ensemble de la définition des temps de réponse de la fonction de sécurité (SFRT) et sur la façon dont ils peuvent être déterminés.

Le fabricant d'un (Sous-)Module F attribue le temps maximal d'acquittement de l'appareil (DAT) à la valeur par défaut du paramètre F_WD_Time dans le fichier GSD. Un outil de développement est alors en mesure de proposer le F_WD_Time nécessaire à cette relation de communication 1:1 entre le pilote de l'hôte F et le pilote de l'appareil F.

NOTE L'outil de développement est alors en mesure de calculer les temps de réaction de la fonction de sécurité à condition de disposer de toutes les autres valeurs. Voir 9.3.2.

8.1.4 F_WD_Time_2 (temps de fonctionnement du chien de garde F secondaire)

Ce paramètre F peut être éventuellement utilisé pour étendre le F_WD_Time régulier d'un temps de fonctionnement F_WD_Time_2 supplémentaire par le bit 3 de l'octet de contrôle, comme démontré à la Figure 37 (MNR "n5"). Ce temps de fonctionnement supplémentaire est exigé pour la mise à jour de la configuration de l'hôte et/ou des appareils, par exemple le temps de basculer d'une AR à l'autre dans un ensemble d'AR.

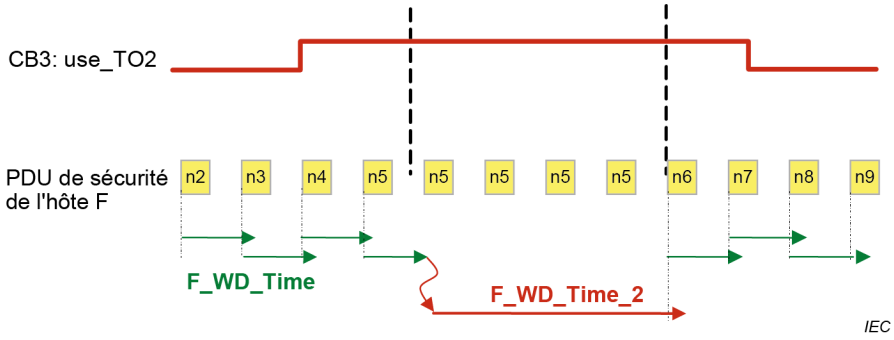


Figure 37 – Effet de F_WD_Time_2

Le paramètre F_WD_Time_2 est codé comme suit: Unsigned16. Base de temps: *1 ms*. La plage de valeurs est comprise entre 1 et 65 535. CB3 = 1 ("use_TO2") est un indicateur destiné au pilote d'appareil F pour l'activation du temps de fonctionnement F_WD_Time_2 une seule fois. Le temps de fonctionnement F_WD_Time normal démarre immédiatement après la réception du PDU de sécurité suivant avec un nouveau MNR. Préalablement à un redémarrage du temps de fonctionnement F_WD_Time_2, l'hôte F doit réinitialiser CB3.

8.1.5 F_Prm_Flag1 (Paramètres de gestion de la couche de sécurité)

8.1.5.1 Structure de F_Prm_Flag1

Les paragraphes 8.1.5.2 à 8.1.5.5 décrivent les caractéristiques de l'octet du paramètre F_Prm_Flag1. Sa structure est représentée à la Figure 38:

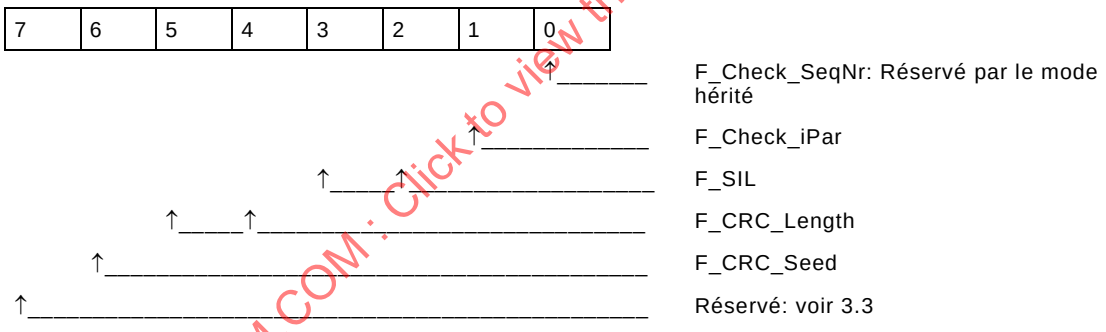


Figure 38 – F_Prm_Flag1

8.1.5.2 F_Check_SeqNr

Ce paramètre est réservé si hérité du mode V1, ignoré en mode V2.

8.1.5.3 F_Check_iPar

La valeur "0" doit toujours être attribuée à ce paramètre spécifique au fournisseur dans le cas d'une utilisation normale. Ce paramètre est réservé au fabricant dans les systèmes homogènes. Il n'est pas lié au mécanisme de serveur d'iParamètres.

Il est codé comme suit: Bit 1 de l'octet de paramètre "F_Prm_Flag1" (voir Figure 39).

7	6	5	4	3	2	1	0		
						0		=	Pas de vérification (la notation dans GSD doit être "NoCheck")
						1		=	Vérification (utilisation spécifique au fabricant; la notation dans GSD doit être "Check")

Figure 39 – F_Check_iPar

8.1.5.4 F_SIL(phase SIL)

Les différentes fonctions de sécurité qui utilisent la communication de sécurité peuvent exiger différents niveaux d'intégrité de sécurité (SIL 1 à SIL 3). Les (Sous-)Modules F sont capables de comparer le SIL qui leur a été attribué au SIL configuré (F_SIL). Si le niveau d'intégrité de sécurité est supérieur à celui du (Sous-)Module F connecté, une valeur est attribuée au bit d'état de la "défaillance de l'appareil", ce qui déclenche une réaction d'état de sécurité. Il existe quatre phases différentes: SIL 1 à SIL 3, NoSIL (voir Figure 40).

Il est codé comme suit: Bits 2 et 3 de l'octet de paramètre "F_Prm_Flag1".

7	6	5	4	3	2	1	0		
				0	0			=	SIL 1 (la notation dans GSD doit être "SIL1")
				0	1			=	SIL 2 (la notation dans GSD doit être "SIL2")
				1	0			=	SIL 3 (la notation dans GSD doit être "SIL3")
				1	1			=	Pas de SIL (la notation dans GSD doit être "NoSIL"): dans les appareils d'automatisme industriel, par exemple

Figure 40 – F_SIL

8.1.5.5 F_CRC_Length (longueur de la signature CRC2)

Selon le paramètre F_CRC_Seed, une signature CRC2 de 3 ou 4 octets est exigée (voir Figure 41). Ce paramètre transfère la longueur prévue de la signature CRC2 dans le PDU de sécurité vers le pilote de l'appareil F pendant le démarrage.

Il est codé comme suit: Bits 4 et 5 de l'octet de paramètre "F_Prm_Flag1".

