IEC 61784-3-3

Edition 3.0 2016-07

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 61784-3-3:2016-07(en-fr)

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.

IEC Catalogue - webstore.iec.ch/catalogue
The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

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 It also gives information on projects, replaced and withdrawn publications.

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

Electropedia - www.electropedia.org
The world's leading online dictionary of electronic and electrical terms containing 20 000 terms and definitions in English and French, with equivalent terms in 15 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary
65 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

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

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

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

Catalogue IEC - webstore.iec.ch/catalogue
Application autonome pour consulter tous les renseignements bibliographiques sur les Normes internationales, Spécifications techniques, Rapports techniques et autres documents de l'IEC. Disponible pour PC, Mac OS, tablettes Android et iPad.

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

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

Electropedia - www.electropedia.org
Le premier dictionnaire en ligne de termes électroniques et électriques. Il contient 20 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans 15 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

Glossaire IEC - std.iec.ch/glossary
65 000 entrées terminologiques électrotechniques, en anglais et en français, extraites des articles Termes et Définitions des publications IEC parues depuis 2002. Plus certaines entrées antérieures extraites des publications des CE 37, 77, 86 et CISPR de l'IEC.

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 3.0 2016-07

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

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

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

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

ICS 25.040.40, 35.100.05

ISBN 978-2-8322-3481-5

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 third edition cancels and replaces the second edition published in 2010. This edition constitutes a technical revision. This edition includes the following significant technical changes with respect to the previous edition:

- Legacy V1-mode removed from this protocol edition;
- Protocol extensions to protect against possible loopbacks (LP extensions);
- Protocol extensions to keep SIL3 for safety networks with large numbers of participants (XP extensions) and subsequent new F-Parameter "F_CRC_Seed";
- Introduction of random and disjoint Codename based MonitoringNumbers (MNR) besides to the previous Consecutive Numbers;

- Provisions for Channel Granular Passivation and subsequent new F-Parameter "F_Passivation";
- GSD extensions due to new F-Parameters;
- Notations according to the CP3 family in IEC 61158 (e.g. IO Controller);
- Additional diagnosis message types;
- Diverse error corrections and fixes of typos;
- Updated documents in bibliography.

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

FDIS	Report on voting
65C/851/FDIS	65C/854/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.

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.

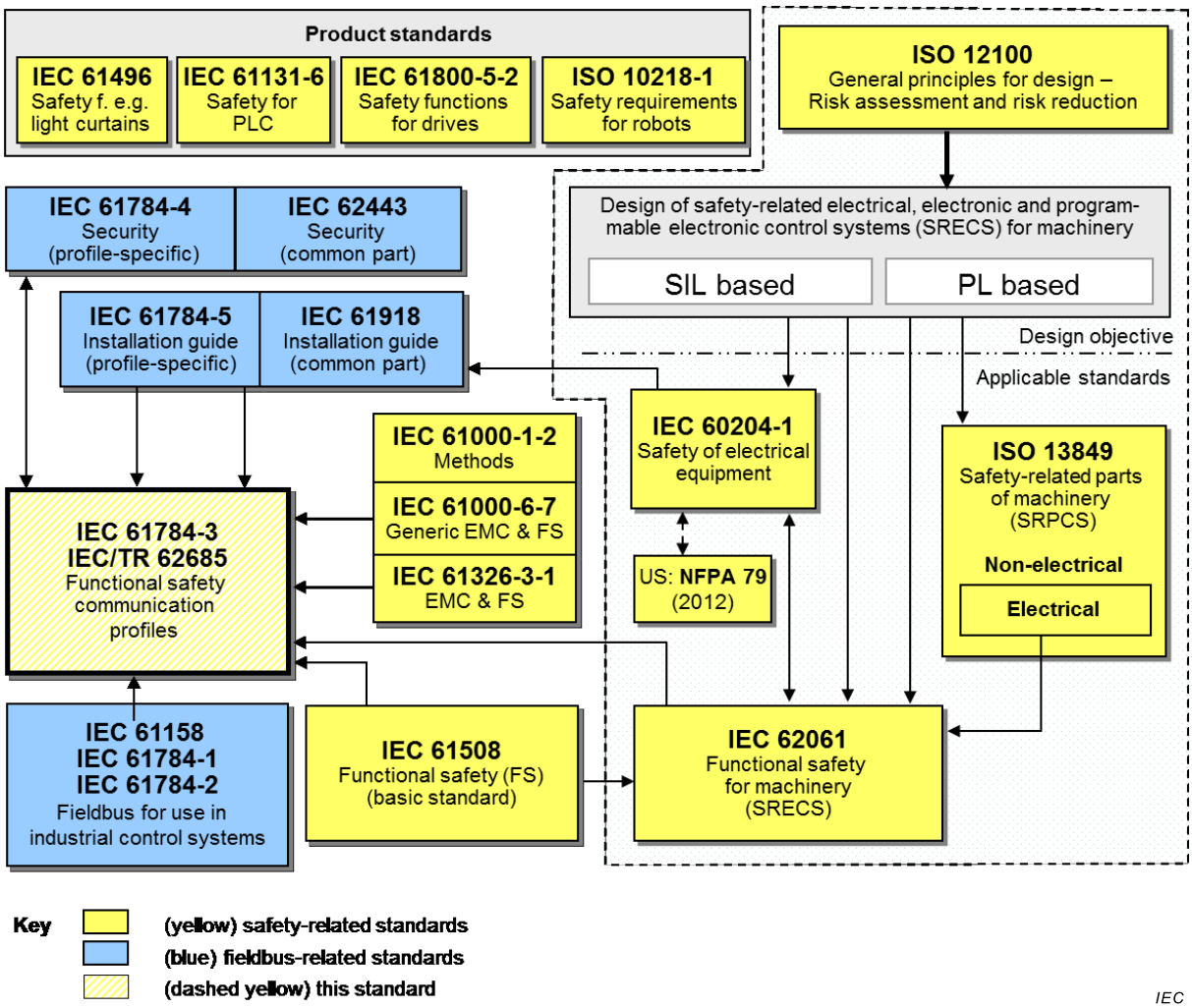
0 Introduction

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 fieldbus enhancements continue to emerge, addressing applications for 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.

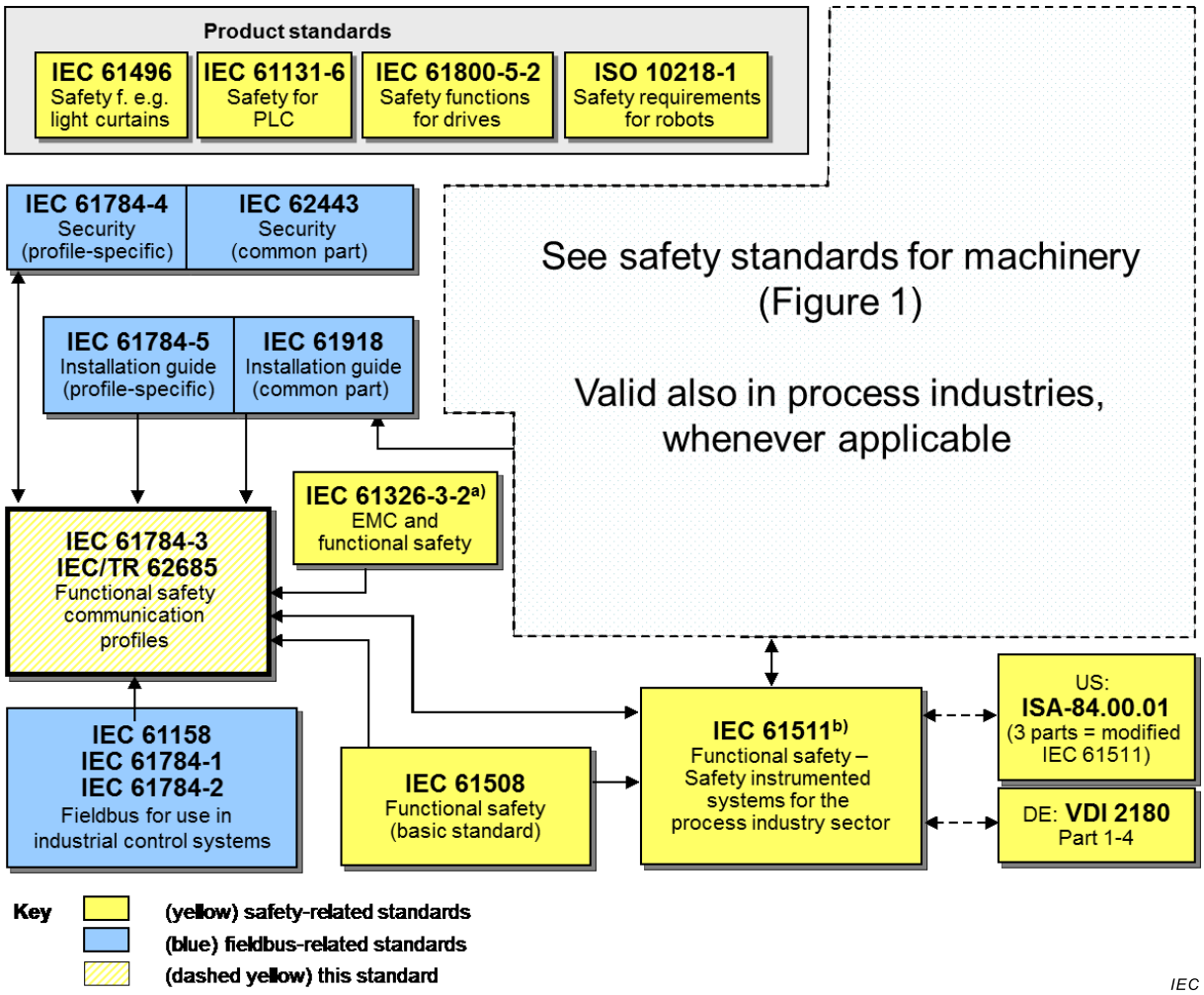
Figure 1 shows the relationships between this standard and relevant safety and fieldbus standards in a machinery environment.



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 or IEC 61000-6-7.

[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 (FSCP) within this system – implementation of a functional safety communication profile in a standard device is not sufficient to qualify it as a safety device.

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;
– functional safety communication profiles for several communication profile families in IEC 61784-1 and IEC 61784-2, including safety layer extensions to the communication service and protocols sections of 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 rights:

US 6907542	[SI]	System, device and method for determining the reliability of data carriers in a failsafe system network
US 6725419 DE 59910661.1 EP 1064590	[SI]	Automation system and method for operating an automation system
US 7808917 DE 50 2005 001 819.2 EP 1686732	[SI]	Method and system for transmitting telegrams
US 7640480 DE 50 2005 004 305.7 EP 1802019	[SI]	Detection of errors in the communication of data
EP 1921525	[SI]	Security-related system component e.g. guard door, for automation system of production system, has comparing unit comparing signatures for identity, where component supports security-related operation during sameness of signatures
EP 13172092.2	[SI]	Method and System for Detecting Errors when Transmitting Data from a Transmitter to at Least One Receiver

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 either free of charge or under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statements of the holders of these patent rights are registered with IEC.

Information may be obtained from:

[SI] Siemens Aktiengesellschaft
CT IP M&A
Otto-Hahn-Ring 6
81739 München
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.

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

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. This safety communication layer is intended for implementation in safety devices only.

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

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

IEC 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 61131-2:2007, *Programmable controllers – Part 2: Equipment requirements and tests*

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

---

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

IEC 61158-3-3, *Industrial communication networks – Fieldbus specifications – Part 3-3: Data-link layer service definition – 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:—[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 61918:2013, *Industrial communication networks – Installation of communication networks in industrial premises*

---

3 To be published.

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

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

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

ISO 13849-1:2006, *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*

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.

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

3.1.1 Common terms and definitions

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

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

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

[SOURCE: IEC 61918:2013, 3.1.2]

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

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

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

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

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

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

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

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

<method> procedure used to calculate the redundant data

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

Note 2 to entry: See also [33], [34][4].

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

3.1.1.10
error
discrepancy between a computed, observed or measured value or condition and the true, specified or theoretically correct value or condition

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

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

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

3.1.1.11
failure
termination of the ability of a functional unit to perform a required function or operation of a functional unit in any way other than as required

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

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

3.1.1.12
fault
abnormal condition that may cause a reduction in, or loss of, the capability of a functional unit to perform a required function

4 Figures in square brackets refer to the bibliography.

Note 1 to entry: IEC 60050-191:1990, 191.05.01 defines “fault” as a state characterized by the inability to perform a required function, excluding the inability during preventive maintenance or other planned actions, or due to lack of external resources.

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

3.1.1.13
fieldbus
communication system based on serial data transfer and used in industrial automation or process control applications

3.1.1.14
fieldbus system
system using a *fieldbus* with connected devices

3.1.1.15
frame
denigrated synonym for DLPDU

3.1.1.16
Frame Check Sequence
FCS
redundant data derived from a block of data within a DLPDU (frame), using a hash function, and stored or transmitted together with the block of data, in order to detect data corruption

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

Note 2 to entry: See also [33], [34].

3.1.1.17
hash function
(mathematical) function that maps values from a (possibly very) large set of values into a (usually) smaller range of values

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

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

[SOURCE: IEC TR 62210:2003, 4.1.12, modified – addition of “usually” and notes]

3.1.1.18
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

3.1.1.19
master
active communication entity able to initiate and schedule communication activities by other stations which may be masters or slaves

3.1.1.20
message
ordered series of octets intended to convey information

[SOURCE: ISO/IEC 2382-16:1996, 16.02.01, modified – character replaced by octet]

3.1.1.21
nuisance trip
spurious trip with no harmful effect

Note 1 to entry: Internal abnormal errors can be caused in communication systems such as wireless transmission, for example by too many retries in the presence of interferences.

3.1.1.22
proof test
periodic test performed to detect dangerous hidden failures in a *safety-related system* so that, if necessary, a repair can restore the system to an “as new” condition or as close as practical to this condition

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

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

3.1.1.23
performance level
PL
discrete level used to specify the ability of safety-related parts of control systems to perform a safety function under foreseeable conditions

[SOURCE: ISO 13849-1:2006, 3.1.23]

3.1.1.24
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 1 to entry: A PELV circuit is similar to an SELV circuit that is connected to protective earth.

[SOURCE: IEC 61131-2:2007, 3.54]

3.1.1.25
redundancy
existence of more than one means for performing a required function or for representing information

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

3.1.1.26
reliability
probability that an automated system can perform a required function under given conditions for a given time interval (t1,t2)

Note 1 to entry: 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 to entry: The term "reliability" is also used to denote the reliability performance quantified by this probability.

Note 3 to entry: 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 to entry: Reliability differs from availability.

[SOURCE: IEC 62059-11:2002, 3.17, modified – use automated system, two notes added]

3.1.1.27
residual error probability
RP
probability of an error undetected by the SCL safety measures

3.1.1.28
residual error rate
statistical rate at which the SCL safety measures fail to detect errors

3.1.1.29
risk
combination of the probability of occurrence of harm and the severity of that harm

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

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

3.1.1.30
safety communication channel
communication channel starting at the top of the SCL of the source and ending at the top of the SCL of the sink

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

3.1.1.31
safety communication layer
SCL
communication layer above the FAL that includes all necessary additional measures to ensure safe transmission of data in accordance with the requirements of IEC 61508

3.1.1.32
safety connection
connection that utilizes the safety protocol for communications transactions

3.1.1.33
safety data
data transmitted across a safety network using a safety protocol

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

3.1.1.34
safety device
device designed in accordance with IEC 61508 and which implements the functional safety communication profile

3.1.1.35
safety extra-low-voltage
SELV
electrical circuit in which the voltage cannot exceed a.c. 30 V r.m.s., 42,4 V peak or d.c. 60 V in normal and single-fault condition, including earth faults in other circuits

Note 1 to entry: An SELV circuit is not connected to protective earth.

[SOURCE: IEC 61131-2:2007, 3.59]

3.1.1.36
safety function
function to be implemented by an E/E/PE safety-related system or other risk reduction measures, that is intended to achieve or maintain a safe state for the EUC, in respect of a specific hazardous event

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

3.1.1.37
safety function response time
worst case elapsed time following an actuation of a safety sensor connected to a fieldbus, until the corresponding safe state of its safety actuator(s) is achieved in the presence of errors or failures in the safety function

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

3.1.1.38
safety integrity level
SIL
discrete level (one out of a possible four), corresponding to a range of safety integrity values, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest

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

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

Note 3 to entry: A safety integrity level (SIL) is not a property of a system, subsystem, element or component. The correct interpretation of the phrase “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.

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

3.1.1.39
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 to entry: In practice, several safety measures are combined to achieve the required safety integrity level.

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

3.1.1.40
safety PDU
SPDU
PDU transferred through the safety communication channel

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

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

3.1.1.41
safety-related application
programs designed in accordance with IEC 61508 to meet the SIL requirements of the application

3.1.1.42
safety-related system
system performing *safety functions* according to IEC 61508

3.1.1.43
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

3.1.1.44
spurious trip
trip caused by the safety system without a process demand

3.1.1.45
uniform distribution
probability distribution where all values from a finite set are equally likely to occur

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

3.1.2 CPF 3: Additional terms and definitions

3.1.2.1
bit
binary digit
encoded binary information without a technical unit

3.1.2.2
Codename
unique identification between safety communication peers

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

3.1.2.4
CPD-Tool
dedicated program in service computers connected to the fieldbus for the purpose of configuration, parameterization and diagnosis of particular field devices

3.1.2.5
cycle
interval at which a list of instructions or an activity is repetitively and continuously executed

3.1.2.6
device access point
DAP
item used to address a modular IO device as an entity

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

Note 2 to entry: This note applies to the French language only.

3.1.2.7
device acknowledgment time
DAT
elapsed time in an F-Device starting with the reception of a safety PDU with a new *MonitoringNumber* in the device access point until an appropriate response safety PDU has been generated and returned to the device access point

Note 1 to entry: This note applies to the French language only.

3.1.2.8
driver
software module used for abstracting the hardware with respect to the remaining application software

3.1.2.9
fail-safe
F
ability of a system that, by adequate technical or organizational measures, prevents from hazards either deterministically or by reducing the risk to a tolerable measure

Note 1 to entry: Equivalent to functional safety

3.1.2.10
fail-safe values
FV
values which are issued instead of process values when the safety function is set to a fail-safe state

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

Note 2 to entry: This note applies to the French language only.

3.1.2.11
fail-safe state
operational mode of a safety function or final element (actuator) that by adequate technical measures prevents from hazards either deterministically or by reducing the risk to a tolerable measure

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

3.1.2.12
F-Device
passive CP 3/RTE communication peer that is able to perform the FSCP 3/1 protocol, usually triggered by the F-Host for data exchange

3.1.2.13
F-Driver
software administering safety PDUs within F-Hosts and F-Devices according to the FSCP 3/1 specifications

3.1.2.14
F-Host
data processing unit that is able to perform the FSCP 3/1 protocol and to service the black channel

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

3.1.2.15
F-Module
passive communication peer within a modular F-Device or F-Slave that is able to perform the FSCP 3/1 protocol, usually triggered by the F-Host for data exchange

Note 1 to entry: This is usually a safety-related input or output module.

