IEC 61784-3-3

Edition 2.0 2010-06

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

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

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

IEC 61784-3-3:2010

IEC Central Office
3, rue de Varembé
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It also gives information on projects, replaced and withdrawn publications.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.

IEC 61784-3-3

Edition 2.0 2010-06

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

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

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

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

PRICE CODE
CODE PRIX XF

ICS 25.040.40, 35.100.05

ISBN 978-2-88912-943-0

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES –

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

FOREWORD

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

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 second edition cancels and replaces the first edition published in 2007. This edition constitutes a technical revision. The main changes with respect to the previous edition are listed below:

— updates in relation with changes in IEC 61784-3;
— introduction of a secondary watchdog timer (F_WD_Time_2) to cover the use cases 'configuration-in-run', or 'maintenance of fault tolerance systems', or both (7.1.3, 7.2.3, 7.2.6, 8.1.1, 8.1.4, 8.1.6.2);
— missing GSDL definitions conveyed from other approved documents (8.3.2.1);
— missing CRC signature calculation for a GSD conveyed from other approved documents (8.3.3.3);

— constraints for the parameter value assignment of the primary watchdog timer 'F_WD_Time' (9.3.3);

— identification of the safety parameterization state of an F-Device or F-Module via field IM4 (signature) within the I&M functions (9.6.2);

— updated documents in bibliography.

This bilingual version (2012-02) corresponds to the monolingual English version, published in 2010-06.

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

FDIS	Report on voting
65C/591A/FDIS	65C/603/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.

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

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

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

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

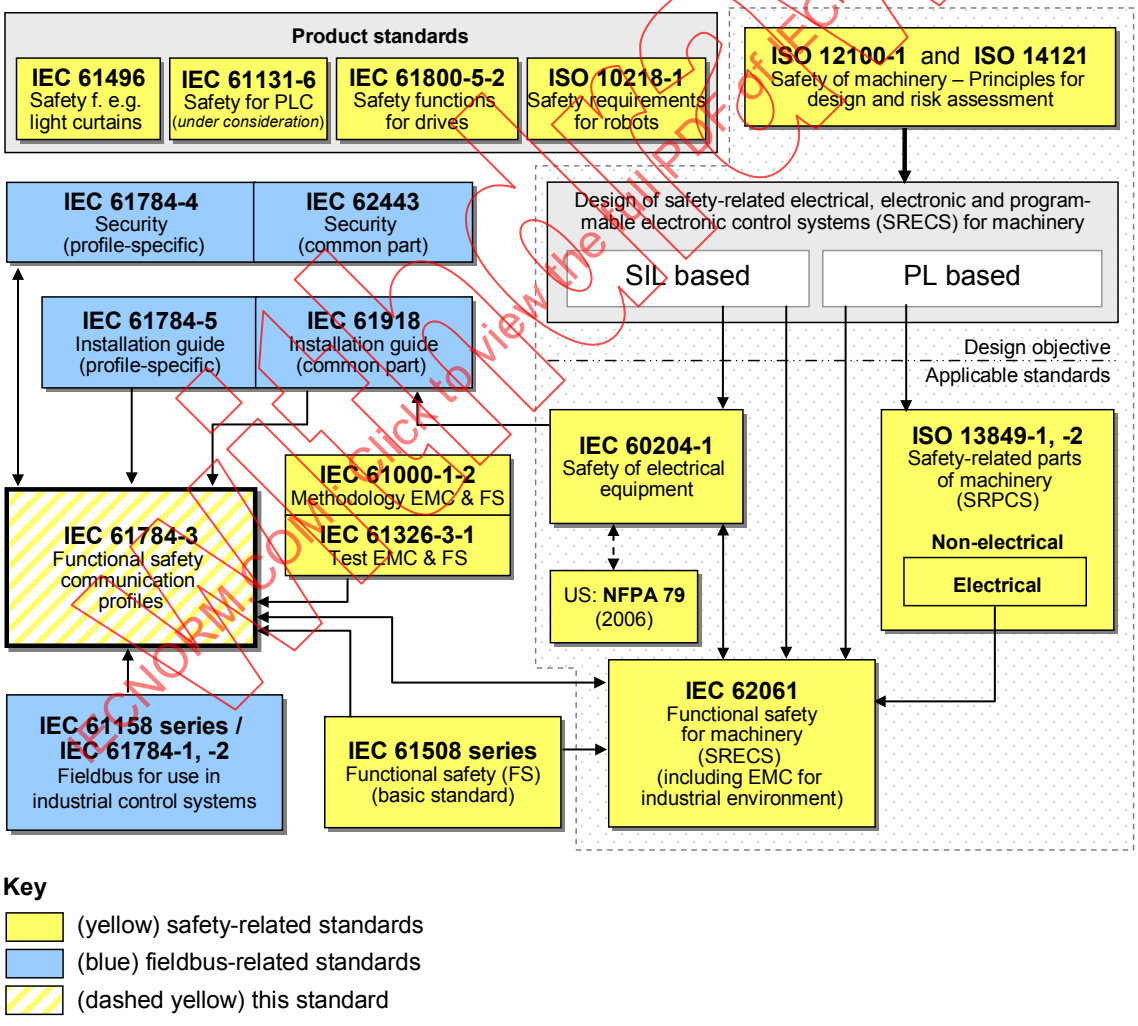
0 Introduction

0.1 General

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

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

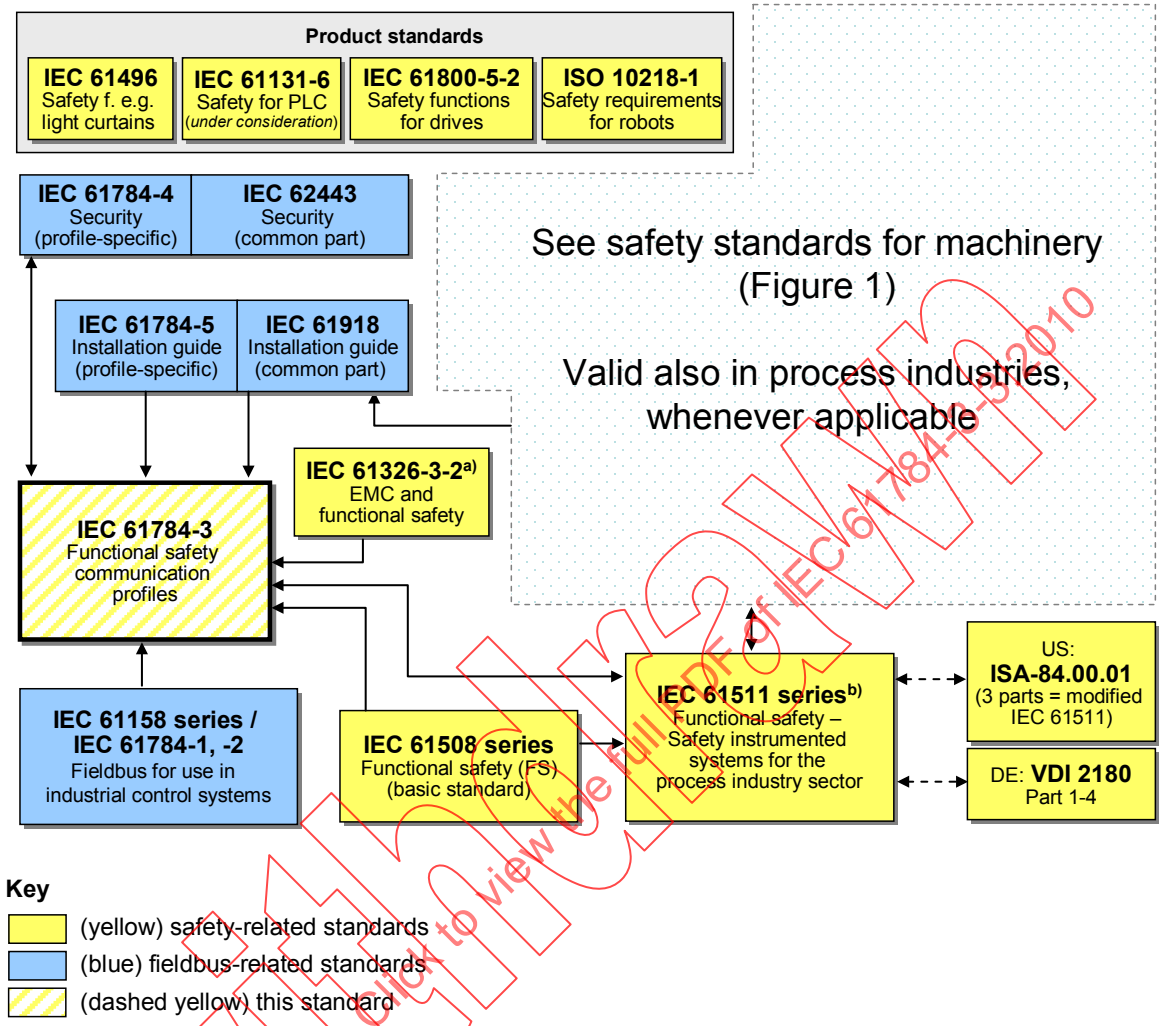
Figure 1 shows the relationships between this standard and relevant safety and fieldbus standards in a machinery environment.



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

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

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



[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.

0.2 Patent declaration

The International Electrotechnical Commission (IEC) draws attention to the fact that it is claimed that compliance with this document may involve the use of patents concerning the functional safety communication profiles for family 3 as follows, where the [xx] notation indicates the holder of the patent right:

EP1267270-A2	[SI]	Method for data transfer
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
EP1686732	[SI]	Method and system for transmitting protocol data units
EP1802019	[SI]	Identification of errors in data transmission
EP1921525-A1	[SI]	Method for operation of a safety-related 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
I IA AS FA TC
76187 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.

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

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

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

2 Normative references

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

IEC 61784-5-3, *Industrial communication networks – Profiles – Part 5-3: 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*

---

3 In preparation.

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*

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

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

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*

3 Terms, definitions, symbols, abbreviated terms and conventions

3.1 Terms and definitions

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

3.1.1 Common terms and definitions

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

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

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

3.1.1.4
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 [32], [33][4].

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

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

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

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

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

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

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

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

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

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

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

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.

---

4 Figures in square brackets refer to the bibliography.

5 To be published.

NOTE 2 See also [32], [33].

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

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

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

[IEC/TR 62210, modified]

3.1.1.15
hazard
state or set of conditions of a system that, together with other related conditions will inevitably lead to harm to persons, property or environment

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

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

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

3.1.1.21
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]

3.1.1.22
redundancy
existence of means, in addition to the means which would be sufficient for a functional unit to perform a required function or for data to represent information

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

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

3.1.1.23
reliability
probability that an automated system can perform a required function under given conditions for a given time interval (t1,t2)

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

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

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

NOTE 4 Reliability differs from availability.

[IEC 62059-11, modified]

3.1.1.24
risk
combination of the probability of occurrence of harm and the severity of that harm

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

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

3.1.1.25
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

3.1.1.26
safety connection
connection that utilizes the safety protocol for communications transactions

3.1.1.27
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.

3.1.1.28
safety device
device designed in accordance with IEC 61508 and which implements the functional safety communication profile

3.1.1.29
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

6 To be published.

NOTE An SELV circuit is not connected to protective earth.

[IEC 61131-2]

3.1.1.30
safety function
function to be implemented by an E/E/PE safety-related system or other risk reduction measures, that is intended to achieve or maintain a safe state for the EUC, in respect of a specific hazardous event

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

[IEC 61508-4:2010, modified]

3.1.1.31
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 61784-3:2010[7], 5.2.4 and addressed by the functional safety communication profiles defined in this part.

3.1.1.32
safety integrity level (SIL)
discrete level (one out of a possible four), corresponding to a range of safety integrity values, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest

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

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

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

[IEC 61508-4:2010]

3.1.1.33
safety measure
<this standard> measure to control possible communication *errors* that is designed and implemented in compliance with the requirements of IEC 61508

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

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

3.1.1.34
safety-related application
programs designed in accordance with IEC 61508 to meet the SIL requirements of the application

3.1.1.35
safety-related system
system performing *safety functions* according to IEC 61508

---

7 In preparation.

8 To be published.

3.1.1.36
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

3.1.1.37
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 (Binary Digit)
encoded binary information without a technical unit

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

NOTE Depending on a particular safety function, de-energizing may not be the only possibility for a fail-safe state.

3.1.2.13
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

3.1.2.14
F-Driver
software administering safety PDUs within F-Hosts and F-Devices according to the FSCP 3/1 specifications

3.1.2.15
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.

3.1.2.16
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.

3.1.2.17
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

3.1.2.18
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.

3.1.2.19
function block (FB)
self-contained program part possessing a specific functionality

3.1.2.20
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

3.1.2.21
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.

3.1.2.22
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.

3.1.2.23
IO-Module
addressable sub input/output unit within a modular IO-Device

3.1.2.24
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.

3.1.2.25
IO-System
IO-Controller and its associated IO-Devices

3.1.2.26
iParameter
individual or technology specific F-Device parameters

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

3.1.2.27
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

3.1.2.28
master (class 1)
active CP 3/1 communication peer triggering slaves for data exchange

3.1.2.29
process values (PV)
input and output data (in a safety PDU) that are required to control an automated process

3.1.2.30
qualifier
additional qualifying bits within *process values* indicating the status of each individual input

3.1.2.31
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.

3.1.2.32
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

3.1.2.33
universal serial bus (USB)
external bus standard that supports data transfer rates up to 480 Mbit/s

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

3.1.2.34
V1-mode
FSCP 3/1 services and protocol according to [48]

3.1.2.35
V2-mode
FSCP 3/1 services and protocol according to this part

3.1.2.36
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	
EMC	Electromagnetic Compatibility	
EMI	Electromagnetic Interference	
EUC	Equipment Under Control	[IEC 61508-4:2010]
E/E/PE	Electrical/Electronic/Programmable Electronic	[IEC 61508-4:2010]

FAL	Fieldbus Application Layer	[IEC 61158-5]
FCS	Frame Check Sequence	
FS	Functional Safety	
FSCP	Functional Safety Communication Profile	
HD	Hamming Distance	
MTBF	Mean Time Between Failures	
MTTF	Mean Time To Failure	
PDU	Protocol Data Unit	[ISO/IEC 7498-1]
PELV	Protective Extra Low Voltage	
PFD	Probability of dangerous Failure on Demand	[IEC 61508-6:2010[9]]
PFH	Average frequency of dangerous failure [h^{-1}] per hour	[IEC 61508-6:2010]
PhL	Physical Layer	[ISO/IEC 7498-1]
PL	Performance Level	[ISO 13849-1]
PLC	Programmable Logic Controller	
SCL	Safety Communication Layer	
SELV	Safety Extra Low Voltage	
SFRT	Safety Function Response Time	
SIL	Safety Integrity Level	[IEC 61508-4:2010]

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[10]
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	General Station Description (file associated with device)
GSDL	General Station Description Language (for CP 3/1 and CP 3/2 devices)
GSDML	General Station Description Markup Language (for CP 3/RTE devices)

---

9 To be published.

10 For trade name declarations, see Clause 4.

HAT	Host Acknowledgement Time	
I/O	Input/Output	
LED	Light Emitting Diode	
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	
SR	(Functional) Safety-Related	
SSID	Service Set Identifier	
UML	Unified Modeling Language	[57]
USB	Universal Serial Bus	[62]
VLAN	Virtual Local Area Network	
WCDT	Worst Case Delay Time	
WDTime	Watchdog Time	
WPA2	Wi-Fi Protected Access 2	[26]
XML	eXtensible Markup Language	[59], [60], [61]

3.3 Conventions

This part uses UML2 notation for the drawing of the state charts and a condensed form for sequence charts [57]. 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, any CRC signature calculation resulting in a "0" value, will use the value "1" instead.

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™[11]) 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

11 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.

(PROFIsafe™[11]) 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.

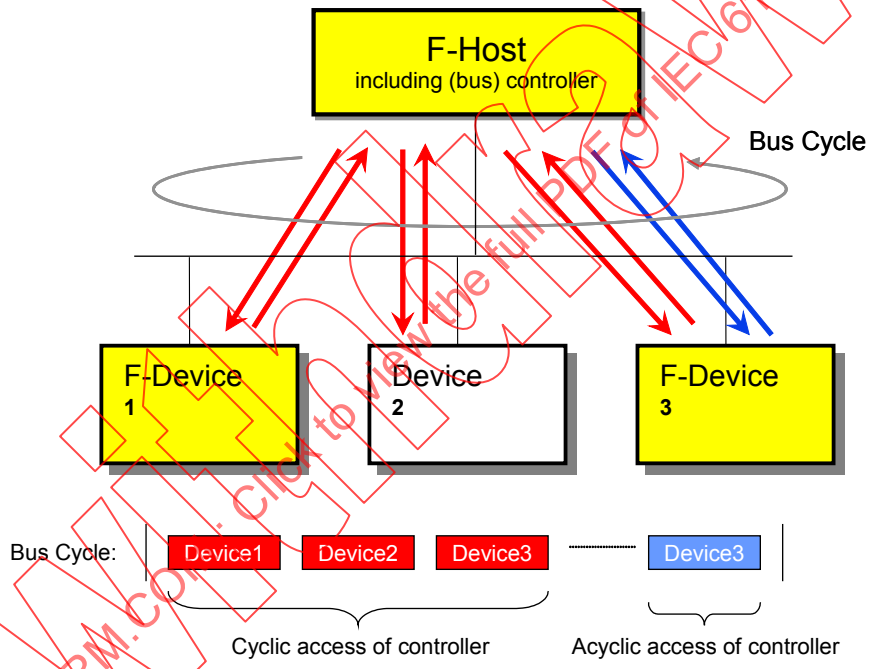


Figure 3 – Basic communication preconditions for FSCP 3/1

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).

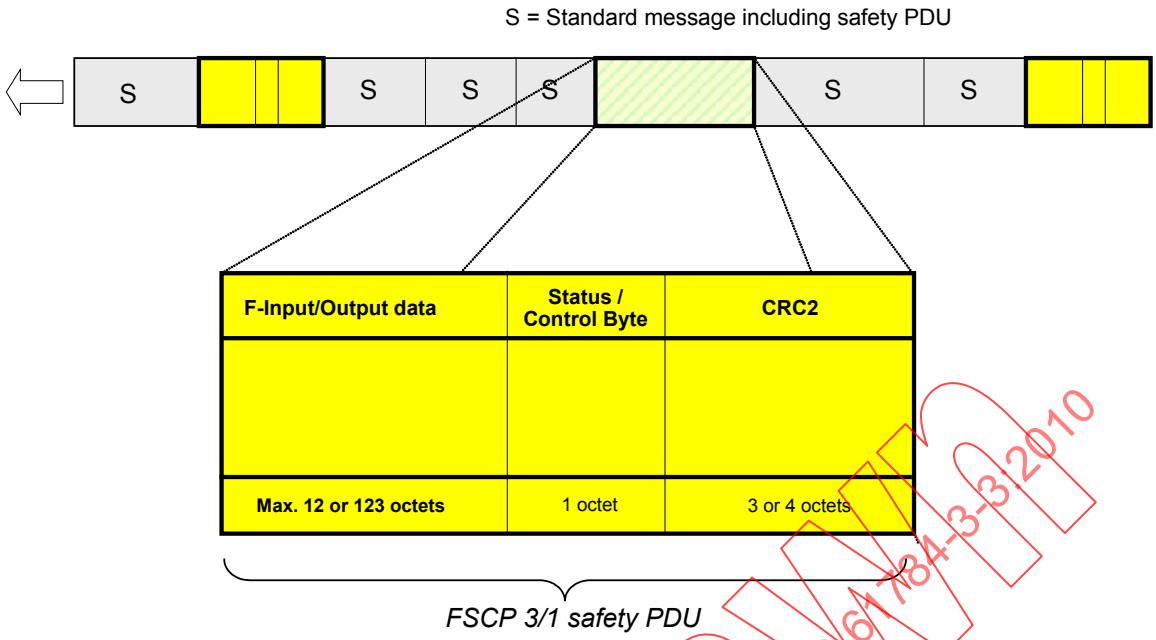


Figure 4 – Structure of an FSCP 3/1 safety PDU

FSCP 3/1 provides two operational modes: V1- and V2-mode. While the measures of the V1-mode are sufficient for the safety 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. Safety communication between PROFINET CBA components (see CP 3/3) is not 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.

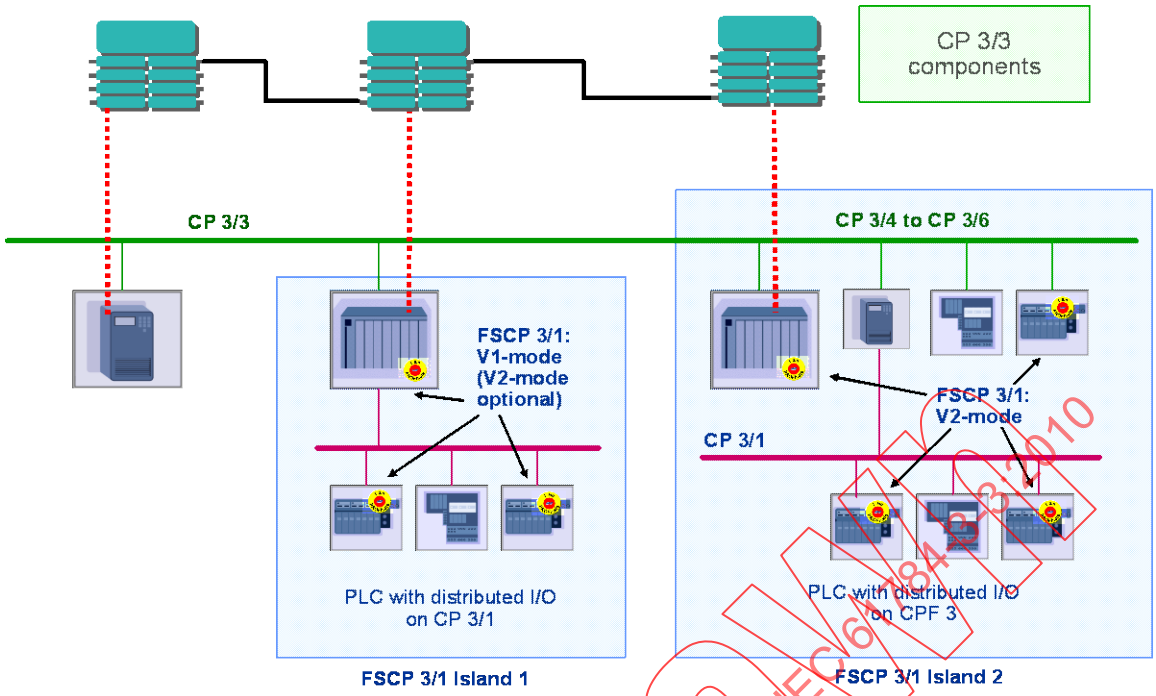


Figure 5 – Safety communication modes

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 IEC 61784-3:2010 Annex D, 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 assessment 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 assessment shall be observed ([44], [45]).

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 [31].

FSCP 3/1 meets the requirements of NE97 [58].

5.2 Safety functional requirements

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

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

b) Safety communication shall be suitable for Safety Integrity Level SIL3 (see IEC 61508), control category 4 (see EN 954-1 [25]), and PL e (see ISO 13849-1).

c) Safety communication shall use a single-channel communication system. Redundancy may only be used optionally for increased availability.

d) Implementation of the safety 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 61326-3-1 and IEC 61326-3-2, if there are no particular product standards.

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

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

j) Safety communication shall be suitable for NE97 [58] and meet the requirements of IEC 61784-3:2010 Annex D.

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 61784-3:2010, 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.

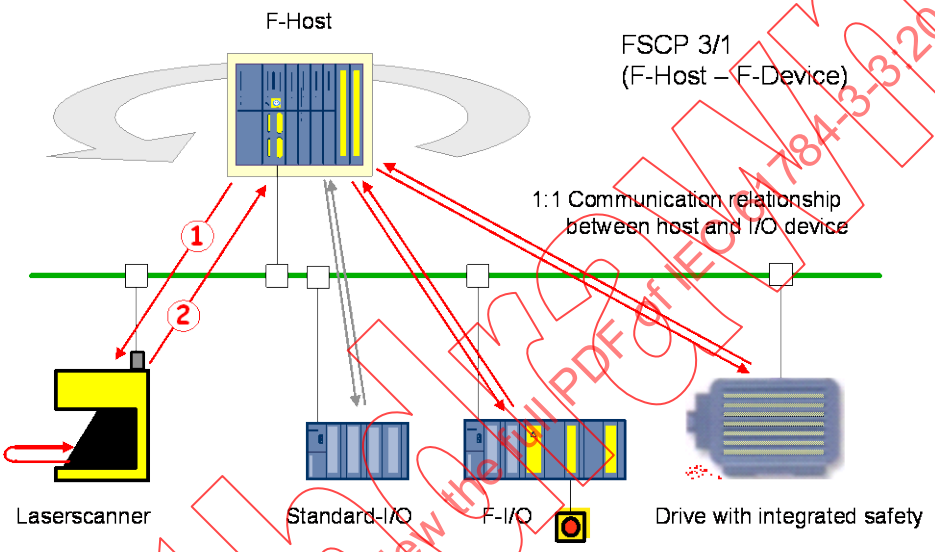


Figure 6 – Standard CPF 3 transmission system

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

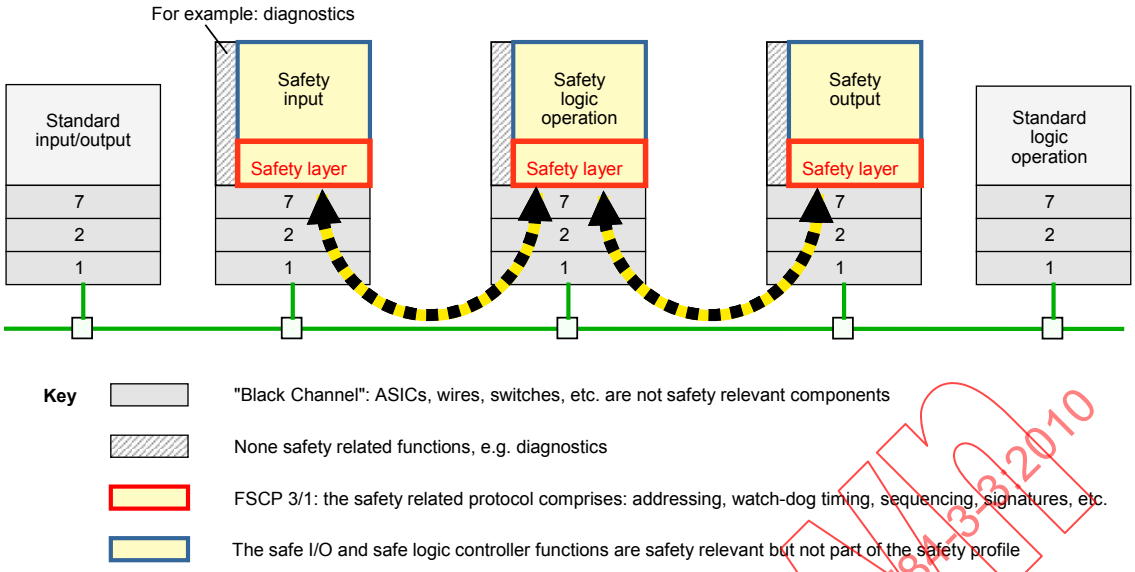


Figure 7 – Safety layer architecture

Transmission is performed via electrical 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.

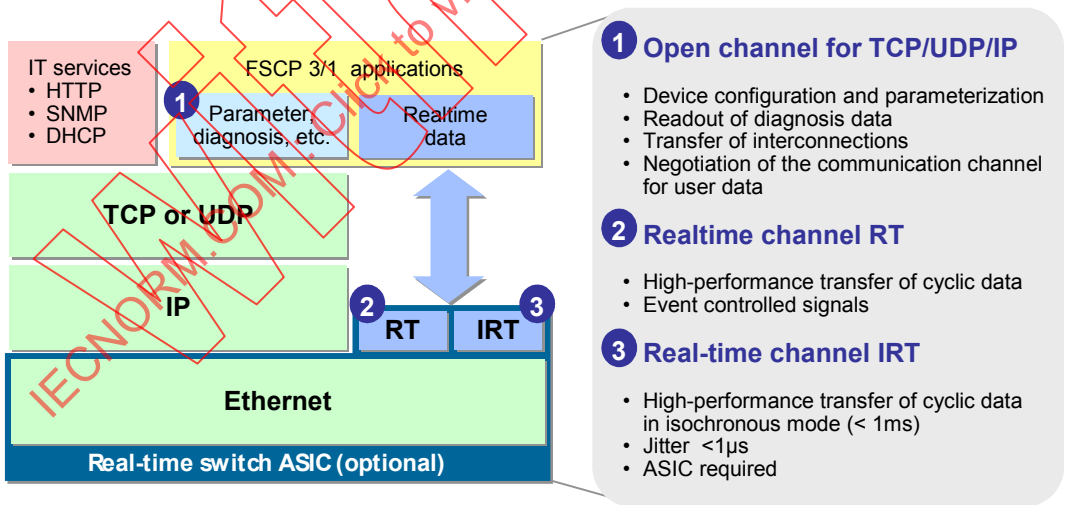


Figure 8 – Basic communication layers

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.

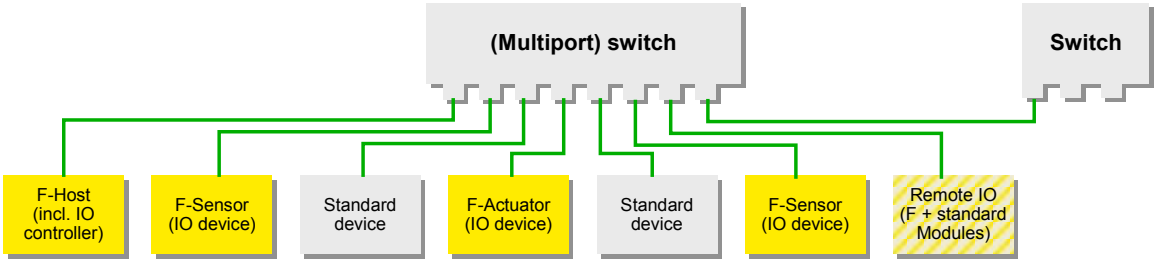


Figure 9 – Multiport switch bus structure

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.

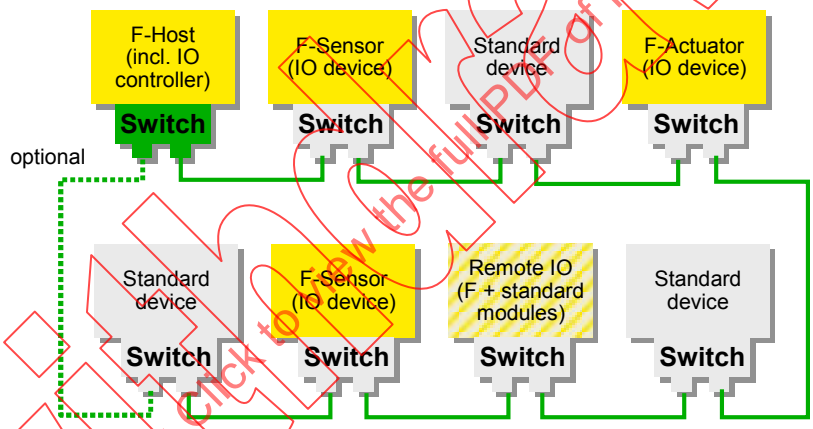


Figure 10 – Linear bus structure

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).

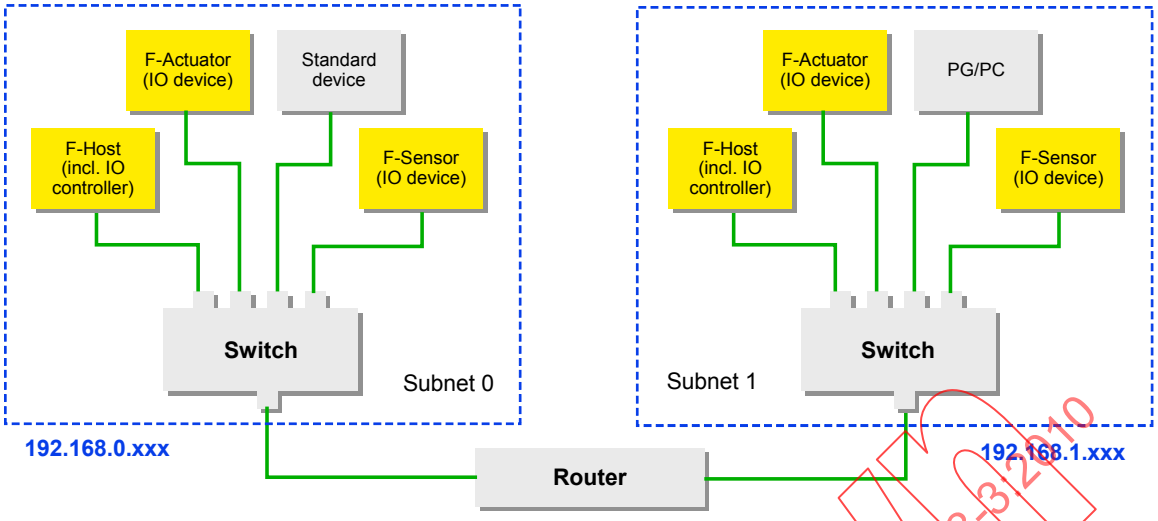
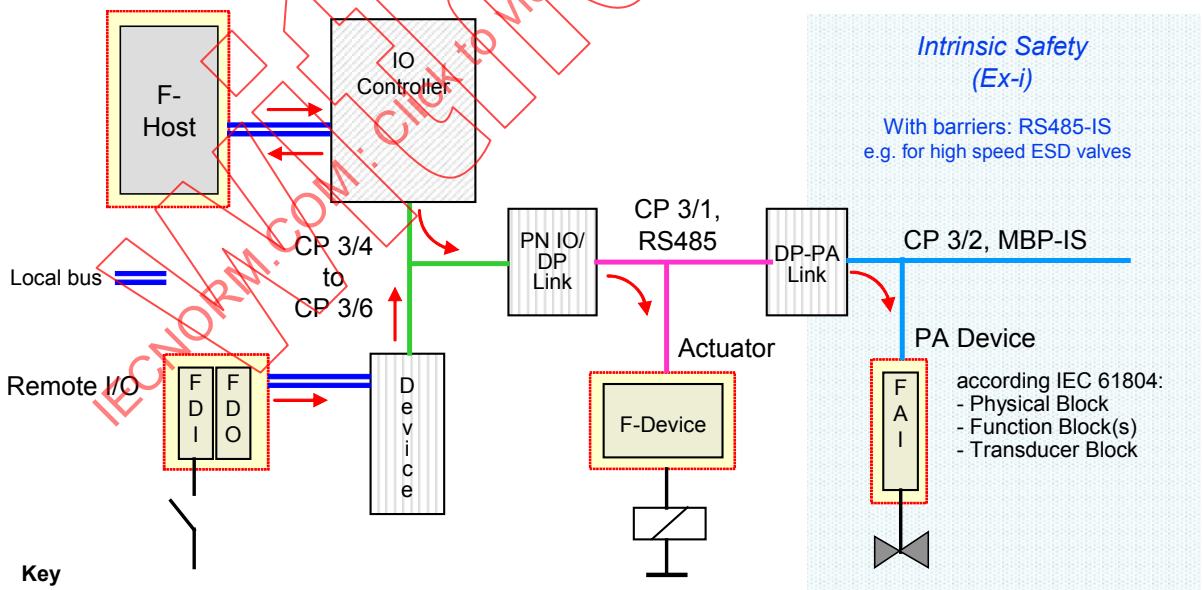


Figure 11 – Crossing network borders with routers

In contrast to the typical fieldbus system configuration, Figure 12 shows the possible bus structure, i.e. how far the safety profile extents into the individual units. A standard remote IO, for example, can comprise an F-Module for the connection of an emergency stop pushbutton. Thus the whole FSCP 3/1 transmission path reaches from the F-Host 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 [48] for details of the V1-mode on CP 3/1.



Key

MBP-IS	Data transmission for explosion-proof areas
RS485	High speed data transmission
RS485-IS	Special RS485 for explosion-proof areas
F-DI	Safety digital input
F-DO	Safety digital output
F-AI	Safety analog input
PA Device	Device according process automation device model (IEC 61804)

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.

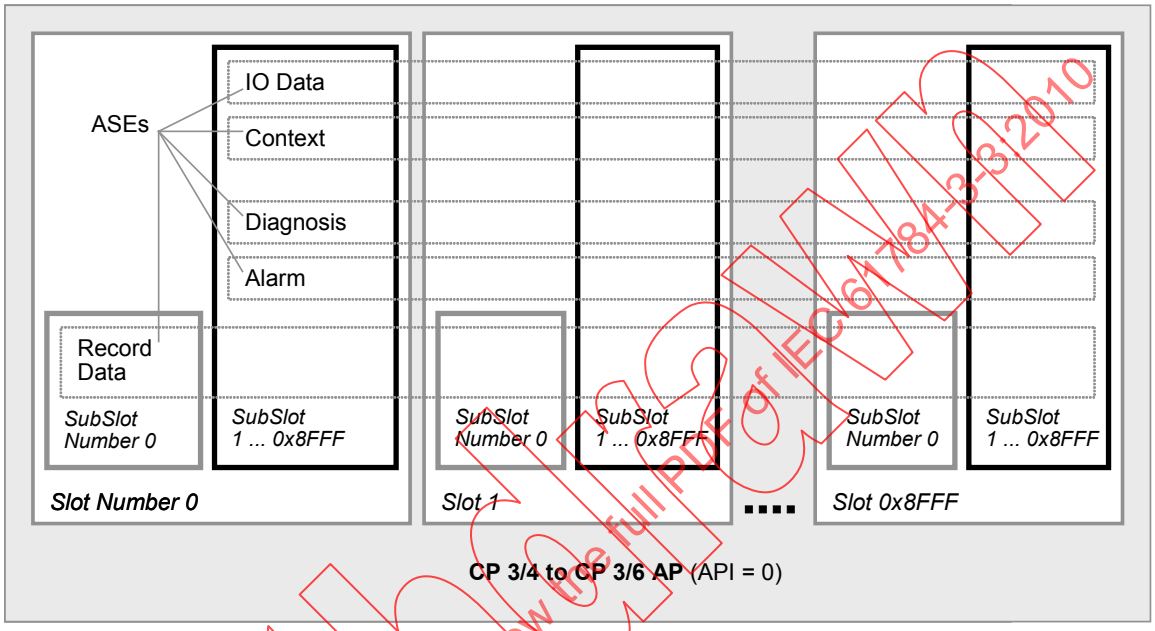


Figure 13 – Device model

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.

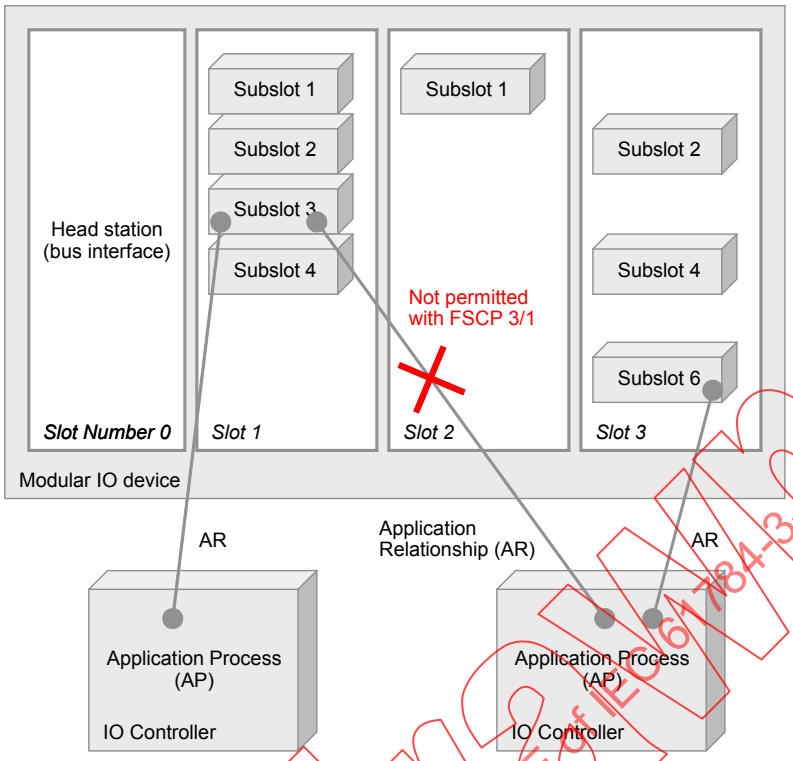


Figure 14 – Application relationships of a modular device

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.

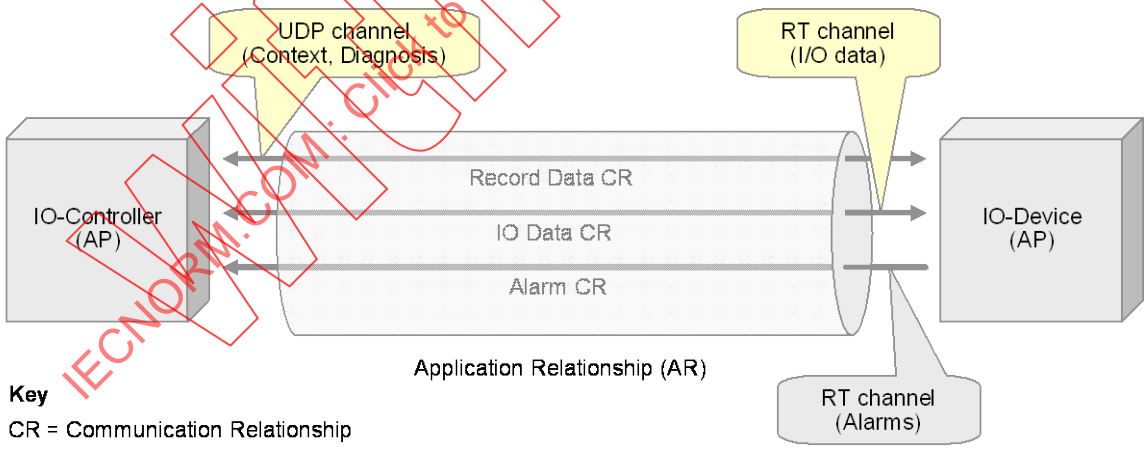
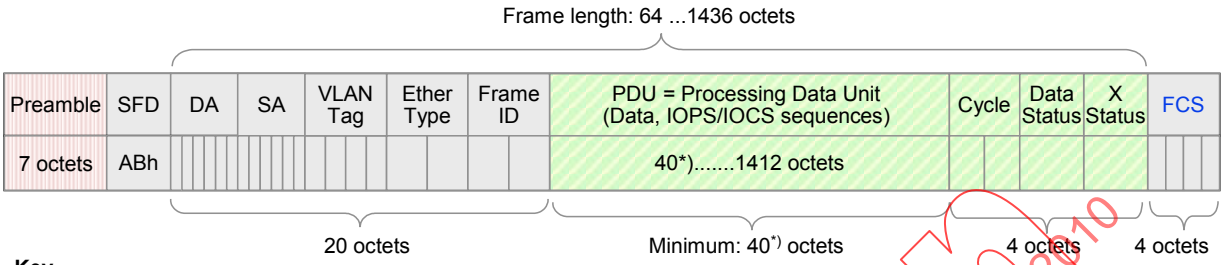


Figure 15 – Application and communication relationships (AR/CR)

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.



Key

Preamble	= AAAAAAAAAAAAAAh
SFD	= Start Frame Delimiter: ABh
DA	= Destination Address (6 octets)
SA	= Source Address (6 octets)
VLAN Tag	= indicates a certain priority; optional
Ether Type	= Ethernet Frame Type: 8892h for CP 3/4 to CP 3/6 (2 octets)
Frame ID	= Frame Identification (CP 3/4 to CP 3/6 message type)
IOPS	= IO Provider Status: good/bad and location (optional/GSD)
IOCS	= IO Consumer Status: good/bad and location (optional/GSD)
Cycle	= Cycle Counter (2 octets); multiples of 31,25µs
Data Status	= Information on redundancy, validity, device state, etc.
X Status	= Transfer Status (1 octet); always "00h"
FCS	= 32 bit CRC (104C11DB7h)

*) with VLAN-Tag minimum of user data to be transferred is 36 octets

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	
Unsigned64	8	
Float32	4	V1- and V2-mode
Float64	8	
Date		
TimeOfDay with date indication		
TimeOfDay without date indication		
TimeDifference with date indication		

Data type name	Number of octets	Used in
TimeDifference without date indication		
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.

See [67] for general information on data types.

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).

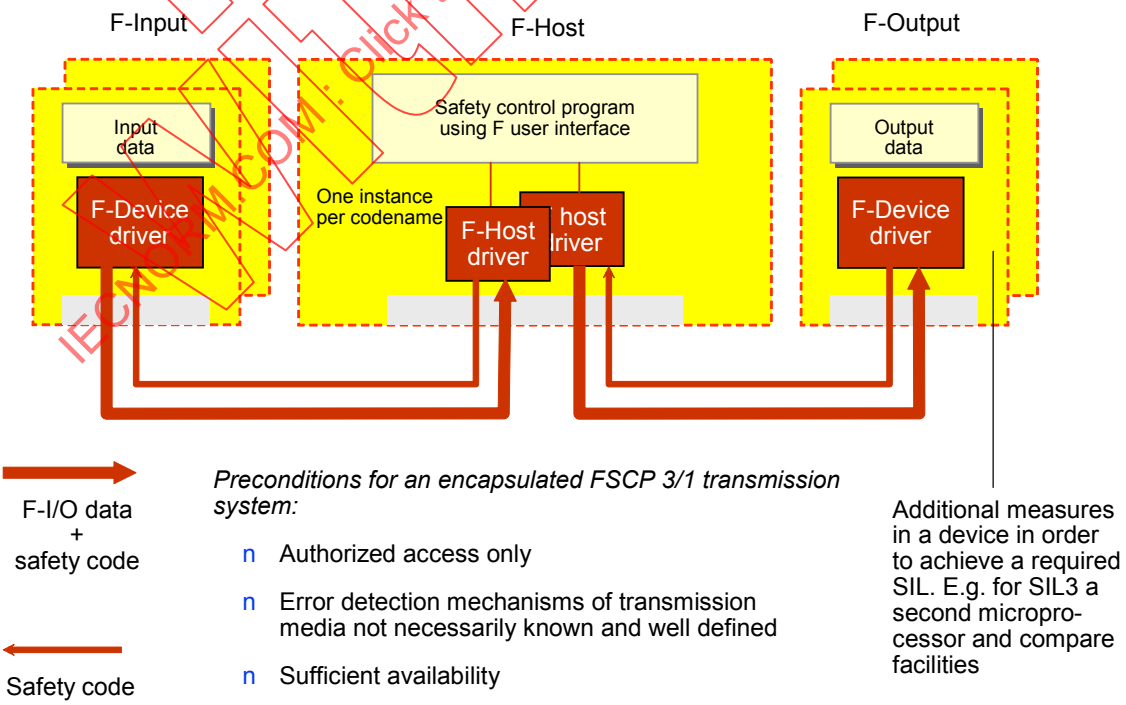


Figure 17 – FSCP 3/1 communication structure

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). 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.

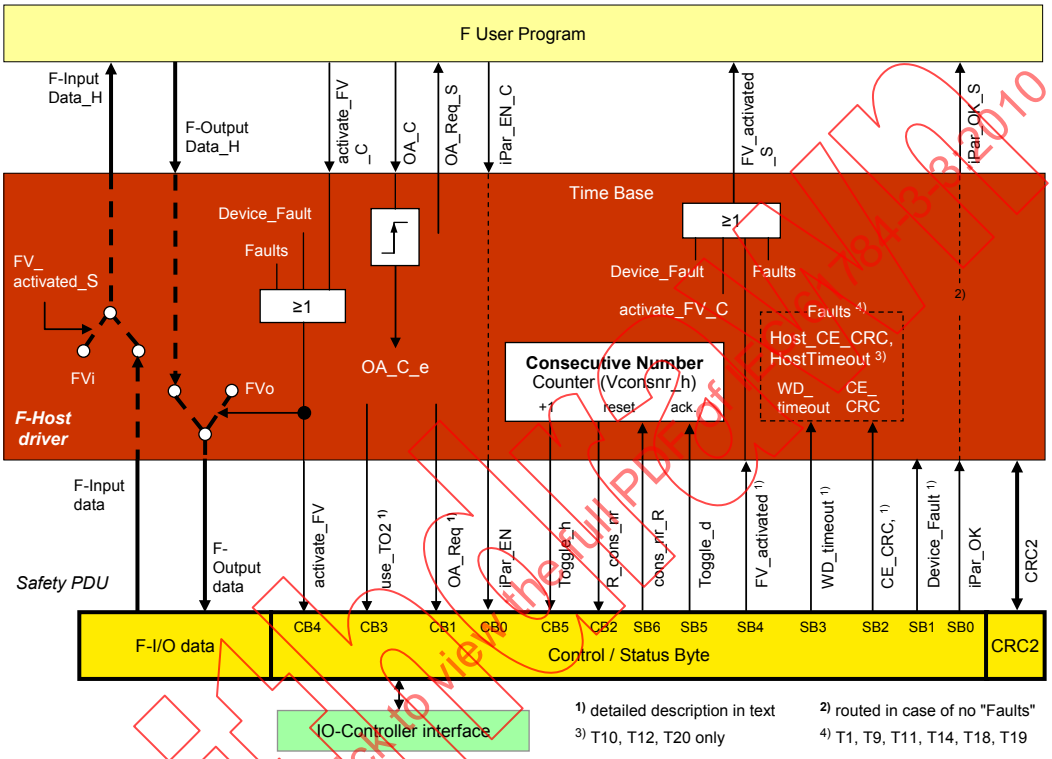


Figure 18 – F user interface of F-Host driver instances

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 62. 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:

activate_FV_C 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.

FV_activated_S 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.

iPar_EN_C — 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.

iPar_OK_S — This variable (type: bit) indicates to the F control program the end of iParameteri-zation and the readiness to resume F-I/O data exchange (Figure 41). 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.

OA _C (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.

OA_Req_S — 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 OA_Req_S (="1") as soon as the fault/error has been eliminated and operator acknowledgement is possible. Once the acknowledgement occurred (OA_C = "1") the F-Device driver will reset the request variable OA_Req_S (= "0").

Input values
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)

Output values
PVo Process output values (→F-Output_Data_D)
FVo Fail-safe output values (=0), used instead of PVo for F-Output_Data_D

6.2 F-Device services

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, CB3, 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.

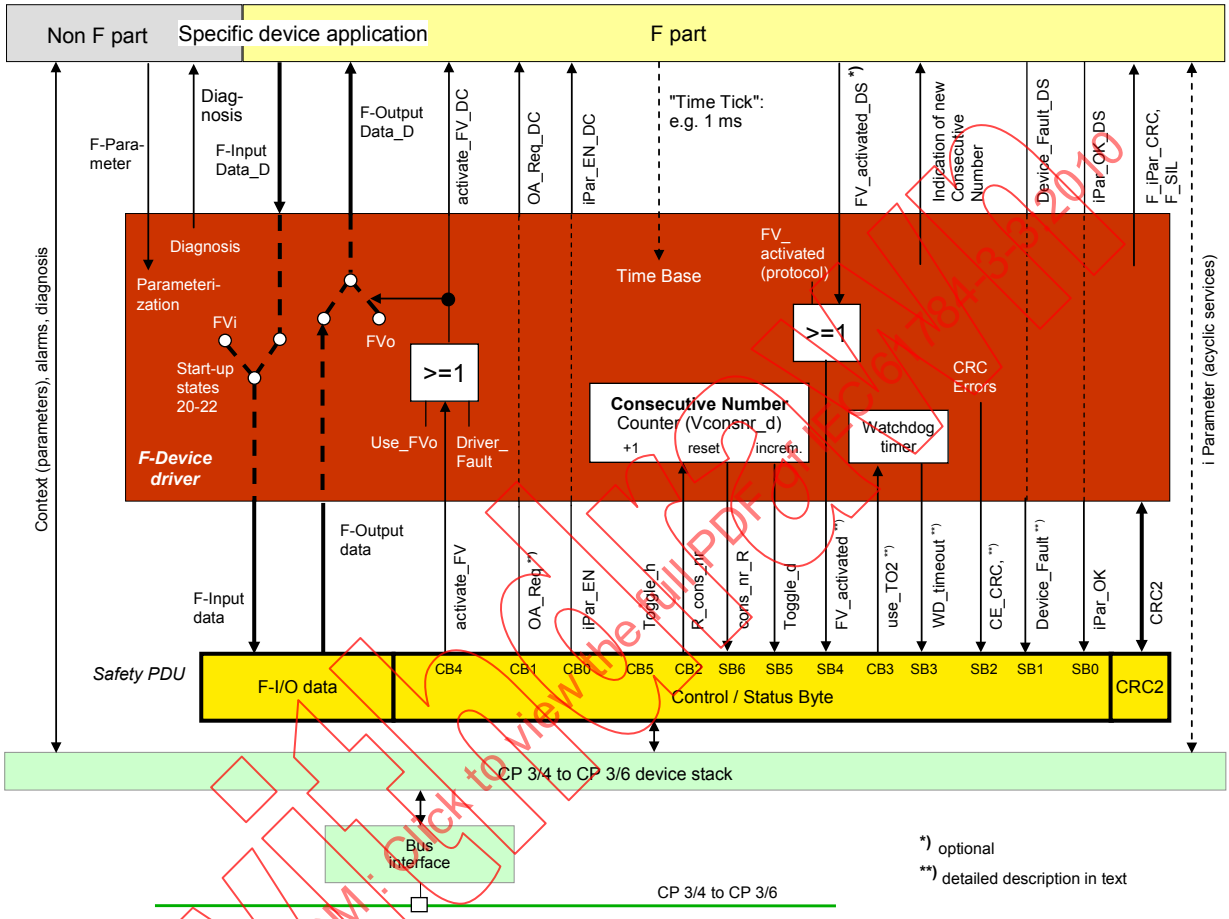


Figure 19 – F-Device driver interfaces

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), see 8.1.2
0x0041	65	Safety destination address not valid (F_Dest_Add), see 8.1.2
0x0042	66	Safety source address not valid (F_Source_Add), see 8.1.2
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

Hex	Number	Diagnosis Information
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.

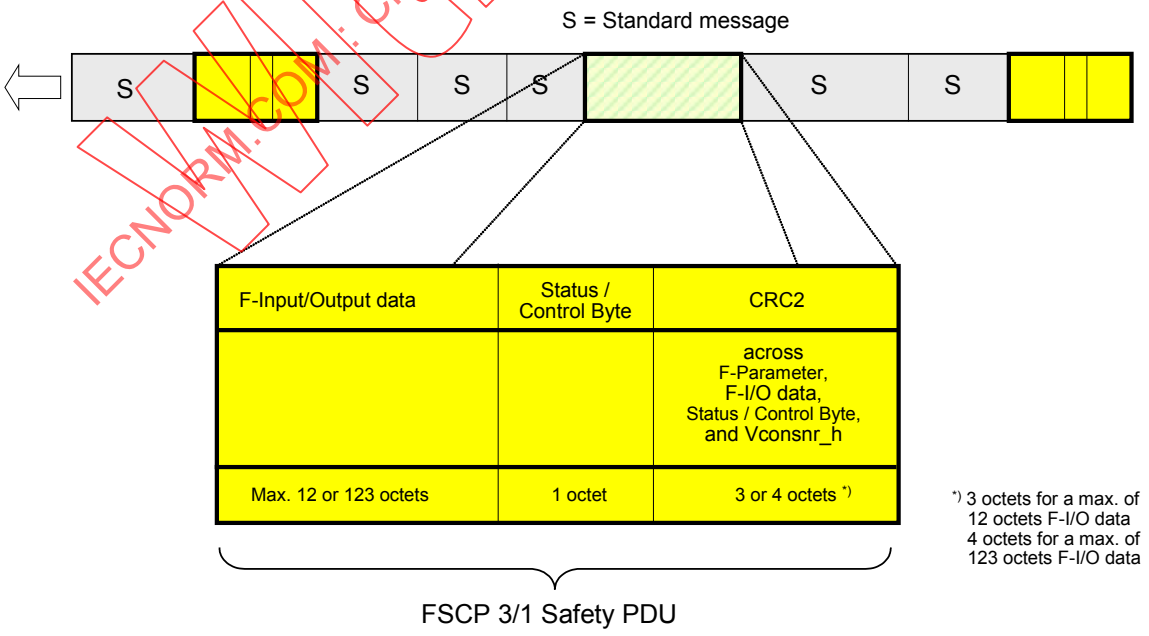


Figure 20 – Safety PDU for CPF 3

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.

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 F-I/O peripherals are accommodated in this safety PDU section. The data type coding corresponds to the one of CP 3/RTE and is defined system wide within IEC 61158-5-10. Subclause 8.5.2 recommends and specifies standardized data types and data structures for several families of safety devices such as remote 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 subslot. 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	Communi-cation fault: WD-timeout	Communi-cation 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) changes of consecutive number, if an F-Device/Module either provides no channel specific signal qualifiers, and one or more channels failed, or it detects another malfunction. This behavior allows for faster reaction times in the event of a failure than via timeout. 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	Use F_WD_Time_2 (secondary watchdog)	Reset Vconsnr_d	Operator acknowledge requested	iParameter assignment deblocked
-	-	Toggle_h	activate_FV	Use_TO2	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). Signal name is "iPar_EN".

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). Signal name is "OA_Req".

Bit 2 is set when the F-Host detects a communication error, either by the Status Byte or by itself. As a consequence 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. Signal name is "R_cons_nr".

Bit 3 is set when the F-Host driver gets informed inherently that an intended update process of the safety fieldbus components in case of 'configuration in run' or 'maintenance of a fault tolerance system' is taking place.

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. Signal name is "activate_FV".

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. Signal name is "Toggle_h".

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 [48] on details of the V1-mode.

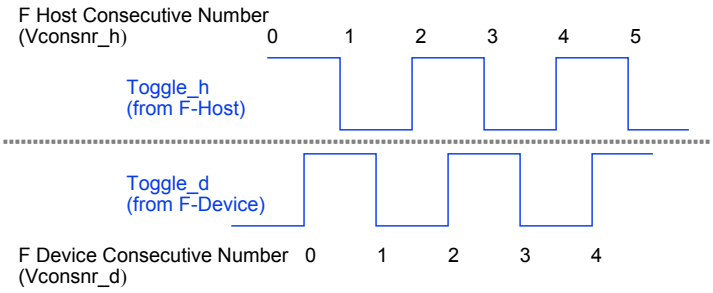


Figure 23 – The Toggle Bit function

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).

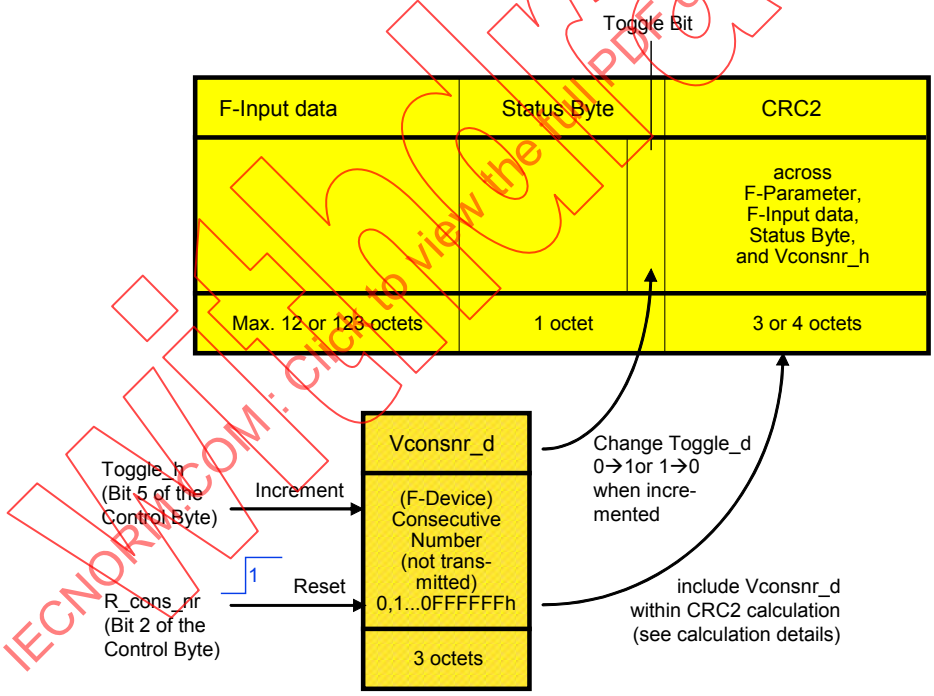


Figure 24 – F-Device Consecutive Number

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.

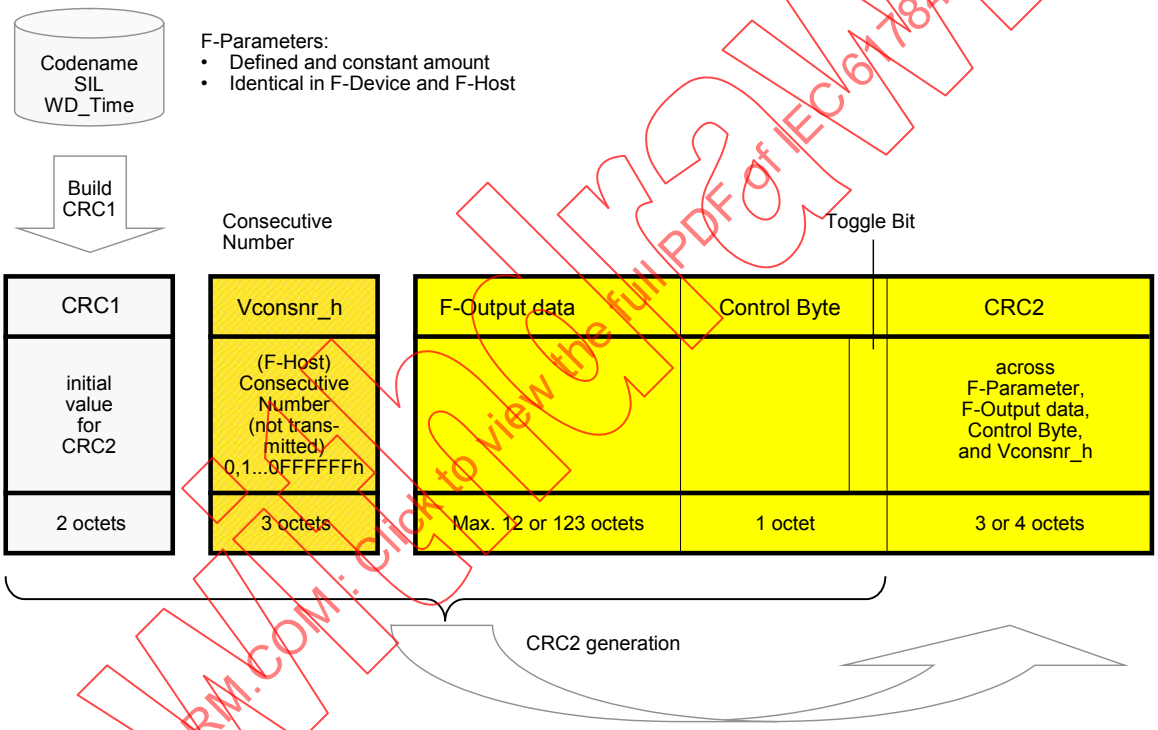


Figure 25 – CRC2 generation (F-Host output)

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 assessment 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".

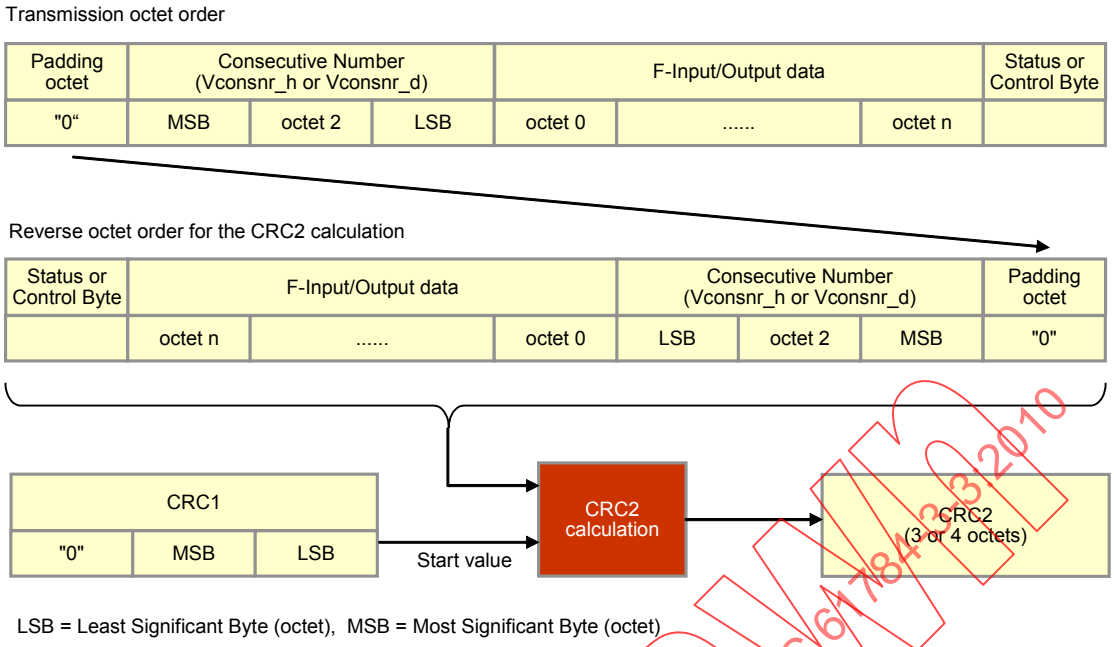


Figure 26 – Details of the CRC2 calculation (reverse order)

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.

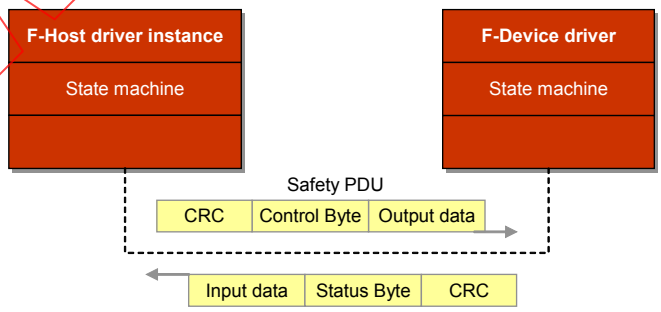


Figure 27 – Safety layer communication relationship

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.

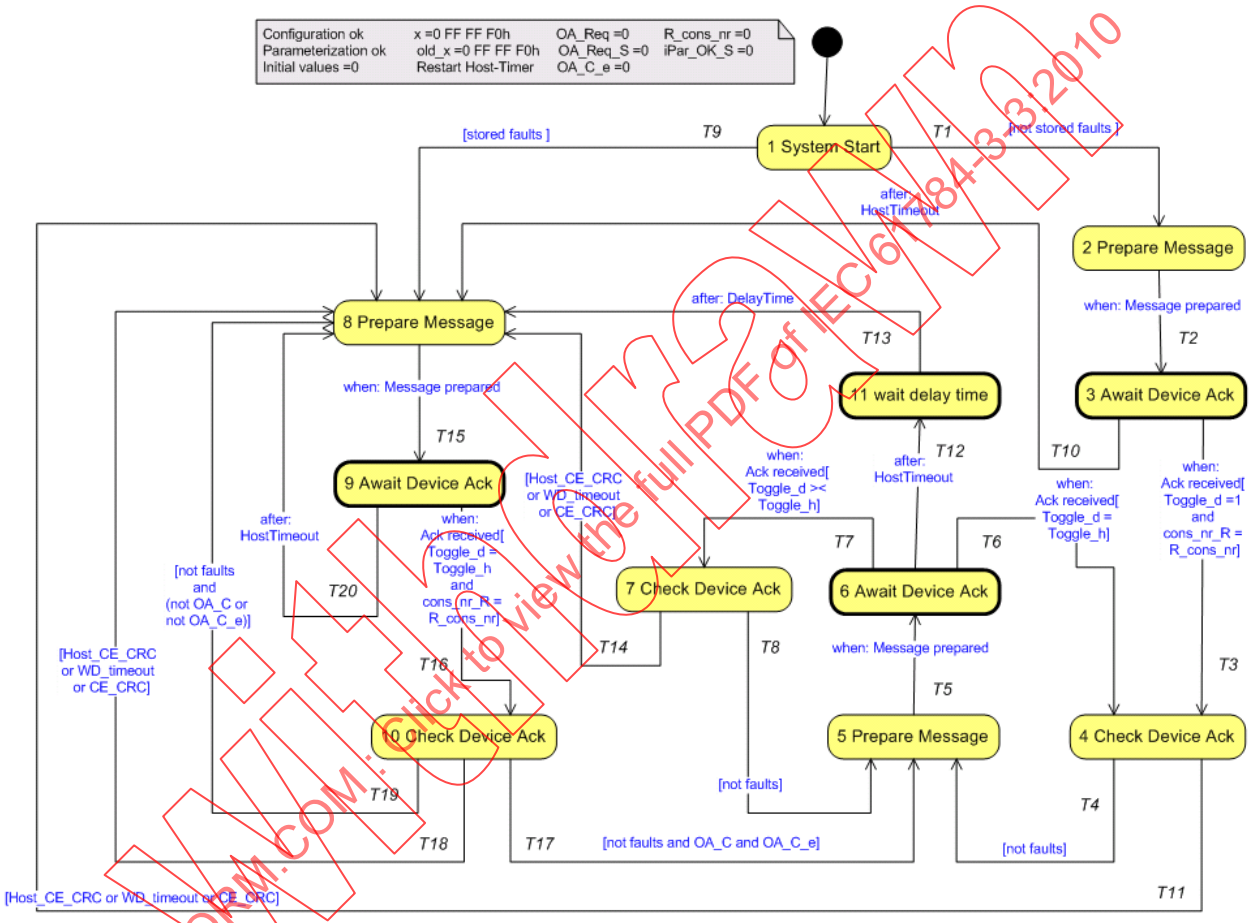


Figure 28 – F-Host state diagram

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 *regular* 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 *CRC-error* (Host_CE_CRC) including virtual consecutive number (x) and for potential *F-Device faults* within the Status Byte (WD_timeout, CE_CRC)
5 Prepare Message	Preparation of a *regular* 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 *CRC-error* (Host_CE_CRC) including previous (old_x) virtual consecutive number and for potential *F-Device faults* 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 *CRC-error* (Host_CE_CRC) including virtual consecutive number (x) and for potential *F-Device faults* within the Status Byte (WD_timeout, CE_CRC). Once a fault occurred, no automatic restart of a safety function is permitted unless an operator 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 acknowledge with the next power-on. A delay time of 0 ms is permitted.