7	6	5	4	3	2	1	0		
		0	0					=	Signature CRC2 à 3 octets; la notation dans GSD doit être "3-Byte-CRC")
		0	1					=	Héritage: Cette attribution de paramètre ne doit pas être utilisée pour les nouveaux développements
		1	0					=	Signature CRC2 à 4 octets; la notation dans GSD doit être "4-Byte-CRC")
		1	1					=	Réservé

Figure 41 – F_CRC_Length

8.1.5.6 F_CRC_Seed (valeur de départ pour CRC2)

Avec F_CRC_Seed =0, le pilote de l'appareil F doit utiliser CRC_FP (16 bits) comme valeur de départ et un compteur en tant que MNR pour une intégration dans le calcul de la signature CRC2 (voir 7.1.5 et 7.1.7) selon les versions de protocole précédentes.

Avec F_CRC_Seed =1, le pilote de l'appareil F doit utiliser la valeur "1" comme valeur de départ, le protocole CRC-FP+, et le MonitoringNumber virtuel établi sur le nom de code pour une intégration dans le calcul de la signature CRC2 (voir 7.1.6 et 7.1.8).

L'outil de développement d'un hôte F ajuste son pilote selon cette entrée. Le paramètre est distribué au pilote de l'appareil F au cours du démarrage.

Il est codé comme suit (voir Figure 42): Bit 6 de l'octet de paramètre "F_Prm_Flag1".

7	6	5	4	3	2	1	0

0 = CRC-FP en tant que valeur de départ et compteur (la notation dans GSD est "CRC-Seed16")

1 = "1" en tant que valeur de départ et CRC-FP+/MNR (la notation dans GSD est "CRC-Seed24/32")

Figure 42 – F_CRC_Seed

Le Tableau 17 indique les combinaisons admises de F_CRC_Seed et de F_Passivation.

Tableau 17 – Combinaisons admises de F_CRC_Seed et de F_Passivation

F_CRC_Seed	F_Passivation	
0	1	Non admise
1	0 / 1	Admise

8.1.6 F_Prm_Flag2 (Paramètres de gestion de la couche de sécurité)

8.1.6.1 Structure de F_Prm_Flag2

Le 8.1.6.3 et le 8.1.6.4 décrivent les caractéristiques de l'octet du paramètre F_Prm_Flag2. Sa structure est représentée à la Figure 43.

7	6	5	4	3	2	1	0

↑_____ F_Passivation

↑_____ Réservé: voir 3.3

↑_____ Réservé: voir 3.3

↑_____↑_____↑_____ F_Block_ID

↑_____↑_____ F_Par_Version

Figure 43 – F_Prm_Flag2

8.1.6.2 F_Passivation

Les indications données en 6.1 et à la Figure 14 décrivent le concept de Passivation granulaire des canaux (CGP) par opposition à la passivation complète des (Sous-)Modules F. Un outil de développement de l'hôte F définit ce paramètre sur "0" lorsqu'un hôte F ne prend pas en charge la CGP (voir Figure 44). Un (Sous-)Module F qui prend en charge la CGP doit vérifier ce paramètre "F_Passivation". Un (Sous-)Module F qui ne prend pas en charge la CGP doit réagir en cas de F_Passivation =1 avec "La version de l'ensemble de paramètres F est incorrecte".

7	6	5	4	3	2	1	0		
							0	=	Passivation du (Sous-)Module F du fait de "Device_Fault" (la notation dans GSD doit être "Device/Module")
							1	=	Passivation granulaire des canaux (CGP) du fait d'anomalies de canal de signalisation individuel en utilisant le modèle de qualificatif de [56] (la notation dans GSD doit être "Channel")

Figure 44 – F_Passivation

8.1.6.3 F_Block_ID (identification du type de paramètres)

Pour distinguer les paramètres des modes FSCP 3/1 ultérieurs, l'identification du type de paramètre "F_Block_ID" est codée de la manière suivante: Bits 3, 4 et 5 de l'octet de paramètre "F_Prm_Flag2" (voir Figure 45). Il est obligatoire pour permettre à la couche de sécurité de vérifier F_Block_ID.

7	6	5	4	3	2	1	0		
		0	0	0				=	No F_WD_Time_2, no F_iPar_CRC
		x	x	1				=	F_iPar_CRC
		x	1	x				=	F_WD_Time_2
		1	x	x				=	Réservé

Figure 45 – F_Block_ID

8.1.6.4 F_Par_Version (numéro de version de l'ensemble de paramètres F)

Ce compteur de versions a pour objet d'identifier les versions d'un mode opérationnel à l'intérieur du pilote de l'appareil F. Le pilote de l'appareil F doit répondre par un message de diagnostic spécifique dans le cas où la version demandée de la couche de sécurité ne correspond pas à celle mise en œuvre (voir 6.3.2 et Figure 46). Le contrôle de validité des paramètres F doit être réalisé par le pilote de l'appareil F.

7	6	5	4	3	2	1	0		
0	0							=	Mode V1 hérité, qui ne doit pas être utilisé pour de nouvelles mises en œuvre (la notation dans GSD doit être "V1-mode")
0	1							=	Valide pour le mode V2 (la notation dans GSD doit être "V2-mode")
1	0							=	Réservé
1	1							=	Réservé

Figure 46 – F_Par_Version

8.1.7 F_iPar_CRC (valeur d'iPar_CRC dans les iParamètres)

L'outil CPD d'un (Sous-)Module F particulier calcule une signature CRC (iPar_CRC) dans tous les iParamètres lorsque la session de paramétrage et de mise en service a abouti. Si le résultat du calcul est "0", la valeur doit être définie sur "1". La valeur de départ CRC recommandée pour ce calcul est "1". La valeur au format *hexadécimal* doit être transférée au moins manuellement à l'outil de développement et attribuée au champ d'entrée "F_iPar_CRC".

Ce paramètre est transmis au (Sous-)Module F lors du démarrage et est utilisé dans le cadre d'un contrôle de cohérence iParamètre dans le (Sous-)Module F avant de commencer une opération de sécurité normale. En "mode d'essai FSCP" (8.6.4.5) d'un (Sous-)Module F, la valeur "0" doit être attribuée à ce paramètre. Dans ce cas, le (Sous-)Module F ignore le contrôle de cohérence. Chaque fois que le (Sous-)Module F reconnaît une discordance entre la signature iPar_CRC calculée en local et la valeur de F_iPar_CRC, il doit définir des valeurs Failsafe (FV).

Ce paramètre est facultatif. Le bit 3 du paramètre F "F_Prm_Flag2" indique sa présence. Il est codé comme suit: Unsigned32

8.1.8 Calcul de F_Par_CRC (dans les paramètres F)

L'outil de développement génère cette signature CRC dans les paramètres F. La valeur de départ pour cette signature CRC est "0". Exception à la règle générale: Si le résultat du calcul est "0" et le paramètre F F_CRC_Seed =0, la signature CRC reste "0". Voir 8.3.3.2 pour plus d'informations sur l'ordre des paramètres F qui doivent être utilisés pour générer cette signature CRC. Le polynôme générateur CRC 16 bits (*0x4EAB*) est utilisé.