3.1.2.16
F-Slave
passive CP 3/1 or CP 3/2 communication peer that is able to perform the FSCP 3/1 protocol, usually triggered by the F-Host for data exchange

3.1.2.17
fault reaction
indication of a communication malfunction by setting the fault bits in the Status Byte and a corresponding automatic safe reaction within the components

Note 1 to entry:

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-IO data to be set to fail-safe values.

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

3.1.2.18
function block
FB
self-contained program part possessing a specific functionality

Note 1 to entry: This note applies to the French language only.

3.1.2.19
host acknowledgment time
HAT
elapsed time in an F-Host starting with the reception of a safety PDU with a certain *MonitoringNumber* until an appropriate safety PDU with a changed *MonitoringNumber* has been generated and returned to the master/IO-Controller

Note 1 to entry: This note applies to the French language only.

3.1.2.20
IO-Controller
active communication entity able to initiate and schedule CP 3/RTE communication activities by other entities which may be IO-Controllers or IO-Devices

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

Note 2 to entry: The IO-Controller interface is called FSPMCTL according to IEC 61158-5-10.

3.1.2.21
IO-Device
passive communication entity able to receive messages and send them in response to another CP 3/RTE communication entity which may be an IO-Controller or other IO-Devices

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

Note 2 to entry: The IO-Device interface is called FSPMDEV according to IEC 61158-5-10.

3.1.2.22
IO-Module
addressable sub input/output unit within a modular IO-Device

3.1.2.23
IO-Supervisor
engineering station enabled to read and write data from and to an IO-Device

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

3.1.2.24
IO-System
IO-Controller and its associated IO-Devices

3.1.2.25
iParameter
individual or technology specific F-Device parameters

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

3.1.2.26
iPar-Server
standardised mechanism to store and retrieve individual or technology specific F-Device parameters within the standard part of an F-Host or its controlled subsystem

3.1.2.27
master
active CP 3/1 communication peer triggering slaves for data exchange

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

3.1.2.28
MonitoringNumber
MNR
means to ensure authenticity and the correct order of transmitted safety PDUs

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

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

Note 3 to entry: This note applies to the French language only.

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

Note 1 to entry: This note applies to the French language only.

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

3.1.2.31
shared IO
inputs and outputs in field devices that can be accessed by several controllers

Note 1 to entry: Even though CP 3/RTE is permitting shared IO, 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) *MonitoringNumber* in both the F-Host and the F-Device

3.1.2.33
universal serial bus
USB
external bus standard

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

Note 2 to entry: This note applies to the French language only.

3.1.2.34
V2-mode
FSCP 3/1 services and protocol according to this part

3.1.2.35
VLAN tag
extension within Ethernet messages that enables particular user groups on large networks to run their own virtual network via priorities and VLAN-IDs, using appropriate switches, without impacting other user groups and vice versa

3.2 Symbols and abbreviated terms

3.2.1 Common symbols and abbreviated terms

BSC	Binary Symmetric Channel	
CP	Communication Profile	[IEC 61784-1/2]
CPF	Communication Profile Family	[IEC 61784-1/2]
CRC	Cyclic Redundancy Check	
DLL	Data Link Layer	[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	
FIT	Failure In Time (equals 10^{-9} failure per hour)	
FS	Functional Safety	
FSCP	Functional Safety Communication Profile	
HD	Hamming Distance	
IACS	Industrial Automation and Control System	
MTBF	Mean Time Between Failures	
MTTF	Mean Time To Failure	
NSR	Non Safety Related	
PDU	Protocol Data Unit	[ISO/IEC 7498-1]
Pe	Bit error probability	
PELV	Protective Extra Low Voltage	
PFD	Probability of dangerous Failure on Demand	[IEC 61508-4:2010]
PFH	Average frequency of dangerous failure [h^{-1}] per hour	[IEC 61508-4:2010]
PhL	Physical Layer	[ISO/IEC 7498-1]
PL	Performance Level	[ISO 13849-1]
PLC	Programmable Logic Controller	
RP	Residual Error Probability	
SCL	Safety Communication Layer	
SELV	Safety Extra Low Voltage	
SFRT	Safety Function Response Time	
SIL	Safety Integrity Level	[IEC 61508-4:2010]
SIS	Safety Instrumented Systems	
SL	Security Level	[IEC 62443]
SMS	Security Management System	[IEC 62443]

SPDU	Safety PDU
SR	Safety Related

3.2.2 CPF 3: Additional symbols and abbreviated terms

AES-CCMP	Advanced Encryption Standard – Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
AP	Application Process
API	Application Process Identifier
AR	Application Relationship
ASE	Application Service Element
ASIC	Application Specific Integrated Circuit
C	Coverage
CGP	Channel-granular Passivation
CiR	Configure in Run
CP 3/1	Communication profile commonly known as PROFIBUS DP[5]
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
CRC_FP	16 bit CRC2 seed value of the F-Host (across F-Parameter = F_Par_CRC)
CRC_FP+	32 bit CRC value across F-Parameter
DAP	Device Access Point
DAT	Device Acknowledgment Time
DP	Decentralized Peripherals
F	Identifier for safety items (fail-safe, functional safe)
FB	Function Block
FV	Fail-safe Values
GSD	General Station Description (file associated with device)
GSDL	General Station Description Language (for CP 3/1 and CP 3/2 devices)
GSDML	General Station Description Markup Language (for CP 3/RTE devices)
HAT	Host Acknowledgment Time
IO	Input/Output
LED	Light Emitting Diode
MNR	MonitoringNumber
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 [52]

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

USB	Universal Serial Bus	[57]
VLAN	Virtual Local Area Network	
WCDT	Worst Case Delay Time	
WDTime	Watchdog Time	
WPA2	Wi-Fi Protected Access 2	[29]
XML	eXtensible Markup Language	[54], [55], [56]

3.3 Conventions

This part uses UML2 notation for the drawing of the state charts and a condensed form for sequence charts [52]. 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, reserved bit ("res") within the Status/Control Byte and the F-Parameters shall be set to "0" and ignored by the receiver in order to avoid hassles with future versions of the FSCP 3/1 devices.

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™[6]) defines communication profiles based on IEC 61158-2 Type 3, IEC 61158-3-3, IEC 61158-4-3, IEC 61158-5-3, IEC 61158-5-10, IEC 61158-6-3, and IEC 61158-6-10.

The basic profiles CP 3/1 and CP 3/2 are defined in IEC 61784-1; CP 3/4, CP 3/5 and CP 3/6 are defined in IEC 61784-2. The CPF 3 functional safety communication profile FSCP 3/1 (PROFIsafe™[6]) 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, parameterization, diagnosis, and maintenance purposes.

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

---

6 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 and compliance with conditions for their use (such as testing and validation).

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

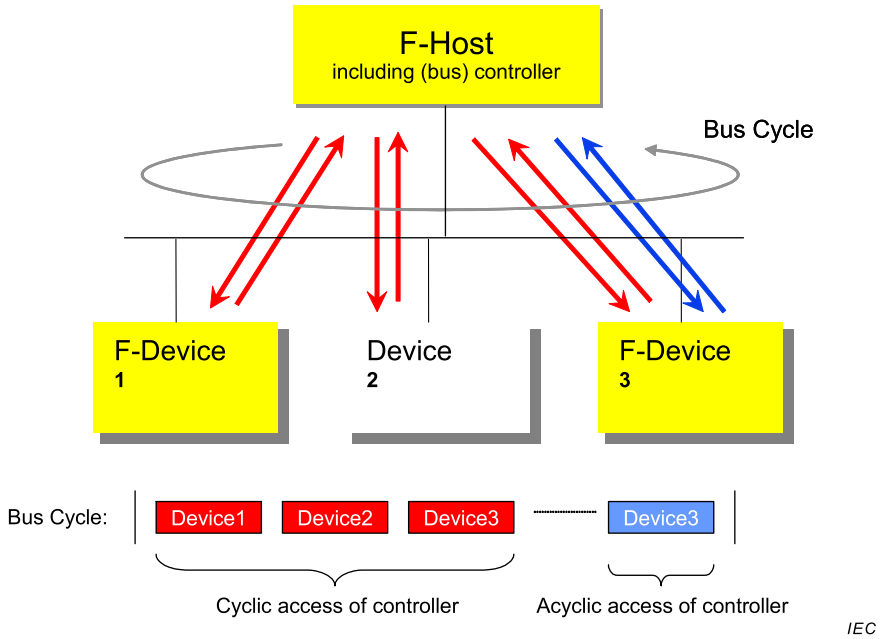


Figure 3 – Basic communication preconditions for FSCP 3/1

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

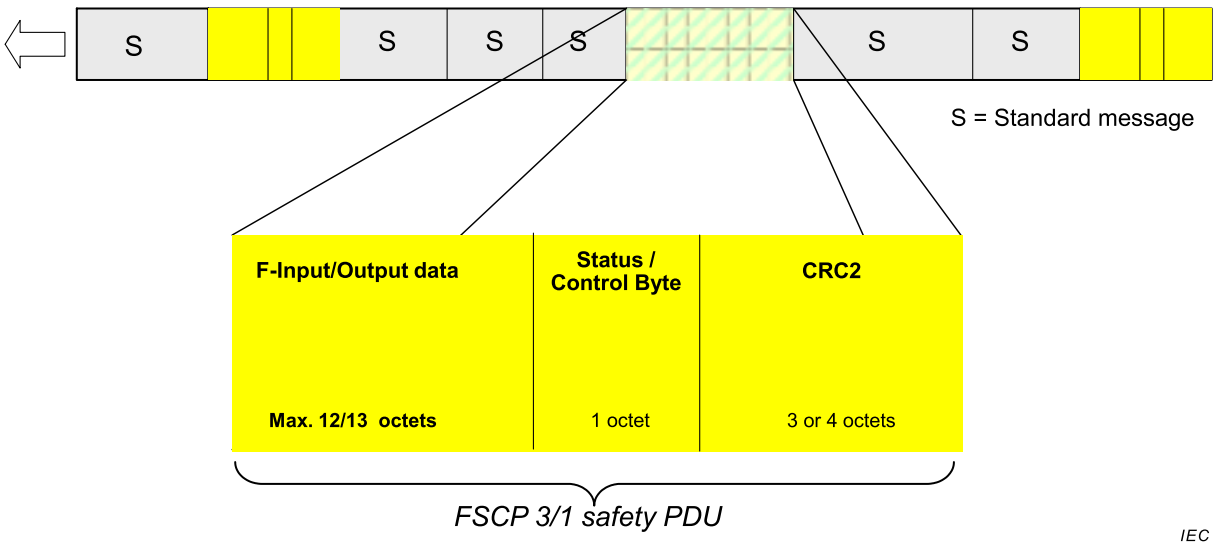


Figure 4 – Structure of an FSCP 3/1 safety PDU

FSCP 3/1 provides the so-called V2-mode. The V2-mode specified in this version covers recent developments within the Ethernet based CP 3/RTE such as programmable routing of messages and scientific findings on CRC properties.

Figure 5 provides an overview on FSCP 3/1 within the CP 3/1 and CP 3/RTE architectures.

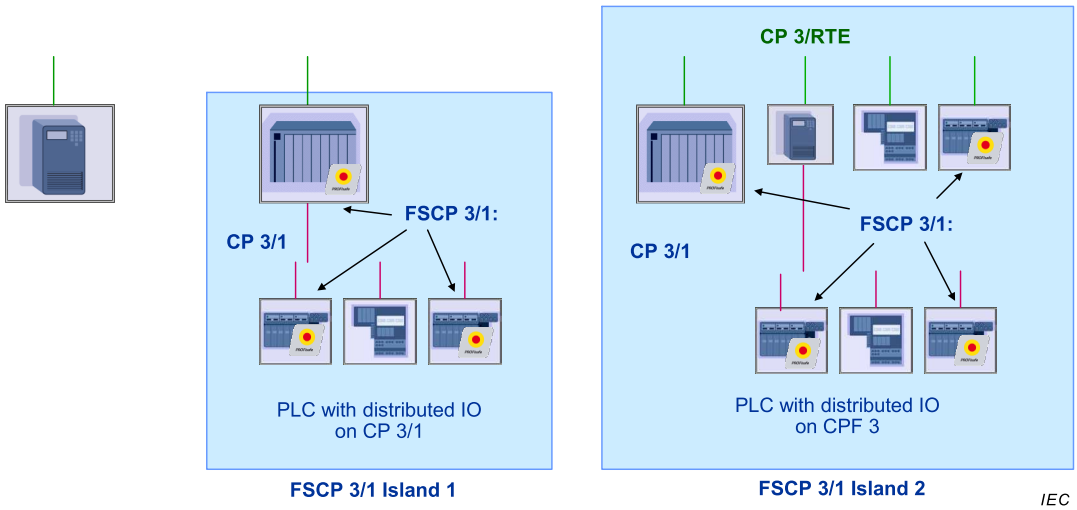


Figure 5 – Safety communication on CPF 3

While automation solutions with distributed IO gained widely acceptance through PROFIBUS (CP 3/1 and CP 3/2) and the industrial Ethernet based PROFINET (CP 3/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 5.5.3. 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.

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 in IEC 61784-3:— 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 focuses on safety communication specific F-Parameters (8.1) and on device specific individual iParameters (8.2). The requirements for handling and supply of the F-Parameters are described in 8.3. Subclause 8.4 deals with securing the data structures that are to be exchanged between the communicating partners and that represent the configuration of a device. Subclause 8.5 shows how the data structure information can be used to configure F-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 ([41], [70]).

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 meets the requirements of NE97 [53].

5.2 Safety functional requirements

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

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

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

c) Safety communication shall use a single-channel communication system. 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- 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 or IEC 61326-3-2, if there are no particular product standards.

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

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

j) Safety communication shall be suitable for NE97 [53] and meet the requirements of IEC 61784-3:— 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:—, 5.5 is required for FSCP 3/1.

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

Table 1 – Deployed measures to master errors

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

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

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

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

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

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

5.4 Safety communication layer structure

5.4.1 Principle of FSCP 3/1 safety communications

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

On this basis, safety communication is performed by

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

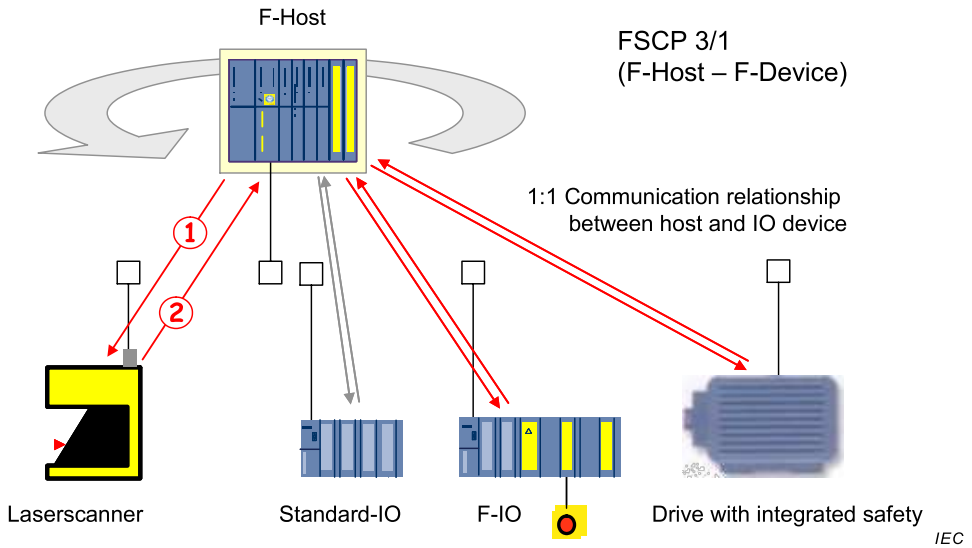


Figure 6 – Standard CPF 3 transmission system

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

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

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

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

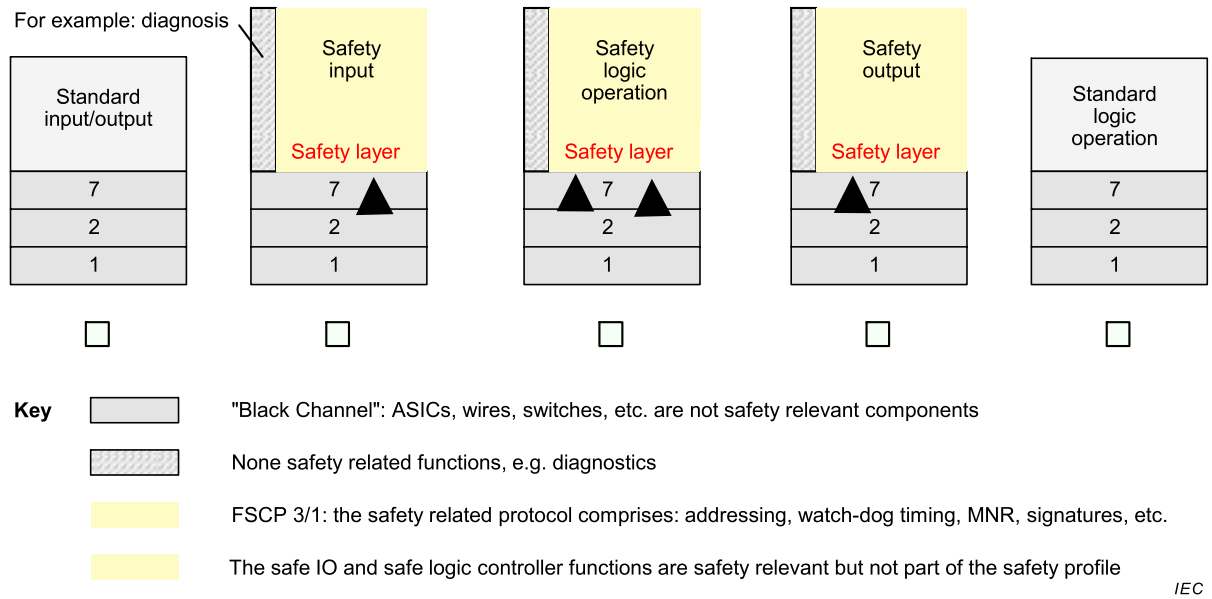


Figure 7 – Safety layer architecture

Transmission is performed via electrical 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.

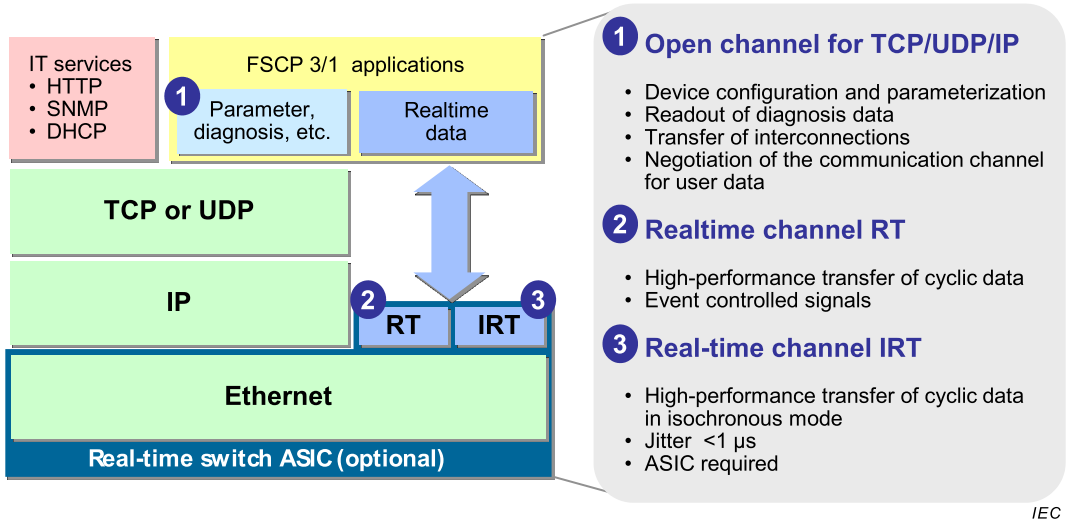


Figure 8 – Basic communication layers

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

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.