TRAN-SITION	SOURCE STATE	TARGET STATE	ACTION
T1	1	2	use FV, activate_FV =1, FV_activated_S =1 Toggle_h =1
T2	2	3	send safety PDU
T3	3	4	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

TRAN-SITION	SOURCE STATE	TARGET STATE	ACTION
			else use PVo, activate_FV =0 iPar_OK_S =iPar_OK
T9[a]	1	8	use FV, activate_FV =1, FV_activated_S =1, Toggle_h =1, R_cons_nr =1, x =0
T10	3	8	restart host-timer, store faults, use FV, activate_FV =1, FV_activated_S =1, Toggle_h = not Toggle_h, R_cons_nr =1, x =0
T11	4	8	store faults, use FV, activate_FV =1, FV_activated_S =1, Toggle_h = not Toggle_h, R_cons_nr =1, x =0
T12	6	11	use FV, activate_FV =1, FV_activated_S =1, R_cons_nr =1, x =0
T13	11	8	store faults, Toggle_h = not Toggle_h, restart host-timer
T14	7	8	restart host-timer, store faults, use FV, activate_FV =1, FV_activated_S =1, Toggle_h = not Toggle_h, R_cons_nr =1, x =0
T15	8	9	send safety PDU
T16	9	10	restart host-timer
T17	10	5	reset stored faults, OA_Req_S =0, OA_Req =0, OA_C_e =0, R_cons_nr =0, 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
T18	10	8	store faults, OA_Req =0, OA_Req_S =0, OA_C_e =0, use FV, activate_FV =1, FV_activated_S =1, Toggle_h = not Toggle_h, R_cons_nr =1, x =0
T19	10	8	OA_Req_S =1, OA_Req =1, **if** OA_C =0 **then** OA_C_e =1 use FV, activate_FV =1, FV_activated_S =1, Toggle_h = not Toggle_h, R_cons_nr =0, old_x =x, x =x+1, **if** x =01000000h **then** x =1

TRAN-SITION	SOURCE STATE	TARGET STATE	ACTION
T20	9	8	store faults, OA_Req =0, OA_Req_S =0, OA_C_e =0, use FV, activate_FV =1, FV_activated_S =1, Toggle_h = not Toggle_h, R_cons_nr =1, x =0, restart host-timer
a Implementation of transition T9 depends on the safety design concept of a particular system manufacturer.			

INTERNAL ITEMS	TYPE	DEFINITION
x	Counter	x is representing the local consecutive number within the F-Host driver instance. It is not transmitted to its counterpart within the F-Device, but is synchronizing those via a Toggle Bit in the Control Byte. The actual counter value of x is incorporated in the CRC2 calculation and thus checked against transmission faults. Value range is 0 … 0FFFFFFh. During start-up this incremental counter is set to 0FFFFF0h and starts from there. The F-Host increments the virtual consecutive number after each acknowledged reception of the respective virtual consecutive number of its F-Device modulo 0FFFFFFh, skipping the value "0" and continuing with "1".
old_x	Counter	Previous value of the current local consecutive number x. It is necessary to store this previous value of the consecutive number in order to distinguish the initial cycle from later ones.
DelayTime	Timer	This delay time is to cover power off settling time within the whole system. It is within the host/system manufacturer's responsibility to define this parameter.
host-timer	Timer	This timer checks whether the next valid safety PDU from the F-Device did arrive in time. The host engineering tool is responsible to define this watchdog time. Value range is 0 … 65 535 ms.
OA_C_e	Flag	By means of this auxiliary variable (bit) it is ensured that the safe state will be left only after a signal change of OA_C from 0 → 1 (edge). Without this mechanism an operator could overrule safe states by permanently actuating the OA_C signal.
faults	Flags	Until an operator acknowledgement (OA_C), persistent storage of the following faults is required within the F-Host only (no F-Device persistence): - Host_CE_CRC - HostTimeout - CE_CRC (Status Bit 2) - WD_timeout (Status Bit 3)
	Activity State	Within these interruptable "activity" states the host waits for new inputs such as timeout or acknowledgement [34].
	Action State	Within these non-interruptable "action" states events like timeout, message received or operator acknowledgement are deferred until the next "activity" state [34].

7.2.3 F-Device state diagram

Figure 29 shows the F-Device state diagram and Table 5 describes the states, transitions, and internal items. The diagrams are following the UML2 notation.

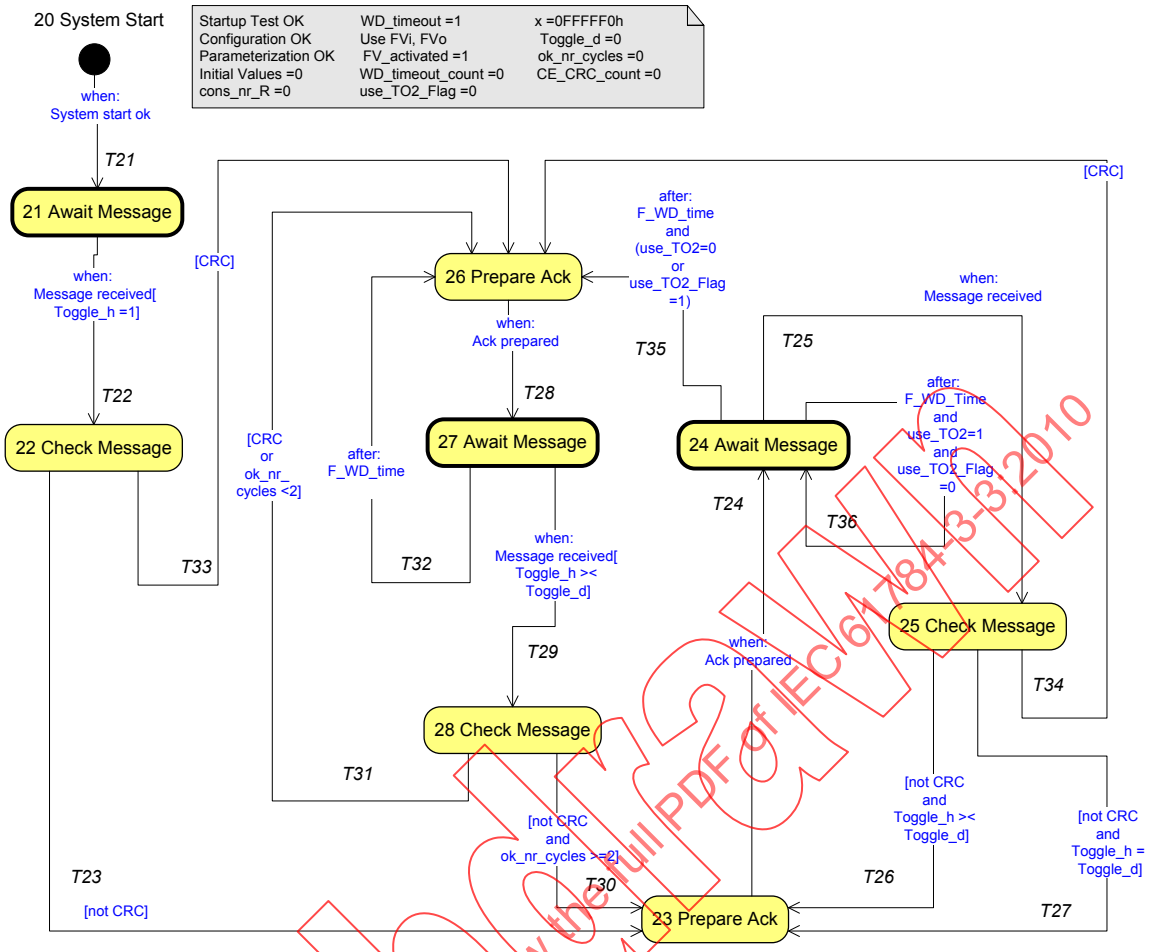


Figure 29 – F-Device state diagram

The terms used in Figure 29 are specified below:

[Toggle_h = Toggle_d]	UML notation of a condition (guard) to fire the transition. In this case it means: Bit Toggle_h has not changed value ("not toggled")
[Toggle_h >< Toggle_d]	Bit Toggle_h has changed value ("toggled")
[CRC]	F-Device recognizes CRC fault (communication and/or consecutive number error)
F_WD_Time	Watchdog time defined by the F-Parameter "F_WD_Time"
use_TO2	CB3 within the Control Byte indicating usage of the secondary watchdog time F_WD_Time_2
use_TO2_Flag	Auxiliary flag
Ack	Acknowledgement safety PDU of the F-Device
Message received	any new safety PDU received; ignore safety PDU with all values = 0

Table 5 – F-Device states and transitions

STATE NAME	STATE DESCRIPTION
20 System Start	Initial state of the device upon power-on. Upon power-on the *output* F-Device is setting "0". Immediately after F-Parameterization it is setting fail-safe values. Upon power-on the *input* F-Device is sending "0". Immediately after F-Parameterization it is sending process values.
21 Await Message	Safety Layer is waiting on next safety PDU from F-Host
22 Check Message	Check received safety PDU for *CRC-error* including virtual consecutive number
23 Prepare Ack	Preparation of *regular* safety PDU for the F-Host (Acknowledgement)
24 Await Message	Safety Layer is waiting on next regular safety PDU from F-Host
25 Check Message	Check received safety PDU for *CRC-error* including virtual consecutive number
26 Prepare Ack	Preparation of safety PDU for the F-Host (Acknowledgement with fault bits)
27 Await Message	Safety Layer is waiting on next safety PDU from F-Host (exception handling)
28 Check Message	Check received safety PDU for *CRC-error* including virtual consecutive number

TRAN-SITION	SOURCE STATE	TARGET STATE	ACTION
T21	20	21	-
T22	21	22	**if** R_cons_nr =1 **then** x=0, cons_nr_R =1
T23	22	23	use PVi, FVo, FV_activated =1, CE_CRC =0, WD_timeout =0, Toggle_d = Toggle_h, restart device-timer, ok_nr_cycles =ok_nr_cycles +1
T24	23	24	send safety PDU
T25	24	25	**if** Toggle_h <> Toggle_d **then** restart device-timer x=x+1, **if** x =01000000h **then** x =1, cons_nr_R =0 **if** R_cons_nr =1 **then** x=0, cons_nr_R =1 **if** use_TO2 =0 **then** use_TO2_Flag =0
T26	29	23	Use PVi, Toggle_d = Toggle_h, **if** ok_nr_cycles <4 ok_nr_cycle =ok_nr_cycle +1 **if** ok_nr_cycles <4 **then** use FVo, FV_activated =1 **else** use PVo, FV_activated =0 **if** activate_FV =1 **then** use FVo **else** use PVo
T27	25	23	Use PVi, Toggle_d = Toggle_h, **if** ok_nr_cycles <4 **then** use FVo, FV_activated =1 **else** use PVo, FV_activated =0 **if** activate_FV =1 **then** use FVo **else** use PVo
T28	26	27	Send safety PDU
T29	27	28	**if** R_cons_nr =1 **then** x=0, cons_nr_R =1 **else** x=x+1, **if** x =01000000h **then** x =1, cons_nr_R =0

TRAN-SITION	SOURCE STATE	TARGET STATE	ACTION
T30	28	23	use PVi, FVo, FV_activated =1, Toggle_d = Toggle_h, restart device-timer, ok_nr_cycles =ok_nr_cycles +1
T31	28	26	Toggle_d = Toggle_h, restart device-timer, **if** CRC **then** CE_CRC =1, CE_CRC_count =1, ok_nr_cycles =0, **else** ok_nr_cycles =ok_nr_cycles +1, **if** CE_CRC_count >0 **then** CE_CRC =1, CE_CRC_count = CE_CRC_count -1, **else** CE_CRC =0, **if** WD_timeout_count >0 **then** WD_timeout =1, WD_timeout_count = WD_timeout_count -1 **else** WD_timeout =0
T32	27	26	Use PVi, FVo, FV_activated =1, WD_timeout =1, WD_timeout_count =1, ok_nr_cycles =0, restart device timer, Toggle_d = Toggle_h
T33	22	26	Use PVi, FVo, FV_activated =1, CE_CRC =1, CE_CRC_count =1, WD_timeout =0, ok_nr_cycles =0, restart device-timer, Toggle_d = Toggle_h
T34	25	26	Use PVi, FVo, FV_activated =1, CE_CRC =1, CE_CRC_count =1, ok_nr_cycle =0, restart device-timer, Toggle_d = Toggle_h
T35	24	26	Use PVi, FVo, FV_activated =1, WD_timeout =1, WD_timeout_count =1, ok_nr_cycles =0, restart device timer, Toggle_d = Toggle_h
T36	24	24	restart device timer with F_WD_Time_2 use_TO2_Flag =1

INTERNAL ITEM	TYPE	DEFINITION
x	Counter	x is representing the real local consecutive number within the F-Device. It is not transmitted to its counterpart within the F-Host, but synchronized with those via a Toggle Bit within the Control Byte. That means it is incremented each time when the Toggle Bit within the Control Byte (Toggle_h) changes its state from 0 → 1 or from 1 → 0 counting modulo 0 FF FF FFh, skipping the value "0" and continuing with "1". The counter value of x is reset to 0 in case the Control Bit "R_cons_nr" is set (1). The respective counter value of x is incorporated in the CRC2 calculation and thus checked against transmission faults. Value range is 0 … 0 FF FF FFh. During start-up this incremental counter is set to 0 FF FF F0h and starts from there.
ok_nr_cycles	Counter	During start-up and after a fault, the F-Device shall set FVo and FV_activated =1 for at least 3 cycles. It is the task of this incremental counter "ok_nr_cycles" to count these cycles from 0 to 3.

INTERNAL ITEM	TYPE	DEFINITION
CE_CRC_count	Counter	This decremental counter is used to guarantee that the bit "CE_CRC" within the Status Byte is set at least for 1 cycle or for a maximum of 2 cycles. Value range is 0,1.
WD_timeout_count	Counter	This decremental counter is used to guarantee the bit "WD_timeout" within the Status Byte is set at least for 1 cycle or for a maximum of 2 cycles. Value range is 0,1.
device-timer	Timer	This timer checks whether the next valid safety PDU did arrive in time. The F-Parameter "F_WD_Time" is used to define this watchdog time. Value range is 0 … 65 535 ms.

7.2.4 Sequence diagrams

Figure 30 to Figure 33 are showing the interaction messages of F-Host and F-Device during start-up phase. Three phases are covered: both partners during start-up, the F-Host temporarily switches power off or the F-Device temporarily switches power off while its partner is still operating. The figures are informing about the states and the corresponding transitions. Numbers within circles represent the states the respective F-Host and F-Device are passing through.

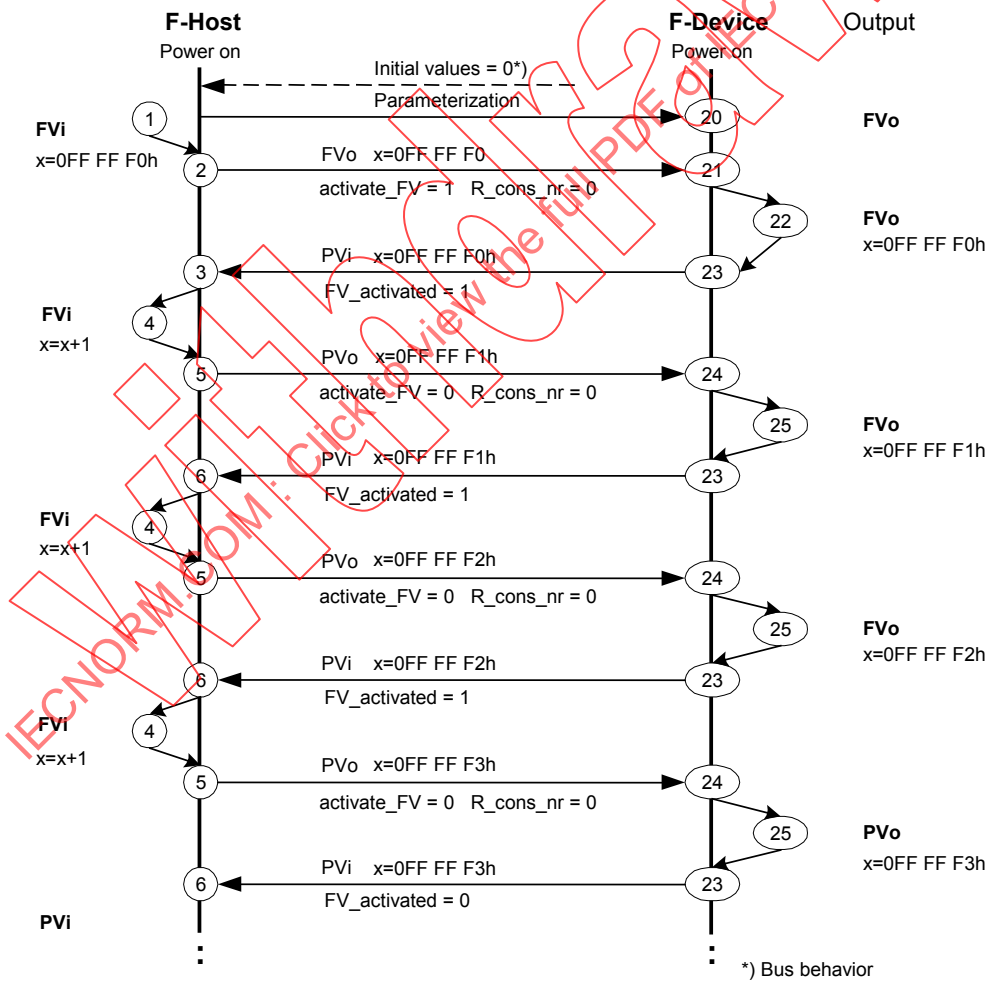


Figure 30 – Interaction F-Host / F-Device during start-up

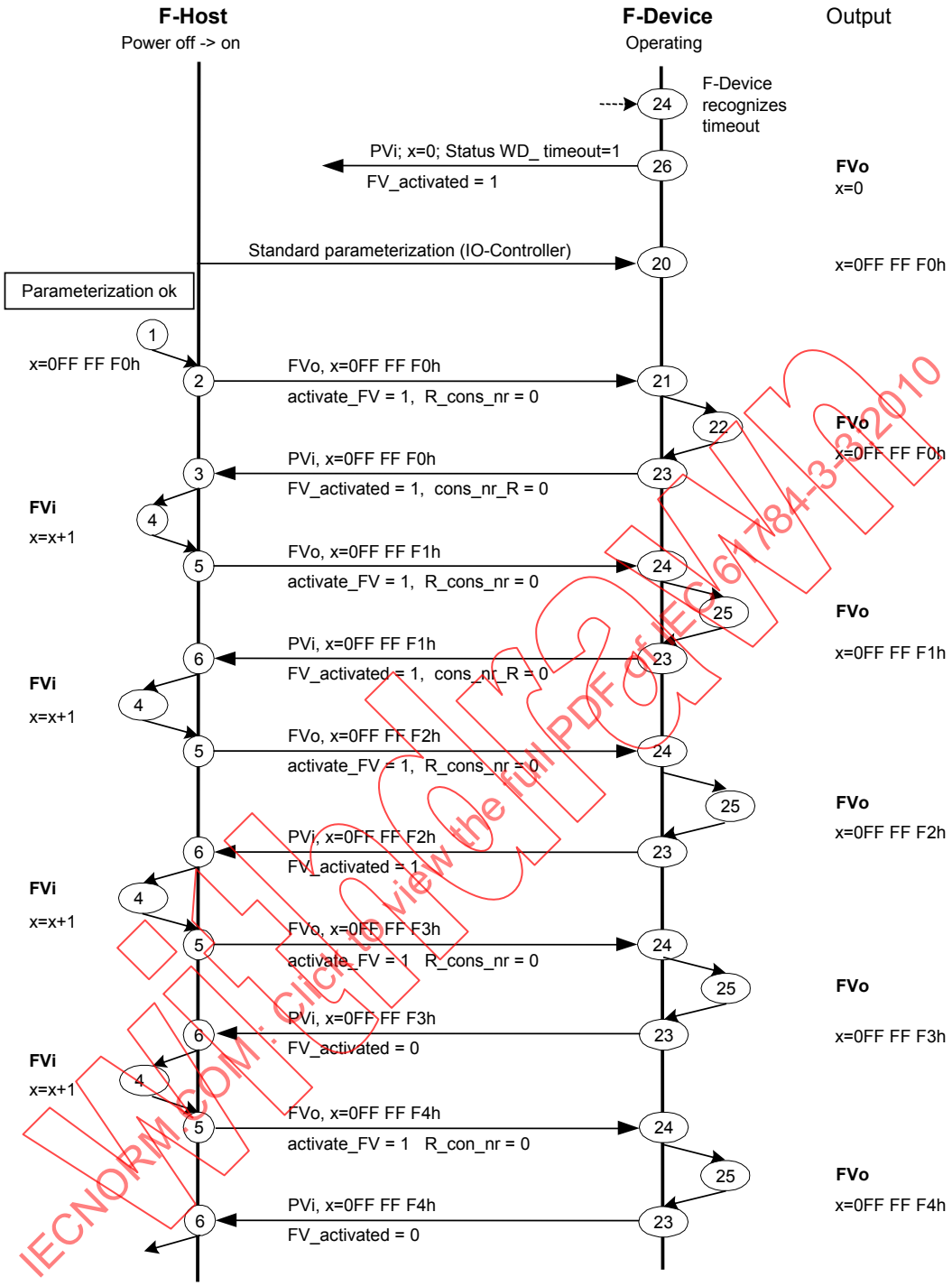


Figure 31 – Interaction F-Host / F-Device during F-Host power off → on

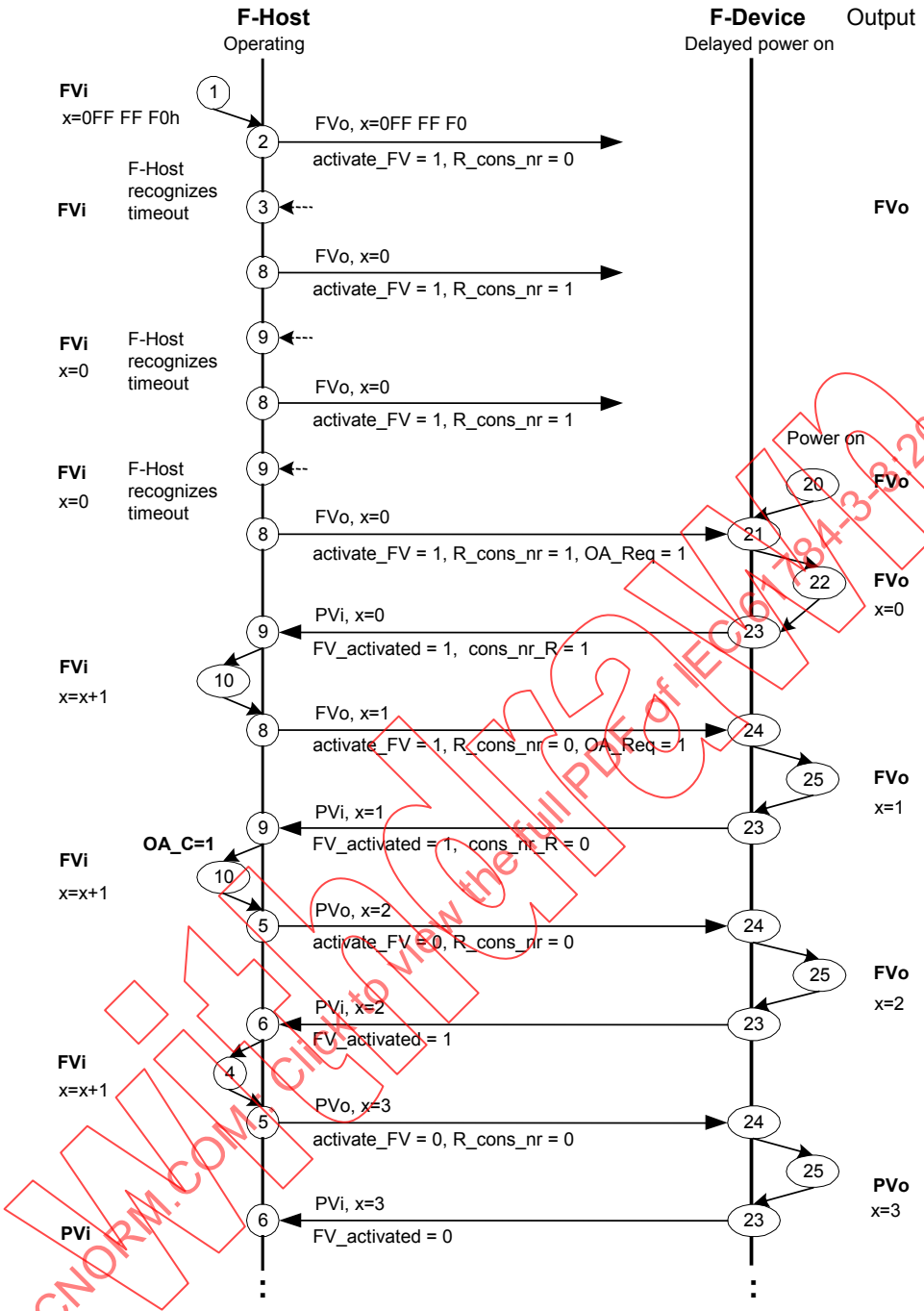


Figure 32 – Interaction F-Host / F-Device with delayed power on

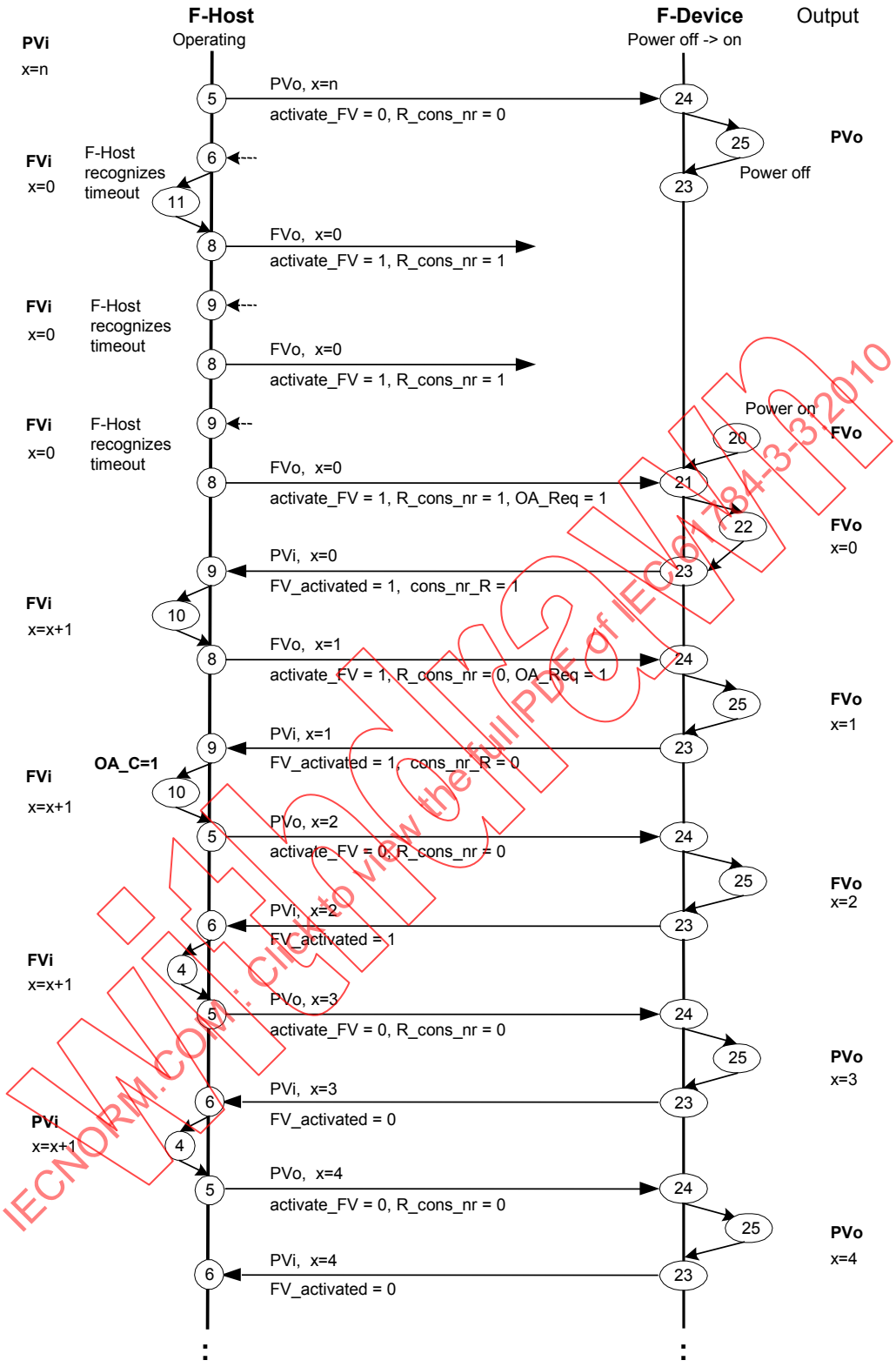


Figure 33 – Interaction F-Host / F-Device during power off → on

Figure 34 and Figure 35 are showing the interaction messages between F-Host and F-Device while CRC faults are detected on either side.

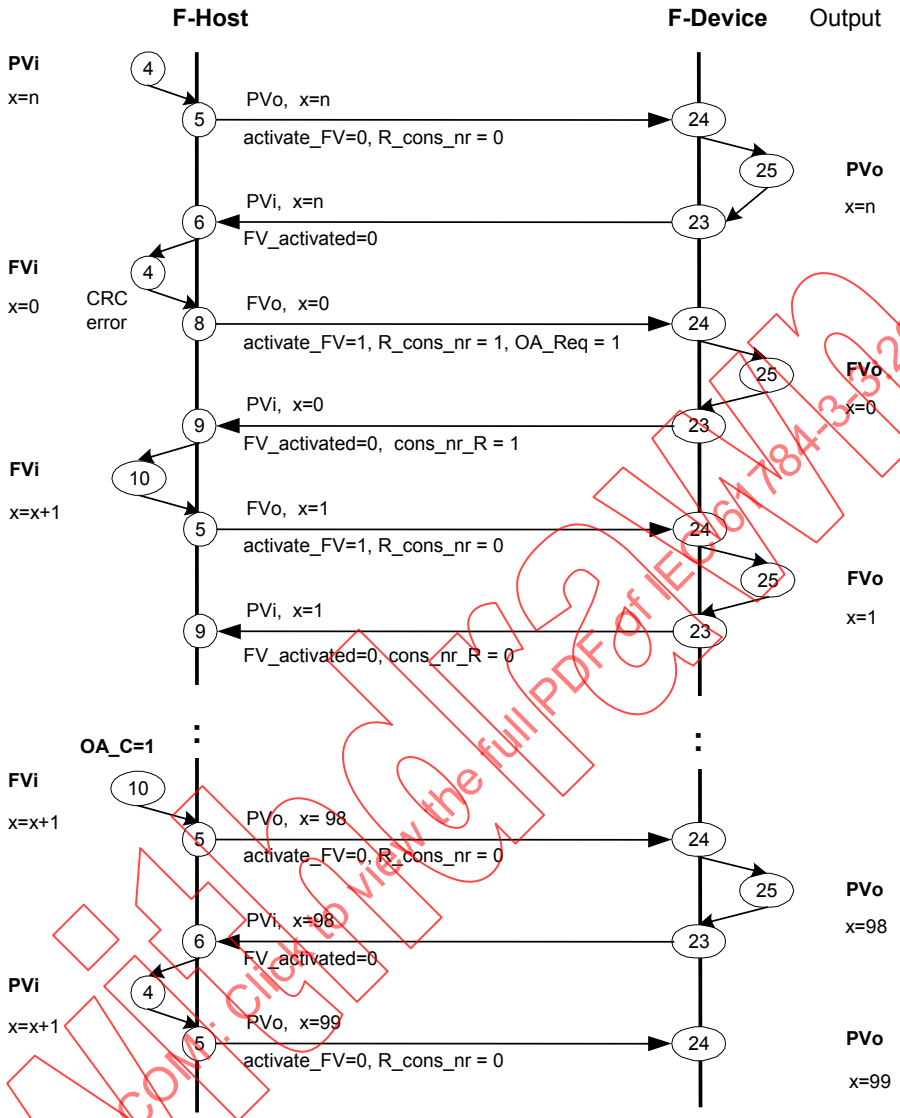


Figure 34 – Interaction F-Host / F-Device while host recognizes CRC error

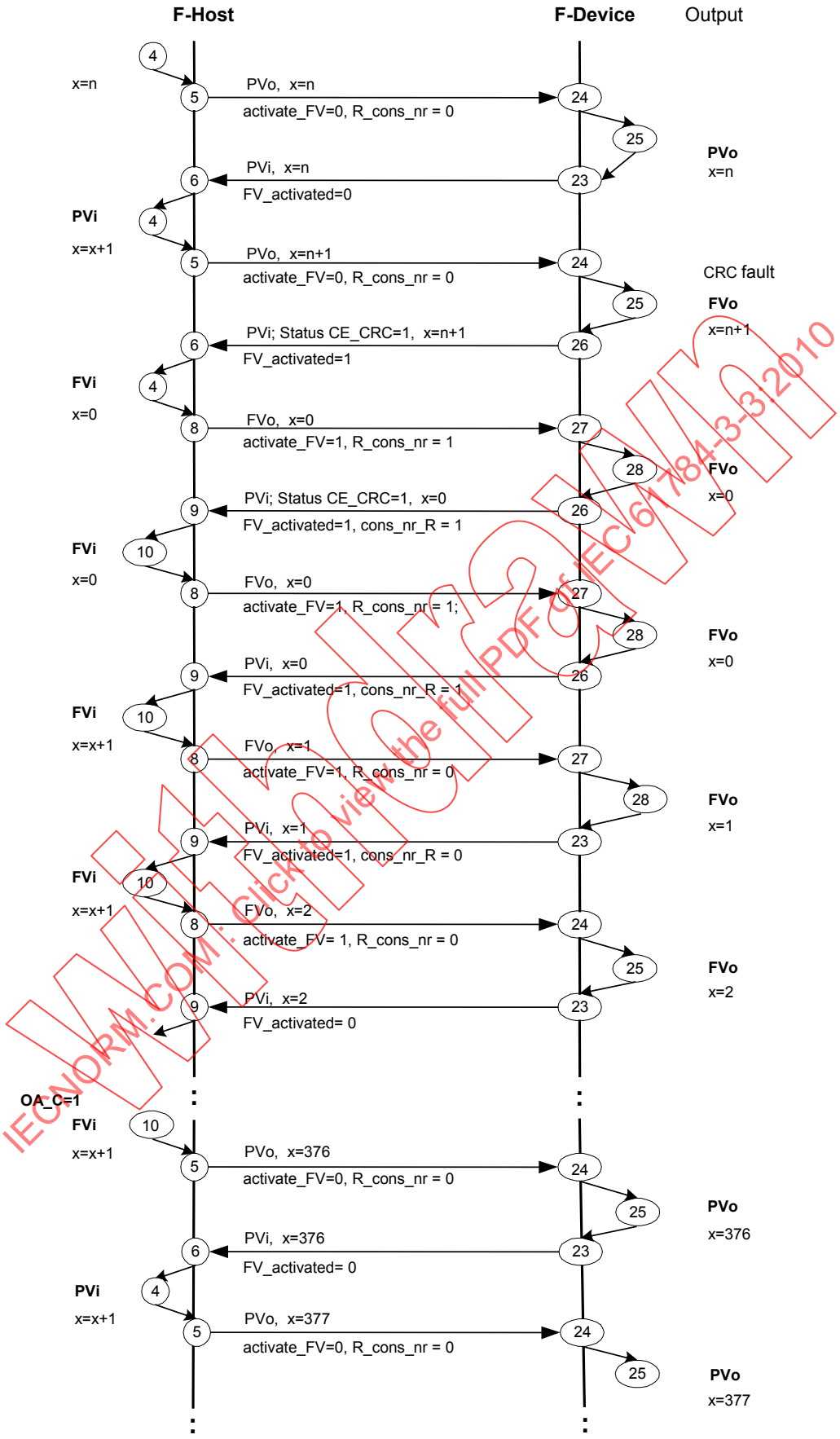


Figure 35 – Interaction F-Host / F-Device while device recognizes CRC error

7.2.5 Timing diagram for a counter reset

Figure 36 demonstrates the consequences of an F communication fault on the consecutive number counter and depending items. Only after such a fault, bit 2 of the Control Byte "R_cons_nr" is set (=1) and in consequence the output values of an F-Output-Device are set to "0" and the consecutive number counter is set to "0" (Vconsnr_d). At the same time bit 4 of the Control Byte "activate_FV" is set (=1) thus causing the F-Output-Device to set-up its own fail-safe state whenever this state cannot be achieved with the regular output values (FV).

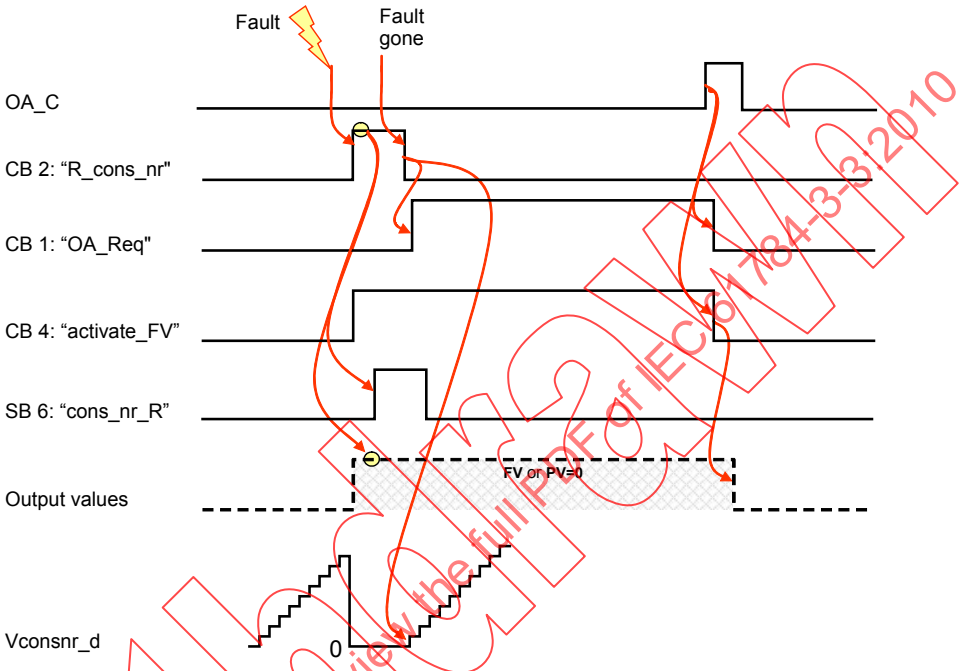


Figure 36 – Impact of the counter reset signal

Meanwhile the F-Host is sending the signal "OA_Req" as bit 1 of the Control Byte to the F-Device. This signal can be used to indicate the user via LED (9.1) that an error occurred and an Operator Acknowledgement is requested (OA_C). Right after the fault is gone the following actions take place:

- counter reset resumes its default value (R_cons_nr = 0);
- the consecutive number counter restarts counting.

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

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

7.2.6 Monitoring of safety times

7.2.6.1 Normal operation

Figure 37 demonstrates how the F driver is using the underlying CP 3/RTE communications and how some monitoring times are defined. Meaning of the short arrows: in CP 3/RTE, the IO Controller sends the same safety PDU more frequently to the F-Device than a new safety PDU is generated by the F driver within the host cycle time in the F-Host (consecutive number = n+1). In return the F-Device is sending the (acknowledgement) safety PDU to the IO Controller more frequently than the F Driver in the F-Device is generating a new safety PDU.

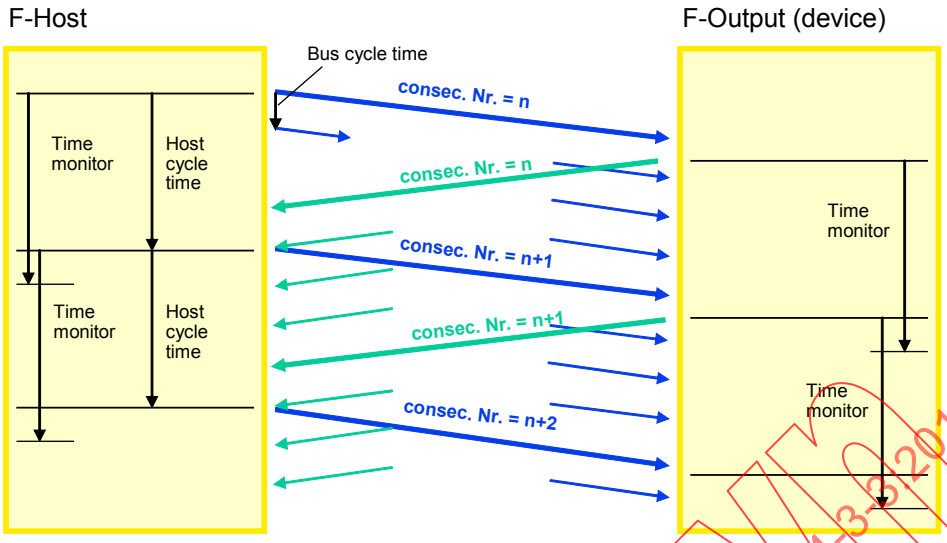


Figure 37 – Monitoring the message transit time F-Host ↔ F-Output

Figure 37 is showing the time monitoring within the F-Host and an F-Output device. Figure 38 is showing the time monitoring within the F-Input device and the F-Host. Short arrows in the figures are representing FSCP 3/1 PDUs with the currently valid (virtual) consecutive number but possibly different process values.

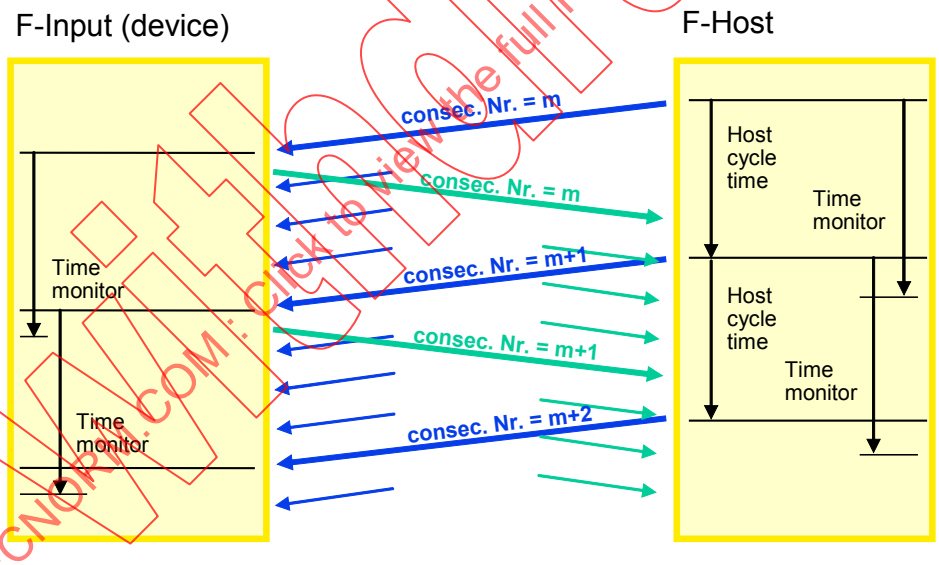


Figure 38 – Monitoring the message transit time F-Input ↔ F-Host

Other timing constraints are listed below:

Startup (Synchronization) To synchronize after a system start, the F-Host driver starts with the virtual consecutive number "0FFFFF0h". Next, the F-Host increments the virtual consecutive number after each acknowledged reception of the respective virtual consecutive number of its F-Device modulo "0FFFFFFh", skipping the value "0" and continuing with "1". At the latest before the monitoring time is about to expire, F-Input/F-Output expects a message with a virtual consecutive number that is incremented by 1. An F-Output supplies fail-safe values (FVo) after it has received a virtual consecutive number of "0".

F protocol cycle

An F-Input/F-Output returns a safety PDU to the F-Host with the same virtual consecutive number (F protocol cycle) to acknowledge the reception of a safety PDU.

The F-Host cycle time shall not exceed the F protocol cycle time (it may be shorter).

Time monitor (Watchdog)

The arrival of a new correct safety PDU at the F-Device within the watchdog time is being monitored. This verification can be performed as often as necessary, but at least once at the end of the monitoring time interval. When the watchdog time expires, the related recipient switches over to a safe state.

The slowest CP 3/RTE cycle time shall not be longer than *half* of the watchdog time. The F-Host cycle time may be shorter than the watchdog time.

Monitoring the consecutive number

A new correct safety PDU is characterized by the fact that at least the virtual consecutive number has been incremented by 1 and that either the entire rest of the safety PDU part is unchanged or has been changed faultlessly. This means that an incorrect change of the virtual consecutive number by *+1* is recognized directly by CRC2. This will then lead to a fault reaction.

Safety PDU repetition

A complete safety PDU repetition in the case that a new correct safety PDU has not been received within the watchdog time interval is not supported.

SIL monitor

Every corrupted message (CRC and virtual consecutive number fault) will be counted during a configurable SIL monitor time period (T). The fail-safe values are set whenever more than one such fault occurred, i.e. one detected corrupted message can be tolerated (*variant A*). The cases, where the whole PDU of the telegram = "0" (for example at start-up), shall not be counted.

In practice it can be shown that the counting actually always remains zero. This is the reason for an optimization of complexity resulting in *variant B*, where the SIL monitor time (T) is set to infinite. In this case, the simplified F-Host state chart of Figure 28 shall be taken into account where any detected corrupted message is not tolerated and always leads to a safe state.

Whenever such an unlikely event of a detected corrupted message should occur during the shift of production or operation, the responsible operator is assigned to play the role of the SIL-Monitor and can tolerate the indication and acknowledge it. However, with any further indication within the same shift a serious cause has to be assumed that needs immediate repair or elimination.

It is up to the F-Host manufacturer to implement variant A. However, a detailed realization is not specified here for the sake of individual adaptations to the particular system environments. The SIL monitor shall only be implemented within the F-Host.

Monitor time period (T)

The SIL monitor time period *T* is a constant value with the dimension hour (h) that results from the requested SIL and the configured CRC length (9.5.1). Table 6 specifies the SIL monitor times.

Table 6 – SIL monitor times

SIL	CRC	Length of safety PDU	Time period (h)
3	24 bit	≤ 16 octets	>10
2	24 bit	≤ 16 octets	>1
3	32 bit	≤ 128 octets	>10
2	32 bit	≤ 128 octets	>1

7.2.6.2 Extended watchdog time on request after user interaction

For use cases such as 'Configuration in Run' [69] or 'Maintenance of Fault Tolerance Systems' a certain time is required to update the affected devices. This update time usually is longer than the regular primary watchdog time (F_WD_Time) defined for a safety application. In order to avoid nuisance trips, the F-Host driver can use once a secondary watchdog time (F_WD_Time_2) to extend the primary watchdog time for these planned and monitored events as shown in Figure 39.

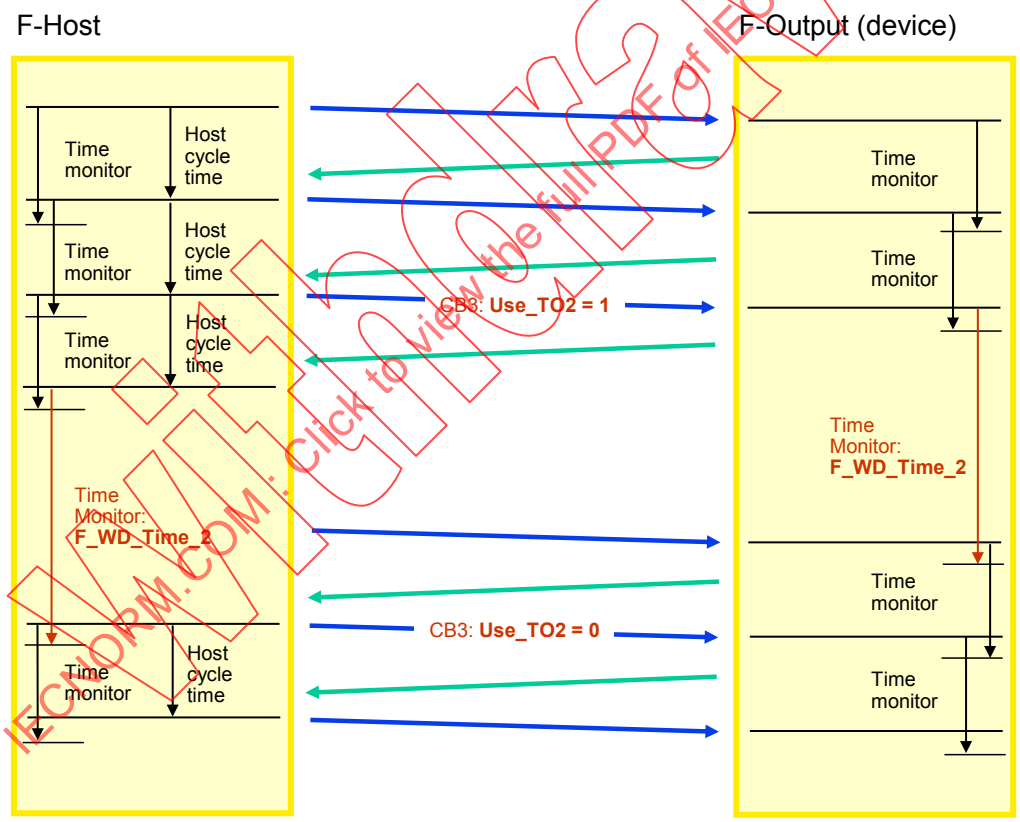


Figure 39 – Extended watchdog time on request

7.3 Reaction in the event of a malfunction

7.3.1 Repetition

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

Remedial action: The data are transferred cyclically. Thus, an incorrect message with a safety PDU that is inserted once will immediately be overwritten by a correct message. The thereby *possible delay* of an emergency request can be *one watchdog time*.

7.3.2 Loss

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

Remedial action: Lost information will be discovered by stringently incrementing and examining the consecutive number.

7.3.3 Insertion

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

Remedial action: Due to the stringently sequential expectation of the consecutive number, the recipient will discover an inserted message.

7.3.4 Incorrect sequence

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

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

7.3.5 Corruption of safety data

Quote: "The malfunction of a bus device or the transmission link perturbs safety messages."

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

F-Parameter data	Safety PDU			
	F-I/O data	Status or Control Byte	(Virtual) Consecutive Number	CRC2
F-Parameter: Codename, WD time, SIL, etc.				Across F-I/O data, Status or Control Byte, (Virtual) Consecutive Number, and F-Parameters
	m octets	1 octet	3 octets	3 or 4 octets

Figure 40 – F-Parameter data and CRC

The CRC2 signature is generated across the F-Parameters (including the codename), the F I/O data, the virtual consecutive number, and the Control/Status Byte (see 7.1.5 and Figure 40). The codename (source-destination relationship) of F-Host and F-Device is defined during the configuration phase with the help of an engineering tool and retentively stored.

After a repair, the F-Address of an F-Module/Device shall be restored / adjusted before the safety operation is resumed.

7.3.6 Delay

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

Remedial action:

- Consecutive number in the sender data and in the acknowledgment data.
- Watchdog time in the respective recipient (watchdog time for F communication).

The watchdog time is defined 9.3.3.

7.3.7 Masquerade

Quote: "The malfunction of a bus device causes safety-relevant messages and non-safety-relevant messages to be mixed up".

Remedial action: The data are coming from the correct sender and are going to the correct recipient (authenticity). This authenticity is guaranteed through inclusion of the F-Parameters with the F-Address (F source-destination relationship) into the CRC2 signature.

Principle of safe addressing:

Detecting the interconnection of safety-relevant and non-safety-relevant messages is guaranteed by the fact that a standard device is not capable of creating a safety PDU with the correct CRC2 and the correct consecutive number.

Detecting data from a different sender or for a different recipient is guaranteed by the fact that the F sender that belongs to the F source-destination relationship (codename) is the only one that generates exactly the matching CRC signature that is expected by the F receiver. At the same time, the recipient employs this CRC signature for implicitly checking the authenticity of the F sender address (since it was included in the CRC).

A retentive selection of the F address in the individual devices can be achieved through one of the following methods:

— coding switch in the unit for the codename (the F-Device address of compact Devices, for example);

— a one-time device parameterization by software that requires to be checked whether the correct device has been addressed. This shall be repeated when such a unit is replaced;

— by address mechanisms that are independent of CPF 3 addressing.

Sabotage is not assumed.

7.3.8 Memory failures within switches

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

See Figure 9 and Figure 10 as possible safety network examples for the following considerations. Central elements of these networks are switches, which are fairly complex active network components. They can have different faults. Messages may be sent to the wrong destination or their data content can be perturbed. Furthermore a switch can send stored messages over and over again even when the sender already was shut down. Table 7

contains a list of possible switch faults and their remedial measures to achieve sufficient safety.

Table 7 – Remedies for switch failures

Fault type	Detection and Mastering
Perturbed data	CRC signature (24 bit)
Wrong destination	Codename (2 x 16 bit)
Lost safety message	Consecutive number (24 bit) and Timeout
Duplicated message	Consecutive number (24 bit)
Delayed message	Timeout
Retransmission of stored messages with less than 3 consecutive safety PDUs in series. The F-Host is no longer connected.	Consecutive number (24 bit) and no automatic restart
Retransmission of stored messages with 3 or more consecutive safety PDUs in series. The F-Host is no longer connected.	Consecutive number (24 bit) and fault reaction via the Control Byte (Figure 36)

The following faults are detected / mastered:

— The F-Host faults or *its* safety PDUs do not reach the receiver. A switch transmits the messages of its revolving buffer without the correct consecutive number instead. The F-Device recognizes a consecutive number fault and sets failsafe values.

— A single message of the switch buffer is retransmitted and has a safety PDU with the correct consecutive number. This fault will be detected due to the 24 bit consecutive number and the fact that the restart of the F-Output-Device needs an OA_C = 1 (Operator Acknowledgement).

— A switch transmits messages with safety PDUs out of its revolving buffer *with* the correct consecutive numbers and this message sequence starts within the safety watchdog time. This fault will be detected due to the 24 bit consecutive number and the fact that the restart of the F-Output-Device needs an OA_C = 1 (Operator Acknowledgement).

7.3.9 Network boundaries and router

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

For CP 3/RTE networks with routers Figure 11 applies and the corresponding explanations. Let's assume such a system with subnetworks connected via routers. The following considerations are demonstrating that a single error will not misdirect a safety PDU to the wrong F-Device and will not cause it to switch to a dangerous state.

The router connects two or more subnets over layer 3 levels. Every F-Host and F-Device can be configured to "use router" together with an appropriate router address. The router manages IP addresses of the connected subnets. Table 8 contains a list of fault types and the constraints for router operation to achieve sufficient safety.

Table 8 – Safety network boundaries

Fault type	Consequences	Detection and Mastering
Router holds the wrong address of an F-Device	Router receives message for that particular F-Device. Result: Target not found.	Timeout of F-Device
Two F-Devices with identical addresses. One in subnet 0, the other one in subnet 1 Constraint: 2-Port-Router as in Figure 11	1) F-Device of subnet 0 not found in subnet 0 2) F-Device of subnet 0 not reachable in subnet 1 3) F-Device of subnet 1 not reachable in subnet 0 4) F-Device of subnet 1 correct in subnet 1	By standard CP 3/RTE
Two F-Devices with identical addresses. One in subnet 0, the other one in subnet 1 Constraint: Router with single port (for example PC, Laptop):	1) F-Device of subnet 0 not found in subnet 0 2) Address doubling in subnet 1	Single port routers are not building (safety) network boundaries

7.4 F-Startup and change coordination

7.4.1 Standard startup procedure

The startup of the F-Devices/Modules is based on the standard CP 3/RTE. The safety layers within the F-Host and the F-Device are starting at their own whenever the CP 3/RTE channels are communicating with each other cyclically. The previously executed supply of the safety layers with their special F-Parameters is embedded in the normal configuration and parameterization process ("Context") of CP 3/RTE. Any repetition of the F-Parameter supply with identical values at runtime shall be ignored; deviating values shall result in a safe state.

NOTE See [48] for details of the V1-mode.

Figure 15 shows the basic communication mechanisms of CP 3/RTE. Document [55], IEC 61158-5-10, and IEC 61158-6-10 are providing information on the startup sequences of an IO-Controller and its IO-Devices, which are part of the F-Devices.

7.4.2 iParameter assignment deblocking

Due to a diagnosis message of the F-Device that needs additional iParameters (8.2) or per external request, the F-Host sets bit 0 ("iParameter Assignment Deblocked") within the Control Byte of its next safety PDU. The F-Device then receives via "Write-Record"-commands - data set by data set - the iParameters and acknowledges at the end by setting bit 0 ("F-Device has new iParameter values assigned") within the Status Byte of its next safety PDU (Figure 41).

Deblocking only is permitted if there is no hazardous process state. The variables "iPar_EN_C" and "iPar_OK_S" which are correlated with bit 0 of the Status/Control Byte can be used in the context of the Proxy-FB-iParameterization (8.6.2). It cannot be used in the context of the iPar-Server (8.6.4). The signal sequence in Figure 41 is exemplifying a possible application.

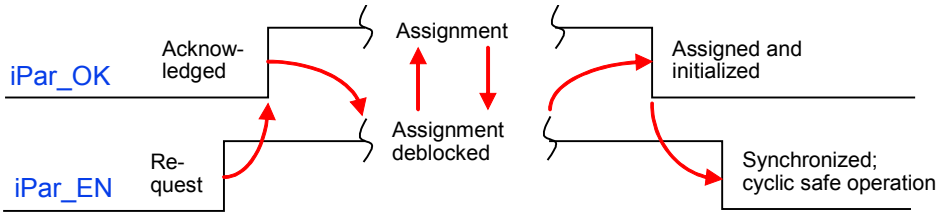


Figure 41 – iParameter assignment deblocking by the F-Host

8 Safety communication layer management

8.1 F-Parameter

8.1.1 Summary

The parameter values of the CP 3/RTE devices on the black channel are assigned according to the standard CP 3/RTE, i.e. via GSD files based on the GSD description languages (see [43] and [47]). The F-Parameters additionally required for the safety layer can be loaded via several alternative parameterization options.

Summary of the F-Parameters:

- F_S/D_Address — "Codename" between sender and recipient
- F_WD_Time — Watchdog time in the F-Device/Module (default in the GSD file: maximum processing time of the F-Device/Module)
- F_WD_Time_2 — Optional secondary watchdog time in F-Devices/Modules designed for 'Configuration in Run' or 'fault tolerance systems' to extend the time monitoring in case of planned upates by authorized personnel only (7.2.6.2)
- F_Prm_Flag1 + 2 — Parameter octets containing several parameters for the profile management
  - F_Check_SeqNr — V2-mode: consecutive number always to be included in CRC2 generation
  - F_Check_iPar — Manufacturer specific use within homogeneous systems
  - F_SIL — Check: configured SIL = employed SIL?
  - F_CRC_Length — CRC2 length
  - F_Block_ID — Parameter block type identification
  - F_Par_Version — Version No. of F-Parameters/FSCP 3/1 operational mode
- F_iPar_CRC — Value of the iParameter CRC calculation, at least manually transferred from a CPD tool to the engineering tool
- F_Par_CRC — CRC1 signature calculation across the F-Parameters

8.1.2 F_Source/Destination_Address (codename)

The addresses of the F components of a safety control loop such as F-Input, F-Host and F-Output shall be unambiguous within the borders of one subnet. Subnets are connected to each other via (2-port) routers, which are natural borders for CP 3/RTE (5.4.2). Locally, each F-Device holds the configured source-destination relationship of the safety communication link with its partner ("F_Source/Destination_Address" or short "F_S/D_Address"). It is retentively stored in the F-Devices, is a part of the F-Parameter set, and, consequently, is cyclically checked by the safety layer. The F_S/D_Address parameters are logic address designations that can be assigned *freely* but *unambiguously*. They are allocated to the CP 3/RTE addresses during the configuration (7.3.7). The addresses *0* and *0FFFFh* shall be *excluded*.

The parameter consists of two parts: "F_Source_Add" and "F_Dest_Add": each of data type Unsigned16

8.1.3 F_WD_Time (F-Watchdog time)

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

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

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

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

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

8.1.4 F_WD_Time_2 (secondary F-Watchdog time)

This secondary F-Watchdog time can be used optionally to extend the regular F-Watchdog time by one extra time F_WD_Time_2 that is needed for the update of F-Devices/Modules as demonstrated in Figure 42.

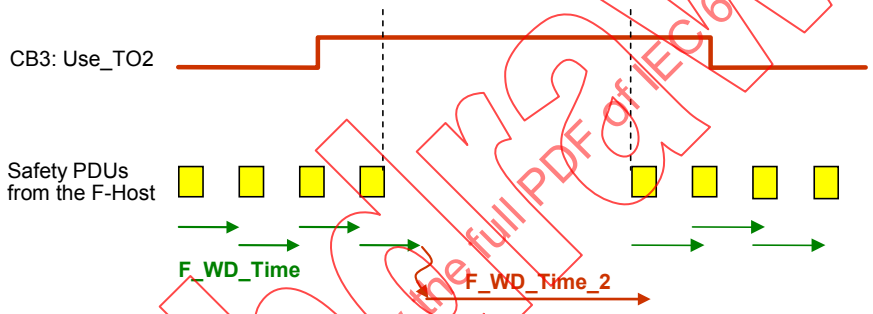


Figure 42 – Effect of F_WD_Time_2

The F_WD_Time_2 parameter is encoded as follows: Unsigned16. Time base: *1 ms*. The value range is 1 to 65 535.

8.1.5 F_Prm_Flag1 (Parameters for the safety layer management)

8.1.5.1 Structure of F_Prm_Flag1

Subclauses 8.1.5.2 to 8.1.5.5 are describing the details of the F_Prm_Flag1 parameter octet. It has the structure as in Figure 43:

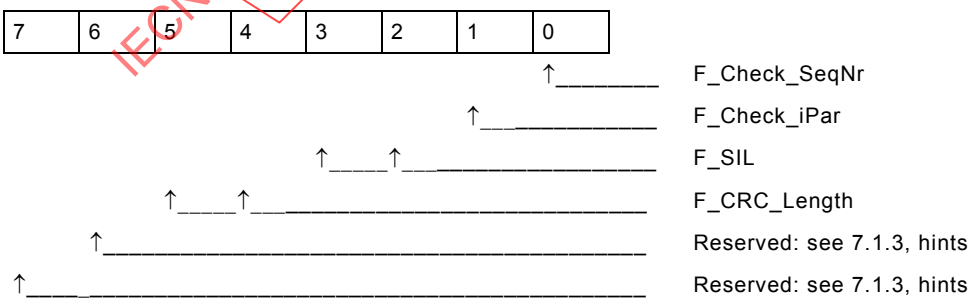


Figure 43 – F_Prm_Flag1

8.1.5.2 F_Check_SeqNr (consecutive number in CRC2)

This parameter defines whether or not the consecutive number shall be included in the CRC2 signature (see Figure 44). The parameter is distributed to the F component during startup.

It is encoded as follows: Bit 0 of the parameter octet "F_Prm_Flag1"

7	6	5	4	3	2	1	0		
							0	=	No check (Don't care in V2-mode; notation in GSD shall be "NoCheck")
							1	=	Check (Don't care in V2-mode; notation in GSD shall be "Check")

Figure 44 – F_Check_SeqNr

8.1.5.3 F_Check_iPar

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

It is encoded as follows: Bit 1of the parameter octet "F_Prm_Flag1"

7	6	5	4	3	2	1	0		
						0		=	No check (notation in GSD shall be "NoCheck")
						1		=	Check (manufacturer specific use)

Figure 45 – F_Check_iPar

8.1.5.4 F_SIL (SIL stage)

FSCP 3/1 permits parallel operation of standard communication and safety-relevant communication. The different safety functions using safety-relevant communication may require different safety integrity levels (SIL 1 ...SIL 3). The F-Devices are able to compare their own assigned SIL with the configured SIL (F_SIL). If it is higher than the SIL of the connected F-Device/Module, the "device failure" Status Bit is set and a safe state reaction is triggered. There are four different stages: SIL 1...SIL 3, NoSIL (see Figure 46).

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

7	6	5	4	3	2	1	0		
				0	0			=	SIL 1 (notation in GSD shall be "SIL1")
				0	1			=	SIL 2 (notation in GSD shall be "SIL2")
				1	0			=	SIL 3 (notation in GSD shall be "SIL3")
				1	1			=	No SIL (notation in GSD shall be "NoSIL"): for example in PA devices

Figure 46 – F_SIL

8.1.5.5 F_CRC_Length (length of the CRC2 signature)

Depending on the length of the F I/O data (12 or 123 octets) and the SIL stage, a CRC of 2, 3, or 4 octets is required (see Figure 47). This parameter transfers the expected length of the CRC2 signature in the safety PDU to the F component during startup.

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

7	6	5	4	3	2	1	0		
		0	0					=	3 octet CRC2 signature (V2-mode only; notation in GSD shall be "3-Byte-CRC")
		0	1					=	2 octet CRC2 signature (V1-mode only; notation in GSD shall be "2-Byte-CRC")
		1	0					=	4 octet CRC2 signature (optional in V1/V2-mode; notation in GSD shall be "4-Byte-CRC")
		1	1					=	Reserved: see 7.1.3, hints

Figure 47 – F_CRC_Length

8.1.6 F_Prm_Flag2 (Parameters for the safety layer management)

8.1.6.1 Structure of F_Prm_Flag2

Subclauses 8.1.6.2 to 8.1.6.3 are describing the details of the F_Prm_Flag2 parameter octet. It has the structure as in Figure 48:

7	6	5	4	3	2	1	0	
					↑_____	↑_____	↑_____	Reserved: see 7.1.3, hints
		↑_____	↑_____	↑_____				F_Block_ID
↑_____	↑_____							F_Par_Version

Figure 48 – F_Prm_Flag2

8.1.6.2 F_Block_ID (type identification of parameters)

In order to distinct parameters for future FSCP 3/1 modes, parameter type identification "F_Block_ID" is encoded in the following manner: Bits 3, 4 and 5 of the parameter octet "F_Prm_Flag2" (see Figure 49). It is mandatory for the safety layer to check the F_Block_ID.

7	6	5	4	3	2	1	0		
		0	0	0				=	No F_iPar_CRC, no F_WD_Time_2
		0	0	1				=	F_iPar_CRC (Figure 51)
		0	1	0				=	F_WD_Time_2 (Figure 42), no F_iPar_CRC
		0	1	1				=	F_WD_Time_2 and F_iPar_CRC
		1	0	0				=	Reserved
		1	0	1				=	Reserved
		1	1	0				=	Reserved
		1	1	1				=	Reserved

Figure 49 – F_Block_ID

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

The purpose of this version counter is to identify new releases of an operational mode inside the safety layer. The F-Device shall respond with a device-specific diagnosis message in case the requested version of the safety layer does not match the implemented version (see 6.3.2 and Figure 50). Validity checking of F-Parameters shall be done by the safety layer.

7	6	5	4	3	2	1	0

0	0	=	Valid for V1-mode (notation in GSD shall be "V1-mode")
0	1	=	Valid for V2-mode (notation in GSD shall be "V2-mode")
1	0	=	Reserved: see 7.1.3, hints
1	1	=	Reserved: see 7.1.3, hints

Figure 50 – F_Par_Version

8.1.7 F_iPar_CRC (value of iPar_CRC across iParameters)

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

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

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

8.1.8 F_Par_CRC (CRC1 across F-Parameters)

The engineering tool is generating this CRC1 signature across the F-parameters. The initial value for CRC1 is 0. See 8.3.3.2 for details on the order of the F-Parameters to be used for generating the CRC1 signature. The same 16-bit CRC polynomial is used (1*4EAB*h). CRC1 is the initial value for cyclic CRC2 computation.

The following rules apply for the different CRC2 polynomials:

- In case of a 24 bit CRC polynomial (1*5D6DCB*h) the initial value for CRC2 calculations is "00xxxx", where xxxx=CRC1.
- In case of a 32 bit CRC polynomial (1*F4ACFB13*h) the initial value for CRC2 calculations is "0000xxxx", where xxxx=CRC1.

It is encoded as: Unsigned16.

8.1.9 Structure of the F-Parameter record data object

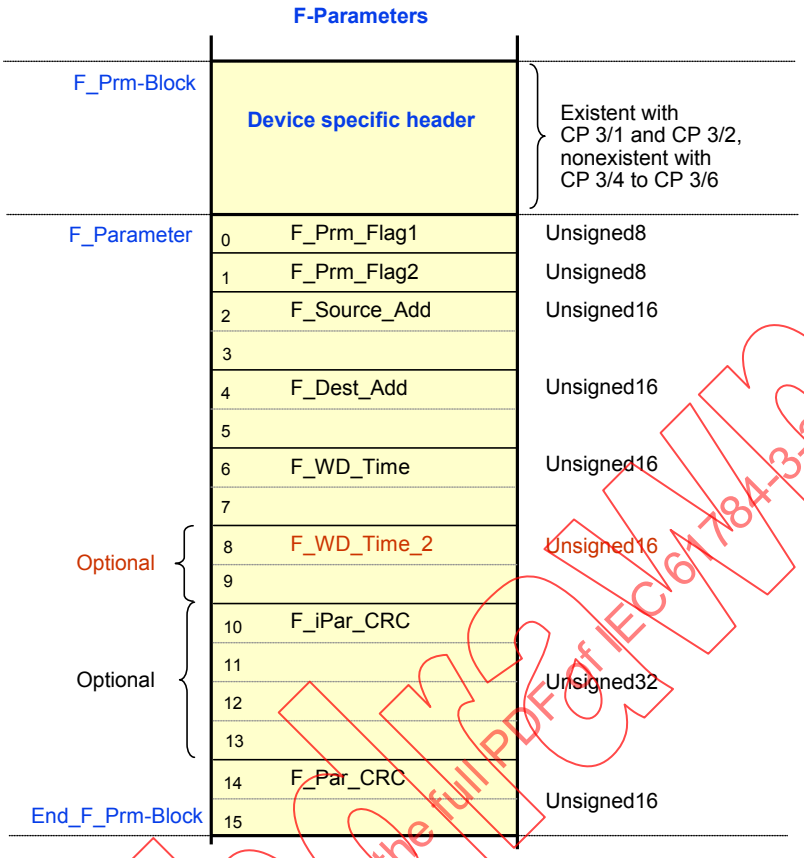


Figure 51 – F-Parameter

The Figure 51 shows the structure of the F-Parameter block within a CP 3/RTE record data object. The octet ordering is according to standard CP 3/RTE. The following applies to modular F-Devices: For each F-Submodule, an F_Parameter-Block is inserted in the context message (Figure 13). The allocation of the submodule to the F-Device comes about the chosen subslot number.

8.1.10 F-Data fraction

See 7.1.6.

8.2 iParameter and iPar_CRC

F_Devices are increasingly provided with smart functions that require extensive individual F-Device parameter values to be assigned. These safety-related parameters are called iParameters. In particular in the event of a device replacement it is expedient to load these parameters directly via the bus on the standard path. These parameter records usually exceed the range of parameterization data based on GSD (several laser scanners with approximately 1 kB per protection zone may lead to an overall quantity of up to *90 kB* and more) and so this FSCP 3/1 specification provides additional mechanisms.

Figure 52 shows a proposal for the structuring of large amounts of iParameters for up- and download purposes. The absolute upper limit for iParameters is 2^{22}-1 octets; the lower limit is 4 octets. Thus segmentation is required with CP 3/1 whenever the total exceeds 240 octets as shown in Figure 52. No segmentation is required with CP 3/RTE.

The CRC signature ("iPar_CRC") shall be calculated across the iParameters (Figure 52) using any appropriate CRC polynomial and filled into the 4 octet iPar_CRC in hexadecimal format

and displayed on the CPD-Tool. Whenever the calculation results in a "0", the value shall be set to "1". Inclusion of the iPar_CRC value in the iParameters as shown in Figure 52 is optional. No safety proof of sufficient residual error rate is required when using FSCP 3/1's 32 bit CRC polynomial.

The F_source/destination relationship (codename) allows checking of delivery to the configured recipient. Inclusion in the iParameters as shown in Figure 52 is optional.

