

INTERNATIONAL STANDARD

NORME INTERNATIONALE



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

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



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2007 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester.

If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de la CEI ou du Comité national de la CEI du pays du demandeur.

Si vous avez des questions sur le copyright de la CEI ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de la CEI de votre pays de résidence.

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

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
info@iec.ch
www.iec.ch

About the IEC

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

About IEC publications

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

Useful links:

IEC publications search - www.iec.ch/searchpub

The advanced search enables you to find IEC publications by a variety of criteria (reference number, text, technical committee,...).

It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

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

Electropedia - www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 30 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary (IEV) on-line.

Customer Service Centre - webstore.iec.ch/csc

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

A propos de la CEI

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

A propos des publications CEI

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

Liens utiles:

Recherche de publications CEI - www.iec.ch/searchpub

La recherche avancée vous permet de trouver des publications CEI en utilisant différents critères (numéro de référence, texte, comité d'études,...).

Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

Just Published CEI - webstore.iec.ch/justpublished

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

Electropedia - www.electropedia.org

Le premier dictionnaire en ligne au monde de termes électroniques et électriques. Il contient plus de 30 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans les langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (VEI) en ligne.

Service Clients - webstore.iec.ch/csc

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

INTERNATIONAL STANDARD

NORME INTERNATIONALE



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

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

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

PRICE CODE
CODE PRIX

XE

ICS 25.040; 35.100.05

ISBN 978-2-83220-722-2

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

CONTENTS

FOREWORD.....	8
INTRODUCTION.....	10
1 Scope.....	13
2 Normative references	13
3 Terms, definitions, symbols, abbreviated terms and conventions	15
3.1 Terms and definitions	15
3.1.1 Common terms and definitions	15
3.1.2 CPF 3: Additional terms and definitions	19
3.2 Symbols and abbreviated terms.....	23
3.2.1 Common symbols and abbreviated terms	23
3.2.2 CPF 3: Additional symbols and abbreviated terms	23
3.3 Conventions	24
4 Overview of FSCP 3/1 (PROFIsafe™)	25
5 General	27
5.1 External documents providing specifications for the profile.....	27
5.2 Safety functional requirements	27
5.3 Safety measures	28
5.4 Safety communication layer structure.....	29
5.4.1 Principle of FSCP 3/1 safety communications	29
5.4.2 CPF 3 communication structures	30
5.5 Relationships with FAL (and DLL, PhL)	33
5.5.1 Device model.....	33
5.5.2 Application and communication relationships.....	33
5.5.3 Message format.....	35
5.5.4 Data types	35
6 Safety communication layer services	36
6.1 F-Host services	36
6.2 F-Device services.....	39
6.3 Diagnosis	40
6.3.1 Safety alarm generation.....	40
6.3.2 F-Device safety layer diagnosis including the iPar-Server.....	40
7 Safety communication layer protocol	41
7.1 Safety PDU format	41
7.1.1 Safety PDU structure	41
7.1.2 Safety I/O data	42
7.1.3 Status and Control Byte.....	42
7.1.4 (Virtual) Consecutive Number	44
7.1.5 CRC2 Signature	45
7.1.6 Appended standard I/O data	46
7.2 FSCP 3/1 behavior	46
7.2.1 General	46
7.2.2 F-Host state diagram	47
7.2.3 F-Device state diagram.....	50
7.2.4 Sequence diagrams.....	54
7.2.5 Timing diagram for a counter reset	60

7.2.6	Monitoring of safety times.....	60
7.3	Reaction in the event of a malfunction.....	63
7.3.1	Repetition.....	63
7.3.2	Loss	63
7.3.3	Insertion	63
7.3.4	Incorrect sequence	63
7.3.5	Corruption of safety data	63
7.3.6	Delay.....	64
7.3.7	Masquerade	64
7.3.8	Memory failures within switches	65
7.3.9	Network boundaries and router.....	66
7.4	F-Startup and change coordination.....	66
7.4.1	Standard startup procedure	66
7.4.2	iParameter assignment deblocking	66
8	Safety communication layer management.....	67
8.1	F-Parameter	67
8.1.1	Summary	67
8.1.2	F_Source/Destination_Address (codename)	67
8.1.3	F_WD_Time (F-Watchdog time).....	68
8.1.4	F_Prm_Flag1 (Parameters for the safety layer management)	68
8.1.5	F_Prm_Flag2 (Parameters for the safety layer management)	69
8.1.6	F_iPar_CRC (value of iPar_CRC across iParameters).....	70
8.1.7	F_Par_CRC (CRC1 across F-Parameters).....	71
8.1.8	Structure of the F-Parameter record data object	71
8.1.9	F-Data fraction	71
8.2	iParameter and iPar_CRC	72
8.3	Safety parameterization.....	73
8.3.1	Objectives	73
8.3.2	GSD and GSDML safety extensions	73
8.3.3	Securing safety parameters and GSD data	74
8.4	Safety configuration	76
8.4.1	Securing the safety I/O data description (CRC7).....	76
8.4.2	Dataltem data type section examples	77
8.5	Data type information usage	79
8.5.1	F-Channel driver.....	79
8.5.2	Rules for standard F-Channel drivers	80
8.5.3	Recommendations for F-Channel drivers	80
8.6	Safety parameter assignment mechanisms.....	81
8.6.1	F-Parameter assignment	81
8.6.2	General iParameter assignment.....	82
8.6.3	System integration requirements for iParameterization tools.....	83
8.6.4	iPar-Server	84
9	System requirements.....	92
9.1	Indicators and switches	92
9.2	Installation guidelines.....	93
9.3	Safety function response time	93
9.3.1	Model	93
9.3.2	Calculation and optimization	95
9.3.3	Adjustment of watchdog times for FSCP 3/1	96

9.3.4	Engineering tool support.....	97
9.3.5	Retries (repetition of messages).....	97
9.4	Duration of demands	98
9.5	Constraints for the calculation of system characteristics	99
9.5.1	Probabilistic considerations	99
9.5.2	Safety related constraints	101
9.5.3	Non safety related constraints (availability).....	102
9.6	Maintenance.....	102
9.6.1	F-Module commissioning / replacement.....	102
9.6.2	Identification and maintenance functions	102
9.7	Safety manual	103
9.8	Wireless transmission channels.....	103
9.8.1	Black Channel approach.....	103
9.8.2	Availability.....	104
9.8.3	Security measures.....	104
9.8.4	Stationary and mobile applications	106
9.9	Conformance classes	106
10	Certification	107
10.1	Safety policy	107
10.2	Obligations	108
Annex A (informative) Additional information for functional safety communication profiles of CPF 3.....		109
A.1	Hash function calculation.....	109
A.2	Response time measurements.....	111
Bibliography.....		115
Table 1 – Deployed measures to master errors		28
Table 2 – Data types used for FSCP 3/1		35
Table 3 – Safety layer diagnosis messages		41
Table 4 – F-Host states and transitions.....		48
Table 5 – F-Device states and transitions		52
Table 6 – SIL monitor times		63
Table 7 – Remedies for switch failures.....		65
Table 8 – Safety network boundaries		66
Table 9 – I/O data structure items (Version 2).....		76
Table 10 – Sample F-Channel drivers		80
Table 11 – Requirements for iParameterization.....		83
Table 12 – Specifier for the iPar-Server Request		87
Table 13 – Structure of the Read_RES_PDU ("read record").....		88
Table 14 – Structure of the Write_REQ_PDU ("write record").....		89
Table 15 – Structure of the Pull_RES_PDU ("Pull").....		89
Table 16 – Structure of the Push_REQ_PDU ("Push")		89
Table 17 – iPar-Server states and transitions.....		91
Table 18 – iPar-Server management measures.....		92
Table 19 – Information to be included in the safety manual.....		103

Table 20 – Security measures for WLAN (IEEE 802.11i)	105
Table 21 – Security measures for Bluetooth (IEEE 802.15.1)	106
Table 22 – F-Host conformance class requirements	107
Table A.1 – The table "Crctab24" for 24 bit CRC signature calculations	110
Table A.2 – The table "Crctab32" for 32 bit CRC signature calculations	111
Figure 1 – Relationships of IEC 61784-3 with other standards (machinery)	10
Figure 2 – Relationships of IEC 61784-3 with other standards (process)	11
Figure 3 – Basic communication preconditions for FSCP 3/1	25
Figure 4 – Structure of an FSCP 3/1 safety PDU	26
Figure 5 – Safe communication modes	27
Figure 6 – Standard CPF 3 transmission system	29
Figure 7 – Safety layer architecture	30
Figure 8 – Basic communication layers	30
Figure 9 – Multiport switch bus structure	31
Figure 10 – Linear bus structure	31
Figure 11 – Crossing network borders with routers	32
Figure 12 – Complete safety transmission paths	32
Figure 13 – Device model	33
Figure 14 – Application relationships of a modular device	34
Figure 15 – Application and communication relationships (AR/CR)	34
Figure 16 – Message format	35
Figure 17 – FSCP 3/1 communication structure	37
Figure 18 – F user interface of F-Host driver instances	37
Figure 19 – F-Device driver interfaces	39
Figure 20 – Safety PDU for CPF 3	42
Figure 21 – Status Byte	42
Figure 22 – Control Byte	43
Figure 23 – The Toggle Bit function	44
Figure 24 – F-Device Consecutive Number	44
Figure 25 – CRC2 generation (F-Host output)	45
Figure 26 – Details of the CRC2 calculation (reverse order)	46
Figure 27 – Safety layer communication relationship	46
Figure 28 – F-Host state diagram	47
Figure 29 – F-Device state diagram	51
Figure 30 – Interaction F-Host / F-Device during start-up	54
Figure 31 – Interaction F-Host / F-Device during F-Host power off → on	55
Figure 32 – Interaction F-Host / F-Device with delayed power on	56
Figure 33 – Interaction F-Host / F-Device during power off → on	57
Figure 34 – Interaction F-Host / F-Device while host recognizes CRC error	58
Figure 35 – Interaction F-Host / F-Device while device recognizes CRC error	59
Figure 36 – Impact of the counter reset signal	60

Figure 37 – Monitoring the message transit time F-Host ↔ F-Output	61
Figure 38 – Monitoring the message transit time F-Input ↔ F-Host	61
Figure 39 – F-Parameter data and CRC	64
Figure 40 – iParameter assignment deblocking by the F-Host	67
Figure 41 – F_Prm_Flag1	68
Figure 42 – F_Check_SeqNr	68
Figure 43 – F_Check_iPar	69
Figure 44 – F_SIL	69
Figure 45 – F_CRC_Length	69
Figure 46 – F_Prm_Flag2	70
Figure 47 – F_Block_ID	70
Figure 48 – F_Par_Version	70
Figure 49 – F-Parameter	71
Figure 50 – iParameter block	72
Figure 51 – F-Parameter extension within the GSDML specification	74
Figure 52 – CRC1 including iPar_CRC	75
Figure 53 – Algorithm to build CRC0	75
Figure 54 – DataItem section for F_IN_OUT_1	77
Figure 55 – DataItem section for F_IN_OUT_2	78
Figure 56 – DataItem section for F_IN_OUT_5	78
Figure 57 – DataItem section for F_IN_OUT_6	79
Figure 58 – F-Channel driver as "glue" between F-Device and user program	79
Figure 59 – Layout example of an F-Channel driver	80
Figure 60 – F-Parameter assignment for simple F-Devices and F-Slaves	81
Figure 61 – F and iParameter assignment for complex F-Devices	82
Figure 62 – System integration of CPD-Tools	84
Figure 63 – iPar-Server mechanism (commissioning)	84
Figure 64 – iPar-Server mechanism (for example F-Device replacement)	85
Figure 65 – iPar-Server request coding ("status model")	86
Figure 66 – Coding of SR_Type	87
Figure 67 – iPar-Server request coding ("alarm model")	88
Figure 68 – iPar-Server state diagram	90
Figure 69 – Example safety function with a critical response time path	93
Figure 70 – Simplified typical response time model	94
Figure 71 – Frequency distributions of typical response times of the model	94
Figure 72 – Context of delay times and watchdog times	95
Figure 73 – Timing sections forming the FSCP 3/1 F_WD_Time	96
Figure 74 – Frequency distribution of response times with message retries	97
Figure 75 – Retries with CP 3/1	98
Figure 76 – Retries with CP 3/RTE	98
Figure 77 – Residual error probabilities for the 24-bit polynomial	99
Figure 78 – Properness of the 32-bit polynomial for 52 octets	100
Figure 79 – Properness of the 32-bit polynomial for 132 octets	100

Figure 80 – Monitoring of corrupted messages.....	101
Figure 81 – Security for WLAN networks.....	104
Figure 82 – Security for Bluetooth networks.....	105
Figure A.83 – Typical "C" procedure of a cyclic redundancy check.....	109
Figure A.84 – Comparison of the response time model and a real application	112
Figure A.85 – Frequency distribution of measured response times.....	113
Figure A.86 – F-Host with standard and safety-related application programs	114

Withdrawn

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 provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with an IEC Publication.
- 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.

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 as follows, where the [xx] notation indicates the holder of the patent right:

EP1267270-A2	[SI]	Verfahren zur Datenübertragung in einem Rechnersystem
WO00/045562-A1	[SI]	Method and device for determining the reliability of data carriers
WO99/049373-A1	[SI]	Shortened data message of an automation system

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

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

Information may be obtained from:

[SI]	Siemens AG A&D AS FA TC Karlsruhe Germany
------	--

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

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

This bilingual version (2013-05) corresponds to the monolingual English version, published in 2007-12.

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

FDIS	Report on voting
65C/470/FDIS	65C/481/RVD

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

The French version of this standard has not been voted upon.

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

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

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

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

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.