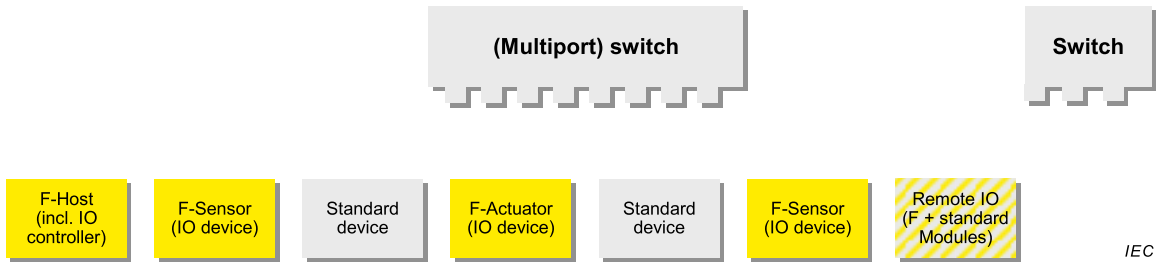


Figure 9 – Multiport switch bus structure

In order to avoid a system shut down in case of a failing device a ring structure (see 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.

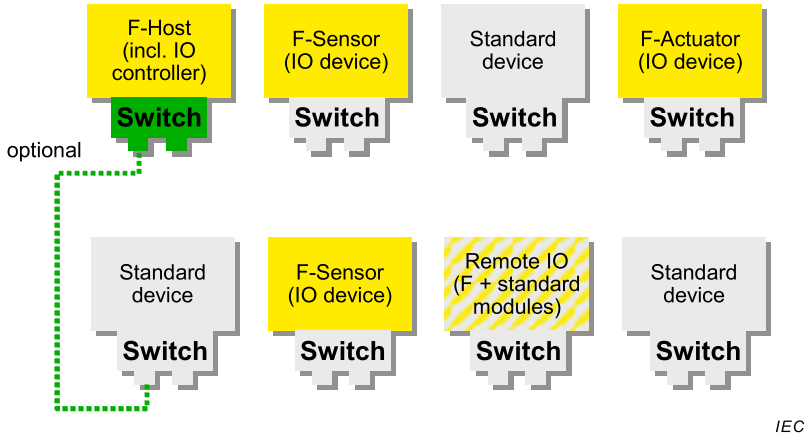


Figure 10 – Linear bus structure

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 (see Figure 8). It is the (OSI layer 3) task of routers to redirect messages on an IP-Address level (see Figure 11). Thus routers are natural borders for CP 3/RTE systems where RT_CLASS_UDP is not permitted or not supported.

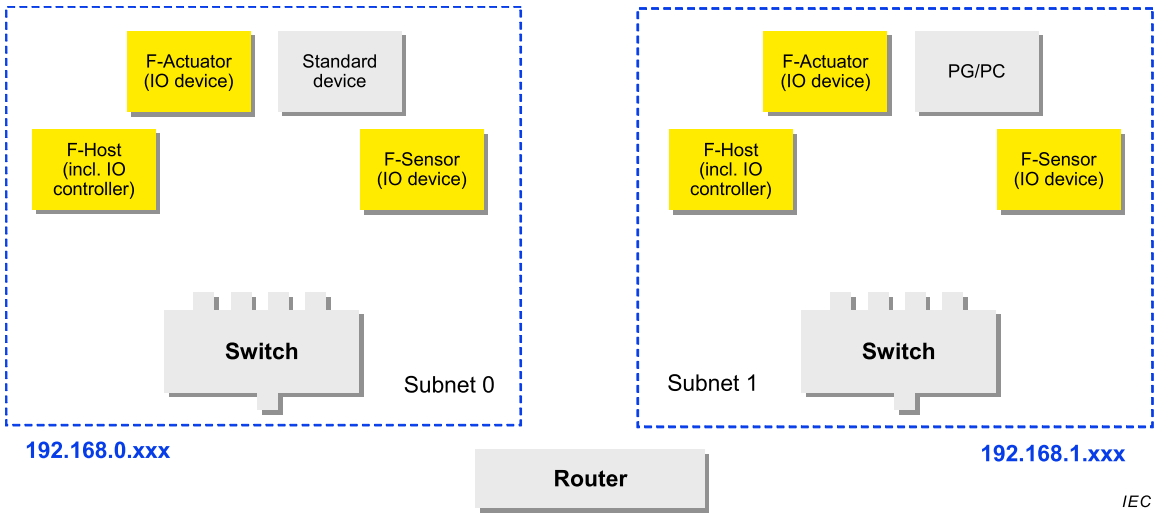


Figure 11 – Crossing network borders with routers

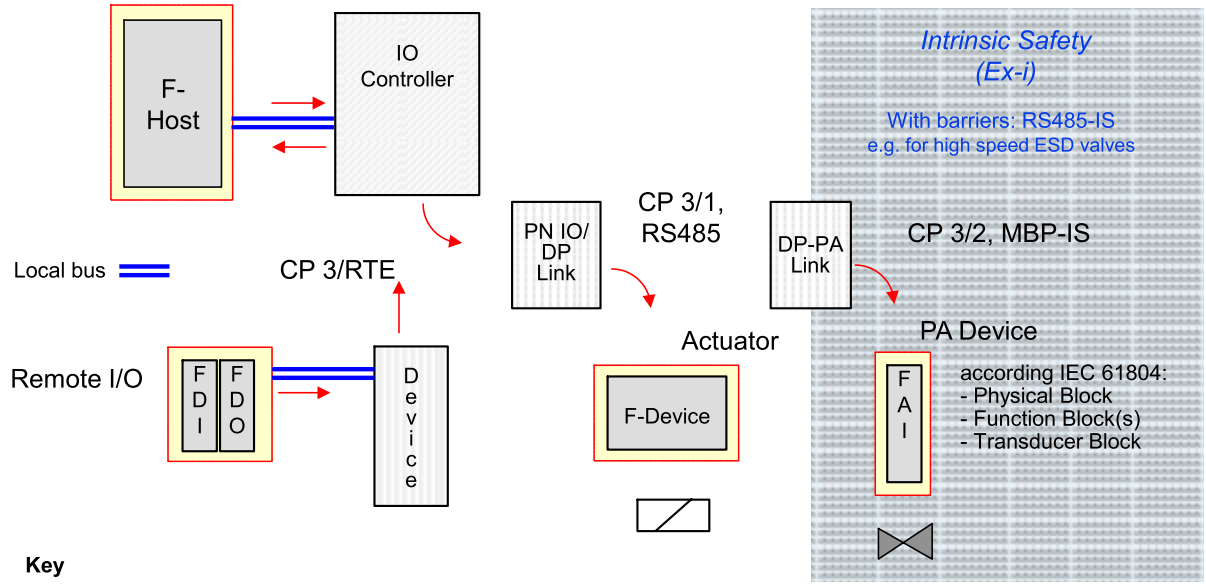
The following restrictions apply for FSCP 3/1.

- Wireless LAN permitted. However, uniqueness of Codenames ("F_S/D_Addresses") shall be guaranteed within islands.
- Single port routers are not permitted (7.3.11).

If Real-Time protocols are crossing routers, the Codenames within the entire network shall be unambiguous and the Codename checks shall identify unambiguous relationships and via additional measures both transmission directions.

In contrast to the fieldbus system configuration, Figure 12 shows the possible network structure, i.e. how far the safety profile extents into the individual units. A standard remote IO, for example, can comprise an F-Module for the connection of an emergency stop pushbutton. Thus the whole FSCP 3/1 transmission path reaches from the F-Host across its backplane bus via CP 3/RTE 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.



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)

IEC

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 shows the internal structure of an application process for a modular field device. Optionally it could have several of these APs. The application process is subdivided into as many slots and subslots as needed to represent the physical IOs of the device. In contrast to CP 3/1, CP 3/RTE provides one hierarchical level more: the subslots.

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.

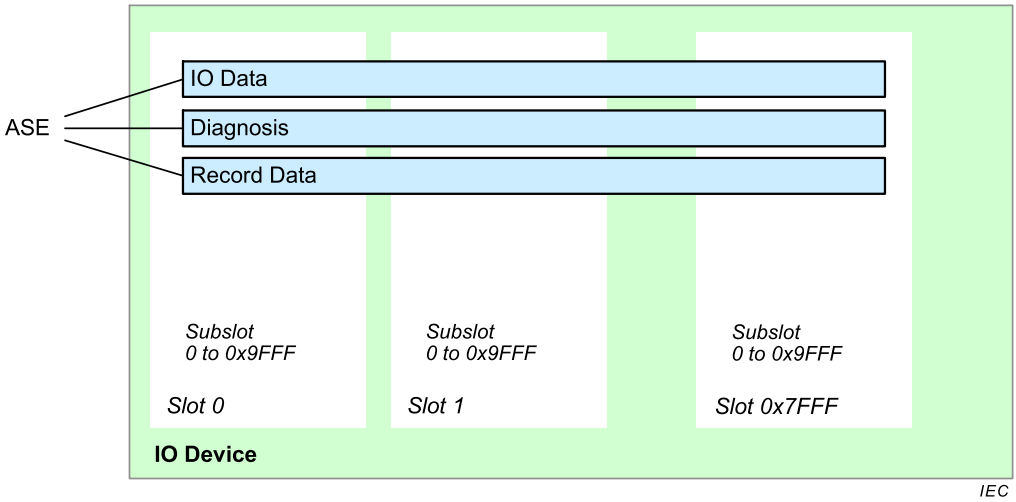


Figure 13 – IO Device model

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

5.5.2 Application and communication relationships

CP 3/RTE in general permits shared input. Since FSCP3/1 is based on 1:1 communication relationships, shared input cannot be used for functional safety.

5.5.3 Data types

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

Table 2 – Data types for FSCP 3/1

Data type name	Number of octets
Integer16	2
Integer32	4
Unsigned8 (used as bits)	1
Unsigned16 (used as bits) [a]	2
Unsigned32 (used as bits) [a]	4
Float32	4
Unsigned8+Unsigned8	2
Float32+Unsigned8 (enumerated)	5
F_MessageTrailer4Byte	4
F_MessageTrailer5Byte	5
[a] It is highly recommended to use multiple Unsigned8 instead.	

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

See [62] for general information on data types and 8.4.1 for functional safety coding.

6 Safety communication layer services

6.1 F-Host services

Figure 14 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).

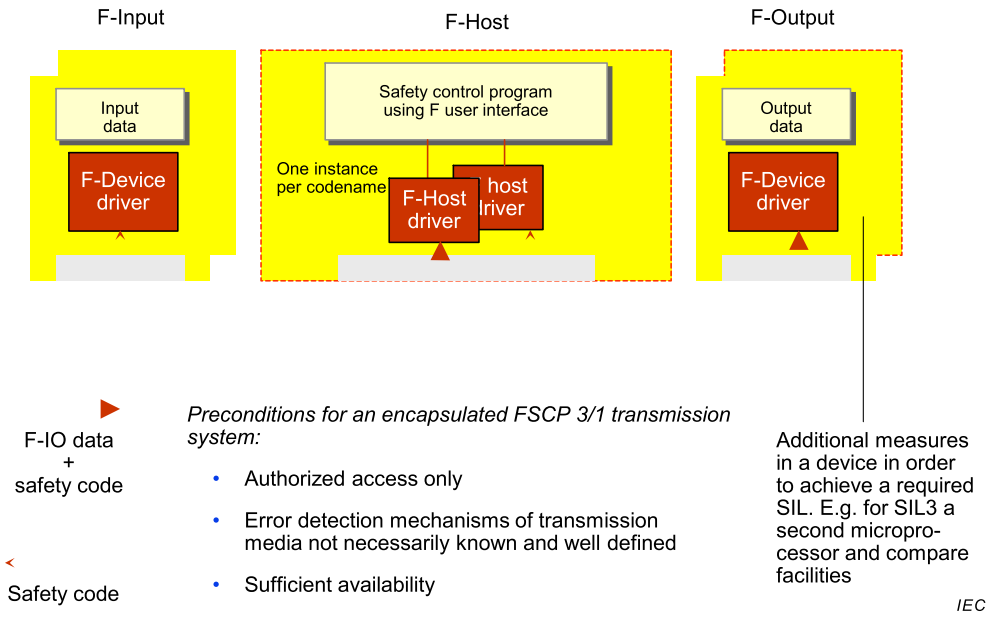


Figure 14 – FSCP 3/1 communication structure

The entire standard CPF 3 communication equipment between F-Drivers belongs to the black channel. The arrows in Figure 14 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.

NOTE It is possible for F-Devices/F-Modules to provide F-Input and F-Output data.

Safety PDU management and F-Parameterization are tasks of the F drivers within the F-Host and the F-Devices. They provide also the measures to support the additional system features "Configure in Run" (CiR) according to [64] and "Channel-granular Passivation" based on [66].

The F user interface at the safety control program level is shown in Figure 15.

"Configure in Run" (CiR) or "Maintenance of Fault Tolerant Systems" according to [64] are planned activities that shall be monitored by authorized personnel only. CiR shall only be activated and de-activated by an operator. It shall not be set/reset via the "F User Program".

The design of corresponding safety-related parts of the F-Host shall exclude any unintended activation of CiR as well as guarantee the deactivation of CiR after terminating the reconfiguration.

The F-Host shall set and reset "use_TO2" (CiR) for all the F-Devices thus affecting all F-Devices simultaneously.

The F-Host shall extend the regular (primary) watchdog time (F_WD_Time) by a secondary watchdog time (F_WD_Time_2) once only (see Figure 20, Figure 28, Figure 29, 7.2.6.2, 8.1.1, 8.1.4).

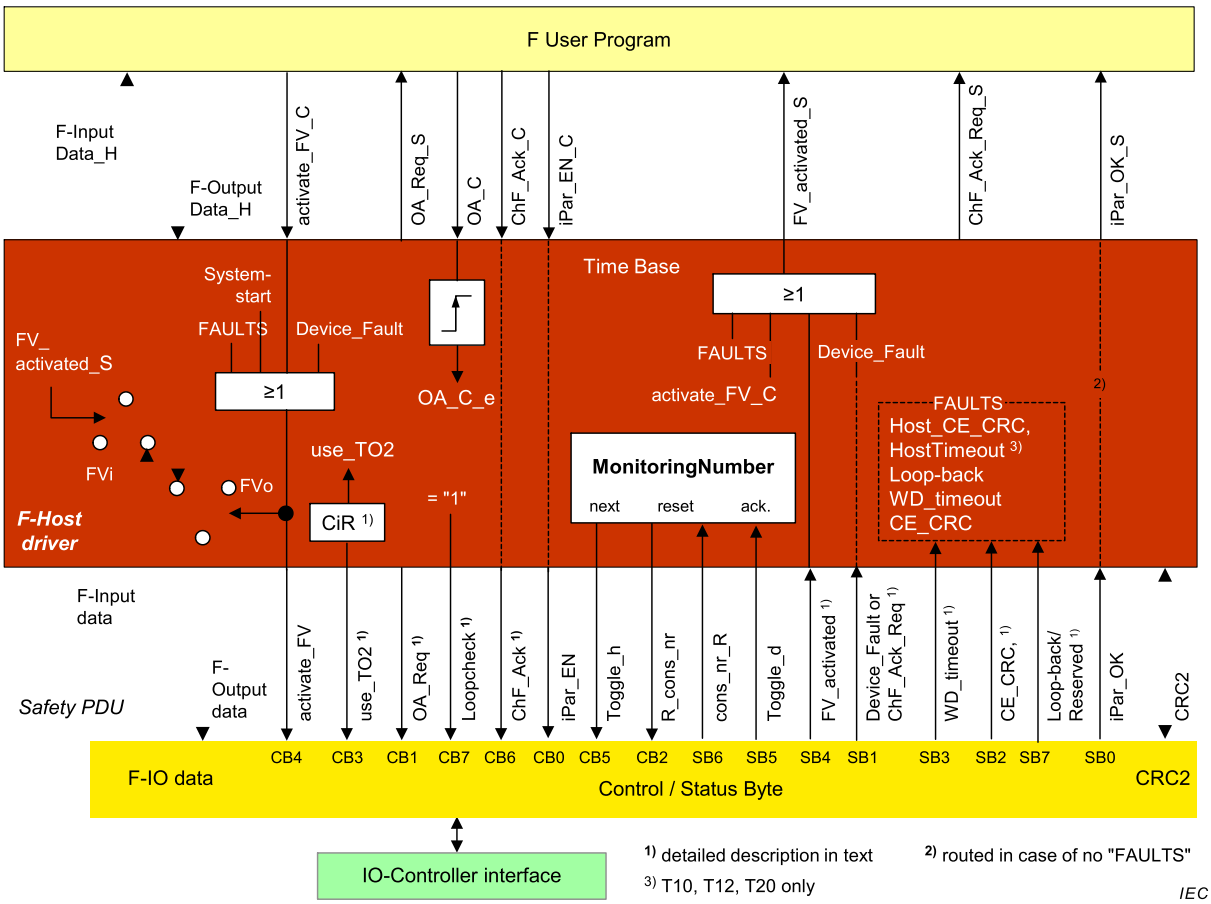


Figure 15 – F user interface of F-Host driver instances

The need for "Channel-granular Passivation" can be seen in 5.4.2 and Figure 12. The FSCP 3/1 transmission path reaches for example an F-Module of a Remote IO. Usually, the F-Module provides several signal channels each for a safety sensor as shown in Figure 16. Each signal channel can be associated with an individual safety function. In case one channel fails, the F-Module will cause all associated safety functions to enter the fail-safe state. The option "Channel-granular Passivation" based on [66] allows for an individual fail-safe state only for that safety function, which is impacted by the failed signal channel.