Identification and maintenance functions (I&M) are mandatory for all the CPF 3 devices. They provide codes identifying the type and release of a particular device/module. Including such information in the iParameter set can be used to check the validity of a replacement device with its own I&M functions. Inclusion in the iParameters as shown in Figure 52 is optional. Device manufacturers can use their own codings.

The length of the iParameter block can be helpful to efficiently organize the up- and download processes within the devices. Inclusion in the iParameters as shown in Figure 52 is optional.

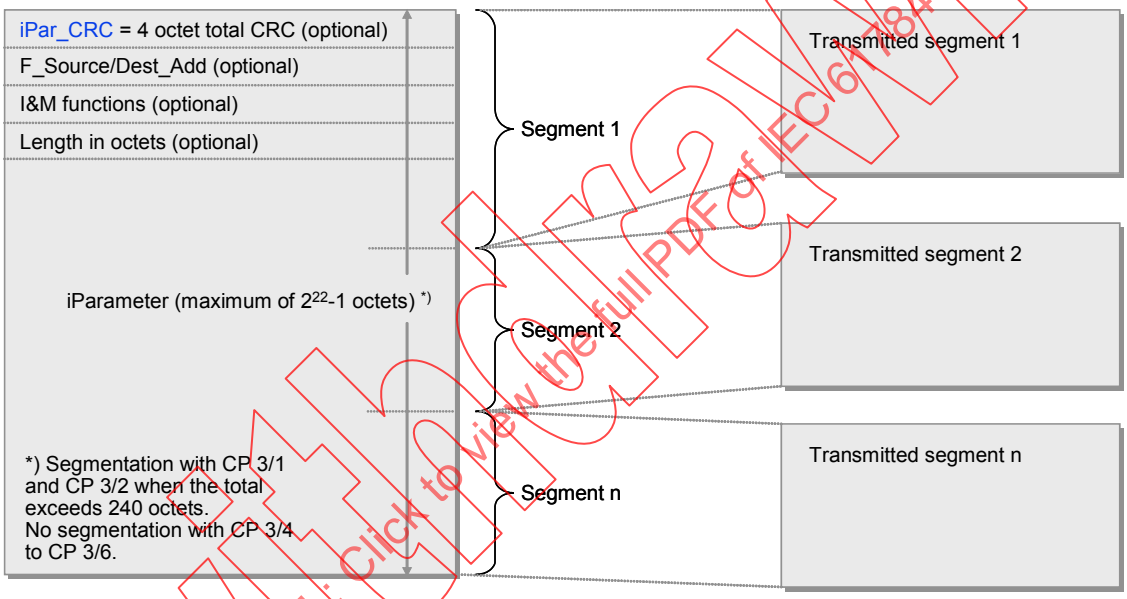


Figure 52 – iParameter block

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

8.3 Safety parameterization

8.3.1 Objectives

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

For iParameterization the possibility of an individual Proxy-FB is defined since the very first beginning of FSCP 3/1. This Proxy-FB is based on the recommendations of [49] and the F-Device manufacturer takes responsibility for it. The Proxy-FB concept is described in 8.6.2.

For small amount of iParameters such as for input modules of a remote I/O the Proxy-FB concept implicates too much logistic overhead and thus a standardized Proxy-FB, the "iPar-Server" is specified here. In contrast to the Proxy-FB the F-Host/system manufacturer takes

responsibility for the iPar-Server and provides this feature either within the standard function block library or as a built-in function. The iPar-Server concept is specified in 8.6.4.

The small set of identical F-Parameters through all the different F-Devices is passed over to the safety-related network configuration part of an engineering tool via GSD (general station description) and thus provides a constant and uncomplex user interface. Moreover it protects against a GSD version dilemma and correlated approval efforts of the network configuration part.

After the adjustment of the F-Parameters during network configuration, an F-Parameter record is compiled and stored within the F-Host/IO-controller for start-up of the network.

The F-Parameter "F_IO_StructureDescCRC" is used to ensure correct usage of the F-I/O data structure and data types by the F user program and thus is not transferred to the F-Device during start-up.

8.3.2 GSDL and GSDML safety extensions

8.3.2.1 GSDL extensions

FSCP 3/1 supports physical or virtual module oriented devices. The General Station Description Language (GSDL) specification [43] (see ISO 15745-3 also) therefore defines keywords to structure and identify the F-Parameter block information of F-Modules shown in Figure 51. The possible F-Parameter value selections are contained in a General Station Description (GSD) file associated with an F-Slave the F-Module is designed for. The following keywords in Table 9 are defined.

Table 9 — GSDL keywords for F-Parameters and F-I/O structures

GSDL Keyword	Description
F_Ext_Module_Prm_Data_Len	The parameter associated with this keyword indicates the total length of the F_Prm-Block shown in Figure 51, usually 14 or 18 octets depending on F_iPar_CRC
F_Ext_Module_Prm_Data_Const (offset)	With the help of the parameter associated with this keyword a fixed value can be entered into one of the 4 header octets of the F_Prm-Block shown in Figure 51. The position of an octet is indicated by an offset 0…3
F_Ext_Module_Prm_Data_Const (0)	Indicates the F_Prm_Block length including the F-iPar_CRC, e.g. 0x12
F_Ext_Module_Prm_Data_Const (1)	Identification of the F_Prm-Block = 5 (fix)
F_Ext_Module_Prm_Data_Const (2)	Slot of the F-Module
F_Ext_Module_Prm_Data_Const (3)	Reserved. Shall be set "0".
F_Ext_Module_Prm_Data_Ref (offset)	With the help of the parameter associated with this keyword a user selectable value at configuration time can be entered into one of the octets 0…13 of the F_Prm-Block shown in Figure 51. The position of an octet is indicated by an offset 4…16. The parameter is pointing to an ExtUserPrmData range definition within other parts of the GSD file
F_ParamDescCRC	The parameter associated with this keyword secures the safety-related parts of the F-Parameter descriptions within the GSD file. See 8.3.3.3 for details on how to determine this CRC0 signature
F_IO_StructureDescCRC	The parameter associated with this keyword secures the description of the F-I/O data structure (cyclically transferred process values). See [43] and 8.4.1 for details on how to determine this CRC7 signature
F_IO_StructureDescVersion	The parameter associated with this keyword indicates the version of an F_IO data structure description. A value of 1 indicates a 16-bit CRC7 signature while a value of 2 indicates a 32-bit CRC7 signature. If this attribute is not present, a value of 1 is assumed

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

8.3.2.2 GSDML extensions

The F-Parameters of a particular F-Device are defined with the help of its GSD file. The description is provided using the General Station Description Markup Language (GSDML) based on XML (see ISO 15745-3, ISO 15745-4, and [47]).

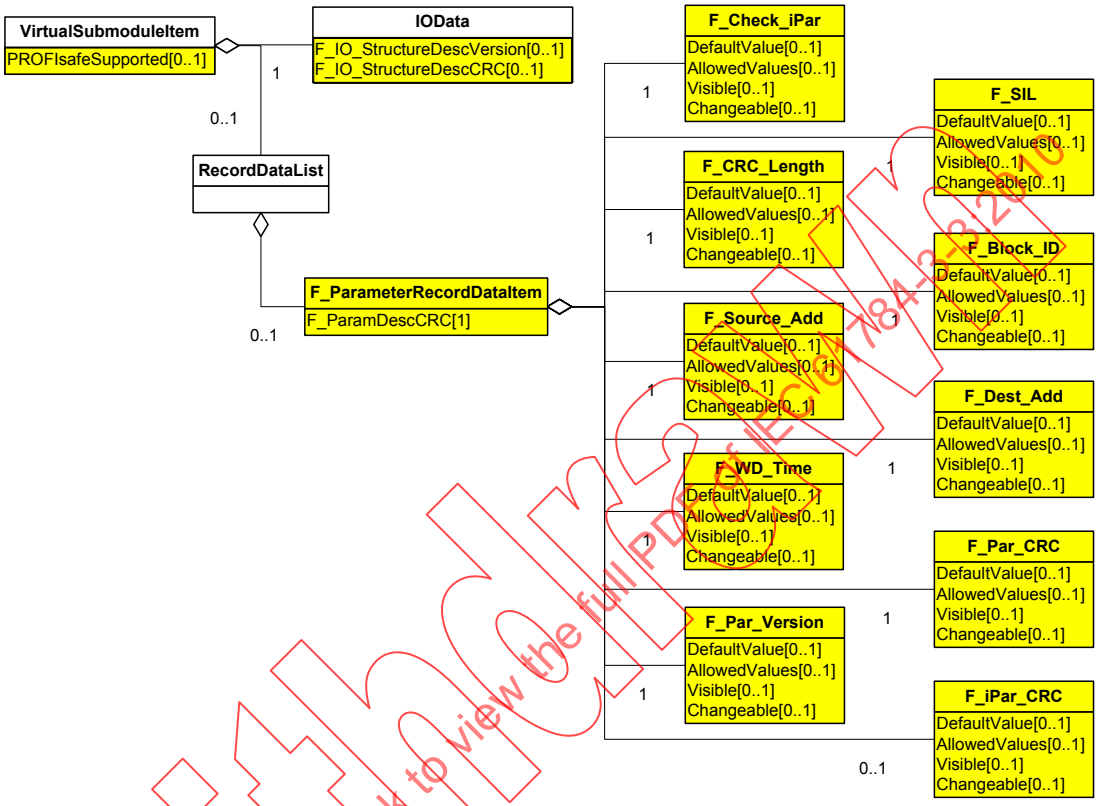


Figure 53 – F-Parameter extension within the GSDML specification

Figure 53 is showing the extensions within the GSDML. The section "VirtualSubmoduleItem" provides an additional attribute "F_ParamDescCRC". This is the CRC signature (CRC0) of the F-Parameter description in Figure 53. The "F_IO_StructureDescCRC" in section "IOData" secures the formats of the F-Input and F-Output data. The "F_IO_StructureDescVersion" indicates the version of an F_IO data structure description (see 8.3.3).

8.3.3 Securing safety parameters and GSD data

8.3.3.1 General

It is vital for the safety of the system to secure the safety parameters of the safety layer (F-Parameters) and of the safety technology of the F-Device (iParameters) as well as the configured safety I/O data structures. This is done via CRC signatures, persistent storage within the F-Device and in the F-Host and periodical comparison of CRC signatures.

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

8.3.3.2 CRC1 and iPar_CRC across safety parameters

Figure 25 is only showing the CRC1 signature across the F-Parameters that shall be involved in the CRC2 signature generating process. However, optionally there can be involved more CRC signatures as follows in this clause.

In order to secure the F-Parameters, the engineering tool of the F-Host is generating the *CRC1* signature as described in 8.1.7. The CRC polynomial to use is 1*4EAB*h. The CRC1 signature is build across all F-Parameters in the octet order of Figure 51 excluding the optional F_iPar_CRC. Whenever bit 3 of the F-Parameter "F_Block_ID" is set "1" the F_iPar_CRC signature shall be included at the beginning of the calculation as shown in Figure 54.

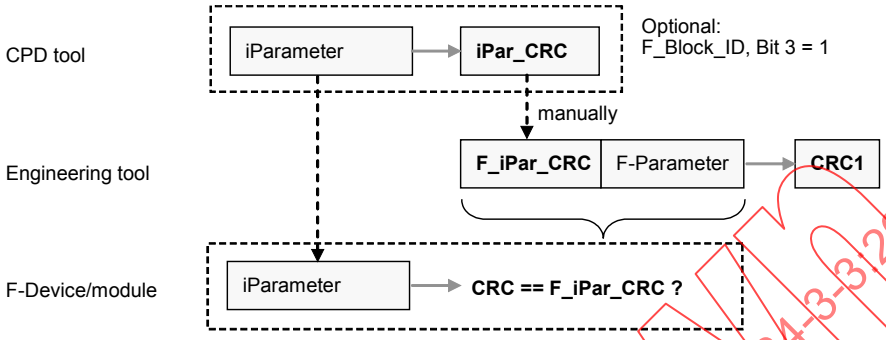


Figure 54 – CRC1 including iPar_CRC

The generated CRC1 signature value (Unsigned16) is stored and used further in the inverse octet order (see 7.1.5).

8.3.3.3 CRC0 across GSD data

In order to make sure that safety relevant parameters of the F-Device will not change unnoticed during lifetime of a storage media and can be read safely into the configuration tool they all are CRC protected. The parameter "F_ParamDescCRC" contains a 2-octet CRC signature (CRC0) generated with the help of the same 16-bit CRC polynomial (1*4EAB*h) that is used all over FSCP 3/1.

In case of a GSD file for an F-Slave (CP 3/1 or CP 3/2) the CRC0 signature calculation starts with the first F_Ext_User_Prm_Data_Ref(4) and scans across all keywords of the same type and their F-Parameter definitions in the "ExtUserPrmData" description and "PrmText" selection sections. The pseudo code in Figure 55 demonstrates the algorithm of how to generate the 2 octet CRC0 nearly independent from the structure of the GSD file and the comments, thus allowing the designer of the file a maximum of freedom and changeability. The underlined characters are included in the calculation.

```
//Every F_Ext_User_Prm_Data_Ref(x) one after the other in ascending order (byte offset, bit offset)
//The header of the F_Prm-Block is ignored
for (F_Par_Ref = 0; F_Para_Ref < number of elements; F_Para_Ref ++)
{
        if (list parameter==TRUE)  // PrmText with at least two selections
        {
                // in case of F parameters with "PrmText" definitions
                // read name of corresponding F_Parameter
                // e.g. ExtUserPrmData              = 8 "F_CRC_Length"
                // read data format (0: Bit, 1: Unsigned8, 2: Unsigned16, 3: Unsigned32)
                // read Bit offset (0 if Unsigned8/Unsigned16/Unsigned32)
                // e.g. BitArea(4-5) 0 0-2                                  → 0, 4
                // read default value (LoByte, HiByte)
                // e.g. BitArea(4-5) 0 0-2                                  → 0, 0
                // now read corresponding PrmText via the text selections
                // e.g. PrmText             =       3
                // Text(0)                  =       "3-Byte-CRC"
                // Text(1)                  =       "2-Byte-CRC"
                // Text(2)                  =       "4-Byte-CRC"
                //  EndPrmText
                for (value = 0; value <= Max (Prmtext); value ++)
                {
                        // read actual value as text
                        //  e.g.                                            → "3-Byte-CRC"
                        // read actual value as number (index) (LoByte, HiByte)
                        //  e.g.                                            → 0, 0
                }
        }
        else
        // in case of F parameters with edit fields:
        {
                // read name of corresponding F_Parameter in ascending order
                // e.g. ExtUserPrmData      = 2 "F_Dest_Add"
                // read data format (0: Bit, 1: Unsigned8, 2: Unsigned16, 3: Unsigned32)
                // read Bit offset (0 if Unsigned8/Unsigned16/Unsigned32)
                // e.g. Unsigned16 1 1-65534                                → 2, 0
                // read default value (starting with LoByte)
                // Unsigned16 1 1-65534                                     → 1, 0
                // read lower limit (starting with LoByte)
                // Unsigned16 1 1-65534                                     → 1, 0
                // read upper limit (starting with LoByte)
                // Unsigned16 1 1-65534                                     → 254, 255
        }
}
// end of algorithm
```

Figure 55 – Algorithm to build CRC0 (GSDL)

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

In case of a GSD file for an F-Device (CP 3/RTE) the calculation of the 2-octet CRC signature runs across all F_ParameterRecordDataItem sections (Figure 53), including all F-Parameters and their definitions. The pseudo-code in Figure 56 demonstrates the algorithm of how to build the CRC0 nearly independent from the structure and the comments of the GSD file, thus allowing the designer of the file a maximum of design freedom and changeability without conflicts.

NOTE Some F-Parameters can be specified as invisible in GSD files for CP 3/RTE devices by setting Visible ="false". An F-Parameter will not be considered in the calculation of CRC0 in case of Visible ="false".

If attributes of F-Parameters are omitted in a GSD file, defaults of the GSDML schema still apply and shall be included in the CRC0 calculation.

```
while (F_Parameter_to_read())
{
// the F_ParameterRecordDataItem section to be read in ascending order (byte offset, bit offset).
// F-Parameter Name
// F-Parameter DataType (0: Bit / BitArea, 1: Unsigned8, 2: Unsigned16, 3: Unsigned32)
// F-Parameter BitOffset (0 if Unsigned8/Unsigned16/Unsigned32)
  // read DefaultValue (starting with LoByte, two bytes for bit parameters, Unsigned8, Unsigned16;
  // four bytes for Unsigned32)
  if (value_range) // Edit field or list parameter with one value only
  {
  // read AllowedValue 1st digit (starting with LoByte of LowerLimit)
  // read AllowedValue 2nd digit (starting with LoByte of UpperLimit)
  }
  else // List parameters with at least two textual selections
  {
   // for each AllowedValue in AllowedValueList: read AllowedValue textual description character by
   // character, then corresponding numeric value (LoByte, HiByte)
}
// end of algorithm.
```

Figure 56 – Algorithm to build CRC0 (GSDML)

For sample GSD files for F-Devices (CP 3/RTE) contact the organizations in Annex B.

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

8.4 Safety configuration

8.4.1 Securing the safety I/O data description (CRC7)

The F-I/O data structure is described in the "IOData" section of the GSD file. One attribute is the "F_IO_StructureDescCRC" = CRC7. This CRC7 is built across the attributes in Table 10 in the listed order (Version 2). The 32 bit CRC polynomial (1*F4ACFB13*h) shall be used to calculate the signature. Permitted data types for FSCP 3/1 are listed in 5.5.4. The previous version 1 of the I/O data structure item set did not comprise the attribute VERSION and the data types Integer32 and Unsigned8+Unsigned8. Thus, no keyword VERSION in a particular GSD file indicates the data types Integer32 and Unsigned8+Unsigned8 are not available, the CRC7 signature shall be calculated using the 16 bit CRC polynomial (1*4EAB*h), and the length of the CRC7 signature is 2 octets.

The parameter "F_IO_StructureDescCRC" is not transmitted to the F-Device at start-up time. The engineering tool can use this mechanism to ensure correct configuration.

Table 10 – I/O data structure items (Version 2)

Attribute name	Length	Description
VERSION	1 octet	Indicates a particular set of I/O data structure items.
IN_ADDRESS_RANGE	2 octets	Length in octets of the whole IOData Input section (including F_MessageTrailer)
COUNT_PS_INPUT_BYTES_COMPOSITE	2 octets	Input: Length of all "Float32+Unsigned8" DataItems (5 × number of)
COUNT_PS_INPUT_BYTES_U8_U8	2 octets	Input: Length of all "Unsigned8+Unsigned8" DataItems (2 x number of)
COUNT_PS_INPUT_CHANNELS_BOOL_MAX	2 octets	Input: Number of all bool channels ("used as bits") in maximum mode (for example 1oo1 mode)

Attribute name	Length	Description
COUNT_PS_INPUT_BYTES_BOOL_MAX	2 octets	Input: Length of all bool DataItems (in octets) in maximum mode (for example 1oo1 mode)
COUNT_PS_INPUT_CHANNELS_INT	2 octets	Input: Number of all Integer16 DataItems
COUNT_PS_INPUT_CHANNELS_DINT	2 octets	Input: Number of all Integer32 DataItems
COUNT_PS_INPUT_CHANNELS_REAL	2 octets	Input: Number of all Float32 DataItems
OUT_ADDRESS_RANGE	2 octets	Length in octets of the whole IOData Output section (including F_MessageTrailer)
COUNT_PS_OUTPUT_BYTES_COMPOSITE	2 octets	Output: Length of all “Float32+Unsigned8” DataItems (5 × number of)
COUNT_PS_OUTPUT_BYTES_U8_U8	2 octets	Output: Length of all “Unsigned8+Unsigned8” DataItems (2 x number of)
COUNT_PS_OUTPUT_CHANNELS_BOOL	2 octets	Output: Number of all bool channels (“used as bits”)
COUNT_PS_OUTPUT_BYTES_BOOL	2 octets	Output: Length of all Bool DataItems (in octets)
COUNT_PS_OUTPUT_CHANNELS_INT	2 octets	Output: Number of all Integer16 DataItems
COUNT_PS_OUTPUT_CHANNELS_DINT	2 octets	Output: Number of all Integer32 DataItems
COUNT_PS_OUTPUT_CHANNELS_REAL	2 octets	Output: Number of all Float32 DataItems
DATA_STRUCTURE_CRC	4 octets	“F_IO_StructureDescCRC” = CRC7

8.4.2 DataItem data type section examples

8.4.2.1 Approach

Subclauses 8.4.2.2 to 8.4.2.5 are containing example DataItem sections according to some F Channel driver types in 8.5.2 using the attributes described in Table 10.

Permitted data types for FSCP 3/1 are listed in 5.5.4. For 32 bit Boolean the data type Unsigned32 shall be used.

See [67] for general information on data types.

8.4.2.2 F_IN_OUT_1

Input: 32 bit Boolean
Output: 32 bit Boolean

The coding of the DataItem section for the F_IN_OUT_1 F_Channel_Driver example is shown in Figure 57. Table 10 contains a description of the variables.

```
<IOData>
        <Input Consistency="All items consistency">
                <DataItem DataType="Unsigned32" UseAsBits="true" TextId="Inputs" />
                <DataItem DataType="F_MessageTrailer4Byte" TextId="Safety" />
        </Input>
        <Output Consistency="All items consistency">
                <DataItem DataType="Unsigned32" UseAsBits="true" TextId="Outputs" />
                <DataItem DataType="F_MessageTrailer4Byte" TextId="Safety" />
        </Output>
</IOData>

VERSION                                  02
IN_ADDRESS_RANGE                         08
COUNT_PS_INPUT_BYTES_COMPOSITE           00
COUNT_PS_INPUT_BYTES_U8_U8               00
COUNT_PS_INPUT_CHANNELS_BOOL             32
COUNT_PS_INPUT_BYTES_BOOL                04
COUNT_PS_INPUT_CHANNELS_INT              00
COUNT_PS_INPUT_CHANNELS_DINT             00
COUNT_PS_INPUT_CHANNELS_REAL             00
OUT_ADDRESS_RANGE                        08
COUNT_PS_OUTPUT_BYTES_COMPOSITE          00
COUNT_PS_OUTPUT_BYTES_U8_U8              00
COUNT_PS_OUTPUT_CHANNELS_BOOL            32
COUNT_PS_OUTPUT_BYTES_BOOL               04
COUNT_PS_OUTPUT_CHANNELS_ INT            00
COUNT_PS_OUTPUT_CHANNELS_DINT            00
COUNT_PS_OUTPUT_CHANNELS_ REAL           00
DATA STRUCTURE CRC                       0x9EBE9328
```

Figure 57 – DataItem section for F_IN_OUT_1

8.4.2.3 F_IN_OUT_2

Input: 16 bit Boolean, 16 bit Integer;
Output: 16 bit Boolean, 16 bit Integer

The coding for the F_IN_OUT_2 F_Channel_Driver example is shown in Figure 58.

```
<IOData>
        <Input Consistency="All items consistency">
                <DataItem DataType="Unsigned16" UseAsBits="true" TextId="Inputs" />
                <DataItem DataType="Integer16" UseAsBits="false" TextId="AI channel" />
                <DataItem DataType="F_MessageTrailer4Byte" TextId="Safety" />
        </Input>
        <Output Consistency="All items consistency">
                <DataItem DataType="Unsigned16" UseAsBits="true" TextId="Outputs" />
                <DataItem DataType="Integer16" UseAsBits="false" TextId="AO channel" />
                <DataItem DataType="F_MessageTrailer4Byte" TextId="Safety" />
    </Output>
</IOData>

VERSION                                  02
IN_ADDRESS_RANGE                         08
COUNT_PS_INPUT_BYTES_COMPOSITE           00
COUNT_PS_INPUT_BYTES_U8_U8               00
COUNT_PS_INPUT_CHANNELS_BOOL             16
COUNT_PS_INPUT_BYTES_BOOL                02
COUNT_PS_INPUT_CHANNELS_INT              01
COUNT_PS_INPUT_CHANNELS_DINT             00
COUNT_PS_INPUT_CHANNELS_REAL             00
OUT_ADDRESS_RANGE                        08
COUNT_PS_OUTPUT_BYTES_COMPOSITE          00
COUNT_PS_OUTPUT_BYTES_U8_U8              00
COUNT_PS_OUTPUT_CHANNELS_BOOL            16
COUNT_PS_OUTPUT_BYTES_BOOL               02
COUNT_PS_OUTPUT_CHANNELS_ INT            01
COUNT_PS_OUTPUT_CHANNELS_DINT            00
COUNT_PS_OUTPUT_CHANNELS_ REAL           00
DATA_STRUCTURE_CRC                       0x82288330
```

Figure 58 – DataItem section for F_IN_OUT_2

8.4.2.4 F_IN_OUT_5

Input: Composite (Float32+Unsigned8)

The coding for the F_IN_OUT_5 F_Channel_Driver example is shown in Figure 59.

```
<IOData>
        <Input Consistency="All items consistency">
                <DataItem DataType="Float32+Unsigned8" TextId="AI channel" />
                <DataItem DataType="F_MessageTrailer4Byte" TextId="Safety" />
        </Input>
        <Output Consistency="All items consistency">
                <DataItem DataType="F_MessageTrailer4Byte" TextId="Safety" />
    </Output>
</IOData>

VERSION                                  01
IN_ADDRESS_RANGE                         09
COUNT_PS_INPUT_BYTES_COMPOSITE           05
COUNT_PS_INPUT_CHANNELS_BOOL             00
COUNT_PS_INPUT_BYTES_BOOL                00
COUNT_PS_INPUT_CHANNELS_INT              00
COUNT_PS_INPUT_CHANNELS_REAL             00
OUT_ADDRESS_RANGE                        04
COUNT_PS_OUTPUT_BYTES_COMPOSITE          00
COUNT_PS_OUTPUT_CHANNELS_BOOL            00
COUNT_PS_OUTPUT_BYTES_BOOL               00
COUNT_PS_OUTPUT_CHANNELS_ INT            00
COUNT_PS_OUTPUT_CHANNELS_ REAL           00
DATA_STRUCTURE_CRC                       0x8CAC
```

Figure 59 – DataItem section for F_IN_OUT_5

8.4.2.5 F_IN_OUT_6

Input: Composite Readback (Float32 + Unsigned8), Status Unsigned8, Status Unsigned8, Status Unsigned8

The coding of the DataItem section for the F_IN_OUT_6 F_Channel_Driver example is shown in Figure 60. Table 10 contains a description of the variables.

```
<IOData>
        <Input Consistency="All items consistency">
                <DataItem DataType="Float32+Unsigned8" TextId="AI channel" />
                <DataItem DataType="Unsigned8" UseAsBits="false" TextId="Status1" />
                <DataItem DataType="Unsigned8" UseAsBits="false" TextId="Status2" />
                <DataItem DataType="Unsigned8" UseAsBits="false" TextId="Status3" />
                <DataItem DataType="F_MessageTrailer4Byte" TextId="Safety" />
        </Input>
        <Output Consistency="All items consistency">
                <DataItem DataType="Float32+Unsigned8" UseAsBits="false"TextId="AO channel" />
                <DataItem DataType="F_MessageTrailer4Byte" TextId="Safety" />
    </Output>
</IOData>

VERSION                                  01
IN_ADDRESS_RANGE                         12
COUNT_PS_INPUT_BYTES_COMPOSITE           05
COUNT_PS_INPUT_CHANNELS_BOOL             24
COUNT_PS_INPUT_BYTES_BOOL                03
COUNT_PS_INPUT_CHANNELS_INT              00
COUNT_PS_INPUT_CHANNELS_REAL             00
OUT_ADDRESS_RANGE                        09
COUNT_PS_OUTPUT_BYTES_COMPOSITE          05
COUNT_PS_OUTPUT_CHANNELS_BOOL            00
COUNT_PS_OUTPUT_BYTES_BOOL               00
COUNT_PS_OUTPUT_CHANNELS_ INT            00
COUNT_PS_OUTPUT_CHANNELS_ REAL           00
DATA_STRUCTURE_CRC                       0xF33
```

Figure 60 – DataItem section for F_IN_OUT_6

8.5 Data type information usage

8.5.1 F-Channel driver

The F I/O data cyclically transferred between an F-Device and an F-Host (Real-time Channel)) needs to be controlled by a user program. A programmer is either expecting appropriate Function Blocks ("F-Channel driver") within her/his programmer's tool libraries that she/he is able to embed into the customer program. Or she/he is expecting access to discrete logically addressable input or output variables (for example for ladder logic). Figure 61 is illustrating such a programmer's view on "F-Channel driver" function blocks.

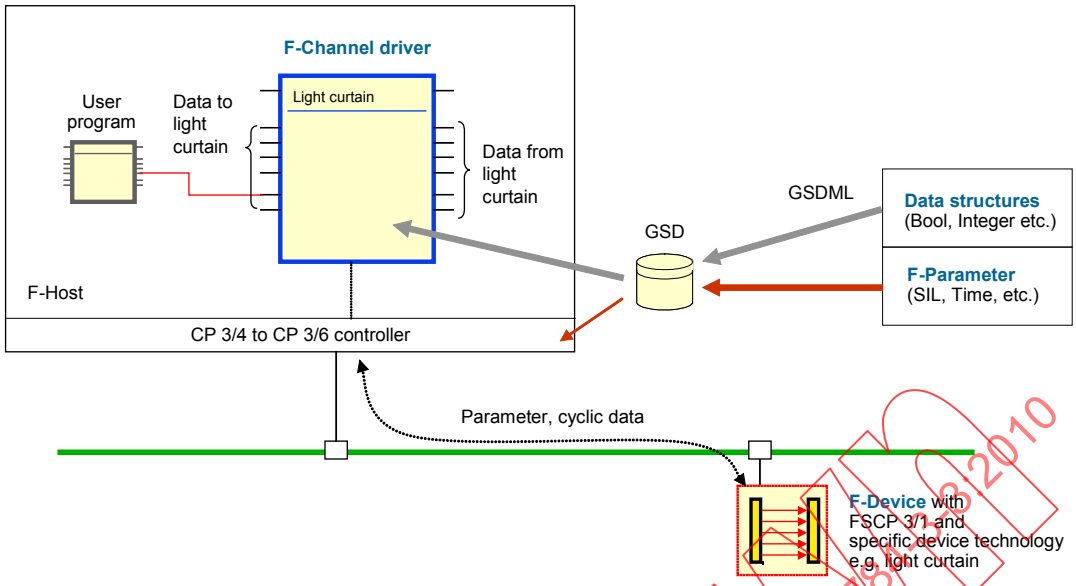


Figure 61 – F-Channel driver as "glue" between F-Device and user program

8.5.2 Rules for standard F-Channel drivers

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

- The data structure shall be described in the IODataSection of the GSD file. See detailed description in 8.3.2.
- A composed data structure shall have the following order: First all mixed types of Float32 + Unsigned8 if available. Then all Unsigned8, Unsigned16, Unsigned32 variables if available. Then all Integer16 variables if available. Then all floating-point variables if available.

Table 11 contains a list of sample F-Channel drivers. The drivers are representing different F-Input and F-Output data structures according to the associated safety PDUs. The permitted data types for FSCP 3/1 are listed in 5.5.4. Thus, 32 Boolean values shall be mapped into data type Unsigned32 and 8 bit into the data type Unsigned8. See 8.4.2 for details.

Table 11 – Sample F-Channel drivers

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

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

Constraints:

- unused bits shall be set to "0";
- status and fault indications of an F-Device shall be defined within the input data structure if necessary (for example qualifier).

8.5.3 Recommendations for F-Channel drivers

Figure 62 shows a layout example of an F channel host driver for a complex F-Device.

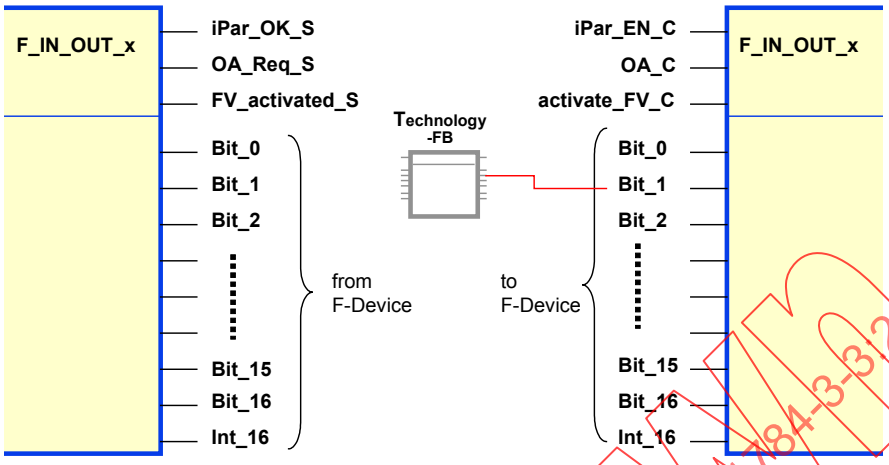


Figure 62 – Layout example of an F-Channel driver

The terms used in Figure 62 and the driver behaviors are specified below:

iPar_EN_C	iParametrization enabled
iPar_OK_S	iParametrization completed
OA_C	Operator Acknowledgement (for resumption after fault)
OA_Req_S	When fault (Watchdog, CRC, Cons. Nr.) detected and removed
FV_activated_S	Fail-safe values activated by F-Device
activate_FV_C	Fail-safe values to be activated within F-Device
Fixed behavior of F channel driver	Fail-safe values set to "0"

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

For performance reasons the F-Channel driver may be split into two function blocks, one for inputs and one for outputs (Figure 62). There is a fixed behavior of the F channel drivers in respect to fail-safe values: whether the data structure consists of bit (Unsigned8), Integer16, Float32 or Float32 + Unsigned8, every value is set to "0". If actuators cannot agree to FV = "0", other values may be implemented either hard-coded or via iParameters. User programs may activate these device specific fail-safe values via bit 4 within the Control Byte (see 7.1.3). If sensors cannot agree to FV = "0", additional user program logic may turn them into individual values using the "activate_ FV_C" input of the F-Channel driver.

8.6 Safety parameter assignment mechanisms

8.6.1 F-Parameter assignment

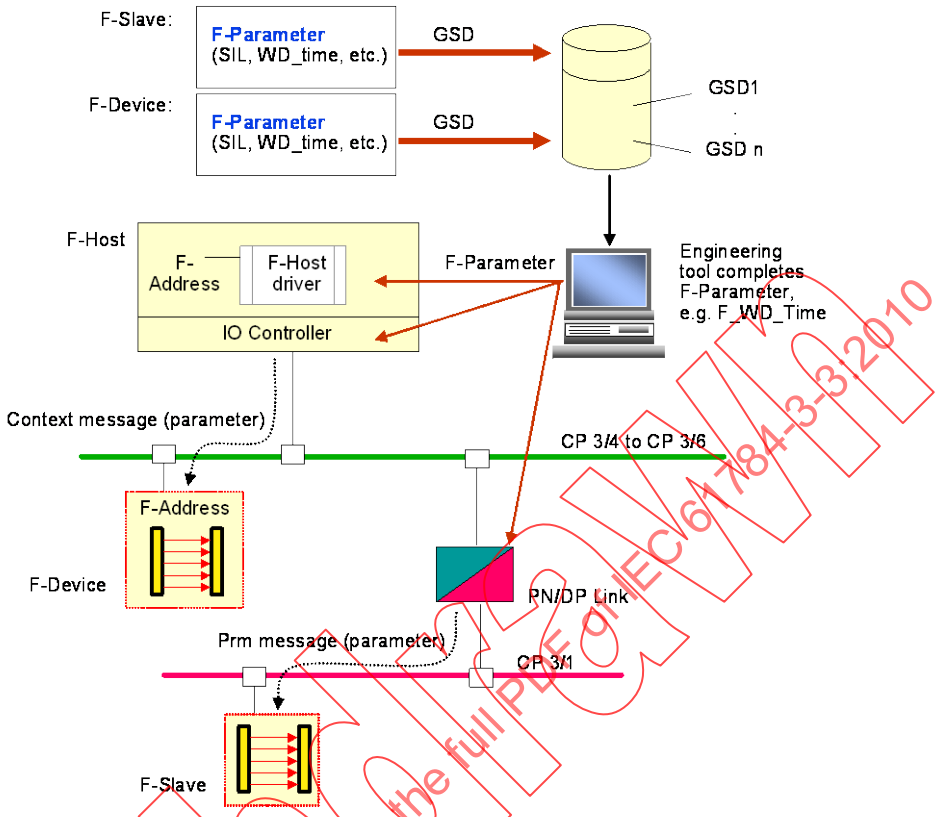


Figure 63 – F-Parameter assignment for simple F-Devices and F-Slaves

Simple F-Devices without iParameters can be supplied via the standard Context Message path. See IEC 61158-5-10, IEC 61158-6-10, and [55]. The total amount of F-Parameters hereby cannot exceed the upper limit of 234 octets (Figure 63).

8.6.2 General iParameter assignment

For complex devices with iParameters a (safety) decision shall be made whether an automatic startup assignment is favored over a separate assignment from a dedicated CPD-Tool for the particular F-Device as requested in IEC 62061. In each case the F-Host shall deblock the assignment only, if there is no hazardous process state (7.4.2). Principally, two ways are possible that can complement each other:

- iParameter value assignment via special proxy function blocks in an F-Host and an appropriate iParameter data set;
- iParameter value assignment through a dedicated CPD-Tool via an IO-Supervisor (Engineering tool/PC).

CPF 3 is offering a standard communication platform for control programs through the *Communication Function Blocks* according IEC 61131-3 and *Proxy Function Blocks* according IEC 61131-3, in particular the ST (Structured Text) programming language, thus supporting the first one. F-Device manufacturers are enabled to provide portable control software for their devices.

Figure 64 represents an example how CPF 3 standards can be used to provide a very comfortable and flexible system support for F-Devices. The dedicated CPD-Tool of the device manufacturer communicates (1) with its F-Device (here: light curtain) either on a direct and separate link (for example USB) or via acyclic services = Read/Write Record Data (see

Figure 15) across the fieldbus concurrently with the cyclic data communication. After parameterization and commissioning, the Proxy Function Block may be activated to upload the iParameters into the controller (2) where they are ready for download in case of device replacement (repair).

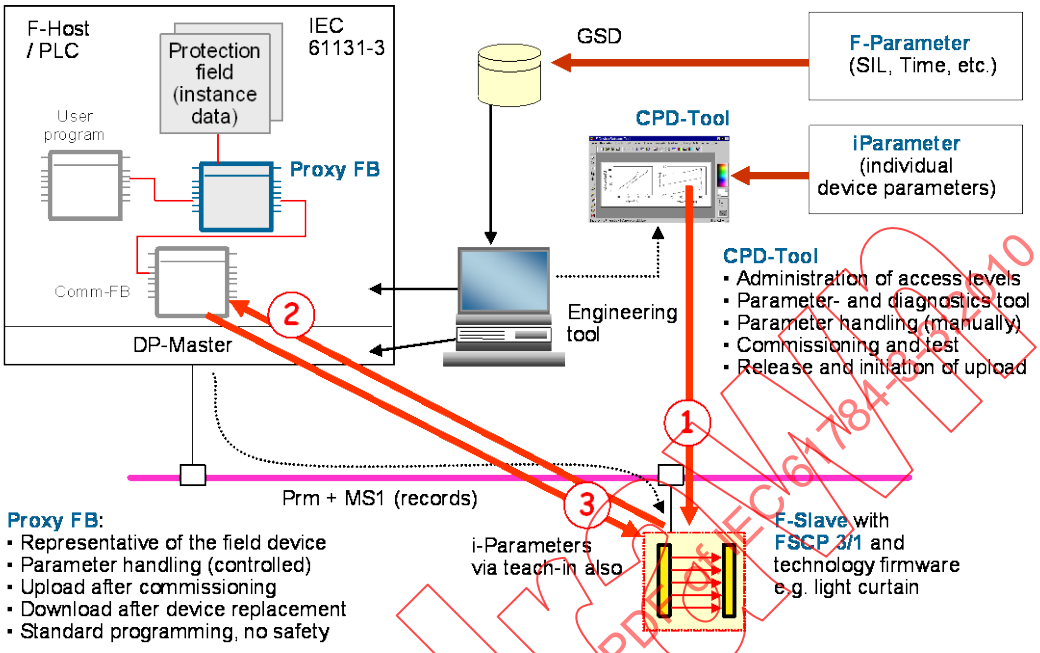


Figure 64 – F and iParameter assignment for complex F-Devices

Recipe programs via program controlled dynamic iParameter assignments can solve the requirements for more flexibility in today's manufacturing areas. Thus several different data sets of for example coordinates for detection zones of light curtains ("blanking") can be assigned one after the other (Figure 64). The identification number of the actual iParameter data set shall be communicated cyclically within the F-I/O data.

8.6.3 System integration requirements for iParameterization tools

Table 12 contains a list of requirements to be fulfilled by iParameterization procedures.

Table 12 – Requirements for iParameterization

No.	System requirement
R1	CPD-Tool to be designed for compatible personal computers or laptops and operating systems WIN2000 or later
R2	Several CPD-Tools or instances of CPD-Tools should be able to run concurrently
R3	CP 3/1: Master class 2 interface boards shall provide a uniform API (application programmer's interface) such that CPD-Tools can be configured to run on different brands
R4	CP 3/RTE: IO-Supervisor interface shall be defined in such a manner that the "acyclic" services of CP 3/RTE can be used for an F-Device directly connected to a CP 3/RTE network
R5	CPF 3: IO-Supervisor interface shall be defined in such a manner that the "acyclic" services of CP 3/RTE can be used for an F-Device directly connected to a CP 3/RTE network or via " Link" to an F-Slave connected to a "subsidiary" CP 3/1-network (initiate, read and write records, etc.)
R6	Connections R4 and R5 should be possible via F-Host programmers port also
R7	"PN/DP-Links" should be available both as stand-alone device or integrated in controller
R8	Fieldbus interface indication: an F-Device shall indicate its type of fieldbus interface. Not needed if a uniform API (see R3) is defined that fits to CPF 3 acyclic communications

No.	System requirement
R9	Path to project database as "Invocation" parameter or usage of an integrated engineering tool interface to store F-Device data within that over-all project database. Automatic versioning of iParameter data sets should be possible
R10	Name of Station/address should be defined as "Invocation" parameter
R11	Path to the GSD file should be defined as "Invocation" parameter
R12	Multiple language support should be defined as "Invocation" parameter. Host-Engineering-Tool to define default language upon invocation
R13	Authorization (roles and access rights) should be inherited from the Host-Engineering-Tool to the CPD-Tool upon invocation
R14	Download of iParameters to the F-Device: octet stream of iParameters should be defined such that it can be stored within the IO controller and transferred to the F-Device upon general parameterization. PROXY-FB still is the favourite solution for FSCP 3/1
R15	Version: APIs (see R3 and R4) shall provide a version number such that CPD-Tools can automatically adjust themselves
R16	Printout: It should be possible to "remote control" the individual CPD-Tools from the Host-Engineering-Tool for batch printing or to deliver the printout in a standardized format (for example HTML) to the Host-Engineering-Tool
R17	Up- and Download of iParameters: It should be possible to "remote control" the dedicated CPD-Tools from the Host-Engineering-Tool for batch "iParameterization" or deliver the iParameters in a standardized format to the Host-Engineering-Tool (see R14)
R18	The CPD-Tool should be enabled to submit default symbol names (for example "OSSD1") to the Host Engineering Tool and get in return the assigned final symbol names of the project in case of diagnosis. The submission of default symbol names is possible with the GSD file of CP 3/RTE
R19	In order to achieve independence from the underlying black channel, the same securing principle for the transmission of iParameter data shall be used as with the cyclic data exchange described in Figure 26 and the associated clause, i.e. calculation of the iPar CRC32 shall be in reverse byte order (the initial value shall not be zero). A manufacturer can use his own method to secure the iParameters as long as the criteria are fulfilled (iPar-Server, CPD-Tool)

Figure 65 is illustrating the system aspects of the CPD-Tool-Integration. The CPD-Tool may be either connected to:

- the F-Device directly (for example USB, RS232);
- the F-Host via a programmer port;
- the CP 3/RTE and the CP 3/1 through a Link;
- the CP 3/1 or CP 3/2.

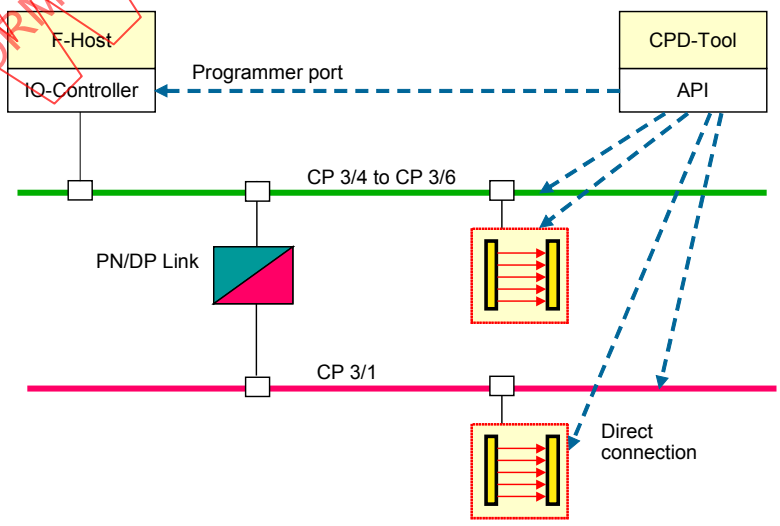


Figure 65 – System integration of CPD-Tools

8.6.4 iPar-Server

8.6.4.1 General description and constraints

The iPar-Server concept is a specialised form of the more general Proxy-FB concept as pointed out in 8.3.1. It is the responsibility of F-Host manufacturers to provide this feature as stated in Table 23 be it realised within the non-safety part of an F-Host as the parameterization master or within a controlled subsystem such as a non-safety PLC or an industrial computer on the same network.

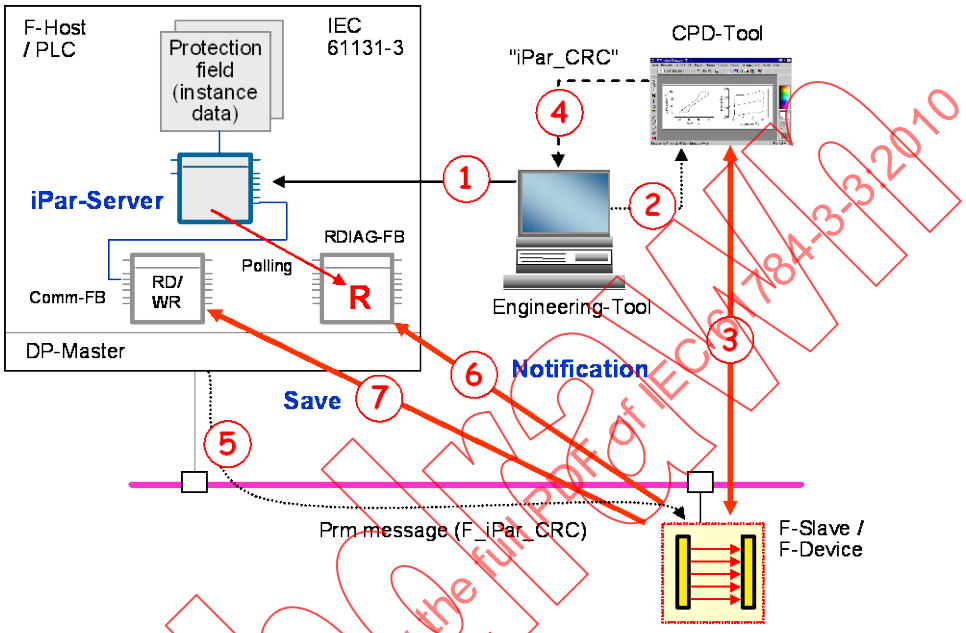


Figure 66 – iPar-Server mechanism (commissioning)

Figure 66 demonstrates the principle steps of the iPar-Server mechanism via an example. Together with the network configuration and F-Parameterisation of an F-Slave/F-Device an associated iPar-Server function is instantiated (step 1). The F-Slave/F-Device is able to go in the data exchange mode using a safe state (FV). An associated CPD tool can be launched via an appropriate interface (step 2) from the engineering tool propagating at least the node address of the configured device. Parameterization, commissioning, test, etc. can be executed with the help of the CPD tool (step 3). After finalization, the iPar_CRC signature is being calculated and displayed in hexadecimal form for at least copying and pasting of this value into the "F_iPar_CRC" entry field of the configuration part of the engineering tool (step 4). A restart of the F-Slave/F-Device is necessary to transfer the "F_iPar_CRC" parameter into the F-Slave/F-Device (step 5). After final verification and release the F-Slave/F-Device is enabled to initiate an upload notification (step 6) to its iPar-Server instance. It thereby is using the diagnosis means of CPF 3 (8.6.4.2 and [49]). The iPar-Server is polling the diagnosis information (for example RDIAG FB) to interpret the request (R) and to establish the upload process (step 7) which stores the iParameters as instance data within the iPar-Server host.

Figure 67 is showing the second part of the iPar-Server mechanism. In case of the replacement of a defect F-Slave/F-Device (step 1) the F-Slave/F-Device receives its F-Parameters including the "F_iPar_CRC" (step 2) at start-up. As iParameters normally are missing in a replacement or non-remanent F-Slave/F-Device it initiates a download notification (step 3) to its iPar-Server instance. It thereby is using the diagnosis means of CPF 3 (8.6.4.2 and [49]). The iPar-Server is polling the diagnosis information (for example RDIAG FB) to interpret the request (R) and to establish the download process (step 4). Through this transfer the F-Slave/F-Device is enabled to provide the original functionality without further engineering or CPD tools.

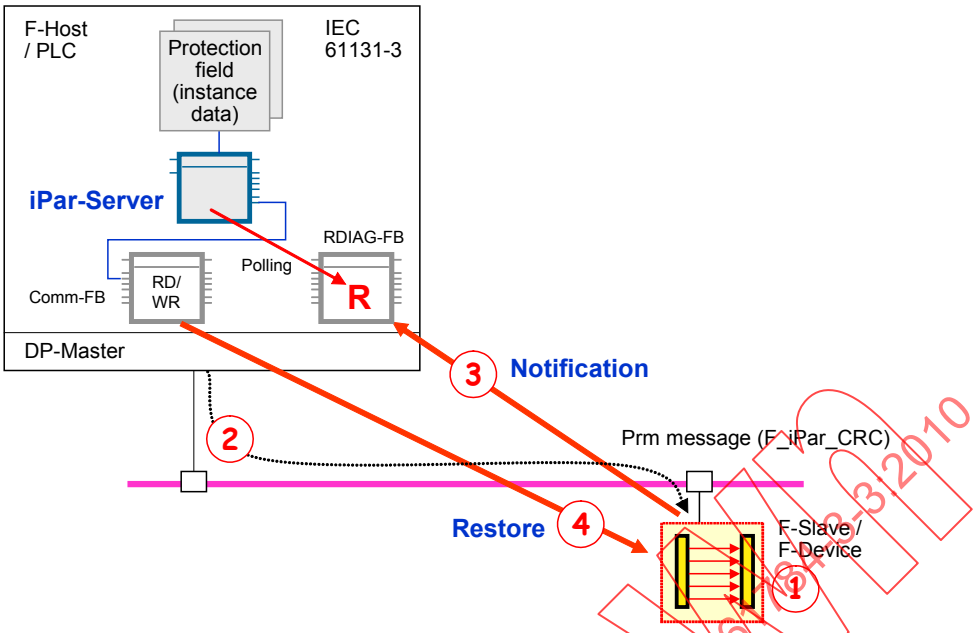


Figure 67 – iPar-Server mechanism (for example F-Device replacement)

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

- Each iPar-Server instance shall support a minimum of 2^{15}-1 octets of iParameters per F_Source/Destination_Address (device/submodule/module).
- The iParameters are stored as one fixed block of data as shown in Figure 52.
- The iPar-Server is not safety-related. It can be implemented or launched within a standard host or within the standard part of an F-Host (Figure 67).
- The iPar-Server only shall be available in conjunction with the V2-mode of the FSCP 3/1.
- It is the responsibility of the F-Slave/F-Device manufacturer that the downloaded iParameter set matches for example the correct type and version of the replacement device.
- An F-Module/F-Slave/F-Device only shall initiate an iPar-Server-Request when the black channel guarantees delivery of the notification.
- One repetition is permitted whenever a "Restore" attempt failed. The associated safety function remains in safe state (FV).
- "Restore" only shall be executed upon start-up of the system/F-Device.

8.6.4.2 Notification

The only standard mechanism for an F-Slave/F-Module to notify the iPar-Server on CPF 3 type networks is via a diagnosis message. However, in contrast to the standard diagnosis context the iPar-Server notification does not need information propagation to any visualisation tool for maintenance interaction. Out of several different types on CP 3/1 and CP 3/2, specified in IEC 61158-5-3, the preferred diagnosis information coding relates to the "Status Model" [50]. In order to avoid conflicts with already existing types a new status type "iPar-Server Request" (type = 7) has been defined within a previously reserved range.

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

Figure 68 is showing the iPar-Server request coding for CP 3/1 and CP 3/2.

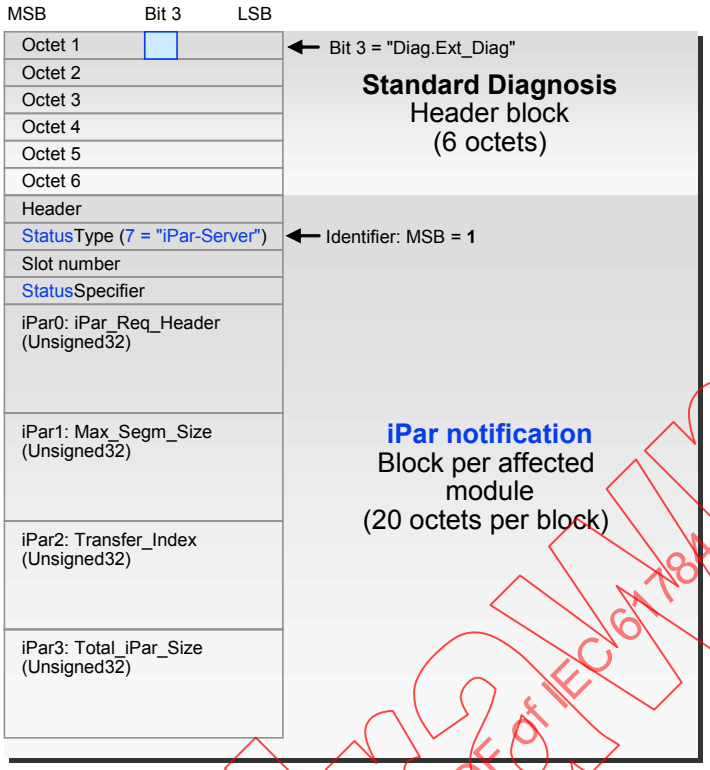


Figure 68 – iPar-Server request coding ("status model")

Each coding of the "iPar-Server Request" starts with the six mandatory octets of the standard diagnosis block. The "Diag.ext.diag" flag (bit 3 of the first octet) shall not be impacted as no LED indicator shall be light up if no defect is to be reported. The next four octets are following the standard coding as described in IEC 61158-5-3 and in Figure 68. Status type is the new "iPar-Server Request" (7). The Status specifier shall be set "0". The body of the "iPar-Server Request" contains the specifiers as defined in Table 13.

An F-Module within a remote I/O always uses the coding of Figure 68 or an appropriate subset, whenever it can be deployed in a CP 3/1 or CP 3/RTE remote I/O device. A remote I/O shall only cast one notification at a time and thus save or restore iParameters F-Module by F-Module. Design hints for cases of diagnosis congestion (e.g. "Diag.Ext_Diag_Overflow") can be found in [50].

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

It is the task of the headstation of a remote I/O device to transform the iPar-Server request coding into the appropriate format of the actual communication profile (Figure 68 or Figure 70).

Table 13 – Specifier for the iPar-Server Request

iPar specifier	Name	Octet 3	Octet 2	Octet 1	Octet 0	Definition
iPar0	iPar_Req_Header	SR_Version	Reserved	N_Count	SR_Type	Type of iPar-Server request (Unsigned32)
iPar1	Max_Segm_Size	0x00h	0x00h	0x00h	0…234	Maximum permitted net size of a segment in octets (Unsigned32)
iPar2	Transfer_Index	0x00h	0x00h	0x00h	0…254 (255)	Index for the read/write record transfer (Unsigned32)

iPar specifier	Name	Octet 3	Octet 2	Octet 1	Octet 0	Definition
iPar3	Total_iPar_Size					Total length of iParameter octets (Unsigned32)

NOTE 1 Reserved: See 7.1.3, hints.

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

NOTE 3 A "Transfer_Index" of 255 may conflict with other services such as a CALL of I&M functions.

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

NOTE 5 A replacement device may not know the correct size of iParameter of its predecessor. In this case the notification for Restore may contain "Total_iPar_Size = 0", which means the iPar-Server will download the complete iParameter data set.

NOTE 6 N_Count is a sequence counter for notifications (for CP 3/1 and CP 3/2 only), counting from 1 to 15 and over again.

The parameter "SR_Version" shall be set to 0x01h. The parameter "N_Count" shall start with "1" and be incremented with each notification (only in case of CP 3/1 and CP 3/2) until the value 15 and continued with "1" all over again. The parameter "SR_Type" shall be coded as shown in Figure 69.

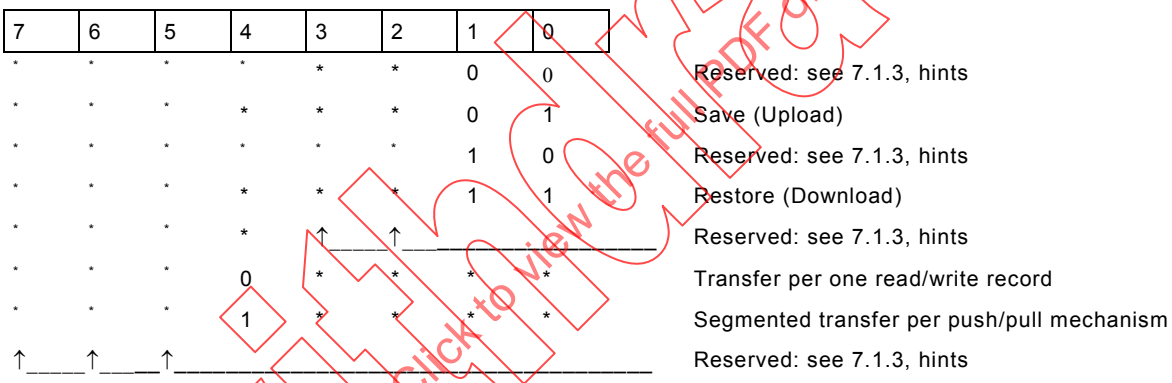


Figure 69 – Coding of SR_Type

A possible realization of the counterpart within for example the non-safety part of an F-Host is specified in [49] and called RDIAG communication function block.

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

The preferred diagnosis information coding on CP 3/RTE for the iPar-Server relates to the "Alarm Model" and on the standard "Upload&Retrieval" alarm defined in IEC 61158-5-10 and IEC 61158-6-10. Figure 70 is showing the iPar-Server request coding for CP 3/RTE (IEC 61784-2).

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

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

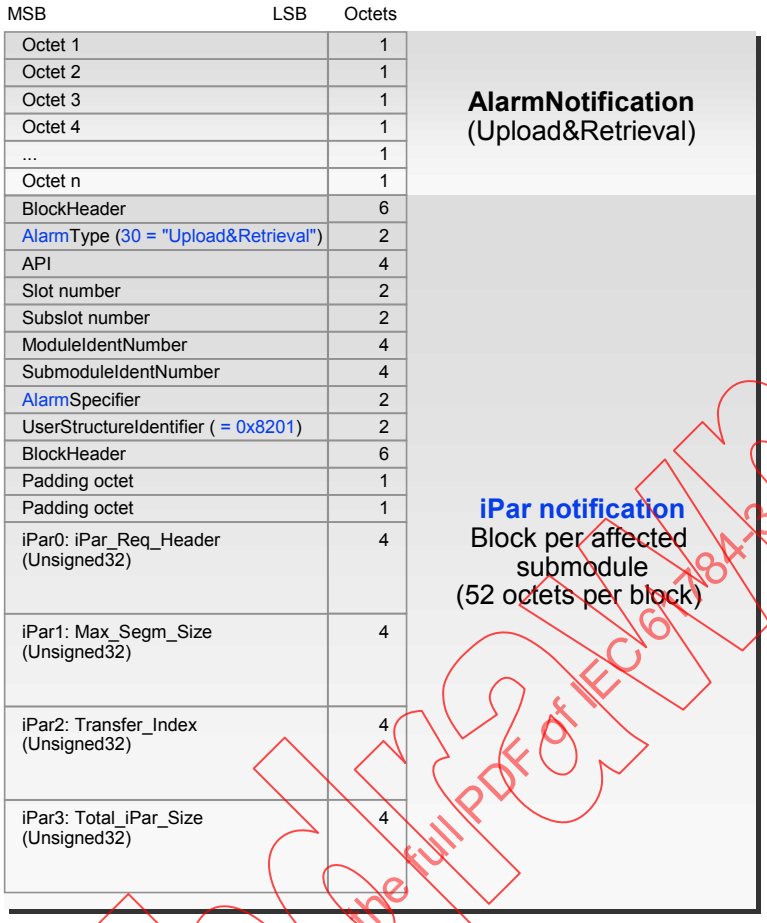


Figure 70 – iPar-Server request coding ("alarm model")

8.6.4.3 Services

The iPar-Server is a small program that is invoked at each main cycle for example within the non-safety-related part of an F-Host. It polls the diagnosis information of the particular F-Slaves/ F-Modules, looking for any of the two kinds of requests "Save" and "Restore". In order to execute these requests it uses the standard "read record" and "write record" acyclic services as defined in IEC 61158-5-3. For small amounts of iParameters an ordinary unsegmented version per single "read record" and "write record" is sufficient (Table 14 and Table 15). A possible realization of these two functions based on IEC 61131-3 programming languages is specified in [49] and called RDREC and WRREC communication function blocks. It is highly recommended for F-Host systems to provide these function blocks within the library for its non-safety related part.

Table 14 – Structure of the Read_RES_PDU ("read record")

Structure of the Read_RES_PDU	Size	Coding	Notes	
Function_Num	1 octet	0x5E	Indicates "read", fix	Header
Slot_Number	1 octet	0 … 255	Location of module	
Index	1 octet	0 … 254	"Transfer_Index"	
Length of net data	1 octet	0 … 240	Length of iPar segment	
iParameter (segment)	n octets	-	n = 240 maximum per record	Data
NOTE Corresponding structures for CP 3/RTE can be found in [49].				

Table 15 – Structure of the Write_REQ_PDU ("write record")

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

For amounts of iParameters exceeding the record or buffer limit of a particular F-Slave/ F-Module an extended version of the "read record" and "write record" acyclic services can be used, specified in IEC 61158-5-3 as the so-called "Pull" and "Push" services (Table 16 and Table 17).

Table 16 – Structure of the Pull_RES_PDU ("Pull")

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

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

Table 17 – Structure of the Push_REQ_PDU ("Push")

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

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

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

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

An F-Module within a remote I/O always uses an appropriate coding, whenever it can be deployed in a CP 3/1 or CP 3/RTE remote I/O device. It is the task of the headstation of a remote I/O device to transform the iParameter transfer coding into the appropriate format of the actual communication profile and back.

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

8.6.4.4 Protocol

Figure 71 is showing the iPar-Server state diagram and Table 18 describes the iPar-Server states, transitions, and internal items. See 7.2.2 on general information about UML2 notation.

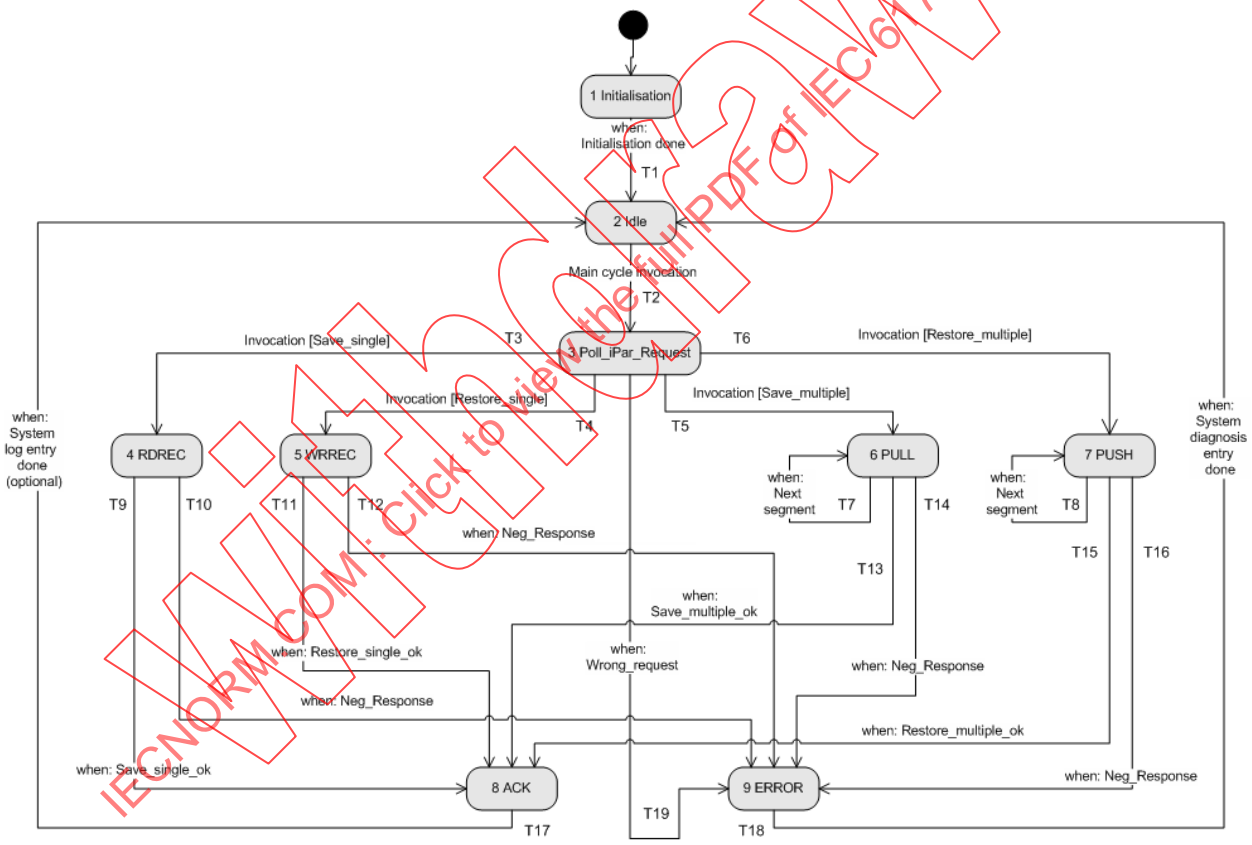


Figure 71 – iPar-Server state diagram

The terms used in Figure 71 are specified below:

Save_single	iPar-Server request to save (upload) an iParameter block per one single record (RDREC)
Restore_single	iPar-Server request to restore (download) an iParameter block per one single record (WRREC)
Save_multiple	iPar-Server request to save (upload) a larger iParameter block per multiple records (PULL)

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

Table 18 – iPar-Server states and transitions

STATE NAME	STATE DESCRIPTION
1 Initialisation	Cold start state; initialise outputs if defined
2 Idle	Idle state, no actions
3 Poll_iPar_Request	Upon main cycle invocation or similar activity in a controlled subsystem, the iPar-Server request within the body of the diagnosis information is interpreted and the corresponding system service shall be launched. In case of errors the ERROR state shall be entered
4 RDREC	Within this state the system function RDREC according [49] or a similar function shall be invoked that executes a read function according to the CP 3/1 or CP 3/2 in IEC 61158-5-3
5 WRREC	Within this state the system function WRREC according [49] or a similar function shall be invoked that executes a write function according to the CP 3/1 or CP 3/2 in IEC 61158-5-3
6 PULL	Within this state the system function PULL shall be invoked that executes a multiple read function via the "Extended_Function_Num" = 0x02 according to the CP 3/1 or CP 3/2 in IEC 61158-5-3
7 PUSH	Within this state the system function PUSH shall be invoked that executes a multiple write function via the "Extended_Function_Num" = 0x01 according to the CP 3/1 or CP 3/2 in IEC 61158-5-3
8 ACK	Within this state any successful save and restore action can be recorded in a "system iPar-Server log file" (optional)
9 ERROR	Whenever a system function such as RDREC, WRREC, PULL, or PUSH aborts with an error, or in case of an erroneous request, the iPar-Server shall create within this state a system diagnosis entry

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

TRAN-SITION	SOURCE STATE	TARGET STATE	ACTION
T13	6	8	Start entry of a successful POLL execution in the system log file (optional)
T14	6	9	Start system diagnosis entry
T15	7	8	Start entry of a successful PUSH execution in the system log file (optional)
T16	7	9	Start system diagnosis entry
T17	8	2	Go to sleep (idle)
T18	9	2	Go to sleep (idle)
T19	3	9	Start system diagnosis entry

8.6.4.5 iPar-Server management

The iPar-Server management measures to ensure authenticity, validity and data integrity of the iParameters are listed in Table 19. It is the responsibility of the F-Module, F-Slave, or F-Device to provide the safety measures for the save and restore mechanisms. The iPar-Server is just storing the iParameters as a stream of octets and can be a standard parameter server for non-safety-related devices also.

Table 19 – iPar-Server management measures

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

Item / phase	Clauses	Description
iPar-Server	-	An F-Module, F-Slave, or F-Device only shall launch an iPar-Server request after successful start-up parameterization (F-Parameters)
LED indication	9.1	As long as the F-Module, F-Slave, or F-Device did not accomplish to save its iParameters or while in FSCP test mode it shall indicate this state via the LED indicators described in 9.1. The blinking frequency in this case shall be 2 Hz

8.6.4.6 iParameter size in GSD

An F-Module, F-Slave, or F-Device can indicate the maximum size of its iParameters via the keyword entry "Max_iParameter_Size" in its GSD file ("Max_iParameterSize" in GSDML). See [43] and [47] for details.

9 System requirements

9.1 Indicators and switches

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

— checking of the equipment and if necessary its reparation or replacement;

— verification of the safety function;

— Operator Acknowledgement (OA_C).

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

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

Subclauses 7.3.7 and 8.1.2 are providing information on how to enter the F_S/D_Address of F-Devices via switches.

9.2 Installation guidelines

The installation guidelines of IEC 61918 and the CPF 3 specific amendments in IEC 61784-5-3 shall apply. Additional information can be retrieved from [44].

9.3 Safety function response time

9.3.1 Model

A safety function may consist of several sensors such as light curtains and E-Stop buttons, a safety logic program within an F-Host, and an actuator such as a motor (Figure 72). Each sensor has its own signal path and thus a particular typical response time.