INTRODUCTION

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

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

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

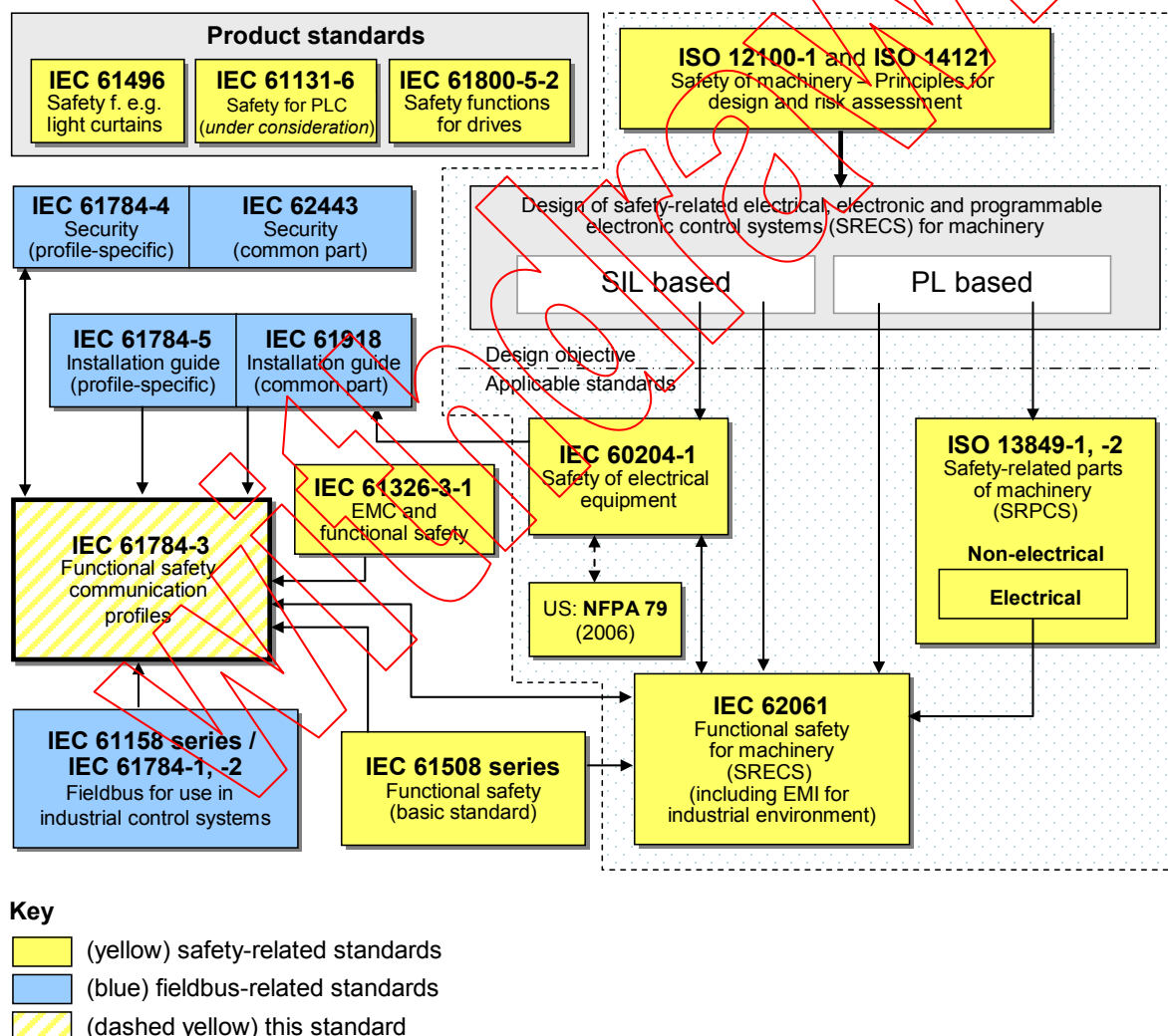
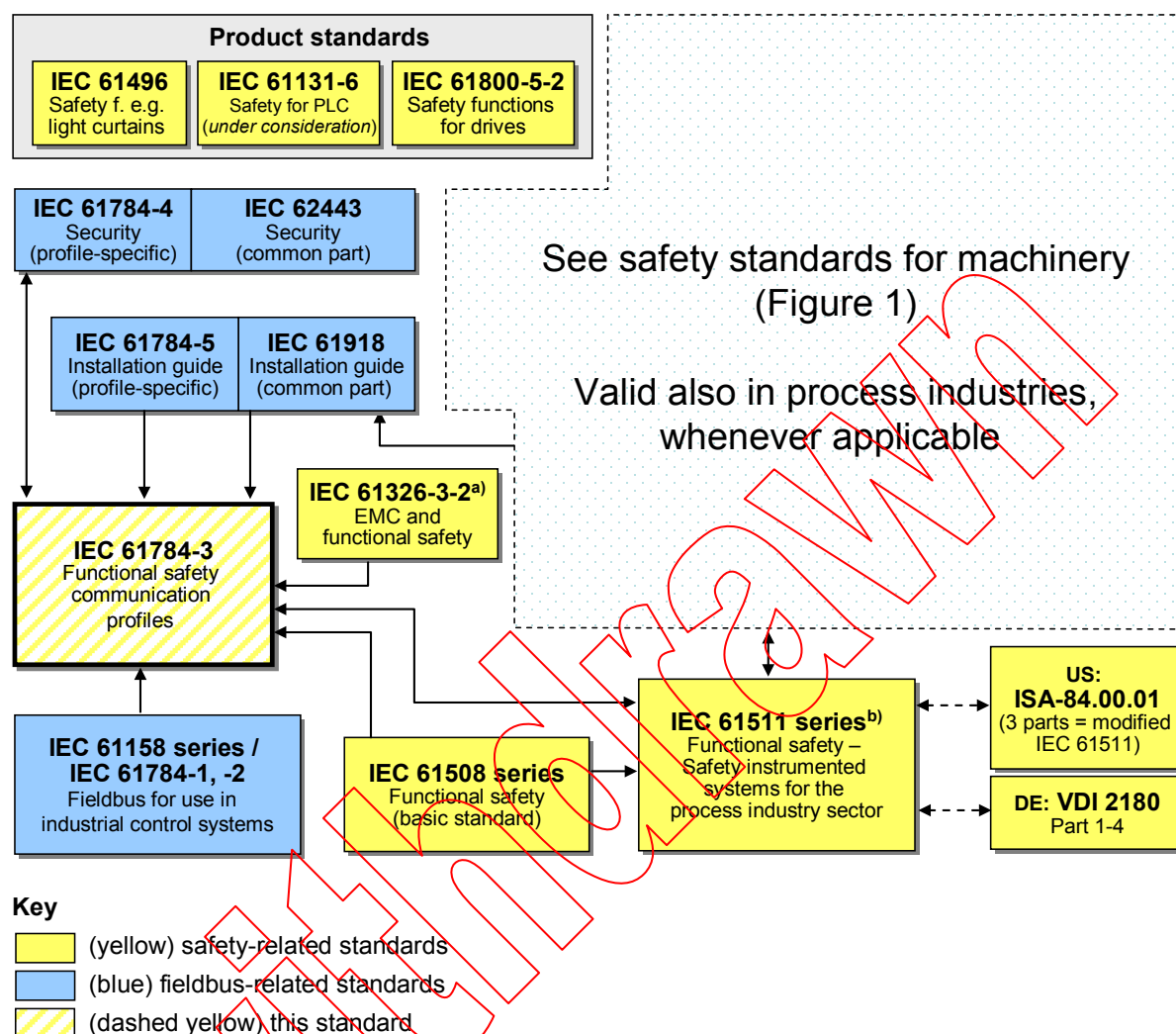


Figure 1 – Relationships of IEC 61784-3 with other standards (machinery)

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



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

^b EN ratified.

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

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

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

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

This standard describes

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

Withdrawn

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES –

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

1 Scope

This part of the IEC 61784-3 series 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.

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 part¹ 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 for functional safety. These mechanisms may be used in various industrial applications such as process control, manufacturing automation and machinery.

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

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

2 Normative references

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

IEC 61010-1, *Safety requirements for electrical equipment for measurement, control, and laboratory use – Part 1: General requirements*

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

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

IEC 61158 (all parts), *Industrial communication networks – Fieldbus specifications*

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

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

IEC 61158-4-3, *Industrial communication networks – Fieldbus specifications – Part 4-3: Data-link layer protocol specification*

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

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

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

IEC 61158-6-3, *Industrial communication networks – Fieldbus specifications – Part 4-3: Application layer protocol specification*

IEC 61158-6-10, *Industrial communication networks – Fieldbus specifications – Part 4-10: Application layer protocol specification*

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 applications²*

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 EM environment²*

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

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

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

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

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

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

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

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

IEC 62280-1:2002, *Railway applications – Communication, signalling and processing systems – Part 1: Safety-related communication in closed transmission systems*

IEC 62280-2, *Railway applications – Communication, signalling and processing systems – Part 2: Safety-related communication in open transmission systems*

IEC/TR 62390, *Common automation device – Profile guideline*

² To be published.

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

ISO 15745-3, *Industrial automation systems and integration – Open systems application integration framework – Part 3: Reference description for IEC 61158-based control systems*

ISO 15745-4, *Industrial automation systems and integration – Open systems application integration framework – Part 4: Reference description for Ethernet-based control systems – Amendment 1: PROFINET profiles*

3 Terms, definitions, symbols, abbreviated terms and conventions

3.1 Terms and definitions

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

3.1.1 Common terms and definitions

3.1.1.1 availability

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

NOTE Availability depends on MTBF (mean time between failure) and MDT (mean down time):
$$\text{Availability} = \text{MTBF} / (\text{MTBF} + \text{MDT}).$$

3.1.1.2 black channel

communication channel without available evidence of design or validation according to IEC 61508 series

3.1.1.3 communication channel

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

3.1.1.4 communication system

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

3.1.1.5 connection

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

3.1.1.6 Cyclic Redundancy Check (CRC)

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

<method> procedure used to calculate the redundant data

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

NOTE 2 See also [28], [29]³.

³ Figures in square brackets refer to the bibliography.

3.1.1.7

error

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

NOTE 1 An error can be caused by a faulty item, e.g. a computing error made by faulty computer equipment.

[IEV 191-05-24], [IEC 61508-4:1998], [IEC 61158]

NOTE 2 Errors may be due to design mistakes within hardware/software and/or corrupted information due to electromagnetic interference and/or other effects.

NOTE 3 Errors do not necessarily result in a *failure* or a *fault*.

3.1.1.8

failure

termination of the ability of a functional unit to perform a required function

NOTE 1 The definition in IEV 191-04-01 is the same, with additional notes.

[IEC 61508-4:1998], [ISO/IEC 2382-14.01.11]

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

3.1.1.9

fault

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

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

[IEC 61508-4:1998], [ISO/IEC 2382-14.01.10]

3.1.1.10

fieldbus

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

3.1.1.11

fieldbus system

system using a *fieldbus* with connected devices

3.1.1.12

frame

denigrated synonym for DLPDU

3.1.1.13

Frame Check Sequence (FCS)

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

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

NOTE 2 See also [28], [29].

3.1.1.14

hash function

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

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

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

[IEC 62210, modified]

3.1.1.15

hazard

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

3.1.1.16

master

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

3.1.1.17

message

ordered series of octets intended to convey information

[ISO/IEC 2382-16.02.01, modified]

3.1.1.18

nuisance trip

spurious trip with no harmful effect

NOTE Internal abnormal errors can be caused in communication systems such as wireless transmission, for example by too many retries in the presence of interferences.

3.1.1.19

proof test

periodic test performed to detect failures in a *safety-related system* so that, if necessary, the system can be restored to an “as new” condition or as close as practical to this condition

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

[IEC 61508-4 and IEC 62061, modified]

3.1.1.20

protective extra-low-voltage (PELV)

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

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

[IEC 61131-2]

3.1.1.21

redundancy

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

EXAMPLE Duplicated functional components and the addition of parity bits are both instances of redundancy.

NOTE 1 Redundancy is used primarily to improve reliability or availability.

NOTE 2 The definition in IEC 191-15-01 is less complete.

[IEC 61508-4:1998], [ISO/IEC 2382-14.01.12]

3.1.1.22
reliability

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

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

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

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

NOTE 4 Reliability differs from availability.

[IEC 62059-11, modified]

3.1.1.23
risk

combination of the probability of occurrence of harm and the severity of that harm
[IEC 61508-4:1998]

3.1.1.24
safety communication layer (SCL)

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

3.1.1.25
safety connection

connection that utilizes the safety protocol for communications transactions

3.1.1.26
safety data

data transmitted across a safety network using a safety protocol

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

3.1.1.27
safety device

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

3.1.1.28
safety extra-low-voltage (SELV)

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

NOTE An SELV circuit is not connected to protective earth.

[IEC 61131-2]

3.1.1.29
safety function

function to be implemented by an E/E/PE safety-related system, other technology *safety-related system* or external risk reduction facilities, which is intended to achieve or maintain a safe state for the EUC, in respect of a specific hazardous event
[IEC 61508-4:1998]

3.1.1.30**safety function response time (SFRT)**

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

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

3.1.1.31**safety integrity level (SIL)**

discrete level (one out of a possible four) for specifying the safety integrity requirements of the *safety functions* to be allocated to the E/E/PE safety-related systems, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest

NOTE The target failure measures for the four safety integrity levels are specified in Tables 2 and 3 of IEC 61508-1.

[IEC 61508-4:1998]

3.1.1.32**safety measure**

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

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

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

3.1.1.33**safety-related application**

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

3.1.1.34**safety-related system**

system performing *safety functions* according to IEC 61508

3.1.1.35**slave**

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

3.1.1.36**spurious trip**

trip caused by the safety system without a process demand

3.1.2 CPF 3: Additional terms and definitions**3.1.2.1****bit**

encoded binary information without a technical unit (**B**inary **D**igit)

3.1.2.2**codename**

unique identification between safety communication peers

NOTE Instance of "connection authentication" as described in IEC 61784-3.

3.1.2.3 configuration

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

NOTE 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.