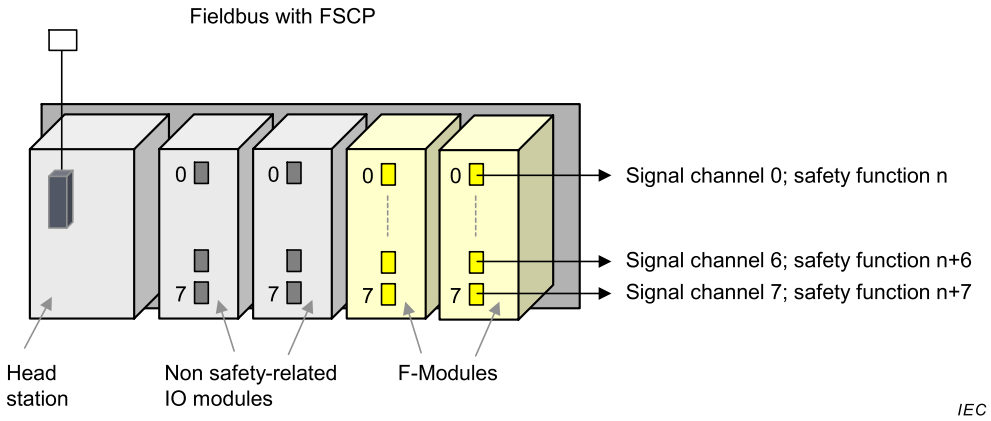


Figure 16 – Motivation for "Channel-related Passivation"

There are several variables available to the programmer to manipulate these safety processes according to the standards. The variables are carrying similar names – normally extended by an index "_C" (Control) or "_S" (Status) – like the corresponding bits within the Status and Control Bytes but may have some control logic in between within the F driver. See also 8.5.2 and Figure 63.

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 set/reset 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 evaluate 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 each and every channel of the F-Module. See [66].

With output devices this variable indicates via "1" that each and every channel of the F-Module is set to fail-safe values "0" (default behavior) or an F-Output device specific value controlled by the "activate_FV" signal (= bit 4 of the Control Byte). See [66].

This variable (type: bit) represents the result of a logical "OR" of the signals: Faults, activate_FV_C, FV_acivated (SB4), Device_Fault/ ChF_Ack_Req, and Systemstart (implicit).

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 iParameterization and the readiness to resume F-IO data exchange

(Figure 40). It shall be updated with the value of "iPar_OK" within the transitions T4, T8, and T17 of the F-Host state machine if the Status bit 1 "Device_Fault" (implementation case: F-Passivation =0) 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 set/reset this variable (type: bit). In changing this variable to "1" the user is able to resume a safety function after a fault reaction (safety function specific) via an F-Host user program.

OA_Req_S — This variable (type: bit) indicates a request for acknowledgment prior to the resumption of a safety function. In case the F-Host driver or an F-Device detects a communication error or an F-Device fault (F_Passivation = 0), 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 acknowledgment is possible. Once the acknowledgment occurred (OA_C = "1") the F-Device driver will reset the request variable OA_Req_S (= "0").

ChF_Ack_C (Channel Operator Acknowledgment) — F_Passivation =1 (see 8.1.6.2): Every F control program shall set/reset this variable (type: bit). In changing this variable to "1" the user is able to resume a safety function after any cleared signal channel fault within an F-Device/Module via an F-Host user program. This signal can be omitted and represented by signal OA_C instead.

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

Input values

- PVi Process input values (←F-Input_Data_D, see Figure 17)
- FVi Fail-safe input values, used instead of PVi for F-Input_Data_D (Figure 17).

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 17 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 (1 ms) to the F-Device driver in order to feed the watchdog timers.

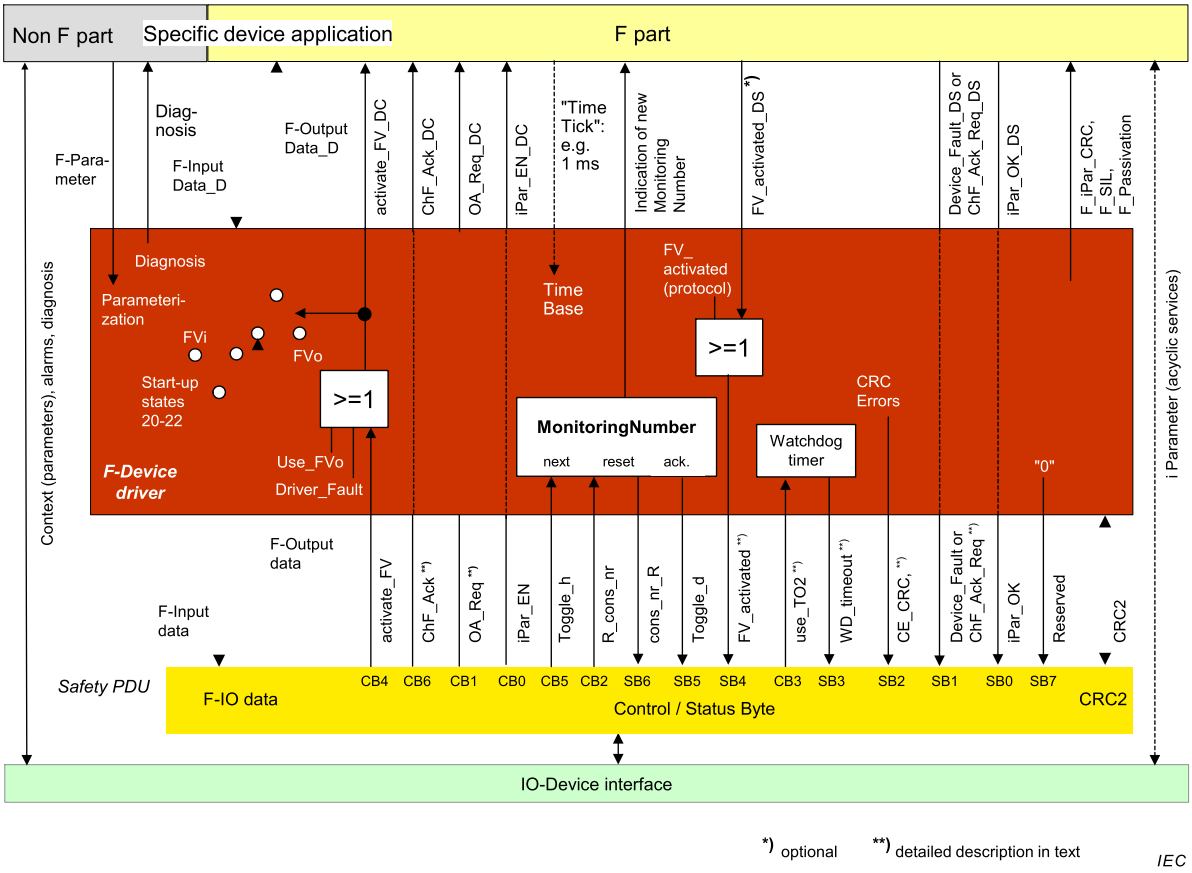


Figure 17 – F-Device driver interfaces

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-IO data usually are passed through except during start-up (FVi instead) or in case of faults (FVo instead). The received safety PDUs are containing Control Bytes with Control Bits CB0 to CB6 (in case of F_CRC_SEED =0: CB7 also). Some of these signals are passed through to the application interface without interaction. An indication of a new MonitoringNumber is provided to facilitate the implementation of demands with sufficient duration (at least one FSCP 3/1 cycle = two different MonitoringNumbers).

In return safety PDUs are prepared for transmission. They are containing Status Bytes with Status Bits SB0 to SB6. One of these is passed through, the 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.

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

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

activate_FV_DC This safety-related variable indicates the F-Output data are fail-safe values (FV = 0). It can be used to force the outputs of an F-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 each and every output channel is set to fail-safe values. For combined input and output devices this variable (type: bit) indicates via "1" the device application is delivering fail-safe values ("0") to the FSCP 3/1 driver for each and every input and output channel is set to fail-safe values.

OA_Req_DC The F-Device application shall use this non-safety-related variable to indicate locally the request for an operator acknowledgment (*OA_C* within F-Host) usually via a LED. Implementation is optional for F-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 or *ChF_Ack_Req_DS* F_Passivation =0 (see 8.1.6.2): Fault recognized by the specific device application;
F_Passivation =1 (see 8.1.6.2): Fault recognized by any signal channel of an F-Device/Module via qualifier (see [66]) is cleared and can be acknowledged.

ChF_Ack_DC F_Passivation =1 (see 8.1.6.2): The F-Host user program sets this variable to "1". This acknowledgment confirms that the signal channel fault has been cleared and personal has left the protection area.

6.3 Diagnosis

6.3.1 Safety alarm generation

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

6.3.2 F-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 an assigned range for FSCP 3/1 within the coding table of the field "ChannelErrorType" in IEC 61158-6-10.

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 or mismatch (F_Source_Add), see 8.1.2
0x0043	67	Safety watchdog time value is 0 ms (F_WD_Time, F_WD_Time_2)
0x0044	68	Parameter "F_SIL" exceeds SIL from specific device application
0x0045	69	Parameter "F_CRC_Length" does not match the generated values
0x0046	70	Version of F-Parameter set incorrect
0x0047	71	Data inconsistent in received F-Parameter block (CRC1 error)
0x0048	72	Device specific or unspecified diagnosis information, see manual
0x0049	73	Save iParameter watchdog time exceeded
0x004A	74	Restore iParameter watchdog time exceeded
0x004B	75	Inconsistent iParameters (iParCRC error)
0x004C	76	F_Block_ID not supported
0x004D	77	Transmission error: data inconsistent (CRC2 error)
0x004E	78	Transmission error: timeout (F_WD_Time or F_WD_Time_2 elapsed)
0x004F	79	Reserved: do not use numbers, do not evaluate numbers

F-Devices/Modules using the iPar-Server mechanism to store and retrieve iParameters within an F-Host or its controlled subsystem can report dedicated diagnosis information via separate additional codings.

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

Transmission errors (codes 77 and 78) shall not lead to diagnosis message flooding, for example via waiting on correct PROFIsafe communication first prior to new diagnosis messages.

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

Further information can be retrieved from [45] and [68].

7 Safety communication layer protocol

7.1 Safety PDU format

7.1.1 Safety PDU structure

Figure 18 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 for each F-Module its own safety PDU.

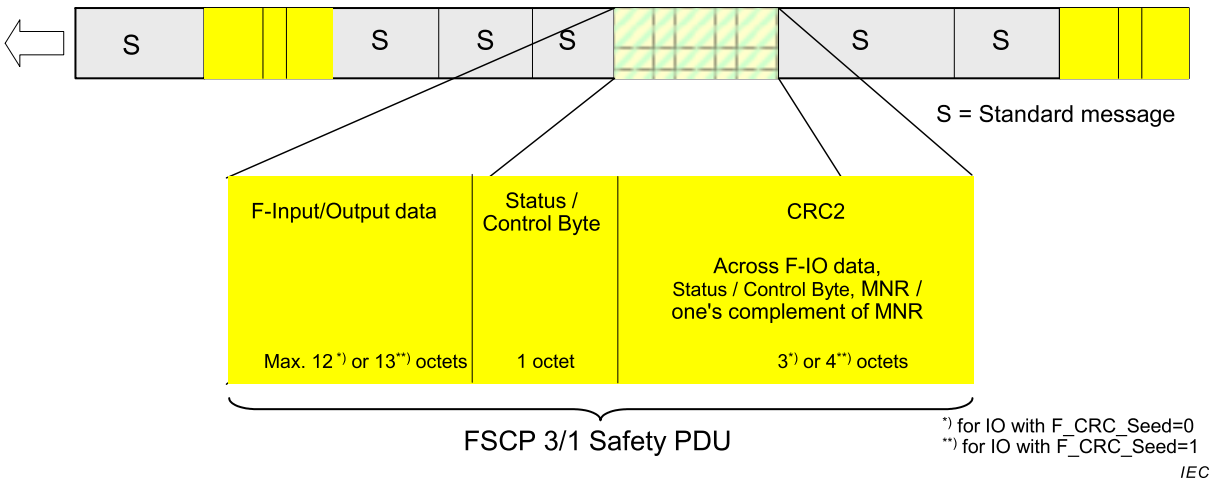


Figure 18 – Safety PDU for CPF 3

In addition to F-IO data (Figure 18 shows the minimum F-IO data an F-Host shall support), 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 7.1.9 provide a detailed description of the elements of the safety PDU structure.

7.1.2 Safety IO data

The F-IO data of the F-IO peripherals are accommodated in this safety PDU section. The data type coding corresponds to the one of CP 3/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 IO, light curtains, laser scanners, drives, etc.

Besides the compact devices, there are *modular devices* with F and standard IO units and subaddresses (Figure 13). 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.

7.1.3 Status and Control Byte

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

Figure 19 – Status Byte

The Status Byte shown in Figure 19 is contained in each safety PDU of a CP 3/RTE submodule transmitted from a device to its controller (Figure 18).

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

– Bit 1 at F_Passivation = 0 shall be set by the specific device technology firmware for at least two (2) changes of the MonitoringNumber, if an F-Device/Module is not able to

guarantee the safety integrity of the process data to be transmitted. Signal name in this implementation case is "Device_Fault".

– Bit 1 at F_Passivation = 1 shall be set by the specific device technology firmware if at least one of the channels of an F-Device/Module had been set to Fail-safe Values (FV) due to a signal channel fault and this fault is eliminated (cleared). Duration constraints for this signal are not necessary. A failure within the F-Device/Module (not within a single channel) shall cause each and every channel to switch to the fail-safe state and all qualifiers to bad. Signal name in this implementation case is "ChF_Ack_Req". See [66].

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

– Bit 3 is set if the F-Device is recognizing an F communication fault, 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 fault (Figure 17 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 change the virtual MonitoringNumber within the F-Host. Signal name is "Toggle_d".

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

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

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

Figure 20 – Control Byte

The Control Byte shown in Figure 20 is being sent with each safety PDU of a subslot from the IO-Controller to the device (Figure 18).

– 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 acknowledgment (OA_C) usually *via a LED* (9.1). Signal name is "OA_Req".

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

– Bit 3 is set when the F-Host driver gets informed via CiR input (Figure 15) that an intended update process of the safety fieldbus components in case of "Configure in Run" or "maintenance of a fault tolerant system" is taking place. This informs the F-Device to extend the watchdog time F_WD_Time once only by F_WD_Time_2 (see 6.1). Signal name is "Use_TO2".

– Bit 4 can be set to force the outputs of an F-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 change the virtual MonitoringNumber within the F-Device. See 7.1.4 for more details. Signal name is "Toggle_h".
– Bit 6 is set by the F application within an F-Host user program after clearance of at least one signal channel fault within an F-Device/Module indicated by Bit 1 (ChF_Ack_Req) of the Status Byte and personal has left the protection area. PV are activated. See [66]. Signal name is "ChF_Ack".
– Bit 7 is set to "1" for all F-Devices/F-Modules with implementations according to FSCP 3/1 versions prior to this release (F_CRC_Seed =0). Since these F-Devices/F-Modules will always return Status Bytes with Bit 7 = "0" a potential loop-back of messages can be detected by the F-Host driver if this Bit 7 returns "1". Signal name is "Loopcheck".
– Bit 7 is set to "0" for all F-Devices/F-Modules with a GSD entry F_CRC_Seed =1 and reserved for future use.

7.1.4 (Virtual) MonitoringNumber

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

FSCP 3/1 is not transmitting the MNR with each and every safety PDU. It uses a virtual MNR instead. It is called virtual due to the fact that it cannot be seen within the safety PDU. This approach uses MonitoringNumbers located within the F-Host and the F-Device and a Toggle Bit within the Status Byte and the Control Byte to change the appropriate MNR synchronously (Figure 21).

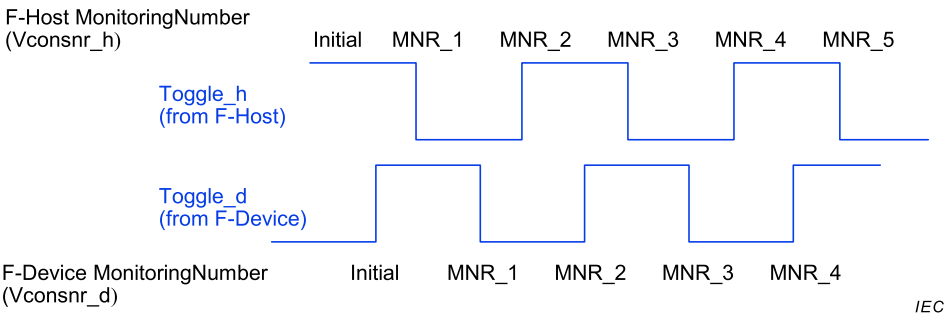


Figure 21 – The Toggle Bit function

The checking for correctness and for the synchronism of the two independent MNR is performed by including the MonitoringNumbers in the CRC2 calculation. CRC2 then is transmitted with each and every safety PDU (Figure 22).

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

Figure 22 illustrates the mechanism for the MNR within the F-Device. The MNR is reset when the F-Host sends R_cons_nr = "1" within the Control Byte (see 7.1.3).

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

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

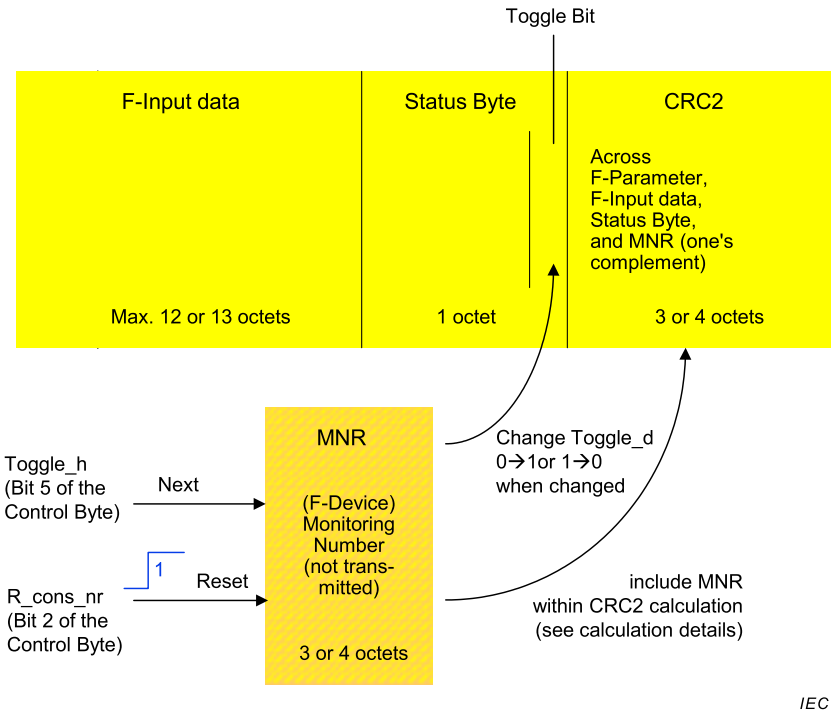


Figure 22 – F-Device MonitoringNumber

7.1.5 (Virtual) MNR mechanism (F_CRC_Seed=0)

FSCP 3/1 uses *24 bit counters* for the MonitoringNumber in this case. Thus, the Monitoring-Number counts in a cyclic mode from 1 to 0xFFFFFF, wrapping over back to 1 at the end (see Table 4 and Table 5). The counter value is represented by MNR.

Table 4 – MonitoringNumber of an F-Host PDU

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

Table 5 – MonitoringNumber of an F-Device PDU

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

7.1.6 (Virtual) MNR mechanism (F_CRC_Seed=1)

FSCP 3/1 provides an extended procedure that is activated via the GSD entry "F_CRC_Seed" =1 (see 8.1.5.2). It allows for the compatibility to IEC 65C/747/CD:2013, especially to the fault model of implicit transmission.