Il est codé comme suit: Unsigned16.

8.1.9 Structure de l'objet de données d'enregistrement du paramètre F

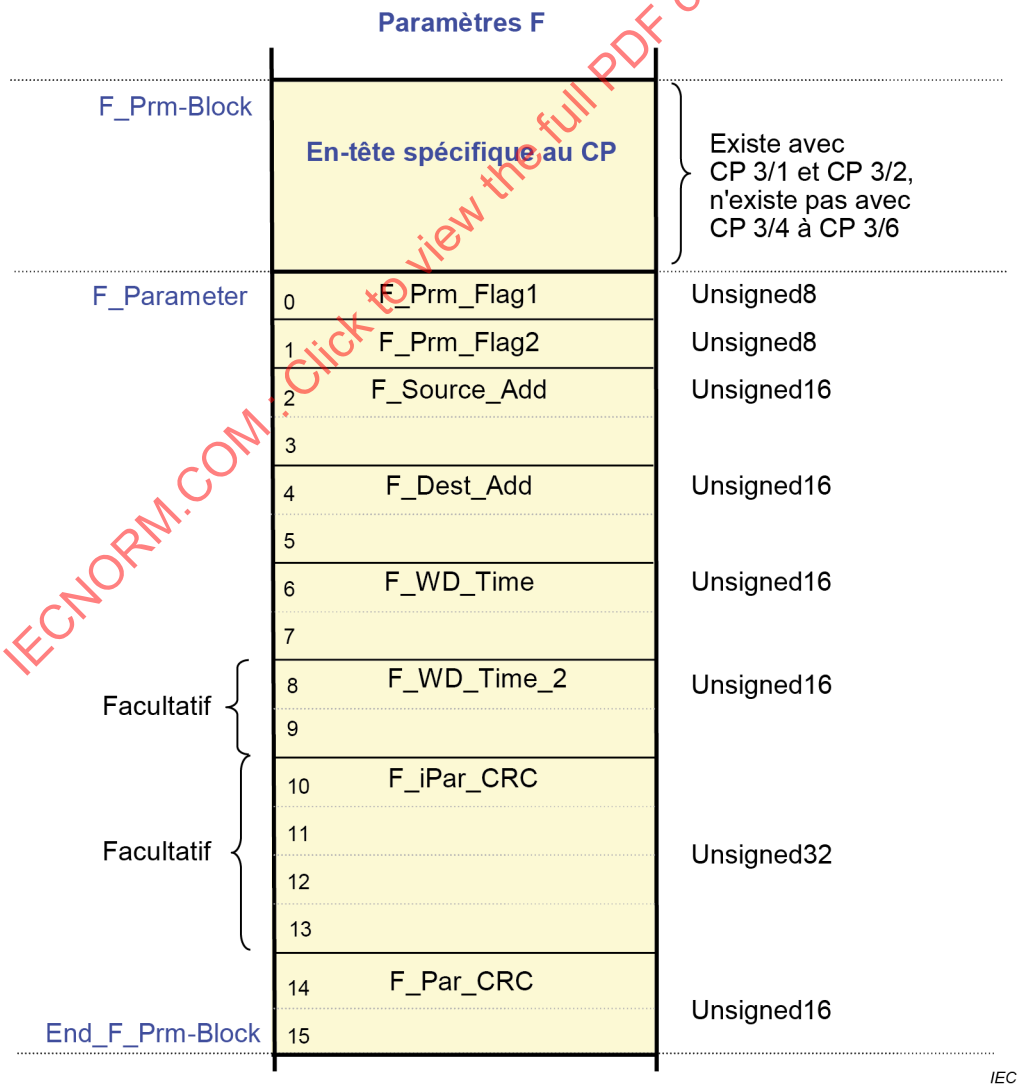


Figure 47 – Paramètre F

La Figure 47 représente la structure du bloc de paramètres F pour les (Sous-)Modules F. L'ordre des octets est conforme au protocole CPF 3. Pour CP 3/4 à CP 3/6, le bloc de paramètres F est attribué au sous-module F par le numéro de sous-intervalle.

8.2 iParamètre et iPar_CRC

Les (Sous-)Modules F présentent de plus en plus de fonctions intelligentes qui exigent l'attribution de nombreuses valeurs de paramètre individuelles. Ces paramètres relatifs à la sécurité sont appelés iParamètres. Ces (Sous-)Modules F peuvent nécessiter des paramètres supplémentaires qui ne sont pas fournis par le maître/contrôleur d'entrée-sortie. En particulier, si un appareil est remplacé, il est opportun de charger ces paramètres par le biais du bus directement par la voie normale. En règle générale, ces enregistrements de paramètre dépassent l'éventail de données de paramétrage qui repose sur la GSD (plusieurs lecteurs laser qui disposent d'environ 1 Ko par zone de protection peuvent générer une quantité de données globale de *90 kB*, voire plus). Par conséquent, cette spécification FSCP 3/1 fournit des mécanismes supplémentaires.

La Figure 48 représente une proposition de structure de grandes quantités d'iParamètres aux fins de téléchargement amont et aval des données. La limite supérieure absolue des iParamètres est de 2^{22}-1 octets, la limite inférieure étant de 4 octets. Par conséquent, une segmentation est exigée avec CP 3/1 lorsque le total dépasse 240 octets, comme représenté à la Figure 48. Aucune segmentation n'est exigée avec CP 3/4 à CP 3/6.

La signature CRC ("iPar_CRC") doit être calculée dans les iParamètres (Figure 48) à l'aide d'un polynôme CRC approprié, et intégrée dans l'iPar_CRC à 4 octets au format hexadécimal, puis affichée dans l'outil CPD. Si le résultat du calcul est "0", la valeur doit être définie sur "1". La valeur de départ CRC recommandée pour ce calcul est "1". L'introduction de la valeur iPar_CRC dans les iParamètres comme représenté à la Figure 48 est facultative. Aucune preuve de sécurité du taux d'erreurs résiduelles suffisant n'est exigée lors de l'utilisation du polynôme CRC à 32 bits FSCP 3/1.

La relation F_Source/Destination (nom de code) permet de vérifier la remise au destinataire configuré. L'introduction dans les iParamètres comme représenté à la Figure 48 est facultative.

Les fonctions d'identification et de maintenance (I&M) sont obligatoires pour tous les appareils CPF 3. Elles fournissent des codes qui permettent d'identifier le type et la version d'un (Sous-)Module particulier. L'introduction de ce type d'informations dans l'ensemble d'iParamètres peut être utilisée pour vérifier la validité d'un appareil de remplacement avec ses propres fonctions I&M. L'introduction dans les iParamètres comme représenté à la Figure 48 est facultative. Les fabricants d'appareils peuvent utiliser leurs codages personnels.