3.1.2.4 consecutive number

means to ensure completeness and the right order of transmitted safety PDUs

NOTE 1 Instance of "sequence number" as described in IEC 61784-3.

NOTE 2 The consecutive number can be transmitted with each safety PDU (V1-mode) or only secured via the transmitted CRC signature (V2-mode).

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 Usually this is called a head station.

3.1.2.8 device acknowledgement time (DAT)

elapsed time in an F-Device starting with the reception of a safety PDU with a new consecutive number 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

3.1.2.11 fail-safe values (FV)

values which are issued instead of process values when the system is set to a fail-safe state

NOTE In this part the fail-safe values (FV) shall always be set to "0".

3.1.2.12 F-Device

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

3.1.2.13**F-Driver**

software administering safety PDUs within F-Hosts and F-Devices according to the FSCP 3/1 specifications

3.1.2.14**F-Host**

data processing unit that is able to perform the FSCP 3/1 protocol and to service the "black channel"

NOTE This is usually a PLC or an IPC with an adequate operating system.

3.1.2.15**F-Module**

passive communication peer within a modular F-Device or F-Slave that is able to perform the FSCP 3/1 protocol, usually triggered by the F-Host for data exchange

NOTE This is usually a safety-related input or output module.

3.1.2.16**F-Slave**

passive 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.

3.1.2.17**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

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

Within F-CPU: Corresponding user program reaction possible. F-I/O-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.

3.1.2.18**function block (FB)**

self-contained program part possessing a specific functionality

3.1.2.19**host acknowledgement time (HAT)**

elapsed time in an F-Host starting with the reception of a safety PDU with a certain consecutive number until an appropriate safety PDU with an incremented consecutive number has been generated and returned to the master/IO-controller

3.1.2.20**IO-Controller**

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

NOTE Within CP 3/1 this task is corresponding to a master class 1.

3.1.2.21**IO-Device**

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

NOTE Within CP 3/1 this task is corresponding to a slave.

3.1.2.22

IO-Module

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

3.1.2.23

IO-Supervisor

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

NOTE 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.

3.1.2.24

IO-System

IO-Controller and its associated IO-Devices

3.1.2.25

iParameter

individual or technology specific F-Device parameters

NOTE Typical iParameters are the protection zone coordinates of a laser scanner.

3.1.2.26

iPar-Server

standardised mechanism to store and retrieve individual or technology specific F-Device parameters within the standard part of an F-Host or its controlled subsystem

3.1.2.27

master (class 1)

active CP 3/1 communication peer triggering slaves for data exchange

3.1.2.28

process values (PV)

input and output data in a safety PDU that are required to control an automated process

3.1.2.29

qualifier

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

3.1.2.30

shared I/O

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

NOTE Even though CP 3/RTE is permitting shared I/O it is not permitted with FSCP 3/1.

3.1.2.31

toggle bit

one bit of the Control and Status Byte to synchronize the (virtual) consecutive counters in both the F-Host and the F-Device

3.1.2.32

universal serial bus (USB)

external bus standard that supports data transfer rates up to 480 Mbps

NOTE USB is replacing serial and parallel computer ports and is used for fast direct connections between service computers and field devices.

3.1.2.33**V1-mode**

FSCP 3/1 services and protocol according to [42]

3.1.2.34**V2-mode**

FSCP 3/1 services and protocol according to this part

3.1.2.35**VLAN tag**

extension within Ethernet messages that enables particular user groups on large networks to run their own virtual network via priorities and VLAN-IDs, using appropriate switches, without impacting other user groups and vice versa

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

CP	Communication Profile	[IEC 61784-1]
CPF	Communication Profile Family	[IEC 61784-1]
CRC	Cyclic Redundancy Check	
DLL	Data Link Layer	[ISO/IEC 7498-1]
DLPDU	Data Link Protocol Data Unit	
EMI	Electro-Magnetic Interference	
EUC	Equipment Under Control	[IEC 61508-4:1998]
FAL	Fieldbus Application Layer	[IEC 61158-5]
FCS	Frame Check Sequence	
FSCP	Functional Safety Communication Profile	
HD	Hamming Distance	
E/E/PE	Electrical/Electronic/Programmable Electronic	[IEC 61508-4:1998]
PDU	Protocol Data Unit	[ISO/IEC 7498-1]
PELV	Protective Extra Low Voltage	
PFD	Average Probability of Failure on Demand	[IEC 61508-6:1998]
PFH	Probability of Failure per Hour	[IEC 61508-6:1998]
PhL	Physical Layer	[ISO/IEC 7498-1]
PLC	Programmable Logic Controller	
SCL	Safety Communication Layer	
SELV	Safety Extra Low Voltage	
SFRT	Safety Function Response Time	
SIL	Safety Integrity Level	[IEC 61508-4:1998]

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

CP 3/1	Communication profile commonly known as PROFIBUS DP
CP 3/2	Communication profile commonly known as PROFIBUS PA
CP 3/RTE	Communication profile commonly known as PROFINET IO
CPU	Central Processing Unit
CR	Communication Relationship
DAP	Device Access Point
DAT	Device Acknowledgement Time
DP	Decentralized Peripherals
F	Identifier for safety items (fail-safe, functional safe)
FB	Function Block
FV	Fail-safe Values
GSD	Generic Station Description
GSDML	Generic Station Description Markup Language
HAT	Host Acknowledgement Time
I/O	Input/Output
LED	Light Emitting Diode
MTBF	MeanTime Between Failure
MTTF	MeanTime To Failure
PA	Process Automation
PN IO	PROFINET IO = CP 3/4 to 3/6
PSK	Pre-shared Key
PV	Process Values
RADIUS	Remote Authentication Dial In User Service
S	Standard
SSID	Service Set Identifier
UML	Unified Modeling Language
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
WCDT	Worst Case Delay Time
WDTime	Watchdog Time
WPA2	Wi-Fi Protected Access 2 (corresponds to IEEE802.11i)
XML	extensible Markup Language (World Wide Web Consortium)

3.3 Conventions

This part uses UML2 notation for the drawing of the state charts and a condensed form for sequence charts [51]. The transition tables are depicted following the recommendations of IEC 62390.

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

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

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

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 61158-3-3, IEC 61158-4-3, 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 part.

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, parameterisation, diagnosis, and maintenance purposes.

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

- (virtual) consecutive numbering;
- watchdog time monitoring with acknowledgement;
- codename per communication relationship;
- cyclic redundancy checking for data integrity.

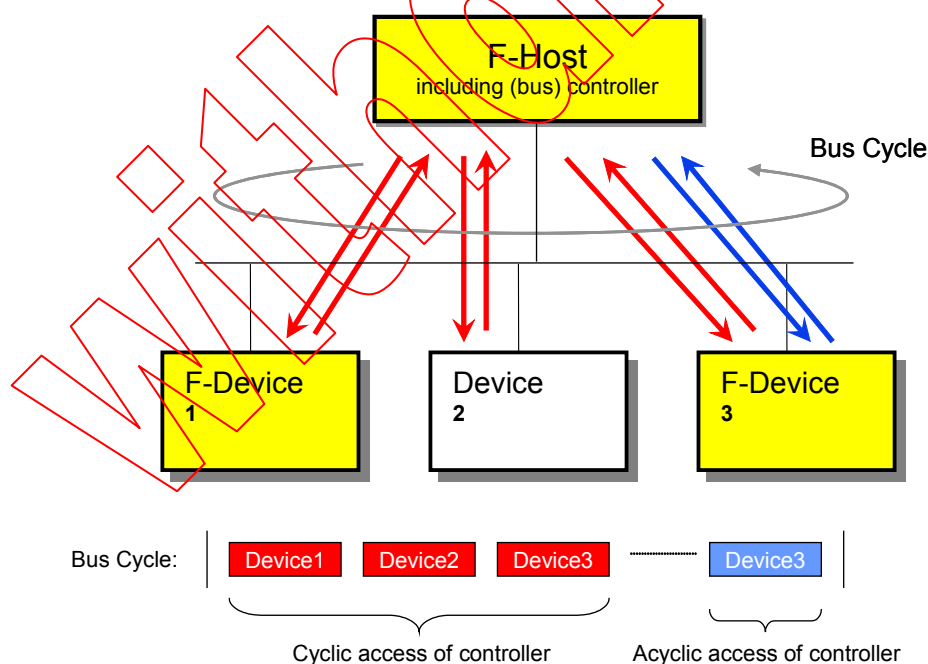


Figure 3 – Basic communication preconditions for FSCP 3/1

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 International Standard and does not constitute an endorsement by IEC of the trade name holder or any of its products. Compliance to this standard does not require use of the registered logos for PROFIBUS™, PROFINET™ or PROFIsafe™. Use of the registered logos for PROFIBUS™, PROFINET™ or PROFIsafe™ requires permission of PNO.

The consecutive numbering uses a range that is big enough to secure any malfunction caused by message storing network elements. Every safety device returns a message with a safety PDU for acknowledgement 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 unique codename per communication relationship is established for authentication reasons and is encoded within an initial CRC signature value for the cyclically calculated and transmitted CRC2 signature (Figure 4).

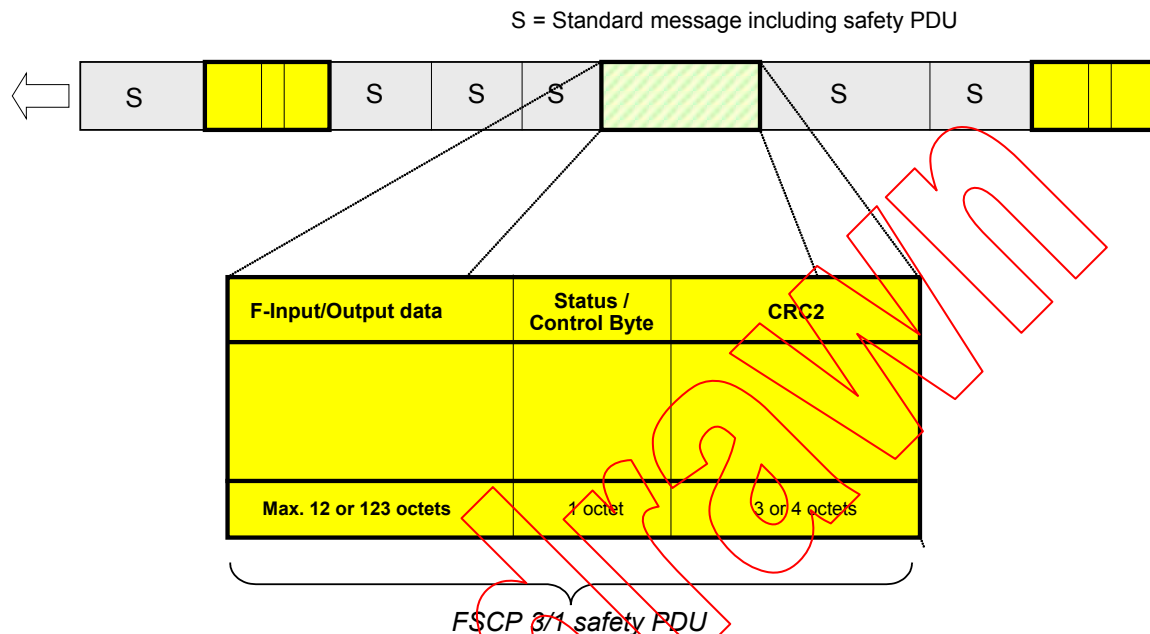


Figure 4 – Structure of an FSCP 3/1 safety PDU

FSCP 3/1 provides two operational modes: V1- and V2-mode. While the measures of the V1-mode are sufficient for the safe data transmission on pure CP 3/1 networks, the more "generous" features of Ethernet / CP 3/RTE such as wider address space and buffering switch components are requiring some extensions to the FSCP 3/1 protocol thus leading to the V2-mode. The V1-mode is restricted to CP 3/1 whereas the V2-mode is required for CP 3/4 to CP 3/6 and/or CP 3/1. This part only describes the details of the extended functionality of the so-called V2-mode. Safe communication between PROFINET CBA components (see CP 3/3) is not yet defined. Figure 5 provides an overview on FSCP 3/1 within the CP 3/1 and CP 3/RTE architectures.

While automation solutions with distributed I/O gained widely acceptance through PROFIBUS (CP 3/1 and CP 3/2) and the industrial Ethernet based PROFINET (CP 3/RTE), 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 part 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/RTE 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 5.5.4. Subclauses 6.1 to 6.3 are unveiling the F-Host and F-Device services as well as the possible diagnosis messages of the safety layer.