This procedure splits the use of MonitoringNumber into two phases. The first phase is characterized as systemstart (INITIALx) or in case of fault and as long as Bit 2 (R_cons_nr) in the

Control Byte is set to "1" (RESETx). The second phase is characterized as cyclic communication. "CRC_FP+" is the 32 bit CRC signature (*0xF4ACFB13*) which includes the same F-Parameters as "CRC_FP" (see Table 6 and Table 7).

Table 6 – MonitoringNumber of an F-Host PDU

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

Table 7 – MonitoringNumber of an F-Device PDU

MACRO	ACTION (Pseudocode)
INITIALxD	MNR= one's complement of CRC_FP+; CN_incrNR_64 [1] = 0x5851F42D4C957F2D * Codename; SwapHL = shl (CN_incrNR_64 [1], 32) + shr (CN_incrNR_64 [1], 32); Modifier = received CRC2 XOR calculated CRC2 according 7.1.8; no CRC2 check in state 22; CN_incrNR_64 [2] = 0xAB16D2792302FE5A * (SwapHL + Modifier) +1;
RESETxD	cons_nr_R =1; MNR= one's complement of CRC_FP+; CN_incrNR_64 [1] = 0x5851F42D4C957F2D * Codename; SwapHL = shl (CN_incrNR_64 [1], 32) + shr (CN_incrNR_64 [1], 32); Modifier = received CRC2 XOR calculated CRC2 according 7.1.8; no CRC2 check in states 22, 25, and 28; CN_incrNR_64 [2] = 0xAB16D2792302FE5A * (SwapHL + Modifier) +1;

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

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

CN_incrNR_64 [0], CN_incrNR_64 [1], CN_incrNR_64 [2], and SwapHL are unsigned 64 bit variables. CRC_FP+, CRC2, and Modifier are unsigned 32 bit variables.

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

An example of the first 5 values of the MonitoringNumbers is shown in Table A.4. The MonitoringNumber is a 32 bit value. The "one's complement" is used to differentiate between safety PDUs from the F-Host and safety PDUs from the F-Device in order to detect a Loopback error.

For Codename see 8.1.2.

7.1.7 CRC2 Signature (F_CRC_Seed=0)

In case of F_CRC_Seed = 0, the following applies: Once the F-Parameters (source-destination relationship or Codename, SIL, watchdog times, etc.) have been transferred to the F-Device, the identical parameters are employed in an identical procedure in the F-Host and in the F-Device/Module for producing a CRC_FP signature as a seed value for the calculation of CRC2 that is transferred cyclically. For information on how this CRC_FP is build, see 8.3.3.2. This CRC_FP signature, the F-IO data, the Status or Control Byte and the corresponding MNR are used for generating another 3 octet CRC2 signature within the F-Host (see Figure 23).

In the F-Device, the identical CRC2 signature is generated and the signatures are compared. The subsequent cyclic transfers require only a CRC2 signature comparison (that can be done very rapidly).

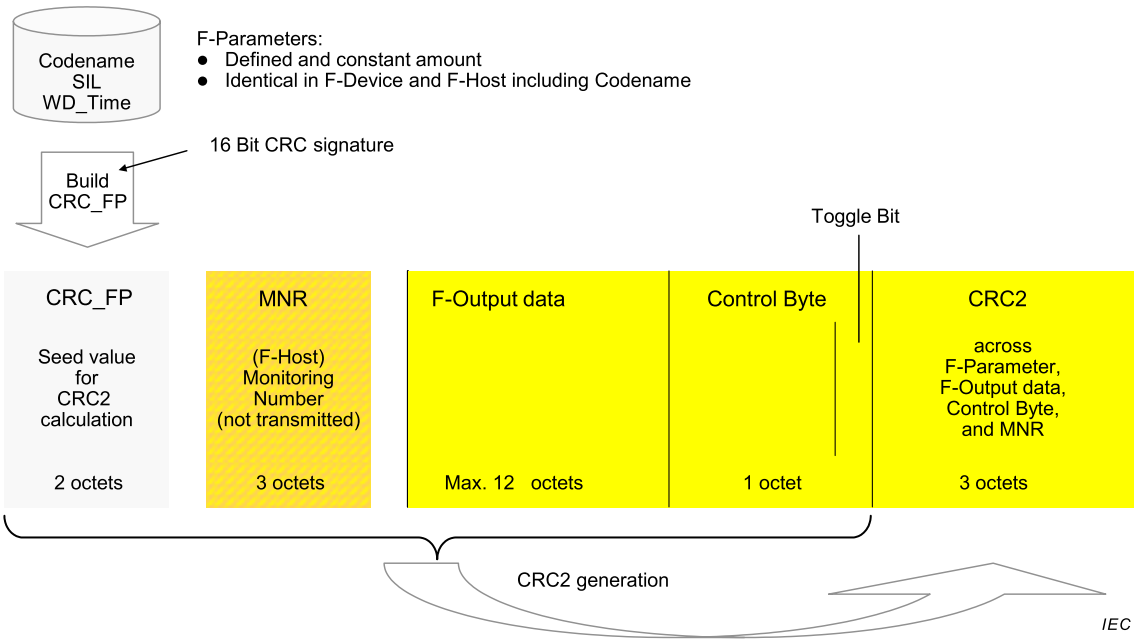


Figure 23 – F-Host CRC2 signature generation (F_CRC_Seed=0)

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.

For better error detection even if there are identical CRC polynomials within the black channel and in the safety layer, the CRC2 signature calculation includes the octets of Figure 23 in reverse order (see Figure 24).

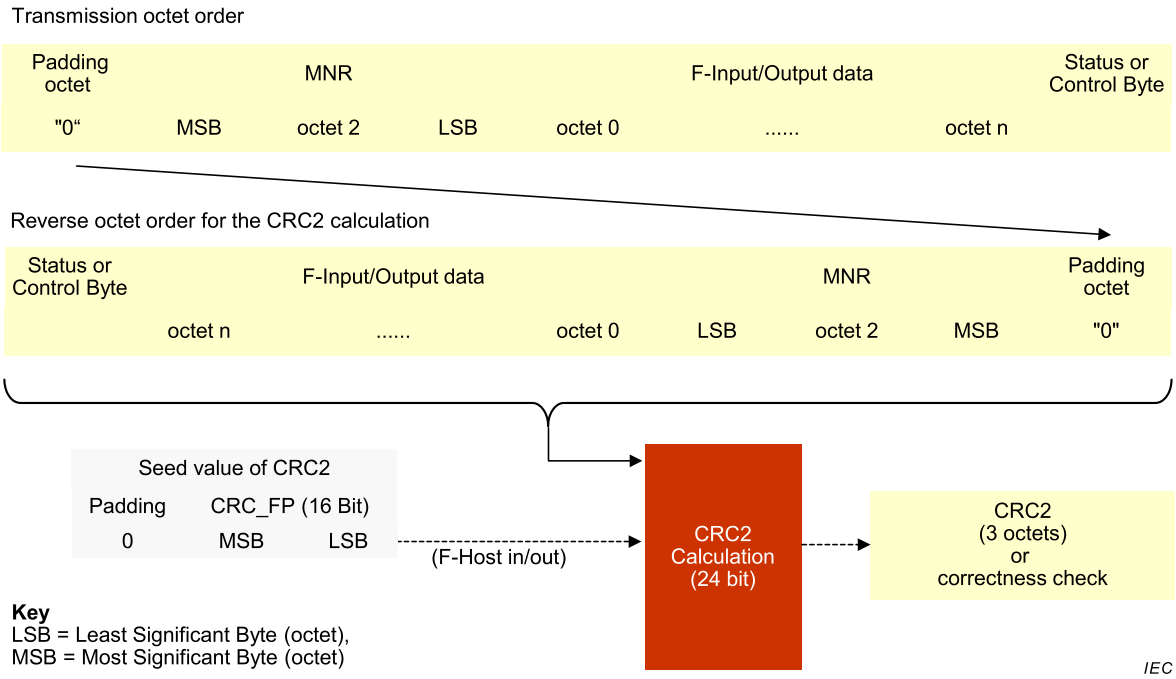


Figure 24 – Details of the CRC2 signature calculation (F_CRC_Seed=0)

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

7.1.8 CRC2 Signature (F_CRC_Seed=1)

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

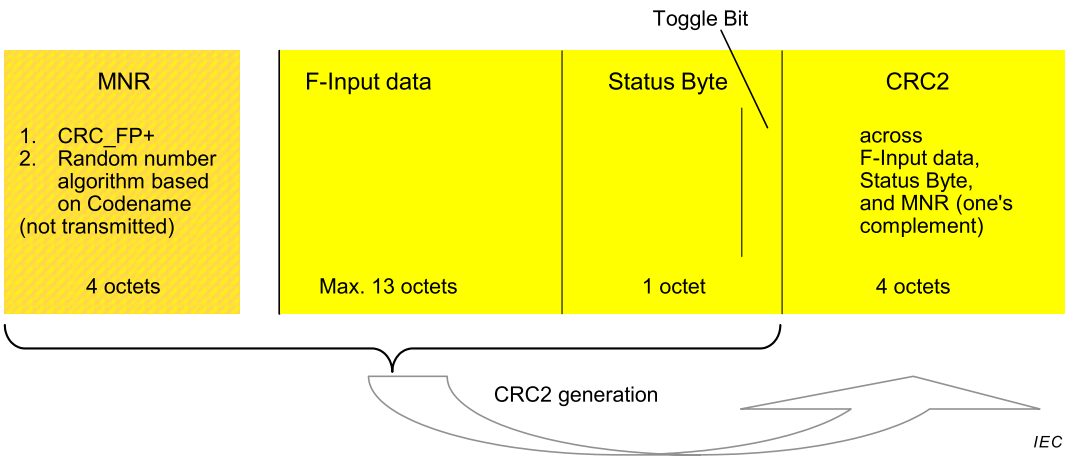


Figure 25 – CRC2 signature calculation (F_CRC_Seed=1)

The CRC2 signature calculation includes the octets in reverse order (see Figure 26).

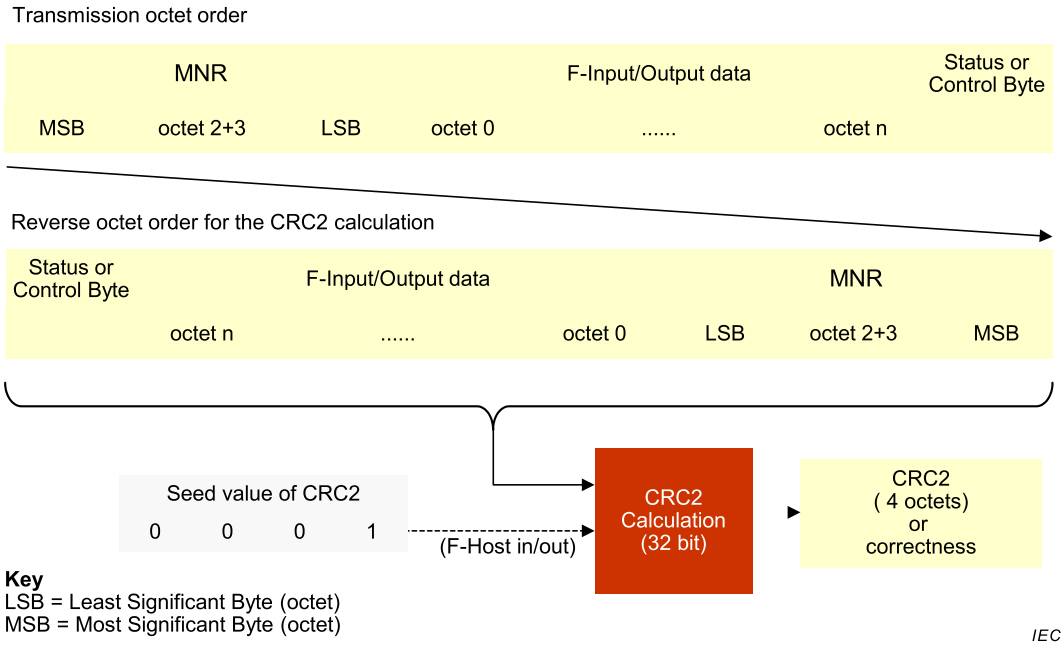


Figure 26 – Details of the CRC2 signature calculation (F_CRC_Seed=1)

The F-Host driver uses the same CRC2 signature calculation procedure in Figure 26 to check the correctness of the F-Device safety PDU including the Status Byte, F-Input data, and the one's complement of the MNR.

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

7.1.9 Non-safety IO data

Non-safety IO data cannot be appended to a safety PDU. For compact F-Devices, this can be achieved by allocating separate virtual slot or subslot identifications. F-modules within mixed 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 MNR. The monitoring of safety PDU transit times is described in 7.2.6.

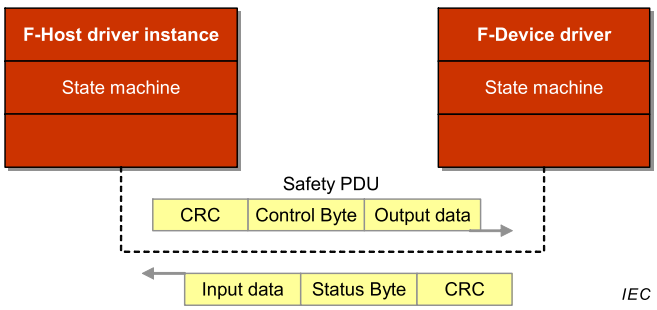


Figure 27 – Safety layer communication relationship

7.2.2 F-Host state diagram

Figure 28 shows the F-Host state diagram and Table 9 describes the F-Host states, transitions, and internal items. The diagrams are following the UML2 notation.

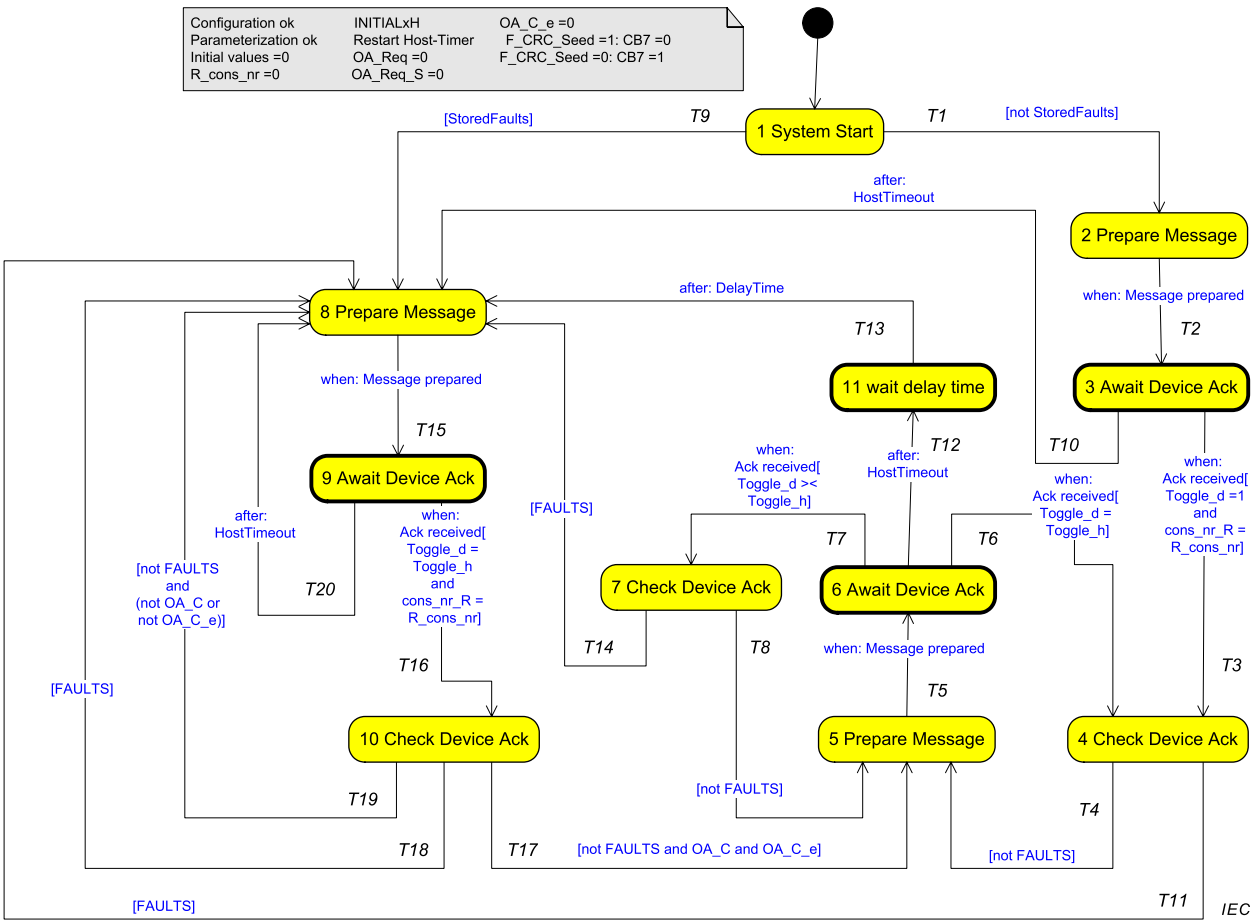


Figure 28 – F-Host state diagram

The terms used in Figure 28 are specified in Table 8.

Table 8 – Definition of terms used in F-Host state diagram

Term	Definition
Initial values	Any safety PDU values =0
HostTimeout	F-Host recognizes local timeout while awaiting an F-Device acknowledgment within F_WD_Time. This HostTimeout shall be extended once only by F_WD_Time_2 in case of "use_TO2" = 1 (F_WD_Time + F_WD_Time_2), similar to the F-Device (see 6.1, 8.1.4).
Host_CE_CRC	F-Host recognizes CRC fault while analyzing the received safety PDU
Device_Fault	F_Passivation =0 (see 8.1.6.2): F-Device reported fault 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
INITIALxH	Macro see 7.1.5 and 7.1.6
FAULTS	This variable is true (=1) if one of the following bit is set: - SB2 (CE_CRC) - SB3 (WD_timeout) - SB7 (Status Byte, Bit7), if F_CRC_Seed =0 - Host_CE_CRC
StoredFaults	This variable is true (=1) if any of the FAULTS bit and/or HostTimeout had been stored at shut down
Ack received	Any new safety PDU received; ignore safety PDU with all values = 0

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

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

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

Table 9 – 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 (Acknowledgment).
4 Check Device Ack	Check received safety PDU for a CRC-error (Host_CE_CRC) including virtual MNR 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 (Acknowledgment)
7 Check Device Ack	Check received safety PDU for a CRC-error (Host_CE_CRC) including previous (old_MNR) virtual MNR 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 (Acknowledgment)
10 Check Device Ack	Check received safety PDU for a CRC-error (Host_CE_CRC) including virtual MNR 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 acknowledgment signal (OA_C) arrived.