La longueur du bloc iParamètre peut être utile à l'organisation efficace des processus de téléchargement amont et aval des données dans les appareils. L'introduction dans les iParamètres comme représenté à la Figure 48 est facultative.

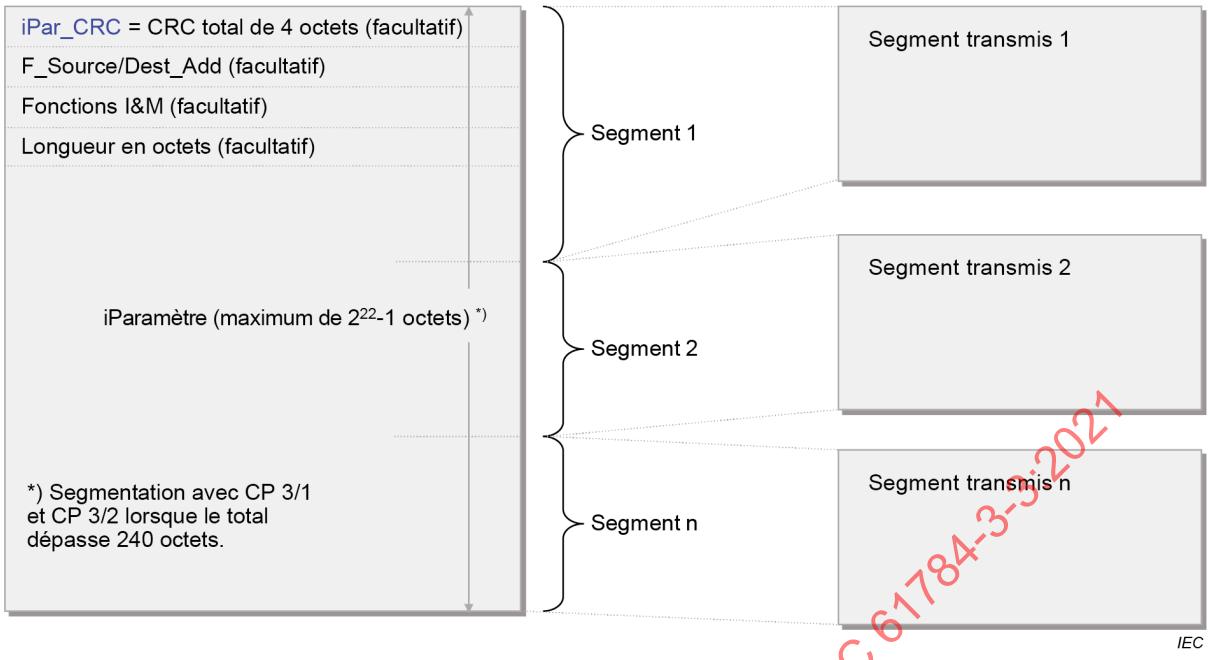


Figure 48 – Bloc iParamètre

Voir 8.6 pour plus d'informations sur la gestion de plusieurs segments iParamètre.

8.3 Paramétrage de sécurité

8.3.1 Objectifs

FSCP 3/1 fournit des méthodes proportionnées pour la fourniture de paramètres F et iParamètres des (Sous-)Modules F en raison des nombreuses manipulations des appareils de terrain dans les industries de fabrication et de transformation. L'un des principaux objectifs consiste à maintenir la stabilité d'un petit ensemble défini de paramètres F (niveau de communication) entre tous les (Sous-)Modules F et à fournir des interfaces d'iParamétrage afin de réduire le plus possible la dépendance entre le fabricant du système et celui de l'appareil, et donc à clairement définir les responsabilités.

Le fournisseur du (Sous-)Module F assume la responsabilité de l'intégrité (intégrité, authenticité et opportunité des données) de l'iParamètre.

Pour toute quantité d'iParamètres, un bloc de fonctions proxy normalisé, le "Serveur d'iParamètres", est spécifié dans le présent document. Le fabricant du système de l'hôte F prend la responsabilité du serveur d'iParamètres et propose cette fonction soit dans une bibliothèque de blocs de fonctions normalisée, soit sous la forme d'une fonction intégrée. Le concept de serveur d'iParamètres est spécifié en 8.6.4.

Le petit ensemble de paramètres F identiques des différents (Sous-)Modules F a été délaissé en faveur d'un outil de développement par GSD, ce qui offre ainsi une interface d'application constante et simple.

Après l'ajustement des paramètres F à la suite de la configuration de réseau, un enregistrement de paramètres F est compilé et stocké dans l'hôte F et le maître/contrôleur d'entrée-sortie pour le démarrage du système d'automatisation.

Le paramètre F "F_IO_StructureDescCRC" permet de s'assurer que le programme d'application F utilise correctement la structure des données d'entrée-sortie F et les types de données et n'est donc pas transféré vers le (Sous-)Module F lors du démarrage.

8.3.2 Extensions de sécurité GSDL et GSDML

8.3.2.1 CP 3/1 et CP 3/2: Extensions GSDL

FSCP 3/1 utilise la structure d'appareils définie par CP 3. Les appareils CP 3/1 ou CP 3/2 sont structurés à l'aide de modules placés dans des intervalles. Tous les paramètres sont définis pour les modules et leur sont attribués. Par conséquent, la spécification du langage de description générale de station (General Station Description Language ou GSDL) [35] pour le type 3 défini dans l'IEC 61158 définit les mots clés qui visent à structurer et identifier les informations de bloc de paramètres F des modules F représentés à la Figure 47. Les sélections de valeurs possibles du paramètre F se trouvent dans un fichier de description générale de station (GSD) associé à un esclave qui héberge les modules F pour lesquels il est conçu. Les mots clés ci-dessous du Tableau 18 sont définis.

Tableau 18 – Mots clés GSDL des paramètres F et des structures d'entrée-sortie F

Mot clé GSDL	Description
F_Ext_Module_Prm_Data_Len	Le paramètre associé à ce mot clé indique la longueur totale du bloc F_Prm représenté à la Figure 47.
F_Ext_Module_Prm_Data_Const (décalage)	A l'aide du paramètre associé à ce mot clé, une valeur fixe peut être entrée dans l'un des 4 octets d'en-tête du bloc F_Prm représenté à la Figure 47. La position d'un octet est indiquée par un décalage 0…3.
F_Ext_Module_Prm_Data_Const (0)	Indique la longueur F_Prm_Block qui inclut le F_iPar_CRC (0x12, par exemple).
F_Ext_Module_Prm_Data_Const (1)	Identification du bloc F_Prm = 5 (fixe).
F_Ext_Module_Prm_Data_Const (2)	Intervalle du module F.
F_Ext_Module_Prm_Data_Const (3)	Réservé. Doit être défini sur 0.
F_Ext_Module_Prm_Data_Ref (décalage)	A l'aide du paramètre associé à ce mot clé, une valeur sélectionnable par l'utilisateur au moment de la configuration peut être entrée dans l'un des octets 0 à 13 du bloc F_Prm représenté à la Figure 47. La position d'un octet est indiquée par un décalage 4 à 16. Le paramètre pointe vers une définition de plage ExtUserPrmData dans les autres parties du fichier GSD.
F_ParamDescCRC	Le paramètre associé à ce mot clé protège les parties relatives à la sécurité des descriptions du paramètre F dans le fichier GSD. Voir 8.3.3.3 pour plus d'informations sur la manière de déterminer cette signature CRC0.
F_IO_StructureDescCRC	Le paramètre associé à ce mot clé protège la description de la structure de données d'entrée-sortie F (valeurs de processus transférées de manière cyclique). Voir [35] et 8.4.2 pour plus d'informations sur la manière de déterminer cette signature F_IO_StructureDescCRC.
F_IO_StructureDescVersion	Le paramètre associé à ce mot clé indique la version d'une description de la structure de données d'entrée-sortie F. Une valeur de 1 indique une signature F_IO_StructureDescCRC de 16 bits, tandis qu'une valeur de 2 indique une signature F_IO_StructureDescCRC de 32 bits. Si cet attribut est absent, la valeur 1 est admise par hypothèse