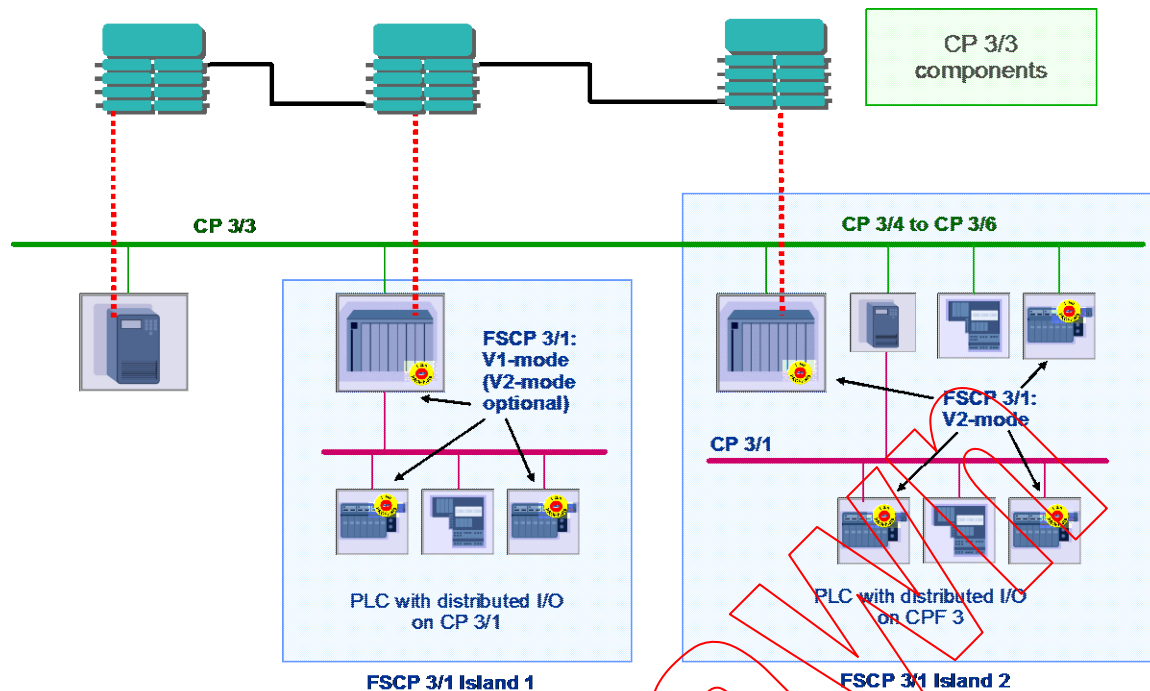


Figure 5 – Safe communication modes

Clause 7 starts with an overview on the safety PDU (7.1), continues with a description of the state machines in F-Host and F-Device and sequence diagrams in the Unified Modeling Language 2 format (7.2.2 to 7.2.4). Associated timing constraints are contained in 7.2.5 and 7.2.6. Following the format of [27], 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 is focusing 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 are representing the configuration of a device. Subclause 8.5 shows how the data structure information can be used to configure F-Channel drivers for more complex F-Devices 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 9. The reasoning for certification is pointed out in 10.1 and the details in 10.2. An informative annex contains examples for fast CRC signature calculations and a bibliography. Two additional FSCP 3/1 guidelines for electrical safety and certification shall be observed ([38], [39]).

5 General

5.1 External documents providing specifications for the profile

In addition to the normative references in Clause 2, the technology in this part has been approved according to GS-ET-26 [27].

FSCP 3/1 meets the requirements of NE97 [52].

5.2 Safety functional requirements

The following requirements have been mandatory 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 control category 4 (see EN 954-1).
- c) Safety communication shall use a single-channel communication system. Redundancy may only be used optionally for increased availability.
- d) Implementation of the safe transmission protocol shall be restricted to the communication end devices (F-Host or F-CPU – F-Device and /or F-I/O-Module).
- e) There shall always be a 1:1 communication relationship between an F-Device and its F-Host.
- f) The transmission duration times shall be monitored.
- g) Environmental conditions shall be according to general automation requirements mainly IEC 61326-3 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 [52] and meet the requirements of GS-ET-26 [27].

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, 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) Consecutive number ^a	Timeout with receipt ^b	Codename for sender and receiver ^c	Data consistency check ^d
Corruption				X
Unintended repetition	X			
Incorrect sequence	X			
Loss	X	X		
Unacceptable delay		X		
Insertion	X	X	X	
Masquerade		X	X	X
Addressing			X	
Revolving memory failures within switches	X			

^a Instance of "sequence number" of IEC 61784-3.

^b Instance of "time expectation" and "feedback message" of IEC 61784-3.

^c Instance of "connection authentication" of IEC 61784-3.

^d Instance of "data integrity assurance" of IEC 61784-3.

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 the IEC 62280-1 and IEC 62280-2.

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.

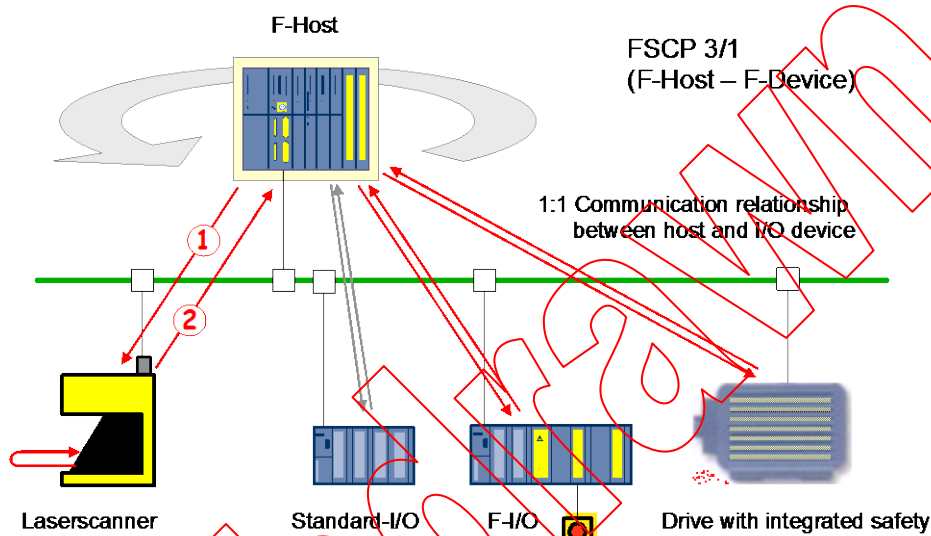


Figure 6 – Standard CPF 3 transmission system

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 (fault) probability under a certain limit. This includes

- Random malfunctions, for example due to EMI impact on the transmission channel
- Failures / faults of the standard hardware
- Systematic malfunctions of components within the standard hardware and software

This principle delimits the certification effort to the "safe transmission functions". The "standard transmission system" (Black Channel) does not need any additional certification.

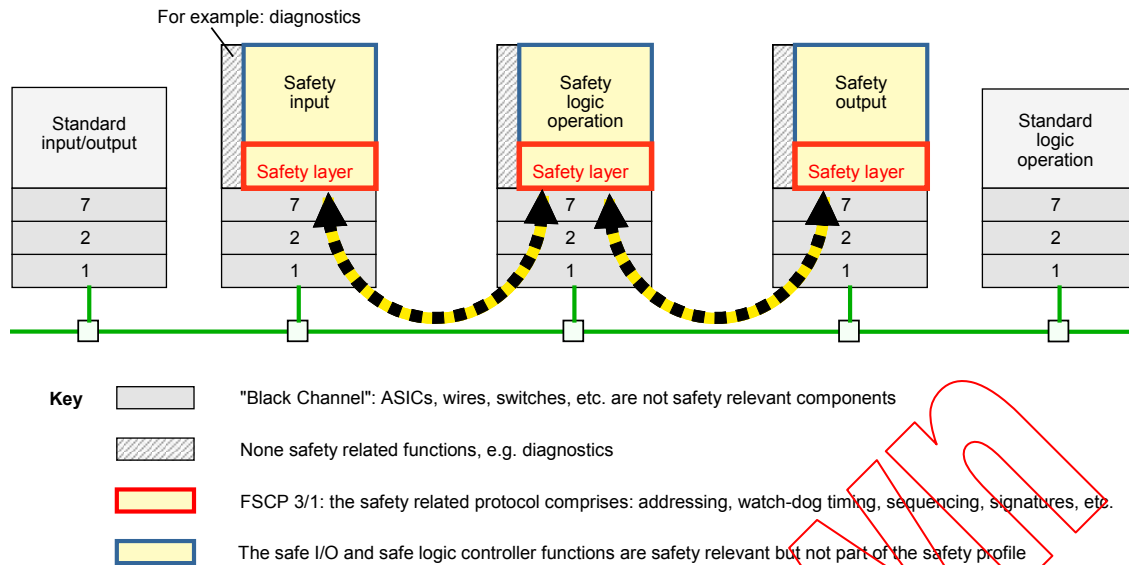


Figure 7 – Safety layer architecture

Transmission is performed via electrical or optical conductors. 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/RTE are shown in Figure 8. While the cyclic safety communication of FSCP 3/1 is using the realtime channels RT or IRT (CP 3/RTE of IEC 61784-2) the other services are using the so-called open channel via TCP/IP or UDP.

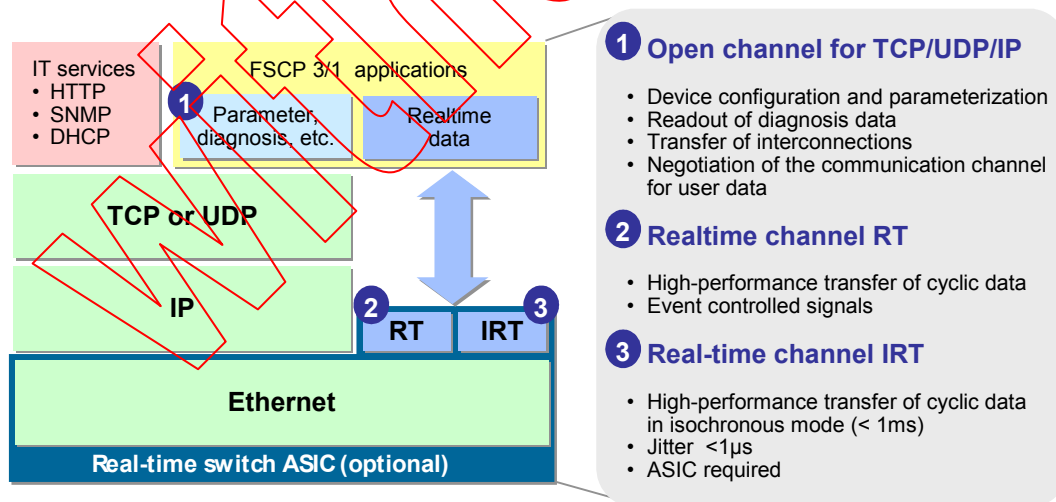


Figure 8 – Basic communication layers

Figure 9 shows the typical (star) topology of one possible CP 3/RTE wiring with multiport switches as hubs. One failing device will not shut down the whole network. However, the wiring effort may be unfavorable.

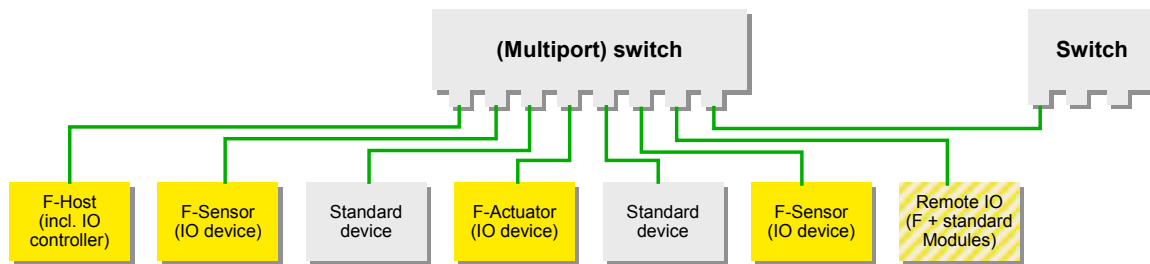


Figure 9 – Multiport switch bus structure

CP 3/RTE provides an alternative via Switch-ASIC that each device may integrate in its communication interface. This way a line topology much like CP 3/1 is possible. In order to avoid a system shut down in case of a failing device a ring structure (Figure 10) is highly recommended. However, in this case some restrictions exist:

- At least one participant within the ring (in Figure 10 the F-Host) shall have a redundancy management to detect any interruption and to reorganize the transmission to the destinations.
- The changeover time of the switch management in such a case shall not exceed the minimum watchdog time of any F-Device within the same island.

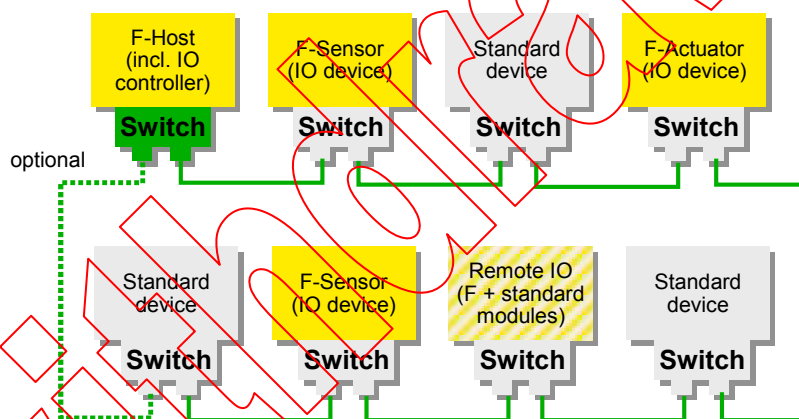


Figure 10 – Linear bus structure

The networks in Figure 9 and Figure 10 belong each to one CP 3/RTE system with one particular IP-Address as the Real-Time protocol (RT or IRT) in layer 2 cannot pass beyond this IP-Address space (Figure 8). It is the (OSI layer 3) task of routers to redirect messages on an IP-Address level (Figure 11). Thus routers are natural borders for CP 3/RTE systems. The following restrictions apply for FSCP 3/1.

- Wireless LAN permitted. However, uniqueness of F-addresses shall be guaranteed within islands
- Switches are not permitted, which allow crossing of network borders (islands)
- Single port routers are not permitted (7.3.9).