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

TRAN-SITION	SOURCE STATE	TARGET STATE	ACTION
			else use PVo, activate_FV =0 iPar_OK_S =iPar_OK
T18	10	8	store faults, OA_Req =0, OA_Req_S =0, OA_C_e =0, use FV, activate_FV =1, FV_activated_S =1, Toggle_h = not Toggle_h, RESETxH
T19	10	8	OA_Req_S =1, OA_Req =1, if OA_C =0 then OA_C_e =1 use FV, activate_FV =1, FV_activated_S =1, Toggle_h = not Toggle_h, RUNxH
T20	9	8	store faults, OA_Req =0, OA_Req_S =0, OA_C_e =0, use FV, activate_FV =1, FV_activated_S =1, Toggle_h = not Toggle_h, RESETxH restart host-timer

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

b Device Fault is not considered in the logic operation if F-Passivation =1.

INTERNAL ITEMS	TYPE	DEFINITION
RESETxH	Macro	See 7.1.5 and 7.1.6
RUNxH	Macro	See 7.1.5 and 7.1.6
MNR	Variable	MNR is representing the local MonitoringNumber within the F-Host driver instance. It is not transmitted to its counterpart within the F-Device, but is synchronizing those via a Toggle Bit in the Control Byte. The actual MNR is incorporated in the CRC2 calculation and thus checked against transmission faults.
old_MNR	Variable	Previous value of the current local MNR. It is necessary to store this previous value of the MNR.
DelayTime	Timer	This delay time is to cover power off settling time within the whole system. It is within the host/system manufacturer's responsibility to define this parameter.
host-timer	Timer	This timer checks whether the next valid safety PDU from the F-Device did arrive in time. The host engineering tool is responsible to define this watchdog time. Value range is 0 to 65 535 ms.
OA_C_e	Flag	By means of this auxiliary variable (bit) it is ensured that the safe state will be left only after a signal change of OA_C from 0 → 1 (edge). Without this mechanism an operator could overrule safe states by permanently actuating the OA_C signal.
faults	Flags	Until an operator acknowledgment (OA_C), persistent storage of the FAULT bit (see Table 8) is required within the F-Host only (no F-Device persistence):
	Activity State	Within these interruptable "activity" states the host waits for new inputs such as timeout or acknowledgment [34].
	Action State	Within these non-interruptable "action" states events like timeout, message received or operator acknowledgment 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 11 describes the states, transitions, and internal items. The diagrams are following the UML2 notation.

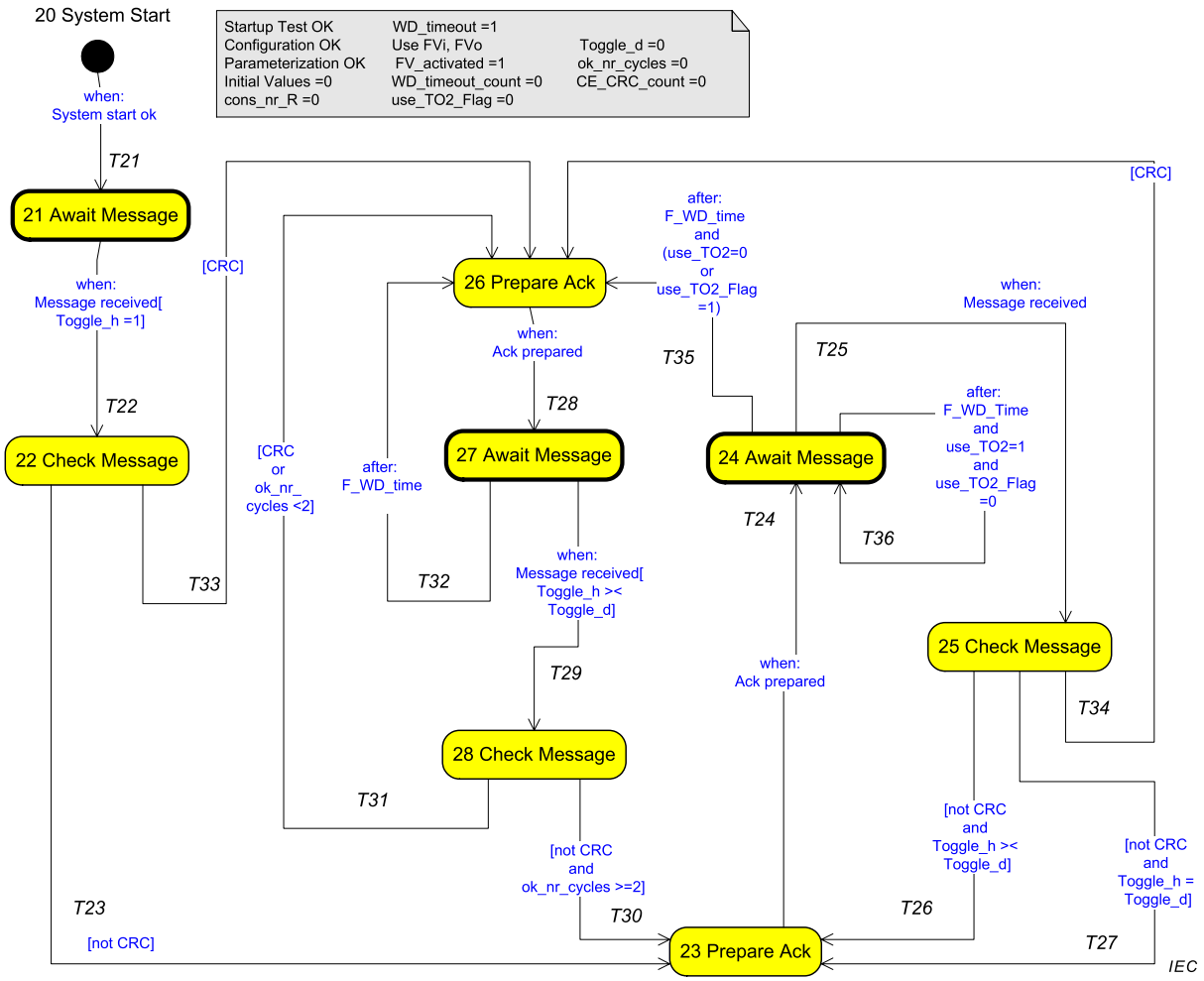


Figure 29 – F-Device state diagram

The terms used in Figure 29 are specified in Table 10.

Table 10 – Definition of terms used in Figure 29

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

Table 11 – 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 MNR
23 Prepare Ack	Preparation of regular safety PDU for the F-Host (Acknowledgment)
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 MNR
26 Prepare Ack	Preparation of safety PDU for the F-Host (Acknowledgment with fault bits)
27 Await Message	Safety Layer is waiting on next safety PDU from F-Host (exception handling)
28 Check Message	Check received safety PDU for CRC-error including virtual MNR

TRAN-SITION	SOURCE STATE	TARGET STATE	ACTION
T21	20	21	-
T22	21	22	**if** R_cons_nr =1 **then** RESETxD **else** INITIALxD
T23	22	23	use PVi, FVo, FV_activated =1, CE_CRC =0, WD_timeout =0, Toggle_d =Toggle_h, restart device-timer, ok_nr_cycles =ok_nr_cycles +1
T24	23	24	send safety PDU

T25	24	25	**if** Toggle_h >< Toggle_d
			then
			  restart device-timer
			  if R_cons_nr =1 and activate_FV =1
			  then RESETxD
			  else RUNxD

T26	25	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 **if** use_TO2 =0 **then** use_TO2_Flag =0
T27	25	23	Use PVi, Toggle_d = Toggle_h, **if** ok_nr_cycles <4 **then** use FVo, FV_activated =1 **else** use PVo, FV_activated =0 **if** activate_FV =1 **then** use FVo
T28	26	27	Send safety PDU
T29	27	28	**if** R_cons_nr =1 **then** RESETxD **else** RUNxD

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_cycles =0, restart device-timer, Toggle_d = Toggle_h
T35	24	26	Use PVi, FVo, FV_activated =1, WD_timeout =1, WD_timeout_count =1, ok_nr_cycles =0, restart device timer, Toggle_d = Toggle_h
T36	24	24	restart device timer with F_WD_Time_2 use_TO2_Flag =1

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

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

7.2.4 Sequence diagrams

Figure 30 to Figure 35 show 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 shows the regular start of safety PDU transmissions between F-Host and F-Device after power on. A possible sequence of MonitoringNumbers is shown in Table A.4.

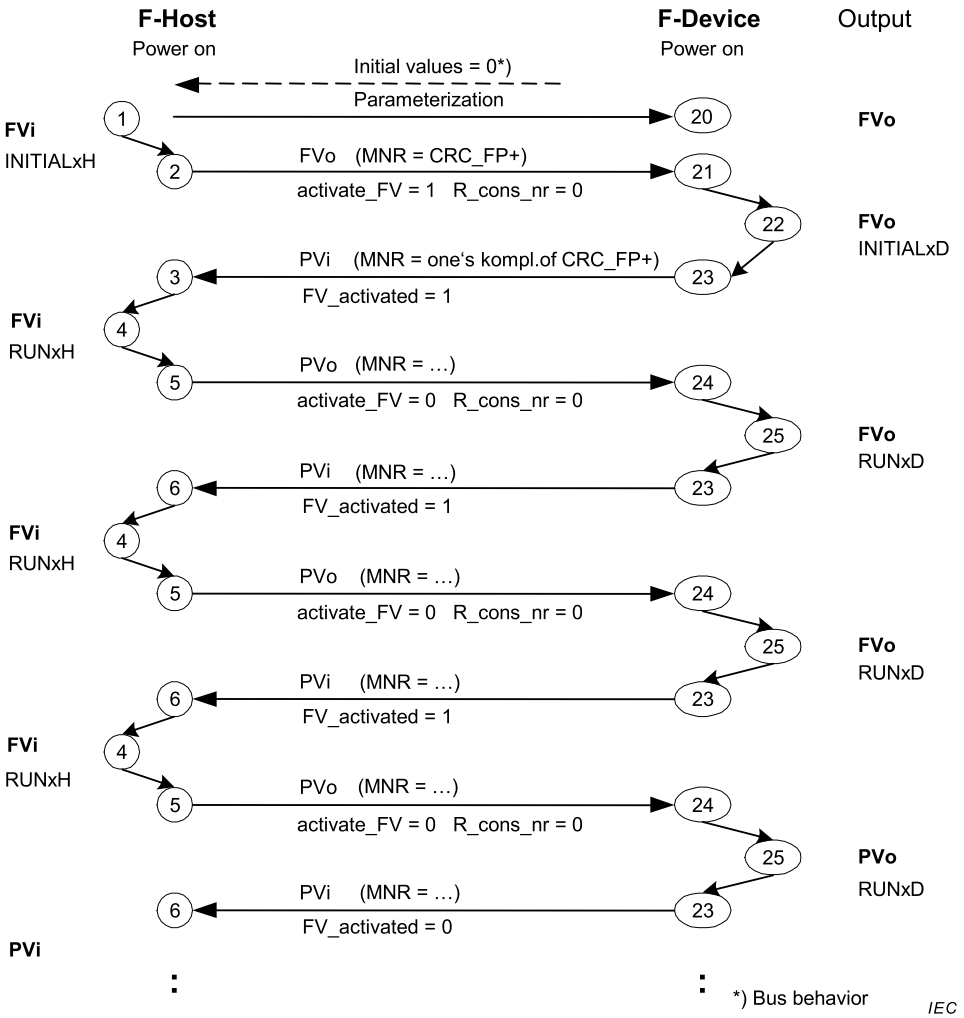


Figure 30 – Interaction F-Host / F-Device during start-up

Figure 31 shows an example with F-Parameter assignment in case the F-Device is already operating and the F-Host is switching from power off to power on.

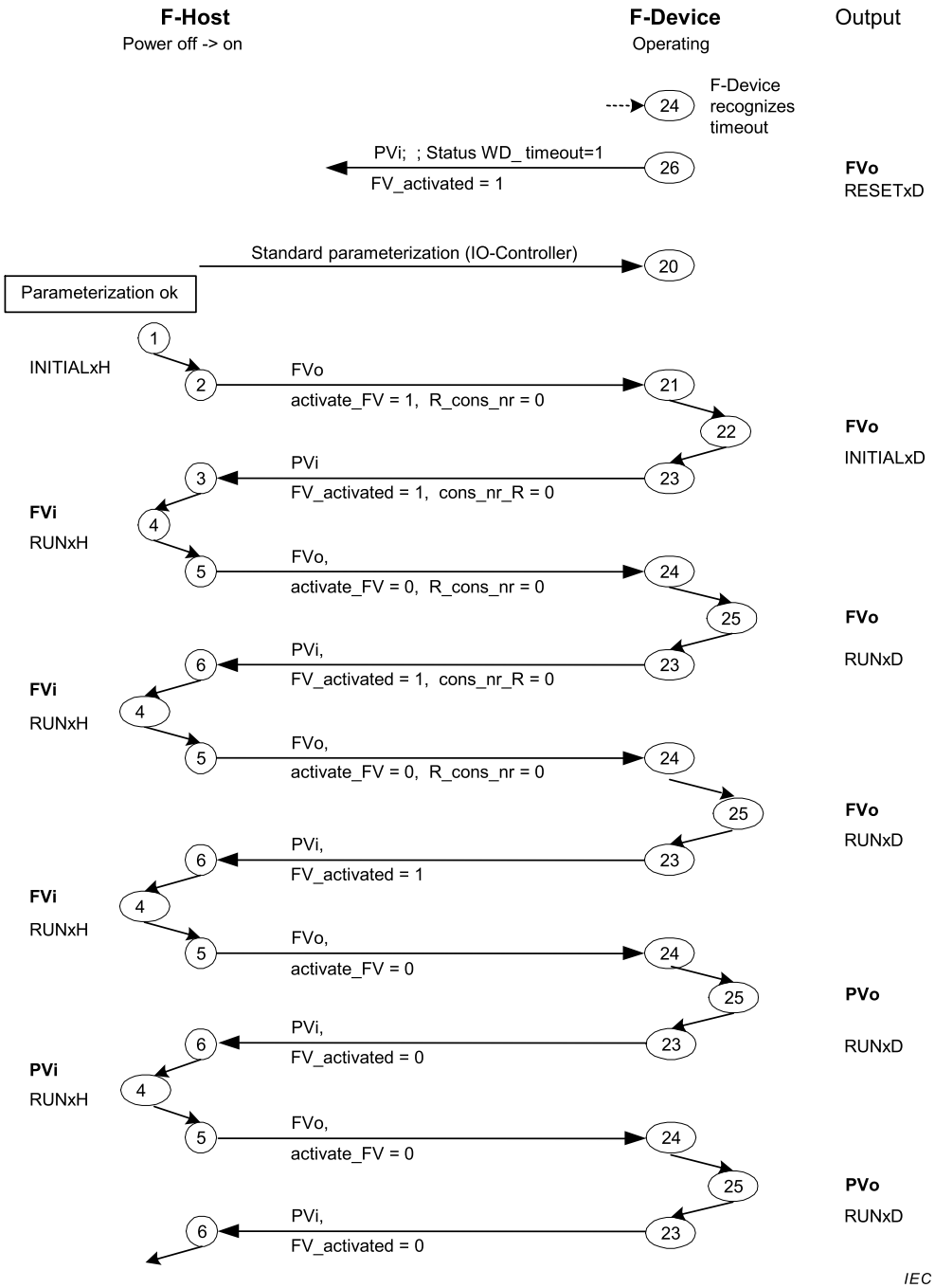


Figure 31 – Interaction F-Host / F-Device during F-Host power off → on

Figure 32 shows an example with F-Parameter assignment in case the F-Host is already operating and the F-Device is switching power on after a delay.

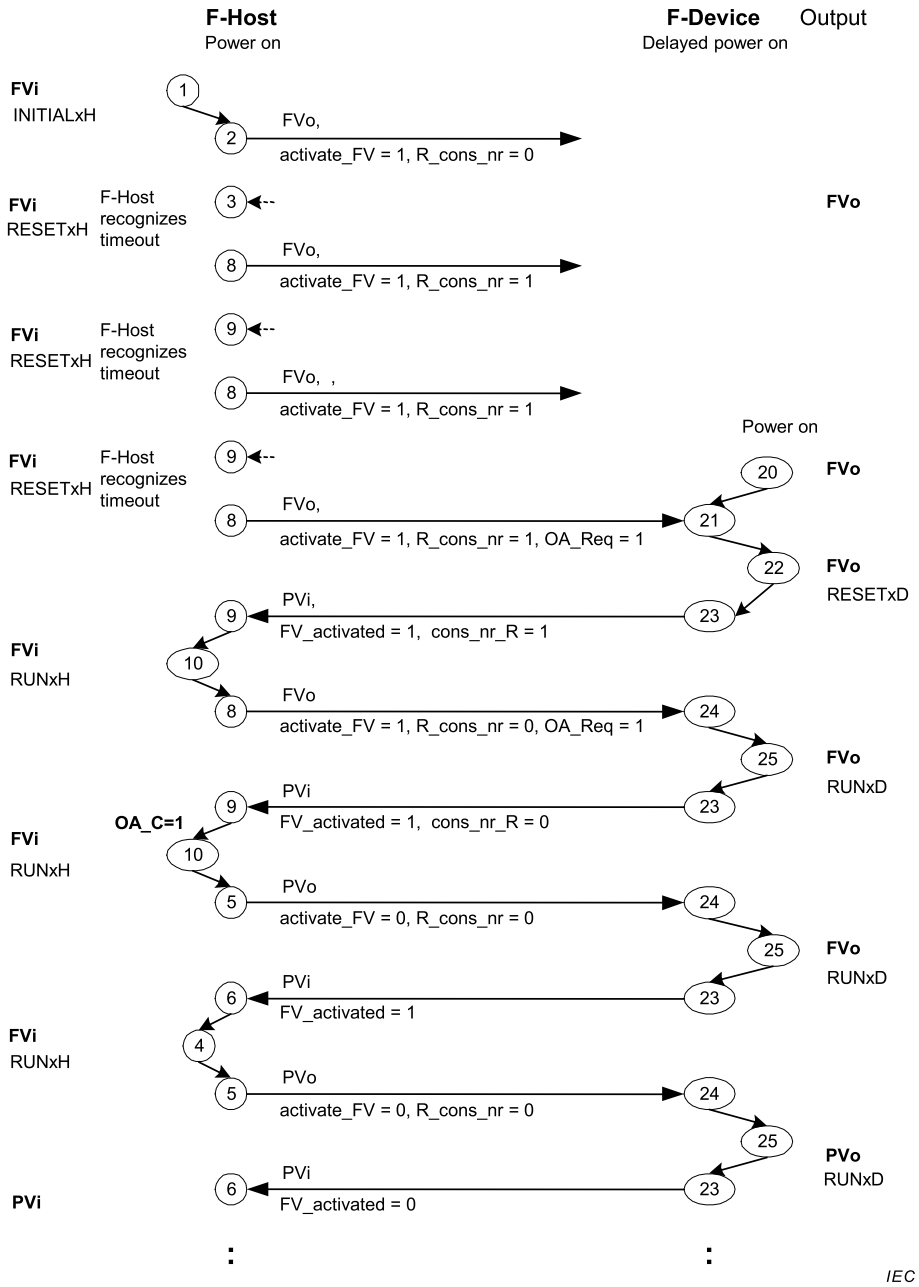


Figure 32 – Interaction F-Host / F-Device with delayed power on

Figure 33 corresponds to Figure 32. It shows the case when the F-Host is already operating and the F-Device switches power off and after a delay switches power on again.