Il est recommandé d'utiliser un paramétrage structuré. Voir 8.6.4.6 pour d'autres extensions GSDL.

8.3.2.2 CP 3/4 à CP 3/6: Extensions GSDML

FSCP 3/1 utilise la structure d'appareils définie par CP 3. Les appareils CP 3/4 à CP 3/6 sont structurés à l'aide de modules et de sous-modules placés dans des intervalles et des sous-intervalles. Tous les paramètres sont définis pour les sous-modules et leur sont attribués. Les paramètres F d'un (Sous-)Module F particulier sont définis à l'aide de son fichier GSD. La description est fournie en langage de balisage de description générale de station (GSDML) pour le type 10 défini dans l'IEC 61158, fondé sur le langage XML (voir [38]).

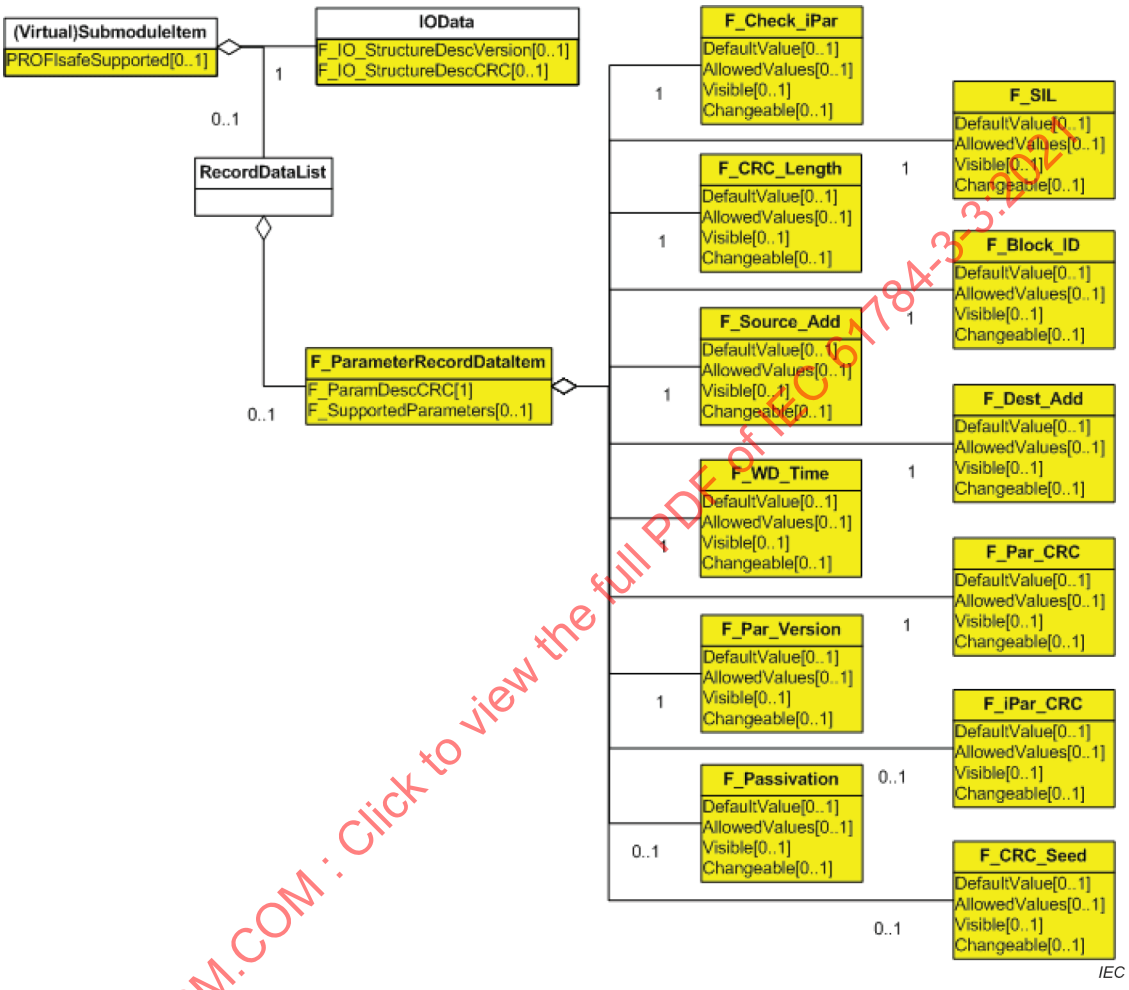


Figure 49 – Extension du paramètre F dans la spécification GSDML

La Figure 49 représente les extensions en langage GSDML. L'élément "(Virtual)SubmoduleItem" fournit les attributs suivants:

- "F_ParamDescCRC": Il s'agit de la signature CRC (CRC0) de la description du paramètre F selon la Figure 49;
- "F_SupportedParameters": Indication directe des paramètres F facultatifs pris en charge dans l'enregistrement de ces mêmes paramètres (information décodée de "F_Block_ID"). Pour plus d'informations, voir [38].

Le "F_IO_StructureDescCRC" de l'élément "IOData" protège les formats des données d'entrée F et de sortie F. La "F_IO_StructureDescVersion" indique la version d'une description de la structure de données d'entrée-sortie F (voir 8.3.3).

Dans le langage GSDML, les paramètres F F_CRC_Seed et F_Passivation sont facultatifs. Les deux paramètres doivent être présents ou aucun de ces deux paramètres ne doit être présent. Leur présence indique la prise en charge du protocole FSCP 3/1 conformément au présent document. Pour empêcher l'interruption des outils de développement par la présence des nouveaux paramètres F, intégrer l'attribut RequiredSchemaVersion= "V2.32" (V2.34/V2.35 recommandé) à la description du Sous-module F.