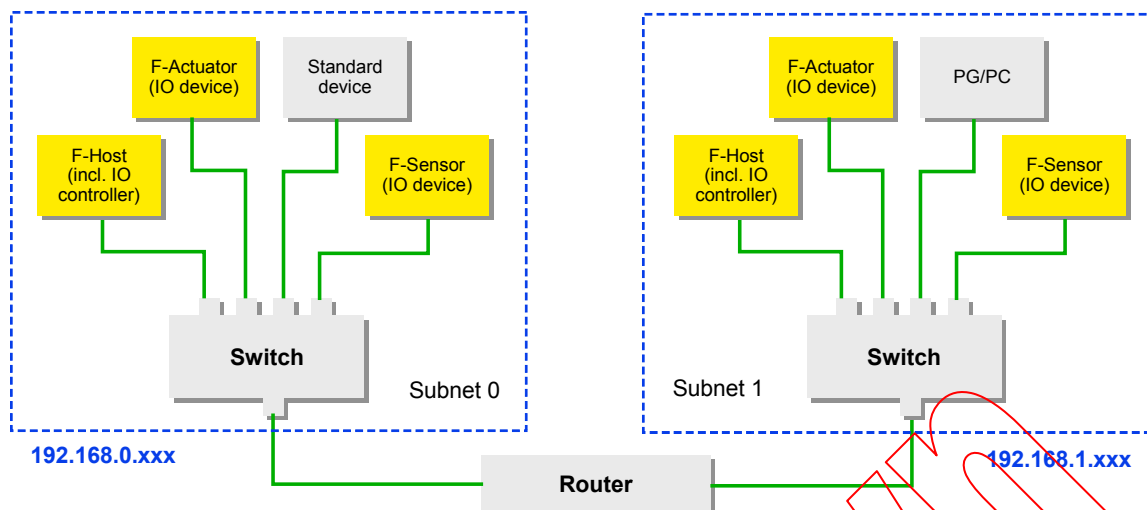


Figure 11 – Crossing network borders with routers

In contrast to the typical fieldbus system configuration, Figure 12 shows the possible bus structure, i.e. how far the safety profile extends 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 across its backplane bus via CP 3/RTE (PN IO) into the IO device and across a possible other backplane into the final F-Module. 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.

NOTE See [42] for details of the V1-mode on CP 3/1.

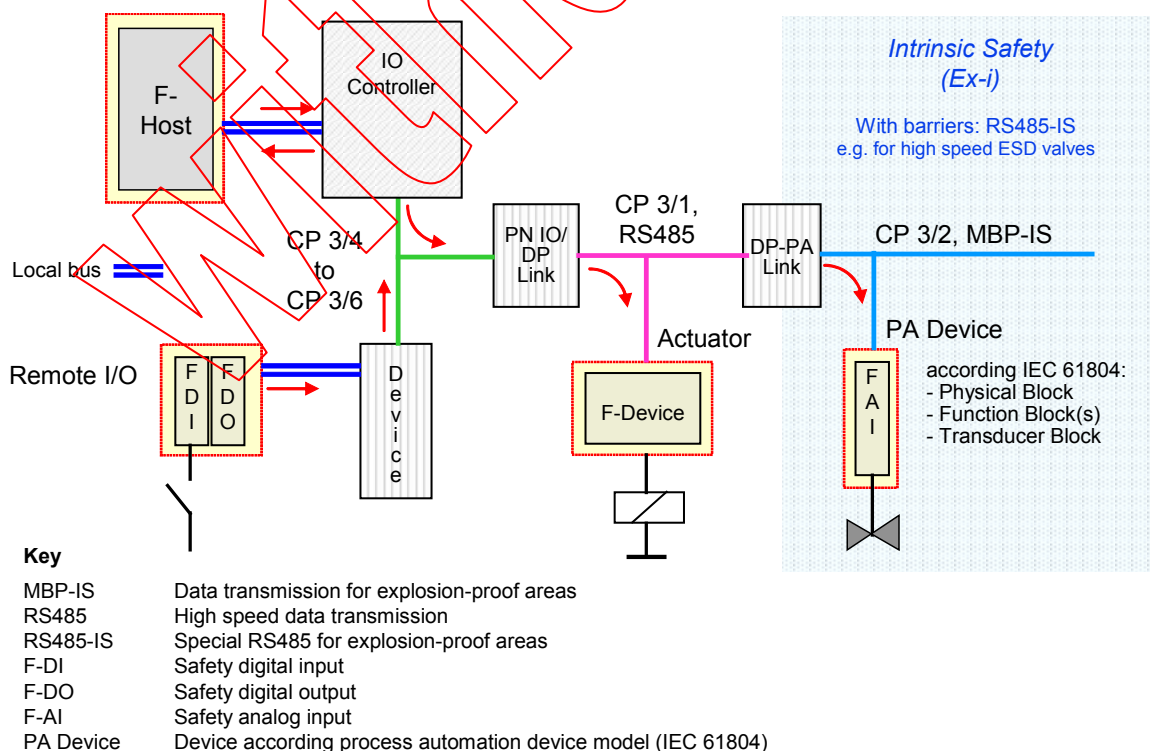


Figure 12 – Complete safety transmission paths

5.5 Relationships with FAL (and DLL, PhL)

5.5.1 Device model

The CP 3/RTE as well as the CP 3/1 device model is assuming one or several application processes (AP) within the device. Figure 13 is showing 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 slots and subslots as needed to represent the physical I/Os of the device. In contrast to CP 3/1, CP 3/RTE provides one hierarchical level more: the subslots.

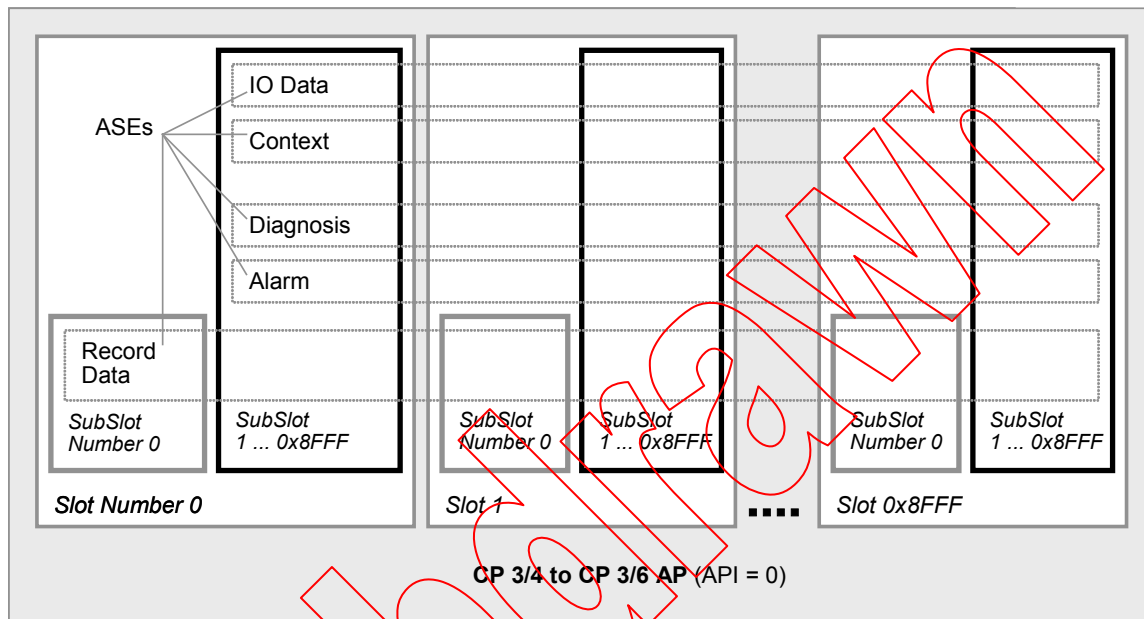


Figure 13 – Device model

Within the subslots, 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. The device manufacturer is responsible for the actual mapping of the device functionality to the CP 3/RTE device model (assignment of slots and subslots) via its GSD file.

5.5.2 Application and communication relationships

In order to use the services mentioned above, it is always necessary to establish an application relationship (AR), and within this AR, communication relationships (CR) for the data objects to be exchanged between the stations (Device, IO Controller) via ASEs. Figure 14 shows an example of the basic structure of a modular IO-Device and possible application relationships to IO-Controllers.

An IO-Controller uses a "Connect" frame within a special CP 3/RTE message to initiate the establishment of an AR during system start-up. Thereby it transfers the following data set to the device.

- General communication parameters of this Application Relationship (AR)
- Communication Relationships (CRs) to be established, including their parameters
- Model and mapping data of the device
- Alarm CRs to be established, including their parameters.

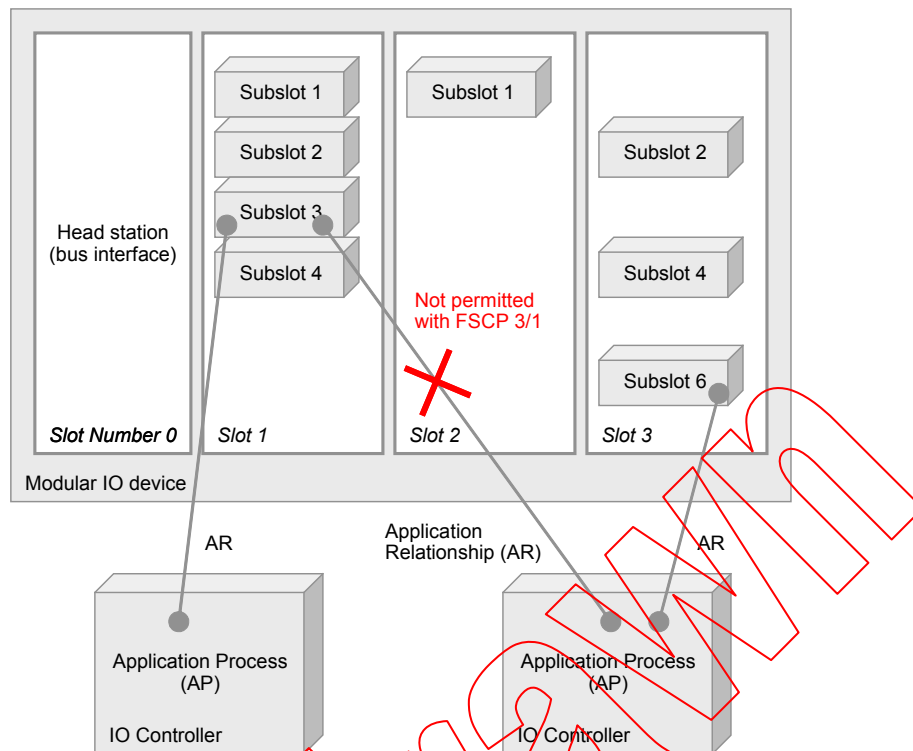


Figure 14 – Application relationships of a modular device

The IO device checks the received data and establishes the required CRs. Possibly occurring errors are reported back to the IO controller. Data exchange begins with the positive acknowledgement of the device to a "Connect" call. Two FSCP 3/1 ARs from different APs to one subslot are not permitted.

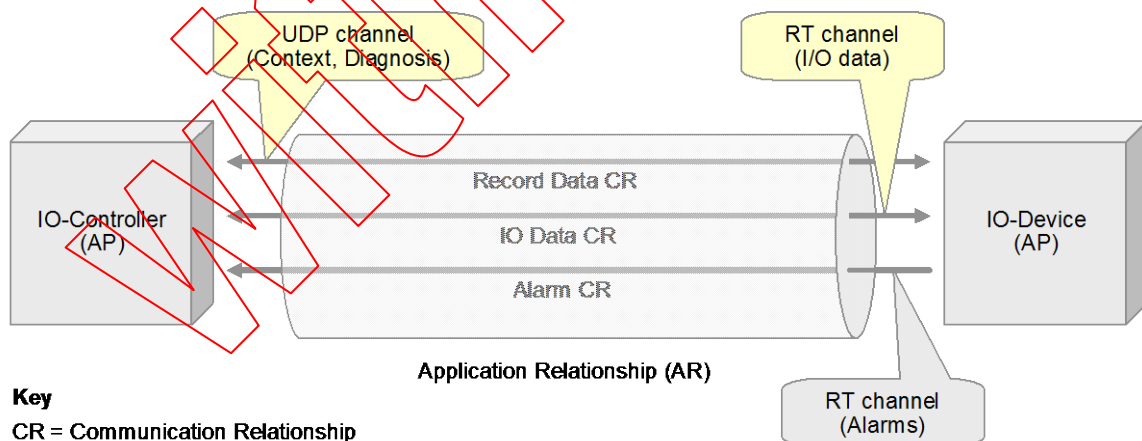


Figure 15 – Application and communication relationships (AR/CR)

At this time, IO data could still be indicated as invalid, because the start-up parameter assignment of the IO devices is still lacking. Following the "Connect" call, the IO controller transfers the start-up parameter assignment data (Context) to the IO device over the Record Data CR (Figure 15). The IO controller uses one "write frame" per configured submodule and finalizes the transfer with an "end of parameterization". In return, the IO device acknowledges the positive start-up parameter assignment with an "application ready". From now on, the AR is established.

5.5.3 Message format

The CP 3/RTE message format for realtime data exchange is shown in Figure 16. A frame check sequence (FCS) of 32 bit is securing the transmission across the network. FSCP 3/1 is not taking any benefit of this measure.



Figure 16 – Message format

5.5.4 Data types

CPF 3 uses the basic data types listed in Table 2. For safety reasons only a restricted number of data types can be used for FSCP 3/1.

Table 2 – Data types used for FSCP 3/1

Data type name	Number of octets	Used in
Integer8	1	
Integer16	2	V1- and V2-mode
Integer32	4	V2-mode
Integer64	8	
Unsigned8 (used as bits)	1	V1- and V2-mode
Unsigned16 (used as bits)	2	V2-mode
Unsigned32 (used as bits)	4	V2-mode
Unsigned16	2	
Unsigned32	4	
Unsigned 64	8	
Float32	4	V1- and V2-mode
Float64	8	
Date		
TimeOfDay with date indication		
TimeOfDay without date indication		
TimeDifference with date indication		
TimeDifference without date indication		

Data type name	Number of octets	Used in
NetworkTime		
NetworkTimeDifference		
Visible String	1,2,3, ...	
Unsigned8+Unsigned8	2	V1- and V2-mode
Float32 + Unsigned8 (enumerated)	5	V1- and V2-mode
F_MessageTrailer4Byte	4	V1- and V2-mode
F_MessageTrailer5Byte	5	V2-mode

Data types for usage within the V2-mode are restricted to Unsigned8, Unsigned16, Unsigned32, Integer16, Integer32, Float32 and the composed data type Float32 + Unsigned8.