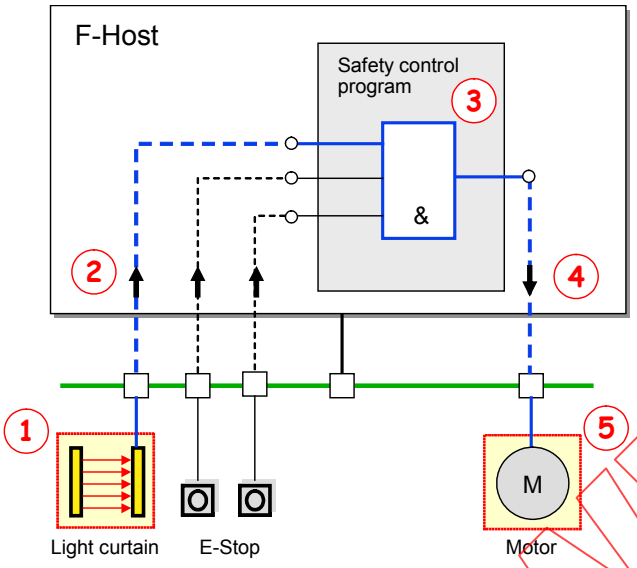
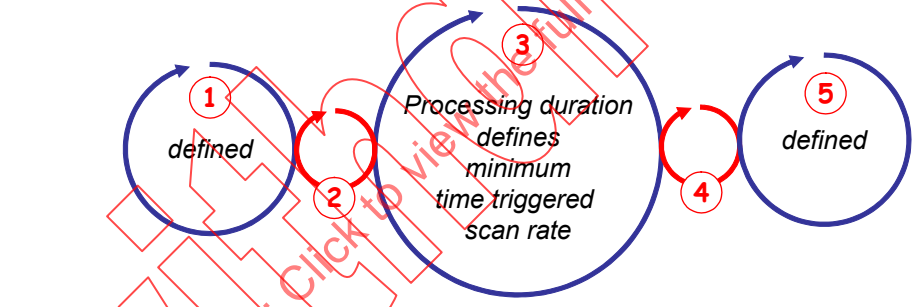


Figure 72 – Example safety function with a critical response time path

This typical response time consists of several individual time values including the bus transfer times as shown in the simplified typical response time model of Figure 73. An example is used to show the principle, which can be adopted for the internal response time model of a complex device.



	Input delay	Transmission delay	Processing delay *)	Transmission delay	Output delay
Example:	3, 4, 5, 6 ms	1, 2 ms	5, 6, 7, ... 15 ms	1, 2 ms	3, 4, 5, 6 ms

*) min. processing time: 5ms; time triggered scan rate for this example = 10ms

Figure 73 – Simplified typical response time model

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

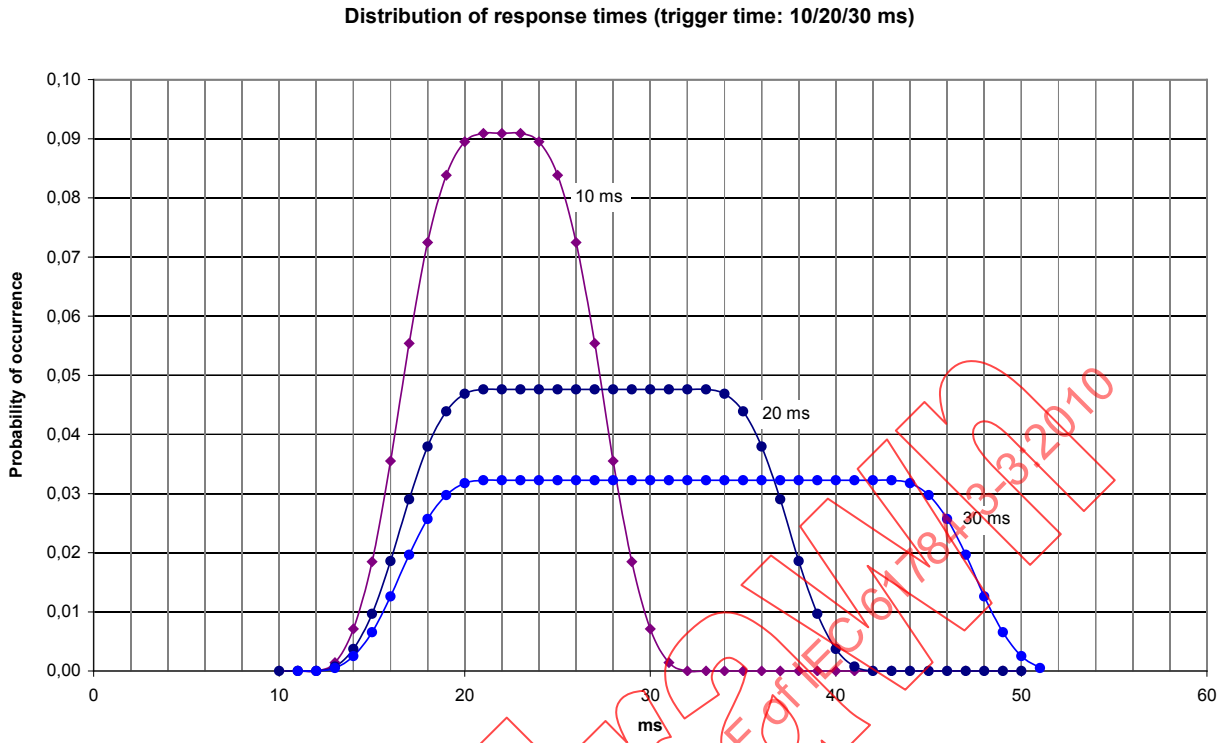


Figure 74 – Frequency distributions of typical response times of the model

Any of these elements are having minimum (= processing) and maximum delay times (= processing + waiting). The actual delay may be any time (or time interval) in between these values. In this model the F-Host is supposed to be a combined controller for standard and safety programs. The safety program is executed within a separate time triggered program level and may need a processing time of 5 ms. Trigger time in this case is each other 10 ms. This results in a processing delay of minimal 5 ms and a maximum of 15 ms. In total, the minimum delay for this safety function is 13 ms and the maximum delay is 31 ms. Figure 74 shows the frequency distributions of typical response times of the model for a time trigger of 10 ms, 20 ms and 30 ms.

9.3.2 Calculation and optimization

The model for typical response times in 9.3.1 is used to define the safety function response time. Each of the cycles in the model can vary between a best case and a worst case delay time ($WCDT_i$). Every cycle has for safety reasons its superposed watchdog timer ($WDTime_i$), which takes the necessary actions to activate the safe state whenever a failure or error occurs within that particular entity. Figure 75 illustrates the context of the worst case delay times and the watchdog times.

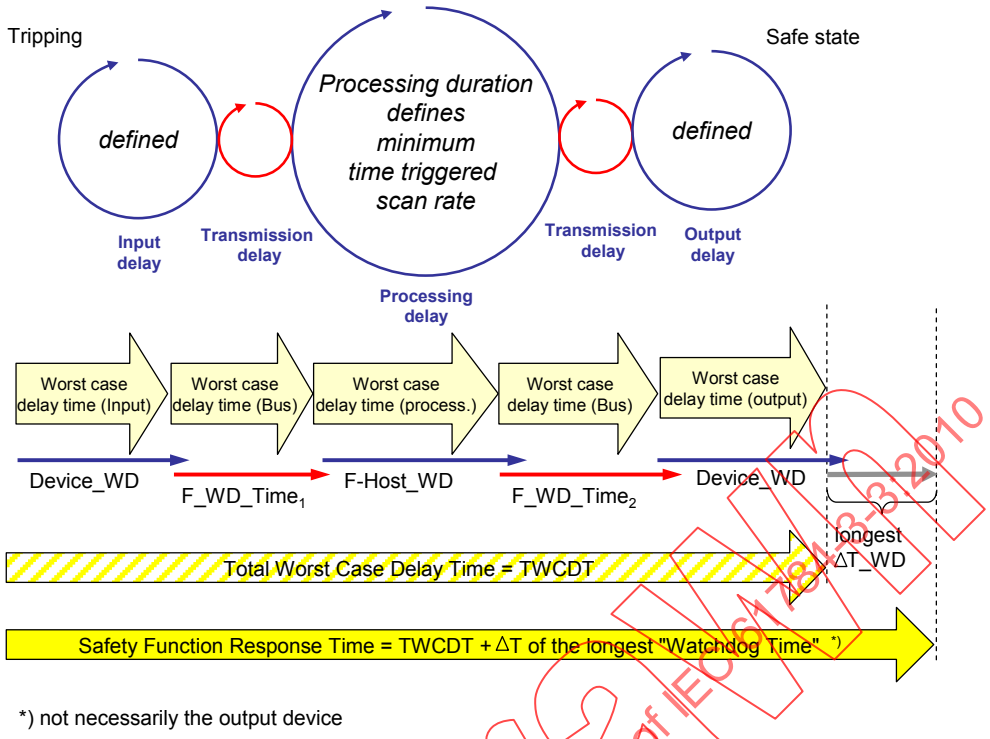


Figure 75 – Context of delay times and watchdog times

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

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

Where

SFRT Safety function response time

TD Transmission delay

$WCDT_i$ Worst case delay time of entity i

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

– Input: $OFDT_{Input}$

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

– F-Host: $OFDT_{F\text{-}Host}$

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

– Output: $OFDT_{Output}$

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

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

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

9.3.3 Adjustment of watchdog times for FSCP 3/1

The F-Parameter F_WD_Time determines the watchdog time for a FSCP 3/1 1:1 communication relationship (8.1.3). Figure 76 is illustrating that the minimum watchdog time is composed of four timing sections (DAT – Bus – HAT - Bus). Whenever the F driver (6.2) in a compact F-Device or in an F-Module of a modular device recognizes a safety PDU (FSCP 3/1 frame) with a new consecutive number (m) it restarts the watchdog timer. It then processes the FSCP 3/1 protocol while taking the *currently available process values* and prepares a new safety PDU. The elapsed time for this operation is called "DAT = Device Acknowledgement Time".

NOTE In case of a modular F-Device the DAT includes internal transfer times across the backplane bus.

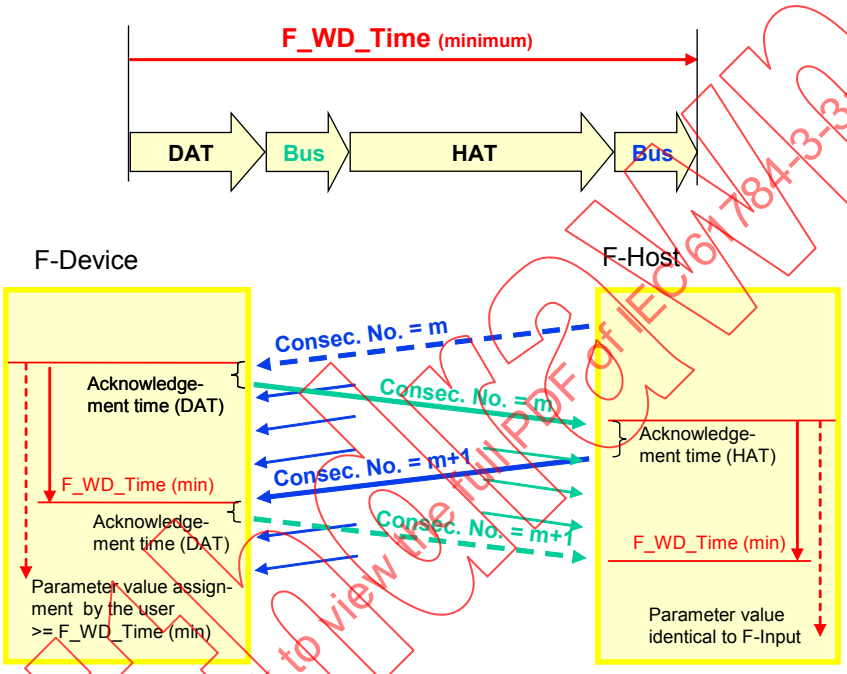


Figure 76 – Timing sections forming the FSCP 3/1 F_WD_Time

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

The watchdog time that shall be assigned to the F-Parameter is longer than *the minimum watchdog time* to ensure that an emergency event has been caught.

According to 8.1.3 the value to be assigned to F_WD_Time in the example of Figure 73 (Time trigger = 10 ms) would be 2 x bus transmission (2 × 2 ms) plus DAT of the device (6 ms) and the F-Host (15 ms): F_WD_Time = 4 ms + 6 ms + 15 ms = 25 ms. An adjustment of a shorter watchdog time will not affect the safety of a system. It may cause nuisance trips and thus affect its availability.

The fact that a device can extend the bus transfer times in the event of a diagnosis message shall also be taken into account in reserving the necessary time allowance within the watchdog timer adjustments. Additional supervisor devices (or master class 2 within CP 3/1) have minor influence on the response times as shown in Figure A.3. Other influences are described in 9.3.5.

The equation (1) in 9.3.2 is valid in case the timings for DAT, HAT, and bus transmissions can be guaranteed. The primary F-Parameter F_WD_Time shall be assigned a value that is slightly greater than the sum of DAT, HAT, and two times the bus transmission time. It is highly recommended for the difference between the assigned parameter value and the sum to not exceed 30 %. System manufacturers can adjust this rule to their individual needs.

9.3.4 Engineering tool support

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

9.3.5 Retries (repetition of messages)

In case of extreme electromagnetic interference or devices that are not conform to the fieldbus standards in stressing the data communication lines with unacceptable electrical noise, fieldbus systems tend to use retry mechanisms to increase the availability. It is good engineering practice during the commissioning phase to check each connection to all of the devices -standard or safety - for its number of retries and if necessary to take appropriate measures such as correct application of the installation guidelines or usage of conformance tested devices (Clause 10). This will not only help to increase the availability but also provide short reaction times without nuisance trips (Figure 77).

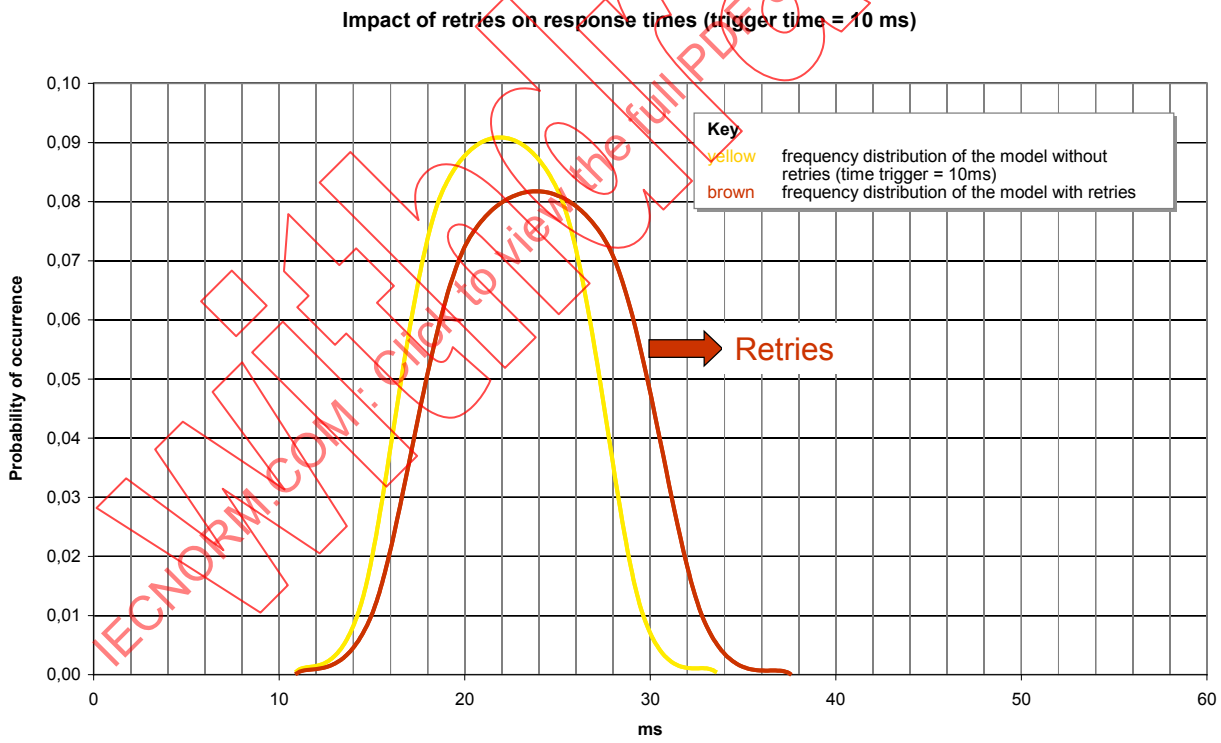


Figure 77 – Frequency distribution of response times with message retries

Figure 78 is illustrating the retry mechanisms with CP 3/1, whereas Figure 79 is illustrating the retry mechanisms for CP 3/RTE. It may also be necessary for safety assessments to know about the retry behavior of the black channels.

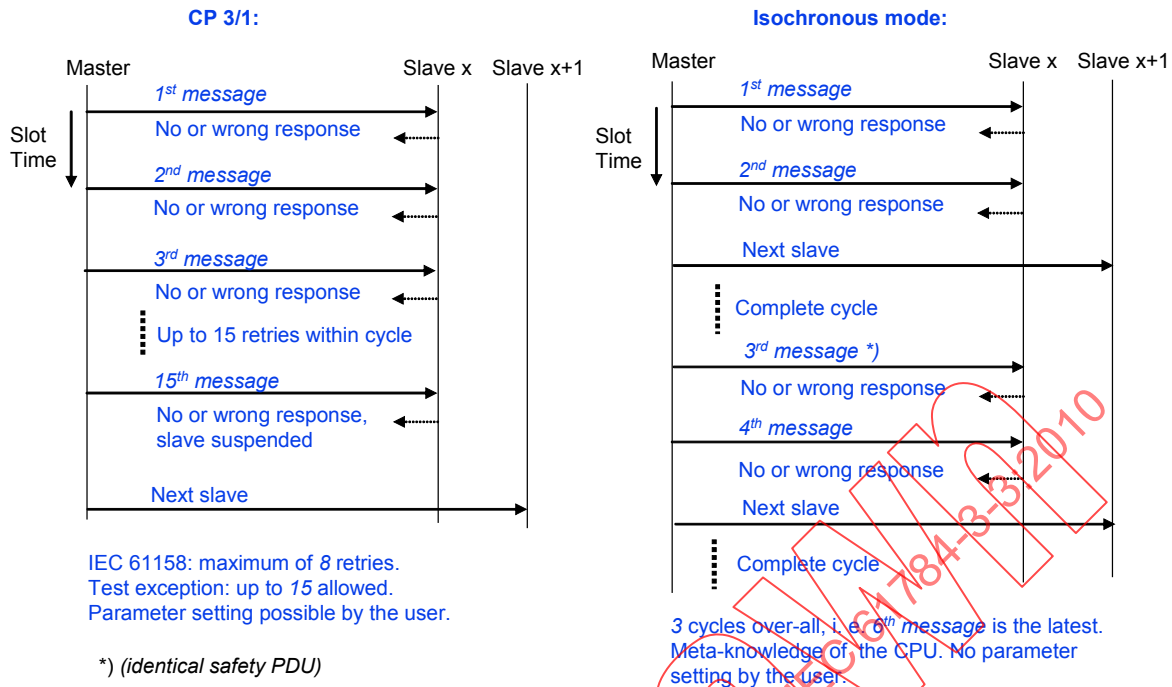


Figure 78 – Retries with CP 3/1

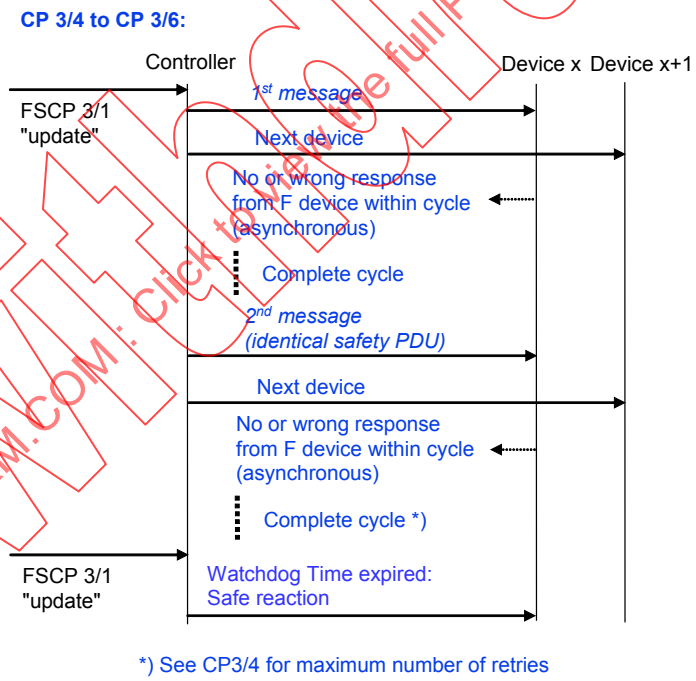


Figure 79 – Retries with CP 3/RTE

9.4 Duration of demands

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

— shall be present as long as or longer than the Process Safety Time or the FSCP 3/1 timeout (F_WD_Time) respectively;

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

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

9.5 Constraints for the calculation of system characteristics

9.5.1 Probabilistic considerations

The data integrity checking mechanism of the FSCP 3/1 V2-mode is totally independent from the mechanisms of the underlying communication system, which then is called a "black channel". Thus it can be used for backplane communication channels also.

According to IEC 62280-1 and IEC 62280-2, the "properness" of the used CRC polynomials has to be proven. This requires calculation of the residual error probability as a function of the bit error probability for a given polynomial, here for the 24-bit version (15*D6DCB*h), as well as for the 32-bit version (1*F4ACFB13*h).

Figure 80 is showing the diagrams of residual error probabilities for the 24-bit polynomial. The calculated diagrams are for data lengths including the CRC signature.

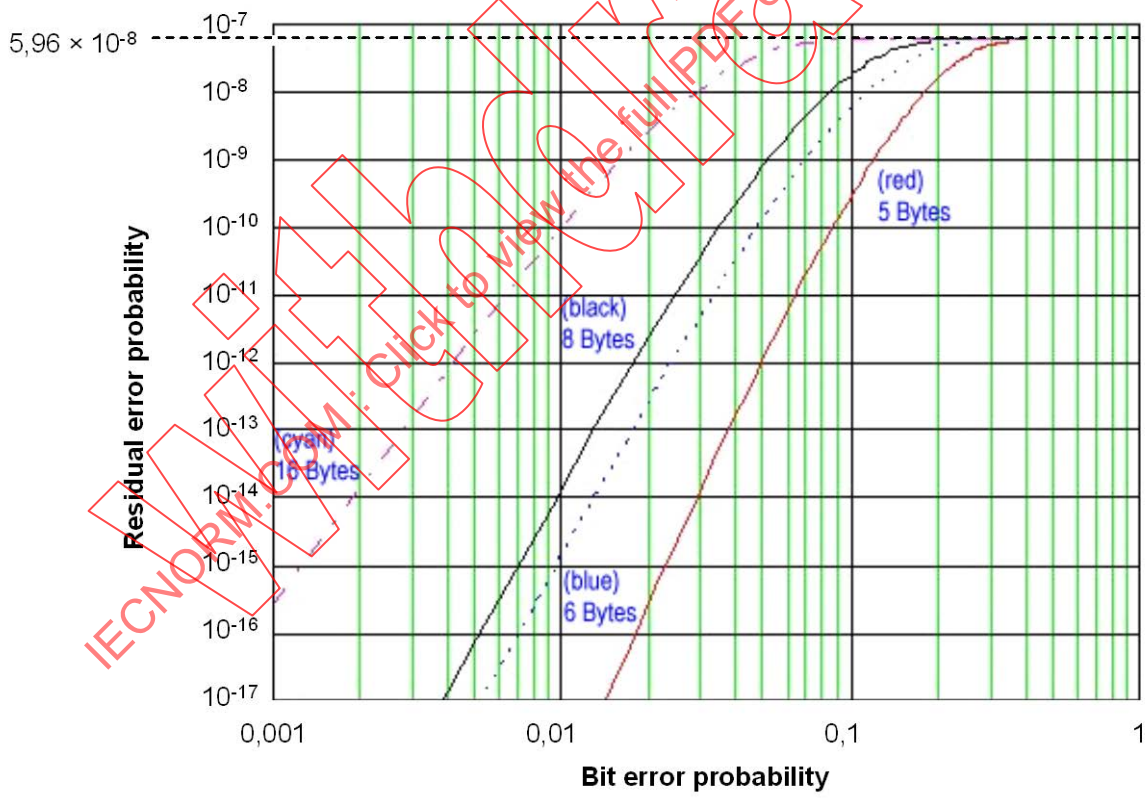


Figure 80 – Residual error probabilities for the 24-bit polynomial

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

Figure 81 and Figure 82 are showing the diagrams for the 32-bit polynomial.

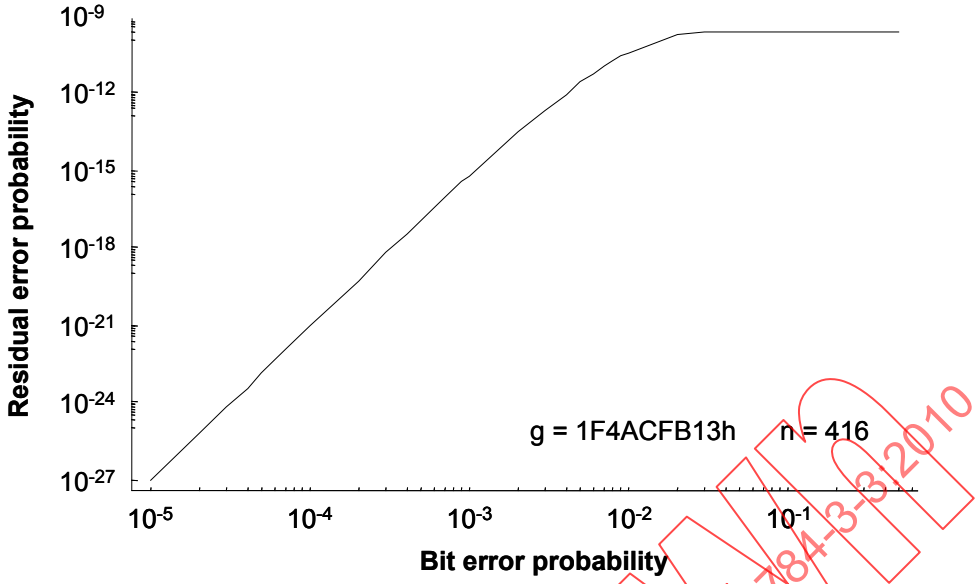


Figure 81 – Properness of the 32-bit polynomial for 52 octets

The terms used in Figure 81 and Figure 82 are specified below:

g = generator polynomial 1*F4ACFB13*h

n = bit length of data including CRC signature

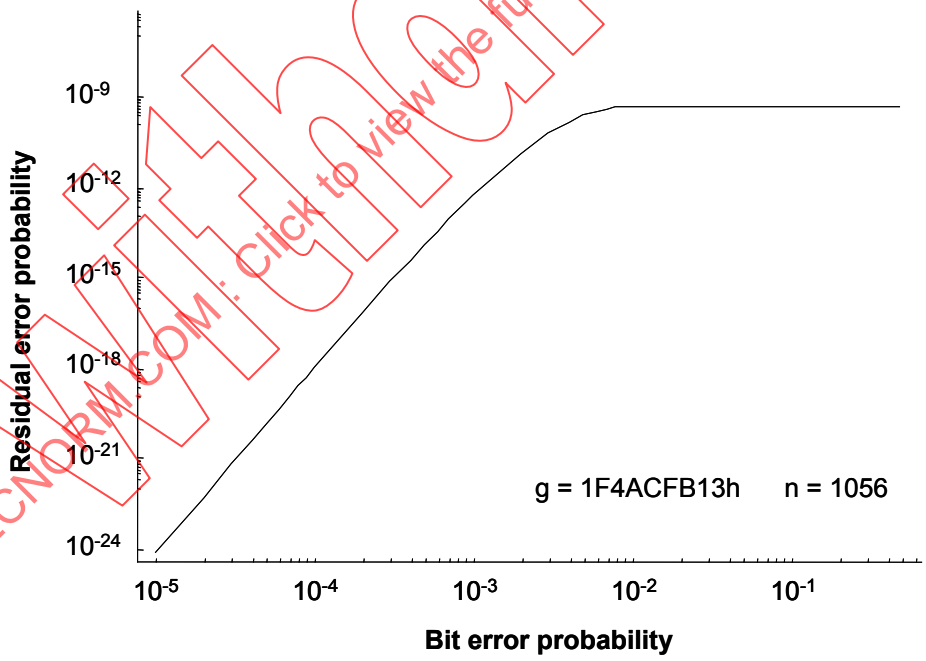


Figure 82 – Properness of the 32-bit polynomial for 132 octets

Summarizing reflections about any perturbing influences lead directly to Figure 83. The combination of the bus failure causes provides a (fictive) frequency of corrupted messages on the transmission system. The standard error detecting mechanisms of CP 3/RTE (1st Filter) are recognizing every fault up to a certain level, thus only special bit patterns are reaching the safety layer mechanism. For the number of undetected corrupted messages the worst-case value of 2^{-n} shall not be taken (n = 24 or 32), since the overall frequency of corrupted safety PDUs on the bus is continuously monitored.

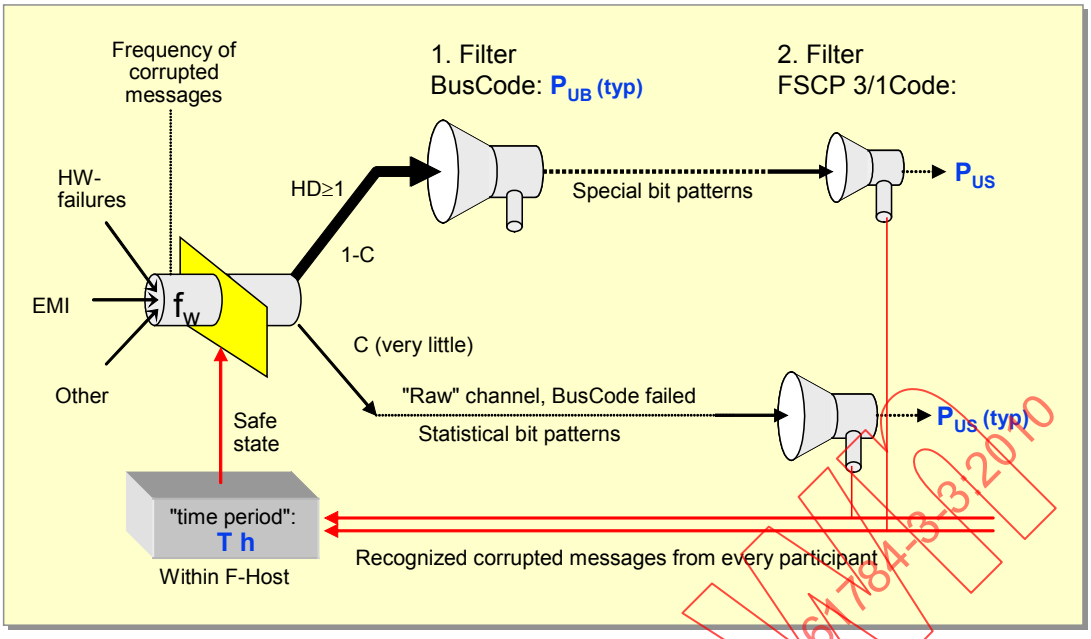


Figure 83 – Monitoring of corrupted messages

The terms used in Figure 83 are specified below:

fw = frequency of corrupted messages

EMI = electromagnetic interference

HD = hamming distance

c = frequency of occurrence

T = measurement period in hours (see 7.2.6).

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

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

9.5.2 Safety related constraints

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

Generally:

- All devices provide electrical safety SELV/PELV and a CPF 3 conformance test report
- Safety devices are designed for normal industrial environment according to IEC 61000-6-2 or IEC 61131-2 and provide increased immunity according to IEC 61326-3-1 and IEC 61326-3-2

V1-mode:

- Assumed number of safety-related messages per second and per 1:1 FSCP 3/1 communication relationship
  CP 3/1: 100
  CP 3/2: 10
- Number of retries per channel type (see 9.3.5):
  CP 3/1: 15 (IEC 61158-6-3: maximum of 8)

CP 3/2: 15 (IEC 61158-6-3: maximum of 8)
Backplane bus: 8 (within hosts or modular field devices)

- Black Channel CRC polynomials:
  Black Channel shall not use the safety layer CRC polynomials 14EABh and 1F4ACFB13h
  Black Channel polynomials shall not be divisible by C599h
- Active buffering network elements:
  CP 3/1: 2 messages maximum with links and/or repeater
- Octet-wise splitting of safety PDU:
  Not permitted

V2-mode:

- Assumed number of safety-related messages per second and per 1:1 FSCP 3/1 communication relationship
  < 10 000
- Number of retries per channel type (see 9.3.5):
  No restrictions
- Numbers of safety-related message sinks per safety function:
  No restrictions
- Black Channel CRC polynomials:
  No restrictions
- Active buffering network elements:
  No restrictions; any switch permitted (see 7.3.8 and 5.4.2)
- Safety islands:
  Single port routers are not permitted as borders for a safety island (see 7.3.9)
- Octet-wise splitting of safety PDU:
  No restrictions

9.5.3 Non safety related constraints (availability)

- Cyclic data exchange between hosts and field devices within a defined time period (sign of life)
- Guaranteed delivery of entire safety PDUs at the safety layer (data integrity)

Generally:

— CP 3/1: No spurs (branch lines)
— CP 3/RTE: Only one F-Host per submodule
— Ethernet-Switches shall be suitable for standard industrial environment as defined for example in IEC 61131-2

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

9.6 Maintenance

9.6.1 F-Module commissioning / replacement

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

9.6.2 Identification and maintenance functions

Identification and maintenance functions (I&M) are defining a set of parameters in an F-Device to identify device types and individual devices via a CPF 3 network and to support its maintenance [46]. These functions can be used to support the iParameterization as defined in

8.2. F-Devices/Modules shall implement the mandatory set of I&M functions. Additionally, F-Devices/Modules shall fill the field IM4 (signature) with a signature that indicates the safety configuration and parameterization state of the F-Device/Module if this signature is not otherwise incorporated in the overall F-Host project signature.

9.7 Safety manual

According to IEC 61508-2, F-Host and F-Device suppliers shall provide a safety manual. In case of FSCP 3/1, the instructions, information and parameters of Table 20 shall be included.

Table 20 – Information to be included in the safety manual

Item	Instruction and/or parameter	Remark
Safety handling	Instructions on how to configure, parameterize, commission, test, and lock this device safely in accordance with IEC 61508	See 9.1 (LED) and 7.3.7 (F-Address)
Power supply	Requirements for electrical safety (PELV), ripple, noise, interrupts, etc. shall be defined	See [44] for country specific constraints such as current limitation
Electrical safety	All network devices used in conjunction with this device shall meet the requirements of IEC 61010-1 or IEC 61131-2 (for example PELV)	See [44]
Electromagnetic immunity (EMI)	Applied tests and results (manufacturer declaration or test report from competent test laboratory)	According to IEC 62061, IEC 61326-3-1 or IEC 61326-3-2 whatever is applicable or device specific standard such as IEC 61496 [6]; [44]
Isolation	Applied test voltages and duration at the fieldbus communication port	See [44]
Network components	Constraints on switches, router, and other network components	See 7.3.8, 7.3.9, 9.5.2, and 9.5.3
Installation	According to IEC 61918 and IEC 61784-5-3	See also [64]
Commissioning	Usage of the check list in IEC 61784-5-3 on for example proper addressing, retry checking, signal quality, etc.	See also [65]
iParameter	Verification of safety functions shall include a check whether all F_iPar_CRC are > "0".	See 8.6.4.5
Maintenance	Conditions and procedures for part replacement; Identification	See 9.6
Life cycle	Parameter value(s) for Proof Test Interval	According to IEC 61508
Response time	Parameter values for DAT, WCDT, WDTime	See 9.3.2 and 9.3.3
Safety for machinery (electrical)	Parameter values for SIL claim, PFH (probability of failure per hour)	According to IEC 62061
Safety for machinery (non-electrical)	Parameter values for PL (Performance level), MTTFd (Meantime to dangerous failure)	According to ISO 13849-1
Safety for process automation	Parameter values for SIL claim, PFD (probability of failure on demand), interconnection possibilities to achieve higher SIL	According to IEC 61511 and [30]
Security	Instructions on how to establish an adequate level of security defining security zones with security gates.	See 9.8, [44], [53]
Assessment reports	Conformance test reports from the fieldbus organization and safety assessment reports from competent assessment bodies	See [45] and Clause 10

9.8 Wireless transmission channels

9.8.1 Black channel approach

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

9.8.2 Availability

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

9.8.3 Security measures

Before any deployment of a safety application with FSCP 3/1 and wireless components an assessment for dangerous threats such as eavesdropping or data manipulation shall be executed as pointed out in [44]. In case of no threat, no security measures are necessary. There are two possible threats identified so far:

- Willful changes of parameters of F-Devices and safety programs
- Attacks on the cyclic communication, for example simulation of the safety communication

In order to secure the wireless network against these cases the measures in Table 21 shall be considered according to IEEE 802.11i [26] for industrial WLAN as pointed out in IEC 61784-2 for class A devices. Figure 84 is providing an overview on the security measures.

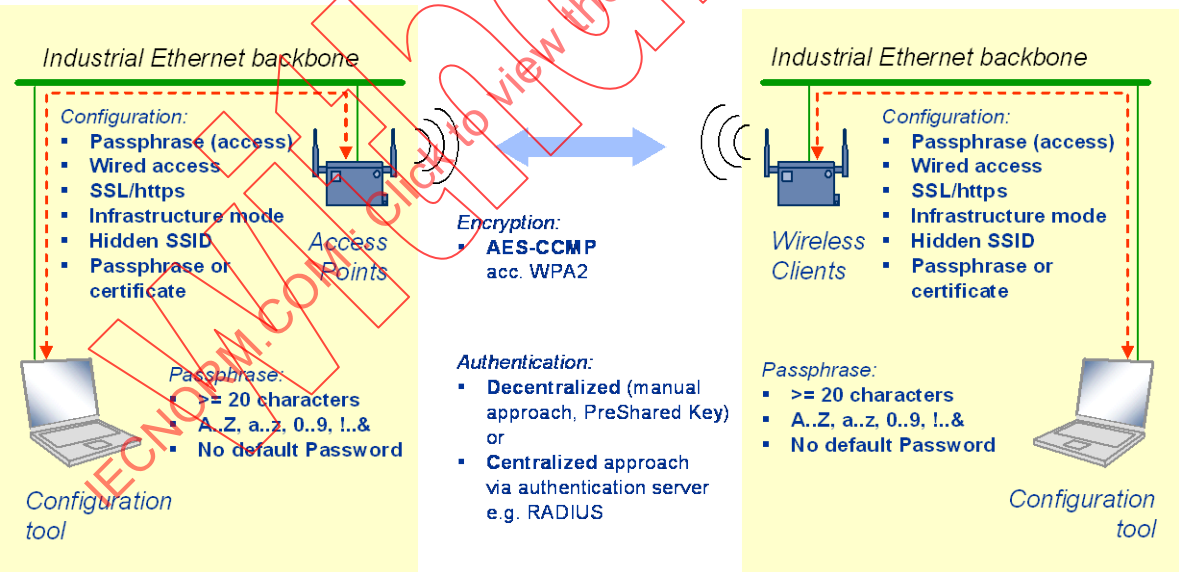


Figure 84 – Security for WLAN networks

The terms used in Figure 84 are specified below:

AES-CCMP	Advanced Encryption Standard - Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
RADIUS	Remote Authentication Dial In User Service
SSID	Service Set Identifier
SSL	Secure Sockets Layer
WPA2	Wi-Fi Protected Access 2 (corresponds to IEEE 802.11i [26])

Access Point	Coordinating station of a wireless service set according IEEE 802.11
Wireless Client	Member station of a wireless service set according IEEE 802.11

Table 21 – Security measures for WLAN (IEEE 802.11i)

No.	Item	Measure
1	Administration of the wireless access point and the wireless client	Only wired access is permitted using SSL or https. The administration password/passphrase shall not be the default password
2	Quality of the passphrase for administration	The length of the pass-phrase shall be ≥ 20 characters. Characters shall be a mix of alphabetical, numerical, and special signs
3	Operational modes	The *Infrastructure Mode* is permitted only. The *Ad hoc Mode* shall not be deployed
4	Authentication approaches	Either the *Decentralized Approach* (manual deployment of the authentication keys) or the *Centralized Approach* (dedicated authentication server for example RADIUS) are permitted. In case of a central authentication server in conjunction with roaming care shall be taken that the handover times are shorter than the cycle times
5	Authentication procedures	For authentication either *Shared Key* (= Preshared Secret) or *Certificates* are permitted
6	Quality of the pass-phrase for encryption	The length of the pass-phrase shall be ≥ 20 characters (see [26] H.4 Suggested pass-phrase-to PSK mapping). Characters shall be a mix of alphabetical, numerical, and special signs
7	Encryption of cyclic data communication (safety PDU)	*AES-CCMP* (according *WPA2*) [26] shall be deployed as encryption algorithm.
8	Hidden SSID	The wireless access point shall be configured in such a way that the SSID is hidden. The deployed SSID shall not be the default SSID
NOTE 1 The length of the pass-phrase should be acceptable since passwords or passphrases are to be entered only once during a commissioning session. NOTE 2 Encryption of cyclic data communication is securing against data manipulation.		

In order to secure the wireless network the measures in Table 22 shall be considered according IEEE 802.15.1 [27] for Bluetooth as pointed out in IEC 61784-2 for class A devices. Figure 85 is providing an overview on the security measures.

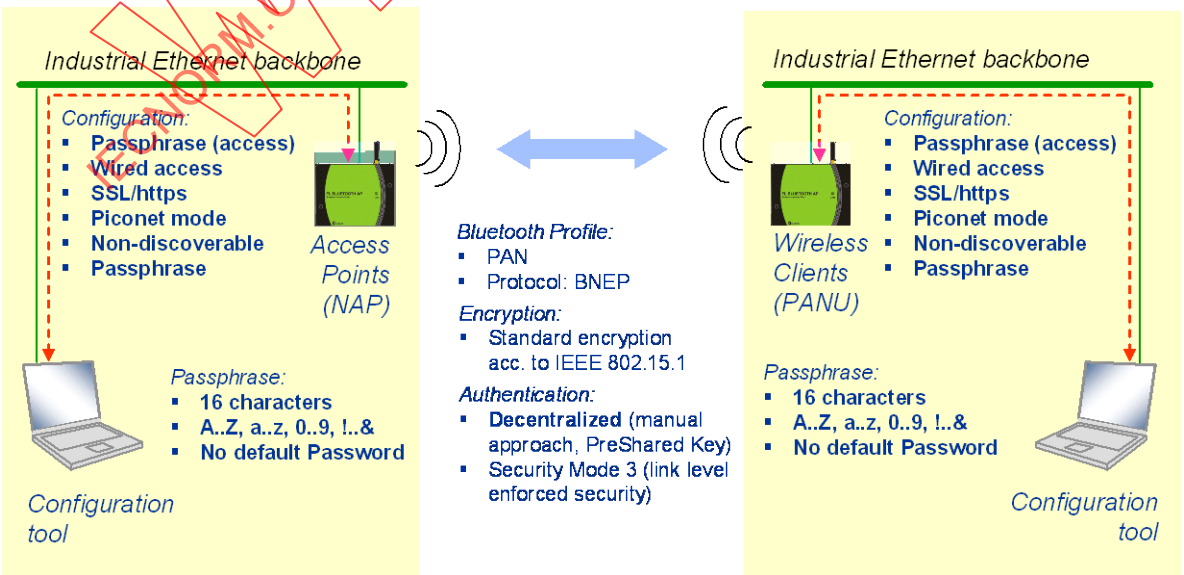


Figure 85 – Security for Bluetooth networks

The terms used in Figure 85 are specified below:

SSL	Secure Sockets Layer
PAN	Personal Area Network
BNEP	Bluetooth Network Encapsulation Protocol
NAP	Network Access Point
PANU	Personal Area Network User
Access Point	Coordinating station (master) of a wireless piconet according IEEE 802.15.1 [27]
Wireless Client	Member station (slave) of a wireless piconet according IEEE 802.15.1

Table 22 – Security measures for Bluetooth (IEEE 802.15.1)

No.	Item	Measure
1	Administration of the wireless access point and the wireless client	Only wired access is permitted using SSL or https. The administration password/passphrase shall not be the default password
2	Quality of the passphrase for administration	The length of the pass-phrase shall be 16 characters. Characters shall be a mix of alphabetical, numerical, and special signs
2	Operational modes	Devices shall operate in basic piconet mode, i.e. each device shall only communicate within one single piconet. Scatternets shall not be deployed
3	Authentication approaches	Bluetooth devices shall use security mode 3 (link level enforced security) as defined in IEEE 802.15.1 mandatory. Authentication is realized in a decentralized approach with the help of a pass-phrase (PIN). Devices which do not provide means to change the pass-phrase or which only work in security modes 1 (no security) or 2 (service level security) are not allowed
4	Quality of the pass-phrase for encryption	The length of the pass-phrase shall be 16 characters. Characters shall be a mix of alphabetical, numerical, and special signs
5	Encryption of cyclic data communication (safety PDU)	Encryption according IEEE 802.15.1 is mandatory
6	Discoverability	The wireless access point and clients shall be configured in such a way that they are undiscoverable

NOTE 1 The length of the pass-phrase should be acceptable since passwords or passphrases are to be entered only once during a commissioning session.

NOTE 2 Encryption of cyclic data communication is securing against data manipulation.

9.8.4 Stationary and mobile applications

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

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

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

9.9 Conformance classes

Manufacturers of F-Devices rely on some features their counterparts (F-Host) shall support as a minimum besides the conformance to the FSCP 3/1 protocol. The required features are listed in Table 23.

Table 23 – F-Host conformance class requirements

Item	Factory Automation	Process Automation	Note
GSD-Support	V5.04 (PB-DP) of [43]; V2.0 (PN-IO) of [47] or later versions	ditto	Regarding F-Parameters only
Communication function blocks according IEC 61131-3	Minimum communication function block set is: RDREC, WRREC, RDIAG, RALRM [49]	ditto	MS1 support is a precondition. Optional for other application profiles: GETIO_PART, SETIO_PART
iPar-Server	System manufacturers shall provide the "iPar-Server" services with at least 2^{15} octets	ditto	It is highly recommended for system manufacturers to provide the communication function blocks RDREC, WRREC, RDIAG (RALRM) [49]
Quantities (bit)	Maximum of 64 bit (Bool) coded as Unsigned8, -16, -32	ditto	Sizes of supported minimum data structures
Quantities (data types)	12 octet I/O	ditto	Sizes of supported minimum data structures
Data types	Unsigned8, -16, -32, Integer16, -32, No Real (Float)	all FSCP 3/1 data types: Unsigned8, -16, -32, Integer16, -32, Float32, Unsigned8+Unsigned8, Float32+Unsigned8	FSCP 3/1 rules for F-Channel drivers shall be observed
F-Host driver interface	All signals	All signals	
Diagnosis	Highly recommended: safety layer error messages (6.3.2)	Highly recommended: safety layer error messages (6.3.2)	Recommended literature: [50]
MS1	mandatory	mandatory	according CP 3/1
MS2	not through the controller (PLC)	optional	Small CPUs may not be able to carry high traffic through load
SIL claim	3 (within special application areas such as CNC: minimum 2)	3	
Tool-Integration, Parameteri-zation	Tool interface that meets the requirements of Table 12	According to [63] or via tool interface that meets the requirements of Table 12	

10 Assessment

10.1 Safety policy

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

- Any device automatically will not be applicable for safety-related applications just by using fieldbus communication and a safety communication layer.
- In order to enable a product for safety-related applications, appropriate development processes according to safety standards shall be observed (see IEC 61508, IEC 61511, IEC 60204-1, IEC 62061, ISO 13849-2) and/or an assessment from a competent assessment body shall be achieved.
- The manufacturer of a safety product is responsible for the correct implementation of the safety communication layer technology, the correctness and completeness of the product documentation and information.

- Additional important information about actual corrigendums through concluded change requests shall be considered for implementation and assessment. This information can be obtained from the organizations listed in Annex B.

The complete information is also available in [66].

10.2 Obligations

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

NOTE Examples of such “Authorities” are the BGIA (Berufsgenossenschaftliches Institut für Arbeitsschutz / BG - Institute for Occupational Safety and Health) in Germany, HSE (Health and Safety Executive) in UK, FM (Factory Mutual / Property Insurance and Risk Management Organization), UL (Underwriters Laboratories Inc. / Product Safety Testing and Certification Organization), or the INRS (Institut National de Recherche et de Sécurité) in France.

For FSCP 3/1 the rules on assessments within IEC 61784-3 apply. Additional information can be retrieved from [45].

Annex A
(informative)

Additional information for functional safety communication profiles of CPF 3

A.1 Hash function calculation

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

For the 24-bit CRC signature, the value 1*5D6DCB*h is used as the generator polynomial. The number of data bits may be odd or even. The value that is generated after the last octet corresponds to the transferred CRC signature.

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

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

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

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

where

- r represents the 24 bit CRC signature result
- q represents the pointer to the actual octet value that needs CRC calculation. After reading the value this pointer shall be incremented for the next octet via q++.
- the initial value of r is "0".

For this calculation Table A.1 is used.

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

CRC lookup table (0...255)							
0x000000	0x5D6DCB	0xBADB96	0xE7B65D	0x28DAE7	0x75B72C	0x920171	0xCF6CBA
0x51B5CE	0x0CD805	0xEB6E58	0xB60393	0x796F29	0x2402E2	0xC3B4BF	0x9ED974
0xA36B9C	0xFE0657	0x19B00A	0x44DDC1	0x8BB17B	0xD6DCB0	0x316AED	0x6C0726
0xF2DE52	0xAFB399	0x4805C4	0x15680F	0xDA04B5	0x87697E	0x60DF23	0x3DB2E8
0x1BBAF3	0x46D738	0xA16165	0xFC0CAE	0x336014	0x6E0DDF	0x89BB82	0xD4D649
0x4A0F3D	0x1762F6	0xF0D4AB	0xADB960	0x62D5DA	0x3FB811	0xD80E4C	0x856387
0xB8D16F	0xE5BCA4	0x020AF9	0x5F6732	0x900B88	0xCD6643	0x2AD01E	0x77BDD5
0xE964A1	0xB4096A	0x53BF37	0x0ED2FC	0xC1BE46	0x9CD38D	0x7B65D0	0x26081B
0x3775E6	0x6A182D	0x8DAE70	0xD0C3BB	0x1FAF01	0x42C2CA	0xA57497	0xF8195C
0x66C028	0x3BADE3	0xDC1BBE	0x817675	0x4E1ACF	0x137704	0xF4C159	0xA9AC92
0x941E7A	0xC973B1	0x2EC5EC	0x73A827	0xBCC49D	0xE1A956	0x061F0B	0x5B72C0
0xC5ABB4	0x98C67F	0x7F7022	0x221DE9	0xED7153	0xB01C98	0x57AAC5	0x0AC70E
0x2CCF15	0x71A2DE	0x961483	0xCB7948	0x0415F2	0x597839	0xBECE64	0xE3A3AF
0x7D7ADB	0x201710	0xC7A14D	0x9ACC86	0x55A03C	0x08CDF7	0xEF7BAA	0xB21661
0x8FA489	0xD2C942	0x357F1F	0x6812D4	0xA77E6E	0xFA13A5	0x1DA5F8	0x40C833
0xDE1147	0x837C8C	0x64CAD1	0x39A71A	0xF6CBA0	0xABA66B	0x4C1036	0x117DFD
0x6EEBCC	0x338607	0xD4305A	0x895D91	0x46312B	0x1B5CE0	0xFCEABD	0xA18776
0x3F5E02	0x6233C9	0x858594	0xD8E85F	0x1784E5	0x4AE92E	0xAD5F73	0xF032B8
0xCD8050	0x90ED9B	0x775BC6	0x2A360D	0xE55AB7	0xB8377C	0x5F8121	0x02ECEA
0x9C359E	0xC15855	0x26EE08	0x7B83C3	0xB4EF79	0xE982B2	0x0E34EF	0x535924
0x75513F	0x283CF4	0xCF8AA9	0x92E762	0x5D8BD8	0x00E613	0xE7504E	0xBA3D85
0x24E4F1	0x79893A	0x9E3F67	0xC352AC	0x0C3E16	0x5153DD	0xB6E580	0xEB884B
0xD63AA3	0x8B5768	0x6CE135	0x318CFE	0xFEE044	0xA38D8F	0x443BD2	0x195619
0x878F6D	0xDAE2A6	0x3D54FB	0x603930	0xAF558A	0xF23841	0x158E1C	0x48E3D7
0x599E2A	0x04F3E1	0xE345BC	0xBE2877	0x7144CD	0x2C2906	0xCB9F5B	0x96F290
0x082BE4	0x55462F	0xB2F072	0xEF9DB9	0x20F103	0x7D9CC8	0x9A2A95	0xC7475E
0xFAF5B6	0xA7987D	0x402E20	0x1D43EB	0xD22F51	0x8F429A	0x68F4C7	0x35990C
0xAB4078	0xF62DB3	0x119BEE	0x4CF625	0x839A9F	0xDEF754	0x394109	0x642CC2
0x4224D9	0x1F4912	0xF8FF4F	0xA59284	0x6AFE3E	0x3793F5	0xD025A8	0x8D4863
0x139117	0x4EFCDC	0xA94A81	0xF4274A	0x3B4BF0	0x66263B	0x819066	0xDCFDAD
0xE14F45	0xBC228E	0x5B94D3	0x06F918	0xC995A2	0x94F869	0x734E34	0x2E23FF
0xB0FA8B	0xED9740	0x0A211D	0x574CD6	0x98206C	0xC54DA7	0x22FBFA	0x7F9631

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

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

r = crctab32 [((r >> 24) ^ *q++) & 0xff] ^ (r << 8) (A.2)

For this calculation Table A.2 is used.

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

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

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

A.2 Response time measurements

In 9.3.1 a simplified model for typical response times is described. The congruence between the model and a real multivendor application for 15 000 sample measurements is shown in Figure A.2. In this case the transmission rate had been 1,5 Mbit/s and the F-Host was executing the safety-related application (program) every other 20 ms.

Additional computers such as programmers or diagnosis panels using acyclic access to the network (Figure 3) are having little or no impact on the response times if the network is

configured according to the manufacturer's recommendation. Figure A.3 shows the frequency distribution of response times of a real CP 3/1 and FSCP 3/1 multivendor application with 1,5 Mbit/s and 2 different stress situations. The blue curve represents 22 000 measurements with a stand alone safety PLC. The dark blue curve represents 6 500 measurements with the same safety PLC, an additional programmer (PG) periodically displaying the program status, and a diagnosis panel (PC) periodically displaying the status of the beams of a light curtain. Both PG and PC were communicating via the acyclic services of the CP 3/1 (master class 2).

It demonstrates that additional two supervisor devices as expected are little or not impacting the response times. The curves are close to a bell curve distribution with a minimum reaction time of 13 ms, a maximum reaction time of 35 ms, and an average reaction time of 24 ms.

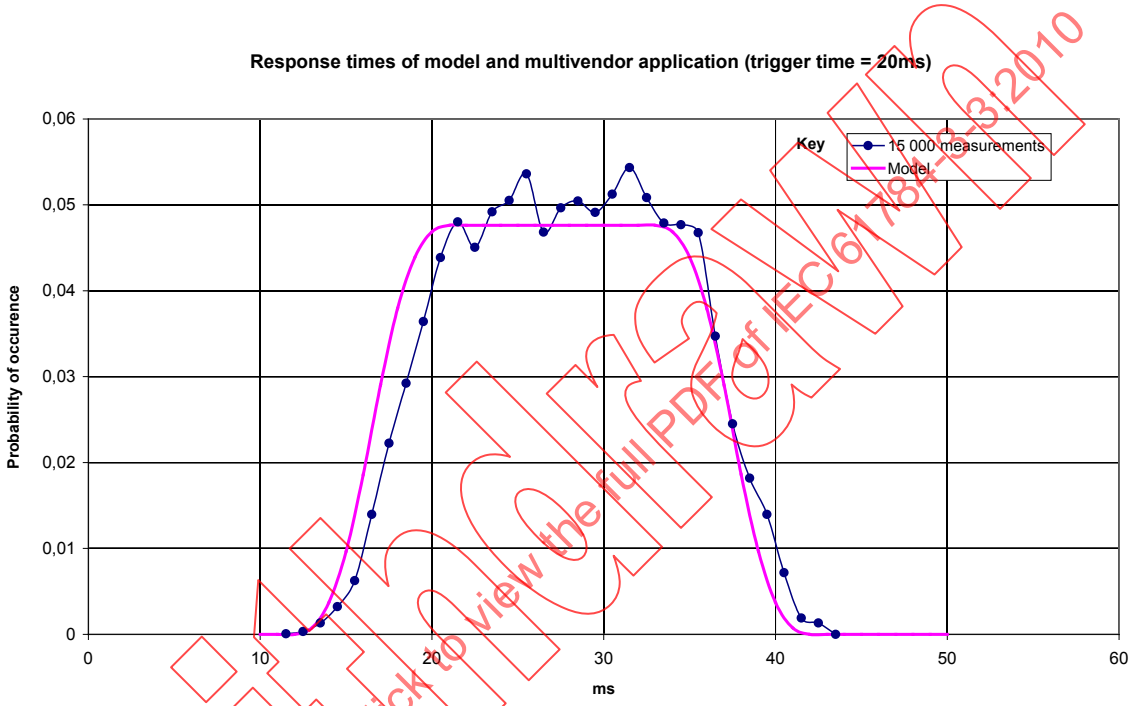


Figure A.2 – Comparison of the response time model and a real application

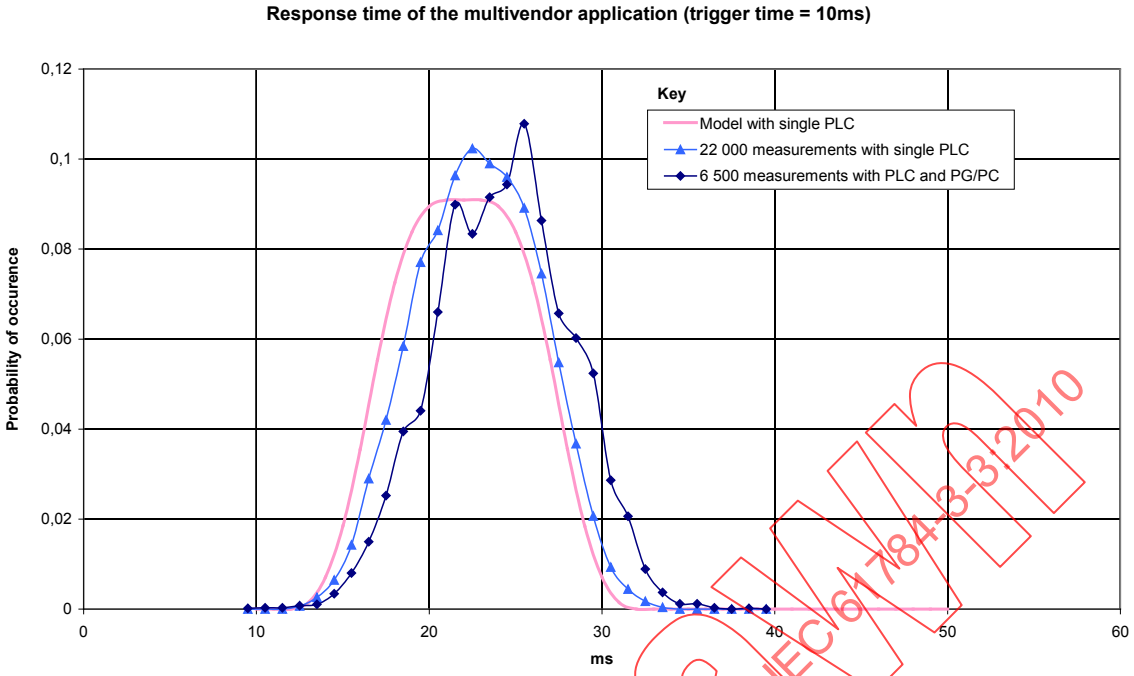


Figure A.3 – Frequency distribution of measured response times

The colours used in Figure A.3 are specified below:

cyan — Model with single PLC (CPU)

blue — 22 000 response time measurements with a multivendor application and a single PLC (F-Host)

dark blue — 6 500 response time measurements with a multivendor application using one single PLC (F-Host), plus one programmer (master class 2) for the function "cyclic program status", plus one extra diagnosis panel (second master class 2) for the function "cyclic light curtain status"

The F-Host of the model is sharing the same CPU for standard and safety programs. Both programs are executed within different operating system levels to provide logical separation of the safety-related application program from the standard program. Figure A.4 is showing examples of different segmentations of the standard program for several time trigger values. It demonstrates that a change in the standard program part is not impacting the execution of the safety program. However, it can be important to balance out the update of standard and safety outputs if it is necessary to use signals from the other part for the purpose of coordination.

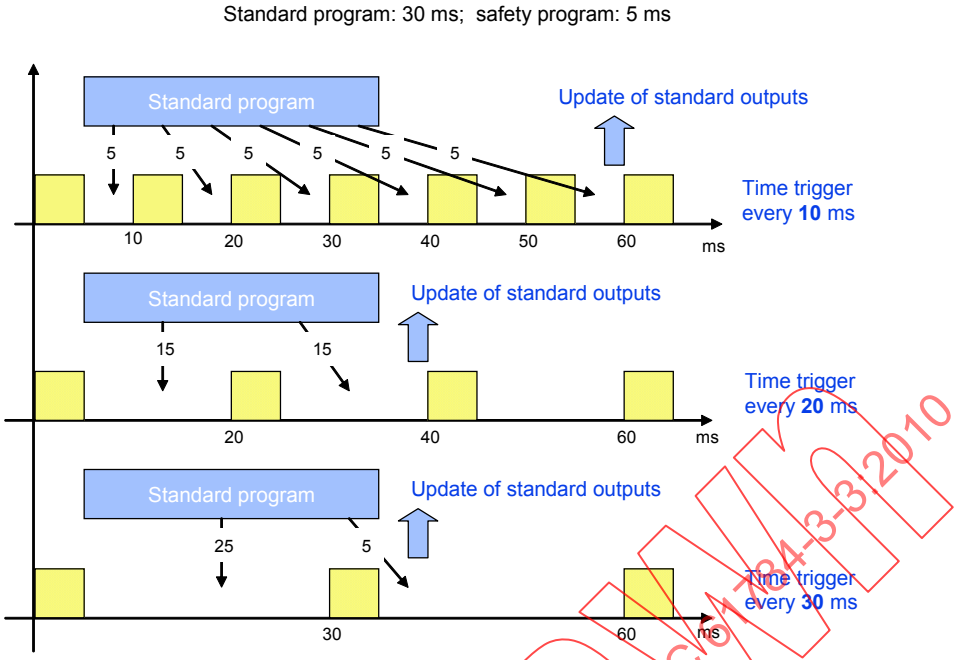


Figure A.4 – F-Host with standard and safety-related application programs

Annex B
(informative)

Information for assessment of the functional safety communication profiles of CPF 3

Information about test laboratories which test and validate the conformance of FSCP 3/1 products with IEC 61784-3-3 can be obtained from the National Committees of the IEC or from the following organization:

PROFIBUS Nutzerorganisation e.V. (PNO)
Haid-und-Neu-Str. 7
76131 Karlsruhe
GERMANY

Phone: +49 721 96 58 590
Fax: +49 721 96 58 589
E-mail: info@profibus.com
URL:www.profibus.com or
URL:www.profisafe.net

Bibliography

[1] IEC 60050 (all parts), *International Electrotechnical Vocabulary*

NOTE See also the IEC Multilingual Dictionary – Electricity, Electronics and Telecommunications (available on CD-ROM and at <http://www.electropedia.org>)

[2] IEC 60870-5-1, *Telecontrol equipment and systems – Part 5: Transmission protocols – Section One: Transmission frame formats*

[3] IEC/TS 61000-1-2, *Electromagnetic compatibility (EMC) – Part 1-2: General – Methodology for the achievement of the functional safety of electrical and electronic equipment with regard to electromagnetic phenomena*

[4] IEC 61131-6[12], *Programmable controllers – Part 6: Functional safety*

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

[6] IEC 61496 (all parts), *Safety of machinery – Electro-sensitive protective equipment*

[7] IEC 61508-1:2010[13], *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements*

[8] IEC 61508-4:2010[13], Functional safety of electrical/electronic/programmable electronic *safety-related systems – Part 4: Definitions and abbreviations*

[9] IEC 61508-5:2010[13], *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 5: Examples of methods for the determination of safety integrity levels*

[10] IEC 61508-6:2010[13], *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3*

[11] IEC 61784-4[14], *Industrial communication networks – Profiles – Part 4: Secure communications for fieldbuses*

[12] IEC 61784-5 (all parts), *Industrial communication networks – Profiles – Part 5: Installation of fieldbuses – Installation profiles for CPF x*

[13] IEC 61800-5-2, *Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional*

[14] IEC 61804 (all parts), *Function blocks (FB) for process control*

[15] IEC/TR 62059-11, *Electricity metering equipment – Dependability – Part 11: General concepts*

[16] IEC/TR 62210, *Power system control and associated communications – Data and communication security*

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

[18] ISO/IEC Guide 51:1999, *Safety aspects — Guidelines for their inclusion in standards*

[19] ISO/IEC 2382-14, *Information technology – Vocabulary – Part 14: Reliability, maintainability and availability*

[20] ISO/IEC 2382-16, *Information technology – Vocabulary – Part 16: Information theory*

[21] ISO/IEC 7498 (all parts), *Information technology – Open Systems Interconnection – Basic Reference Model*

[22] ISO 10218-1, *Robots for industrial environments – Safety requirements – Part 1: Robot*

[23] ISO 12100-1, *Safety of machinery – Basic concepts, general principles for design – Part 1: Basic terminology, methodology*

[24] ISO 14121, *Safety of machinery – Principles of risk assessment*

---

12 In preparation.

13 To be published

14 Proposed new work item under consideration.

[25] EN 954-1:1996[15], *Safety of machinery – Safety related parts of control systems – General principles for design*

[26] IEEE 802.11i-2004 Amendment to IEEE Std 802.11, 1999 Edition (Reaff 2003): *IEEE Standard for Information technology – Telecommunications and information exchange between system – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications – Amendment 6: Medium Access Control (MAC) Security Enhancements*

[27] IEEE 802.15.1-2005: *IEEE Standard for Information technology – Telecommunications and information exchange between systems-Local and metropolitan area networks – Specific requirements*

[28] ANSI/ISA-84.00.01-2004 (all parts), *Functional Safety: Safety Instrumented Systems for the Process Industry Sector*

[29] VDI/VDE 2180 (all parts), *Safeguarding of industrial process plants by means of process control engineering*

[30] VDI/VDE-Richtlinien 2180, Part 1-4: 2006, *Safeguarding of industrial process plants by means of process control engineering*, (in German language),

[31] GS-ET-26[16], *Grundsatz für die Prüfung und Zertifizierung von Bussystemen für die Übertragung sicherheitsrelevanter Nachrichten*, May 2002. HVBG, Gustav-Heinemann-Ufer 130, D-50968 Köln ("*Principles for Test and Certification of Bus Systems for Safety relevant Communication*")

[32] ANDREW S. TANENBAUM, *Computer Networks*, 4th Edition, Prentice Hall, N.J., ISBN-10:0130661023, ISBN-13: 978-0130661029

[33] W. WESLEY PETERSON, *Error-Correcting Codes*, 2nd Edition 1981, MIT-Press, ISBN 0-262-16-039-0

[34] BRUCE P. DOUGLASS, *Doing Hard Time*, 1999, Addison-Wesley, ISBN 0-201-49837-5

[35] *New concepts for safety-related bus systems*, 3rd International Symposium "Programmable Electronic Systems in Safety Related Applications ", May 1998, from Dr. Michael Schäfer, BG-Institute for Occupational Safety and Health.

[36] DIETER CONRADS, *Datenkommunikation*, 3rd Edition 1996, Vieweg, ISBN 3-528-245891

[37] German IEC subgroup DKE AK 767.0.4: *EMC and Functional Safety*, Spring 2002

[38] NFPA79 (2002), *Electrical Standard for Industrial Machinery*

[39] GUY E. CASTAGNOLI, *On the Minimum Distance of Long Cyclic Codes and Cyclic Redundancy-Check Codes*, 1989, Dissertation No. 8979 of ETH Zurich, Switzerland

[40] GUY E. CASTAGNOLI, STEFAN BRÄUER, and MARTIN HERRMANN, *Optimization of Cyclic Redundancy-Check Codes with 24 and 32 Parity Bits*, June 1993, IEEE Transactions On Communications, Volume 41, No. 6

[41] SCHILLER F and MATTES T: *An Efficient Method to Evaluate CRC-Polynomials for Safety-Critical Industrial Communication*, Journal of Applied Computer Science, Vol. 14, No 1, pp. 57-80, Technical University Press, Łódź,Poland, 2006

[42] SCHILLER F and MATTES T: *Analysis of CRC-polynomials for Safety-critical Communication by Deterministic and Stochastic Automata*, 6th IFAC Symposium on Fault Detection, Supervision and Safety for Technical Processes, SAFEPROCESS 2006, pp. 1003-1008, Beijing, China, 2006

[43] PROFIBUS Guideline: *Specification for PROFIBUS Device Description and Device Integration, Volume 1: GSD*, V5.1, July 2008. Order-No. 2.122

[44] PROFIBUS Guideline: *PROFIsafe – Environmental Requirements*, V2.5, March 2007. Order-No. 2.232

[45] PROFIBUS Guideline: *PROFIsafe – Test Specification for F-Slaves, F-Devices, and F-Hosts*, V2.1, March 2007. Order-No. 2.242

---

[15] To be replaced by ISO 13849-1 and/or IEC 62061.

[16] This document has been one of the starting points for this part. It is currently undergoing a major revision.

[46] PROFIBUS Profile Guideline, Part 1: *Identification & Maintenance Functions*, V1.2, October 2009. Order-No. 3.502

[47] PROFIBUS Guideline: *GSDML Specification for PROFINET IO*, Version 2.2, July 2008. Order-No. 2.352

[48] PROFIBUS Guideline: *PROFIsafe – Profile for Safety Technology*, V1.30, June 2004. Order-No. 3.092

[49] PROFIBUS Guideline: *Communication Function Blocks on PROFIBUS DP and PROFINET IO*, V2.0, November 2005. Order-No. 2.182

[50] PROFIBUS Profile Guideline, Part 3: *Diagnosis, Alarms, and Time Stamping*, V1.0, June 2004. Order-No. 3.522

[51] PROFINET Guideline: *PROFINET Cabling and Interconnection Technology*, Version 2.0, May 2007. Order-No. 2.252

[52] PROFINET Guideline: *Installation Guideline PROFINET Part 2, Network Components*, Version 1.01, Februar 2004. Order-No. 2.252p2

[53] PROFINET Guideline: *PROFINET Security*, V1.0, March 2005. Order-No. 7.002

[54] MANFRED POPP, *The New Rapid Way to PROFIBUS DP*, 2002. Order-No. 4.072

[55] MANFRED POPP, *Industrial Communication with PROFINET*, 2007. Order-No. 4.182

[56] OPC Foundation, < www.opcfoundation.org >

[57] Object Management Group, *Unified Modeling Language: Superstructure*, Version 2.0; Formal/05-07-04;available at < www.omg.com >

[58] NAMUR, *NE97 – Fieldbus for safety-related uses*, 2003; available at < www.namur.de >

[59] REC-xml-20081126, *Extensible Markup Language (XML) 1.0 (Fifth Edition)* – W3C Recommendation 26 November 2008,
available at < www.w3.org/TR/2008/REC-xml-20081126 >

[60] REC-xmlschema-1-20041028, *XML Schema Part 1: Structures (Second Edition)* – W3C Recommendation 28 October 2004,
available at < www.w3.org/TR/2004/REC-xmlschema-1-20041028 >

[61] REC-xmlschema-2-20041028, *XML Schema Part 2: Datatypes (Second Edition)* – W3C Recommendation 28 October 2004,
available at < www.w3.org/TR/2004/REC-xmlschema-2-20041028 >

[62] USB Implementers Forum, Inc , *Universal Serial Bus Revision 2.0 specification*,
available at < http://www.usb.org/developers/docs >

[63] PROFIBUS Specification: Amendment *PA-Devices on PROFIsafe*, V1.01, March 2009; Order-No. 3.042

[64] PROFIBUS Guideline: *Cabling and Assembly*, V1.0.6, May 2006. Order No. 8.022

[65] PROFIBUS Guideline: *Commissioning*, V1.0.2, November 2006. Order No. 8.032

[66] PROFIBUS Guideline: *PROFIsafe Policy*, V1.3, February 2003. Order No. 2.282

[67] PROFIBUS Profile Guideline, Part 2: *Data types, Programming Languages, and Platforms*, V1.0, September 2006. Order-N. 3.512

[68] PROFIBUS Specification: *Amendment PROFIdrive on PROFIsafe*, V2.1, April 2009. Order-No. 3.272

[69] PROFINET Specification[17]: *Configuration in Run*, dV0.1, August 2009. Order-No. 2.512

———————

[17] In preparation.