En cas de rétrocompatibilité avec les versions précédentes du protocole FSCP 3/1, un Sous-module F doit être décrit une seconde fois dans le fichier GSD, sans F_CRC_Seed et F_Passivation, mais avec F_CRC_Length=3-Byte-CRC à la place de 4-Byte-CRC.

Les Sous-modules F qui prennent en charge les deux paramétrages de F_Passivation exigent également des ensembles séparés de descriptions dans le fichier GSD en raison des différents formats de données d'entrée-sortie avec ou sans qualificatifs.

8.3.3 Protection des paramètres de sécurité et des données GSD

8.3.3.1 Généralités

Il est essentiel pour la sécurité du système de protéger les paramètres de sécurité de la couche de sécurité (paramètres F) et pour le (Sous-)Module F (iParamètres), ainsi que les structures de données d'entrée-sortie de sécurité choisies. Cette protection est assurée par les signatures CRC, leur stockage définitif dans le (Sous-)Module F et l'hôte F et une comparaison régulière des signatures CRC.

Pour éviter que l'outil de développement n'utilise des données de description d'appareil perturbées (GSD), les parties relatives à la sécurité qui le composent sont également protégées par signature CRC.

8.3.3.2 F_Par_CRC et iPar_CRC dans les paramètres de sécurité

La Figure 21 représente uniquement la signature CRC1 des paramètres F qui doivent être concernés par le processus de génération de signature CRC2. Toutefois, d'autres signatures CRC peuvent éventuellement être concernées, comme indiqué ci-après en 8.3.3.2.

Pour protéger les paramètres F, l'outil technique de l'hôte F génère la signature *F_Par_CRC* comme décrit en 8.1.7. Le polynôme CRC qui doit être utilisé est *0x4EAB*. La signature CRC est conçue dans tous les paramètres F dans l'ordre des octets indiqué à la Figure 47, à l'exclusion du F_iPar_CRC facultatif. Chaque fois que la valeur "1" est attribuée au bit 3 du paramètre F "F_Block_ID", la signature F_iPar_CRC doit être placée au début du calcul, comme représenté à la Figure 50.

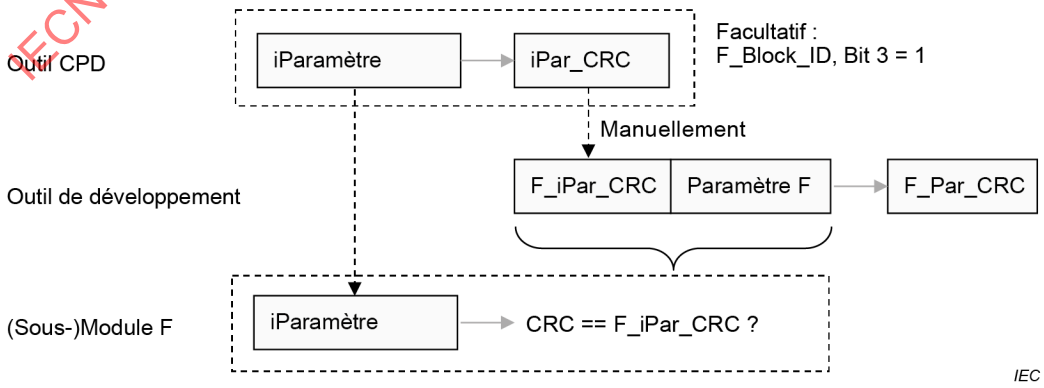


Figure 50 – Signature F_Par_CRC incluant iPar_CRC

Cette procédure doit également être utilisée pour le calcul de CRC_FP (voir 7.1.7) et de CRC_FP+ (voir 7.1.6).

8.3.3.3 CRC0 dans les données GSD

Pour s'assurer que les paramètres relatifs à la sécurité du (Sous-)Module F ne changent pas de manière inaperçue au cours du cycle de vie d'un support de stockage et peuvent être lus en toute sécurité dans l'outil de développement, ces paramètres sont tous protégés par signature CRC. Le paramètre "F_ParamDescCRC" contient une signature CRC à 2 octets (CRC0) générée à l'aide du même polynôme CRC 16 bits (0x4EAB) que celui utilisé avec l'ensemble du protocole FSCP 3/1. Le Tableau 19 décrit l'algorithme de sérialisation et de calcul.

Tableau 19 – Algorithme de génération de CRC0

1	Trier les paramètres F par ordre croissant et par décalage d'octet et de bit (tels qu'ils apparaissent dans l'enregistrement des paramètres F représenté à la Figure 47).
2	Pour chaque paramètre F visible énuméré, sérialiser: a) le nom du paramètre F b) un octet pour le type de données (0 = Bit/BitArea, 1 = Unsigned8, 2 = Unsigned16, 3 = Unsigned32) c) un octet pour le décalage de bits dans l'octet (0-7 pour le type de données Bit/BitArea, 0 pour les autres types de données) d) la valeur par défaut e) la ou les valeurs admises.
3	Il existe deux méthodes de sérialisation des valeurs admises: sous forme d'une plage de valeurs, ou sous forme d'une énumération. a) Une plage de valeurs ne contient que des valeurs. Elle est sérialisée sous la forme d'une valeur minimale et d'une valeur maximale. Lorsqu'il n'existe qu'une seule valeur admise, cette valeur est utilisée à la fois pour la valeur minimale et la valeur maximale. Cette forme est utilisée pour les paramètres F composés uniquement de valeurs numériques (par exemple, F_Source_Add), et elle est également utilisée pour les paramètres F qui comportent des noms normalisés en plus de leur valeur numérique, lorsqu'il n'existe qu'une seule valeur admise. b) Une énumération comprend des paires composées d'un nom et de sa valeur associée, triées par valeur croissante. Cette forme est utilisée pour les paramètres F qui comportent des noms normalisés en plus de leur valeur numérique (par exemple, F_SIL), lorsqu'il existe plusieurs valeurs admises.
4	Les règles suivantes doivent être prises en considération pour les chaînes et les valeurs numériques soumises à sérialisation: a) Les chaînes (noms) sont sérialisées caractère par caractère au moyen de leur code ASCII. La sérialisation ne concerne ni une longueur de chaîne, ni un caractère nul d'extrémité. b) Les valeurs numériques sont sérialisées dans un ordre d'octets petit-boutiste (octet de poids faible en premier). Les valeurs de type Bit/BitArea, Unsigned8, et Unsigned16 sont sérialisées sous forme d'entier non signé 16 bits, tandis que les valeurs de type Unsigned32 sont sérialisées sous forme d'entier non signé 32 bits.
5	Calculer le CRC à 2 octets parmi le flux d'octets au moyen du polynôme CRC *0x4EAB*.