Single bits to be coded within an Unsigned8, Unsigned16, or Unsigned32 data type due to its higher efficiency in comparison to the data type Boolean.

6 Safety communication layer services

6.1 F-Host services

Figure 17 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 driver and the corresponding partner within an F-Device is identified by a unique *codename* (one of the F-Parameters).

The whole standard CPF 3 communication equipment between F-Drivers belongs to the "Black channel". The arrows in Figure 17 are indicating the cyclic data transport 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. As an acknowledgment, the F-Input merely receives the safety addenda (safety code).

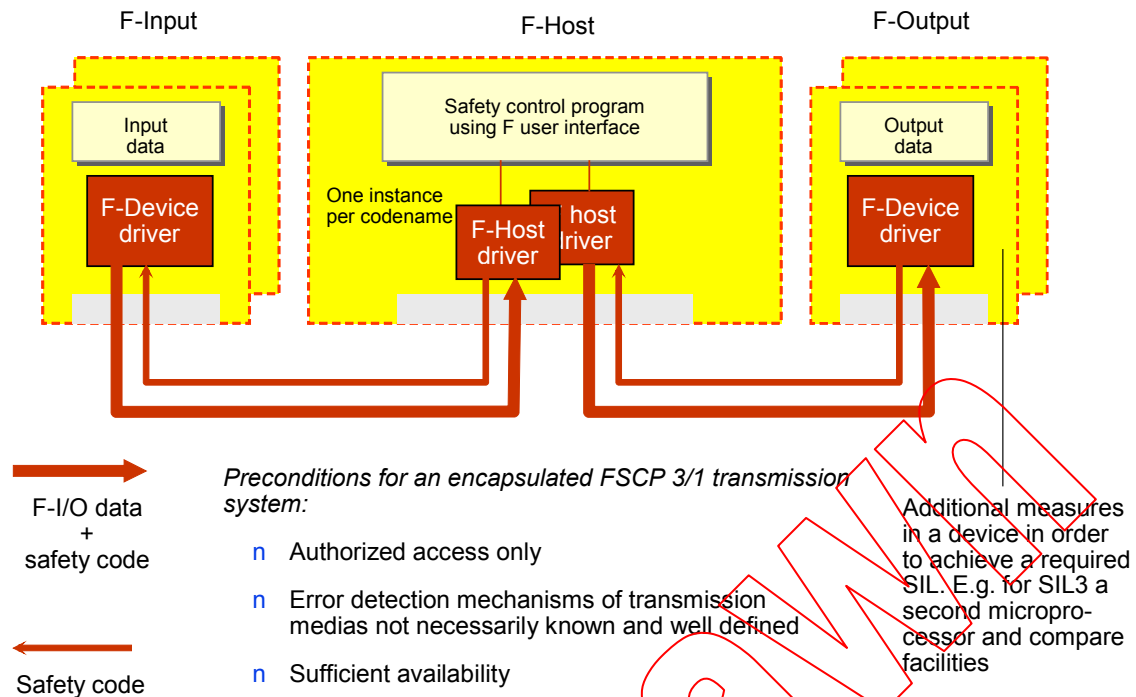


Figure 17 – FSCP 3/1 communication structure

Accordingly, the F-Output receives the safety addenda in addition to the F-Output data, and uses it for acknowledgment.

Safety PDU management and F-Parameterization are tasks of the F drivers within the F-Host and the F-Devices. Figure 18 shows the F user interface at the safety control program level.

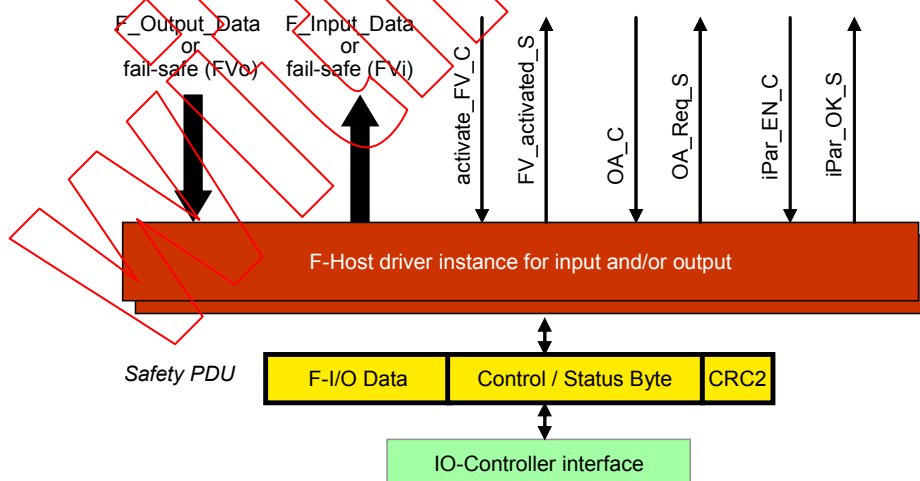


Figure 18 – F user interface of F-Host driver instances

There are several variables available to the programmer to manipulate 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 59. 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 control program in accordance with 9.9:

<i>activate_FV_C</i>	Every safety control program that deals with a corresponding F-Device shall use this variable (type: bit). With input devices (for example sensors) this variable set to "1" causes the driver to deliver fail-safe values ("0") to the F control program. With output devices (for example actuators) this variable set to "1" causes the driver to send fail-safe values ("0") to the device and to set bit 4 of the Control Byte to "1". The safety concept of the output device defines the kind of information of these two that shall be used to achieve the safe state.
<i>FV_activated_S</i>	Every F control program that deals with a corresponding F-Device shall use this variable (type: bit). With input devices this variable indicates via "1" the driver is delivering fail-safe values ("0") to the F-Host program for every input value. Hint: in order to handle inputs individually special qualifier bits may be added to the input data. With output devices this variable indicates via "1" that every output 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). Hint: in order to handle outputs individually (for example motor axes) special qualifier bits may be used.
<i>iPar_EN_C</i>	This variable (type: bit) set to "1" allows an F control program to switch the F-Device into a mode during which it will accept iParameters. It is directly related to the control signal "iPar_EN" (= bit 0 of the Control Byte) and does not affect the F-Host states. If necessary, the variable "activate_FV_C" shall be set to "1" also.
<i>iPar_OK_S</i>	This variable (type: bit) indicates to the F control program the end of iParameterization and the readiness to resume safe I/O data exchange (Figure 40). It shall be updated with the value of "iPar_OK" within the transitions T4, T8, and T17 of the F-Host state machine if the Status bit 1 "Device_Fault" is not set. Otherwise it holds the previous value. It does not affect the F-Host states. The variables "iPar_EN_C" and "activate_FV_C" can be reset.
<i>OA_C</i> (Operator Acknowledgment)	Every F control program shall use this variable (type: bit). In changing this variable to "1" the user is able to resume a safety function after a fault reaction (fail-safe control loop specific) via an F-Host user program.
<i>OA_Req_S</i>	This variable (type: bit) indicates a request for acknowledgement prior to the resumption of a safety function. In case the F-Host driver or an F-Device detects a communication error or an F-Device fault, fail-safe values will be activated. The F-Device driver then sets the variable <i>OA_Req_S</i> (= "1") as soon as the fault/error has been eliminated and operator acknowledgement is possible. Once the acknowledgement occurred (<i>OA_C</i> = "1") the F-Device driver will reset the request variable <i>OA_Req_S</i> (= "0").
<i>Input values</i>	PVi Process input values (←F-Input_Data_D, see Figure 19) FVi Fail-safe input values, used instead of PVi for F-Input_Data_D (Figure 19)
<i>Output values</i>	PVo Process output values (→F-Output_Data_D) FVo Fail-safe output values (=0), used instead of PVo for F-Output_Data_D

Figure 19 illustrates details of the F-Device driver and how it is embedded between the CP 3/RTE interface and the safety part of the specific device application. During the start-up phase the non-safety part of the specific device application receives the F-Parameters and passes them down to the F-Device driver. The driver itself, after checking some of the F-Parameters passes the F-Parameters "F_iPar_CRC" and "F_SIL" up to the safety part of the specific device application. Usually the specific device application provides a time base (1ms) to the F-Device driver in order to feed the watchdog timers.

The F-Device driver mainly deals with safety PDUs that are received or transmitted via the realtime IO Data Communication Relationship of CP 3/RTE (5.5.2). The F I/O 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, CB1, CB2, CB4, and CB5. Some of these signals are passed through to the application interface without interaction. An indication of a new Consecutive Number is provided to facilitate the implementation of demands with sufficient duration (at least one FSCP 3/1 cycle = two different Consecutive Numbers).

In return safety PDUs are prepared for transmission. They are containing Status Bytes with Status Bits SB0 ...SB5. One of these is passed through, the driver is generating some of them, and some are coming from the application interface with driver manipulation before the entry into the safety PDU. Driver Fault is set in case of an internal fault of the driver.

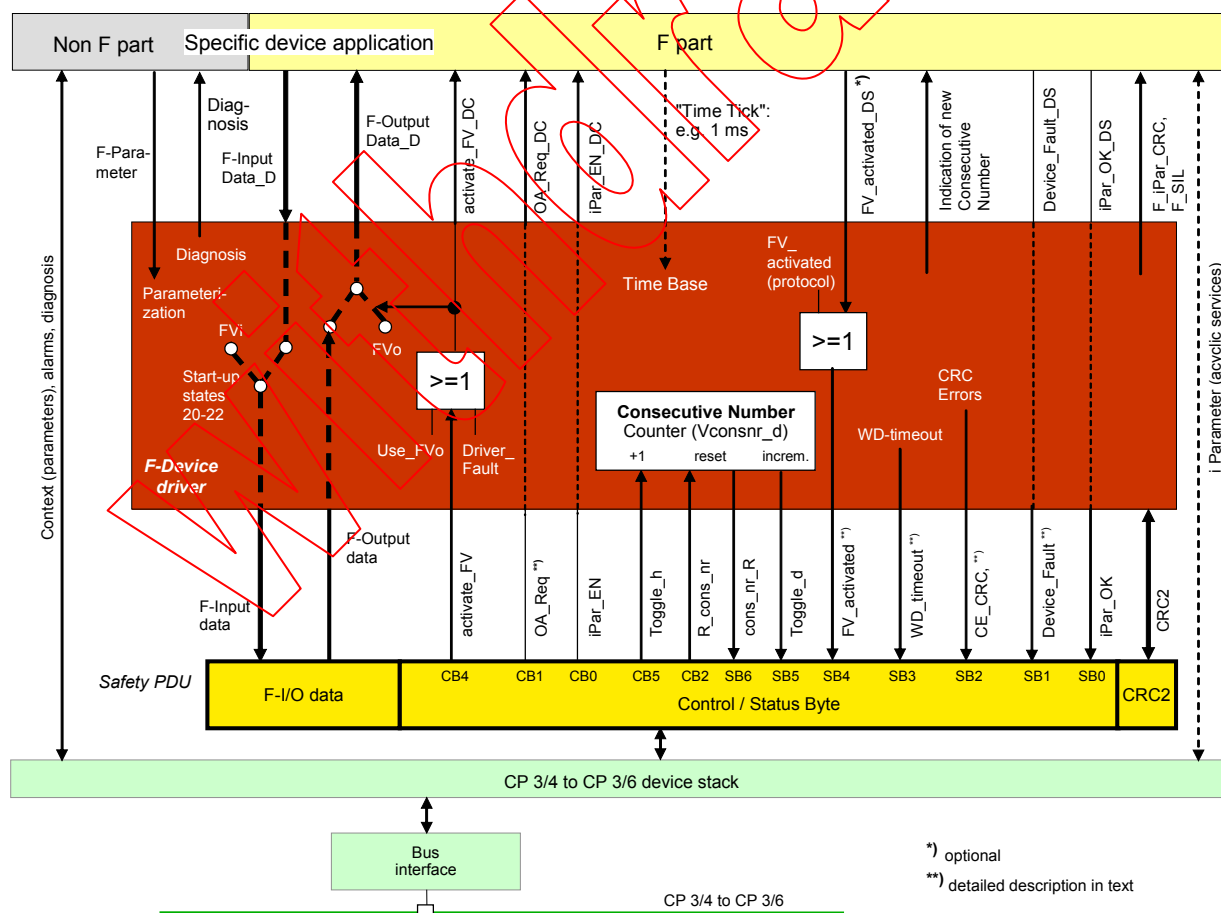


Figure 19 – F-Device driver interfaces

The consecutive number counter is incremented (x+1) when "Toggle_h" is changing its state (0→1; 1→0). R_cons_nr = "1" will reset the counter ("0"). The counter being incremented 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-Device 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.

Hint: in order to handle inputs individually, special qualifier bits may be added to the input data. For output devices this variable indicates via "1" that every output 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 every input value and every output is set to fail-safe values.

OA_Req_DC The F-Device application shall use this non-safety-related variable to indicate locally the request for an operator acknowledgement (OA_C within F-Host) usually via a LED. Implementation is optional for F-Devices.

iPar_EN_DC This variable if set to "1" indicates a parameterization request (F-Device needs new iParameters)

iPar_OK_DS This variable if set to "1" indicates that the F-Device (its specific device application) has new iParameter values assigned

Device_Fault_DS Fault recognized by the specific device application

6.3 Diagnosis

6.3.1 Safety alarm generation

Due to fast polling cycles of the user program, the speed of detecting modifications of the F I/O 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-Device safety layer diagnosis including the iPar-Server

In order to report diagnosis information of the FSCP 3/1 F-Device driver to a human machine interface device, the driver passes its information to the F-Device application which is using standard CP 3/RTE mechanisms for propagation to the IO-Controller. Every standard diagnosis option of CP 3/RTE is possible, preferably the Channel-Related-Diagnosis. There is a reserved area for FSCP 3/1 within the coding table of the field "ChannelErrorType".

Table 3 shows the different types of diagnosis information of the FSCP 3/1 protocol layer within F-Devices.