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

RÉSEAUX DE COMMUNICATION INDUSTRIELS – PROFILS –

Partie 3-3: Bus de terrain de sécurité fonctionnelle – Spécifications supplémentaires pour CPF 3

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (CEI) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de la CEI). La CEI a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, la CEI – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de la CEI"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec la CEI, participent également aux travaux. La CEI collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de la CEI concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de la CEI intéressés sont représentés dans chaque comité d'études.
3) Les Publications de la CEI se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de la CEI. Tous les efforts raisonnables sont entrepris afin que la CEI s'assure de l'exactitude du contenu technique de ses publications; la CEI ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de la CEI s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de la CEI dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de la CEI et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) La CEI elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de la CEI. La CEI n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à la CEI, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de la CEI, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de la CEI ou de toute autre Publication de la CEI, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.

La Norme internationale CEI 61784-3-3 a été établie par le sous-comité 65C: Réseaux de communication industriels, du comité d'études 65 de la CEI: Mesure, commande et automation dans les processus industriels.

Cette seconde édition annule et remplace la première édition parue en 2007, dont elle constitue une révision technique. Les principales modifications par rapport à l'édition précédente sont énumérées ci-dessous:

— mises à jour par rapport aux changements apportés à la CEI 61784-3;
— présentation d'un temporisateur secondaire (F_WD_Time_2) couvrant l'utilisation des cas de « configuration en cours » et/ou de « maintenance des systèmes de tolérance aux pannes » (7.1.3, 7.2.3, 7.2.6, 8.1.1, 8.1.4, 8.1.6.2);
— définitions GSDL manquantes provenant d'autres documents approuvés (8.3.2.1);
— calcul de signature CRC manquant pour un GSD provenant d'autres documents approuvés (8.3.3.3);

— contraintes d'attribution de valeur de paramètre du temporisateur principal F_WD_Time (9.3.3);

— identification de l'état de paramétrage de sécurité d'un dispositif F ou d'un module F grâce au champ IM4 (signature) des fonctions I&M (9.6.2);

— documents mis à jour dans la bibliographie.

La présente version bilingue (2012-02) correspond à la version anglaise monolingue publiée en 2010-06.

Le texte anglais de cette norme est issu des documents 65C/591A/FDIS et 65C/603/RVD.

Le rapport de vote 65C/603/RVD donne toute information sur le vote ayant abouti à l'approbation de cette norme.

La version française de cette norme n'a pas été soumise au vote.

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

Une liste de toutes les parties de la série CEI 61784-3, présentées sous le titre général *Réseaux de communication industriels – Profils – Bus de terrain de sécurité fonctionnelle*, est disponible sur le site web de la CEI.

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

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

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

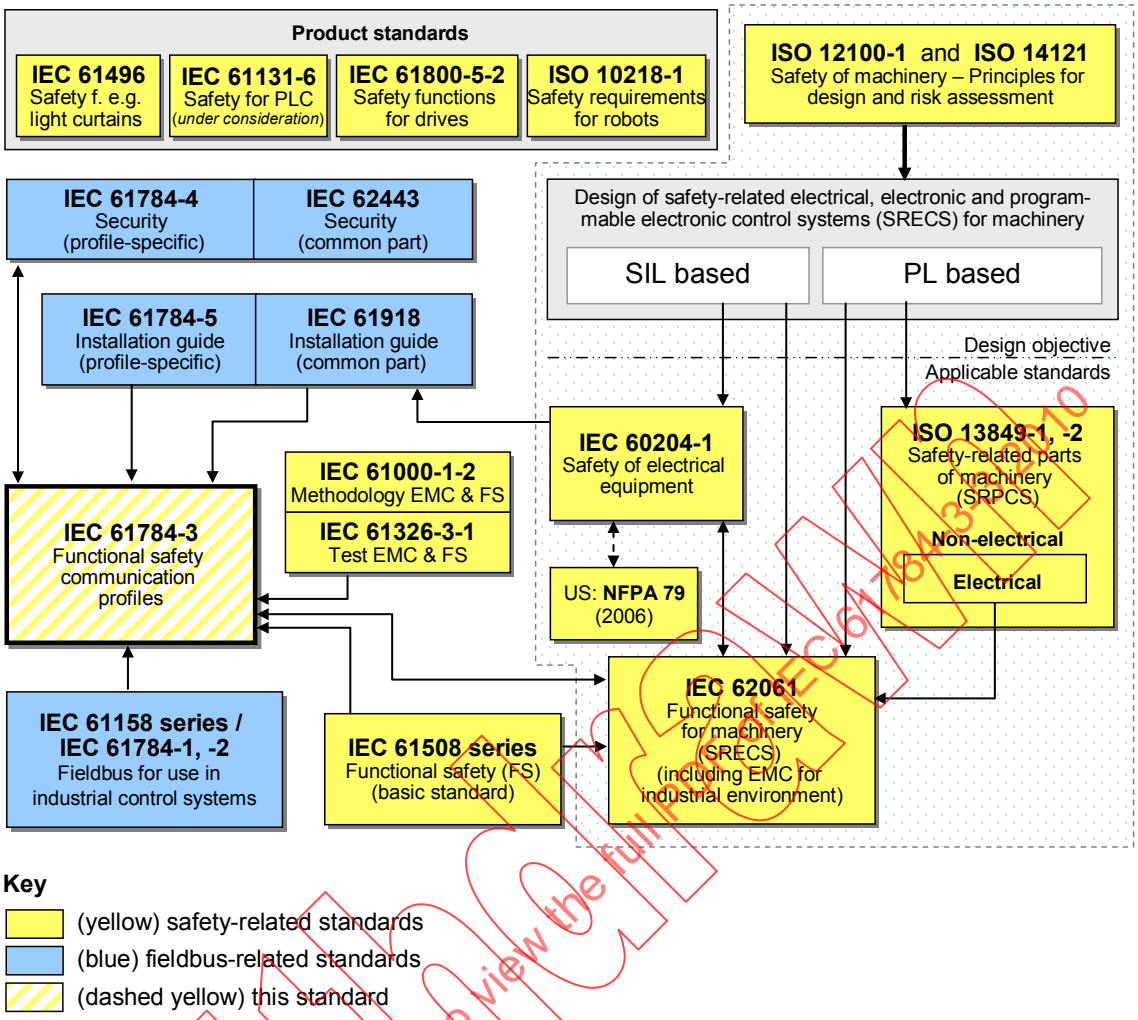
0 Introduction

0.1 Généralités

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

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

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



Key

(yellow) safety-related standards
(blue) fieldbus-related standards
(dashed yellow) this standard

Légende

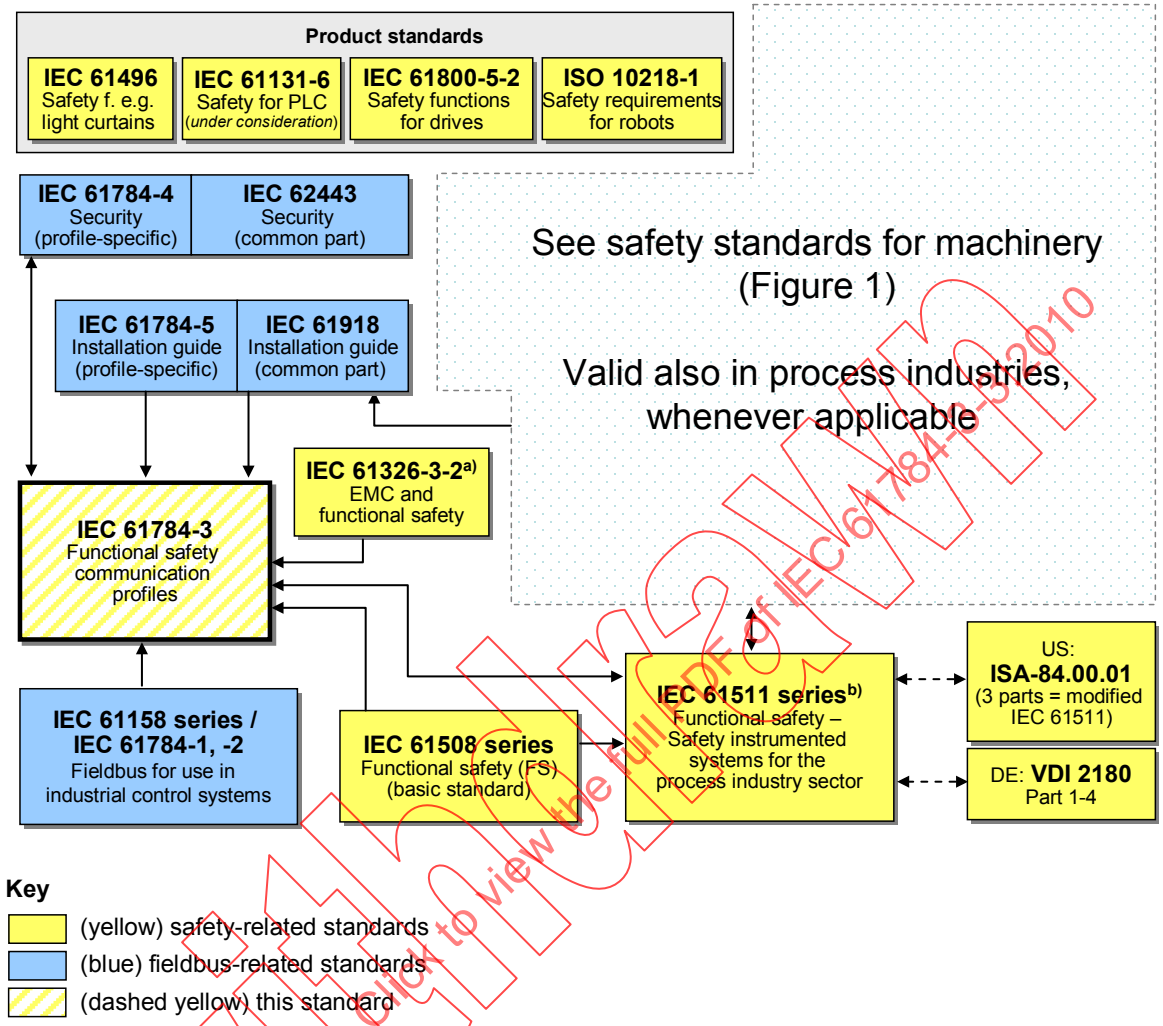
Anglais	Français
Product standards	Normes de produits
Safety function, e.g. light curtains	Fonction de sécurité, par exemple rideaux de lumière
Safety for PLC (under consideration)	Sécurité relative aux automates programmables (à l'étude)
Safety functions for drives	Fonctions de sécurité applicables aux entraînements
Safety requirements for robots	Exigences de sécurité applicables aux robots
Safety of machinery - ... assessment	Sécurité des machines – principes généraux de conception et appréciation du risque
Security (profile-specific)	Sûreté (spécifique au profil)
Security (common part)	Sûreté (partie commune)
Design of safety-related .... for machinery	Conception des systèmes de commande électriques, électroniques et électroniques programmables relatifs à la sécurité pour les machines
SIL based	Basé sur SIL
PL based	Basé sur PL
Installation guide (profile-specific)	Guide d'installation (spécifique au profil)
Installation guide (common part)	Guide d'installation (partie commune)

Anglais	Français
Design objective	Objectif de conception
Applicable standards	Normes applicables
Safety of electrical equipment	Sécurité des équipements électriques
Safety-related parts of machinery	Parties des systèmes de commande relatives à la sécurité
Non-electrical	Non électrique
Electrical	Electrique
Methodology EMC & functional safety	Méthodologie en matière de compatibilité électromagnétique & sécurité fonctionnelle
Test EMC & functional safety	Essai CEM et sécurité fonctionnelle
Functional safety communication profiles	Profils de communication de sécurité fonctionnelle
IEC 61158 series / Fieldbus for use in industrial control systems	Série CEI 61158 / Bus de terrain pour utilisation dans des systèmes de commande industriels
IEC 61508 series, Functional safety (basic standard)	Série CEI 61508 Sécurité fonctionnelle (norme de base)
Functional safety for machinery .... for industrial environment)	Sécurité fonctionnelle des systèmes de commande électriques, électroniques et électroniques programmables (y compris les interférences électromagnétiques dans l'environnement industriel)
Key	Légende
(yellow) safety-related standards	(jaune) normes relatives à la sécurité
(blue) fieldbus-related standards	(bleu) normes relatives au bus de terrain
(dashed) yellow) this standard	(jaune pointillé) la présente norme
IEC	CEI

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

Figure 1 - Relations entre la CEI 61784–3 et d'autres normes (machines)

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



Légende

Anglais	Français
Product standards	Normes de produits
Safety function, e.g. light curtains	Fonction de sécurité, par exemple barrières photo électriques
Safety for PLC (under consideration)	Sécurité relative aux automates programmables (à l'étude)
Safety functions for drives	Fonctions de sécurité applicables aux entraînements
Safety requirements for robots	Exigences de sécurité applicables aux robots
Security (profile-specific)	Sûreté (spécifique au profil)
Security (common part)	Sûreté (partie commune)
Installation guide (profile-specific)	Guide d'installation (spécifique au profil)
Installation guide (common part)	Guide d'installation (partie commune)
See safety standards for machinery (Figure 1)	Voir normes de sécurité pour les machines (Figure 1)
Valid also in process industries, whenever applicable	Valable également dans les industries de transformation, le cas échéant
Functional safety communication profiles	Profils de communication de sécurité fonctionnelle

Anglais	Français
IEC 61326-3-2 a) EMC and functional safety	CEI 61326-3-2 a) CEM & sécurité fonctionnelle
IEC 61158 series/ IEC 61784-1-2, Fieldbus for use in industrial control systems	Série CEI 61158/ CEI 61784-1,-2 Bus de terrain pour utilisation dans des systèmes de commande industriels
IEC 61508 series, Functional safety (basic standard)	Série CEI 61508 Sécurité fonctionnelle (norme de base)
IEC 61511 seriesb) Functional safety–safety instrumented systems for the process industry sector	Série CEI 61511b) sécurité fonctionnelle – systèmes instrumentés de sécurité pour le secteur des industries de transformation
US: ISA 84.00.1 (3 parts = modified IEC 61511)	US: ISA 84.00.1 (3 parties = CEI 61511 modifiée)
DE : VDI 2180 Part 1 –4	DE : VDI 2180 Parties 1 à 4
Key	Légende
(yellow) safety-related standards	(jaune) normes relatives à la sécurité
(blue) fieldbus-related standards	(bleu) normes relatives au bus de terrain
(dashed) yellow) this standard	(jaune pointillé) la présente norme

a Pour des environnements électromagnétiques spécifiés, sinon CEI 61326-3-1.

b EN ratifiée.

Figure 2 – Relations entre la CEI 61784–3 et d'autres normes (transformation)

Les couches de communication de sécurité mises en œuvre dans le cadre de systèmes relatifs à la sécurité conformément à la série CEI 61508, assurent la confiance nécessaire à accorder à la transmission de messages (information) entre deux participants ou plus sur un bus de terrain dans un système relatif à la sécurité, ou une fiabilité suffisante dans le comportement de sécurité en cas d'erreurs ou de défaillances du bus de terrain.

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

La revendication du SIL qui en résulte pour un système dépend de la mise en œuvre du profil de communication de sécurité fonctionnelle retenu au sein du système – la mise en œuvre du profil de communication de sécurité fonctionnelle dans un dispositif normal ne suffit pas à le qualifier de dispositif de sécurité.

La présente norme décrit:

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

— la description individuelle des profils de sécurité fonctionnelle pour plusieurs familles de profils de communication dans les CEI 61784-1 et CEI 61784-2;

— les extensions de la couche de sécurité aux sections relatives au service et aux protocoles de communication de la série CEI 61158.

0.2 Déclaration de droits de propriété

La Commission électrotechnique internationale (CEI) attire l'attention sur le fait qu'il est déclaré que la conformité avec le présent document peut impliquer l'utilisation de brevets concernant les profils de communication de sécurité fonctionnelle pour la famille 3, où la notation [xx] désigne le détenteur des droits de propriété.

EP1267270-A2 [SI] Method for data transfer

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
EP1686732	[SI]	Method and system for transmitting protocol data units
EP1802019	[SI]	Identification of errors in data transmission
EP1921525-A1	[SI]	Method for operation of a safety-related system

La CEI ne prend pas position eu égard à la preuve, la validité et la portée de ces droits de propriété.

Les détenteurs de ces droits de propriété ont donné l'assurance à la CEI qu'ils consentent à négocier des licences avec des demandeurs du monde entier, en des termes et à des conditions raisonnables et non discriminatoires. A ce propos, la déclaration des détenteurs de ces droits de propriété est enregistrée à la CEI.

Des informations peuvent être obtenues auprès de:

[SI] Siemens AG
I IA AS FA TC
76187 Karlsruhe
ALLEMAGNE

L'attention est attirée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété autres que ceux mentionnés ci-dessus. La CEI ne doit pas être tenue pour responsable de ne pas avoir dûment signalé tout ou partie de ces droits de propriété.

RÉSEAUX DE COMMUNICATION INDUSTRIELS – PROFILS –

Partie 3-3: Bus de terrain de sécurité fonctionnelle – Spécifications supplémentaires pour CPF 3

1 Domaine d'application

La présente partie de la série CEI 61784-3 spécifie une couche de communication relative à la sécurité (services et protocole) fondée sur la CPF 3 de la CEI 61784-1 et les Types 3 et 10 de la CEI 61784-2 (CP 3/1, CP 3/2, CP 3/4, CP 3/5 et CP 3/6) et de la CEI 61158. Elle identifie les principes applicables aux communications de sécurité fonctionnelle définies dans la CEI 61784-3, et appropriés à cette couche de communication de sécurité.

NOTE 1 Elle ne couvre pas les aspects relatifs à la sécurité électrique et à la sécurité intrinsèque. La sécurité électrique concerne les dangers tels que les chocs électriques. La sécurité intrinsèque concerne les dangers associés aux atmosphères explosibles.

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

La présente partie fournit des lignes directrices tant pour les développeurs que pour les évaluateurs de dispositifs et systèmes conformes.

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

2 Références normatives

Les documents de référence suivants sont indispensables pour l'application du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

CEI 60204-1, *Sécurité des machines – Équipement électrique des machines – Partie 1: Règles générales*

CEI 61000-6-2, *Compatibilité électromagnétique (CEM) – Partie 6-2: Normes génériques – Immunité pour les environnements industriels*

CEI 61010-1, *Règles de sécurité pour appareils électriques de mesurage, de regulation et de laboratoire – Partie 1: Exigences générales*

IEC 61131-2, *Programmable controllers – Part 2: Equipment requirements and tests* (disponible uniquement en anglais)

---

1 Dans les pages suivantes de la présente norme, "la présente partie" se substitue à "cette partie de la série CEI 61784-3".

2 Dans les pages suivantes de la présente norme, "CEI 61508" se substitue à "série CEI 61508".

IEC 61131-3, *Programmable controllers – Part 3: Programming languages* (disponible en anglais uniquement)

IEC 61158-2, *Industrial communication networks – Fieldbus specifications – Part 2: Physical layer specification and service definition* (disponible uniquement en anglais)[3]

IEC 61158-3–3, *Industrial communication networks – Fieldbus specifications – Part 3-3: Data-link layer service definition – Type 3 elements* (disponible uniquement en anglais)

IEC 61158-4–3, *Industrial communication networks – Fieldbus specifications – Part 4-3: Data-link layer protocol specification – Type 3 elements* (disponible uniquement en anglais)

IEC 61158-5–3, *Industrial communication networks – Fieldbus specifications – Part 5-3: Application layer service definition – Type 3 elements* (disponible uniquement en anglais)

IEC 61158-5–10, *Industrial communication networks – Fieldbus specifications – Part 5-10: Application layer service definition – Type 10 elements* (disponible uniquement en anglais)

IEC 61158-6–3, *Industrial communication networks – Fieldbus specifications – Part 6-3: Application layer protocol specification – Type 3 elements* (disponible uniquement en anglais)

IEC 61158-6–10, *Industrial communication networks – Fieldbus specifications – Part 6-10: Application layer protocol specification – Type 10 elements* (disponible uniquement en anglais)

CEI 61326-3-1, *Matériel électrique de mesure, de commande et de laboratoire – Exigences relatives à la CEM – Partie 3-1: Exigences d'immunité pour les systèmes relatifs à la sécurité et pour les matériels destinés à réaliser des fonctions relatives à la sécurité (sécurité fonctionnelle) – Applications industrielles générales*

CEI 61326-3-2, *Matériel électrique de mesure, de commande et de laboratoire – Exigences relatives à la CEM – Partie 3-2: Exigences d'immunité pour les systèmes relatifs à la sécurité et pour les matériels destinés à réaliser des fonctions relatives à la sécurité (sécurité fonctionnelle) – Applications industrielles dont l'environnement électromagnétique est spécifié*

CEI 61508 (toutes parties), *Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité*

CEI 61508-2, *Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité – Partie 2: Exigences pour les systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité*

CEI 61511 (toutes parties), *Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur des industries de transformation*

IEC 61784-1, *Industrial communication networks – Profiles – Part 1: Fieldbus profiles* (disponible uniquement en anglais)

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

IEC 61784-3:2010[4], *Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions* (disponible uniquement en anglais)

---

3 Les publications monolingues des séries IEC 61158 et IEC 61784 sont actuellement en cours de traduction.

4 En cours d'élaboration.

IEC 61784-5-3, *Industrial communication networks - Profiles – Part 5-3: Installation of fieldbuses – Installation profiles for CPF 3* (disponible uniquement en anglais)

IEC 61918, *Industrial communication networks – Installation of communication networks in industrial premises* (disponible uniquement en anglais)

CEI 62061, *Sécurité des machines – Sécurité fonctionnelle des systèmes de commande électriques, électroniques et électroniques programmables relatifs à la sécurité*

CEI 62280-1:2002, *Applications ferroviaires – Systèmes de signalisation, de télécommunication et de traitement – Partie 1: Communication de sécurité sur des systèmes de transmission fermés*

CEI 62280-2, *Applications ferroviaires – Systèmes de signalisation, de télécommunication et de traitement – Partie 2: Communication de sécurité sur des systèmes de transmission ouverts*

IEC/TR 62390, *Common automation device – Profile guideline* (disponible uniquement en anglais)

ISO 13849-1, *Sécurité des machines – Parties des systèmes de commande relatives à la sécurité – Partie 1: Principes généraux de conception*

ISO 13849-2, *Sécurité des machines – Parties des systèmes de commande relatifs à la sécurité – Partie 2: Validation*

ISO 15745-3, *Systèmes d'automatisation industrielle et intégration – Cadres d'intégration d'application pour les systèmes ouverts – Partie 3: Description de référence pour les systèmes de contrôle fondés sur la CEI 61158*

ISO 15745-4, *Systèmes d'automatisation industrielle et intégration – Cadres d'intégration d'application pour les systèmes ouverts – Partie 4: Description de référence pour les systèmes de contrôle fondés sur Ethernet*

3 Termes, définitions, symboles, abréviations et conventions

3.1 Termes et définitions

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

3.1.1 Termes et définitions communs

3.1.1.1
disponibilité
probabilité, pour un système automatisé, qu'il ne se produise pas de conditions opérationnelles non satisfaisantes, telles que la perte de production, pendant une période donnée

3.1.1.2
canal noir
canal de communication sans preuve existante de conception ou de validation conformément à la CEI 61508

3.1.1.3
canal de communication
connexion logique entre deux points limites d'un *système de communication*

3.1.1.4
système de communication
disposition de matériels, logiciels et vecteurs de propagation destinée à permettre la transmission de *messages* (couche d'application définie dans l'ISO/CEI 7498) d'une application à une autre

3.1.1.5
connexion
liaison logique entre deux objets d'application de dispositifs identiques ou différents

3.1.1.6
contrôle de redondance cyclique (CRC[5])
<valeur> donnée redondante déduite, et enregistrée ou transmise simultanément, d'un bloc de données afin de détecter toute corruption des données

<méthode> procédure utilisée pour calculer les données redondantes

NOTE 1 Les termes « code CRC » et « signature CRC », et les étiquettes telles que CRC1, CRC2, peuvent également être utilisés dans la présente norme pour se référer aux données redondantes.

NOTE 2 Voir également [32], [33]][6].

3.1.1.7
erreur
écart ou discordance entre une valeur ou une condition calculée, observée ou mesurée, et la valeur ou la condition vraie, prescrite ou théoriquement correcte

[CEI 61508-4:2010[7]], [CEI 61158]

NOTE 1 Les erreurs peuvent être causées par des erreurs de conception du matériel/logiciel et/ou des informations altérées du fait de perturbations électromagnétiques et/ou autres effets.

NOTE 2 Les erreurs ne produisent pas nécessairement une *défaillance* ou une *panne*.

3.1.1.8
défaillance
cessation de l'aptitude d'une unité fonctionnelle à accomplir une fonction requise ou fonctionnement d'une unité fonctionnelle d'une toute autre manière que celle requise

NOTE 1 La définition de la CEI 61508-4 est identique avec des notes complémentaires.

[CEI 61508-4:2010, modifiée], [ISO/CEI 2382-14.01.11, modifiée]

NOTE 2 Une défaillance peut être causée par une *erreur* (par exemple, problème de conception matérielle/logicielle ou rupture de message).

3.1.1.9
panne
condition anormale susceptible de provoquer la réduction ou la perte de la capacité d'une unité fonctionnelle à accomplir une fonction requise

NOTE Le VEI 191-05-01 définit la « panne » comme un état caractérisé par l'incapacité à accomplir une fonction requise, à l'exclusion de l'incapacité au cours de la période de maintenance préventive ou autres actions planifiées, ou du fait de l'absence de ressources externes.

[CEI 61508-4:2010, modifiée], [ISO/CEI 2382-14.01.10, modifiée]

---

5 CRC = *Cyclic Redundancy Check*

6 Les chiffres entre crochets font référence à la bibliographie.

7 A publier.

3.1.1.10
bus de terrain
système de communication basé sur le transfert de données en série et utilisé dans des applications d'automatisation industrielle ou de commande de processus

3.1.1.11
système de bus de terrain
système utilisant un *bus de terrain* avec des dispositifs connectés

3.1.1.12
trame
synonyme discrédité de DLPDU

3.1.1.13
séquence de contrôle de trame (FCS[8])
données redondantes issues d'un bloc de données d'un DLPDU (trame), utilisant une fonction de hachage, et enregistrées ou transmises avec le bloc de données, afin de déterminer l'altération des données

NOTE 1 Il est possible de calculer une FCS à l'aide, par exemple, d'un CRC ou d'une autre fonction de hachage.

NOTE 2 Voir également [32], [33].

3.1.1.14
fonction de hachage
fonction (mathématique) de mise en correspondance des valeurs d'un ensemble (éventuellement) très grand de valeurs en une plage de valeurs (habituellement) plus petite

NOTE 1 Les fonctions de hachage peuvent être utilisées pour déterminer l'altération des données.

NOTE 2 Les fonctions de hachage courantes incluent la parité, la somme de contrôle ou le CRC.

[CEI/TR 62210, modifiée]

3.1.1.15
danger
état ou ensemble de conditions d'un système qui, avec d'autres conditions associées, entraîne inévitablement un préjudice pour les personnes, les biens ou l'environnement

3.1.1.16
maître
entité de communication active capable d'initier et de programmer des activités de communication effectuées par d'autres stations qui peuvent être des maîtres ou des esclaves

3.1.1.17
message
série ordonnée d'octets destinée à communiquer des informations
[ISO/CEI 2382-16.02.01, modifiée]

3.1.1.18
déclenchement de nuisance
déclenchement parasite sans effet préjudiciable

NOTE Les erreurs anormales internes peuvent être générées dans des systèmes de communication tels que des systèmes de transmission par ondes radioélectriques, par exemple, du fait d'un trop grand nombre de nouvelles tentatives en présence de perturbations.

8 FCS = *Frame Check Sequence*

3.1.1.19
essai de validité
essai périodique destiné à détecter les défaillances d'un *système relatif à la sécurité* de telle sorte que, lorsque nécessaire, le système puisse être rétabli dans une condition "comme neuf'' ou dans une condition aussi proche que possible de celle-ci

NOTE Un essai de validité est destiné à confirmer que l'état du système relatif à la sécurité garantit l'intégrité de sécurité spécifiée.

[CEI 61508-4 et CEI 62061, modifiée]

3.1.1.20
niveau de performance (PL[9])
niveau discret utilisé pour spécifier la capacité des parties relatives à la sécurité des systèmes de commande à accomplir une fonction de sécurité dans des conditions prévisibles [ISO 13849-1]

3.1.1.21
très basse tension de protection (TBTP ou PELV)
circuit électrique dans lequel la tension ne peut pas dépasser 30 V efficace en c.a., 42,4 V crête ou 60 V en c.c. dans des conditions normales de premier défaut, à l'exception des défauts à la terre dans d'autres circuits

NOTE Un circuit TBTP est similaire à un circuit TBTS relié à la terre de protection.

[CEI 61131-2]

3.1.1.22
redondance
existence de moyens, outre les moyens qui se révèleraient suffisants pour qu'une unité fonctionnelle accomplisse une fonction requise ou que des données représentent une information

NOTE La définition de la CEI 61508-4 est identique, avec des exemples et des notes supplémentaires.

[CEI 61508-4:2010, modifiée], [ISO/CEI 2382-14.01.12, modifiée]

3.1.1.23
fiabilité
probabilité qu'un système automatisé puisse accomplir une fonction requise, dans des conditions données, pendant un intervalle de temps donné (t1, t2)

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

NOTE 2 Le terme "fiabilité" est aussi employé pour désigner l'aptitude caractérisée par cette probabilité.

NOTE 3 Au cours de la période MTBF ou MTTF, la probabilité qu'un système automatisé exécute une fonction requise dans les conditions données décroît.

NOTE 4 La fiabilité est différente de la disponibilité.

[CEI 62059-11, modifiée]

9 PL = *Performance Level*

3.1.1.24
risque
combinaison de la probabilité d'occurrence d'un dommage ou préjudice et de la gravité de ce dernier

NOTE Pour plus d'informations sur ce concept, se reporter à l'Annexe A de la CEI 61508-5:2010[10].

[CEI 61508-4:2010], [ISO/CEI Guide 51:1999, définition 3.2]

3.1.1.25
couche de communication de sécurité (SCL[11])
couche de communication qui comprend toutes les mesures nécessaires permettant d'assurer la transmission de données en toute sécurité conformément aux exigences de la CEI 61508

3.1.1.26
connexion de sécurité
connexion qui utilise le protocole de sécurité pour des transactions de communications

3.1.1.27
données de sécurité
données transmises par un réseau de sécurité utilisant un protocole de sécurité

NOTE La couche de communication de sécurité ne garantit pas la sécurité des données proprement dites, mais uniquement la transmission en toute sécurité de ces dernières.

3.1.1.28
dispositif de sécurité
dispositif conçu conformément à la CEI 61508 et qui met en œuvre le profil de communication de sécurité fonctionnelle

3.1.1.29
très basse tension de sécurité (TBTS ou SELV)
circuit électrique dans lequel la tension ne peut pas dépasser 30 V efficace en c.a., 42,4 V crête ou 60 V en c.c. dans des conditions normales de premier défaut, y compris les défauts à la terre dans les autres circuits

NOTE Un circuit TBTS n'est pas relié à la terre de protection.

[CEI 61131-2]

3.1.1.30
fonction de sécurité
fonction à réaliser par un système E/E/PE relatif à la sécurité ou par un dispositif externe de réduction de risque, prévue pour assurer ou maintenir un état de sécurité de l'EUC par rapport à un événement dangereux spécifique

NOTE La définition de la CEI 61508-4 est identique, avec un exemple et des références supplémentaires.

[CEI 61508-4:2210, modifiée]

3.1.1.31
temps de réponse de la fonction de sécurité (SFRT[12])
temps écoulé du cas le plus défavorable suite à l'activation d'un capteur de sécurité relié à un bus de terrain, avant que ne soit atteint l'état de sécurité correspondant de son (ses)

---

10 A publier.

11 SCL = *Safety Communication Layer*

12 SRFT = *Safety Function Response Time*

actionneur(s) de sécurité, du fait d'erreurs ou de défaillances avérées dans le canal de fonction de sécurité

NOTE Ce concept, introduit dans la CEI 61784-3:2010[13], 5.2.4, est traité par les profils de communication de sécurité fonctionnelle définis dans la présente partie.

3.1.1.32
niveau d'intégrité de sécurité (SIL[14])
niveau discret (un sur quatre niveaux possibles), correspondant à une plage de valeurs d'intégrité de sécurité, où le niveau d'intégrité de sécurité 4 est le niveau le plus élevé et le niveau d'intégrité de sécurité 1 est le niveau le plus faible

NOTE 1 Les mesures de défaillance cible (voir la CEI 61508-4:2010, 3.5.17) applicables aux quatre niveaux d'intégrité de sécurité sont spécifiées dans les Tableaux 2 et 3 de la CEI 61508-1:2010[15].

NOTE 2 Les niveaux d'intégrité de sécurité sont utilisés pour spécifier les exigences d'intégrité de sécurité des fonctions équivalentes à attribuer aux systèmes E/E/PE relatifs à la sécurité.

NOTE 3 Le niveau d'intégrité de sécurité (SIL) n'est pas une propriété d'un système, sous-système, élément ou composant. L'interprétation correcte de l'expression « système relatif à la sécurité avec SILn » (où n est égal à 1, 2, 3 ou 4) signifie que le système est potentiellement capable de prendre en charge des fonctions de sécurité avec un niveau d'intégrité de sécurité jusqu'à n.

[CEI 61508-4:2010]

3.1.1.33
mesure de sécurité
<la présente norme> mesure permettant de contrôler les *erreurs* de communication éventuelles, qui est conçue et mise en œuvre conformément aux exigences de la CEI 61508

NOTE 1 Dans la pratique, plusieurs mesures de sécurité sont combinées pour atteindre le niveau d'intégrité de sécurité requis.

NOTE 2 Les *erreurs* de communication et les mesures de sécurité associées sont détaillées dans la CEI 61784-3:2010, 5.3 et 5.4.

3.1.1.34
application relative à la sécurité
programmes conçus conformément à la CEI 61508 pour satisfaire aux exigences SIL de l'application

3.1.1.35
système relatif à la sécurité
système qui exécute les *fonctions de sécurité* conformément à la CEI 61508

3.1.1.36
esclave
entité de communication passive capable de recevoir des messages et de les envoyer en réponse à une autre entité de communication qui peut être maître ou esclave

3.1.1.37
déclenchement parasite
déclenchement provoqué par le système de sécurité sans sollicitation du processus

---

13 En cours d'élaboration.

14 SIL = *Safety Integrity Level*

15 A publier.

3.1.2 CPF 3: Termes et définitions supplémentaires

3.1.2.1
bit (chiffre binaire)
informations binaires codées sans unité technique

3.1.2.2
nom de code (*codename*)
identification unique entre des homologues de communication de sécurité

NOTE Instance d'*authentification de connexion* telle que présentée dans la CEI 61784-3.

3.1.2.3
configuration
définition des connexions et paramètres de communication standard des entités de bus d'une application particulière

NOTE La configuration d'une communication de sécurité comprend la définition des connexions de sécurité et des paramètres F des entités de bus relatives à la sécurité d'une application relative à la sécurité particulière.

3.1.2.4
numéro consécutif
moyen permettant de garantir l'exhaustivité et le bon ordre des PDU de sécurité transmis

NOTE 1 Instance de *numéro de séquence* telle que présentée dans la CEI 61784-3.

NOTE 2 Le numéro consécutif peut être transmis avec chaque PDU de sécurité (mode V1) ou peut être uniquement sécurisé grâce à la signature CRC transmise (mode V2).

3.1.2.5
outil CPD
dans les ordinateurs de service connectés au bus de terrain, programme dédié aux besoins de la configuration, du paramétrage et du diagnostic de dispositifs de terrain particuliers

3.1.2.6
cycle
intervalle d'exécution répétitive et continue d'une liste d'instructions ou d'une activité

3.1.2.7
point d'accès du dispositif (DAP[16])
élément permettant d'adresser un dispositif d'entrée-sortie modulaire comme une entité

NOTE En règle générale, il s'agit d'une station de tête.

3.1.2.8
temps d'acquittement du dispositif (DAT[17])
dans un dispositif F, temps écoulé entre la réception d'un PDU de sécurité avec un nouveau numéro consécutif dans le point d'accès du dispositif et la génération, puis le renvoi au point d'accès du dispositif, d'une réponse appropriée de PDU de sécurité

3.1.2.9
pilote
module logiciel permettant d'analyser le matériel en fonction de l'application logicielle restante

---

16 DAP = *Device Access Point*

17 DAT = *Device Acknowledgement Time*

3.1.2.10
à sécurité intégrée (F[18])
aptitude d'un système qui, grâce à des mesures techniques ou organisationnelles pertinentes, protège contre les dangers de manière déterministe ou en réduisant le risque à un niveau tolérable

3.1.2.11
valeurs Failsafe (FV[19]) (à sécurité intégrée)
valeurs remplaçant des valeurs de processus lorsque la fonction de sécurité est définie sur un état de sécurité intégrée

NOTE Dans la présente partie, les valeurs Failsafe (FV) doivent toujours être définies sur 0.

3.1.2.12
état de sécurité intégrée
mode opérationnel d'une fonction de sécurité ou d'un élément final (actionneur) qui, suite à des mesures techniques pertinentes, protège contre les dangers de manière déterministe ou en réduisant le risque à un niveau tolérable

NOTE Selon la fonction de sécurité particulière, la mise hors tension peut ne pas être la seule possibilité caractérisant un état de sécurité intégrée.

3.1.2.13
dispositif F
homologue de communication CP 3/RTE passive permettant d'exécuter le protocole FSCP 3/1, en principe déclenché par l'hôte F pour l'échange de données

3.1.2.14
pilote F
logiciel assurant la gestion des PDU de sécurité à l'intérieur des hôtes F et des dispositifs F conformément aux spécifications FSCP 3/1

3.1.2.15
hôte F
unité de traitement de données permettant d'exécuter le protocole FSCP 3/1 et d'entretenir le canal noir

NOTE En règle générale, il s'agit d'un PLC ou d'un IPC doté d'un système d'exploitation adéquat.

3.1.2.16
module F
dans un dispositif F ou esclave F modulaire, homologue de communication passive permettant d'exécuter le protocole FSCP 3/1, en principe déclenché par l'hôte F pour l'échange de données

NOTE Il s'agit en général d'un module d'entrée ou de sortie relatif à la sécurité.

3.1.2.17
esclave F
homologue de communication CP 3/1 ou CP 3/2 passive permettant d'exécuter le protocole FSCP 3/1, en principe déclenché par l'hôte F pour l'échange de données

3.1.2.18
réaction aux anomalies
indication d'un dysfonctionnement de communication en définissant les bits erronés dans les octets d'état et une réaction sécurisée automatique correspondante à l'intérieur des composants

---

18 F = *Fail-Safe*

19 FV = *Fail-Safe Values*

NOTE

Dans une sortie F:	Arrêt des sorties et/ou réaction sécurisée automatique de l'actionneur.
Dans le CPU F:	Réaction possible du programme utilisateur correspondant. Attribuer des valeurs Failsafe aux données d'entrée-sortie F.
Dans une entrée F:	Lors de la communication, défauts détectés à partir de l'entrée F: Bits erronés définis dans l'octet d'état. Lors de la communication, défauts détectés à partir de l'hôte F: Attribuer des valeurs Failsafe aux données d'entrée F.

3.1.2.19
bloc de fonctions (FB[20])
partie intégrée d'un programme permettant de traiter une fonctionnalité spécifique

3.1.2.20
temps d'acquittement de l'hôte (HAT[21])
dans un hôte F, temps écoulé entre la réception d'un PDU de sécurité avec une certaine numérotation consécutive et la génération, puis le renvoi au maître/contrôleur d'entrée-sortie, d'un PDU de sécurité approprié doté d'un numéro consécutif incrémenté

3.1.2.21
contrôleur d'entrée-sortie
entité de communication active permettant à d'autres entités (des contrôleurs ou dispositifs d'entrée-sortie, par exemple) d'initier et de planifier des activités de communication CP 3/RTE

NOTE Dans CP 3/1, cette tâche correspond à une classe maître 1.

3.1.2.22
dispositif d'entrée-sortie
entité de communication passive permettant de recevoir des messages et de les envoyer en réponse à une autre entité de communication CP 3/RTE (un contrôleur d'entrée-sortie ou d'autres dispositifs d'entrée-sortie, par exemple)

NOTE Dans CP 3/1, cette tâche correspond à un esclave.

3.1.2.23
module d'entrée-sortie
sous-unité adressable d'entrée-sortie à l'intérieur d'un dispositif d'entrée-sortie modulaire

3.1.2.24
superviseur d'entrée-sortie
station d'ingénierie permettant de lire et d'écrire des données sur un dispositif d'entrée-sortie

NOTE Il est utilisé pour la mise en service et le diagnostic. A l'inverse d'un contrôleur d'entrée-sortie, il ne remplit pas un rôle actif lors de l'amorçage d'un système d'entrée-sortie. Un superviseur d'entrée-sortie ne fait pas partie intégrante du système d'entrée-sortie.

3.1.2.25
système d'entrée-sortie
contrôleur d'entrée-sortie et ses dispositifs d'entrée sortie associés

3.1.2.26
iParamètre
paramètres de dispositif F individuels ou spécifiques à la technologie

NOTE Les coordonnées de la zone de protection d'un lecteur laser sont des iParamètres classiques.

---

20 FB = *Function Block*

21 HAT = *Host Acknowledgement Time*

3.1.2.27
serveur d'iParamètres
mécanisme normalisé permettant de stocker et d'extraire des paramètres de dispositif F individuels ou spécifiques à la technologie dans la partie standard d'un hôte F ou de son sous-système contrôlé

3.1.2.28
maître (classe 1)
homologue de communication CP 3/1 actif déclenchant des esclaves pour l'échange de données

3.1.2.29
valeurs de processus (PV[22])
données d'entrée et de sortie (d'un PDU de sécurité) nécessaires au contrôle d'un processus automatisé

3.1.2.30
qualificatif
bits de qualification supplémentaires dans les *valeurs de processus*, indiquant l'état de chaque entrée individuelle

3.1.2.31
entrée-sortie partagée
entrées et sorties dans les dispositifs de terrain auxquelles plusieurs contrôleurs peuvent accéder

NOTE Même si CP 3/RTE admet l'entrée-sortie partagée, elle ne l'est pas avec FSCP 3/1.

3.1.2.32
bit de basculement
bit de l'octet de contrôle et d'état permettant de synchroniser les compteurs consécutifs (virtuels) dans l'hôte F et le dispositif F

3.1.2.33
bus série universel (USB[23])
norme de bus externe prenant en charge des vitesses de transfert de données allant jusqu'à 480 Mbit/s

NOTE USB remplace les ports série et parallèle. Il permet d'assurer une connexion directe et rapide entre les ordinateurs de service et les dispositifs de terrain.

3.1.2.34
mode V1
services et protocole FSCP 3/1 conformément à [48]]

3.1.2.35
mode V2
services et protocole FSCP 3/1 conformément à la présente partie

3.1.2.36
drapeau VLAN
dans les messages Ethernet, extension permettant à des groupes d'utilisateurs particuliers de réseaux volumineux d'exécuter leur propre réseau virtuel grâce à des priorités et des ID VLAN, en utilisant des commutateurs appropriés, et sans influencer les autres groupes, et inversement

22 PV = *Process Values*

23 USB = *Universal Serial Bus*

3.2 Symboles et abréviations

3.2.1 Symboles et abréviations communs

CP	Profil de communication (communication profile)	[CEI 61784-1]
CPF	Famille de profils de communication (*Communication Profile Family)*	[CEI 61784-1]
CRC	Contrôle de redondance cyclique (*Cyclic Redundancy Check)*	
DLL	Couche de liaison de données (	[ISO/CEI 7498-1]
DLPDU	Ensemble (unité) de données de protocole de liaison de données (*Data Link Protocol Data Unit)*	
CEM	Compatibilité électromagnétique	
EMI	Perturbation électromagnétique (	
EUC	Equipement commandé (*Equipment Under Control)*	[CEI 61508-4:2010]
E/E/PE	Électrique/électronique/électronique programmable (	[CEI 61508-4:2010]
FAL	Couche Application de bus de terrain (*Fieldbus Application Layer*)	[CEI 61158-5]
FCS	Séquence de contrôle de trame (*Frame Check Sequence)*	
FS	Sécurité fonctionnelle (*Functional Safety)*	
FSCP	Profil de communication de sécurité fonctionnelle (*Functional Safety Communication Profile)*	
HD	Distance de Hamming (*Hamming Distance*)	
MTBF	Moyenne des temps de bon fonctionnement entre défaillances (*Mean Time Between Failures*)	
MTTF	Durée moyenne de fonctionnement avant défaillance (*Mean Time To Failure*)	
PDU	Ensemble (Unité) de données de protocole (*Protocol Data Unit*)	[ISO/CEI 7498-1]
TBTP ou PELV	Très basse tension de protection	
PFD	Probabilité de défaillance dangereuse sur sollicitation (*Probability of dangerous Failure on Demand*)	[CEI 61508-6:2010[24]]
PFH	Fréquence moyenne de défaillance dangereuse [h^{-1}] par heure	[CEI 61508-6:2010]
PhL	Couche physique (*Physical Layer*)	[ISO/CEI 7498-1]
PL	Niveau de performance (*Performance Level*)	[ISO 13849-1]
PLC	Automate programmable (*Programmable Logic Controller*)	
SCL	Couche de communication de sécurité (*Safety Communication Layer*)	
TBTS ou SELV	Très basse tension de sécurité	
SFRT	Temps de réponse de la fonction de sécurité (*Safety Function Response Time*)	
SIL	Niveau d'intégrité de sécurité (*Safety Integrity Level*)	[CEI 61508-4:2010]

3.2.2 CPF 3: Symboles et abréviations supplémentaires

AES-CCMP	Advanced Encryption Standard - Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
AP	Processus d'Application (
API	Identifiant de processus d'application (*Application Process Identifier*)
AR	Relation d'application (*Application Relationship*)
ASE	Élément de service d'application (*Application Service Element*)
ASIC	Circuit intégré à application spécifique (*Application Specific Integrated Circuit*)

24 A publier.

C	Couverture	
CP 3/1	Profil de communication communément appelé PROFIBUS DP[25]	
CP 3/2	Profil de communication communément appelé PROFIBUS PA	
CP 3/RTE	Profil de communication communément appelé PROFINET IO	
CPU	Unité centrale (*Central Processing Unit*)	
CR	Relation de communication (*Communication Relationship*)	
DAP	Point d'accès au dispositif (*Device Access Point*)	
DAT	Temps d'acquittement du dispositif (*Device Acknowledgement Time*)	
DP	Périphériques décentralisés (*Decentralized Peripherals*)	
F	Identifiant des éléments sécurisés (à sécurité intégrée, sécurité fonctionnelle)	
FB	Bloc de fonctions (*Function Block*)	
FV	Valeurs Failsafe (*Fail-safe Values*)	
GSD	Description générale de station (fichier associé au dispositif)	
GSDL	Langage de description générale de station (pour les dispositifs CP 3/1 et CP 3/2)	
GSDML	General Station Description Markup Language (pour les dispositifs CP 3/RTE)	
HAT	Temps d'acquittement de l'hôte (*Host Acknowledgement Time*)	
E-S	Entrée-sortie	
DEL	Diode Electroluminescente	
PA	Automatisme industriel (*Process Automation*)	
PN IO	PROFINET IO = CP 3/4 à 3/6	
PSK	Clé préalablement partagée (*Pre-Shared Key*)	
PV	Valeurs de processus (*Process Values*)	
RADIUS	Remote Authentication Dial In User Service	
S	Standard	
SR	Relatif à la sécurité (fonctionnelle)	
SSID	Identifiant d'ensemble de service (Service Set Identifier)	
UML	Langage de modélisation unifié (*Unified Modeling Language*)	[57]
USB	Bus de série universel (*Universal Serial Bus*)	[62]
VLAN	Réseau local virtuel (*Virtual Local Area Network*)	
WCDT	Délai du cas le moins favorable (*Worst Case Delay Time*)	
WDTime	Temps de fonctionnement du chien de garde (*Watchdog Time*)	
WPA2	Accès Wi-Fi protégé 2 (*Wi-Fi Protected Access 2*)	[26]
XML	eXtensible Markup Language	[59], [60], [61]

3.3 Conventions

La présente partie utilise la notation UML2 pour le tracé des diagrammes d'état et une forme condensée de diagrammes d'état [57]. Les tableaux de transition sont présentés conformément aux recommandations de la CEI 62390.

Dans la présente partie, l'abréviation F se rapporte aux éléments, technologies, systèmes et unités relatifs à la sécurité (à sécurité intégrée, sécurité fonctionnelle).

Les données par défaut qui doivent être envoyées en cas de défaillance du système ou d'erreurs sont appelées valeurs Failsafe (FV) et leur valeur est nulle (0).

---

[25] Pour les déclarations d'appellation commerciale, voir l'article 4.

Le calcul de la signature CRC ayant pour résultat une valeur 0 utilise la valeur 1 à la place.

L'abréviation CP 3/RTE comprend les trois profils de communication CP 3/4, CP 3/5 et CP 3/6. CP 3/RTE est communément appelé PROFINET IO.

4 Vue d'ensemble de FSCP 3/1 (PROFIsafe™)

La famille de profils de communication 3 (communément appelée PROFIBUS™, PROFINET™[26]) définit des profils de communication sur la base du type 3 de la CEI 61158-2, de la CEI 61158-3-3, la CEI 61158-4-3, la CEI 61158-5-3, la CEI 61158-5-10, la CEI 61158-6-3 et la CEI 61158-6-10.

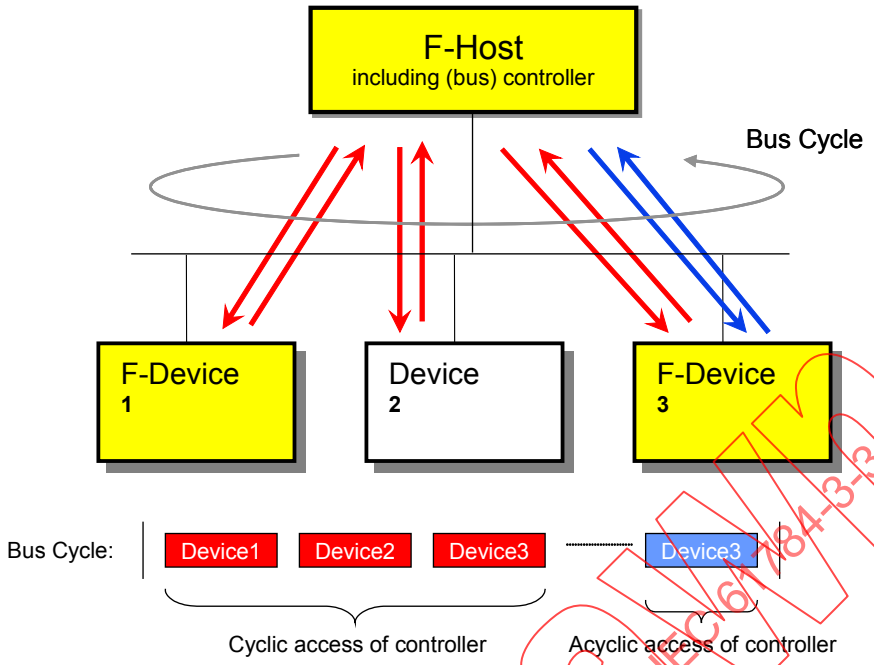
Les profils de base CP 3/1 et CP 3/2 sont définis dans la CEI 61784-1; CP 3/4, CP 3/5 et CP 3/6 sont définis dans la CEI 61784-2. Le profil de communication de sécurité fonctionnelle CPF 3 FSCP 3/1 (PROFIsafe™[26]) est fondé sur les profils de base CPF 3 définis dans la CEI 61784-1 et la CEI 61784-2, ainsi que les spécifications de la couche de communication de sécurité définies dans la présente partie.

Le FSCP 3/1 est basé sur l'échange de données cycliques d'un contrôleur (de bus) avec ses dispositifs (de terrain) associés grâce à une relation de communication un-un (Figure 3). Un contrôleur peut utiliser toute combinaison de dispositifs standards et de sécurité reliés au réseau. Il est également possible d'affecter des tâches de sécurité et normales à différents contrôleurs. Les communications dites acycliques entre les dispositifs et les contrôleurs ou les superviseurs tels que les dispositifs de programmation, sont prévues à des fins de configuration, paramétrage, diagnostic et maintenance.

Les quatre mesures suivantes ont été retenues pour réaliser le protocole FSCP 3/1:

— numérotation consécutive (virtuelle);
— contrôle du temps de fonctionnement du chien de garde avec acquittement;
— nom de code par relation de communication;
— contrôle de redondance cyclique pour l'intégrité des données.

26 PROFIBUS™, PROFINET™ et PROFIsafe™ désignent les appellations commerciales de l'organisme sans but lucratif PROFIBUS Nutzerorganisation e.V. (PNO). Ces informations sont données à l'intention des utilisateurs de la présente Norme internationale et ne signifient nullement que la CEI approuve ou recommande le détenteur de la marque ou de l'un quelconque de ses produits. La conformité à la présente norme n'exige pas l'emploi des logos déposés pour PROFIBUS™, PROFINET™ ou PROFIsafe™. L'emploi des logos déposés pour PROFIBUS™, PROFINET™ ou PROFIsafe™ exige l'autorisation de PNO.

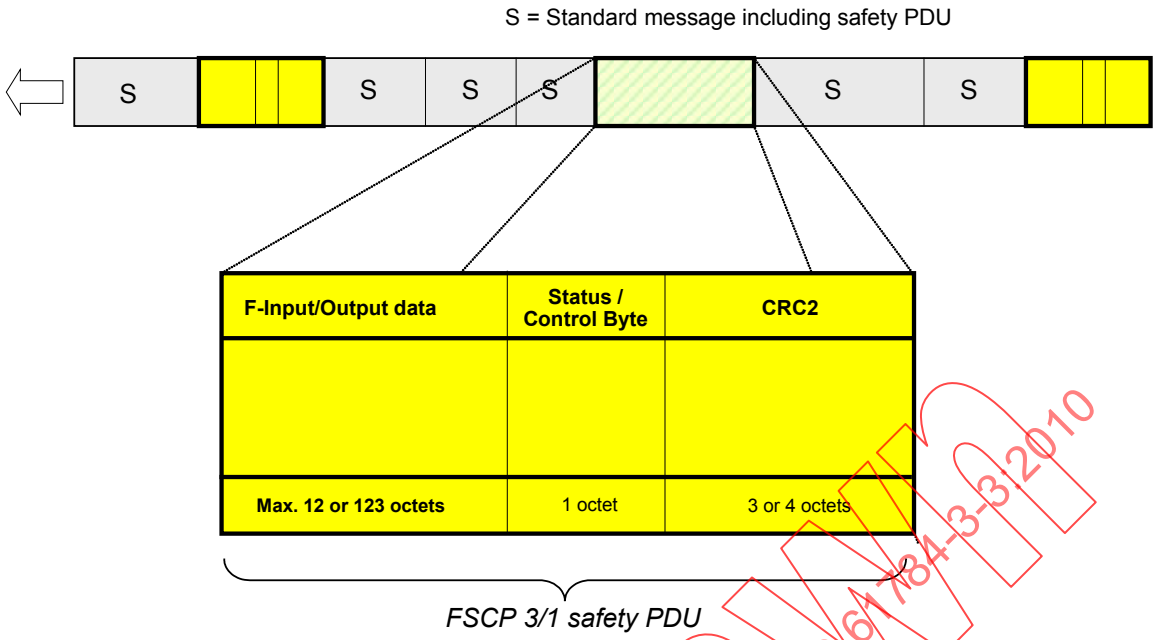


Légende

Anglais	Français
F-Host	Hôte F
Including (bus) controller	Y compris le contrôleur (bu)
Bus cycle	Cycle de bus
F-device	Dispositif F
Device	Dispositif
Cyclic access of controller	Accès cyclique du contrôleur
Acyclic access of controller	Accès acyclique du contrôleur

Figure 3 – Conditions préalables de communication de base pour le protocole FSCP 3/1

La numérotation consécutive utilise une plage suffisamment grande pour sécuriser tout dysfonctionnement provoqué par les éléments de réseau de stockage des messages. Chaque dispositif de sécurité renvoie un message contenant un PDU de sécurité pour acquittement, y compris en l'absence de données de processus. Un temporisateur séparé placé à la fois du côté émetteur et récepteur est utilisé pour chaque relation de communication un-un. Le nom de code unique par relation de communication est établi pour des raisons d'authentification, son codage étant constitué d'une valeur de signature CRC initiale pour la signature CRC2 à calcul et à transmission cyclique (Figure 4).



Légende

Anglais	Français
S = Standard message including safety PDU	S = Message standard incluant le PDU de sécurité
F-Input/Output data	Données d'entrée/sortie F
Status/Control Byte	Octet d'état/de contrôle
Max. 12 or 123 octets	12 ou 123 octets max.
3 or 4 octets	3 ou 4 octets
FSCP 3/1 safety PDU	PDU de sécurité FSCP 3/1

Figure 4 – Structure d'un PDU de sécurité FSCP 3/1

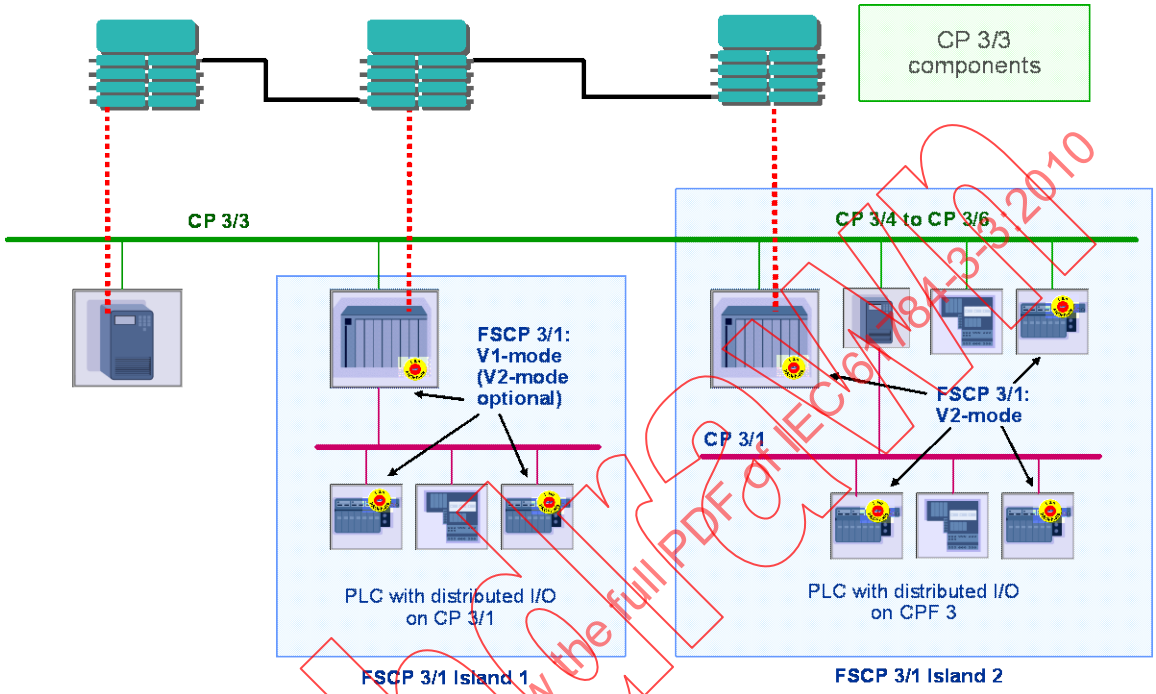
Le FSCP 3/1 fournit deux modes de fonctionnement: les modes V1 et V2. Alors que les mesures du mode V1 permettent une transmission des données en toute sécurité sur des réseaux CP 3/1 véritables, les caractéristiques les plus « généreuses » de Ethernet / CP 3/RTE, telles qu'un plus large espace d'adressage et des composantes de commutation de mise en mémoire tampon, exigent certaines extensions au protocole FSCP 3/1, conduisant ainsi au mode V2. Le mode V1 est limité au CP 3/1, tandis que le mode V2 est requis pour les protocoles CP 3/4 à C/P 3/6 et/ou CP 3/1. La présente partie décrit uniquement les détails de la fonctionnalité étendue du mode dit V2. Une communication de sécurité entre les composantes PROFINET CBA (voir CP 3/3) n'est pas encore définie. La Figure 5 présente FSCP 3/1 dans le cadre d'architectures CP 3/1 et CP 3/RTE.

Les solutions d'automatisation à entrée-sortie distribuée ayant largement fait l'unanimité grâce à PROFIBUS (CP 3/1 et CP 3/2) et PROFINET basé sur Ethernet pour les réseaux industriels (CP 3/RTE), les applications de sécurité reposent toujours sur une deuxième couche de techniques électriques conventionnelles ou de bus spéciaux, ce qui limite l'ingénierie et l'interopérabilité continues. De plus, il n'a pas été possible d'encourager l'utilisation de dispositifs de sécurité modernes (les lecteurs laser ou les dispositifs à sécurité intégrée, par exemple) compte tenu du manque de prise en charge du système. La présente partie et les documents connexes ont pour objet de fournir les technologies génériques correspondantes.

Après cette introduction, les paragraphes 5.1 et 5.2 reprennent respectivement des références supplémentaires pour le développement de la technologie FSCP 3/1 et ses exigences fonctionnelles. Les quatre mesures de sécurité de FSCP 3/1 figurent en 5.3. Les topologies de réseau de CP 3/RTE et leurs mises en correspondance avec CP 3/1 et CP 3/2

sont mentionnées en 5.4. Une brève introduction des relations de communication et des objets de la norme relative au bus de terrain est ensuite présentée en 5.5.

Pour des raisons de sécurité et d'efficacité, la liste des types de données de bus de terrain possibles est limitée à un ensemble concis présenté 5.5.4. Les paragraphes 6.1 à 6.3 dévoilent les services de l'hôte F et du dispositif F, ainsi que les messages de diagnostic possibles de la couche de sécurité.



Légende

Anglais	Français
CP 3/3 components	Composants CP 3/3
CP 3/4 to CP 3/6	CP 3/4 à CP 3/6
FSCP 3/1: V1-mode (V2-mode optional)	FSCP 3/1: mode V1 (mode V2 facultatif)
FSCP 3/1: V2-mode	FSCP 3/1: mode V2
PLC with distributed I/O on CP 3/1	PLC avec entrée-sortie distribuée sur CP 3/1
PLC with distributed I/O on CPF 3	PLC avec entrée-sortie distribuée sur CPF 3

Figure 5 – Modes de communication de sécurité

L'Article 7 commence par une présentation du PDU de sécurité (7.1) et se poursuit par une description des diagrammes d'état de l'hôte F et du dispositif F et des diagrammes séquentiels au format UML 2 (7.2.2 à 7.2.4). Les contraintes de temporisation associées sont présentées en 7.2.5 et 7.2.6. Conformément au format de l'Annexe D de la CEI 61784-3:2010, le paragraphe 7.3 illustre les réactions du système en cas d'éventuels dysfonctionnements. D'autres fonctions du système (le démarrage de la couche de sécurité, par exemple) sont présentées en 7.4. La gestion de la couche des dispositifs de sécurité se concentre sur les paramètres F spécifiques à la communication de sécurité (B.1) et les iParamètres individuels spécifiques au dispositif (8.2). Les exigences de traitement et de fourniture des paramètres F sont présentées en 8.3. Le paragraphe 8.4 aborde la sécurisation des structures de données échangées entre les partenaires qui communiquent et entrant dans la configuration d'un dispositif. Le paragraphe 8.5 explique comment utiliser les informations de structure de données pour configurer les pilotes de canal F de dispositifs F plus complexes afin de limiter les efforts de programmation. Les exigences d'intégration de systèmes des moyens et outils de iParamétrage figurent en 8.6. Les aspects liés aux temps de réponse, aux lignes

directrices d'installation, à la durée des sollicitations, à la maintenance, au manuel de sécurité, à la transmission sans fil et aux classes de conformité de l'hôte F sont présentés en à l'Article 9. Le raisonnement d'évaluation est présenté en 10.1 et les détails en 10.2. Une annexe informative contient des exemples de calculs de signature CRC rapides et une bibliographie. Deux lignes directrices FSCP 3/1 supplémentaires relatives à la sécurité électrique et à l'évaluation doivent être respectées ([44], [45]).

5 Généralités

5.1 Documents externes de spécifications applicables au profil

Outre les références normatives de l'Article 2, la technologie présentée dans cette partie a été approuvée conformément au GS-ET-26 [31].

FSCP 3/1 satisfait aux exigences de NE97 [59].

5.2 Exigences fonctionnelles de sécurité

Les exigences suivantes s'appliquent au développement de la technologie FSCP 3/1.

a) La communication de sécurité et la communication standard doivent être indépendantes. Toutefois, les dispositifs standards et les dispositifs de sécurité doivent être en mesure d'utiliser le même canal de communication.

b) La communication de sécurité doit être conforme au Niveau d'intégrité de sécurité SIL3 (voir la CEI 61508), à la catégorie de contrôle 4 (voir l'EN 954-1 [25]) et au niveau PL e (voir l'ISO 13849-1).

c) La communication de sécurité doit utiliser un système de communication à un seul canal. La redondance peut uniquement être utilisée pour éventuellement augmenter la disponibilité.

d) La mise en œuvre du protocole de transmission de sécurité doit être limitée aux dispositifs d'extrémité de communication (hôte F ou CPU F – dispositif F et/ou module d'entrée-sortie F).

e) La relation de communication entre un dispositif F et son hôte F doit toujours être de type 1:1.

f) Les durées de transmission doivent être surveillées.

g) Les conditions environnementales doivent être conformes aux exigences générales d'automatisation (principalement la CEI 61326-3-1 et la CEI 61326-3-2 en l'absence de normes de produits particulières).

h) Les équipements de transmission (les contrôleurs, les ASIC, les liaisons, les coupleurs, etc.) ne doivent pas être modifiés (canal noir). Les fonctions de sécurité doivent être au-dessus de la couche OSI 7 (c'est-à-dire le profil, et pas de modifications ni d'améliorations apportées au protocole standard)

i) La communication de sécurité ne doit pas réduire le nombre de dispositifs admis. Des restrictions peuvent apparaître pendant la mise en correspondance, dans le cas des applications CP 3/2, en raison des limitations de messages (voir CP 3/2 dans la CEI 61784-1).

j) La communication de sécurité doit être conforme à NE97 [58] et répondre aux exigences de la CEI 61784-3:2010, Annexe D.

5.3 Mesures de sécurité

Les mesures de sécurité mentionnées dans le Tableau 1 pour la maîtrise des erreurs de transmission possibles sont un composant significatif du profil FSCP 3/1. La sélection dans le Tableau 1 des mesures de sécurité génériques figurant dans la CEI 61784-3:2010, 5.5 est requise pour FSCP 3/1.

Les mesures de sécurité doivent être traitées et surveillées dans une unité de sécurité.

Tableau 1 – Mesurées déployées pour maîtriser les erreurs

Erreurs de communication	Mesures de sécurité			
	numéro consécutif (virtuel) [a]	Délai avec réception [b]	Nom de code de l'émetteur et du récepteur [c]	Contrôle de cohérence des données [d]
Corruption				X
Répétition non prévue	X			
Séquence incorrecte	X			
Perte	X	X		
Retard inacceptable		X		
Insertion	X	X	X	
Déguisement		X	X	X
Adressage			X	
Résolution de défaillance mémoire dans les commutateurs	X			

[a] Instance de « numéro de séquence » de la CEI 61784-3.

[b] Instance de « délai » et de « message de réaction » de la CEI 61784-3.

[a] Instance de « authentification de connexion » de la CEI 61784-3.

[d] Instance de « assurance d'intégrité des données » de la CEI 61784-3.

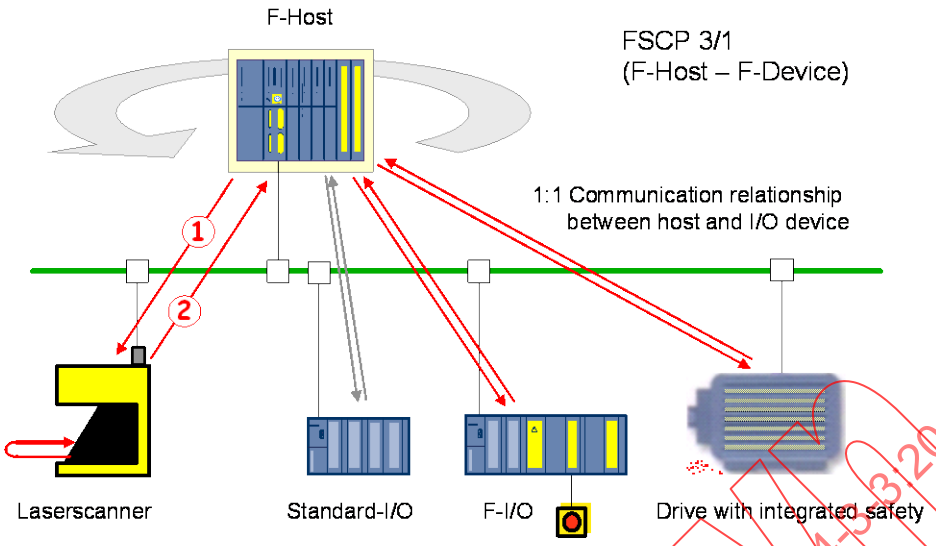
5.4 Structure de la couche de communication de sécurité

5.4.1 Principe des communications de sécurité FSCP 3/1

La communication de sécurité FSCP 3/1 repose sur l'expérience en matière de technique de signalisation ferroviaire, présentée dans la CEI 62280-1 et la CEI 62280-2.

Sur cette base, la communication de sécurité est assurée par

- un système de transmission standard (Figure 6), et
- un protocole de transmission de sécurité supplémentaire venant à l'appui de ce système de transmission standard.