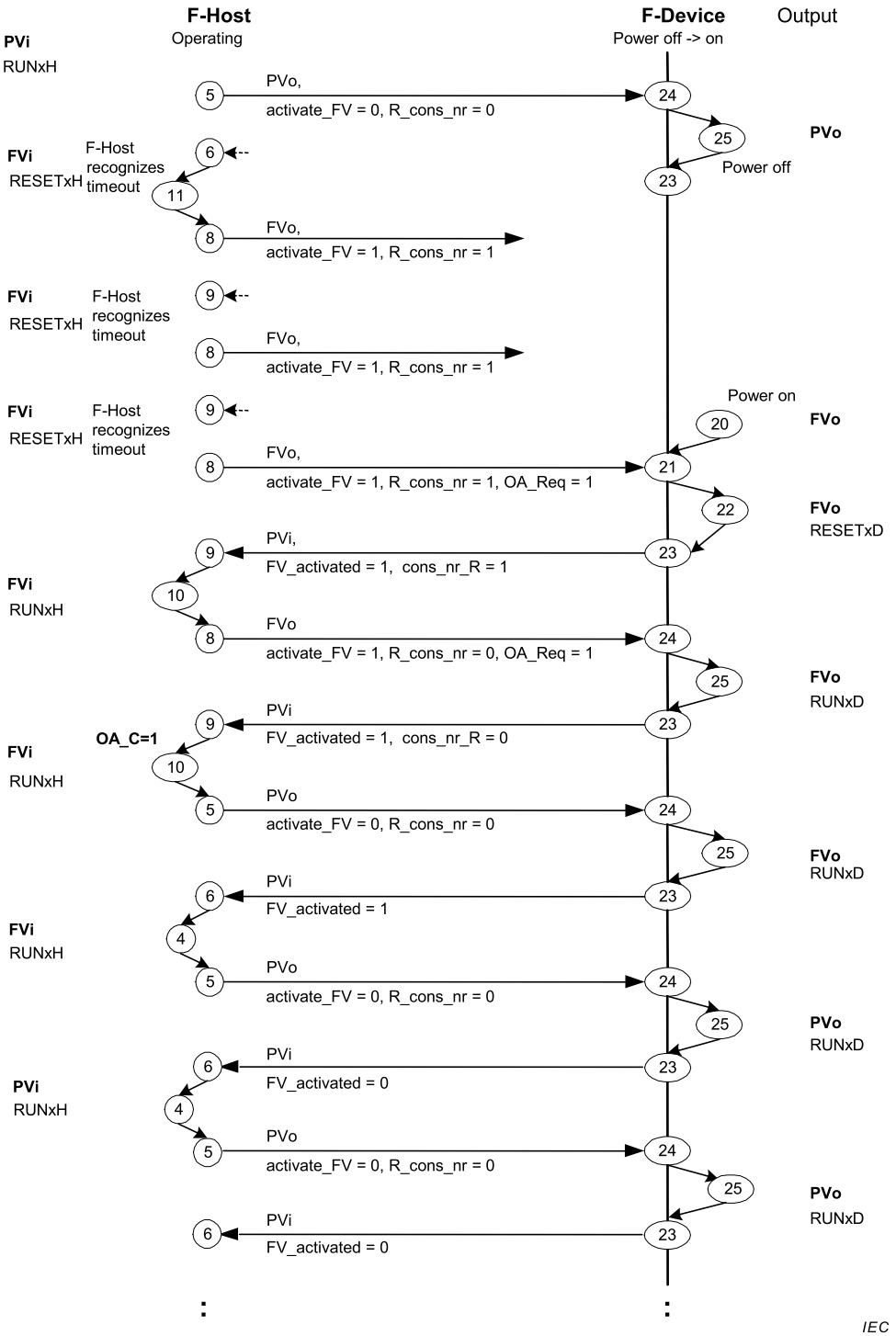


Figure 33 – Interaction F-Host / F-Device during power off → on

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

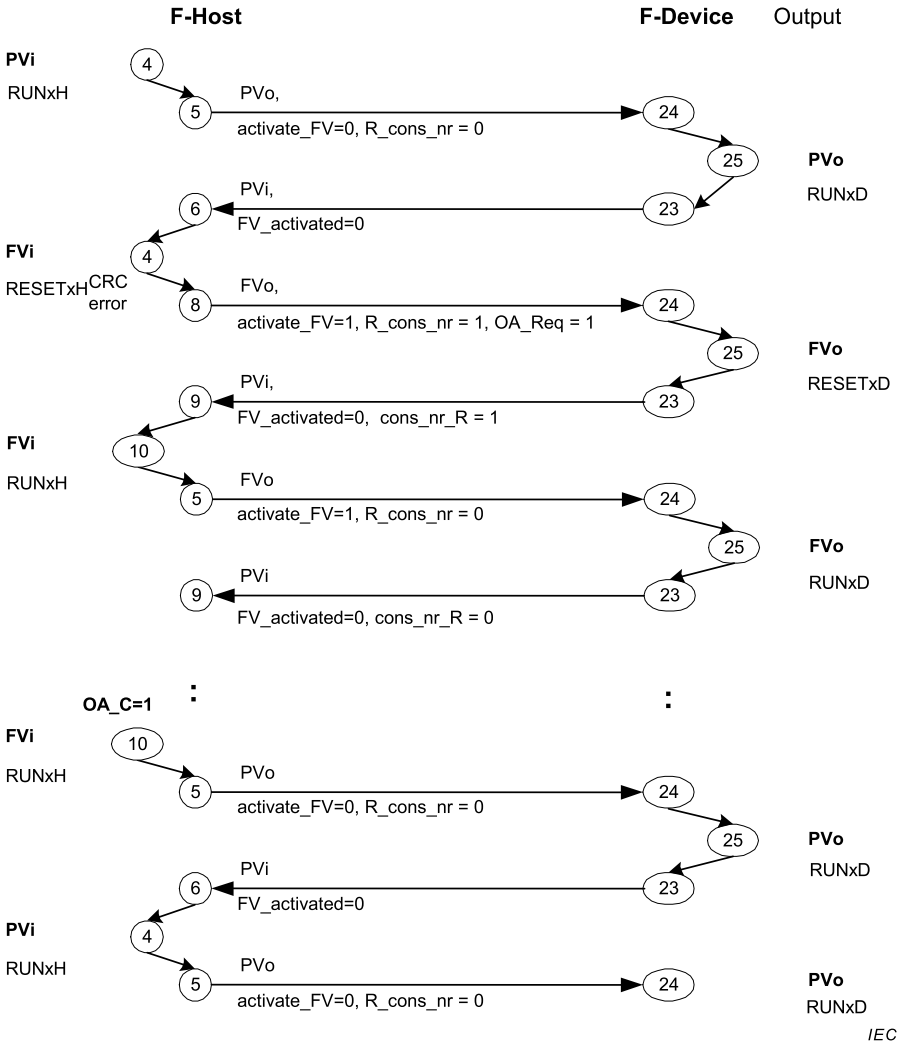


Figure 34 – Interaction F-Host / F-Device while host recognizes CRC error

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

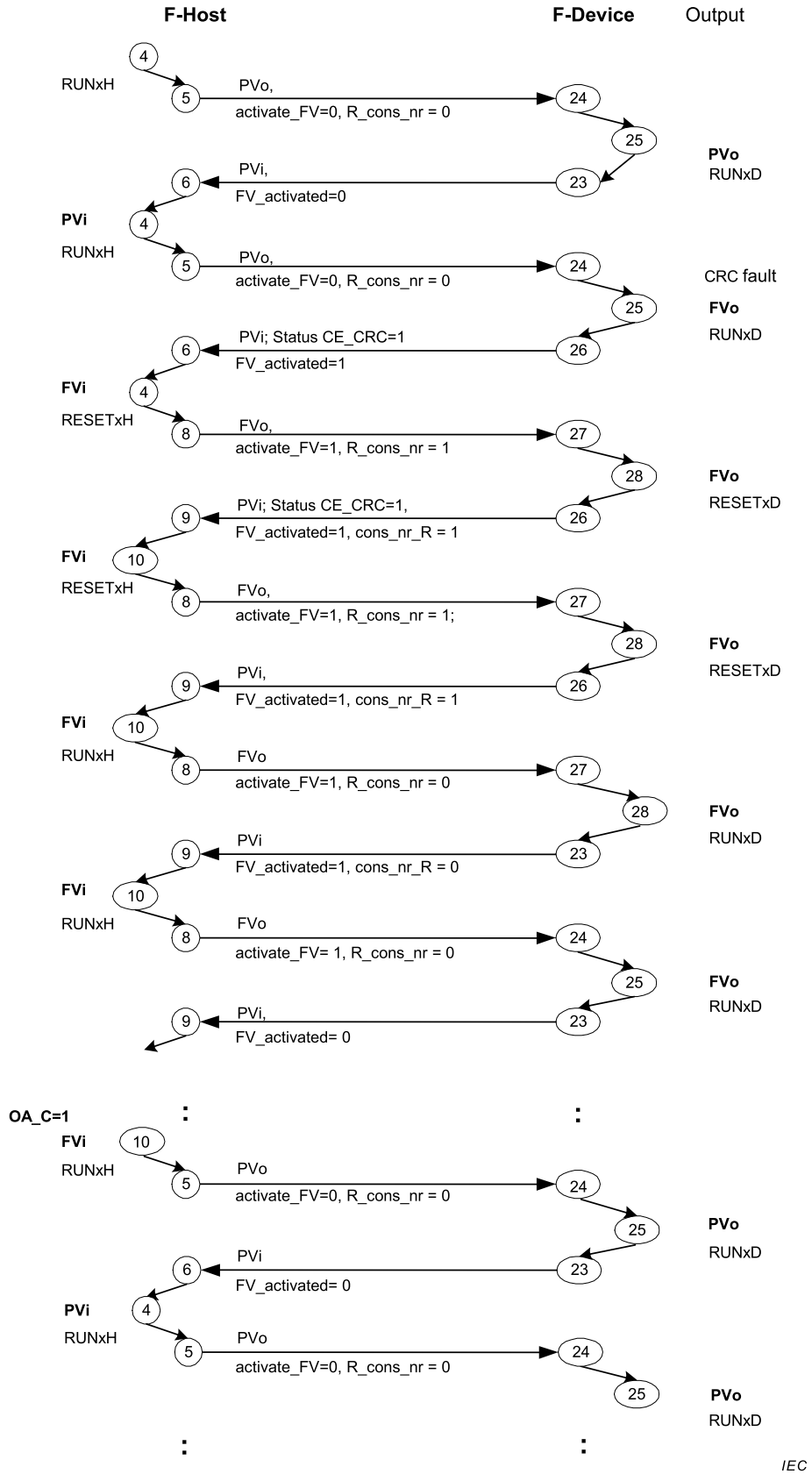


Figure 35 – Interaction F-Host / F-Device while device recognizes CRC error

7.2.5 Timing diagram for a MonitoringNumber reset

Figure 36 demonstrates the consequences of an F communication fault on the Monitoring-Number and depending items.

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

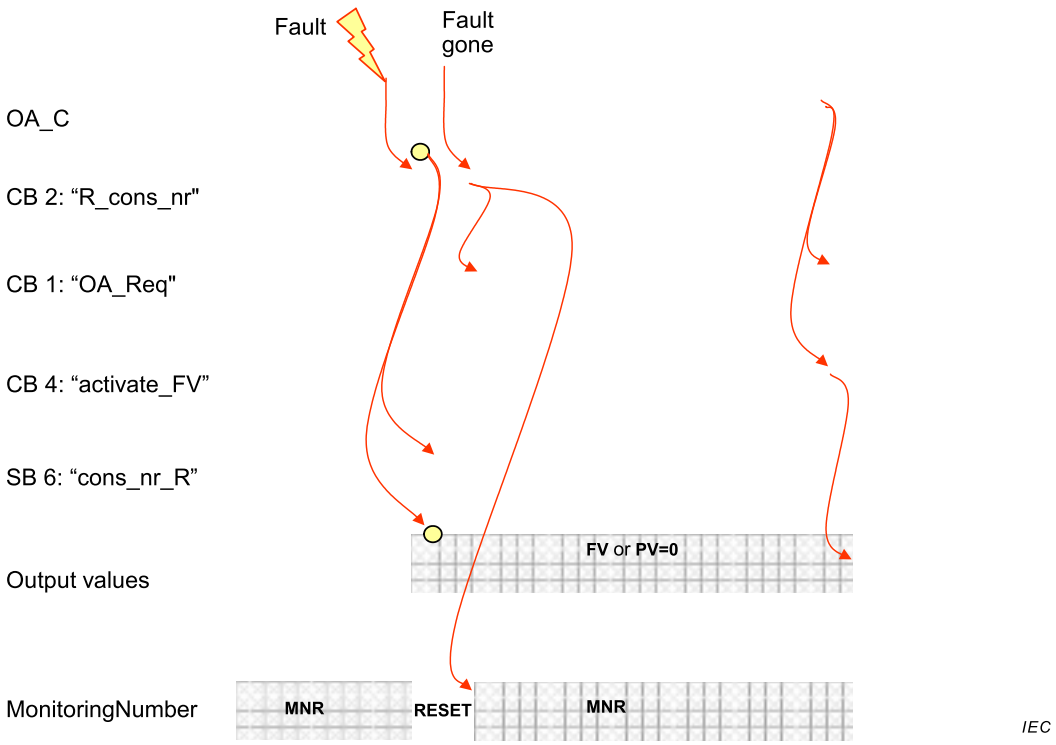


Figure 36 – Impact of the MNR reset signal

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 Acknowledgment is requested (OA_C). Right after the fault is gone the following actions take place:

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

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

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

7.2.6 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. In return the F-Device is sending the (acknowledgment) safety PDU to the IO- Controller more frequently than the F Driver in the F-Device is generating a new safety PDU.

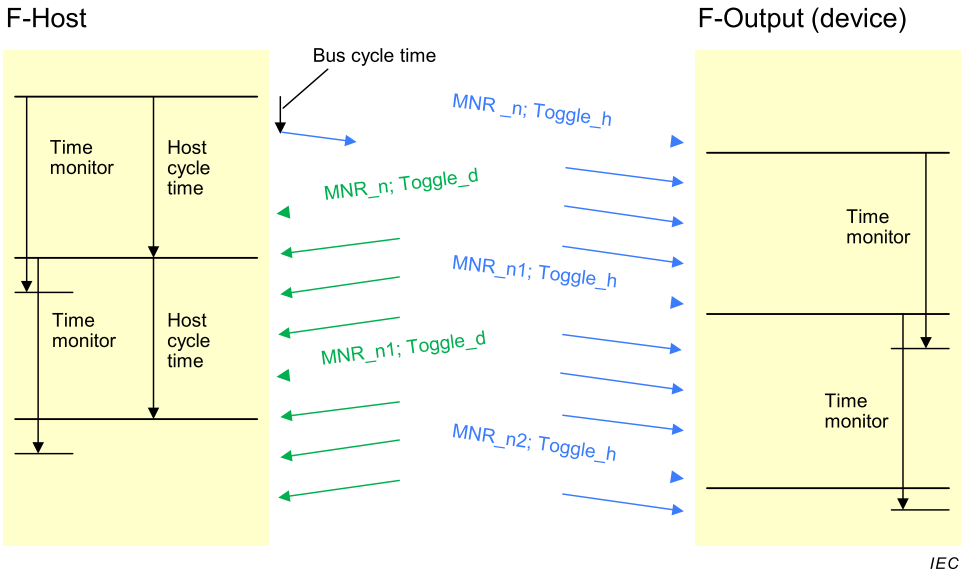


Figure 37 – Monitoring the message transit time F-Host ↔ F-Output

Figure 37 shows 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 represent FSCP 3/1 PDUs with the currently valid (virtual) MNR but possibly different process values.

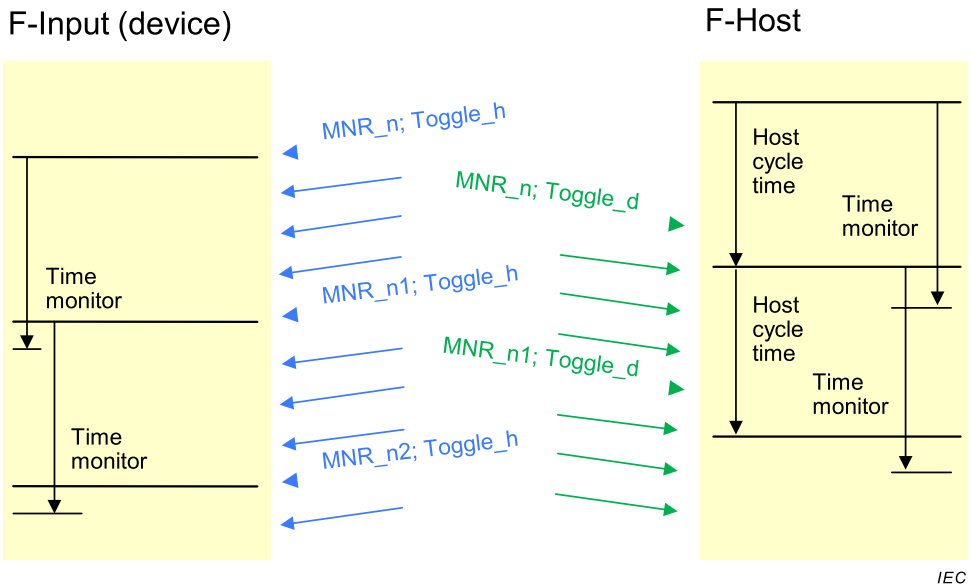


Figure 38 – Monitoring the message transit time F-Input ↔ F-Host

Other timing constraints are listed below:

Startup
(Synchronization)
: To synchronize after a system start, the F-Host driver starts with the virtual initial MNR (see 7.1.5 and 7.1.6).

F protocol cycle
: An F-Input/F-Output returns a safety PDU to the F-Host with the same virtual MNR (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 MNR

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

Safety PDU repetition

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

SIL monitor

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

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

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

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

SIL Monitor time period (T)

The SIL monitor time period T is a constant value with the dimension hour (h) that results from the requested SIL and the configured CRC length (9.5.1). Table 12 specifies the SIL monitor times.

Table 12 – SIL monitor times

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

7.2.6.2 Extended watchdog time on request after user interaction

For use cases such as 'Configure in Run' [64] 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 only (see Figure 41) a secondary watchdog time (F_WD_Time_2) to extend the primary watchdog time for these cases as shown in Figure 39.