Table 3 – Safety layer diagnosis messages

Hex	Number	Diagnosis Information
0x0040	64	Mismatch of safety destination address (F_Dest_Add)
0x0041	65	Safety destination address not valid (F_Dest_Add)
0x0042	66	Safety source address not valid (F_Source_Add)
0x0043	67	Safety watchdog time value is 0 ms (F_WD_Time)
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	CRC1-Fault
0x0048	72	Device specific diagnosis information, see manual
0x0049	73	Save iParameter watchdog time exceeded
0x004A	74	Restore iParameter watchdog time exceeded
0x004B	75	Inconsistent iParameters (iParCRC error)
0x004C	76	Reserved: do not use numbers, do not evaluate numbers
0x004D	77	Reserved: do not use numbers, do not evaluate numbers
0x004E	78	Reserved: do not use numbers, do not evaluate numbers
0x004F	79	Reserved: do not use numbers, do not evaluate numbers

F-Devices using the iPar-Server mechanism to store and retrieve iParameters within an F-Host or its controlled subsystem can report dedicated diagnosis information via separate additional codings. It is highly recommended for F-Devices to use these types within diagnosis messages. However, diagnosis messages can carry summary information for several individual causes.

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

7 Safety communication layer protocol

7.1 Safety PDU format

7.1.1 Safety PDU structure

Figure 20 shows the structure of one single safety PDU that contains the safety input/output data and an additional safety code. A CP 3/RTE message may contain several safety PDUs, for example in case of modular IO devices with several safety modules.

Factory automation and process automation place different requirements upon a safety system. The former deals with short binary I/O ("bit") usually processed at a very high speed; the latter involves longer I/O values ("floating point") that may take slightly more processing time. FSCP 3/1 therefore offers two different safety input/output data lengths that require CRC protection of different complexity to fulfill SIL3 requirements.

Thus, *two operational modes* can be chosen by parameterization: few F I/O data up to 12 octets together with a 24 bit CRC2 (3 octets) and F (process) I/O data up to 123 octets together with a 32 bit CRC2 (4 octets).

In addition, 4 (5) octets in total are required including the Status/Control Byte and 3 (4) octets for the CRC2 code.

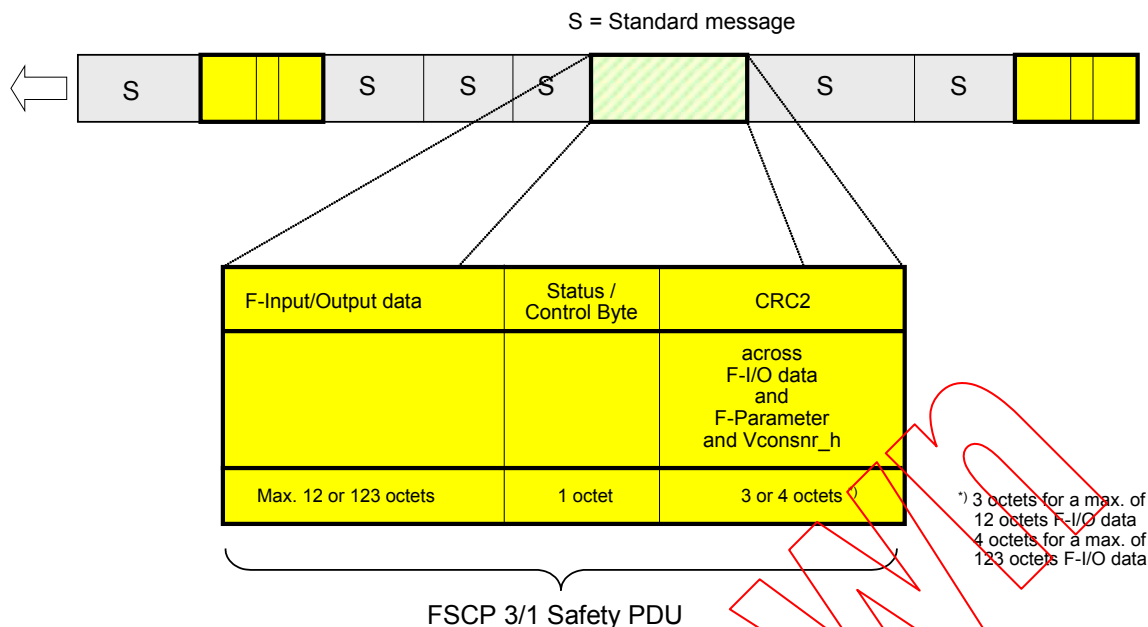


Figure 20 – Safety PDU for CPF 3

Subclauses 7.1.2 through 7.1.6 provide a detailed description of the elements of the safety PDU structure.

7.1.2 Safety I/O data

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

In the case of only a few F I/O data up to 12 octets the 24 bit CRC option shall be chosen by parameterization.

Besides the compact devices, there are *modular devices* with F and standard I/O units and subaddresses (Figure 13 and Figure 14). Their CP 3/RTE head station (DAP), which is considered to be a part of the "Black channel", is used for agreeing the structure of a CP 3/RTE message with several safety PDUs via the start-up parameterization. One safety PDU corresponds to one subplot. The amount of data corresponds to the CP 3/RTE standard amount of data minus 4 or 5 octets respectively. That means for a device head station with m safety modules a reduction of m times 4 or 5 octets respectively.

7.1.3 Status and Control Byte

Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
res	Vconsnr_d has been reset	Toggle Bit	Fail-safe values (FV) activated	Communication fault: WD-timeout	Communication fault: CRC	Failure exists in F-Device or F-Module	F-Device has new iParameter values assigned
-	cons_nr_R	Toggle_d	FV_activated	WD_timeout	CE_CRC	Device_Fault	iPar_OK

Figure 21 – Status Byte

The Status Byte shown in Figure 21 is contained in each safety PDU of a CP 3/RTE submodul transmitted from a device to its controller (Figure 20).

Bit 0 is set when the F-Device (its technology firmware) has new parameter values assigned. Signal name is "iPar_OK".

Bit 1 shall be set by the specific device technology firmware for at least two (2) message cycles, if there is a malfunction in the F-Device. Signal name is "Device_Fault".

Bit 2 is set if the F-Device is recognizing an F communication failure, i.e. if the consecutive number is wrong (detected via CRC2 error in V2-mode) 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 is recognizing an F communication failure, i.e. if the watch dog time in the F-Device 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 error (Figure 19 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 a device-based Toggle Bit indicating a trigger to increment the virtual consecutive number within the F-Host (Vconsnr_h). Signal name is "Toggle_d".

Bit 6 is set when the F-Device has reset its consecutive number counter Vconsnr_d. Signal name is cons_nr_R.

Bit 7 is reserved (res) for future FSCP 3/1 releases.

Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
res	res	Toggle Bit	Fail-safe values (FV) to be activated	res	Reset Vconsnr_d	Operator acknowledge requested	iParameter assignment deblocked
-	-	Toggle_h	activate_FV	-	R_cons_nr	OA_Req	iPar_EN

Figure 22 – Control Byte

The Control Byte shown in Figure 22 is being sent with each safety PDU of a subslot from the IO controller to the device (Figure 20).

Bit 0 is set by the F application within an F-Host in case of a parameterization request (F-Device needs new iParameters)

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-Device to indicate locally the request for an operator acknowledgement (OA_C) usually via a LED (9.1).

Bit 2 is set when the F-Host detects a communication error, either by the Status Byte or by itself. As a consequence thereof the counter of the Virtual Consecutive Number (Vconsnr_d) within the F-Device will be set to "0" (see 7.1.4 and 7.2.5). Bit 2 shall be reset again after an error has gone. Thereafter the consecutive numbering resumes.

Bit 3 is reserved (res) for future FSCP 3/1 releases.

Bit 4 can be set to force the outputs of an F-Device to configured or built-in fail-safe values. See 6.1 for more details.

Bit 5 is a host-based Toggle Bit indicating a trigger to increment the virtual consecutive number within the F-Device (Vconsnr_d). Signal name is "Toggle_h". See 7.1.4 for more details.

Bits 6, 7 are reserved (res) for future FSCP 3/1 releases.

Hint: to avoid hassles with future versions of the FSCP 3/1 devices: Status and Control Bits of type "res" shall be set "0" and ignored by the receiver.

7.1.4 (Virtual) Consecutive Number

The recipient uses the Consecutive Number to monitor whether the sender and the communication channel are still alive. The Consecutive Number is used in an acknowledgment mechanism for monitoring the *propagation times* between sender and recipient. The value "0" is reserved for the first run and for a communication error reaction. In contrast to the V1-mode the V2-mode uses 24 bit counters for the consecutive numbering. Thus, the Consecutive Number counts in a cyclic mode from 1... 0FF FF FFh, wrapping over back to 1 at the end.

NOTE Refer to [42] on details of the V1-mode.

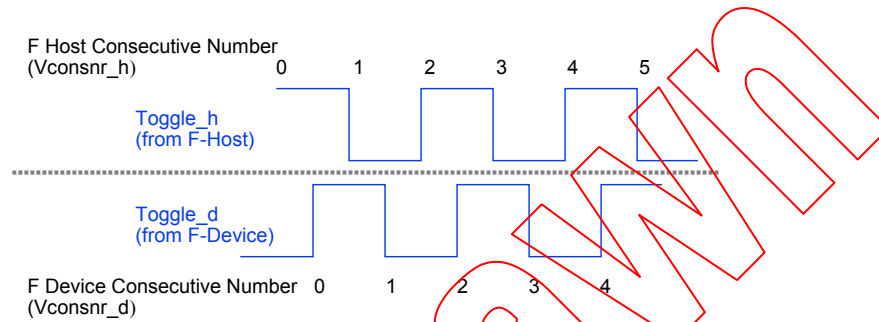


Figure 23 – The Toggle Bit function

Also in contrast to the V1-mode the V2-mode is not transmitting the Consecutive Number with each and every safety PDU. It uses a Virtual Consecutive Number instead. It is called virtual due to the fact that it cannot be seen within the safety PDU. This approach uses 24 bit counters located within the F-Host (Vconsnr_h) and the F-Device (Vconsnr_d) and a Toggle Bit within the Status Byte and the Control Byte to increment the appropriate counters synchronously (Figure 23). The checking for correctness and for the synchronism of the two independent counters is executed by including the consecutive numbers in the CRC2 calculation. CRC2 then is transmitted with each and every safety PDU (Figure 24).

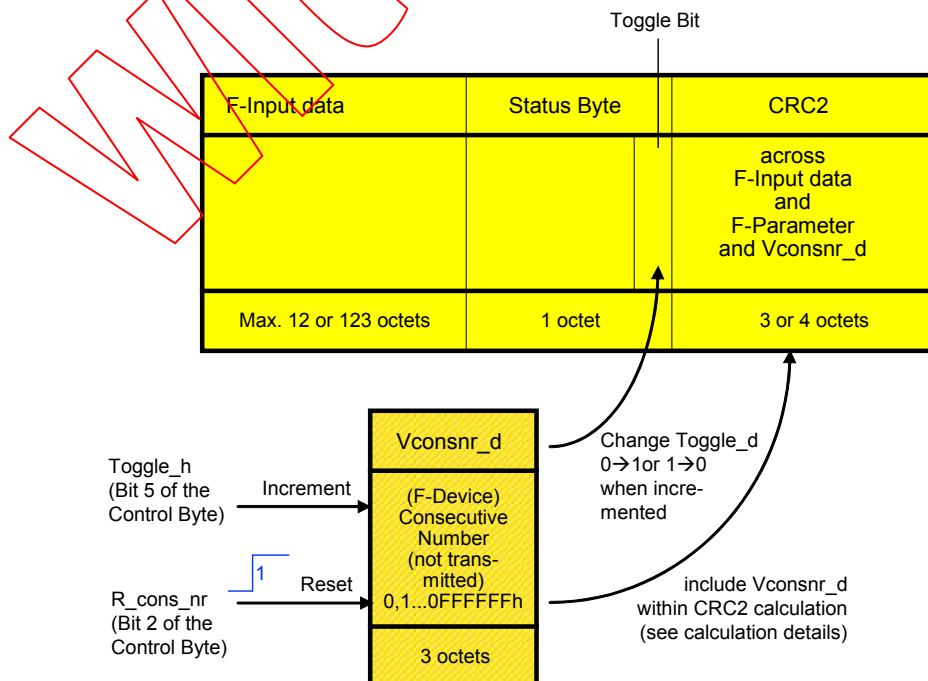


Figure 24 – F-Device Consecutive Number

The transmitted part of the (virtual) consecutive number is reduced to a Toggle Bit, which indicates an increment of the local counter. The counters within F-Host and F-Device are incremented at each edge of the Toggle-Bits (0→1, 1→0). Figure 24 illustrates the mechanism for the counter within the F-Device. The counter is reset to "0" when the F-Host sends $R_cons_nr = "1"$ within the Control Byte (see 7.1.3).

The mechanism for the counter within the F-Host corresponds to the one in the F-Device. However, the counter is reset whenever an error occurs (internally or via Status Byte). The name of this counter is "Vconsnr_h".

7.1.5 CRC2 Signature

Once the F-Parameters (source-destination relationship or codename, SiL, watchdog times, etc.) have been transferred to the F-Device, the identical parameters are employed in an identical procedure in the F-Host and in the F-Device/F-module for producing a 2-octet CRC1 (high octet = 0) signature (CRC1). For information on how this CRC1 is build, see 8.3.3.2. This CRC1 signature, the F I/O data, the Status or Control Byte and the corresponding Consecutive Number (Vconsnr_h or Vconsnr_d) are used for producing another 3-octet / 4-octet CRC2 signature (CRC2) within the F-Host (see Figure 25). The CRC1 signature provides the initial value for the calculation of CRC2 that is transferred cyclically. In the F-Device, the identical CRC signature is generated and the signatures are compared. The subsequent cyclic transfers only require a CRC2 signature comparison (that can be done very rapidly).