Légende

Anglais	Français
(F-Host - F-Device)	(Hôte F - Dispositif F)
1:1 Communication relationship between host and I/O device	Relation de communication 1:1 entre l'hôte et le dispositif d'entrée-sortie
Laser scanner	Lecteur laser
Standard-I/O	Entrée-sortie standard
F-I/O	Entrée-sortie F
Drive with integrated safety	Unité avec sécurité intégrée
F-Host	Hôte F

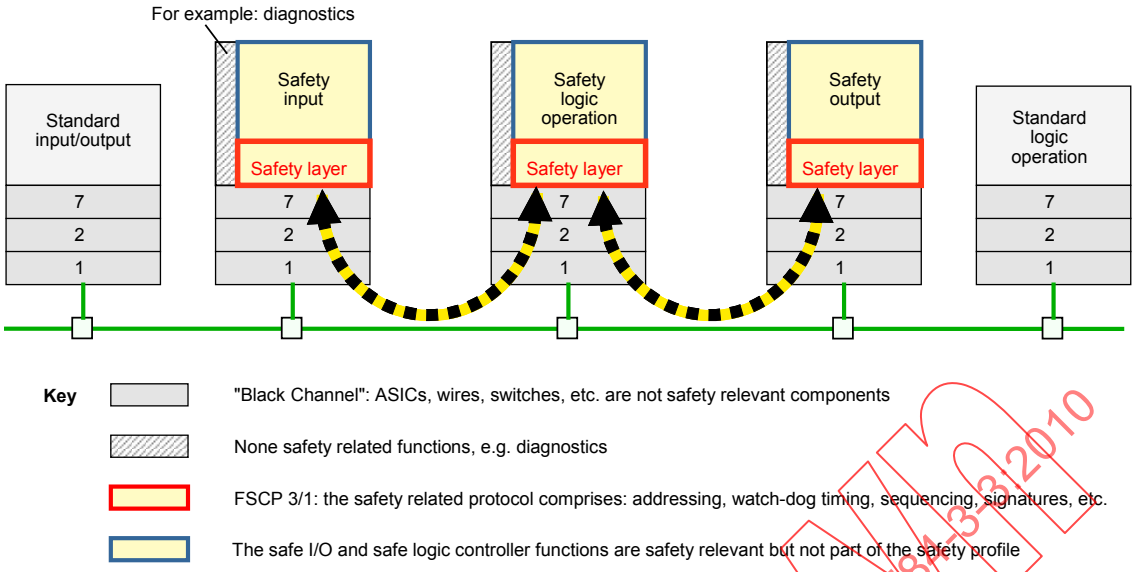
Figure 6 – Système de transmission CPF 3 standard

Le système de transmission standard est composé de l'ensemble du matériel de transmission et des fonctions de protocoles associées (c'est-à-dire les couches OSI 1, 2 et 7 conformément à la Figure 7).

Les applications de sécurité et applications standard partagent simultanément les mêmes systèmes de communication CPF 3 standard. La fonction de transmission sécurisée comprend toutes les mesures de détection déterministe de toutes les pannes/tous les dangers potentiels que le système de transmission standard est susceptible d'infiltrer, ou de maintien de la probabilité d'erreur (anomalie) résiduelle sous une certaine limite. Il s'agit

- de dysfonctionnements aléatoires (en raison, par exemple, de l'impact de l'EMI sur le canal de transmission)
- des défaillances/anomalies du matériel standard
- de dysfonctionnements systématiques des composants dans le matériel et le logiciel standard

Ce principe permet de limiter l'effort d'évaluation aux « fonctions de transmission sécurisée ». Il n'est pas utile de procéder à une évaluation supplémentaire du « système de transmission standard » (canal noir).



Légende

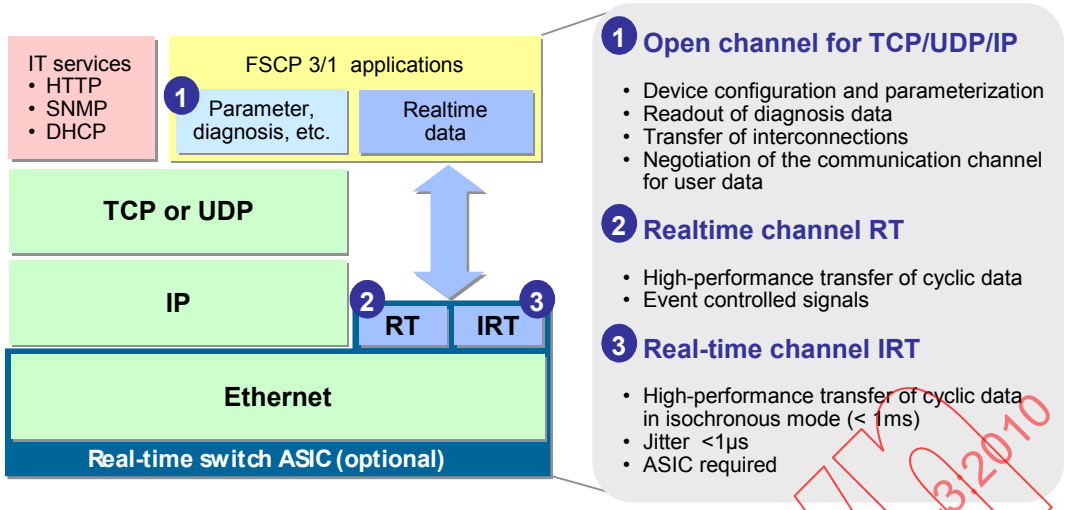
Anglais	Français
For example: diagnosis	Par exemple: diagnostic
Standard input/output	Entrée-sortie standard
Safety input	Entrée de sécurité
Safety layer	Couche de sécurité
Safety logic operation	Opération logique de sécurité
Safety output	Sortie de sécurité
Standard logic operation	Opération logique standard
Key	Légende
"Black Channel": ASICs, wires, switches, etc. are not safety relevant components	"Canal noir": ASIC, fils, commutateurs, etc. ne sont pas des composants relatifs à la sécurité
None safety functions, e.g. diagnosis	Aucune fonction de sécurité (diagnostic, par exemple)
FSCP 3/1: le safety related protocol comprises: addressing, watch-dog timing, sequencing, signatures, etc.	FSCP 3/1: le protocole de sécurité comprend l'adressage, le temps de fonctionnement du chien de garde, le séquencement, les signatures, etc.
The safe I/O and safe logic controller functions are safety relevant but not part of the safety profile	L'entrée-sortie de sécurité et les fonctions du contrôleur logique de sécurité sont adaptées, mais ne font pas partie du profil de sécurité

Figure 7 – Architecture de la couche de sécurité

La transmission est assurée par des conducteurs électriques ou optiques. Les topologies et fonctions de transmission admises du système de transmission standard et les composants du « Canal noir » sont présentés en 5.4.2.

5.4.2 Structures de communication CPF 3

Les couches de communication de base de CP 3/RTE sont présentées dans la Figure 8. Alors que la communication de sécurité cyclique de FSCP 3/1 utilise les canaux en temps réel RT ou IRT (CP 3/RTE de la CEI 61784-2), les autres services utilisent le canal dit ouvert via TCP/IP ou UDP.

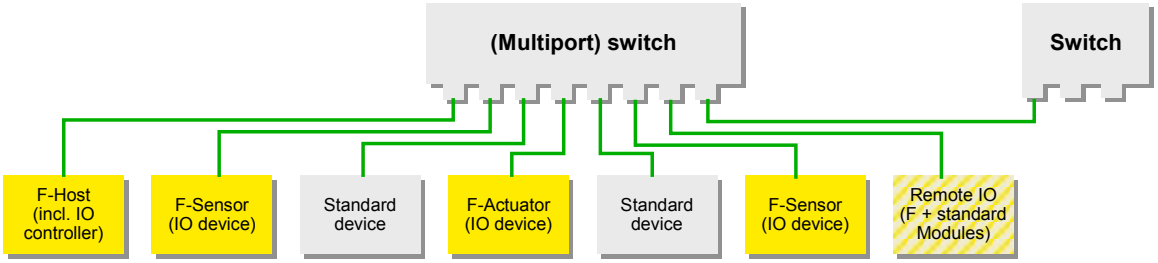


Légende

Anglais	Français
IT services	Service IT
FSCP 3/1 applications	Applications FSCO 3/1
Parameter, diagnosis, etc.	Paramètre, diagnostic, etc.
Realtime data	Données en temps réel
Open channel for TCP/UDP/IP	Canal ouvert pour TCP/UDP/IP
Device configuration and parameterization	Configuration et paramétrage du dispositif
Readout of diagnosis data	Lecture des données de diagnostic
Transfer of interconnections	Transfert des interconnexions
Negotiation of the communication channel for user data	Négociation du canal de communication pour les données utilisateur
Realtime channel RT	Canal RT en temps réel
High-performance transfer of cyclic data	Transfert haute performance des données cycliques
Event controlled signals	Signaux contrôlés par les événements
Real-time channel IRT	Canal IRT en temps réel
High-performance transfer of cyclic data in isochronous mode	Transfert haute performance des données cycliques en mode isochrone
Jitter	Gigue
ASIC required	ASIC requis

Figure 8 – Couches de communication de base

La Figure 9 illustre la topologie (en étoile) classique d'un câblage CP 3/RTE possible, des commutateurs à plusieurs ports faisant office de concentrateurs. Si un dispositif tombe en panne, tout le système n'est pas arrêté. Toutefois, l'effort de câblage peut ne pas être favorable.



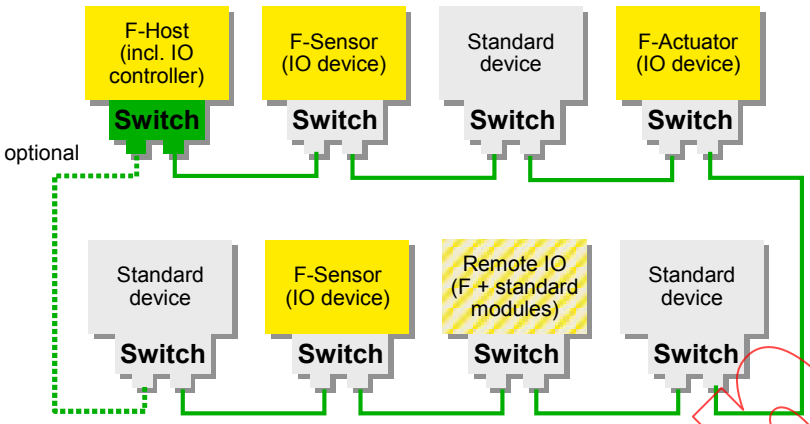
Légende

Anglais	Français
(Multiport) switch	Commutateur (à plusieurs ports)
Switch	Commutateur
F-Host (incl. IO controller)	Hôte F (y compris contrôleur d'entrée-sortie)
F-sensor (IO device)	Capteur F (dispositif d'entrée-sortie)
Standard device	Dispositif standard
F-Actuator (IO device)	Actionneur F (dispositif d'entrée-sortie)
Remote IO (F + standard Modules)	Entrée-sortie distante (F + Modules standard)

Figure 9 – Structure de bus de commutateur à plusieurs ports

CP 3/RTE offre une alternative grâce à Switch-ASIC, que chaque dispositif peut intégrer dans son interface de communication. De cette façon, une topologie linéaire s'apparentant à CP 3/1 est possible. Pour éviter l'arrêt du système en cas de panne d'un dispositif, une structure en anneau (Figure 10) est vivement recommandée. Toutefois, dans ce cas, il existe certaines restrictions:

- Au moins un participant de l'anneau (l'hôte F dans la Figure 10) doit disposer d'une fonction de gestion de redondance afin de détecter toutes les interruptions et réorganiser la transmission vers les destinations.
- Dans ce cas, le temps de passage sur canal sémaphore de secours de la gestion du commutateur ne doit pas dépasser le temps minimal de fonctionnement du chien de garde d'un dispositif F se trouvant dans le même îlot.



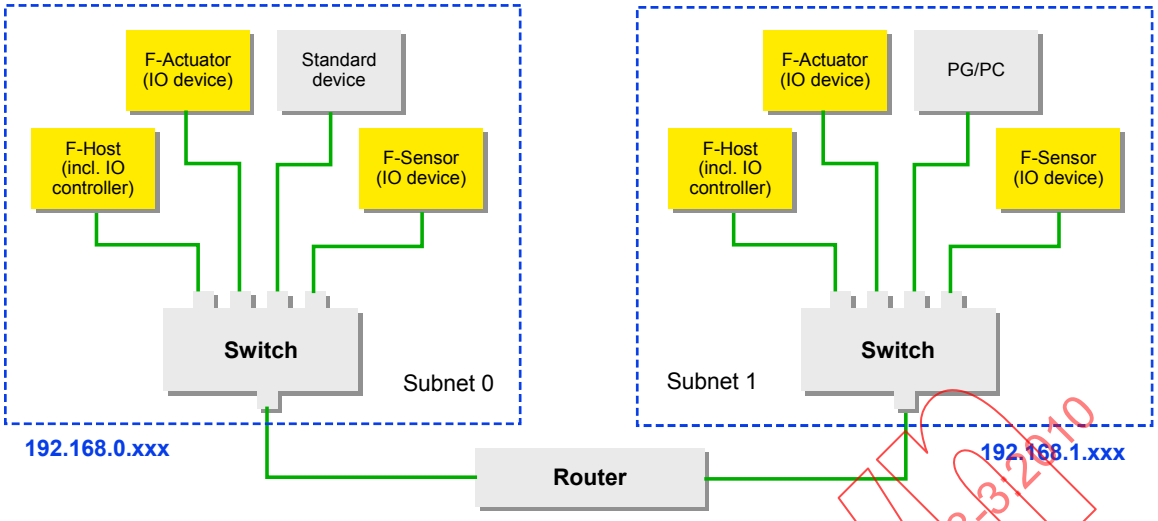
Légende

Anglais	Français
Switch	Commutateur
F-Host (incl. IO controller)	Hôte F (y compris contrôleur d'entrée-sortie)
F-sensor (IO device)	Capteur F (dispositif d'entrée-sortie)
Standard device	Dispositif standard
F-Actuator (IO device)	Actionneur F (dispositif d'entrée-sortie)
Remote IO (F + standard Modules)	Entrée-sortie distante (F + Modules standard)
optional	facultatif

Figure 10 – Structure de bus linéaire

Chacun des réseaux de la Figure 9 et de la Figure 10 appartient à un système CP 3/RTE portant une adresse IP particulière, le protocole en temps réel (RT ou IRT) de la couche 2 ne pouvant pas aller au-delà de cet espace d'adresse IP (Figure 8). Il revient aux routeurs (couche OSI 3) de ré-acheminer les messages vers un niveau d'adresse IP (Figure 11). Par conséquent, les routeurs sont les limites naturelles des systèmes CP 3/RTE. Les restrictions suivantes s'appliquent à FSCP 3/1.

- Réseau local sans fil autorisé. Toutefois, le caractère unique des adresses F doit être garanti à l'intérieur des îlots.
- Les commutateurs ne sont pas admis, ce qui permet de croiser les limites du réseau (îlots).
- Les routeurs à un seul port ne sont pas admis (7.3.9).



Légende

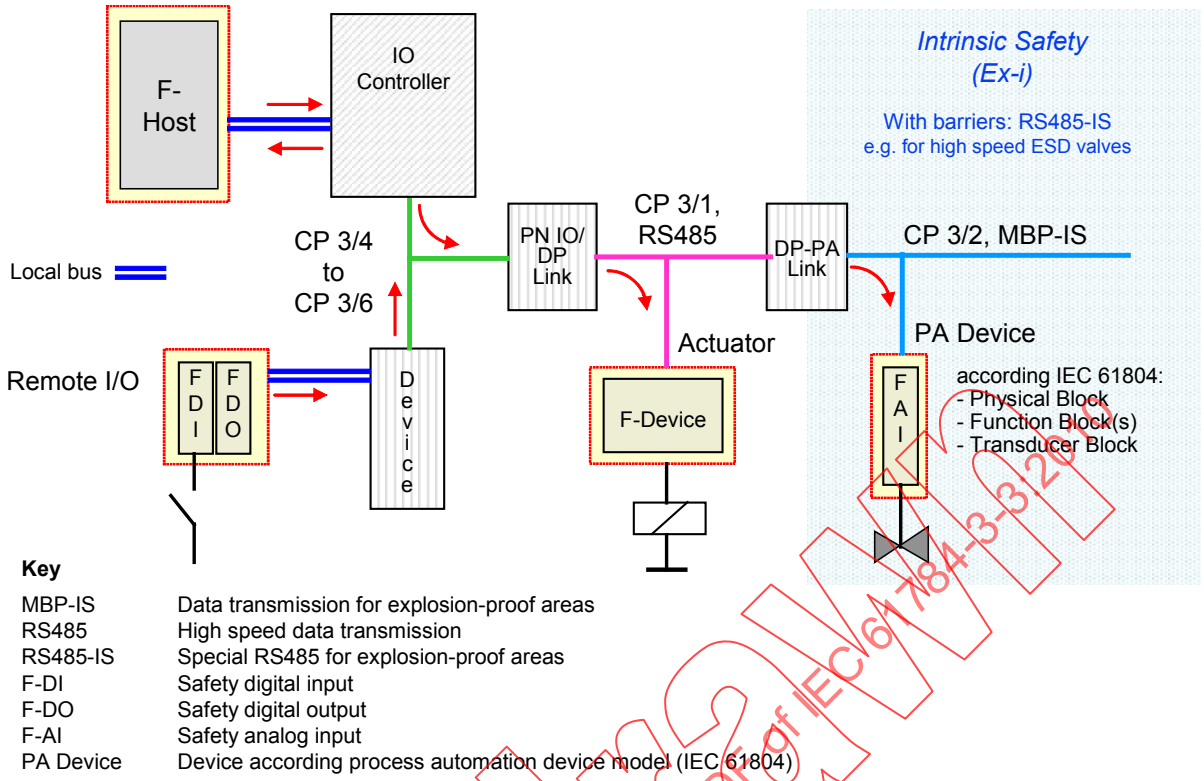
Anglais	Français
Switch	Commutateur
F-Host (incl. IO controller)	Hôte F (y compris contrôleur d'entrée-sortie)
F-sensor (IO device)	Capteur F (dispositif d'entrée-sortie)
Standard device	Dispositif standard
F-Actuator (IO device)	Actionneur F (dispositif d'entrée-sortie)
Remote IO (F + standard Modules)	Entrée-sortie distante (F + Modules standard)
optional	facultatif
Subnet 0	Sous-réseau 0
Subnet 1	Sous-réseau 1
Router	Routeur

Figure 11 – Croisement des limites du réseau avec les routeurs

A l'inverse de la configuration classique d'un système de bus de terrain, la Figure 12 illustre la structure de bus possible, c'est-à-dire la mesure dans laquelle le profil de sécurité s'étend dans les unités individuelles. Par exemple, une entrée-sortie distante standard peut contenir un module F permettant de connecter un bouton d'arrêt d'urgence. Par conséquent, l'ensemble de la voie de transmission FSCP 3/1 passe dans le dispositif d'entrée-sortie par le bus de fond de panier de l'hôte F via CP 3/RTE (PN IO), puis dans le module F final par l'intermédiaire d'un autre fond de panier possible. La couche de sécurité est mise en œuvre à l'intérieur de ces extrémités de communication.

Un fonctionnement à plusieurs contrôleurs ou plusieurs maîtres des hôtes F est admis. Les « entrées F partagées » ne sont pas admises. Un mélange de l'hôte F et de l'hôte standard est possible.

NOTE Voir [48] pour plus de détails sur le mode V1 sur CP 3/1.



Légende

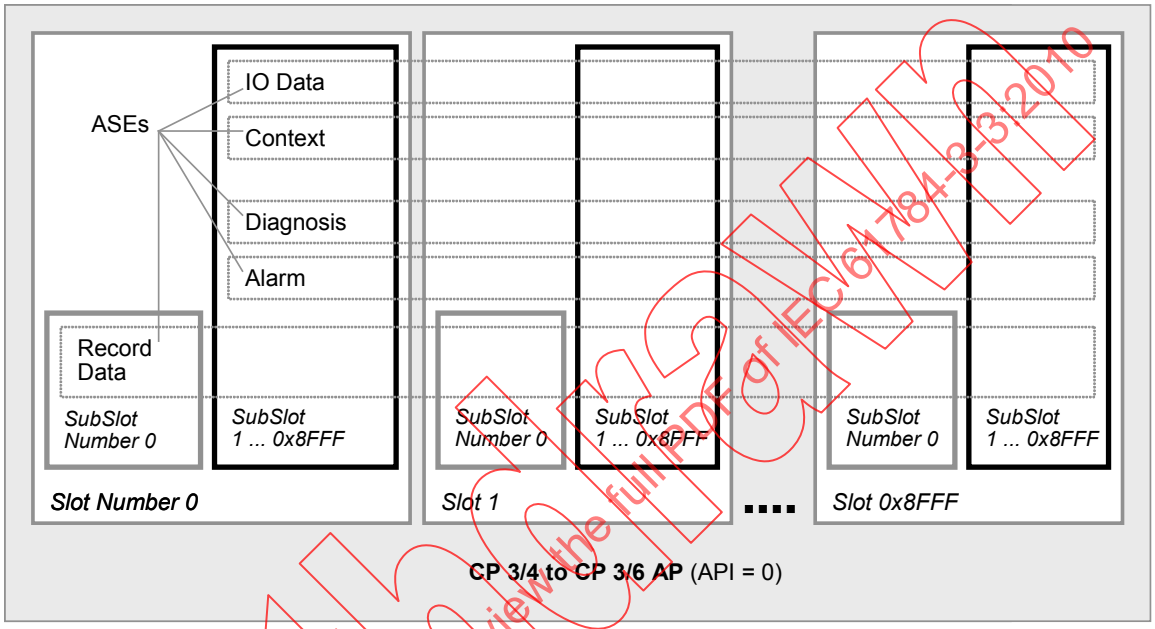
Anglais	Français
F-host	Hôte F
I/O controller	Contrôleur d'entrée-sortie
Intrinsic safety	Sécurité intégrée
With barriers	Avec barrières
e.g. for high speed ESD valves	Par exemple, soupapes ESD à grande vitesse
Local bus	Bus local
To	A
PN IO/DP link	Liaison PN IO/DP
DP-PA link	Liaison DP-PA
Remote I/O	Entrée-sortie distante
Actuator	Actionneur
PA device	Dispositif PA
Device	Dispositif
F-device	Dispositif F
According IEC …	Conformément à la CEI …
Physical block	Bloc physique
Function block(s)	Bloc(s) de fonctions
Transducer block	Bloc de transducteur
Key	Légende
Data transmission for explosion-proof areas	Transmission de données pour zones anti-déflagrantes
High speed data transmission	Transmission de données grande vitesse
Special RS485 for explosion-proof areas	RS485 spécial pour zones anti-déflagrantes
Safety digital input	Entrée numérique de sécurité
Safety digital output	Sortie numérique de sécurité
Safety analog input	Entrée analogique de sécurité
Device according ….	Dispositif conforme au modèle de dispositif d'automatisation industriel (CEI 61804)

Figure 12 – Voies de transmission de sécurité complètes

5.5 Relations avec la FAL (et DLL, PhL)

5.5.1 Modèle de dispositif

Le CP 3/RTE, ainsi que le modèle de dispositif CP 3/1, suppose la présence d'un ou de plusieurs processus d'application (AP) dans le dispositif. La Figure 13 illustre la structure interne d'un processus d'application pour un dispositif de terrain modulaire. Éventuellement, elle peut comporter plusieurs de ces processus d'application. Le processus d'application est divisé en intervalles et sous-intervalles, selon le cas, afin de représenter les entrées-sorties physiques du dispositif. A l'inverse de CP 3/1, CP 3/RTE offre un niveau hiérarchique supplémentaire: les sous-intervalles.



Légende

Anglais	Français
IO data	Données d'entrée-sortie
Context	Contexte
Diagnosis	Diagnostic
Alarm	Alarme
Record data	Données d'enregistrement
Subslot number	Numéro de sous-intervalle
Slot number	Numéro d'intervalle
Slot	Intervalle
To	à

Figure 13 – Modèle de dispositif

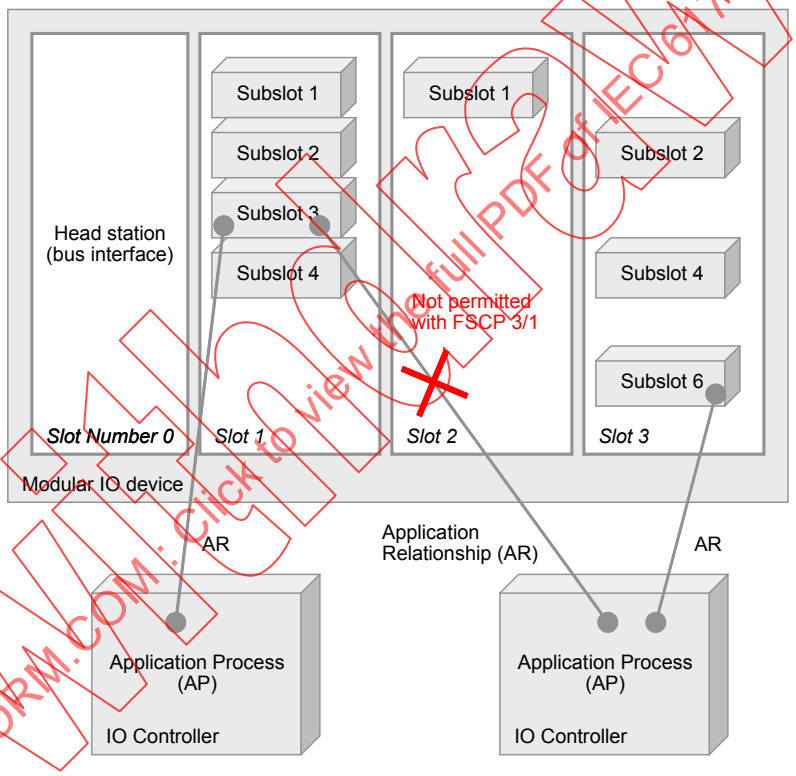
Dans les sous-intervalles, les éléments de service d'application (ASE) offrent un ensemble de services normalisés permettant d'acheminer les demandes et les réponses entre les processus d'application, ainsi que leurs objets de données (données d'entrée-sortie, Contexte (Paramétrage), Diagnostic, Alarmes et Données d'enregistrement, par exemple). Le fabricant du dispositif est chargé de la mise en correspondance réelle des fonctionnalités du dispositif avec le modèle de dispositif CP 3/RTE (attribution d'intervalles et de sous-intervalles) par l'intermédiaire d'un fichier GSD.

5.5.2 Relations d'application et de communication

Pour utiliser les services mentionnés ci-dessus, il est toujours nécessaire d'établir une relation d'application (AR), à l'intérieur de laquelle sont établies des relations de communication (CR) pour les objets de données à échanger entre les stations (dispositif, contrôleur d'entrée-sortie) via les ASE. La Figure 14 illustre un exemple de structure de base d'un dispositif d'entrée-sortie modulaire et des relations d'application possibles avec des contrôleurs d'entrée-sortie.

Un contrôleur d'entrée-sortie utilise une trame « Connect » (Connexion) à l'intérieur d'un message CP 3/RTE particulier afin d'établir une relation d'application au démarrage du système. Il transfère donc l'ensemble de données suivant au dispositif.

- Paramètres généraux de communication de cette relation d'application (AR).
- Relations de communication (CR) à établir, y compris leurs paramètres.
- Modèle et données de mise en correspondance du dispositif.
- Relations de communication d'alarme à établir, y compris leurs paramètres.

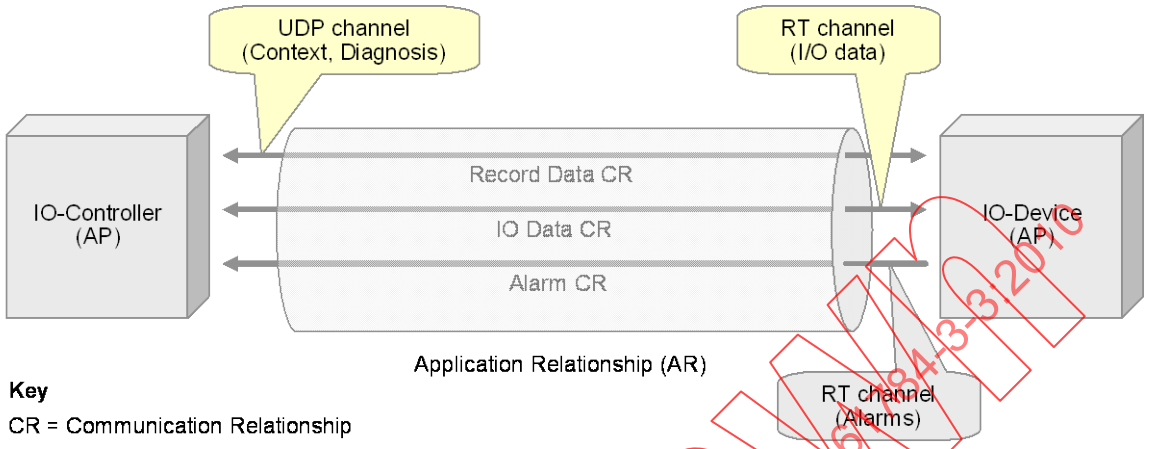


Légende

Anglais	Français
Head station (bus interface)	Station de tête (interface de bus)
Subslot	Sous-intervalle
Not permitted with …	Non autorisé avec …
Slot number	Numéro d'intervalle
Slot	Intervalle
Modular IO device	Dispositif d'entrée-sortie modulaire
Application relationship	Relation d'application
Application process	Processus d'application
IO controller	Contrôleur d'entrée-sortie

Figure 14 – Relations d'application d'un dispositif modulaire

Le dispositif d'entrée-sortie vérifie les données reçues et établit les relations de communication requises. Les éventuelles erreurs sont signalées au contrôleur d'entrée-sortie. L'échange des données commence par l'acquittement positif du dispositif à un appel « Connect » (Connexion). Il n'est pas admis d'établir deux relations d'application FSCP 3/1 provenant de processus d'application différents avec un seul sous-intervalle.



Légende

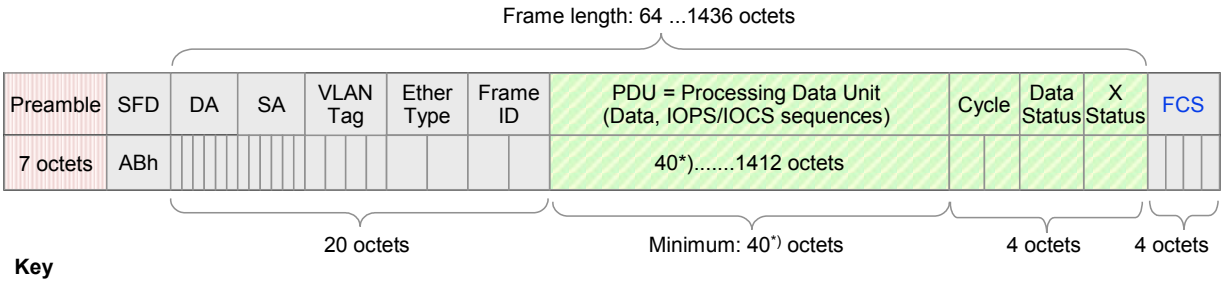
Anglais	Français
UDP channel (context, diagnosis)	Canal UDP (contexte, diagnostic)
RT channel (I/O data)	Canal RT (données d'entrée-sortie)
IO-controller	Contrôleur d'entrée-sortie
Record data CR	CR de données d'entrée-sortie
IO data CR	CR de données d'entrée-sortie
Alarm CR	CR d'alarme
IO-device	Dispositif d'entrée-sortie
Application relationship	Relation d'application
Key	Légende
Communication relationship	Relation de communication
RT channel (alarms)	Canal RT ((alarmes)

Figure 15 – Relations d'application et de communication (AR/CR)

A ce stade, les données d'entrée-sortie peuvent toujours être signalées comme étant non valides, étant donné que le paramètre de démarrage des dispositifs d'entrée-sortie n'a toujours pas été attribué. Suite à l'appel « Connect », le contrôleur d'entrée-sortie transfère les données d'attribution de paramètre de démarrage (Contexte) vers le dispositif d'entrée-sortie grâce à la relation de communication Données d'enregistrement (Figure 15). Le contrôleur d'entrée-sortie utilise une « trame d'écriture » par sous-module configuré, puis met fin au transfert par une « fin de paramétrage ». En retour, le dispositif d'entrée-sortie acquitte l'attribution du paramètre de démarrage par un élément "application ready" (application prête). Dès lors, la relation d'application est établie.

5.5.3 Format de message

Le format de message CP 3/RTE pour l'échange de données en temps réel est présenté dans la Figure 16. Une séquence de contrôle de trame (FCS) de 32 bits protège la transmission sur le réseau. FSCP 3/1 ne profite pas de cette mesure.



Key

Preamble = AAAAAAAAAAAAAAh
SFD = Start Frame Delimiter: ABh
DA = Destination Address (6 octets)
SA = Source Address (6 octets)
VLAN Tag = indicates a certain priority; optional
Ether Type = Ethernet Frame Type: 8892h for CP 3/4 to CP 3/6 (2 octets)
Frame ID = Frame Identification (CP 3/4 to CP 3/6 message type)
IOPS = IO Provider Status: good/bad and location (optional/GSD)
IOCS = IO Consumer Status: good/bad and location (optional/GSD)
Cycle = Cycle Counter (2 octets); multiples of 31,25µs
Data Status = Information on redundancy, validity, device state, etc.
X Status = Transfer Status (1 octet); always "00h"
FCS = 32 bit CRC (104C11DB7h)

*) with VLAN-Tag minimum of user data to be transferred is 36 octets

Légende

Anglais	Français
Frame length	Longueur de trame
Preamble	Préambule
VLAN tag	Drapeau VLAN
Ether type	Type Ether
Frame ID	ID de trame
Processing data unit	Ensemble de données de traitement
Data	Données
IOPS/IOCS sequences	Séquences IOPS/IOCS
Data status	état des données
Etat X	Etat X
Key	Légende
Start frame delimiter	Délimiteur de trame de début
Destination address	Adresse de destination
Source address	Adresse source
Indicates a certain priority; optional	Indique une priorité donnée; facultatif
Ethernet frame type: … for … to ..	Type de trame ethernet: … pour … à …
Frame identification (CP ¾ to CP 3/6 message type)	Identification de trame (type de message CP 3 / 4 à CP 3/6)
IO provider Status: good/bad and location (optional/GSD)	Etat du fournisseur d'entrée-sortie: bon/mauvais et emplacement (facultatif/GSD)
IO consumer Status: good/bad and location (optional/GSD)	Etat du consommateur d'entrée-sortie: bon/mauvais et emplacement (facultatif/GSD)
Cycle counter (2 octets); multiples of	Compteur de cycles (2 octets); multiples de …
Information redundancy …	Redondance et validité des informations, état de dispositif
Transfer status (1 octed); always 00h'	Etat de transfert (1 octet); toujours « 00h »
32 bit CRC	CRC 32 bits
With VLAN –Tag minimum of user data to be transferred is 36 octets.	Avec drapeau VLAN minimal des données utilisateur à transférer égal à 36 octets

Figure 16 – Format de message

5.5.4 Types de données

CPF 3 utilise les types de données de base figurant dans le Tableau 2. Pour des raisons de sécurité, seul un nombre limité de types de données peut être utilisé pour FSCP 3/1.

Tableau 2 – Types de données utilisés pour FSCP 1/3

Nom du type de données	Nombre d'octets	Utilisé dans
Integer8	1	
Integer16	2	les modes V1 et V2
Integer32	4	le mode V2
Integer64	8	
Unsigned8 (utilisé comme bits)	1	les modes V1 et V2
Unsigned16 (utilisé comme bits)	2	le mode V2
Unsigned32 (utilisé comme bits)	4	le mode V2
Unsigned16	2	
Unsigned32	4	
Unsigned64	8	
Float32	4	les modes V1 et V2
Float64	8	
Date		
TimeOfDay avec indication de date		
TimeOfDay sans indication de date		
TimeDifference avec indication de date		
TimeDifference sans indication de date		
NetworkTime		
NetworkTimeDifference		
Visible String (Chaîne visible)	1,2,3, …	
Unsigned8+Unsigned8	2	les modes V1 et V2
Float32+Unsigned8 (énuméré)	5	les modes V1 et V2
F_MessageTrailer4Byte	4	les modes V1 et V2
F_MessageTrailer5Byte	5	le mode V2

Les types de données utilisés dans le mode V2 sont limités à Unsigned8, Unsigned16, Unsigned32, Integer16, Integer32, Float32 et au type de données composées Float32 + Unsigned8.

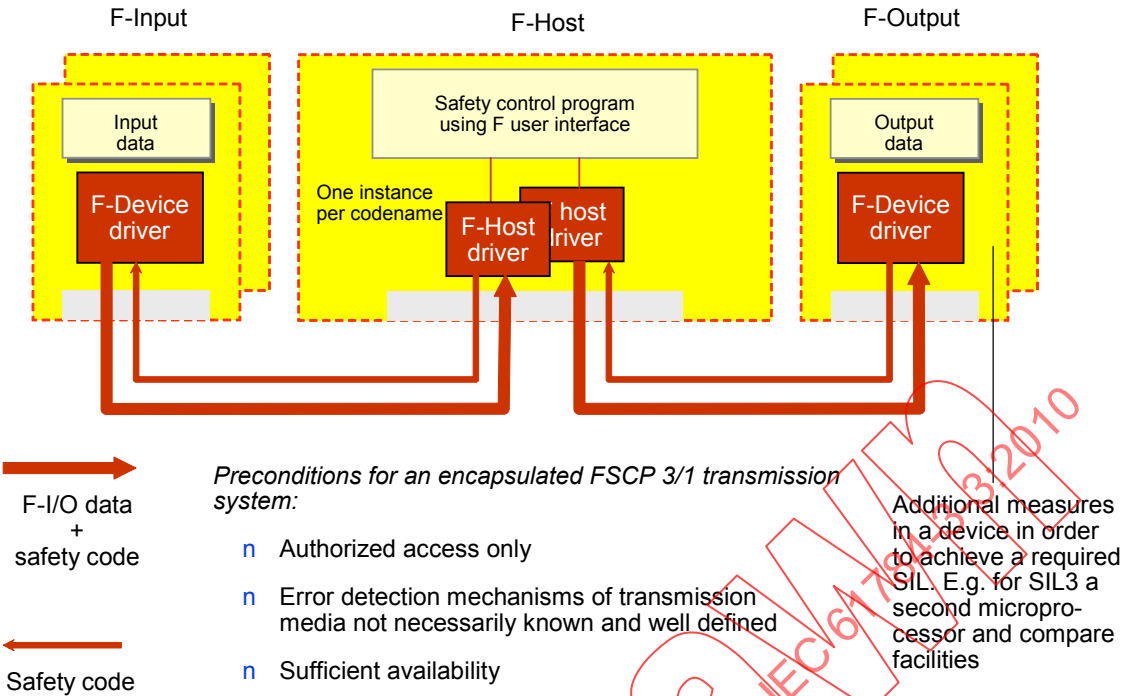
Les bits uniques doivent être codés dans un type de données Unsigned8, Unsigned16 ou Unsigned32 en raison de sa plus grande efficacité comparé au type de données booléen.

Voir [67] pour des informations générales sur les types de données.

6 Services de la couche de communication de sécurité

6.1 Services de l'hôte F

La Figure 17 montre que chaque entrée et sortie F implique une gestion de PDU de sécurité (pilote F) afin de traiter le protocole FSCP 3/1. L'hôte F correspondant fonctionne avec une instance d'un pilote F pour chaque entrée ou sortie F, respectivement. Par conséquent, toutes les relations de type 1:1 entre une instance du pilote F et le partenaire correspondant dans un dispositif F sont identifiées par un *nom de code* unique (l'un des paramètres F).



Légende

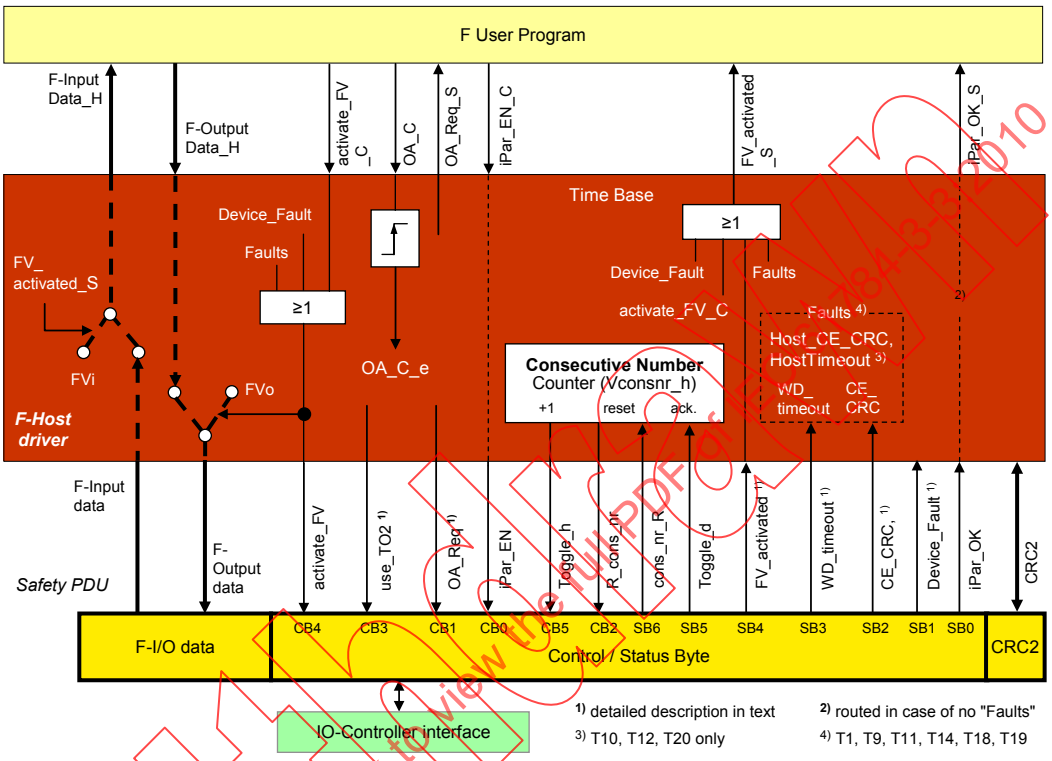
Anglais	Français
F-input	Entrée F
F-host	Hôte F
F-output	Sortie F
Input data	Données d'entrée
Safety control …	Programme de commande de sécurité utilisant l'interface utilisateur F
Output data	Données de sortie
F-device driver	Pilote de dispositif F
One instance per codename	Une instance par nom de code
F-host driver	Pilote d'hôte F
F-I/O data	Données F d'entrée-sortie
Safety code	Code de sécurité
Preconditions for an encapsulated FSCP 3/1 transmission system:	*Conditions préalables pour un système de transmission FSCP 3/1 encapsulé*
Authorized access only	Accès autorisé uniquement
Error detection mechanisms of transmission media not necessarily known and well defined	Mécanismes de détection d'erreurs du support de transmission non nécessairement connu et bien défini
Sufficient availability	Disponibilité suffisante
Additional measures in a devise in order to achieve a required SIL e.g for SIL3 a second microprocessor and compare facilities.	Mesures supplémentaires dans un dispositif afin d'atteindre un SIL requis. Par exemple, pour SIL3, un second microprocesseur et des installations de comparaison

Figure 17 – Structure de communication FSCP 3/1

L'ensemble de l'équipement de communication CPF 3 standard entre les pilotes F appartient au canal noir. Les flèches dans la Figure 17 indiquent le transport de données cycliques entre les pilotes F: le supplément de sécurité (Octet d'état ou de contrôle et CRC2) est transféré

vers l'hôte F en plus des données de l'entrée F. A titre d'acquittement, l'entrée F reçoit simplement le supplément de sécurité (code de sécurité). En conséquence, la sortie F reçoit le supplément de sécurité accompagné des données de la sortie F, et l'utilise pour l'acquittement.

Les tâches de gestion de PDU de sécurité et de paramétrage F incombent aux pilotes F à l'intérieur de l'hôte F et des dispositifs F. La Figure 18 illustre l'interface utilisateur F au niveau du programme de commande de sécurité.



Légende

Anglais	Français
F user program	Programme utilisateur F
F-input	Entrée F
F-output	Sortie F
Faults	Pannes
Time base	Temps de base
F-host driver	Pilote d'hôte F
Consecutive number counter	Compteur de numéros consécutifs
F-input data	Données d'entrée F
Safety PDU	PDU de sécurité
F-output data	Données de sortie F
F-I/O data	Données F d'entrée-sortie
Control / status byte	Octet de contrôle / d'état
IO-controller interface	Interface du contrôleur d'entrée-sortie
Detailed description in text	Description détaillée dans le texte
Only	Uniquement
Routed in case of no « faults »	Acheminé en l'absence de panne

Figure 18 – Interface utilisateur F des instances du pilote de l'hôte F

Le programmeur dispose de plusieurs variables pour manipuler les processus de sécurité conformément aux normes. Ces variables portent des noms similaires (en principe suivi de l'index « _C » (Control) ou « _S » (Status)) comme le bit correspondant dans les octets d'état et de contrôle, mais peuvent faire l'objet d'une certaine logique de commande à l'intérieur du pilote F. Voir également 8.5.2 et la Figure 62. Les indications de mise en œuvre pour le pilote de l'hôte F sont collectées en 8.5.3.

Le programmeur d'un programme de commande de l'hôte F doit disposer des variables suivantes conformément à 9.9:

activate_FV_C Chaque programme de commande de sécurité qui gère un dispositif F correspondant doit utiliser cette variable (type: bit). Si la valeur 1 est attribuée à cette variable des dispositifs d'entrée (des capteurs, par exemple), le pilote fournit des valeurs Failsafe (0) au programme de commande F. Si la valeur 1 est attribuée à cette variable des dispositifs de sortie (des actionneurs, par exemple), le pilote envoie des valeurs Failsafe (0) au dispositif et attribue la valeur 1 au bit 4 de l'octet de contrôle. Le concept de sécurité du dispositif de sortie définit le type d'informations de ces deux pilotes qui doivent être utilisées pour atteindre l'état de sécurité.

FV_activated_S Chaque programme de commande F qui gère un dispositif F correspondant doit utiliser cette variable (type: bit). Si la valeur 1 est attribuée à cette variable dans les dispositifs d'entrée, le pilote fournit des valeurs Failsafe (0) au programme de l'hôte F pour chaque valeur d'entrée. Indication: afin de gérer les entrées individuellement, des bits qualificatifs particuliers peuvent être ajoutés aux données d'entrée.

Si la valeur 1 est attribuée à cette variable dans les dispositifs de sortie, une valeur Failsafe 0 (comportement par défaut) ou une valeur spécifique au dispositif de sortie F contrôlé par le signal « activate_FV » (= bit 4 de l'octet de contrôle) est attribuée à chaque sortie. Indication: afin de gérer les sorties individuellement (les axes de moteur, par exemple), des bits qualificatifs particuliers peuvent être utilisés.

iPar_EN_C Si la valeur 1 est attribuée à cette variable (type: bit), le programme de commande F commute le dispositif F en un mode au cours duquel il accepte iParamètres. Il est directement associé au signal de contrôle « iPar_EN » (= bit 0 de l'octet de contrôle) et n'affecte pas les états de l'hôte F. Le cas échéant, la valeur 1 doit également être attribuée à la variable « activate_FV_C ».

iPar_OK_S Cette variable (type: bit) signale au programme de commande F la fin de l'iParamétrage et la possibilité de reprendre l'échange de données d'entrée-sortie F (Figure 41). Elle doit être mise à jour avec la valeur de « iPar_OK » dans les transitions T4, T8 et T17 du diagramme d'états de l'hôte F si le bit d'état 1 « Device_Fault » n'est pas défini. Sinon, elle conserve la précédente valeur. Elle n'a aucun impact sur les états de l'hôte F. De nouvelles valeurs peuvent être attribuées aux variables iPar_EN_C et activate_FV_C.

OA _C (Acquittement de l'opérateur) Chaque programme de commande F doit utiliser cette variable (type: bit). Si l'utilisateur attribue la valeur 1 à cette variable, il peut reprendre la fonction de sécurité suite à une réaction aux anomalies (spécifique à la boucle de contrôle à sécurité intégrée) à l'aide d'un programme utilisateur de l'hôte F.

OA_Req_S Cette variable (type: bit) indique une demande d'acquittement avant la reprise d'une fonction de sécurité. Si le pilote de l'hôte F ou un

dispositif F détecte une erreur de communication ou une panne du dispositif F, les valeurs Failsafe sont activées. Ensuite, le pilote du dispositif F définit la variable OA_Req_S (="1") dès que la panne/l'erreur a été résolue et que l'acquittement de l'opérateur est possible. Après l'acquittement (OA_C = "1"), le pilote du dispositif F réinitialise la variable de demande OA_Req_S (= "0").

Valeurs d'entrée PVi Valeurs d'entrée de processus (←F-Input_Data_D, voir Figure 19)
FVi Valeurs d'entrée de sécurité intégrée, utilisées à la place de PVi pour F-Input_Data_D (Figure 19)

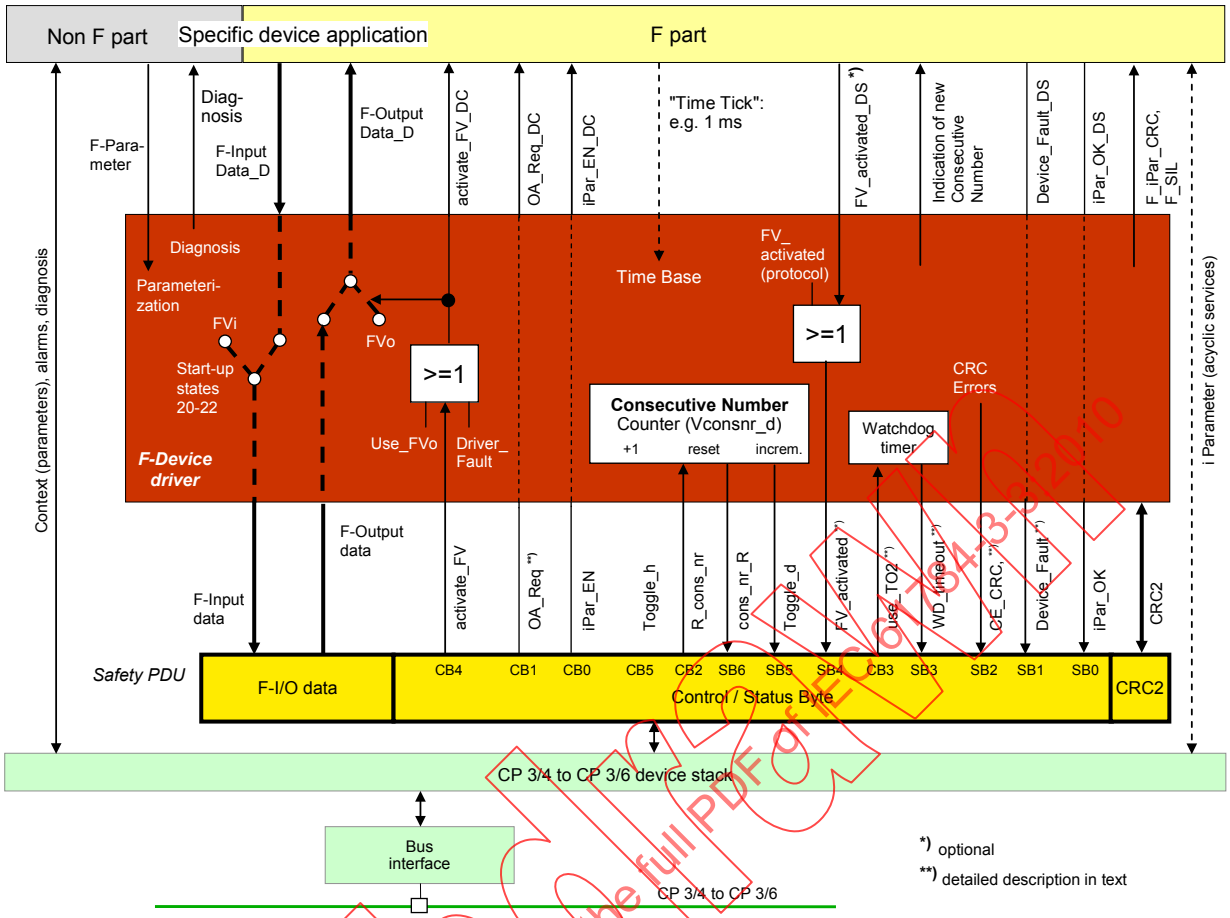
Valeurs de sortie PVo Valeurs de sortie du processus (→F-Output_Data_D)
FVo Valeurs de sortie de sécurité intégrée (=0), utilisées à la place de PVo pour F-Output_Data_D

6.2 Services du dispositif F

La Figure 19 illustre les caractéristiques du pilote du dispositif F et son imbrication entre l'interface CP 3/RTE et la partie relative à la sécurité de l'application du dispositif spécifique. Au cours de la phase de démarrage, la partie non relative à la sécurité de l'application du dispositif spécifique reçoit les paramètres F et les transmet au pilote du dispositif F. Le pilote lui-même, après avoir vérifié certains des paramètres F, transmet « F_iPar_CRC » et « F_SIL » à la partie relative à la sécurité de l'application du dispositif spécifique. En règle générale, l'application du dispositif spécifique offre une base de temps (1 ms) au pilote du dispositif F afin d'alimenter les temporisateurs.

Le pilote du dispositif F traite principalement les PDU de sécurité reçus ou transmis par l'intermédiaire de la relation de communication des données d'entrée-sortie en temps réel de CP 3/RTE (5.5.2). En général, les données d'entrée-sortie F sont transmises, sauf pendant le démarrage (auquel cas, FVi est transmis) ou en cas d'anomalies (auquel cas, FVo est transmis). Les PDU de sécurité reçus contiennent des octets de contrôle avec les bits de contrôle CB0, CB1, CB2, CB3, CB4 et CB5. Certains de ces signaux sont transmis à l'interface d'application sans interaction. Un nouveau numéro consécutif est indiqué afin de faciliter la mise en œuvre des sollicitations avec une durée suffisante (au moins un cycle FSCP 3/1 = deux numéros consécutifs différents).

En retour, les PDU de sécurité sont préparés pour la transmission. Ils contiennent des octets d'état avec les bits d'état SB0 ..SB5. L'un d'eux est transmis, le pilote en générant un, et certains proviennent de l'interface d'application avec manipulation du pilote avant d'entrer dans le PDU de sécurité. Une valeur est attribuée à Driver_Fault en cas d'anomalie interne du pilote.



Légende

Anglais	Français
Non F part	Partie non F
Specific device application	Application de dispositif spécifique
F part	Partie F
F-parameter	Paramètre F
Time base	Temps de base
e.g.	Par exemple
Indication of new consecutive numbers	Indication d'un nouveau numéro consécutif
(protocol)	(protocole)
Context (parameters), alarms, diagnosis	Contexte (paramètres), alarmes, diagnostic
Diagnosis	diagnostic
Consecutive number counter	Compteur de numéros consécutifs
F-input data	Données d'entrée F
Safety PDU	PDU de sécurité
F-output data	Données de sortie F
CRC errors	Erreurs CRC
IParameter (acyclic services)	IParamètre (services acycliques)
Control / status byte	Octet de contrôle / d'état
F-I/O data	Données d'entrée-sortie F
Detailed description in text	Description détaillée dans le texte
CP 3 / 4 to CP 3/6 device stack	Pile de dispositif CP 3 / 4 à CP 3/6
To	à
Bus interface	Interface de bus
Optional	facultatif

Figure 19 – Interfaces du pilote du dispositif F

Le compteur de numéros consécutifs est incrémenté (x+1) lorsque l'état de Toggle_h change (0→1; 1→0). Le compteur est réinitialisé (0) lorsque R_cons_nr = "1". Le compteur en cours d'incrémentation change l'état de Toggle_d (0→1; 1→0). Le contrôle CRC est exécuté avec chaque PDU de sécurité reçu et envoyé (CRC2).

L'application du dispositif spécifique dispose des variables suivantes. Les variables portent des noms similaires (en principe suivis d'une extension DC (Device Control) ou DS (Device Status), comme les bits correspondants dans les octets d'état et de contrôle.

activate_FV_DC Cette variable relative à la sécurité indique que les données de sortie F sont des valeurs Failsafe (FV = 0). Elle peut être utilisée pour forcer les sorties d'un dispositif F à être des valeurs Failsafe configurées ou intégrées.

FV_activated _DS Si la valeur 1 est attribuée à cette variable dans les dispositifs d'entrée, l'application du dispositif fournit des valeurs Failsafe (0) au pilote FSCP 3/1 pour chaque valeur d'entrée.

Indication: afin de gérer les entrées individuellement, des bits qualificatifs particuliers peuvent être ajoutés aux données d'entrée. Si la valeur 1 est attribuée à cette variable dans les dispositifs de sortie, une valeur Failsafe est attribuée à chaque sortie. Si la valeur 1 est attribuée à cette variable dans les dispositifs d'entrée et de sortie combinés (type: bit), l'application du dispositif fournit des valeurs Failsafe (0) au pilote FSCP 3/1 pour chaque valeur d'entrée, et une valeur Failsafe est attribuée à chaque sortie.

OA_Req_DC L'application du dispositif F doit utiliser cette variable non relative à la sécurité pour indiquer localement la demande d'un acquittement de l'opérateur (*OA_C* dans l'hôte F), en général par l'intermédiaire d'une DEL. La mise en œuvre est facultative pour les dispositifs F.

iPar_EN_DC Si la valeur 1 est attribuée à cette variable, cela indique une demande de paramétrage (le dispositif F a besoin de nouveaux iParamètres).

iPar_OK_DS Si la valeur 1 est attribuée à cette variable, de nouvelles valeurs iParamètre sont attribuées au dispositif F (son application spécifique).

Device_Fault_DS Anomalie reconnue par l'application du dispositif spécifique.

6.3 Diagnostic

6.3.1 Génération d'alarme de sécurité

Compte tenu de la rapidité des cycles d'interrogation du programme utilisateur, la vitesse de détection des modifications des données d'entrée-sortie F et de la signature CRC2 est satisfaisante.

En cas d'erreurs de communication, le système est en mesure de réagir à temps de manière sécurisée (grâce aux informations de l'octet d'état, par exemple).

6.3.2 Diagnostic de la couche de sécurité du dispositif F (y compris le serveur d'iParamètres)

Afin de consigner les informations de diagnostic du pilote du dispositif F FSCP 3/1 dans une une interface homme/machine, le pilote les transmet à l'application du dispositif F qui utilise

des mécanismes CP 3/RTE standard pour leur propagation au contrôleur d'entrée-sortie. Chaque option de diagnostic standard de CP 3/RTE est possible, de préférence le diagnostic relatif au canal. La table de codage du champ « ChannelErrorType » contient une zone réservée pour FSCP 3/1.

Le Tableau 3 présente les différents types d'informations de diagnostic de la couche de protocole FSCP 3/1 des dispositifs F.

Tableau 3 – Messages de diagnostic de la couche de sécurité

Hex	Numéro	Informations de diagnostic
0x0040	64	Défaut d'adaptation de l'adresse de destination de sécurité (F_Dest_Add), voir 8.1.2
0x0041	65	Adresse de destination de sécurité non valide (F_Dest_Add), voir 8.1.2
0x0042	66	Adresse source de sécurité non valide (F_Source_Add), voir 8.1.2
0x0043	67	La valeur du temps de fonctionnement du chien de garde de sécurité est de 0 ms (F_WD_Time)
0x0044	68	Le paramètre F_SIL dépasse le niveau d'intégrité de sécurité (SIL) de l'application du dispositif spécifique
0x0045	69	Le paramètre F_CRC_Length ne correspond pas aux valeurs générées
0x0046	70	La version de l'ensemble de paramètres F est incorrecte
0x0047	71	Anomalie CRC1
0x0048	72	Informations de diagnostic spécifique au dispositif, voir le manuel
0x0049	73	Temps de fonctionnement du chien de garde iParamètre de sauvegarde dépassé
0x004A	74	Temps de fonctionnement du chien de garde iParamètre de restauration dépassé
0x004B	75	iParamètres incohérents (erreur iParCRC)
0x004C	76	Réservé: ne pas utiliser les numéros, ne pas évaluer les numéros
0x004D	77	Réservé: ne pas utiliser les numéros, ne pas évaluer les numéros
0x004E	78	Réservé: ne pas utiliser les numéros, ne pas évaluer les numéros
0x004F	79	Réservé: ne pas utiliser les numéros, ne pas évaluer les numéros

Les dispositifs F s'appuyant sur le mécanisme de serveur d'iParamètres pour stocker et extraire des iParamètres dans un hôte F ou son sous-système contrôlé, peuvent consigner des informations de diagnostic dédiées grâce à des codages supplémentaires distincts. Il est vivement recommandé aux dispositifs F d'utiliser ces types dans les messages de diagnostic. Toutefois, les messages de diagnostic peuvent contenir des informations récapitulatives pour plusieurs causes individuelles.

NOTE Il convient que le fabricant d'un dispositif explique la mise en correspondance de causes individuelles et d'un message de diagnostic particulier.

7 Protocole de couche de communication de sécurité

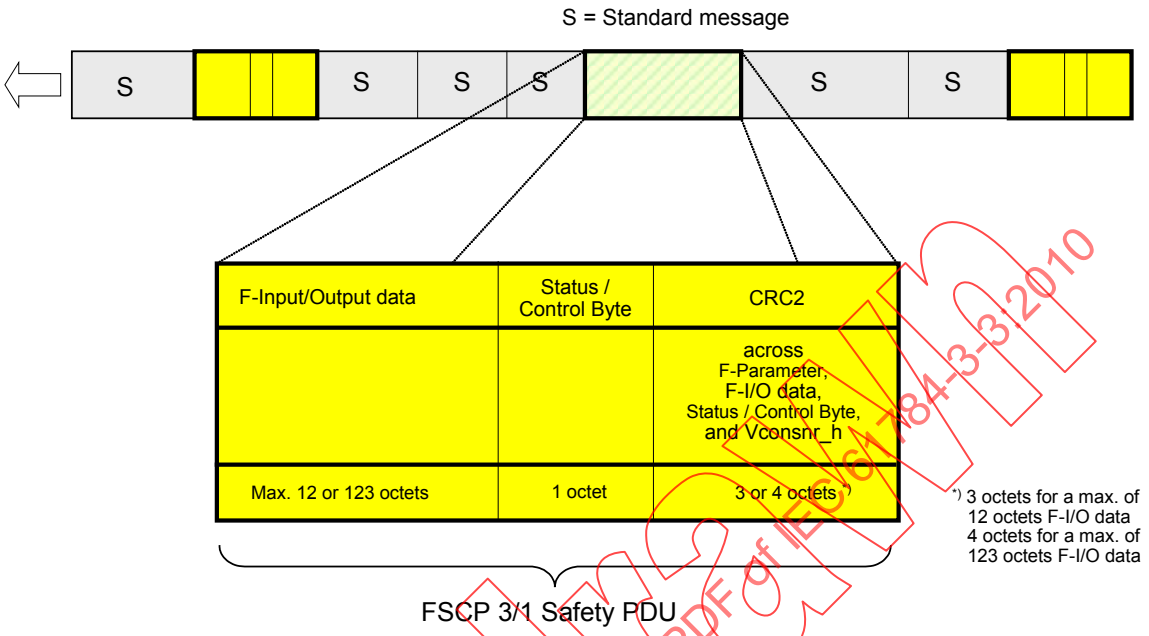
7.1 Format PDU de sécurité

7.1.1 Structure PDU de sécurité

La Figure 20 illustre la structure d'un PDU de sécurité contenant les données d'entrée-sortie de sécurité et un code de sécurité supplémentaire. Un message CP 3/RTE peut contenir plusieurs PDU de sécurité (dans le cas de dispositifs d'entrée-sortie modulaires comportant plusieurs modules de sécurité, par exemple).

L'automatisation des usines et l'automatisation de processus impliquent différentes exigences relatives au système de sécurité. L'automatisation des usines concerne les entrées-sorties binaires courtes ("bit") en général traitées à très grande vitesse. L'automatisation de

processus implique de plus longues valeurs d'entrée-sortie (virgule flottante) dont le temps de traitement peut être sensiblement plus long. Par conséquent, FSCP 3/1 propose deux longueurs de données d'entrée-sortie de sécurité différentes nécessitant une protection CRC de complexité différente pour satisfaire aux exigences de SIL3.



Légende

Anglais	Français
Standard message	Message standard
F-input/output data	Données d'entrée-sortie F
Status/control byte	Octet de contrôle / d'état
Across F-Parameter, F-I/O data, Satus / Control Byte, and Vconsnr_h	Parmi paramètre F, données d'entrée-sortie F, octet de contrôle / d'état et Vconsnr_h
Or	Ou
3 octets for …	3 octets pour un max. de données d'entrée-sortie F de 12 octets 4 octets pour un max. de données d'entrée-sortie F de 123 octets
FSCP 3/1 safety PDU	PDU de sécurité FSCP 3/1

Figure 20 – PDU de sécurité pour CPF 3

Par conséquent, *deux modes* opérationnels peuvent être choisis lors du paramétrage: données d'entrée-sortie F jusqu'à *12 octets* avec un CRC2 de 24 bits (3 octets) et données d'entrée-sortie (de processus) F jusqu'à *123 octets* avec un CRC2 de 32 bits (4 octets).

De plus, 4 (5) octets au total sont nécessaires, y compris l'octet d'état/de contrôle et 3 (4) octets pour le code CRC2.

Les paragraphes 7.1.2 à 7.1.6 donnent une description détaillée des éléments de la structure du PDU de sécurité.

7.1.2 Données d'entrée-sortie de sécurité

Les données d'entrée-sortie F des périphériques d'entrée-sortie F sont présentées dans cette section du PDU de sécurité. Le codage du type de données correspond à celui de CP 3/RTE et est défini à l'échelle du système dans la CEI 61158-5-10. Le paragraphe 8.5.2

recommande et spécifie les types et structures de données normalisés pour plusieurs familles de dispositifs de sécurité (entrée-sortie distante, rideaux de lumière, lecteurs laser, unités, etc.).

En présence de quelques données d'entrée-sortie F jusqu'à 12 octets, l'option de CRC 24 bits doit être choisie lors du paramétrage.

Outre les dispositifs compacts, il existe des *dispositifs modulaires* avec des unités d'entrée-sortie et des sous-adresses standard (Figure 13 et Figure 14). Leur station de tête CP 3/RTE (DAP), considérée comme faisant partie intégrante du canal noir, permet de convenir de la structure d'un message CP 3/RTE avec plusieurs PDU de sécurité grâce au paramétrage de démarrage. Un PDU de sécurité correspond à un sous-intervalle. La quantité de données correspond à la quantité de données standard CP 3/RTE moins 4 ou 5 octets respectivement. Par conséquent, dans le cas de la station de tête d'un dispositif contenant m modules de sécurité, cela signifie une réduction de m fois 4 ou 5 octets respectivement.

7.1.3 Octet d'état et de contrôle

Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
res	Vconsnr_d a été réinitialisé	Bit de basculement	Valeurs Failsafe (FV) activées	Défaut de communication: WD-timeout	Défaut de communication: CRC	Anomalie dans le dispositif F ou le module F	De nouvelles valeurs iParamètre ont été attribuées au dispositif F
-	cons_nr_R	Toggle_d	FV_activated	WD_timeout	CE_CRC	Device_Fault	iPar_OK

Figure 21 – Octet d'état

L'octet d'état présenté dans la Figure 21 est présent dans chaque PDU de sécurité d'un sous-module CP 3/RTE transmis d'un dispositif à son contrôleur (Figure 20).

Le bit 0 est défini lorsque de nouvelles valeurs de paramètre sont attribuées au dispositif F (son microprogramme technologique). Le nom de signal est iPar_OK.

Le bit 1 doit être défini par le microprogramme technologique spécifique au dispositif pour au mois deux (2) changements de numéro consécutif, si un dispositif/module F n'offre aucun qualificatif de signal spécifique au canal, en cas de défaillance d'un ou de plusieurs canaux ou de détection d'un autre dysfonctionnement. En cas de défaillance, les temps de réaction induits par ce comportement sont plus rapides que ceux induits par le délai d'attente. Le nom de signal est Device_Fault.

Le bit 2 est défini si le dispositif F reconnaît un défaut de communication F, c'est-à-dire si le numéro consécutif est erroné (erreur CRC2 en mode V2) ou en cas de transgression de l'intégrité des données (erreur CRC). Ces informations binaires permettent à l'hôte F de dénombrer tous les messages erronés dans un temps T défini et de déclencher un état de sécurité configuré du système si ce nombre dépasse une certaine limite (taux d'erreurs résiduelles maximal). Le nom de signal est CE_CRC. Voir également 9.5.1.

Le bit 3 est défini si le dispositif F reconnaît un défaut de communication F, c'est-à-dire si le temps de fonctionnement du chien de garde du dispositif F est dépassé. Le nom de signal est WD_timeout.

Le bit 4 est défini par la couche de protocole FSCP 3/1 au démarrage et en cas d'erreur de communication (Figure 19 et 7.2). De plus, la partie F de l'application de dispositif spécifique peut également définir ce bit. Le nom de signal est FV_activated.

Le bit 5 est un bit de basculement basé sur le dispositif indiquant le déclenchement de l'incrémentation du numéro consécutif virtuel dans l'hôte F (Vconsnr_h). Le nom de signal est Toggle_d.

Le bit 6 est défini lorsque le dispositif F a réinitialisé son compteur de numéros consécutifs Vconsnr_d. Le nom de signal est cons_nr_R.

Le bit 7 est réservé (res) aux versions ultérieures de FSCP 3/1.

Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
res	res	Bit de basculement	Valeurs Failsafe (FV) à activer	Utilisation de F_WD_Time_2 (chien de garde secondaire)	Réinitialisation de Vconsnr_d	Acquittement de l'opérateur demandé	Attribution d'iParamètre débloquée
-	-	Toggle_h	activate_FV	Use_TO2	R_cons_nr	OA_Req	iPar_EN

Figure 22 – Octet de contrôle

L'octet de contrôle présenté dans la Figure 22 est transmis du contrôleur d'entrée-sortie au dispositif avec chaque PDU de sécurité d'un sous-intervalle (Figure 20).

Le bit 0 est défini par l'application F dans un hôte F en cas de demande de paramétrage (le dispositif F a besoin de nouveaux iParamètres). Le nom de signal est iPar_EN.

Le bit 1 est défini par le pilote de l'hôte F correspondant à la variable OA_Req_S. Il ne s'agit pas d'un signal de sécurité, et il convient que le dispositif F l'utilise pour indiquer localement la demande d'acquittement d'un opérateur (OA_C), en général par l'intermédiaire d'une DEL (9.1). Le nom de signal est OA_Req.

Le bit 2 est défini lorsque l'hôte F détecte une erreur de communication, soit par l'octet d'état soit par lui-même. En conséquence, la valeur 0 est attribuée au compteur de numéros consécutifs virtuels (Vconsnr_d) du dispositif F (voir 7.1.4 et 7.2.5). Le bit 2 doit être réinitialisé après une erreur. Par la suite, la numérotation consécutive reprend. Le nom de signal est R_cons_nr.

Le bit 3 est défini lorsque le pilote de l'hôte F est naturellement informé d'un processus de mise à jour prévu des composants de bus de terrain de sécurité en cas de « configuration en cours » ou de « maintenance des systèmes de tolérance aux pannes ».

Le bit 4 être utilisé pour forcer les sorties d'un dispositif F à être des valeurs Failsafe configurées ou intégrées. Voir 6.1 pour plus de détails. Le nom de signal est activate_FV.

Le bit 5 est un bit de basculement basé sur l'hôte indiquant le déclenchement de l'incrémentation du numéro consécutif virtuel dans le dispositif F (Vconsnr_d). Le nom de signal est Toggle_h. Voir 7.1.4 pour plus de détails. Le nom de signal est Toggle_h.

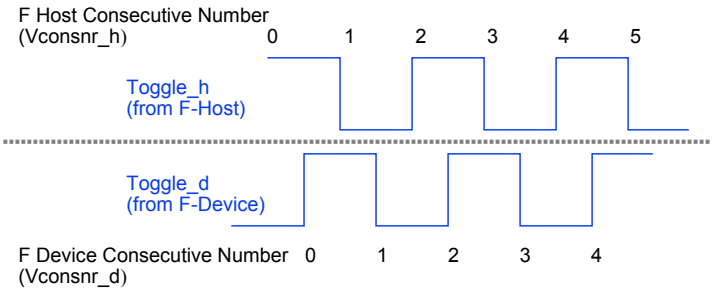
Les bits 6 et 7 sont réservés (res) aux versions ultérieures de FSCP 3/1.