Dans le cas d'un fichier GSD dédié à un esclave F (CP 3/1 ou CP 3/2), les règles d'annotation GSDL suivantes s'appliquent pour le calcul de la signature CRC0 (voir l'exemple du Tableau 20 et du Tableau 22):

- si un paramètre F non inclus dans l'ensemble F_Check_SeqNr, F_Check_iPar, F_CRC_Length, F_CRC_Seed, F_Passivation, F_Block_ID est omis dans le fichier GSD, une valeur fixe nulle est admise par hypothèse et ce paramètre ne doit pas être inclus dans le calcul de CRC0;
- les mots clés F_Ext_User_Prm_Data_Const doivent être ignorés;
- dans le cas où les paramètres F sont décrits sous une forme de structure de bloc (voir les mots clés Prm_Block_Structure_supp / ..._req), les mots clés F_Ext_User_Prm_Data_Ref dirigés vers l'en-tête de bloc doivent être ignorés;

- le mot clé F_Ext_User_Prm_Data_Ref est dirigé vers les ExtUserPrmData où le nom des paramètres F, le type de données, la valeur par défaut et les valeurs numériques admises peuvent être déterminés;
- pour les paramètres F qui comportent des noms normalisés en plus de leurs valeurs numériques, le mot clé Prm_Text_Ref est dirigé vers le PrmText avec ces définitions de noms. Le PrmTxt doit contenir des textes pour toutes les valeurs admises. Les outils de développement/configuration doivent ignorer les textes supplémentaires propres aux valeurs non spécifiées.

Tableau 20 – Exemple de GSD dans la notation GSDL

Déclaration	PrmData référencées	PrmText référencé
F_Ext_User_Prm_Data_Ref(4) = 1	ExtUserPrmData = 1 "F_SIL" BitArea(2-3) 2 0-2 Prm_Text_Ref = 1 EndExtUserPrmData	PrmText = 1 Text(0) = "SIL1" Text(1) = "SIL2" Text(2) = "SIL3" Text(3) = "NoSIL" EndPrmText
F_Ext_User_Prm_Data_Ref(4) = 2	ExtUserPrmData = 2 "F_CRC_Length" BitArea(4-5) 2 2-2 Prm_Text_Ref = 2 EndExtUserPrmData	PrmText = 2 Text(0) = "3-Byte-CRC" Text(1) = "2-Byte-CRC" Text(2) = "4-Byte-CRC" EndPrmText
F_Ext_User_Prm_Data_Ref(4) = 3	ExtUserPrmData = 3 "F_CRC_Seed" Bit(6) 1 1-1 Prm_Text_Ref = 3 EndExtUserPrmData	PrmText = 3 Text(0) = "CRC-Seed16" Text(1) = "CRC-Seed24/32" EndPrmText
F_Ext_User_Prm_Data_Ref(5) = 4	ExtUserPrmData = 4 "F_Passivation" Bit(0) 0 0-0 Prm_Text_Ref = 4 EndExtUserPrmData	PrmText = 4 Text(0) = "Device/Module" Text(1) = "Channel" EndPrmText
F_Ext_User_Prm_Data_Ref(5) = 5	ExtUserPrmData = 5 "F_Block_ID" BitArea(3-5) 0 0-0 EndExtUserPrmData	
F_Ext_User_Prm_Data_Ref(5) = 6	ExtUserPrmData = 6 "F_Par_Version" BitArea(6-7) 1 1-1 Prm_Text_Ref = 5 EndExtUserPrmData	PrmText = 5 Text(0) = "V1-mode" Text(1) = "V2-mode" EndPrmText
F_Ext_User_Prm_Data_Ref(6) = 7	ExtUserPrmData = 7 "F_Source_Add" Unsigned16 1 1-65534 EndExtUserPrmData	
F_Ext_User_Prm_Data_Ref(8) = 8	ExtUserPrmData = 8 "F_Dest_Add" Unsigned16 1 1-65534 EndExtUserPrmData	
F_Ext_User_Prm_Data_Ref(10) = 9	ExtUserPrmData = 9 "F_WD_Time" Unsigned16 500 10-2000 EndExtUserPrmData	
F_Ext_User_Prm_Data_Ref(12) = 10	ExtUserPrmData = 10 "F_Par_CRC" Unsigned16 21211 0-65535 EndExtUserPrmData	

Pour obtenir des modèles de fichiers GSD pour les esclaves F (CP 3/1 ou CP 3/2), s'adresser aux organismes de bus de terrain cités à l'Annexe B.

Dans le cas d'un fichier GSD dédié à un appareil d'entrée-sortie capable d'héberger des Sous-modules F (CP 3/4 à CP 3/6), les règles d'annotation GSDL suivantes s'appliquent pour le calcul de la signature CRC0 (voir l'exemple du Tableau 21 et du Tableau 22):

- certains paramètres F comportent des noms normalisés avec des valeurs numériques associées. Dans la notation GSDML, seuls ces noms doivent être utilisés dans les attributs "DefaultValue" et "AllowedValues". Les valeurs numériques associées peuvent être consultées en 8.1;
- si un paramètre F non inclus dans l'ensemble F_Check_iPar, F_CRC_Length, F_Block_ID est défini comme invisible dans le fichier GSD, une valeur fixe nulle est admise par hypothèse et ce paramètre ne doit pas être inclus dans le calcul de CRC0;
- si un paramètre F (ou des éléments de sa définition) est purement omis du fichier GSD, les valeurs par défaut issues du schéma GSDML correspondant doivent être utilisées. Les paramètres visibles doivent être toujours inclus dans le calcul de CRC0, indépendamment du fait que leurs valeurs soient spécifiées de manière explicite dans un fichier GSD ou qu'elles complètent le schema;
- F_Check_SeqNr n'existe pas dans la définition de la notation GSDML et ne doit donc pas être inclus dans le calcul de CRC0;
- F_Par_Version doit toujours être inclus dans le calcul de CRC0 bien qu'il ait une valeur fixe de "1";
- l'ordre des paramètres F dans l'élément "F_ParameterRecordDataItem" correspond à l'ordre de l'enregistrement des paramètres F, sauf pour F_iPar_CRC.

Tableau 21 – Exemple de GSD dans la notation GSDML

```
<F_ParameterRecordDataItem Index="1" F_ParamDescCRC="56313">
    <F_Check_iPar/>
    <F_SIL DefaultValue="SIL3" AllowedValues="SIL1 SIL2 SIL3"/>
    <F_CRC_Length DefaultValue="4-Byte-CRC" AllowedValues="4-Byte-CRC" Visible="true"/>
    <F_CRC_Seed/>
  <F_Passivation DefaultValue="Device/Module" AllowedValues="Device/Module"/>
    <F_Block_ID DefaultValue="0" AllowedValues="0" Changeable="false"/>
    <F_Par_Version/>
    <F_Source_Add/>
    <F_Dest_Add/>
    <F_WD_Time DefaultValue="500" AllowedValues="10..2000"/>
    <F_Par_CRC DefaultValue="21211"/>
</F_ParameterRecordDataItem
```


Pour obtenir des modèles de fichiers GSD pour les appareils d'entrée-sortie capables d'héberger des Sous-modules F (CP 3/4 à CP 3/6), s'adresser aux organismes de bus de terrain cités à l'Annexe B.