Any changes of stored F-Parameters shall be detected and shall lead to a safe state of the F-Device. The detection mechanisms are depending on the individual implementation of F-Devices and are not subject of this part.

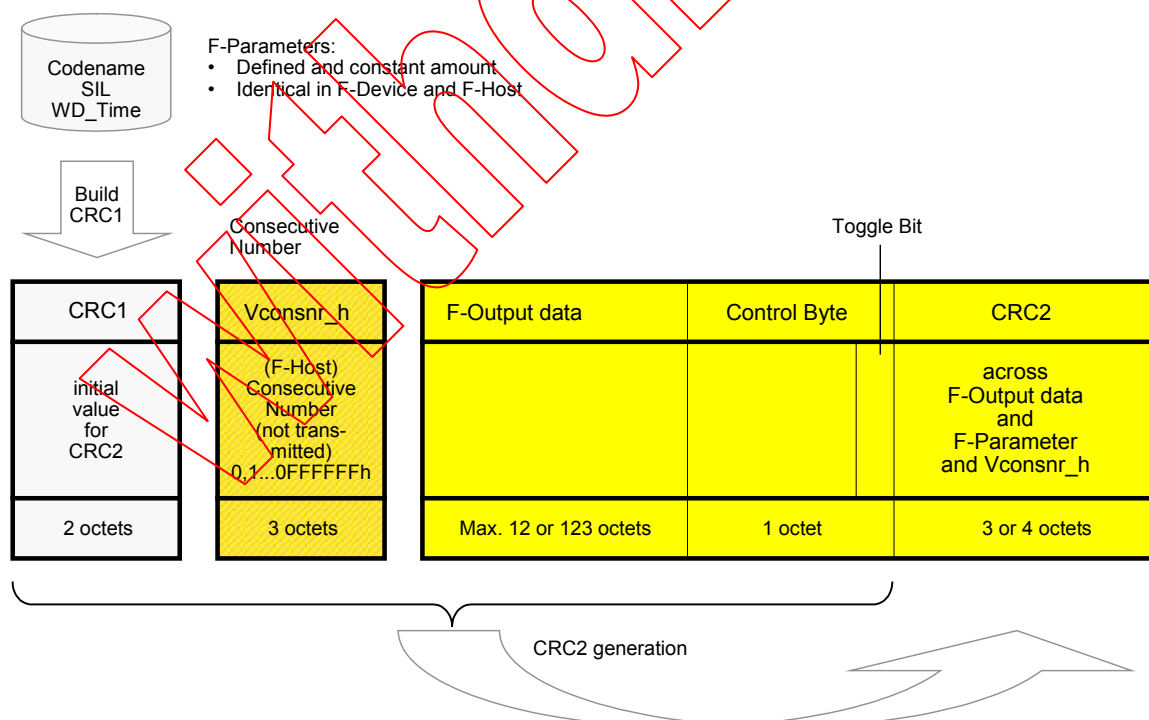


Figure 25 – CRC2 generation (F-Host output)

For better error detection even if there are identical CRC polynomials within the "Black Channel" and in the safety layer, the CRC2 calculation is including the octets of Figure 25 in reverse order (Figure 26). For processing optimization reasons the Consecutive Numbers (Vconsnr_h or Vconsnr_d) are used with 4 octets in the calculations, the additional "padding octet" being "0". A 32-bit counter is not recommended as this would lead to an unacceptable long testing time of the devices during the test and certification process.

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".

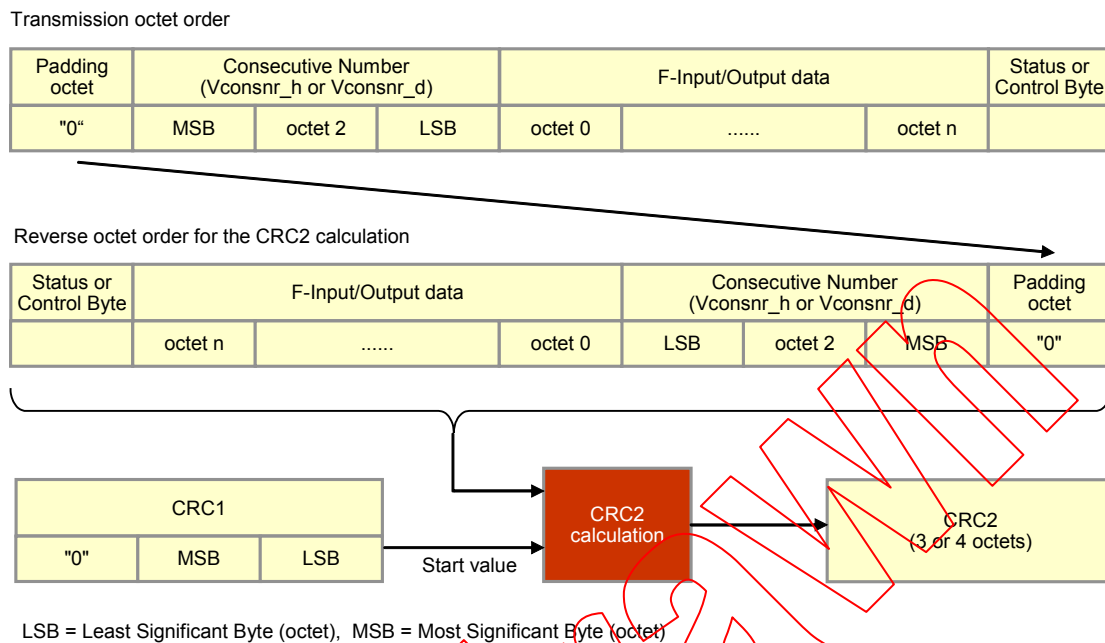


Figure 26 – Details of the CRC2 calculation (reverse order)

7.1.6 Appended standard I/O data

Standard I/O data can be appended to a safety PDU. For compact F-Devices, this can be achieved by allocating separate slot identifications. F-modules within modular devices are able to use this mechanism within CP 3/RTE due to subslot modeling.

7.2 FSCP 3/1 behavior

7.2.1 General

The core of the safety layers within F-Host and F-Device 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 27 shows a simplified model of the safety communication. A special timing diagram in 7.2.5 is illustrating the consequences of a fault on the reset signal for the consecutive number counter. The monitoring of safety PDU transit times is described in 7.2.6.

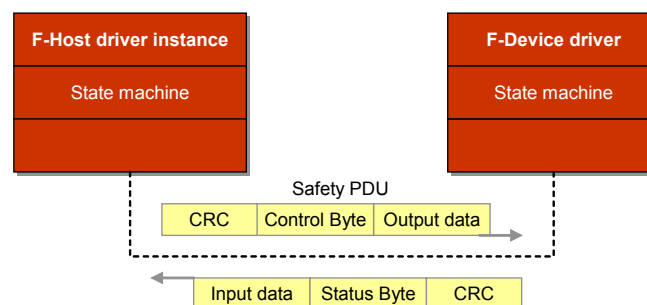


Figure 27 – Safety layer communication relationship

7.2.2 F-Host state diagram

Figure 28 shows the F-Host state diagram and Table 4 describes the F-Host states, transitions, and internal items. The diagrams are following the UML2 notation. 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 acknowledgements are deferred until the next activity state is reached.

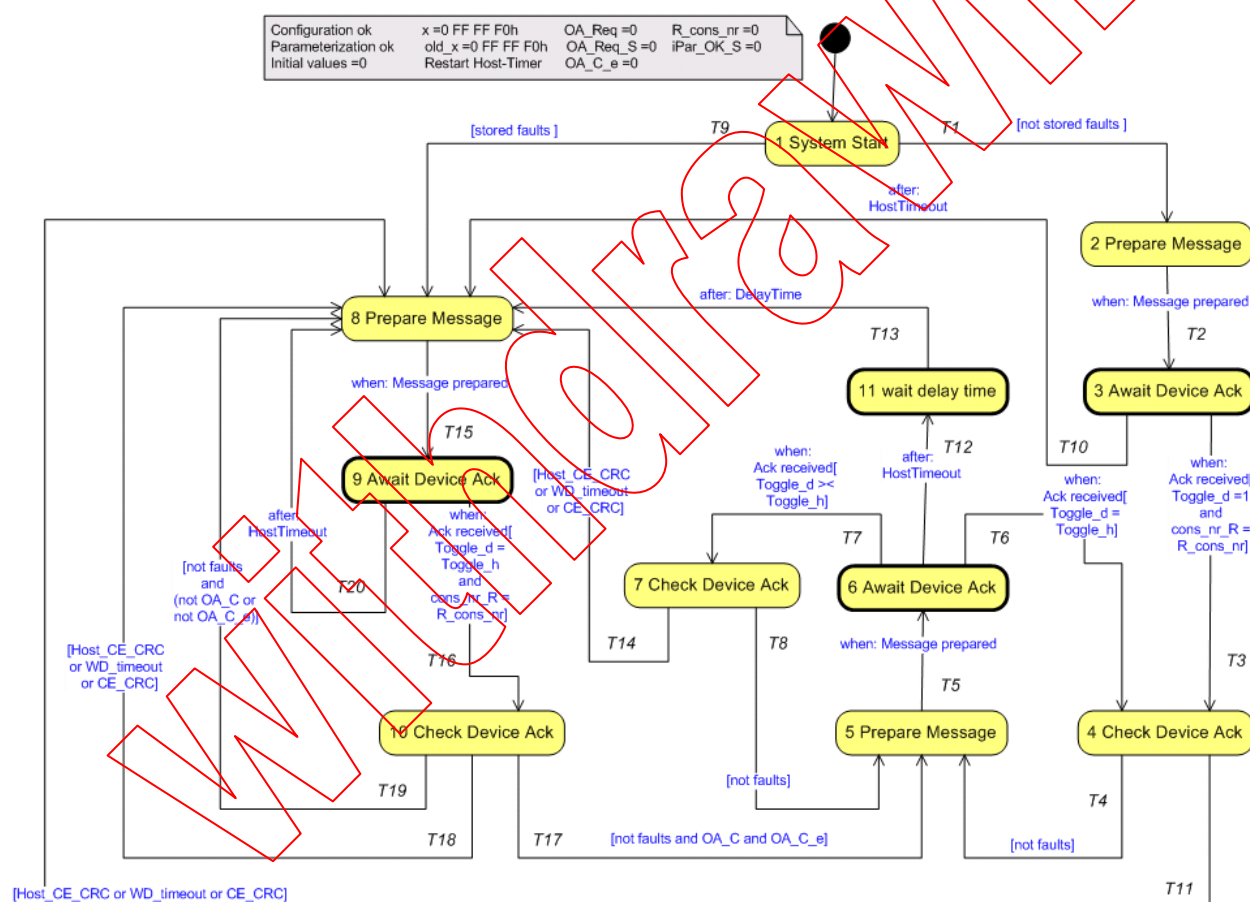


Figure 28 – F-Host state diagram

The terms used in Figure 28 are specified below:

Initial values	any safety PDU values =0
HostTimeout	F-Host recognizes local timeout while awaiting an F-Device acknowledgement
Host_CE_CRC	F-Host recognizes CRC fault while analyzing the received safety PDU
Device_Fault	F-Device reported failure to host; Status Bit 1 =1.
CE_CRC	F-Device reported CRC fault to the F-Host; Status Bit 2 =1
OA_C_e	Auxiliary flag indicating a raising edge of the OA_C signal (0 → 1)
WD_timeout	F-Device reported timeout fault to the F-Host; Status Bit 3 =1
[not faults]	UML notation of a condition (guard) to fire the transition. In this case this variable is true (=1) if none of the following bits are set:

- Host_CE_CRC or
- CE_CRC or
- WD_timeout

[stored faults]

This variable is true (=1) if any of the following bits had been stored:

- Host_CE_CRC or
- HostTimeout or
- CE_CRC or
- WD_timeout

Table 4 – F-Host 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 <i>regular</i> safety PDU for the F-Device	
3	Await Device Ack	Safety Layer is waiting on next regular safety PDU from F-Device (Acknowledgement).	
4	Check Device Ack	Check received safety PDU for a <i>CRC-error</i> (Host_CE_CRC) including virtual consecutive number (x) and for potential <i>F-Device faults</i> within the Status Byte (WD_timeout, CE_CRC)	
5	Prepare Message	Preparation of a <i>regular</i> safety PDU for the F-Device	
6	Await Device Ack	Safety Layer is waiting on next regular safety PDU from F-Device (Acknowledgement)	
7	Check Device Ack	Check received safety PDU for a <i>CRC-error</i> (Host_CE_CRC) including previous (old_x) virtual consecutive number and for potential <i>F-Device faults</i> within the Status Byte (WD_timeout, CE_CRC)	
8	Prepare Message	Preparation of a safety PDU for the F-Device (exception handling)	
9	Await Device Ack	Safety Layer is waiting on next irregular safety PDU from F-Device (Acknowledgement)	
10	Check Device Ack	Check received safety PDU for a <i>CRC-error</i> (Host_CE_CRC) including virtual consecutive number (x) and for potential <i>F-Device faults</i> within the Status Byte (WD_timeout, CE_CRC). Once a fault occurred, no automatic restart of a safety function is permitted unless an operator acknowledgement 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 acknowledgement with the next power-on. A delay time of 0ms 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	restart host-timer
T4	4	5	old_x =x, x =x+1, if x =01000000h then x =1 Toggle_h = not Toggle_h, if FV_activated =1 or activate_FV_C =1 or Device_Fault =1 then use FVi, FV_activated_S =1 else use PVi, FV_activated_S =0 if activate_FV_C =1 or Device_Fault =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 FV_activated =1 or activate_FV_C =1 or Device_Fault =1 then use FVi, FV_activated_S =1 else use PVi, FV_activated_S =0 if activate_FV_C =1 or Device_Fault =1 then use FVo, activate_FV =1 else use PVo, activate_FV =0 iPar_OK_S =iPar_OK