Indication: pour éviter les complications avec les versions ultérieures des dispositifs FSCP 3/1: la valeur 0 doit être attribuée aux bits d'état et de contrôle de type « res », que le récepteur doit ignorer.

7.1.4 Numéro consécutif (virtuel)

Le destinataire utilise le numéro consécutif pour s'assurer que l'émetteur et le canal de communication sont toujours actifs. Le numéro consécutif est utilisé dans un mécanisme d'acquittement pour surveiller les *temps de propagation* entre l'émetteur et le destinataire. La valeur 0 est réservée pour la première exécution et pour la réaction à une erreur de communication. A l'inverse du mode V1, le mode V2 utilise des *compteurs 24 bits* pour la numérotation consécutive. Par conséquent, dans un mode cyclique, le numéro consécutif part de 1 à 0FF FF FFh, revenant à 1 à la fin.

NOTE Voir [48] pour plus de détails sur le mode V1.

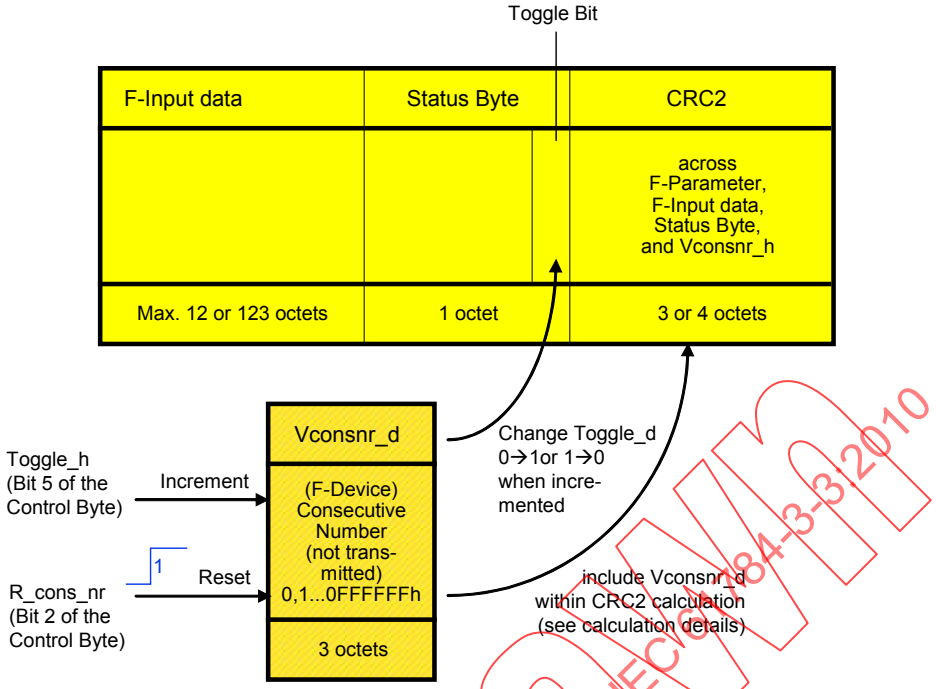


Légende

Anglais	Français
F host consecutive number	Numéro consécutif de l'hôte F
From F-host	De l'hôte F
From F-device	Du dispositif F
F device consecutive number	Numéro consécutif du dispositif F

Figure 23 – Fonction du bit de basculement

De même, à l'inverse du mode V1, le mode V2 ne transmet pas le numéro consécutif avec tous les PDU de sécurité. Il utilise un numéro consécutif virtuel à la place. Il est dit « virtuel » car il est invisible dans le PDU de sécurité. Cette approche s'appuie sur des compteurs 24 bits situés dans l'hôte F (Vconsnr_h) et le dispositif F (Vconsnr_d), un bit de basculement de l'octet d'état et de l'octet de contrôle incrémentant les compteurs appropriés de manière synchrone (Figure 23). L'exactitude et la synchronisation des deux compteurs indépendants sont vérifiées en intégrant les numéros consécutifs dans le calcul CRC2. CRC2 est ensuite transmis avec les PDU de sécurité (Figure 24).



Légende

Anglais	Français
Toggle bit	Bit de basculement
F-input data	Données d'entrée F
Status byte	Octet d'état
Across F-Parameter, F-Input data, Status Byte and Vconsnr_h	Parmi paramètre F, données d'entrée F, octet d'état et Vconsnr_h
Or	Ou
(bit .. of the Control Byte)	(bit ... de l'octet de contrôle)
F-device	Dispositif F
Consecutive number (not transmitted)	Numéro consécutif (non transmis)
Change ...when incremented	Faire passer ... ... ou ... lorsque incrémenté
Include ... within CRC2 calculation(see calculation details)	Inclure ... dans le calcul CRC2 (voir les détails du calcul)

Figure 24 – Numéro consécutif du dispositif F

La partie transmise du numéro consécutif (virtuel) est réduite à un bit de basculement, qui indique un incrément du compteur local. Les compteurs de l'hôte F et du dispositif F sont incrémentés à chaque front des bits de basculement (0→1, 1→0). La Figure 24 illustre le mécanisme du compteur dans le dispositif F. Le compteur est réinitialisé lorsque l'hôte F envoie R_cons_nr = "1" dans l'octet de contrôle (voir 7.1.3).

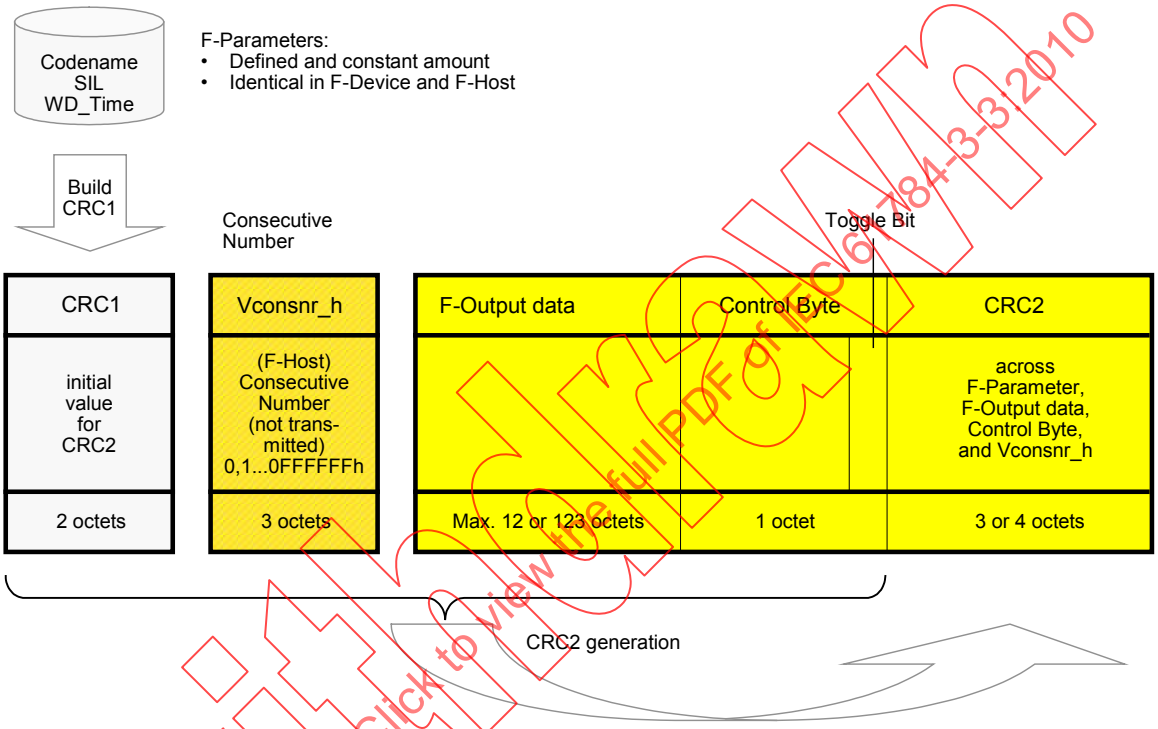
Le mécanisme du compteur dans l'hôte F correspond à celui du dispositif F. Toutefois, le compteur est réinitialisé à chaque fois qu'une erreur se produit (en interne ou par l'octet d'état). Ce compteur s'appelle Vconsnr_h.

7.1.5 Signature CRC2

Une fois les paramètres F (relation source-destination ou nom de code, SIL, temps de fonctionnement du chien de garde, etc.) transmis au dispositif F, les paramètres identiques sont utilisés dans une procédure identique dans l'hôte F et le dispositif F/module F pour produire une signature CRC1 à 2 octets (octet supérieur = 0) (*CRC1*). Pour plus

d'informations relatives à la conception de ce CRC1, voir 8.3.3.2. Cette signature CRC1, les données d'entrée-sortie F, l'octet d'état ou de contrôle et le numéro consécutif correspondant (Vconsnr_h ou Vconsnr_d) sont utilisés pour générer une autre signature CRC2 à 3 octets/4 octets (*CRC2*) dans l'hôte F (voir Figure 25). La signature CRC1 fournit la valeur initiale pour le calcul de CRC2 transmis de manière cyclique. Dans le dispositif F, la signature CRC identique est générée et les signatures sont comparées. Les transferts cycliques consécutifs requièrent uniquement une comparaison (très rapide) de signature CRC2.

Toutes les modifications apportées aux paramètres F stockés doivent être détectées et provoquer un état de sécurité du dispositif F. Les mécanismes de détection dépendent de la mise en œuvre individuelle des dispositifs F, et ne font pas l'objet de la présente partie.



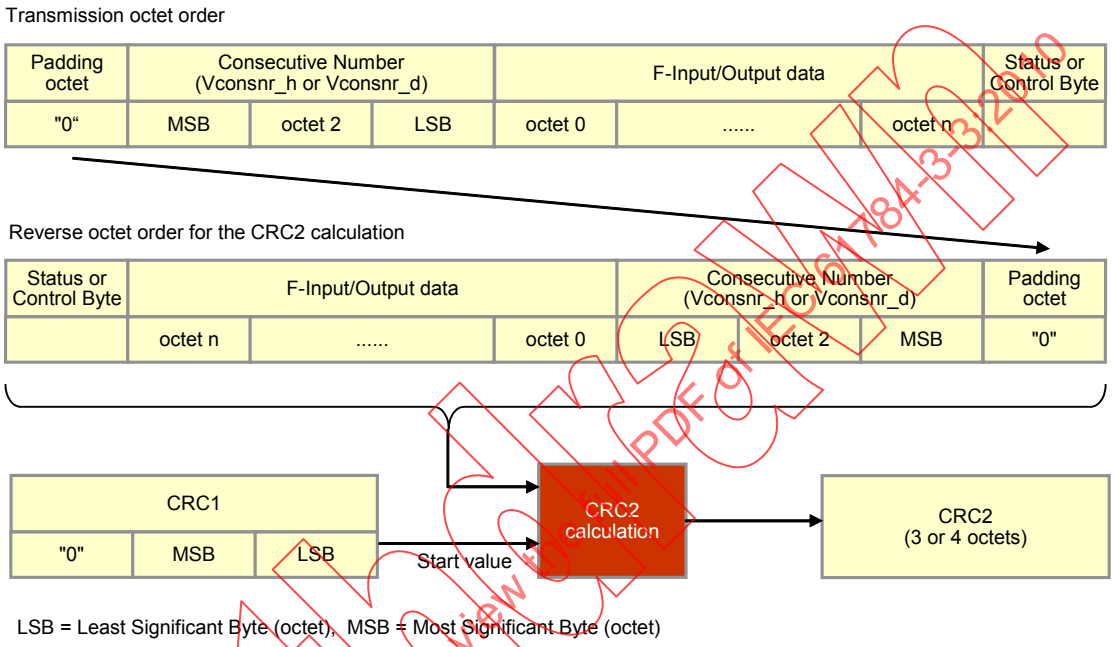
Légende

Anglais	Français
Codename	Nom de code
F-parameters	Paramètres F
Defined and constant amount	Quantité définie et constante
Identical in F-device and F-host	Identique dans dispositif F et hôte F
Build	Construire
Consecutive number	Numéro consécutif
Toggle bit	Bit de basculement
Across F-Parameter, F-Output data, Control Byte and Vconsnr_h	Parmi paramètre F, données d'entrée F, octet d'état et Vconsnr_h
Initial value for CRC2	Valeur initiale pour CRC2
F-host	Hôte F
Consecutive number (not transmitted)	Numéro consécutif (non transmis)
Or	Ou
CRC2 generation	Génération de CRC2

Figure 25 – Génération de CRC2 (sortie de l'hôte F)

Pour faciliter la détection des erreurs, même en présence de polynômes CRC identiques à l'intérieur du canal noir et de la couche de sécurité, le calcul CRC2 intègre les octets de la Figure 25 dans l'ordre inverse (Figure 26). Pour des raisons d'optimisation du traitement, les numéros consécutifs (Vconsnr_h ou Vconsnr_d) sont utilisés avec 4 octets dans les calculs, l'octet de remplissage supplémentaire étant 0. Il n'est pas recommandé d'utiliser un compteur 32 bits. Cela pourrait donner lieu à de trop longues et inacceptables durées d'essai des dispositifs pendant le processus d'essai et d'évaluation.

Pour éviter qu'un PDU de sécurité ne porte qu'un 0, une exception est faite dans ce cas particulier: la valeur 1 est attribuée à CRC2 au lieu de la valeur 0.



Légende

Anglais	Français
Transmission octet order	Ordre de transmission des octets
Padding octet	Octet de remplissage
Consecutive number	Numéro consécutif
Or	Ou
F-input/output data	Données d'entrée-sortie F
Status or control byte	Octet d'état ou de contrôle
Reverse octet ordre …	Ordre inverse des octets pour le calcul CRC2
CRC2 calculation	Calcul CRC2
LSB = …	LSB = octet de poids faible
MSB = …	MSB = octet de poids fort
Start value	Valeur de départ

Figure 26 – Détails du calcul CRC2 (ordre inverse)

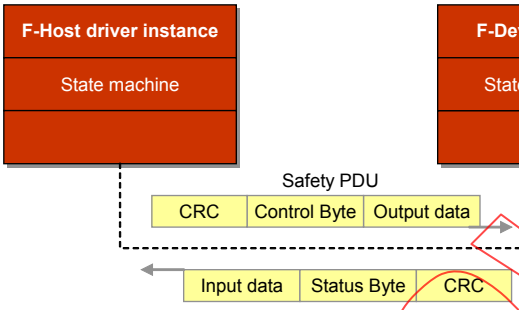
7.1.6 Données d'entrée-sortie standard ajoutées

Des données d'entrée-sortie standard peuvent être ajoutées à un PDU de sécurité. Pour les dispositifs F compacts, cela est possible en attribuant des identifications d'intervalle séparées. Les modules F des dispositifs modulaires peuvent utiliser ce mécanisme dans CP 3/RTE en raison de la modélisation en sous-intervalle.

7.2 Comportement FSCP 3/1

7.2.1 Généralités

Le cœur des couches de sécurité d'un hôte F et d'un dispositif F repose sur un diagramme d'états finis. Son mode de fonctionnement est défini par des diagrammes d'états et des diagrammes séquentiels dans 7.2.2 et 7.2.3. La Figure 27 présente un modèle simplifié de communication de sécurité. Un chronogramme particulier présenté en 7.2.5 illustre les conséquences d'une anomalie du signal de réinitialisation du compteur de numéros consécutifs. La surveillance des temps de passage du PDU de sécurité est présentée en 7.2.6.



Légende

Anglais	Français
F-host driver instance	Instance de pilote d'hôte F
State machine	Diagramme d'états
F-device driver	Pilote de dispositif F
Safety PDU	PDU de sécurité
Control byte	Octet de contrôle
Output data	Données de sortie
Input data	Données d'entrée
Status byte	Octet d'état

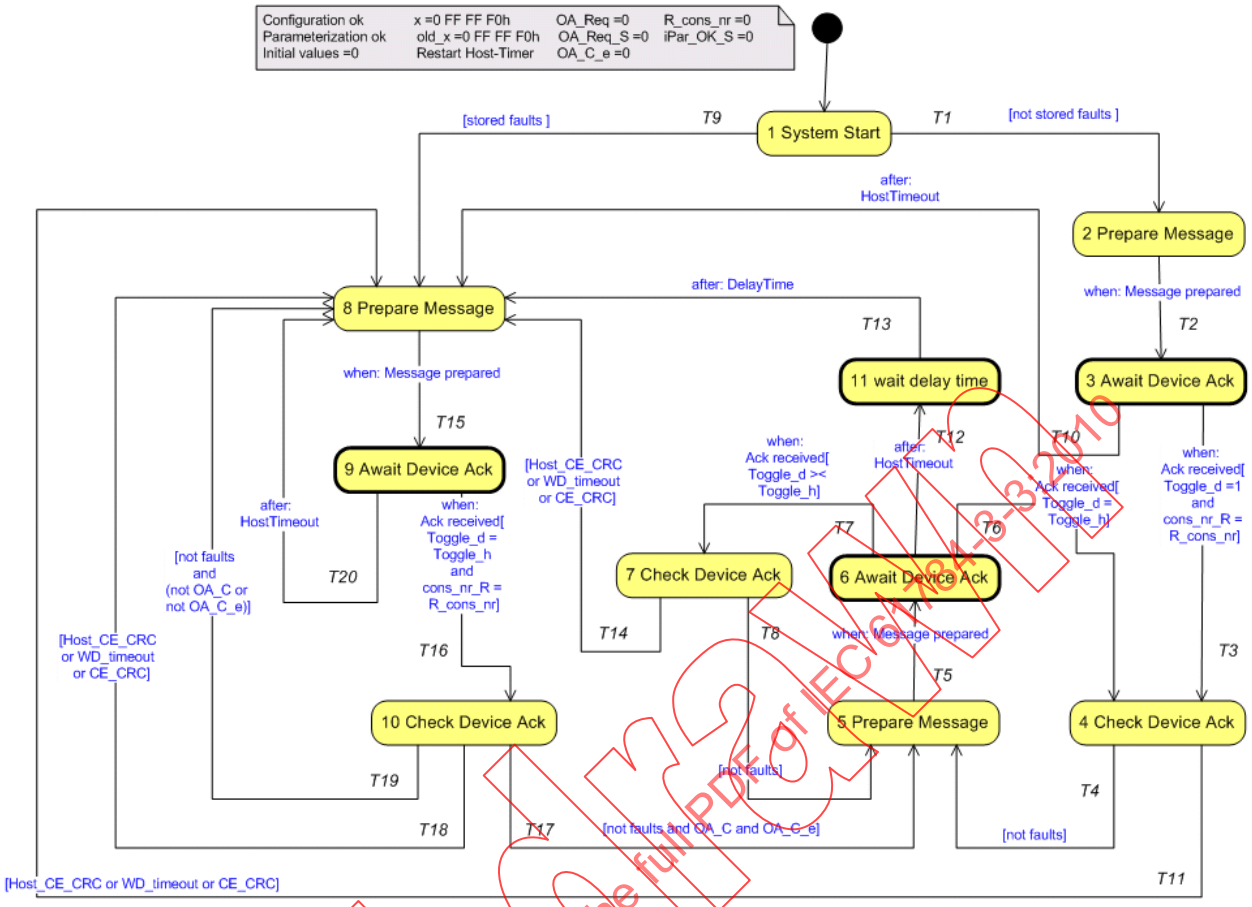
Figure 27 – Relation de communication de la couche de sécurité

7.2.2 Diagramme d'états de l'hôte F

La Figure 28 illustre le diagramme d'états de l'hôte F, et le Tableau 4 décrit les états, les transitions et les éléments internes de l'hôte F. Les diagrammes suivent la notation UML2. Les transitions sont supprimées si un événement se produit (la réception d'un message, par exemple). Si plusieurs transitions sont possibles, les protections [conditions] définissent la transition à supprimer.

Les états 4, 7 et 10 (Vérification de l'acquittement du dispositif) sont appelés états de changement conformément à UML2 sans événement « externe ». Les transitions correspondantes sont supprimées après évaluation des valeurs internes.

Le diagramme est composé d'états d'activité et d'action. Les états d'activité sont encadrés par des lignes en gras, et les actions d'état par des lignes minces. Les états d'activité peuvent être interrompus par de nouveaux événements, ce qui n'est pas le cas des états d'action. Les événements qui composent un état d'action (les délais, les messages reçus ou les acquittements de l'opérateur, par exemple) sont différés jusqu'à l'état d'activité suivant.



Légende

Anglais	Français
Parameterization	Paramétrage
Initial values	Valeurs initiales

Figure 28 – Diagramme d'états de l'hôte F

Les termes utilisés dans la Figure 28 sont spécifiés ci-dessous:

Valeurs initiales	valeurs du PDU de sécurité = 0
HostTimeout	l'hôte F reconnaît le délai local lorsqu'il attend un acquittement du dispositif F
Host_CE_CRC	l'hôte F reconnaît l'anomalie CRC lors de l'analyse du PDU de sécurité reçu
Device_Fault	le dispositif F a signalé une défaillance à l'hôte; bit d'état 1 = 1.
CE_CRC	le dispositif F a signalé une anomalie CRC à l'hôte F; bit d'état 2 = 1
OA_C_e	Drapeau auxiliaire indiquant un front montant du signal OA_C (0 → 1)
WD_timeout	le dispositif F a signalé une anomalie de délai d'attente à l'hôte F; bit d'état 3 = 1
[pas d'anomalie]	notation UML d'une condition (protection) pour supprimer la transition. Dans ce cas, cette variable est « true » (=1) si aucun des bits ci-dessous n'est défini: - Host_CE_CRC ou - CE_CRC ou - WD_timeout
[anomalies	Cette variable est « true » (=1) si l'un des bits ci-dessous a été stocké: - Host_CE_CRC ou

stockées] - HostTimeout ou
- CE_CRC ou
- WD_timeout

Tableau 4 – États et transitions de l'hôte F

NOM D'ETAT	DESCRIPTION DE L'ETAT
1 Démarrage du système	État initial de l'instance du pilote de l'hôte F lors de la mise sous tension. S'il est prévu qu'un système stocke les anomalies, la transition T9 doit être mise en œuvre. Sinon, le système utilise la transition T1 uniquement.
2 Préparation du message	Préparation d'un PDU de sécurité *régulier* pour le dispositif F
3 Attente de Device Ack (l'acquittement du dispositif)	La couche de sécurité attend le PDU de sécurité régulier suivant provenant du dispositif F (Acquittement).
4 Vérification de Device Ack (l'acquittement du dispositif)	Vérification du PDU de sécurité reçu pour une *erreur CRC* (Host_CE_CRC) comprenant le numéro consécutif virtuel (x), et pour les potentielles *anomalies du dispositif F* dans l'octet d'état (WD_timeout, CE_CRC)
5 Préparation du message	Préparation d'un PDU de sécurité *régulier* pour le dispositif F
6 Attente de Device Ack (l'acquittement du dispositif)	La couche de sécurité attend le PDU de sécurité régulier suivant provenant du dispositif F (Acquittement)
7 Vérification de Device Ack (l'acquittement du dispositif)	Vérification du PDU de sécurité reçu pour une *erreur CRC* (Host_CE_CRC) comprenant l'ancien (old_x) numéro consécutif virtuel (x), et pour les potentielles *anomalies du dispositif F* dans l'octet d'état (WD_timeout, CE_CRC)
8 Préparation du message	Préparation d'un PDU de sécurité pour le dispositif F (traitement des exceptions)
9 Attente de Device Ack (l'acquittement du dispositif)	La couche de sécurité attend le PDU de sécurité irrégulier suivant provenant du dispositif F (Acquittement)
10 Vérification de Device Ack (l'acquittement du dispositif)	Vérification du PDU de sécurité reçu pour une *erreur CRC* (Host_CE_CRC) comprenant le numéro consécutif virtuel (x), et pour les potentielles *anomalies du dispositif F* dans l'octet d'état (WD_timeout, CE_CRC). Une fois survenue l'anomalie, aucun redémarrage automatique d'une fonction de sécurité n'est admis tant qu'un signal d'acquittement de l'opérateur (OA_C) n'est pas arrivé.
11 Délai d'attente	Cet état permet d'éviter le stockage d'une anomalie de délai d'attente en cas d'arrêt occasionnel du système, ce qui engendrerait une demande d'acquittement de l'opérateur à la prochaine mise sous tension. Un délai d'attente de 0 ms est admis.

TRAN-SITION	ETAT SOURCE	ETAT CIBLE	ACTION
T1	1	2	use FV, activate_FV =1, FV_activated_S =1 Toggle_h =1
T2	2	3	send safety PDU
T3	3	4	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

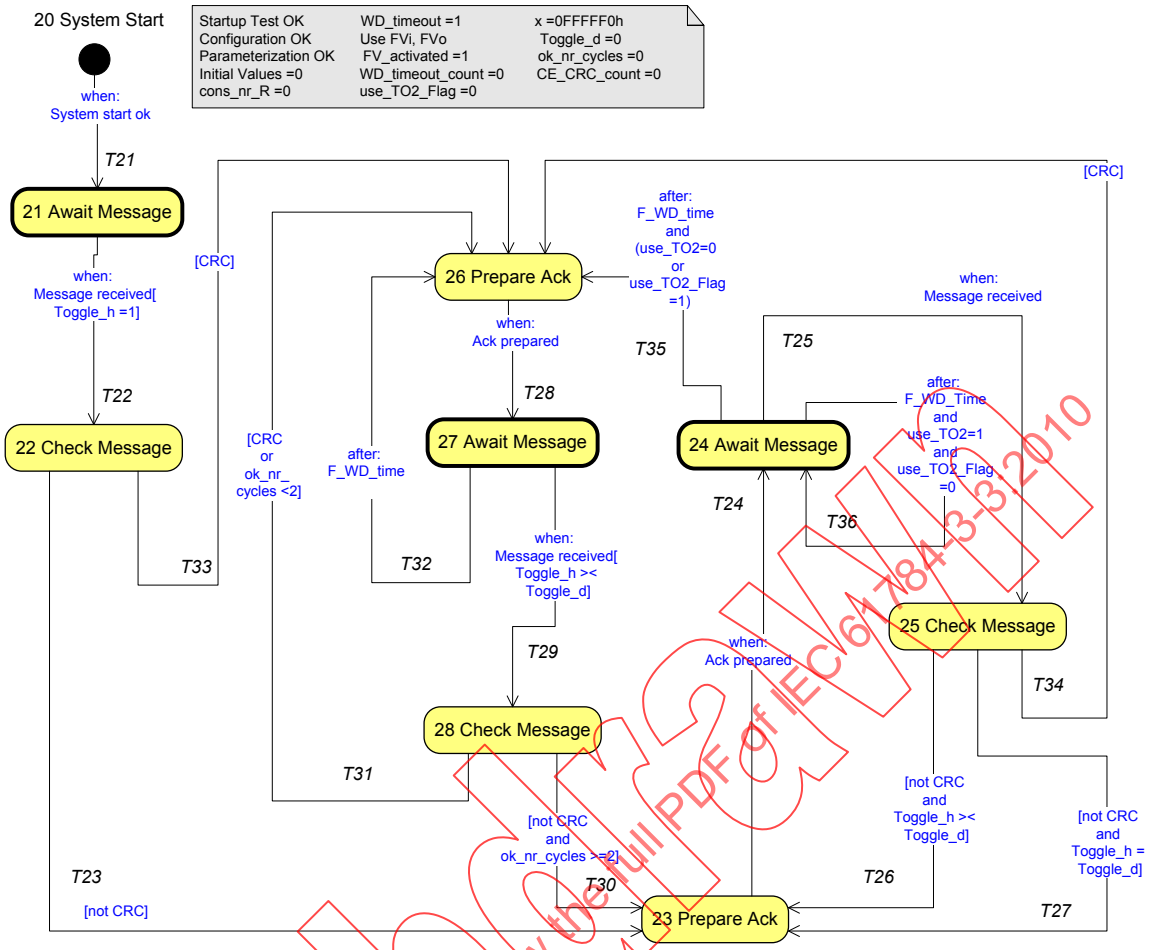
TRAN-SITION	ETAT SOURCE	ETAT CIBLE	ACTION
			iPar_OK_S =iPar_OK
T9[a]	1	8	use FV, activate_FV =1, FV_activated_S =1, Toggle_h =1, R_cons_nr =1, x =0
T10	3	8	restart host-timer, store faults, use FV, activate_FV =1, FV_activated_S =1, Toggle_h = not Toggle_h, R_cons_nr =1, x =0
T11	4	8	store faults, use FV, activate_FV =1, FV_activated_S =1, Toggle_h = not Toggle_h, R_cons_nr =1, x =0
T12	6	11	use FV, activate_FV =1, FV_activated_S =1, R_cons_nr =1, x =0
T13	11	8	store faults, Toggle_h = not Toggle_h, restart host-timer
T14	7	8	restart host-timer, store faults, use FV, activate_FV =1, FV_activated_S =1, Toggle_h = not Toggle_h, R_cons_nr =1, x =0
T15	8	9	send safety PDU
T16	9	10	restart host-timer
T17	10	5	reset stored faults, OA_Req_S =0, OA_Req =0, OA_C_e =0, R_cons_nr =0, 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
T18	10	8	store faults, OA_Req =0, OA_Req_S =0, OA_C_e =0, use FV, activate_FV =1, FV_activated_S =1, Toggle_h = not Toggle_h, R_cons_nr =1, x =0
T19	10	8	OA_Req_S =1, OA_Req =1, **if** OA_C =0 **then** OA_C_e =1 use FV, activate_FV =1, FV_activated_S =1, Toggle_h = not Toggle_h, R_cons_nr =0, old_x =x, x =x+1, **if** x =01000000h **then** x =1

TRAN-SITION	ETAT SOURCE	ETAT CIBLE	ACTION
T20	9	8	store faults, OA_Req =0, OA_Req_S =0, OA_C_e =0, use FV, activate_FV =1, FV_activated_S =1, Toggle_h = not Toggle_h, R_cons_nr =1, x =0, restart host-timer
a La mise en œuvre de la transition T9 dépend du concept de sécurité d'un fabricant de système particulier.			

ELEMENTS INTERNES	TYPE	DEFINITION
x	Compteur	x représente le numéro consécutif local dans l'instance du pilote de l'hôte F. Il n'est pas transmis à son homologue dans le dispositif F, mais assure la synchronisation par l'intermédiaire d'un bit de basculement de l'octet de contrôle. La valeur x réelle du compteur est intégrée dans le calcul CRC2 et donc vérifiée par rapport aux défauts de transmission. La plage de valeurs est comprise entre 0 et 0FFFFFFh. Lors du démarrage, ce compteur incrémentiel est défini sur 0FFFFF0h et démarre de cet endroit. L'hôte F incrémente le numéro consécutif virtuel après chaque réception acquittée du numéro consécutif virtuel respectif de son module de dispositif F 0FFFFFFh, en ignorant la valeur 0 et en poursuivant par 1.
old_x	Compteur	Valeur précédente du numéro consécutif local en cours x. Il est nécessaire de la stocker afin de distinguer le cycle initial des cycles ultérieurs.
DelayTime	Temporisateur	Ce délai d'attente permet de couvrir le temps de stabilisation à la mise hors tension de l'ensemble du système. Le fabricant de l'hôte/du système est chargé de définir ce paramètre.
host-timer	Temporisateur	Ce temporisateur permet de vérifier si le PDU de sécurité valide suivant provenant du dispositif F arrive à temps. L'outil de développement de l'hôte est chargé de définir ce temps de fonctionnement du chien de garde. La plage de valeurs est comprise entre 0 et 65 535 ms.
OA_C_e	Drapeau	Grâce à cette variable (bit) auxiliaire, l'état de sécurité est maintenu tant qu'un signal de changement OA_C de 0 → 1 (front) n'a pas été reçu. Sans l'aide de ce mécanisme, un opérateur pourrait annuler des états de sécurité en activant définitivement le signal OA_C.
faults	Drapeaux	Tant qu'un acquittement de l'opérateur (OA_C) n'a pas été reçu, les anomalies suivantes doivent être stockées en permanence dans l'hôte F uniquement (et pas dans l'hôte F): - Host_CE_CRC - HostTimeout - CE_CRC (bit d'état 2) - WD_timeout (bit d'état 3)
	État d'activité	Dans ces états d'activité qu'il est possible d'interrompre, les hôtes attendent de nouvelles entrées (un délai d'attente ou un acquittement, par exemple) [34].
	État d'action	Dans ces états d'action qu'il est impossible d'interrompre, les événements (délai d'attente, message reçu ou acquittement de l'opérateur, par exemple) sont différés jusqu'à l'état d'activité suivant [34].

7.2.3 Diagramme d'états du dispositif F

La Figure 29 illustre le diagramme d'états du dispositif F, et le Tableau 5 décrit les états, les transitions et les éléments internes. Les diagrammes suivent la notation UML2.



Légende

Anglais	Français
Parameterization	Paramétrage
Initial values	Valeurs initiales
Startup test	Essai de démarrage

Figure 29 – Diagramme d'états du dispositif F

Les termes utilisés dans la Figure 29 sont spécifiés ci-dessous:

[Toggle_h = Toggle_d]	notation UML d'une condition (protection) pour supprimer la transition. Dans ce cas, elle signifie: La valeur du bit Toggle_h n'a pas changé ("pas de basculement")
[Toggle_h >< Toggle_d]	La valeur du bit Toggle_h a changé ("basculement")
[CRC]	Le dispositif F reconnaît l'anomalie CRC (erreur de communication et/ou de numéro consécutif)
F_WD_Time	Temps de fonctionnement du chien de garde défini par le paramètre F F_WD_Time
use_TO2	CB3 de l'octet de contrôle indiquant l'utilisation du temps de fonctionnement du chien de garde secondaire F_WD_Time_2
use_TO2_Flag	Drapeau auxiliaire
Ack	Acquittement du PDU de sécurité du dispositif F
Message reçu	tous les nouveaux PDU reçus; ignorer les PDU de sécurité avec les valeurs = 0

Tableau 5 – États et transitions du dispositif F

NOM D'ETAT	DESCRIPTION DE L'ETAT
20 Démarrage du système	État initial du dispositif lors de la mise sous tension. Lors de la mise sous tension, la valeur du dispositif F de *sortie* est 0. Immédiatement après le paramétrage F, les valeurs Failsafe sont définies. Lors de la mise sous tension, le dispositif F *d'entrée* envoie 0. Immédiatement après le paramétrage F, il envoie des valeurs de processus.
21 Attente de message	La couche de sécurité attend le PDU de sécurité suivant provenant de l'hôte F
22 Vérification de message	Vérification du PDU de sécurité reçu pour l'*erreur* CRC, y compris le numéro consécutif virtuel
23 Préparation de l'acquittement	Préparation d'un PDU de sécurité *régulier* pour l'hôte F (Acquittement)
24 Attente de message	La couche de sécurité attend le PDU de sécurité régulier suivant provenant de l'hôte F
25 Vérification de message	Vérification du PDU de sécurité reçu pour l'*erreur* CRC, y compris le numéro consécutif virtuel
26 Préparation de l'acquittement	Préparation d'un PDU de sécurité pour l'hôte F (Acquittement avec bits erronés)
27 Attente de message	La couche de sécurité attend le PDU de sécurité suivant provenant de l'hôte F (traitement des exceptions)
28 Vérification de message	Vérification du PDU de sécurité reçu pour l'*erreur CRC*, y compris le numéro consécutif virtuel

TRAN-SITION	ETAT SOURCE	ETAT CIBLE	ACTION
T21	20	21	-
T22	21	22	**if** R_cons_nr =1 **then** x=0, cons_nr_R =1
T23	22	23	use PVi, FVo, FV_activated =1, CE_CRC =0, WD_timeout =0, Toggle_d = Toggle_h, restart device-timer, ok_nr_cycles =ok_nr_cycles +1
T24	23	24	send safety PDU
T25	24	25	**if** Toggle_h >< Toggle_d **then** restart device-timer x=x+1, **if** x =01000000h **then** x =1, cons_nr_R =0 **if** R_cons_nr =1 **then** x=0, cons_nr_R =1 **if** use_TO2 =0 **then** use_TO2_Flag =0
T26	29	23	Use PVi, Toggle_d = Toggle_h, **if** ok_nr_cycles <4 ok_nr_cycle =ok_nr_cycle +1 **if** ok_nr_cycles <4 **then** use FVo, FV_activated =1 **else** use PVo, FV_activated =0 **if** activate_FV =1 **then** use FVo **else** use PVo
T27	25	23	Use PVi, Toggle_d = Toggle_h, **if** ok_nr_cycles <4 **then** use FVo, FV_activated =1 **else** use PVo, FV_activated =0 **if** activate_FV =1 **then** use FVo **else** use PVo

TRAN-SITION	ETAT SOURCE	ETAT CIBLE	ACTION
T28	26	27	Send safety PDU

T29	27	28	**if** R_cons_nr =1
			then x=0, cons_nr_R =1
			else x=x+1,
			  if x =01000000h
			  then x =1, cons_nr_R =0

T30	28	23	use PVi, FVo, FV_activated =1, Toggle_d = Toggle_h, restart device-timer, ok_nr_cycles =ok_nr_cycles +1

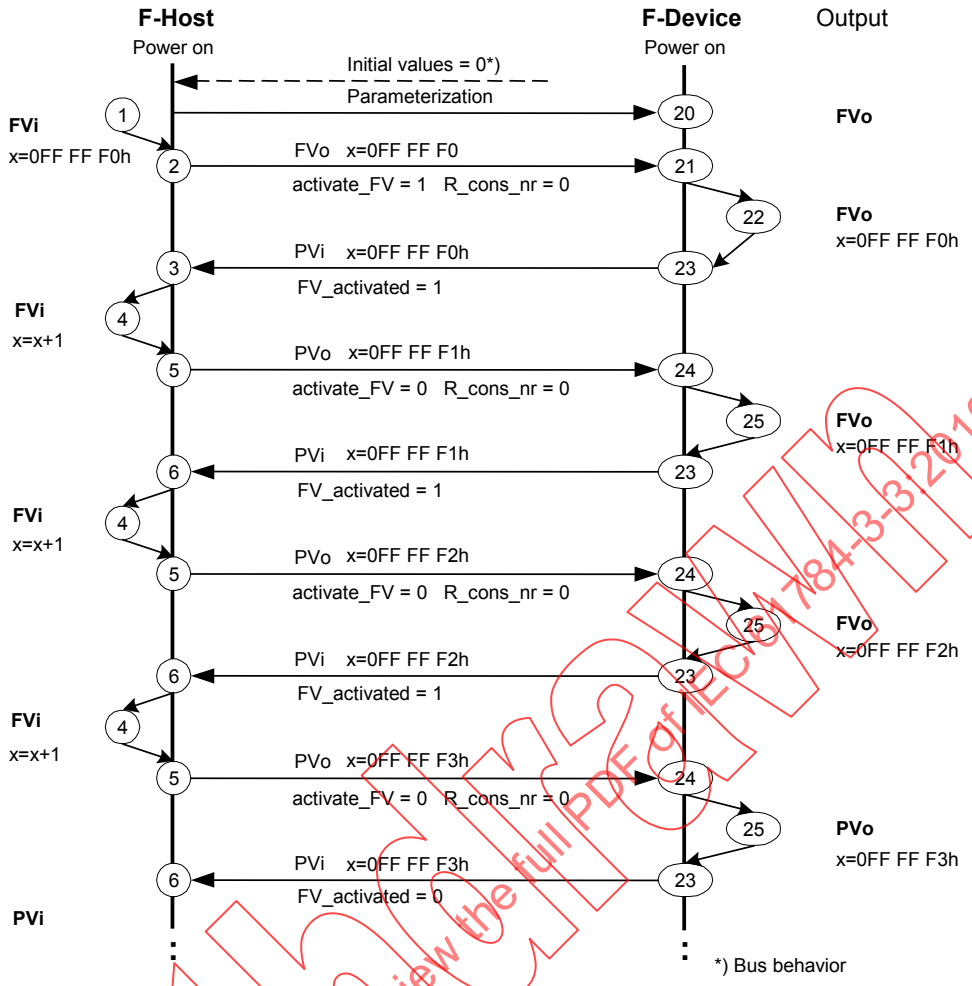
T31	28	26	Toggle_d = Toggle_h,
			restart device-timer,
			if CRC
			then
			  CE_CRC =1,
			  CE_CRC_count =1,
			  ok_nr_cycles =0,
			else
			  ok_nr_cycles =ok_nr_cycles +1,
			  if CE_CRC_count >0
			  then
			  CE_CRC =1,
			  CE_CRC_count = CE_CRC_count -1,
			  else CE_CRC =0,
			if WD_timeout_count >0
			then
			  WD_timeout =1,
			  WD_timeout_count = WD_timeout_count -1
			else WD_timeout =0

T32	27	26	Use PVi, FVo, FV_activated =1, WD_timeout =1, WD_timeout_count =1, ok_nr_cycles =0, restart device timer, Toggle_d = Toggle_h
T33	22	26	Use PVi, FVo, FV_activated =1, CE_CRC =1, CE_CRC_count =1, WD_timeout =0, ok_nr_cycles =0, restart device-timer, Toggle_d = Toggle_h
T34	25	26	Use PVi, FVo, FV_activated =1, CE_CRC =1, CE_CRC_count =1, ok_nr_cycle =0, restart device-timer, Toggle_d = Toggle_h
T35	24	26	Use PVi, FVo, FV_activated =1, WD_timeout =1, WD_timeout_count =1, ok_nr_cycles =0, restart device timer, Toggle_d = Toggle_h
T36	24	24	restart device timer with F_WD_Time_2 use_TO2_Flag =1

ELEMENTS INTERNES	TYPE	DEFINITION
x	Compteur	x représente le numéro consécutif local dans le dispositif F. Il n'est pas transmis à son homologue dans l'hôte F, mais est synchronisé par l'intermédiaire d'un bit de basculement de l'octet de contrôle. Cela signifie qu'il est incrémenté à chaque fois que l'état du bit de basculement de l'octet de contrôle (Toggle_h) change du module de comptage 0 FF FF FFh 0 → 1 ou 1 → 0, en ignorant la valeur 0 et en continuant par 1. La valeur x du compteur est remise à zéro si une valeur (1) est attribuée au bit de contrôle R_cons_nr. La valeur x respective du compteur est intégrée dans le calcul CRC2 et donc vérifiée par rapport aux défauts de transmission. La plage de valeurs est comprise entre 0 et 0 FF FF FFh. Lors du démarrage, ce compteur incrémentiel est défini sur 0 FF FF F0h et démarre de cet endroit.
ok_nr_cycles	Compteur	Lors du démarrage et après une anomalie, le dispositif F doit définir FVo et FV_activated = 1 pendant au moins 3 cycles. Ce compteur incrémentiel ok_nr_cycles est chargé de compter ces cycles de 0 à 3.
CE_CRC_count	Compteur	Ce compteur décrémentiel permet de s'assurer que le bit CE_CRC de l'octet d'état est défini pour au moins 1 cycle ou 2 cycles au maximum. La plage de valeurs est comprise entre 0 et 1.
WD_timeout_count	Compteur	Ce compteur décrémentiel permet de s'assurer que le bit WD_timeout de l'octet d'état est défini pour au moins 1 cycle ou 2 cycles au maximum. La plage de valeurs est comprise entre 0 et 1.
device-timer	Temporisateur	Ce temporisateur permet de vérifier si le PDU de sécurité valide suivant est arrivé à temps. Le paramètre F « F_WD_Time » permet de définir ce temps de fonctionnement du chien de garde. La plage de valeurs est comprise entre 0 et 65 535 ms.

7.2.4 Diagrammes séquentiels

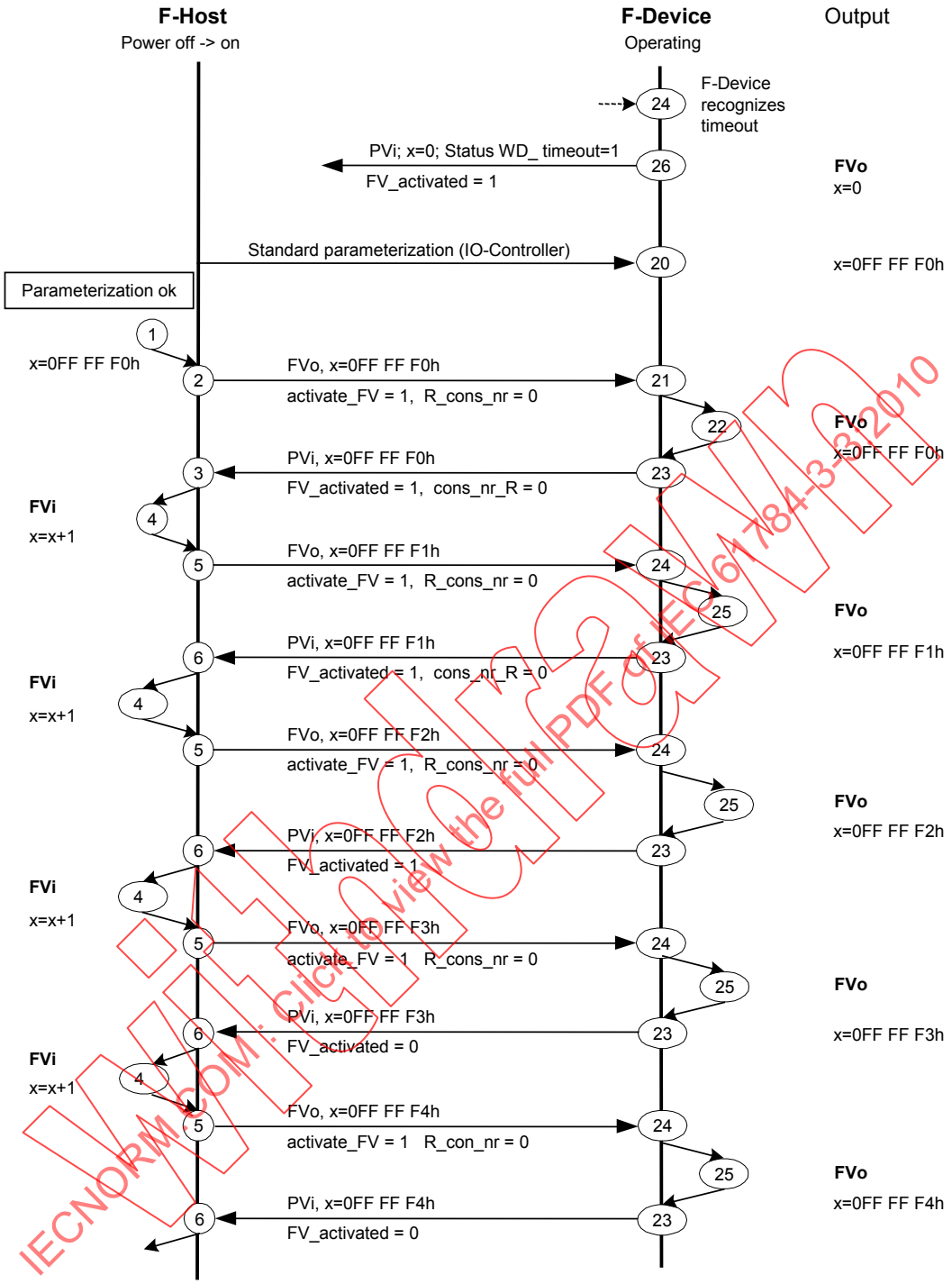
Les Figures 30 à 33 illustrent les messages d'interaction de l'hôte F et du dispositif F pendant la phase de démarrage. Trois phases sont présentées: lors du démarrage, les deux partenaires, l'hôte F ou le dispositif F commute(nt) temporairement la mise hors tension pendant le fonctionnement de leur partenaire. Les figures donnent des informations sur les états et les transitions correspondantes. Les numéros placés dans des cercles représentent les états que traversent respectivement l'hôte F et le dispositif F.



Légende

Anglais	Français
F-host	Hôte F
Power on	Sous tension
F-device	Dispositif F
Output	Sortie
Initial values	Valeurs initiales
Parameterization	Paramétrage
Bus behavior	Comportement du bus

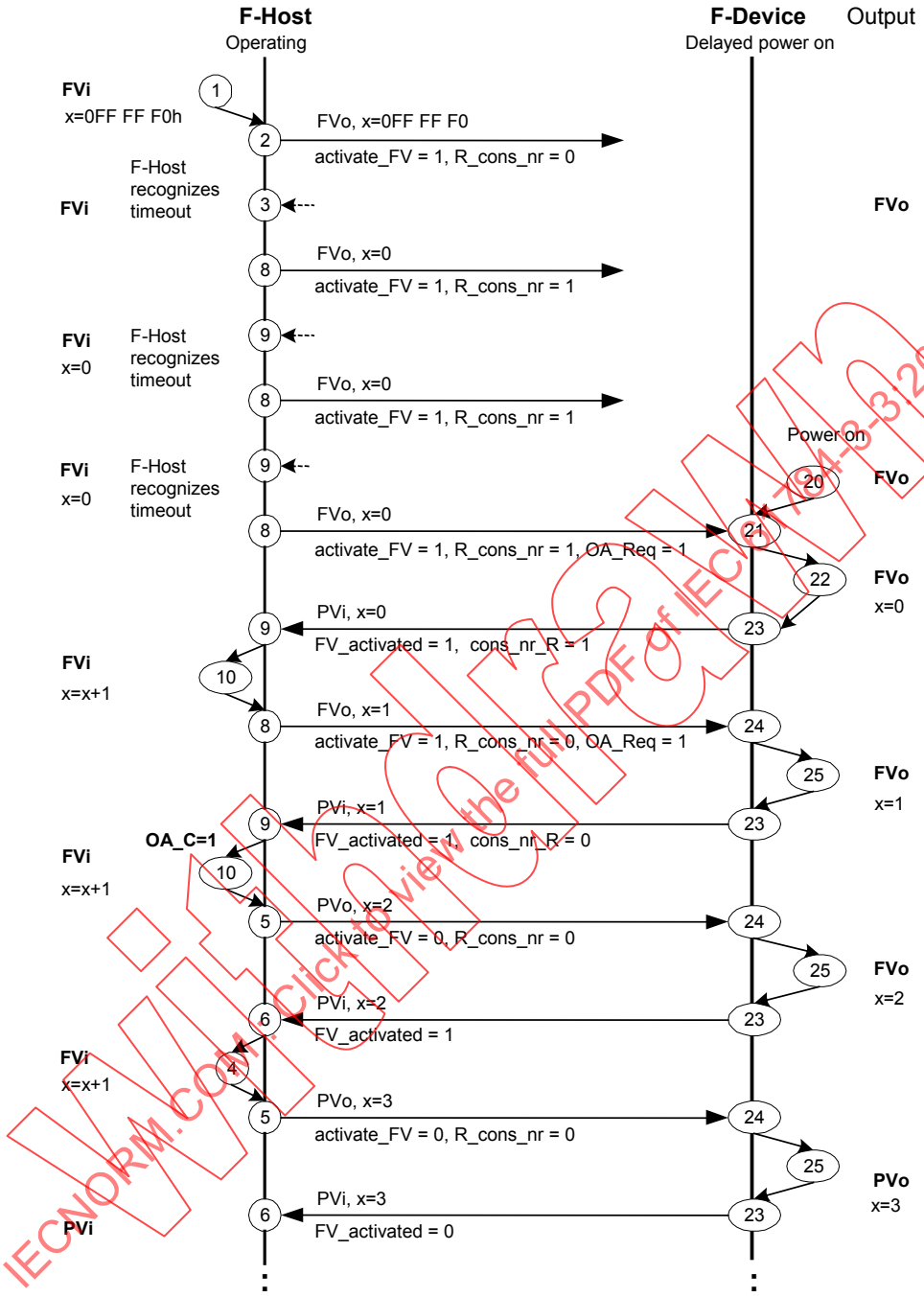
Figure 30 – Interaction de l'hôte F et du dispositif F pendant le démarrage



Légende

Anglais	Français
F-host	Hôte F
Power off -> on	hors tension -> sous tension
F-device	Dispositif F
Output	Sortie
Operating	En fonctionnement
Parameterization	Paramétrage
F-device recognizes timeout	Le dispositif F reconnaît la temporisation
Status	Etat
Standard parameterization (IO controller)	Paramétrage standard (contrôleur d'entrée-sortie)

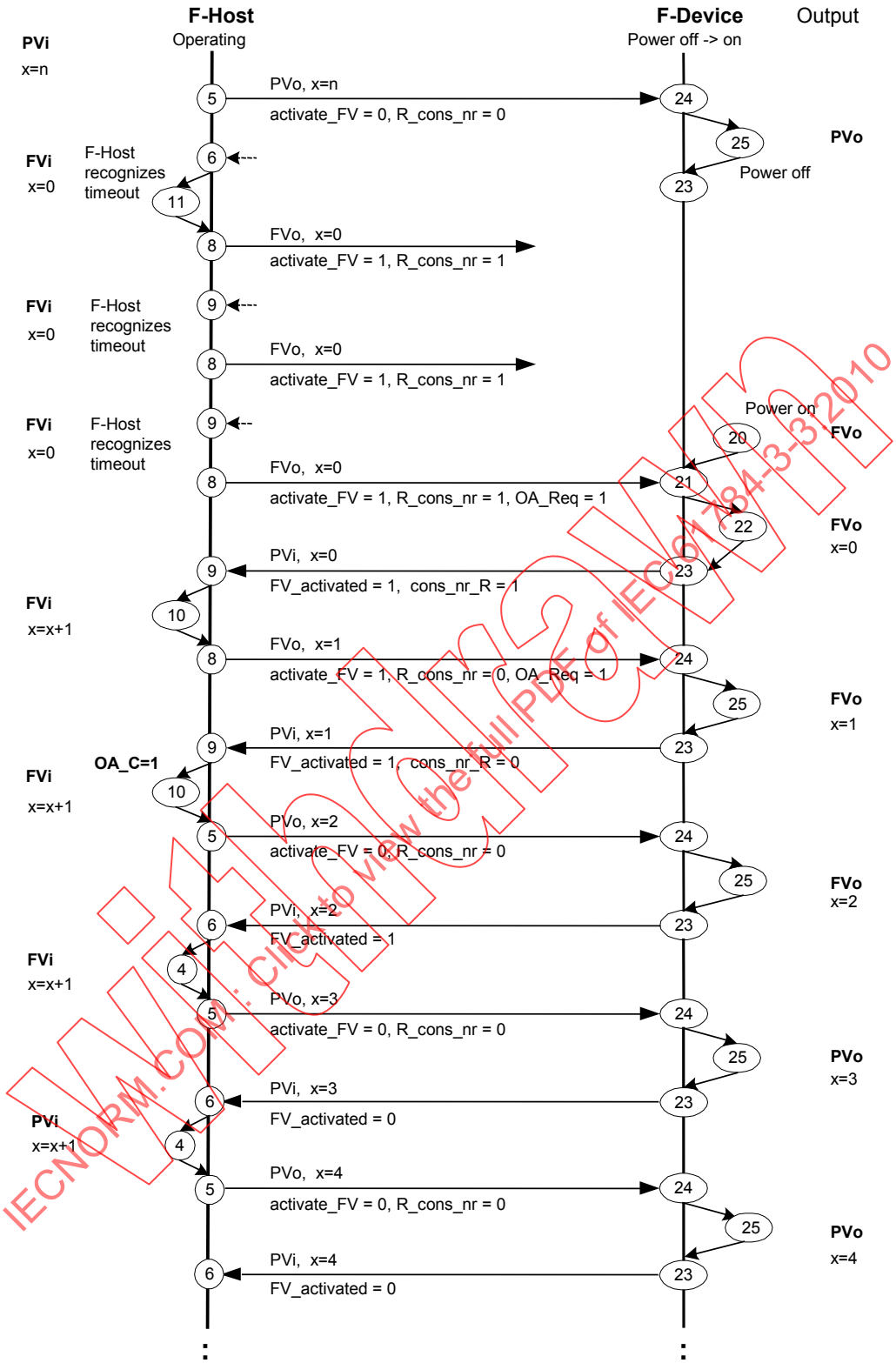
Figure 31 – Interaction de l'hôte F et du dispositif F pendant la mise hors tension de l'hôte F → sous tension



Légende

Anglais	Français
F-host	Hôte F
Delayed power on	mise sous tension retardée
F-device	Dispositif F
Output	Sortie
Operating	En fonctionnement
Power on	Sous tension
F-host recognizes timeout	L'hôte F reconnaît la temporisation

Figure 32 – Interaction de l'hôte F et du dispositif F pendant un report de mise sous tension

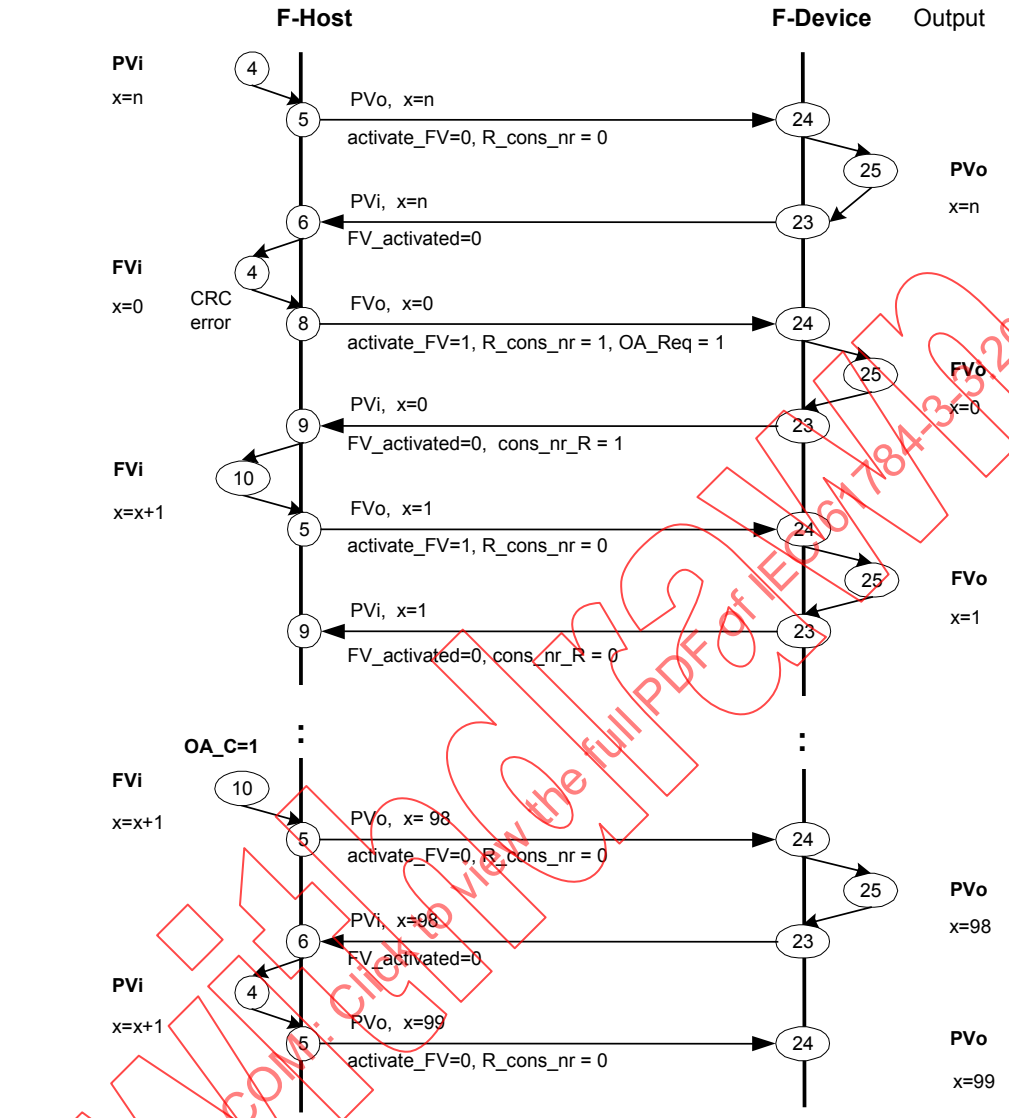


Légende

Anglais	Français
F-host	Hôte F
Power off -> on	hors tension -> sous tension
F-device	Dispositif F
Output	Sortie
Operating	En fonctionnement
F-host recognizes timeout	L'hôte F reconnaît la temporisation
Power on	Sous tension
Power off	Hors tension

Figure 33 – Interaction de l'hôte F et du dispositif F pendant la mise hors tension → sous tension

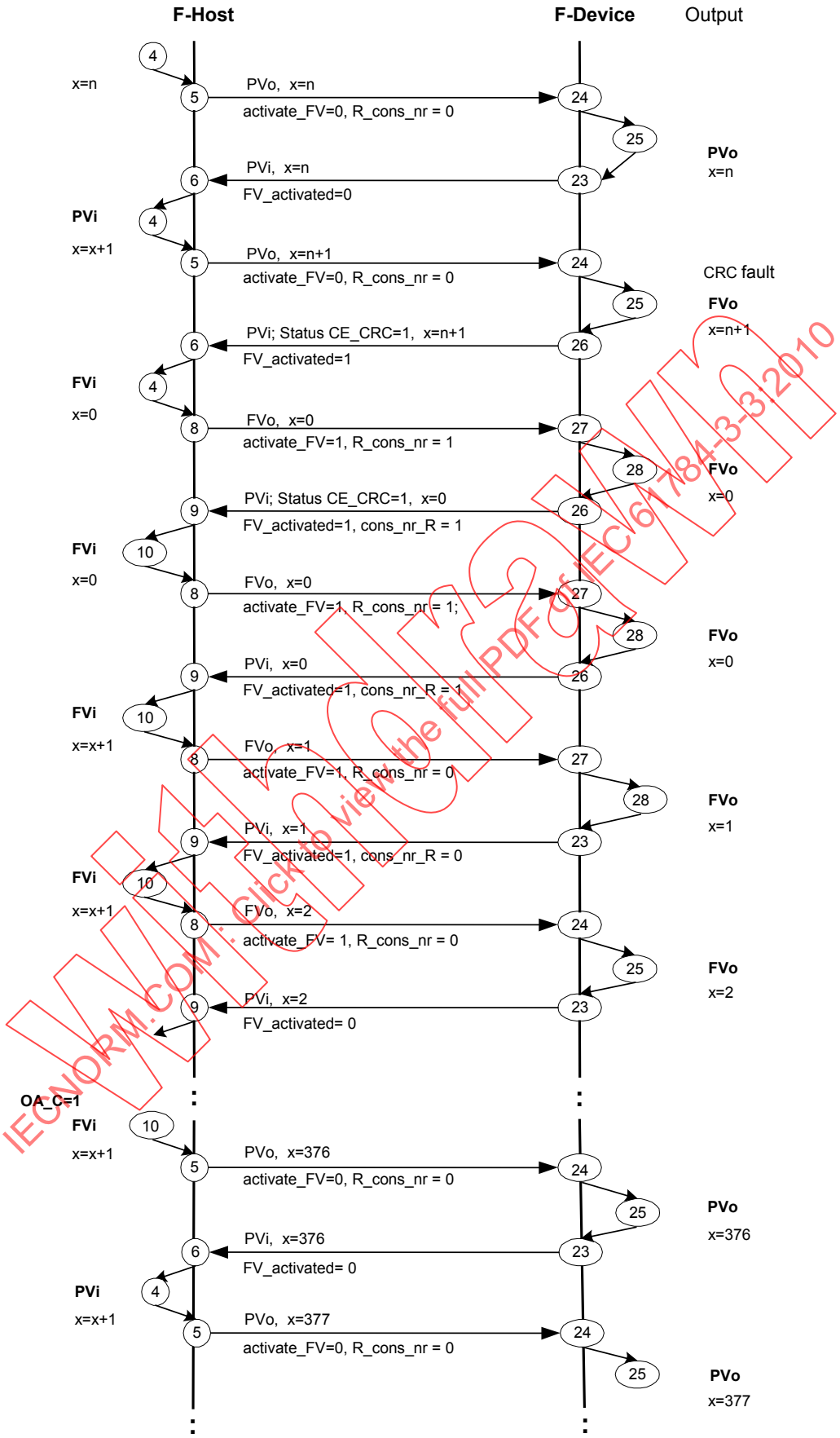
Les Figures 34 et 35 présentent les messages d'interaction entre l'hôte F et le dispositif F lorsque des anomalies CRC sont détectées d'un côté ou de l'autre.



Légende

Anglais	Français
F-host	Hôte F
F-device	Dispositif F
Output	Sortie

Figure 34 – Interaction de l'hôte F et du dispositif F lorsque l'hôte détecte une erreur CRC



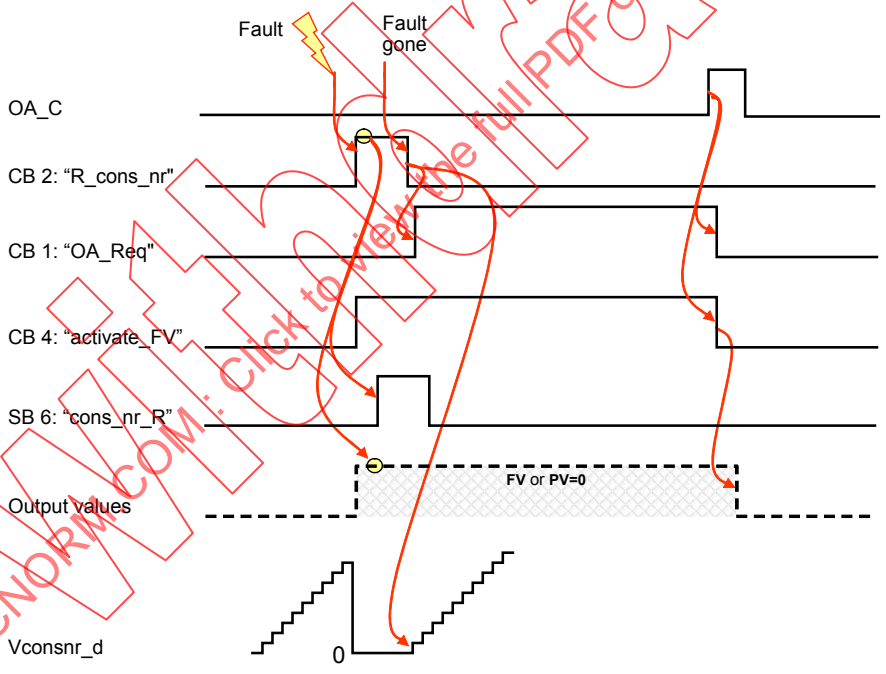
Légende

Anglais	Français
F-host	Hôte F
F-device	Dispositif F
Output	Sortie
CRC fault	Anomalie CRC

Figure 35 – Interaction de l'hôte F et du dispositif F lorsque le dispositif détecte une erreur CRC

7.2.5 Chronogramme de réinitialisation d'un compteur

La Figure 36 présente les conséquences d'un défaut de communication F sur le compteur de numéros consécutifs et les éléments dépendants. Suite à ce type d'anomalie uniquement, une valeur est attribuée au bit 2 de l'octet de contrôle R_cons_nr (=1), les valeurs de sortie d'un dispositif de sortie F étant donc également nulles et la valeur 0 étant attribuée au compteur de numéros consécutifs (Vconsnr_d). Dans le même temps, une valeur (=1) est attribuée au bit 4 de l'octet de contrôle activate_FV, ce qui oblige le dispositif de sortie F à définir son propre état de sécurité intégrée à chaque fois qu'il ne peut être obtenu par des valeurs de sortie régulières (FV).



Légende

Anglais	Français
Fault	Défaut
Fault gone	Défaut corrigé
Output values	Valeurs de sortie
Or	ou

Figure 36 – Impact du signal de réinitialisation du compteur

Au même moment, l'hôte F envoie le signal OA_Req en tant que bit 1 de l'octet de contrôle au dispositif F. Ce signal peut être utilisé pour indiquer à l'utilisateur, via la DEL (9.1), qu'une erreur s'est produite et qu'un acquittement de l'opérateur est demandé (OA_C). Immédiatement après la résolution de l'anomalie, les actions ci-dessous se déroulent:

- la réinitialisation du compteur reprend sa valeur par défaut (R_cons_nr = 0);
- le compteur de numéros consécutifs reprend le comptage.

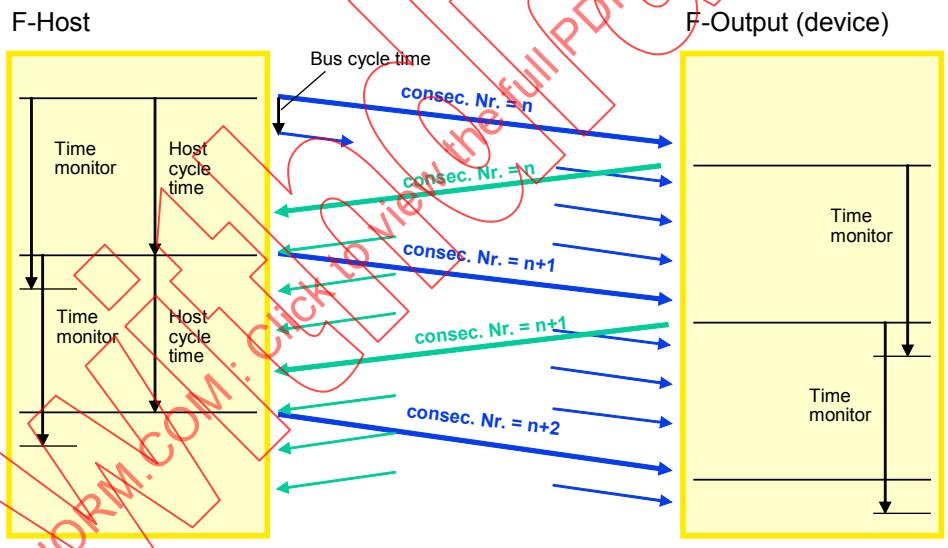
Immédiatement après un acquittement de l'opérateur (OA_C = 1), les actions ci-dessous se déroulent:

- la demande d'un acquittement de l'opérateur reprend sa valeur par défaut (OA_Req = 0);
- la demande d'activation d'un état de sortie de sécurité intégrée reprend sa valeur par défaut (activate_FV = 0);
- les valeurs de sortie du processus apparaissent de nouveau après trois cycles de message.

7.2.6 Surveillance des temps de sécurité

7.2.6.1 Fonctionnement normal

La Figure 37 explique comment le pilote F utilise les communications CP 3/RTE sous-jacentes et la manière dont certains temps de surveillance sont définis. Signification des flèches courtes: dans CP 3/RTE, le contrôleur d'entrée-sortie envoie le même PDU de sécurité au dispositif F plus fréquemment que le pilote F ne génère un nouveau PDU de sécurité dans la durée de cycle de l'hôte F (numéro consécutif = n+1). En retour, le dispositif F envoie le PDU de sécurité (acquittement) au contrôleur d'entrée-sortie plus fréquemment que le pilote F du dispositif F ne génère un nouveau PDU de sécurité.