Tableau 22 – Flux d'octets sérialisé pour les exemples

Contenu GSD	Flux d'octets sérialisé pour le calcul de CRC0
"F_SIL" Type=BitArea, Décalage=2 Valeur par défaut=2 (SIL3) "SIL1", 0 (énumération) "SIL2", 1 "SIL3", 2	0x46, 0x5F, 0x53, 0x49, 0x4C, 0x00, 0x02, 0x02, 0x00, 0x53, 0x49, 0x4C, 0x31, 0x00, 0x00, 0x53, 0x49, 0x4C, 0x32, 0x01, 0x00, 0x53, 0x49, 0x4C, 0x33, 0x02, 0x00,
"F_CRC_Length" Type=BitArea, Décalage=4 Valeur par défaut=2 (4-Byte-CRC) Min=2, Max=2 (plage)	0x46, 0x5F, 0x43, 0x52, 0x43, 0x5F, 0x4C, 0x65, 0x6E, 0x67, 0x74, 0x68, 0x00, 0x04, 0x02, 0x00, 0x02, 0x00, 0x02, 0x00,
"F_CRC_Seed" Type=Bit, Décalage=6 Valeur par défaut=1 (CRC_Seed24/32) Min=1, Max=1 (plage)	0x46, 0x5F, 0x43, 0x52, 0x43, 0x5F, 0x53, 0x65, 0x65, 0x64, 0x00, 0x06, 0x01, 0x00, 0x01, 0x00, 0x01, 0x00,
"F_Passivation" Type=Bit, Décalage=0 Valeur par défaut=0 (Appareil/Module) Min=0, Max=0 (plage)	0x46, 0x5F, 0x50, 0x61, 0x73, 0x73, 0x69, 0x76, 0x61, 0x74, 0x69, 0x6F, 0x6E, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
"F_Block_ID" Type=BitArea, Décalage=3 Valeur par défaut=0 Min=0, Max=0	0x46, 0x5F, 0x42, 0x6C, 0x6F, 0x63, 0x6B, 0x5F, 0x49, 0x44, 0x00, 0x03, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
"F_Par_Version" Type=BitArea, Décalage=6 Valeur par défaut=1 (mode V2) Min=1, Max=1	0x46, 0x5F, 0x50, 0x61, 0x72, 0x5F, 0x56, 0x65, 0x72, 0x73, 0x69, 0x6F, 0x6E, 0x00, 0x06, 0x01, 0x00, 0x01, 0x00, 0x01, 0x00,
"F_Source_Add" Type=Unsigned16 Valeur par défaut=1 Min=1, Max=65534	0x46, 0x5F, 0x53, 0x6F, 0x75, 0x72, 0x63, 0x65, 0x5F, 0x41, 0x64, 0x64, 0x02, 0x00, 0x01, 0x00, 0x01, 0x00, 0xFE, 0xFF,
"F_Dest_Add" Type=Unsigned16 Valeur par défaut=1 Min=1, Max=65534	0x46, 0x5F, 0x44, 0x65, 0x73, 0x74, 0x5F, 0x41, 0x64, 0x64, 0x02, 0x00, 0x01, 0x00, 0x01, 0x00, 0xFE, 0xFF,
"F_WD_Time" Type=Unsigned16 Valeur par défaut=500 Min=10, Max=2000	0x46, 0x5F, 0x57, 0x44, 0x5F, 0x54, 0x69, 0x6D, 0x65, 0x02, 0x00, 0xF4, 0x01, 0x0A, 0x00, 0xD0, 0x07,
"F_Par_CRC" Type=Unsigned16 Valeur par défaut=21211 Min=0, Max=65535	0x46, 0x5F, 0x50, 0x61, 0x72, 0x5F, 0x43, 0x52, 0x43, 0x02, 0x00, 0xDB, 0x52, 0x00, 0x00, 0xFF, 0xFF

La signature CRC0 résultante 56313 (décimale) ou 0xDBF9 (hexadécimale) doit être saisie dans l'attribut F_ParamDescCRC.

Interprétation du fichier GSD: chaque fois que l'outil de développement reconnaît des mots clés F, un logiciel particulier de configuration F (dont la sécurité a en général été évaluée) peut être lancé dans l'outil de développement pour traiter les paramètres F de manière sécurisée.

8.4 Configuration de la sécurité

8.4.1 Ordre des types de données d'entrée-sortie

Les données d'entrée-sortie du SPDU doivent être triées conformément au Tableau 23:

Tableau 23 – Ordre des types de données d'entrée-sortie

Ordre	Nom du type de données d'entrée-sortie
1	Float32+Unsigned8 (utilisé comme bits) [=Type de données PA "composite"]
2	Unsigned8 (utilisé comme bits) + Unsigned8 (utilisé comme bits) [=Type de données PA]
3	Unsigned8 (utilisé comme bits) [=DI, DO]
4	Integer16 [=AI, AO]
5	Integer32
6	Float32

Si un type de données n'est pas présent, les autres prennent sa place.

8.4.2 Protection de la description des données d'entrée-sortie de sécurité

La structure de données d'entrée-sortie F est décrite dans la section "IOData" du fichier GSD. Un attribut est "F_IO_StructureDescCRC". Ce CRC repose sur les attributs du Tableau 24 dans l'ordre indiqué (Version 2). Le polynôme CRC à 32 bits (*0xF4ACFB13*) doit être utilisé pour calculer la signature. Les types de données admis pour FSCP 3/1 figurent en 5.5.3. La précédente version 1 de l'ensemble d'éléments de structure de données d'entrée-sortie ne contenait pas l'attribut VERSION, ni les types de données Integer32 et Unsigned8+Unsigned8. Par conséquent, aucun mot clé F_IO_StructureDescVersion d'un fichier GSD particulier n'indique l'indisponibilité des types de données Integer32 et Unsigned8+Unsigned8, la signature F_IO_StructureDescCRC doit être calculée à l'aide du polynôme CRC à 16 bits (*0x4EAB*), et la longueur de la signature CRC est de 2 octets.

Tous les octets de "COUNT_PS_INPUT_BYTES_BOOL_MAX", à l'exception de celui qui a l'adresse la plus élevée, comptent comme "8" booléens dans COUNT_PS_INPUT_CHANNELS_BOOL_MAX.Tous les octets de "COUNT_PS_OUTPUT_BYTES_BOOL", à l'exception de celui qui a l'adresse la plus élevée, comptent comme "8" booléens dans COUNT_PS_OUTPUT_CHANNELS_BOOL. Seul l'octet qui a l'adresse la plus élevée peut compter comme moins de 8 booléens, si les canaux qui ont l'adresse de bit la plus élevée ne sont pas utilisés.

Si certains canaux booléens ne sont pas utilisés par le Sous-module F, celui-ci doit attribuer la valeur 0 (FVi, FVo) à ces canaux.

Le paramètre "F_IO_StructureDescCRC" n'est pas transmis au Sous-module F lors du démarrage. L'outil de développement de l'hôte doit vérifier F_IO_StructureDescCRC pour assurer une représentation correcte dans l'hôte F.