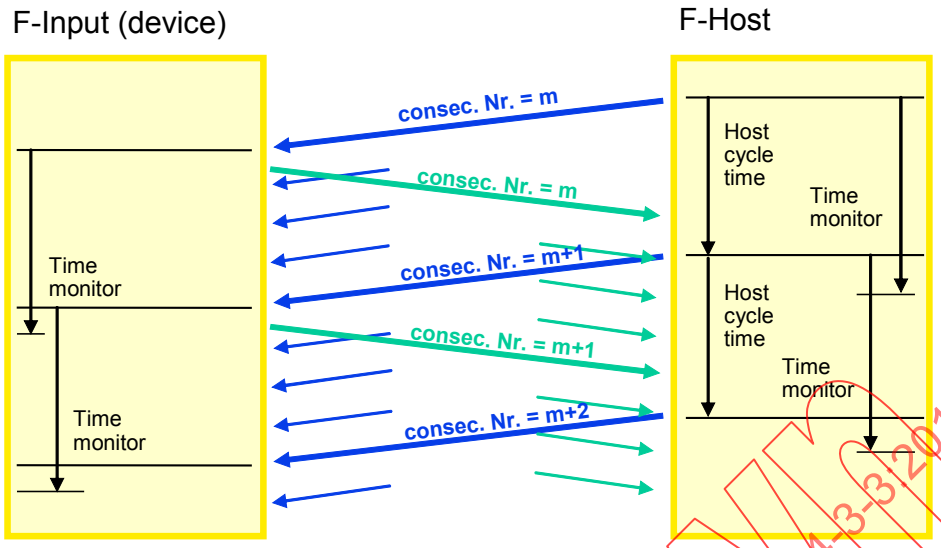


Légende

Anglais	Français
F-host	Hôte F
F-output (device)	Sortie F (dispositif)
Bus cycle time	Durée de cycle du bus
Time monitor	contrôle de temps
Host cycle time	Durée de cycle de l'hôte

Figure 37 – Surveillance de la durée d'acheminement du message Hôte F ↔ Sortie F

La Figure 37 illustre le contrôle du temps dans l'hôte F et un dispositif de sortie F. La Figure 38 illustre le contrôle du temps dans le dispositif d'entrée F et l'hôte F. Les flèches courtes représentent les PDU de FSCP 3/1 comportant un numéro consécutif (virtuel) en cours de validité mais avec d'éventuelles valeurs de processus différentes.



Légende

Anglais	Français
F-host	Hôte F
F-input (device)	entrée F (dispositif)
Time monitor	contrôle de temps
Host cycle time	Durée de cycle de l'hôte

Figure 38 – Surveillance de la durée d'acheminement du message Entrée F ↔ Hôte F

D'autres contraintes de temporisation sont présentées ci-dessous:

Démarrage (Synchronisation) Pour procéder à une synchronisation après le démarrage d'un système, le pilote de l'hôte F démarre avec le numéro consécutif virtuel 0FFFFF0h. Ensuite, l'hôte F incrémente le numéro consécutif virtuel après chaque réception acquittée du numéro consécutif virtuel respectif de son module de dispositif F 0FFFFFFh, en ignorant la valeur 0 et en poursuivant par 1. Juste avant l'expiration du temps de contrôle, l'entrée/la sortie F attend un message comportant un numéro consécutif virtuel incrémenté de 1. Une sortie F fournit des valeurs Failsafe (FVo) après avoir reçu un numéro consécutif virtuel 0.

Cycle de protocole F Une entrée/sortie F renvoie un PDU de sécurité à l'hôte F avec le même numéro consécutif virtuel (cycle de protocole F) afin d'acquitter la réception d'un PDU de sécurité.

La durée de cycle de l'hôte F ne doit pas dépasser la durée de cycle de protocole F (elle peut être plus courte).

Contrôle de temps (chien de garde) L'arrivée d'un nouveau PDU de sécurité correct dans le dispositif F dans le temps de fonctionnement du chien de garde est surveillée. Cette vérification peut être réalisée aussi souvent que nécessaire, mais au moins une fois à l'issue de l'intervalle de temps de contrôle. A l'expiration du temps de fonctionnement du chien de garde, le destinataire concerné bascule à un état de sécurité.

La durée de cycle CP 3/RTE la plus courte ne doit pas dépasser la *moitié* du temps de fonctionnement du chien de garde. La durée de cycle de l'hôte F peut être plus courte que le temps de fonctionnement

du chien de garde.

Surveillance du numéro consécutif

Un nouveau PDU de sécurité correct se caractérise par le fait que le numéro consécutif virtuel au moins a été incrémenté de 1 et que tout le reste du PDU de sécurité n'a pas été modifié ou l'a été de manière erronée. Cela signifie qu'une incrémentation incorrecte de *1* du numéro consécutif virtuel est reconnue directement par CRC2. Cela se traduit par une réaction aux anomalies.

Répétition du PDU de sécurité

La répétition d'un PDU de sécurité complet n'est pas prise en charge si un nouveau PDU de sécurité correct n'a pas été reçu dans l'intervalle du temps de fonctionnement du chien de garde.

Dispositif de surveillance SIL

Tous les messages corrompus (anomalie de CRC et de numéro consécutif virtuel) sont dénombrés pendant un intervalle de temps configurable (T) du dispositif de surveillance SIL. Les valeurs Failsafe sont définies lorsque plusieurs anomalies de ce type se produisent. En d'autres termes, un message corrompu détecté peut être toléré (*variante A*). Les cas dans lesquels l'ensemble du PDU du télégramme = "0" (au démarrage, par exemple) ne doit pas être compté.

En réalité, il peut être démontré que le comptage reste toujours nul. Cela explique la nécessité d'optimiser la complexité donnant la *variante B*, où le temps (T) du dispositif de surveillance SIL est infini. Dans ce cas, le diagramme d'états simplifié de l'hôte F (Figure 28) doit être pris en compte si les messages corrompus ne sont pas tolérés et donnent toujours lieu à un état de sécurité.

A chaque fois qu'un message corrompu est détecté de manière inattendue pendant la production ou l'exploitation, l'opérateur responsable joue le rôle du dispositif de surveillance SIL et peut tolérer et acquitter l'indication. Toutefois, en présence d'indications supplémentaires, une cause sérieuse doit être supposée et faire l'objet d'une réparation ou suppression immédiate.

Il revient au fabricant de l'hôte F de mettre en œuvre la variante A. Toutefois, une réalisation détaillée n'est pas présentée ici afin de permettre des adaptations individuelles en fonction des environnements système particuliers. Le dispositif de surveillance SIL doit uniquement être mis en œuvre dans l'hôte F.

Temps du dispositif de surveillance (T)

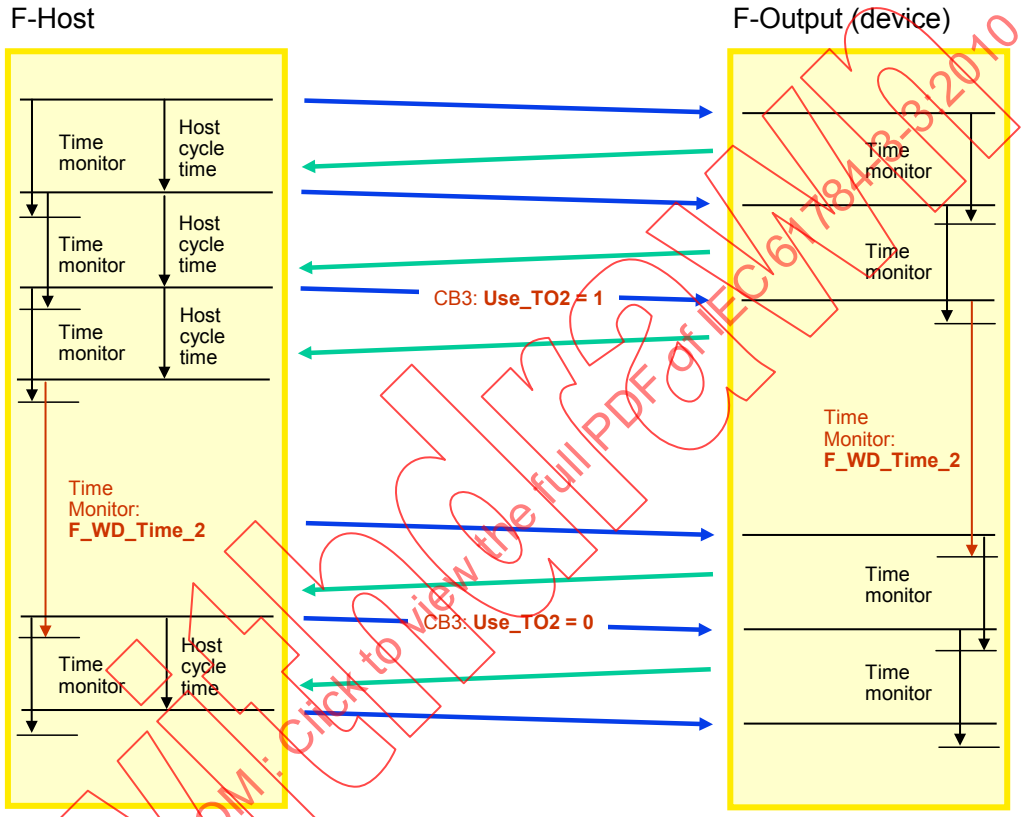
Le temps T du dispositif de surveillance SIL est une valeur constante intégrant la dimension horaire (h) résultant du SIL demandé et de la longueur CRC configurée (9.5.1). Le Tableau 6 précise les temps du dispositif de surveillance SIL.

Tableau 6 – Temps du dispositif de surveillance SIL

SIL	CRC	Longueur du PDU de sécurité	Période de temps (h)
3	24 bits	≤ 16 octets	>10
2	24 bits	≤ 16 octets	>1
3	32 bits	≤ 128 octets	>10
2	32 bits	≤ 128 octets	>1

7.2.6.2 Temps de fonctionnement étendu du chien de garde à la demande après interaction de l'utilisateur

Pour les cas d'utilisation tels que la « configuration en cours » [69] ou la « maintenance des systèmes de tolérance aux pannes », un certain temps est nécessaire à la mise à jour des dispositifs concernés. En règle générale, ce temps de mise à jour est plus long que le temps de fonctionnement du chien de garde principal régulier (F_WD_Time) défini pour une application de sécurité. Afin d'éviter des déclenchements de nuisance, le pilote de l'hôte F peut utiliser une seule fois un temps de fonctionnement du chien de garde secondaire (F_WD_Time_2) pour étendre le temps de fonctionnement du chien de garde principal de ces événements planifiés et surveillés (voir la Figure 39).



Légende

Anglais	Français
F-host	Hôte F
F-output (device)	sortie F (dispositif)
Time monitor	contrôle de temps
Host cycle time	Durée de cycle de l'hôte

Figure 39 – Temps de fonctionnement étendu du chien de garde à la demande

7.3 Réaction en cas de dysfonctionnement

7.3.1 Répétition

Déclaration: « Le dysfonctionnement d'un dispositif de bus génère d'anciens messages obsolètes répétés au mauvais moment, ce qui risque de gêner dangereusement le destinataire (le dispositif de sûreté est signalé comme étant fermé alors qu'il a déjà été ouvert, par exemple). »

Solution palliative: Les données sont transférées de manière cyclique. Par conséquent, un message incorrect relatif à un PDU de sécurité inséré une seule fois est immédiatement

remplacé par un message correct. Le *délai possible* de demande d'urgence peut donc correspondre à un *temps de fonctionnement du chien de garde*.

7.3.2 Perte

Déclaration: « Le dysfonctionnement d'un dispositif de bus supprime un message de sécurité (demande d'arrêt technique de sécurité, par exemple) ».

Solution palliative: Les informations perdues sont reconnues par une incrémentation et un examen rigoureux du numéro consécutif.

7.3.3 Insertion

Déclaration: « Le dysfonctionnement d'un dispositif de bus insère un message de sécurité (désélection de l'arrêt technique de sécurité, par exemple) ».

Solution palliative: En raison d'une attente d'un numéro consécutif rigoureusement séquentiel, le destinataire reçoit un message inséré.

7.3.4 Séquence incorrecte

Déclaration: « Le dysfonctionnement d'un dispositif de bus modifie la séquence du message de sécurité. Exemple: Avant de procéder à l'arrêt technique de sécurité, l'opérateur souhaite sélectionner la vitesse limitée de sécurité. Si ces messages ne sont pas clairs, la machine fonctionne au lieu de s'arrêter. »

Solution palliative: En raison d'une attente d'un numéro consécutif rigoureusement séquentiel, le destinataire reçoit une séquence incorrecte.

7.3.5 Corruption des données de sécurité

Déclaration: « Le dysfonctionnement d'un dispositif de bus ou d'une liaison de transmission perturbe les messages de sécurité. »

Solution palliative: La signature CRC2 reconnaît une perturbation des données entre l'émetteur et le destinataire.

Données de paramètre F	PDU de sécurité			
	Données d'entrée-sortie F	Octet d'état ou de contrôle	Numéro consécutif (virtuel)	CRC2
Paramètre F: Nom de code, délai WD, SIL, etc.				Données d'entrée-sortie, Octet de contrôle ou d'état, Numéro consécutif (virtuel) et paramètres F
	m octets	1 octet	3 octets	3 ou 4 octets

Figure 40 – Données de paramètre F et CRC

La signature CRC2 est générée par l'intermédiaire des paramètres F (y compris le nom de code), des données d'entrée-sortie F, du numéro consécutif virtuel et de l'octet de contrôle/d'état (voir 7.1.5 et la Figure 40). Le nom de code (relation source-destination) de l'hôte F et du dispositif F est défini lors de la phase de configuration à l'aide d'un outil de développement, puis soigneusement stocké.

Après la réparation, l'adresse F d'un module/dispositif F doit être restaurée / ajustée avant de reprendre l'opération de sécurité.

7.3.6 Délai

Déclaration: « *1*. Le volume d'échange de données opérationnelles dépasse la capacité de la liaison de communication. *2*. Un dispositif de bus provoque une situation de surcharge en simulant des messages de sécurité incorrects, causant le retard ou l'empêchement d'un service appartenant au message. »

Solution palliative:

- Numéro consécutif dans les données de l'émetteur et dans les données d'acquittement.
- Temps de fonctionnement du chien de garde chez le destinataire respectif (temps de fonctionnement du chien de garde pour la communication F).

Le temps de fonctionnement du chien de garde est défini en 9.3.3.

7.3.7 Déguisement

Déclaration: « Le dysfonctionnement d'un dispositif de bus provoque le mélange de messages relatifs à la sécurité et de messages non relatifs à la sécurité ».

Solution palliative: Les données proviennent du bon émetteur et se dirigent vers le mauvais destinataire (authenticité). Cette authenticité est garantie par l'introduction de paramètres F dans l'adresse F (relation source-destination F) dans la signature CRC2.

Principe d'adressage sécurisé:

La détection de l'interconnexion des messages relatifs à la sécurité et des messages non relatifs à la sécurité est assurée par le fait qu'un dispositif standard n'est pas en mesure de créer un PDU de sécurité avec les bons CRC2 et numéro consécutif.

La détection des données provenant d'un autre émetteur ou destinées à un autre destinataire est assurée par le fait que l'émetteur F appartenant à la relation source-destination F (nom de code) est le seul qui génère exactement la signature CRC correspondante attendue par le récepteur F. Simultanément, le destinataire utilise cette signature CRC pour vérifier implicitement l'authenticité de l'adresse de l'émetteur F (étant donné qu'elle a été incluse dans le CRC).

L'adresse F peut être soigneusement sélectionnée dans les dispositifs individuels de l'une des façons suivantes:

— codage du commutateur dans l'unité correspondant au nom de code (l'adresse du dispositif F des dispositifs compacts, par exemple);

— un paramétrage unique de dispositif par un logiciel qui doit être vérifié si le bon dispositif a été adressé. L'opération doit être répétée si cette unité est remplacée;

— mécanismes d'adressage indépendants de l'adressage CPF 3.

Le sabotage n'est pas pris en compte.

7.3.8 Anomalies de mémoire dans les commutateurs

Déclaration: "*1*. Le volume d'échange de données opérationnelles dépasse la capacité de la liaison de communication. *2*. Un dispositif de bus provoque une situation de surcharge en simulant des messages incorrects, causant le retard ou l'empêchement d'un service appartenant au message. »

Voir les Figures 9 et 10 pour obtenir des exemples de réseau de sécurité possible dans les cas suivants. Les commutateurs sont les éléments centraux de ces réseaux et sont des composants de réseau actifs particulièrement complexes. Ils peuvent faire l'objet de

différentes anomalies. Les messages peuvent être envoyés à la mauvaise destination ou leur contenu peut être perturbé. De plus, un commutateur peut envoyer perpétuellement des messages stockés, même si l'émetteur a déjà été arrêté. Le Tableau 7 contient une liste des anomalies de commutation possibles et leurs solutions palliatives visant à assurer une sécurité suffisante.

Tableau 7 – Solutions aux anomalies de commutation

Type d'anomalie	Détection et maîtrise
Données perturbées	Signature CRC (24 bits)
Mauvaise destination	Nom de code (2 x 16 bits)
Perte de message de sécurité	Numéro consécutif (24 bits) et délai d'attente
Message en double	Numéro consécutif (24 bits)
Message retardé	Délai d'attente
Retransmission des messages stockés avec moins de 3 PDU de sécurité consécutifs en série. L'hôte F n'est plus connecté.	Numéro consécutif (24 bits) et pas de redémarrage automatique
Retransmission des messages stockés avec au moins de 3 PDU de sécurité consécutifs en série. L'hôte F n'est plus connecté.	Numéro consécutif (24 bits) et réaction aux anomalies via l'octet de contrôle (Figure 36)

Les anomalies suivantes sont détectées/maîtrisées:

— Les anomalies de l'hôte F ou ses PDU de sécurité n'atteignent pas le récepteur. Un commutateur transmet les messages de sa mémoire tampon tournante sans le bon numéro consécutif. Le dispositif F reconnaît une anomalie de numéro consécutif et définit des valeurs Failsafe.

— Un seul message de la mémoire tampon de commutation est retransmis et comporte un PDU de sécurité avec le bon numéro consécutif. Cette anomalie est détectée à cause du numéro consécutif à 24 bits et du fait que le redémarrage de F-Output-Device implique un OA_C =1 (Acquittement de l'opérateur).

— Un commutateur transmet les messages avec des PDU de sécurité depuis sa mémoire tampon tournante avec les bons numéros consécutifs, la séquence de ce message commençant dans le temps de fonctionnement du chien de garde de sécurité. Cette anomalie est détectée à cause du numéro consécutif à 24 bits et du fait que le redémarrage de F-Output-Device implique un OA_C = 1 (Acquittement de l'opérateur).

7.3.9 Limites du réseau et routeur

Déclaration: "1. Le volume d'échange de données opérationnelles dépasse la capacité de la liaison de communication. 2. Un dispositif de bus provoque une situation de surcharge en simulant des messages incorrects, causant le retard ou l'empêchement d'un service appartenant au message. »

Pour les réseaux CP 3/RTE dotés de routeurs, la Figure 11 s'applique avec les explications correspondantes. Soit un système composé de sous-réseaux connectés par des routeurs. Les considérations ci-dessous démontrent qu'une seule erreur ne peut être à l'origine de la transmission d'un PDU de sécurité vers le mauvais dispositif F, ni d'un passage à un état dangereux.

Le routeur connecte au moins deux sous-réseaux sur des niveaux de couche 3. Chaque hôte F et dispositif F peut être configuré pour « utiliser le routeur » avec une adresse de routeur appropriée. Le routeur gère les adresses IP des sous-réseaux connectés. Le Tableau 8 contient une liste des types d'anomalie et des contraintes liées à une opération de routeur pour obtenir un niveau de sécurité suffisant.

Tableau 8 – Limites du réseau de sécurité

Type d'anomalie	Conséquences	Détection et maîtrise
Le routeur ne détient pas la bonne adresse d'un dispositif F	Le routeur reçoit un message pour ce dispositif F particulier. Résultat: cible introuvable.	Délai d'attente du dispositif F
Deux dispositifs F avec adresses identiques. L'une dans le sous-réseau 0, l'autre dans le sous-réseau 1 Contrainte: routeur à 2 ports (voir la Figure 11)	1) Dispositif du sous-réseau 0 introuvable dans le sous-réseau 0 2) Impossible d'atteindre le dispositif du sous-réseau 0 dans le sous-réseau 1 3) Impossible d'atteindre le dispositif du sous-réseau 1 dans le sous-réseau 0 4) Dispositif du sous-réseau 1 correct dans le sous-réseau 1	Par CP 3/RTE standard
Deux dispositifs F avec adresses identiques. L'une dans le sous-réseau 0, l'autre dans le sous-réseau 1 Contrainte: routeur avec un seul port (PC, ordinateur portable, par exemple):	1) Dispositif du sous-réseau 0 introuvable dans le sous-réseau 0 2) double adressage dans le sous-réseau 1	Les routeurs à un seul port ne prévoient pas de limites de réseau (de sécurité)

7.4 Démarrage F et coordination des modifications

7.4.1 Procédure de démarrage standard

Le démarrage des dispositifs/modules F repose sur le profil CP 3/RTE standard. Les couches de sécurité de l'hôte F et du dispositif F commencent d'elles-mêmes à chaque communication cyclique entre canaux CP 3/RTE. Les éléments déjà exécutés des couches de sécurité et leurs paramètres F spéciaux sont intégrés dans le processus normal de configuration et de paramétrage (« Contexte ») de CP 3/RTE. Toutes les répétitions du paramètre F portant des valeurs identiques lors de l'exécution doivent être ignorées, les valeurs qui s'écartent doivent générer un état de sécurité.

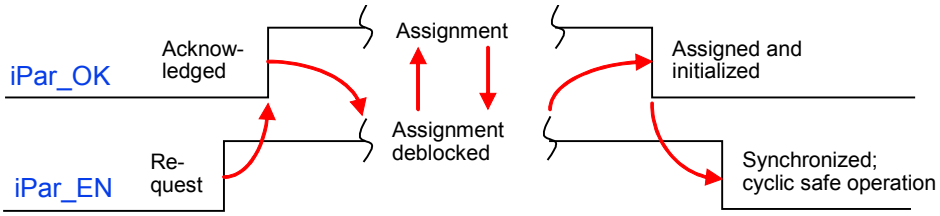
NOTE Voir [48] pour plus de détails sur le mode V1.

La Figure 15 présente les mécanismes de communication de base de CP 3/RTE. Le document [55], la CEI 61158-5-10 et la CEI 61158-6-10 donnent des informations relatives aux séquences de démarrage d'un contrôleur d'entrée-sortie et de ses dispositifs d'entrée-sortie, qui font partie intégrante des dispositifs F.

7.4.2 Déblocage de l'attribution d'iParamètre

En raison d'un message de diagnostic du dispositif F ayant besoin d'iParamètres supplémentaire (8.2) ou suite à une demande externe, l'hôte F définit le bit 0 (« Attribution d'iParamètre débloquée ») dans l'octet de contrôle de son PDU de sécurité suivant. Ensuite, par l'intermédiaire des commandes "Write-Record" (ensemble de données par ensemble de données), le dispositif F reçoit les iParamètres et procède à un acquittement à la fin en définissant le bi 0 (« De nouvelles valeurs iParamètre ont été attribuées au dispositif F ») dans l'octet d'état de son PDU de sécurité suivant (Figure 41).

Le déblocage est uniquement admis en l'absence d'état de processus dangereux. Les variables iPar_EN_C et iPar_OK_S, mises en corrélation avec le bit 0 de l'octet d'état/de contrôle, peuvent être utilisées dans le contexte de Proxy-FB-iParamétrage (8.6.2). Elles ne peuvent pas l'être dans le contexte du serveur d'iParamètres (8.6.4). La séquence de signal de la Figure 41 est un exemple d'application possible.



Légende

Anglais	Français
Acknowledged	Acquitté
Assignment	Attribution
Assigned and initialized	Attribué et initialisé
Request	Demande
Assignment deblocked	Attribution débloquée
Synchronized; cyclic safe operation	Synchronisé; opération de sécurité cyclique

Figure 41 – Déblocage de l'attribution d'iParamètre par l'hôte F

8 Gestion de la couche de communication de sécurité

8.1 Paramètre F

8.1.1 Récapitulatif

Les valeurs de paramètre des dispositifs CP 3/RTE sur le canal noir sont attribuées conformément au profil CP 3/RTE standard, c'est-à-dire grâce à des fichiers GSD reposant sur les langages de description GSD (voir [43] et [47]). De plus, les paramètres F requis pour la couche de sécurité peuvent être chargés selon plusieurs options de paramétrage alternatives.

Récapitulatif des paramètres F:

- F_S/D_Address « Nom de code » entre l'émetteur et le destinataire
- F_WD_Time Temps de fonctionnement du chien de garde dans le dispositif/module F (valeur par défaut dans le fichier GSD: temps de traitement maximal du dispositif/module F)
- F_WD_Time_2 Temps de fonctionnement du chien de garde secondaire dans les dispositifs/modules F conçus pour la « configuration en cours » ou la « maintenance des systèmes de tolérance aux pannes », afin d'étendre le contrôle du temps en cas de mises à jour prévues par le personnel autorisé uniquement (7.2.6.2)
- F_Prm_Flag1 + 2 Octets du paramètre contenant plusieurs paramètres de gestion de profil
  - F_Check_SeqNr Mode V2: toujours inclure le numéro consécutif dans la génération CRC2
  - F_Check_iPar Utilisation spécifique au fabricant dans des systèmes homogènes
  - F_SIL Vérification: SIL configuré = SIL utilisé ?
  - F_CRC_Length Longueur de CRC2
  - F_Block_ID Identification du type de blocage de paramètre
  - F_Par_Version Numéro de version des paramètres F/du mode opérationnel FSCP 3/1

- F_iPar_CRC — Valeur du calcul CRC d'iParamètre, au moins manuellement transférée d'un outil CPD ver l'outil de développement
- F_Par_CRC — Calcul de la signature CRC1 parmi les paramètres F

8.1.2 F_Source/Destination_Address (nom de code)

Les adresses des composants F d'une boucle de contrôle de sécurité (entrée F, hôte F et sortie F, par exemple) doivent être univoques dans les limites d'un sous-réseau. Les sous-réseaux sont interconnectés par l'intermédiaire de routeurs (à 2 ports), qui sont les limites naturelles de CP 3/RTE (5.4.2). En local, chaque dispositif F contient la relation source-destination configurée de la liaison de communication de sécurité avec son partenaire (F_Source/Destination_Address ou F_S/D_Address abrégé). Elle est soigneusement stockée dans les dispositifs F, fait partie intégrante de l'ensemble de paramètres F et, par conséquent, est vérifiée de manière cyclique par la couche de sécurité. Les paramètres F_S/D_Address sont des désignations d'adresse logique qui peuvent être attribuées *librement*, mais *de manière univoque.* Elles sont allouées aux adresses CP 3/RTE pendant la configuration (7.3.7). Les adresses *0* et *0FFFFh* doivent être *exclues*.

Le paramètre est composé de deux parties: F_Source_Add et F_Dest_Add: chacune appartenant au type de données Unsigned16

8.1.3 F_WD_Time (temps de fonctionnement du chien de garde F)

En local, chaque dispositif F et son homologue dans l'hôte F gèrent un temps de fonctionnement du chien de garde F configuré pour chaque relation source-destination. La couche de sécurité démarre ce temporisateur à chaque envoi d'un PDU de sécurité avec un nouveau numéro consécutif.

Ce paramètre F_WD_Time est codé comme suit: Unsigned16. Temps de base: *1 ms*. La plage de valeurs est comprise entre 1 et 65 535.

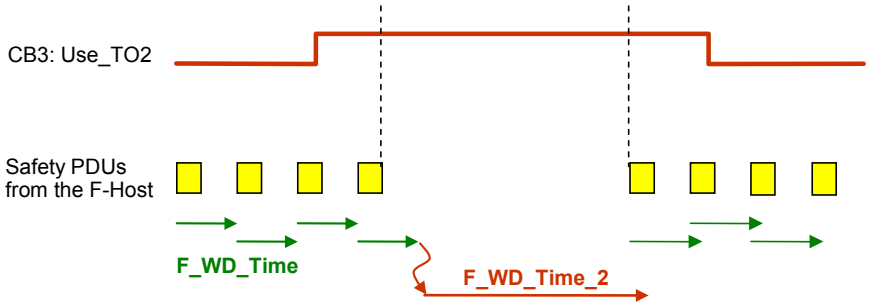
Voir 9.3.3 pour plus de détails sur la manière dont ces temps de fonctionnement du chien de garde s'intègrent dans l'ensemble de la définition des temps de réponse de la fonction de sécurité (SFRT) et sur la manière de les déterminer.

Le fabricant d'un dispositif F attribue le temps maximal d'acquittement du dispositif (DAT) à la valeur par défaut du paramètre F_WD_Time dans le fichier GSD. Un outil de développement peut alors proposer le F_WD_Time nécessaire à cette relation de communication 1:1 particulière.

NOTE L'outil de développement est alors en mesure de calculer les temps de réaction de la fonction de sécurité à condition de disposer de toutes les autres valeurs. Voir 9.3.2.

8.1.4 F_WD_Time_2 (temps de fonctionnement du chien de garde F secondaire)

Ce temps de fonctionnement du chien de garde F secondaire peut être éventuellement utilisé pour étendre le temps de fonctionnement du chien de garde F régulier d'un F_WD_Time_2 supplémentaire nécessaire à la mise à jour des dispositifs/modules F (voir la Figure 42).



Légende

Anglais	Français
Safety PDUs from the F-host	PDU de sécurité de l'hôte F

Figure 42 – Effet de F_WD_Time_2

Ce paramètre F_WD_Time_2 est codé comme suit: Unsigned16. Temps de base: *1 ms*. La plage de valeurs est comprise entre 1 et 65 535.

8.1.5 F_Prm_Flag1 (Paramètres de gestion de la couche de sécurité)

8.1.5.1 Structure de F_Prm_Flag1

Les paragraphes 8.1.5.2 à 8.1.5.5 décrivent les caractéristiques de l'octet du paramètre F_Prm_Flag1. Sa structure est présentée dans la Figure 43:

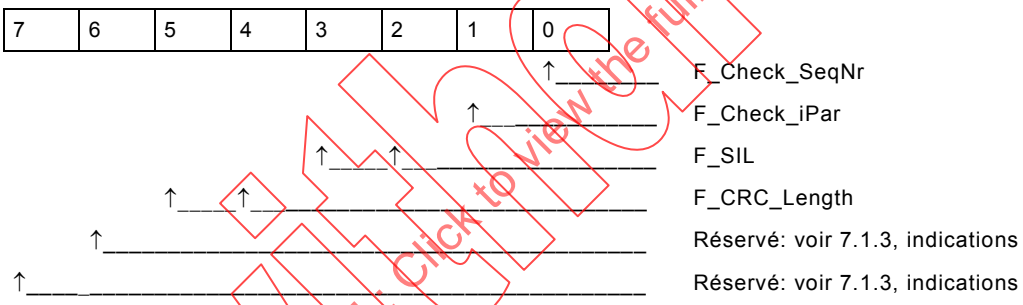


Figure 43 – F_Prm_Flag1

8.1.5.2 F_Check_SeqNr (numéro consécutif dans CRC2)

Ce paramètre détermine si le numéro consécutif doit être inclus dans la signature CRC2 (voir la Figure 44). Le paramètre est distribué au composant F au cours du démarrage.

Il est codé comme suit: Bit 0 de l'octet de paramètre F_Prm_Flag1

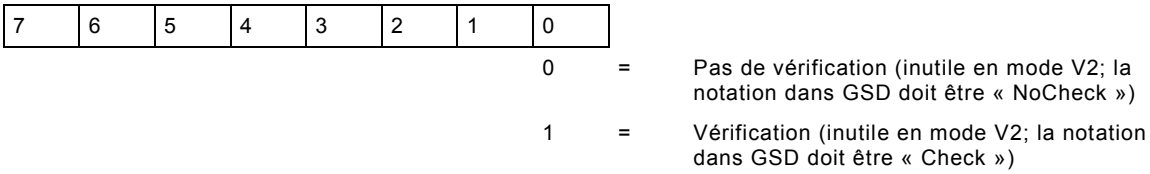


Figure 44 – F_Check_SeqNr

8.1.5.3 F_Check_iPar

La valeur 0 doit toujours être attribuée à ce paramètre dans le cas d'une utilisation normale. Il est réservé au fabricant dans les systèmes homogènes. Il n'est pas lié au mécanisme de serveur d'iParamètres.

Il est codé comme suit: Bit 1 de l'octet de paramètre F_Prm_Flag1

7	6	5	4	3	2	1	0		
						0		=	Pas de vérification (la notation dans GSD doit être « NoCheck »)
						1		=	Vérification (utilisation spécifique au fabricant)

Figure 45 – F_Check_iPar

8.1.5.4 F_SIL (phase SIL)

FSCP 3/1 permet d'assurer un fonctionnement parallèle de la communication standard et de la communication relative à la sécurité. Les différentes fonctions de sécurité utilisant la communication relative à la sécurité peuvent impliquer différents niveaux d'intégrité de sécurité (SIL 1 …SIL 3). Les dispositifs F peuvent comparer le SIL qui leur a été attribué au SIL configuré (F_SIL). Si le niveau d'intégrité de sécurité est supérieur à celui du dispositif/module F configuré, une valeur est attribuée au bit d'état de la « défaillance du dispositif », ce qui déclenche une réaction d'état de sécurité. Il existe quatre phases différentes: SIL 1…SIL 3, NoSIL (voir la Figure 46).

Il est codé comme suit: Bits 2 et 3 de l'octet de paramètre F_Prm_Flag1

7	6	5	4	3	2	1	0		
				0	0			=	SIL 1 (la notation dans GSD doit être « SIL1 »)
				0	1			=	SIL 2 (la notation dans GSD doit être « SIL2 »)
				1	0			=	SIL 3 (la notation dans GSD doit être « SIL3 »)
				1	1			=	Pas de SIL (la notation dans GSD doit être « NoSIL »): dans les dispositifs d'automatisme industriel, par exemple

Figure 46 – F_SIL

8.1.5.5 F_CRC_Length (longueur de la signature CRC2)

Selon la longueur des données d'entrée-sortie F (12 ou 123 octets) et de la phase SIL, un CRC de 2, 3 ou 4 octets est requis (voir la Figure 47). Ce paramètre transfère la longueur prévue de la signature CRC2 dans le PDU de sécurité vers le composant F pendant le démarrage.

Il est codé comme suit: Bits 4 et 5 de l'octet de paramètre F_Prm_Flag1

7	6	5	4	3	2	1	0		
		0	0					=	Signature CRC2 à 3 octets (mode V2 uniquement; la notation dans GSD doit être « 3-Byte-CRC »)
		0	1					=	Signature CRC2 à 2 octets (mode V1 uniquement; la notation dans GSD doit être « 2-Byte-CRC »)
		1	0					=	Signature CRC2 à 4 octets (facultative en mode V1/V2; la notation dans GSD doit être « 4-Byte-CRC »)
		1	1					=	Réservé: voir 7.1.3, indications

Figure 47 – F_CRC_Length

8.1.6 F_Prm_Flag2 (Paramètres de gestion de la couche de sécurité)

8.1.6.1 Structure de F_Prm_Flag2

Les paragraphes 8.1.6.2 à 8.1.6.3 décrivent les caractéristiques de l'octet du paramètre F_Prm_Flag2. Sa structure est présentée dans la Figure 48:

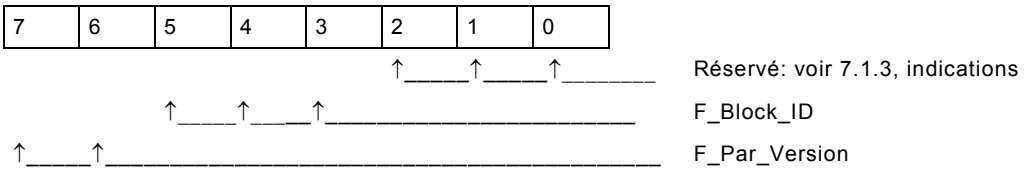


Figure 48 – F_Prm_Flag2

8.1.6.2 F_Block_ID (identification du type de paramètres)

Pour distinguer les paramètres des modes FSCP 3/1 ultérieurs, l'identification du type de paramètre F_Block_ID est codée de la manière suivante: Bits 3, 4 et 5 de l'octet de paramètre F_Prm_Flag2 (voir la Figure 49). Il est obligatoire pour permettre à la couche de sécurité de vérifier F_Block_ID.

7	6	5	4	3	2	1	0		
		0	0	0				=	Pas de F_iPar_CRC, pas de F_WD_Time_2
		0	0	1				=	F_iPar_CRC (XXX)
		0	1	0				=	F_WD_Time_2 (XXX), pas de F_iPar_CRC
		0	1	1				=	F_WD_Time_2 et F_iPar_CRC
		1	0	0				=	Réservé
		1	0	1				=	Réservé
		1	1	0				=	Réservé
		1	1	1				=	Réservé

Figure 49 – F_Block_ID

8.1.6.3 F_Par_Version (numéro de version de l'ensemble de paramètres F)

Ce compteur de versions a pour objet d'identifier les nouvelles versions d'un mode opérationnel à l'intérieur de la couche de sécurité. Le dispositif F doit répondre par un message de diagnostic spécifique au dispositif si la version demandée de la couche de sécurité ne correspond par à celle mise en œuvre (voir 6.3.2 et la Figure 50). Le contrôle de validité des paramètres F doit être réalisé par la couche de sécurité.

7	6	5	4	3	2	1	0		
0	0							=	Valide pour le mode V1 (la notation dans GSD doit être « V1-mode »)
0	1							=	Valide pour le mode V2 (la notation dans GSD doit être « V2-mode »)
1	0							=	Réservé: voir 7.1.3, indications
1	1							=	Réservé: voir 7.1.3, indications

Figure 50 – F_Par_Version

8.1.7 F_iPar_CRC (valeur d'iPar_CRC dans iParamètres)

L'outil CPD d'un dispositif F particulier calcule une signature CRC (iPar_CRC) parmi tous les iParamètres lorsque la session de paramétrage et de mise en service a abouti. Si le résultat du calcul est 0, la valeur doit être définie sur 1. La valeur au format *hexadécimal* doit être

transférée au moins manuellement à l'outil de développement et attribuée au champ d'entrée F_iPar_CRC.

Ce paramètre est transmis au dispositif F lors du démarrage et est utilisé dans le cadre d'un contrôle de cohérence iParamètre dans le dispositif F avant de commencer une opération de sécurité normale. En mode d'essai FSCP d'un dispositif F, la valeur 0 doit être attribuée à ce paramètre (8.6.4.5). Dans ce cas, le dispositif F ignore le contrôle de cohérence. A chaque fois que le dispositif F reconnaît une discordance entre la signature iPar_CRC calculée en local et la valeur de F_iPar_CRC, il doit définir des valeurs Failsafe (FV).

Ce paramètre est facultatif. Le bit 3 du paramètre F « F_Prm_Flag2 » indique sa présence. Il est codé comme suit: Unsigned32

8.1.8 F_Par_CRC (CRC1 parmi les paramètres F)

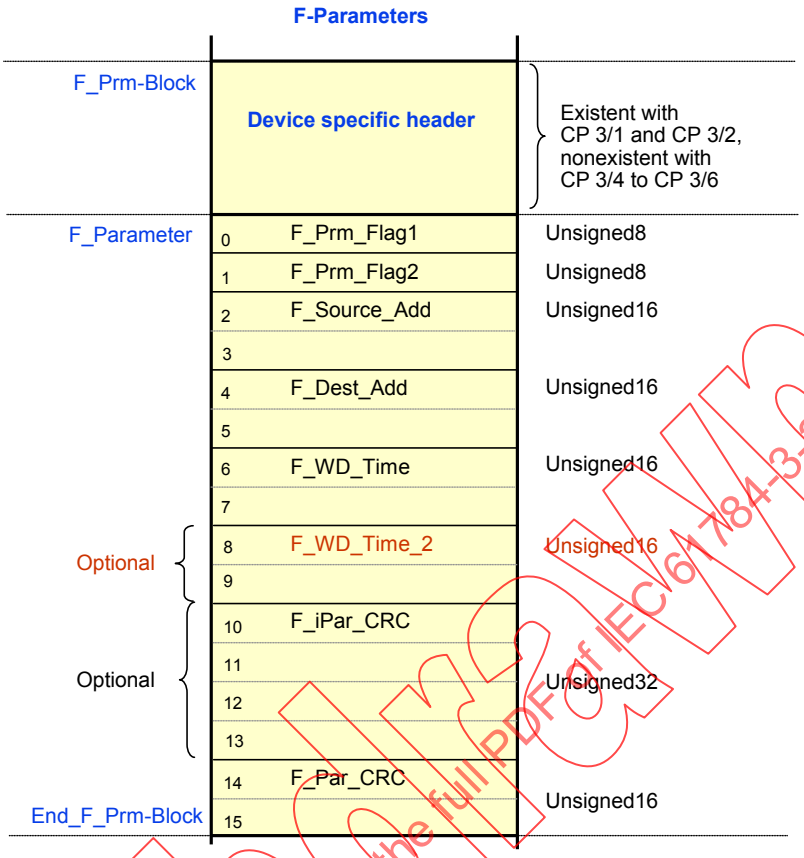
L'outil de développement génère cette signature CRC1 parmi les paramètres F. La valeur initiale de CRC1 est 0. Voir 8.3.3.2 pour plus de détails sur l'ordre des paramètres F à utiliser pour générer la signature CRC1. Le même polynôme CRC de 16 bits est utilisé (1*4EAB*h). CRC1 est la valeur initiale pour le calcul CRC2 cyclique.

Les règles suivantes s'appliquent pour les autres polynômes CRC2:

- En présence d'un polynôme CRC de 24 bits (1*5D6DCB*h), la valeur initiale des calculs CRC2 est 00xxxx, où xxxx = CRC1.
- En présence d'un polynôme CRC de 32 bits (1*F4ACFB13*h), la valeur initiale des calculs CRC2 est 0000xxxx, où xxxx = CRC1.

Il est codé comme suit: Unsigned16.

8.1.9 Structure de l'objet de données d'enregistrement du paramètre F



Légende

Anglais	Français
F-parameters	Paramètres F
Device specific header	En-tête spécifique au dispositif
Existent with CP 3/1 and CP 3/2, non-existent with CP 3/4 to CP 3/6	Existe avec CP 3/1 et CP 3/2, n'existe pas avec CP 3/4 à CP 3/6
Optional	facultatif

Figure 51 – Paramètre F

La Figure 51 illustre la structure du bloc de paramètres F dans un objet de données d'enregistrement CP 3/RTE. L'ordre des octets est conforme au CP 3/RTE standard. Les éléments suivants s'appliquent aux dispositifs F modulaires: Pour chaque sous-module F, un bloc F_Parameter est inséré dans le message de contexte (Figure 13). L'allocation du sous-module au dispositif F produit le numéro de sous-intervalle choisi.

8.1.10 Fraction de données F

Voir 7.1.6.

8.2 iParamètre et iPar_CRC

Les dispositifs F sont de plus en plus dotés de fonctions intelligentes impliquant l'attribution de nombreuses valeurs de paramètre de dispositif F individuelles. Ces paramètres relatifs à la sécurité sont appelés iParamètres. En particulier, si un dispositif est remplacé, il est opportun de charger ces paramètres via le bus directement par la voie normale. En règle générale, ces enregistrements de paramètre dépassent l'éventail de données de paramétrage reposant sur GSD (plusieurs lecteurs laser disposant d'environ 1 Ko par zone de protection peuvent

générer une quantité de données globale de *90 Ko,* voire plus). Par conséquent, cette spécification FSCP 3/1 fournit des mécanismes supplémentaires.

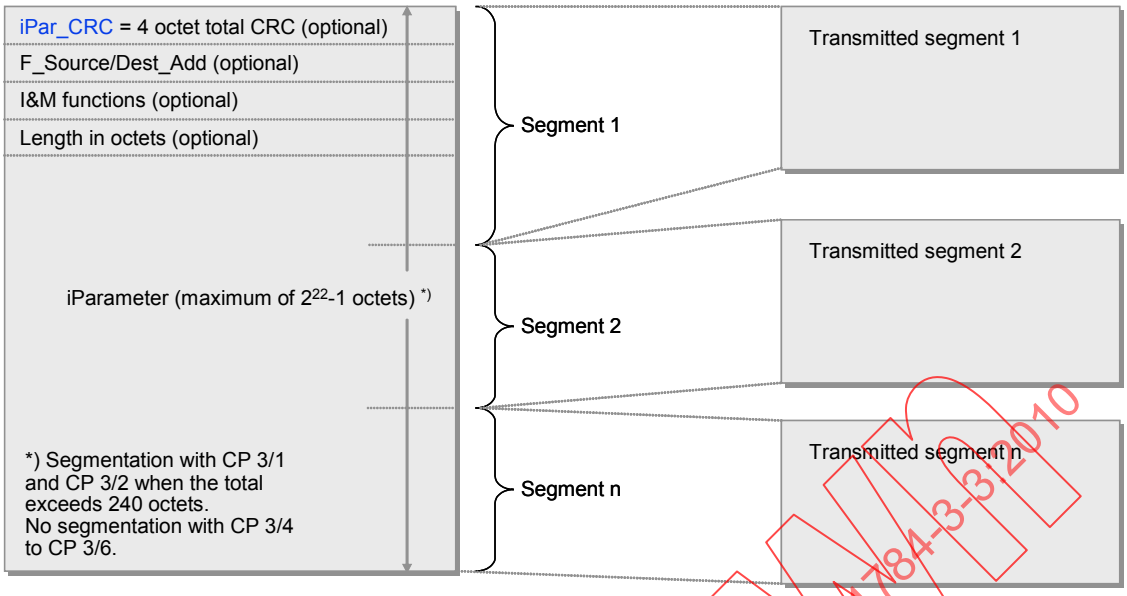
La Figure 52 présente une proposition de structure d'une grande quantité d'iParamètres aux fins de téléchargement amont et aval des données. La limite supérieure absolue des iParamètres est de 2^{22}-1 octets, la limite inférieure étant de 4 octets. Par conséquent, une segmentation est requise avec CP 3/1 lorsque le total dépasse 240 octets (voir la Figure 52). Aucune segmentation n'est requise avec CP 3/RTE.

La signature CRC (iPar_CRC) doit être calculée avec les iParamètres (Figure 52) à l'aide d'un polynôme CRC approprié, placée dans l'iPar_CRC à 4 octets au format hexadécimal et affichée dans l'outil CPD. Si le résultat du calcul est 0, la valeur doit être définie sur 1. L'introduction de la valeur iPar_CRC dans les iParamètres (voir la Figure 52) est facultative. Aucune preuve de sécurité du taux d'erreurs résiduelles suffisant n'est requise lors de l'utilisation du polynôme CRC à 32 bits FSCP 3/1.

La relation source/destination F (nom de code) permet de vérifier la remise au destinataire configuré. L'introduction dans les iParamètres (voir la Figure 52) est facultative.

Les fonctions d'identification et de maintenance (I&M) sont obligatoires pour tous les dispositifs CPF 3. Elles fournissent des codes permettant d'identifier le type et la version d'un dispositif/module particulier. L'introduction de ce type d'informations dans l'ensemble d'iParamètres peut permettre de vérifier la validité d'un dispositif de remplacement avec ses propres fonctions I&M. L'introduction dans les iParamètres (voir la Figure 52) est facultative. Les fabricants de dispositif peuvent utiliser leurs codages personnels.

La longueur du bloc iParamètre peut être utile à l'organisation efficace des processus de téléchargement amont et aval des données dans les dispositifs. L'introduction dans les iParamètres (voir la Figure 52) est facultative.



Légende

Anglais	Français
4 octet total CRC	CRC total de 4 octets
(optional)	(facultatif)
Transmitted segment	Segment transmis
Segment	Segment
I&M functions	Fonctions I&M
Length in octets	Longueur en octets
(maximum of …	(maximum de …
Segmentation with C/P 3/1 and CP 3/2 when the total exceeds 240 octets. No segmentation with CP 3/4to CP 3/6.	Segmentation avec CP 3/1 et CP 3/2 lorsque le total dépasse 240 octets. Pas de segmentation avec CP 3 / 4 à CP 3/6

Figure 52 – Bloc iParamètre

Voir 8.6 pour plus de détails sur la gestion de plusieurs segments iParamètre.

8.3 Paramétrage de sécurité

8.3.1 Objectifs

FSCP 3/1 fournit des méthodes proportionnées pour la fourniture de paramètres F et iParamètre des dispositifs F en raison des nombreuses manipulations des dispositifs de terrain dans les industries de fabrication et de transformation. L'un des principaux objectifs consiste à maintenir la stabilité d'un petit ensemble défini de paramètres F (niveau de communication) entre tous les dispositifs F et de fournir des interfaces d'iParamétrage afin de limiter la dépendance entre le fabricant du système et celui du dispositif et donc, de clairement définir les responsabilités.

Pour l'iParamétrage, la possibilité d'un bloc de fonctions proxy individuel est définie depuis le tout début de FSCP 3/1. Ce bloc de fonctions proxy repose sur les recommandations de [49], et le fabricant du dispositif F en prend la responsabilité. Le concept de bloc de fonctions proxy est décrit en 8.6.2.

Pour les petites quantités d'iParamètres (destinées aux modules d'entrée d'une entrée-sortie distante, par exemple), le concept de bloc de fonctions proxy implique un traitement logistique trop important, un bloc de fonctions proxy normalisé, le serveur d'iParamètres, étant par

conséquent présenté ici. A l'inverse du bloc de fonctions proxy, le fabricant de l'hôte F/du système prend la responsabilité du serveur d'iParamètres et propose cette fonction soit dans une bibliothèque de blocs de fonctions standard, soit sous la forme d'une fonction intégrée. Le concept de serveur d'iParamètres est décrit en 8.6.4.

Le petit ensemble de paramètres F identiques des différents dispositifs F a été délaissé en faveur de la partie configuration de réseau relatif à la sécurité d'un outil de développement via GSD (description générale de station), ce qui offre une interface utilisateur constante et simple. De plus, il évite les conflits de version GSD et des approbations corrélées de la partie configuration de réseau.

Après l'ajustement des paramètres F pendant la configuration de réseau, un enregistrement de paramètre F est compilé et placé dans l'hôte F/le contrôleur d'entrée-sortie pour le démarrage du réseau.

Le paramètre F « F_IO_StructureDescCRC » permet de s'assurer que le programme utilisateur F utilise correctement la structure des données d'entrée-sortie F et des types de données et donc, que ces éléments ne sont pas transférés vers le dispositif F lors du démarrage.

8.3.2 Extensions de sécurité GSDL et GSDML

8.3.2.1 Extensions GSDL

FSCP 3/1 prend en charge les dispositifs orientés module physique ou virtuel. Par conséquent, la spécification GSDL (General Station Description Language) [43] (voir également l'ISO 15745-3) définit les mots clés visant à structurer et identifier les informations de bloc de paramètres F des modules F (voir la Figure 51). Les sélections de valeurs possibles du paramètre F se trouvent dans un fichier GSD (General Station Description) associé à un esclave F du module F pour lequel il est conçu. Les mots clés ci-dessous du Tableau 9 sont définis.

Tableau 9 — Mots clés GSDL des paramètres F et des structures d'entrée-sortie F

Mot clé GSDL	Description
F_Ext_Module_Prm_Data_Len	Le paramètre associé à ce mot clé indique la longueur totale du bloc F_Prm présenté dans la Figure 51, qui est en général de 14 ou 18 octets, en fonction de F_iPar_CRC
F_Ext_Module_Prm_Data_Const (décalage)	A l'aide du paramètre associé à ce mot clé, une valeur fixe peut être entrée dans l'un des 4 octets d'en-tête du bloc F_Prm présenté dans la Figure 51. La position d'un octet est indiquée par un décalage 0…3
F_Ext_Module_Prm_Data_Const (0)	Indique la longueur F_Prm_Block incluant l'iPar_CRC F (0x12, par exemple)
F_Ext_Module_Prm_Data_Const (1)	Identification du bloc F_Prm = 5 (fix)
F_Ext_Module_Prm_Data_Const (2)	Intervalle du module F
F_Ext_Module_Prm_Data_Const (3)	Réservé. Doit être défini sur 0.
F_Ext_Module_Prm_Data_Ref (décalage)	A l'aide du paramètre associé à ce mot clé, une valeur sélectionnable par l'utilisateur au moment de la configuration peut être entrée dans l'un des 0…13 octets du bloc F_Prm présenté dans la Figure 51. La position d'un octet est indiquée par un décalage 4…16. Le paramètre pointe vers une définition de plage ExtUserPrmData dans les autres parties du fichier GSD
F_ParamDescCRC	Le paramètre associé à ce mot clé protège les parties relatives à la sécurité des descriptions du paramètre F dans le fichier GSD. Voir 8.3.3.3 pour plus de détails sur la manière de déterminer cette signature CRC0
F_IO_StructureDescCRC	Le paramètre associé à ce mot clé protège la description de la structure de données d'entrée-sortie (valeurs de processus transférées de manière cyclique). Voir [43] et 8.4.1 pour plus de

Mot clé GSDL	Description
	détails sur la manière de déterminer cette signature CRC7
F_IO_StructureDescVersion	Le paramètre associé à ce mot clé indique la version d'une description de structure de données d'entrée-sortie F. Une valeur 1 indique une signature CRC7 de 16 bits, une valeur 2 indiquant une signature CRC7 de 32 bits. Si cet attribut est absent, la valeur 1 est supposée utilisée

Il est recommandé d'utiliser un paramétrage structuré. Voir 8.6.4.6 pour d'autres extensions GSDL.

8.3.2.2 Extensions GSDML

Les paramètres F d'un dispositif F particulier sont définis à l'aide de son fichier GSD. La description est fournie en langage GSDML (General Station Description Markup Language) basé sur XML (voir l'ISO 15745-3, l'ISO 15745-4 et [47]).

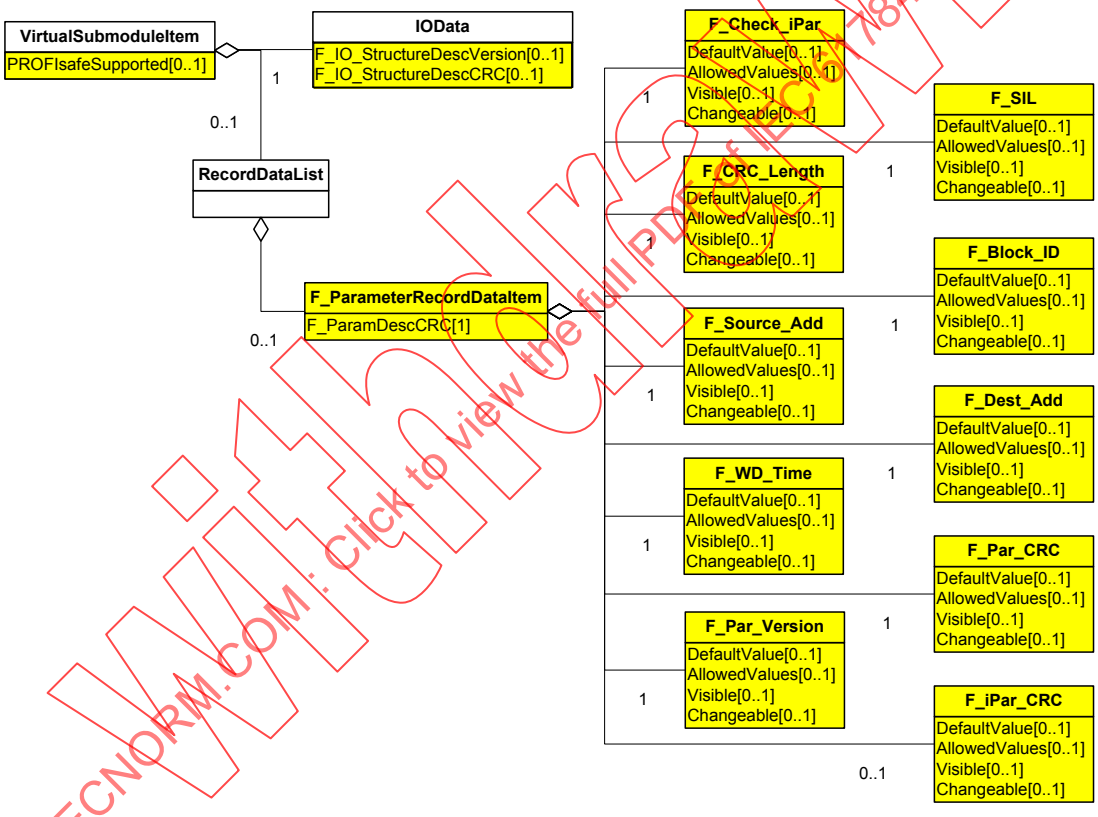


Figure 53 – Extension du paramètre F dans la spécification GSDML

La Figure 53 illustre les extensions en langage GSDML. La section VirtualSubmoduleItem fournit un attribut supplémentaire F_ParamDescCRC. Il s'agit de la signature CRC (CRC0) de la description du paramètre F de la Figure 53. F_IO_StructureDescCRC de la section IOData protège les formats des données d'entrée F et de sortie F. F_IO_StructureDescVersion indique la version d'une structure de données d'entrée-sortie F (voir 8.3.3).

8.3.3 Protection des paramètres de sécurité et des données GSD

8.3.3.1 Généralités

Il est essentiel pour la sécurité du système de protéger les paramètres de sécurité de la couche de sécurité (paramètres F) et de la technologie de sécurité du dispositif F (iParamètres), ainsi que les structures de données d'entrée-sortie de sécurité configurées.

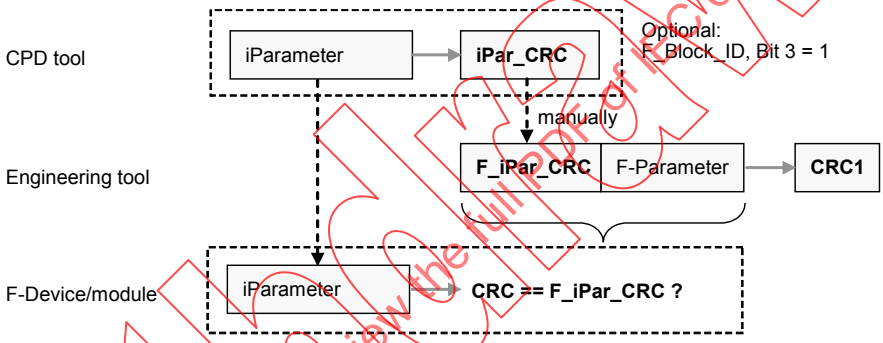
Cette protection est assurée par les signatures CRC, leur stockage définitif dans le dispositif F et l'hôte F et une comparaison régulière des signatures CRC.

Pour éviter que l'outil de développement n'utilise des données de description de dispositif perturbées (GSD), les parties relatives à la sécurité qui le composent sont également protégées par signature CRC.

8.3.3.2 CRC1 et iPar_CRC parmi les paramètres de sécurité

La Figure 25 illustre uniquement la signature CRC1 des paramètres F qui doivent être concernés par le processus de génération de signature CRC2. Toutefois, d'autres signatures CRC peuvent être concernées, comme indiqué ci-après dans le présent article.

Pour protéger les paramètres F, l'outil de développement de l'hôte F génère la signature *CRC1* (voir 8.1.7). Le polynôme CRC à utiliser est 1*4EABh*. La signature CRC1 est conçue parmi tous les paramètres F dans l'ordre des octets indiqué dans la Figure 51, à l'exclusion de F_iPar_CRC facultatif. A chaque fois que la valeur 1 est attribuée au bit 3 du paramètre F « F_Block_ID », la signature F_iPar_CRC doit être placée au début du calcul (voir la Figure 54).



Légende

Anglais	Français
Optional	Facultatif
CPD tool	Outil CPD
IParameter	IParamètre
Engineering tool	Outil de développement
Manually	Manuellement
F-parameter	Paramètre F
F-device/module	Dispositif/module F

Figure 54 – CRC1 incluant iPar_CRC

La valeur de la signature CRC1 générée (Unsigned16) est stockée et utilisée ultérieurement dans l'ordre d'octets inversé (voir 7.1.5).

8.3.3.3 CRC0 parmi les données GSD

Pour s'assurer que tous les paramètres de sécurité appropriés du dispositif F ne changent pas de manière inaperçue au cours du cycle de vie d'un support de stockage et afin de pouvoir les lire en toute sécurité dans l'outil de configuration, ils doivent être protégés par signature CRC. Le paramètre F_ParamDescCRC contient une signature CRC à 2 octets (CRC0) générée à l'aide du même polynôme CRC 16 bits (1*4EAB*h) que celui de FSCP 3/1.

Dans le cas du fichier GSD d'un esclave F (CP 3/1 ou CP 3/2), le calcul de la signature CRC0 commence par le premier F_Ext_User_Prm_Data_Ref(4) et analyse tous les mots clés du

même type, ainsi que leurs définitions de paramètre F dans la description ExtUserPrmData et les sections de sélection PrmText. Le pseudo code présenté dans la Figure 55 illustre l'algorithme de génération de la signature CRC0 à 2 octets, indépendamment de la structure du fichier GSD et des commentaires, ce qui assure au concepteur du fichier un maximum de liberté et de variabilité. Les caractères soulignés sont inclus dans le calcul.

```
//Every F_Ext_User_Prm_Data_Ref(x) one after the other in ascending order (byte offset, bit offset)
//The header of the F_Prm-Block is ignored
for (F_Par_Ref = 0; F_Para_Ref < number of elements; F_Para_Ref ++)
{
        if (list parameter==TRUE)  // PrmText with at least two selections
        {
                // in case of F parameters with "PrmText" definitions
                // read name of corresponding F_Parameter
                // e.g. ExtUserPrmData                  = 8 "F_CRC_Length"
                // read data format (0: Bit, 1: Unsigned8, 2: Unsigned16, 3: Unsigned32)
                // read Bit offset (0 if Unsigned8/Unsigned16/Unsigned32)
                // e.g. BitArea(4-5) 0 0-2                                  → 0, 4
                // read default value (LoByte, HiByte)
                // e.g. BitArea(4-5) 0 0-2                                  → 0, 0
                // now read corresponding PrmText via the text selections
                // e.g. PrmText                 =          3
                // Text(0)                      =          "3-Byte-CRC"
                // Text(1)                      =          "2-Byte-CRC"
                // Text(2)                      =          "4-Byte-CRC"
                //  EndPrmText
                for (value = 0; value <= Max (Prmtext); value ++)
                {
                        // read actual value as text
                        //  e.g.                                            → "3-Byte-CRC"
                        // read actual value as number (index) (LoByte, HiByte)
                        //  e.g.                                            → 0, 0
                }
        }
        else
        // in case of F parameters with edit fields:
        {
                // read name of corresponding F_Parameter in ascending order
                // e.g. ExtUserPrmData          = 2 "F_Dest_Add"
                // read data format (0: Bit, 1: Unsigned8, 2: Unsigned16, 3: Unsigned32)
                // read Bit offset (0 if Unsigned8/Unsigned16/Unsigned32)
                // e.g. Unsigned16 1 1-65534                                → 2, 0
                // read default value (starting with LoByte)
                // Unsigned16 1 1-65534                                     → 1, 0
                // read lower limit (starting with LoByte)
                // Unsigned16 1 1-65534                                     → 1, 0
                // read upper limit (starting with LoByte)
                // Unsigned16 1 1-65534                                     → 254, 255
        }
}
// end of algorithm
```

Figure 55 – Algorithme de génération de CRC0 (GSDL)

Pour obtenir des modèles de fichier GSD pour les esclaves F (CP 3/1 ou CP 3/2), s'adresser aux organisations indiquées dans l'Annexe B.

Dans le cas d'un fichier GSD d'un dispositif F (CP 3/RTE), le calcul de la signature CRC à 2 octets concerne toutes les sections F_ParameterRecordDataItem (Figure 53), y compris tous les paramètres F et leur définitions. Le pseudo code présenté dans la Figure 56 illustre l'algorithme de génération de la signature CRC0 pratiquement indépendante de la structure et des commentaires du fichier GSD, ce qui assure au concepteur du fichier un maximum de liberté de conception et de variabilité sans conflit.

NOTE Certains paramètres F peuvent être spécifiés comme étant invisibles dans le fichier GSD des dispositifs CP 3/RTE en indiquant Visible ="false". Un paramètre F n'est pas pris en compte dans le calcul de CRC0 si Visible ="false".

Si des attributs des paramètres F sont ignorés dans un fichier GSD, les valeurs par défaut du schéma GSDML s'appliquent toujours et doivent être incluses dans le calcul CRC0.

```
while (F_Parameter_to_read())
{
// the F_ParameterRecordDataItem section to be read in ascending order (byte offset, bit offset).
// F-Parameter Name
// F-Parameter DataType (0: Bit / BitArea, 1: Unsigned8, 2: Unsigned16, 3: Unsigned32)
// F-Parameter BitOffset (0 if Unsigned8/Unsigned16/Unsigned32)
  // read DefaultValue (starting with LoByte, two bytes for bit parameters, Unsigned8, Unsigned16;
  // four bytes for Unsigned32)
  if (value_range) // Edit field or list parameter with one value only
  {
  // read AllowedValue 1st digit (starting with LoByte of LowerLimit)
  // read AllowedValue 2nd digit (starting with LoByte of UpperLimit)
  }
  else // List parameters with at least two textual selections
  {
   // for each AllowedValue in AllowedValueList: read AllowedValue textual description character by
   // character, then corresponding numeric value (LoByte, HiByte)
}
// end of algorithm.
```

Figure 56 – Algorithme de génération de CRC0 (GSDML)

Pour obtenir des modèles de fichier GSD pour les dispositifs F (CP 3/RTE), s'adresser aux organisations indiquées dans l'Annexe B.

Interprétation du fichier GSD: à chaque fois que l'outil de configuration reconnaît des mots clés F, un logiciel particulier de configuration F (dont la sécurité a été en général évaluée) peut être lancé dans l'outil de configuration pour traiter les paramètres F de manière sécurisée.

8.4 Configuration de la sécurité

8.4.1 Protection de la description des données d'entrée-sortie de sécurité (CRC7)

La structure de données d'entrée-sortie F est décrite dans la section « IOData » du fichier GSD. Un attribut est F_IO_StructureDescCRC = CRC7. Ce CRC7 repose sur les attributs du Tableau 10 dans l'ordre indiqué (Version 2). Le polynôme CRC à 32 bits (1*F4ACFB13*h) doit être utilisé pour calculer la signature. Les types de données admis pour FSCP 3/1 figurent en 5.5.4. La précédente version 1 de l'ensemble d'éléments de structure de données d'entrée-sortie ne contenait pas l'attribut VERSION, ni les types de données Integer32 et Unsigned8+Unsigned8. Par conséquent, aucun mot clé VERSION d'un fichier GSD particulier n'indique l'indisponibilité des types de données Integer32 et Unsigned8+Unsigned8, la signature CRC7 doit être calculée à l'aide du polynôme CRC à 16 bits (14*EAB*h) et la longueur de la signature CRC7 est de 2 octets.

Le paramètre F_IO_StructureDescCRC n'est pas transmis au dispositif F lors du démarrage. L'outil de développement peut utiliser ce mécanisme pour assurer une configuration correcte.

Tableau 10 – Éléments de structure de données d'entrée-sortie (Version 2)

Nom de l'attribut	Longueur	Description
VERSION	1 octet	Indique un ensemble particulier d'éléments de structure de données d'entrée-sortie.
IN_ADDRESS_RANGE	2 octets	Longueur en octets de toute la section IOData Input (y compris F_MessageTrailer)
COUNT_PS_INPUT_BYTES_COMPOSITE	2 octets	Entrée: longueur de tous les éléments de données Float32+Unsigned8 (5 × nombre de)
COUNT_PS_INPUT_BYTES_U8_U8	2 octets	Entrée: longueur de tous les éléments de

Nom de l'attribut	Longueur	Description
		données Unsigned8+Unsigned8 (2 × nombre de)
COUNT_PS_INPUT_CHANNELS_BOOL_MAX	2 octets	Entrée: nombre de tous les canaux booléens (« faisant office de bits ») en mode maximal (mode 1oo1, par exemple)
COUNT_PS_INPUT_BYTES_BOOL_MAX	2 octets	Entrée: longueur de tous les éléments de données booléens (en octets) en mode maximal (mode 1oo1, par exemple)
COUNT_PS_INPUT_CHANNELS_INT	2 octets	Entrée: nombre de tous les éléments de données Integer16
COUNT_PS_INPUT_CHANNELS_DINT	2 octets	Entrée: nombre de tous les éléments de données Integer32
COUNT_PS_INPUT_CHANNELS_REAL	2 octets	Entrée: nombre de tous les éléments de données Float32
OUT_ADDRESS_RANGE	2 octets	Longueur en octets de toute la section IOData Output (y compris F_MessageTrailer)
COUNT_PS_OUTPUT_BYTES_COMPOSITE	2 octets	Sortie: longueur de tous les éléments de données Float32+Unsigned8 (5 × nombre de)
COUNT_PS_OUTPUT_BYTES_U8_U8	2 octets	Sortie: longueur de tous les éléments de données Unsigned8+Unsigned8 (2 × nombre de)
COUNT_PS_OUTPUT_CHANNELS_BOOL	2 octets	Sortie: nombre de tous les canaux booléens (« faisant office de bits »)
COUNT_PS_OUTPUT_BYTES_BOOL	2 octets	Sortie: longueur de tous les éléments de données booléens (en octets)
COUNT_PS_OUTPUT_CHANNELS_INT	2 octets	Sortie: nombre de tous les éléments de données Integer16
COUNT_PS_OUTPUT_CHANNELS_DINT	2 octets	Sortie: nombre de tous les éléments de données Integer32
COUNT_PS_OUTPUT_CHANNELS_REAL	2 octets	Sortie: nombre de tous les éléments de données Float32
DATA_STRUCTURE_CRC	4 octets	F_IO_StructureDescCRC = CRC7

8.4.2 Exemples de section de type de données DataItem

8.4.2.1 Approche

Les paragraphes 8.4.2.2 à 8.4.2.5 contiennent des exemples de sections DataItem conformes à certains types de pilote de canal F dans 8.5.2 utilisant les attributs décrits dans le Tableau 10.

Les types de données admises pour FSCP 3/1 figurent en 5.5.4. Pour les éléments booléens 32 bits, le type de données Unsigned32 doit être utilisé.

Voir [67] pour obtenir des informations générales relatives aux types de données.

8.4.2.2 F_IN_OUT_1

Entrée: booléen 32 bits
Sortie: booléen 32 bits

Le codage de la section DataItem de l'exemple F_IN_OUT_1 F_Channel_Driver est présenté dans la Figure 57. Le Tableau 10 contient une description des variables.

```
<IOData>
        <Input Consistency="All items consistency">
                <DataItem DataType="Unsigned32" UseAsBits="true" TextId="Inputs" />
                <DataItem DataType="F_MessageTrailer4Byte" TextId="Safety" />
        </Input>
        <Output Consistency="All items consistency">
                <DataItem DataType="Unsigned32" UseAsBits="true" TextId="Outputs" />
                <DataItem DataType="F_MessageTrailer4Byte" TextId="Safety" />
        </Output>
</IOData>
```

VERSION	02
IN_ADDRESS_RANGE	08
COUNT_PS_INPUT_BYTES_COMPOSITE	00
COUNT_PS_INPUT_BYTES_U8_U8	00
COUNT_PS_INPUT_CHANNELS_BOOL	32
COUNT_PS_INPUT_BYTES_BOOL	04
COUNT_PS_INPUT_CHANNELS_INT	00
COUNT_PS_INPUT_CHANNELS_DINT	00
COUNT_PS_INPUT_CHANNELS_REAL	00
OUT_ADDRESS_RANGE	08
COUNT_PS_OUTPUT_BYTES_COMPOSITE	00
COUNT_PS_OUTPUT_BYTES_U8_U8	00
COUNT_PS_OUTPUT_CHANNELS_BOOL	32
COUNT_PS_OUTPUT_BYTES_BOOL	04
COUNT_PS_OUTPUT_CHANNELS_ INT	00
COUNT_PS_OUTPUT_CHANNELS_DINT	00
COUNT_PS_OUTPUT_CHANNELS_ REAL	00
DATA STRUCTURE CRC	0x9EBE9328

Figure 57 – Section DataItem de F_IN_OUT_1

8.4.2.3 F_IN_OUT_2

Entrée: booléen 16 bits, entier 16 bits;
Sortie: booléen 16 bits, entier 16 bits

Le codage de l'exemple F_IN_OUT_2 F_Channel_Driver est présenté dans la Figure 58.