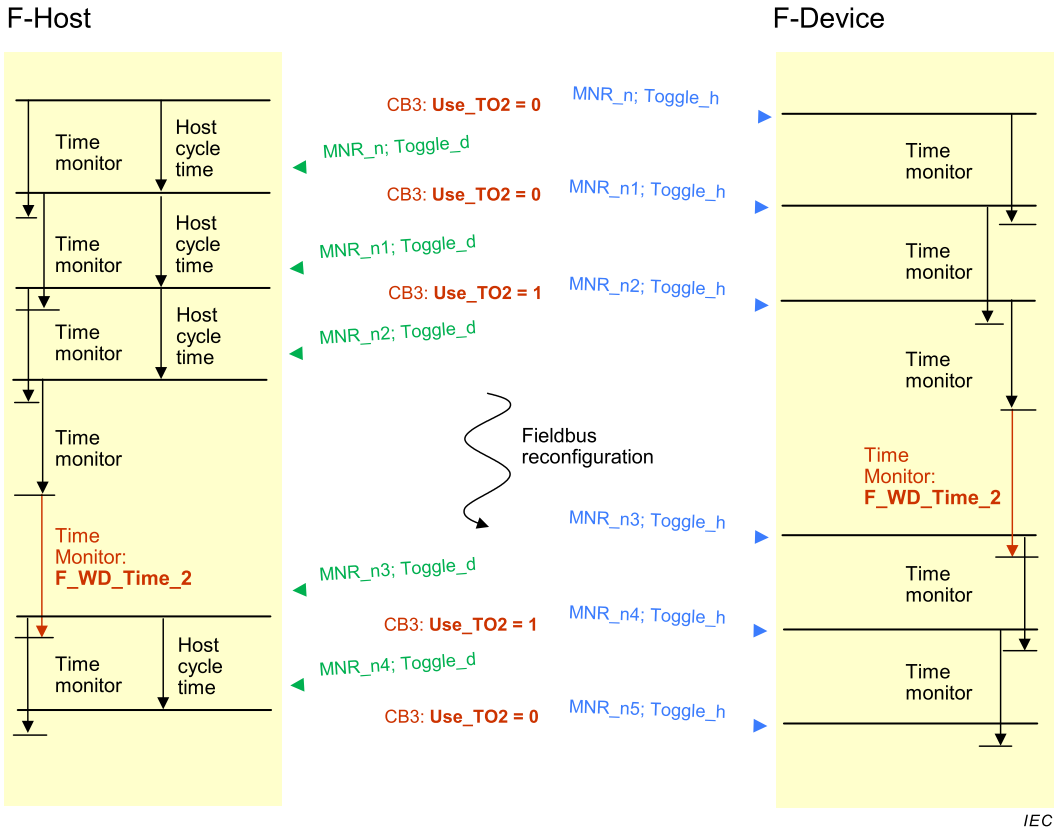


Figure 39 – Extended watchdog time on request

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

7.3 Reaction in the event of a malfunction

7.3.1 Unintended repetition

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

Remedial action: The data within the Black Channel 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 (demand) can be *one watchdog time (see 9.3.3).*

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

7.3.2 Loss

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

Remedial action: Lost information will be discovered by stringently changing and examining the MNR and/or watchdog time within the safety communication layer of the respective recipient.

7.3.3 Insertion

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

Remedial action: Due to the stringently sequential expectation of the MNR, the recipient will detect an inserted safety PDU.

7.3.4 Incorrect sequence

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

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

7.3.5 Corruption of safety data

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

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

The CRC2 signature is generated across the F-Parameters respectively, the F-IO data, the virtual MNR, and the Control/Status Byte (see 7.1.7, 7.1.8, Figure 24, and Figure 26).

7.3.6 Unacceptable 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 PDUs so that a service that belongs to the safety PDU is delayed or prevented."

Remedial action:

- Toggle bit within Control Byte and Status Byte (see 7.1.3)
- Watchdog time in the respective recipient (watchdog time for F communication).

The watchdog time is defined in 9.3.3.

7.3.7 Masquerade

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

Remedial action: The recipient detects (safety) PDUs from senders with incorrect authenticity via the CRC2 signature. The possibility that a non-safety related or unauthorized sender is able to generate an expected FSCP 3/1 safety PDU with the correct CRC2 can be excluded.

7.3.8 Addressing

Principle of safe connection authentication:

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 connection since Codename and direction are included in the CRC via MNR (see 7.1.7, 7.1.8 and 7.3.10).

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

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

Sabotage is not assumed.

7.3.9 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 incorporated safety PDUs 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 incorrect destination or their data content can be perturbed. Furthermore a switch can send stored messages over and over again even when the sender already was shut down. Table 13 contains a list of possible switch faults and their remedial measures to achieve sufficient safety.

Table 13 – Remedies for switch failures

Fault type	Detection and Mastering
Perturbed data	CRC signature (24/32 bit)
Incorrect destination	Codename (2 × 16 bit)
Lost safety message	MonitoringNumber (24/32 bit) and Timeout
Duplicated message	MonitoringNumber (24/32 bit)
Delayed message	Timeout
Retransmission of stored messages with less than 3 consecutive safety PDUs in series. The F-Host is no longer connected.	MonitoringNumber (24/32 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.	MonitoringNumber (24/32 bit) and fault reaction via the Control Byte (Figure 36)

The following faults are detected / mastered:

- The F-Host fails or its safety PDUs do not reach the receiver. A switch transmits the messages of its revolving buffer without the correct MNR instead. The F-Device recognizes a MNR fault and sets Fail-safe Values (FV).
- A single message of the switch buffer is retransmitted and has a safety PDU with the correct MNR. This fault will be detected due to the 24/32 bit MNR and the fact that the restart of the F-Output-Device needs an OA_C = 1 (Operator Acknowledgment).
- A switch transmits messages with safety PDUs out of its revolving buffer with the correct MNRs and this message sequence starts within the safety watchdog time. This fault will be detected due to the 24/32 bit MNR and the fact that the restart of the F-Output-Device needs an OA_C = 1 (Operator Acknowledgment).

7.3.10 Loop-back

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

Remedial action:

F_CRC_Seed = 0: F-Host checks Loop-back via bit 7 of the Status Byte (Figure 19) and F-Output-Device detects Loop-back via timeout;

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

7.3.11 Network boundaries and router

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 incorporated safety PDU is delayed or prevented."

For CP 3/RTE networks with routers Figure 11 and the corresponding explanations apply. Such a system with subnetworks connected via routers is assumed for the following considerations. They demonstrate that a single error will not misdirect a safety PDU to the incorrect F-Device 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 14 contains a list of fault types and the constraints for router operation to achieve sufficient safety.

Table 14 – Safety network boundaries

Fault type	Consequences	Detection and Mastering
Router holds the incorrect 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 shown 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 parameter change at runtime

7.4.1 Standard startup procedure

The startup of the F-Devices/Modules is independent from 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 communication is established. 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 be either rejected or result in a safe state.

See [50], IEC 61158-5-10, and IEC 61158-6-10 for 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" = "iPar_EN") within the Control Byte of its next safety PDU. The F-Device/F-Module 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" ="iPar_OK") within the Status Byte of its next safety PDU (Figure 40).

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 40 is exemplifying a possible application.

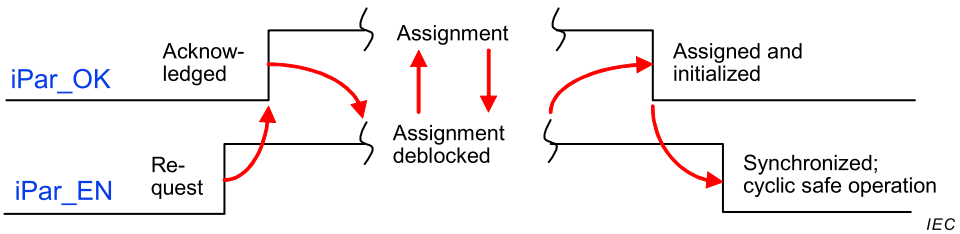


Figure 40 – iParameter assignment deblocking by the F-Host

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 [40] and [43]). 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 "Configure in Run" or "maintenance of fault tolerant systems". The engineering tool calculates and sets

	the value (with reserves for upcoming "CiR" sessions) during commissioning (7.2.6.2)
• F_Prm_Flag1 + 2	Parameter octets containing several parameters for the profile management
– F_Check_SeqNr	V2-mode: the MNR is always included in the CRC2 calculation
– F_Check_iPar	Manufacturer specific use within homogeneous systems
– F_SIL	Check: configured SIL = employed SIL?
– F_CRC_Length	CRC2 signature length
– F_CRC_Seed	Use of different rules for CRC seed value and MNR for the CRC2 signature calculation (see Figure 47)
– F_Passivation	F-Device/Module or Channel-granular Passivation [66]
– F_Block_ID	Parameter block type identification
– F_Par_Version	Version No. of F-Parameters/FSCP 3/1 operational mode
• F_iPar_CRC	Value of the iParameter CRC signature calculation, at least manually transferred from a CPD tool to the engineering tool
• F_Par_CRC	CRC signature calculation across the F-Parameters to secure the transfer from the F-Host to the F-Device

8.1.2 F_Source/Destination_Address (Codename)

The Codenames of the safety communication relationships 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 where RT CLASS UDP is not permitted or not supported (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 checked by the safety layer. The F_S/D_Address parameters are logic address designations that can be assigned *freely* but *unambiguously*. Typically, they are depicted from the F-Host (as source) and F-Device (as destination) during the configuration (7.3.7). The addresses *0* and *0xFFFF* shall be *excluded*.

The parameter consists of two parts: "F_Source_Add" and "F_Dest_Add", each of data type Unsigned16. Table 15 specifies the octet order of the Codename (F_Source/Destination_-Address).

Table 15 – Codename octet order

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

8.1.3 F_WD_Time (F-Watchdog time)

Locally, each F-Device 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 MNR.

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

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

A manufacturer of an F-Device assigns the maximum device acknowledgment time (DAT) to the default value of the parameter F_WD_Time in the GSD file. An engineering tool will then be able to propose the necessary F_WD_Time for this 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 F-Parameter can be used optionally to extend the regular F-WD_Time by one extra time F_WD_Time_2 via Bit 3 of the Control Byte as demonstrated in Figure 41 (MNR "n5"). This extra time is required for the configuration update of F-Devices/Modules.

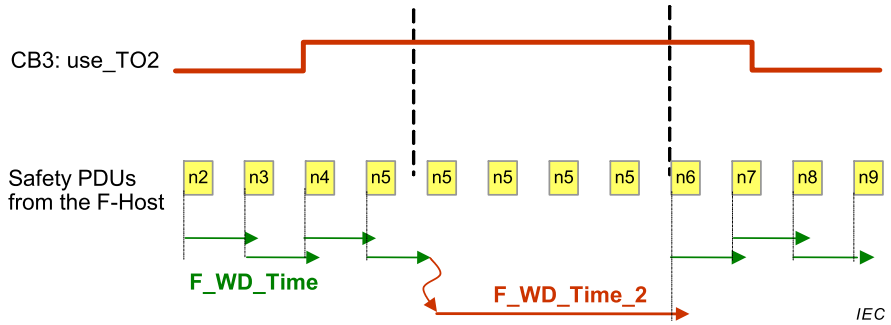


Figure 41 – Effect of F_WD_Time_2

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

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 42:

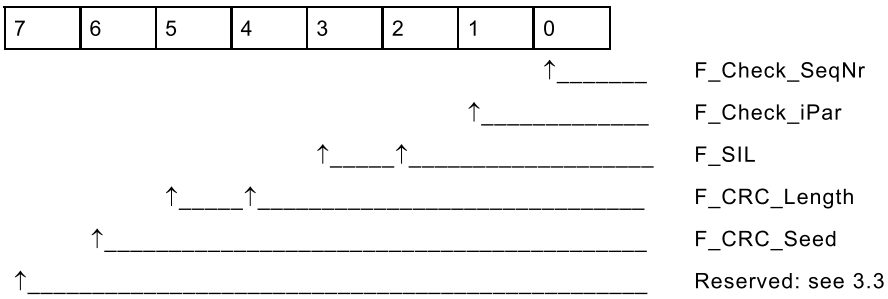


Figure 42 – F_Prm_Flag1

8.1.5.2 F_Check_SeqNr (MNR in CRC2)

This parameter defines whether or not the MNR shall be included in the CRC2 signature (see Figure 43). 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 43 – 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 1 of the parameter octet "F_Prm_Flag1" (see Figure 44).

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

Figure 44 – F_Check_iPar

8.1.5.4 F_SIL (SIL stage)

FSCP 3/1 permits parallel operation of standard communication and safety communication. The different safety functions using safety communication may require different safety integrity levels (SIL 1 to 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 to SIL 3, NoSIL (see Figure 45).

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 45 – F_SIL

8.1.5.5 F_CRC_Length (length of the CRC2 signature)

Depending on the parameter F_CRC_Seed, a CRC2 signature of 3 or 4 octets is required (see Figure 46). 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; notation in GSD shall be "3-Byte-CRC")
		0	1					=	This parameter assignment shall not be used for new developments
		1	0					=	4 octet CRC2 signature; notation in GSD shall be "4-Byte-CRC")
		1	1					=	Reserved

Figure 46 – F_CRC_Length

8.1.5.6 F_CRC_Seed (Seed value for CRC2)

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

With F_CRC_Seed =1, the F-Device/Module indicates the use of a “1” as seed value, the CRC-FP+, and the virtual MonitoringNumber based on Codename for inclusion in the CRC2 signature (see 7.1.6 and 7.1.8).

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

It is encoded as follows (see Figure 47): Bit 6 of the parameter octet "F_Prm_Flag1"

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

Figure 47 – F_CRC_Seed

8.1.6 F_Prm_Flag2 (Parameters for the safety layer management)

8.1.6.1 Structure of F_Prm_Flag2

Subclauses 8.1.6.3 to 8.1.6.4 are describing the details of the F_Prm_Flag2 parameter octet. It has the structure as shown in Figure 48.

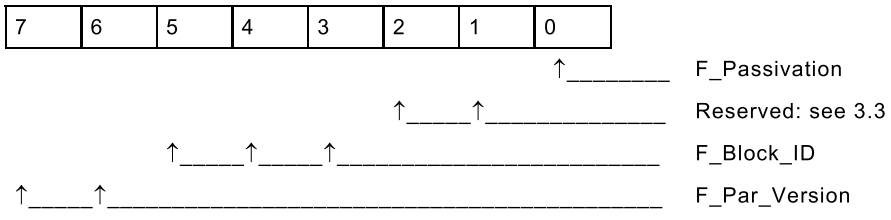


Figure 48 – F_Prm_Flag2

8.1.6.2 F_Passivation

Subclause 6.1 and Figure 16 describe the concept of Channel-granular Passivation (CGP) in contrast to the complete F-Device/Module passivation. An F-Host engineering tool will set this parameter to "0" if an F-Host does not support CGP (see Figure 49). An F-Device/Module supporting CGP shall check this parameter "F_Passivation".

7	6	5	4	3	2	1	0		
							0	=	F-Device/Module passivation upon "Device_Fault" (notation in GSD shall be "Device/Module")
							1	=	Channel-granular Passivation (CGP) upon individual signal channel faults using the qualifier model of [66] (notation in GSD shall be "Channel")

Figure 49 – F_Passivation

8.1.6.3 F_Block_ID (type identification of parameters)

In order to distinct parameters for future FSCP 3/1 modes, parameter type identification "F_Block_ID" is encoded in the following manner: Bits 3, 4 and 5 of the parameter octet "F_Prm_Flag2" (see Figure 50). 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_WD_Time_2, no F_iPar_CRC
		0	0	1				=	No F_WD_Time_2, F_iPar_CRC
		0	1	0				=	F_WD_Time_2, no F_iPar_CRC
		0	1	1				=	F_WD_Time_2, F_iPar_CRC
		1	0	0				=	Reserved
		1	0	1				=	Reserved
		1	1	0				=	Reserved
		1	1	1				=	Reserved

Figure 50 – F_Block_ID

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

The purpose of this version counter is to identify 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 51). Validity checking of F-Parameters shall be done by the safety layer.

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

Figure 51 – 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 recommended CRC seed value for this calculation is "1". The value in *hexadecimal* format shall be transferred at least manually to the engineering tool and assigned to the "F_iPar_CRC" entry field.

This parameter is transmitted to the F-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 Fail-safe Values (FV).

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

8.1.8 F_Par_CRC calculation (across F-Parameters)

The engineering tool is generating this CRC signature across the F-parameters. The seed value for this CRC signature is "0". See 8.3.3.2 for details on the order of the F-Parameters that shall be used for generating this CRC signature. The 16-bit CRC generator polynomial is used (*0x4EAB*).

It is encoded as: Unsigned16.

8.1.9 Structure of the F-Parameter record data object

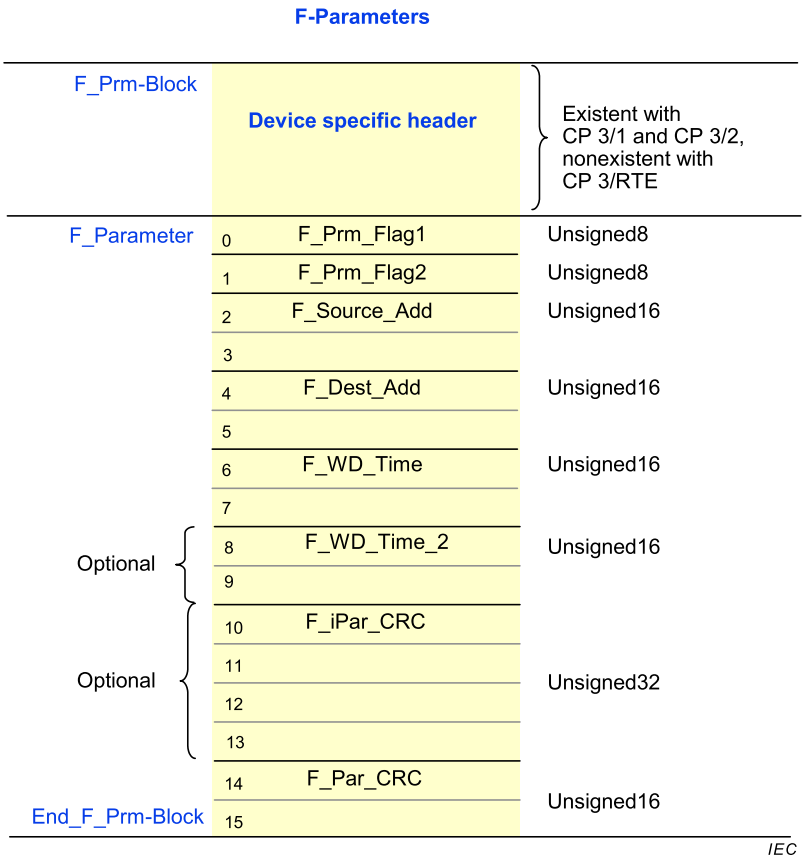


Figure 52 – F-Parameter

The Figure 52 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-Module, an F-Parameter-Block is inserted in the context message (Figure 13). The F-Module can be allocated to the F-Device via the subslot number.

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 53 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 53. No segmentation is required with CP 3/RTE.

The CRC signature ("iPar_CRC") shall be calculated across the iParameters (Figure 53) using any appropriate CRC polynomial and filled into the 4 octet iPar_CRC in hexadecimal format and displayed on the CPD-Tool. Whenever the calculation results in a "0", the value shall be set to "1". The recommended CRC seed value for this calculation is "1". Inclusion of the iPar_CRC value in the iParameters as shown in Figure 53 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 53 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 53 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 53 is optional.

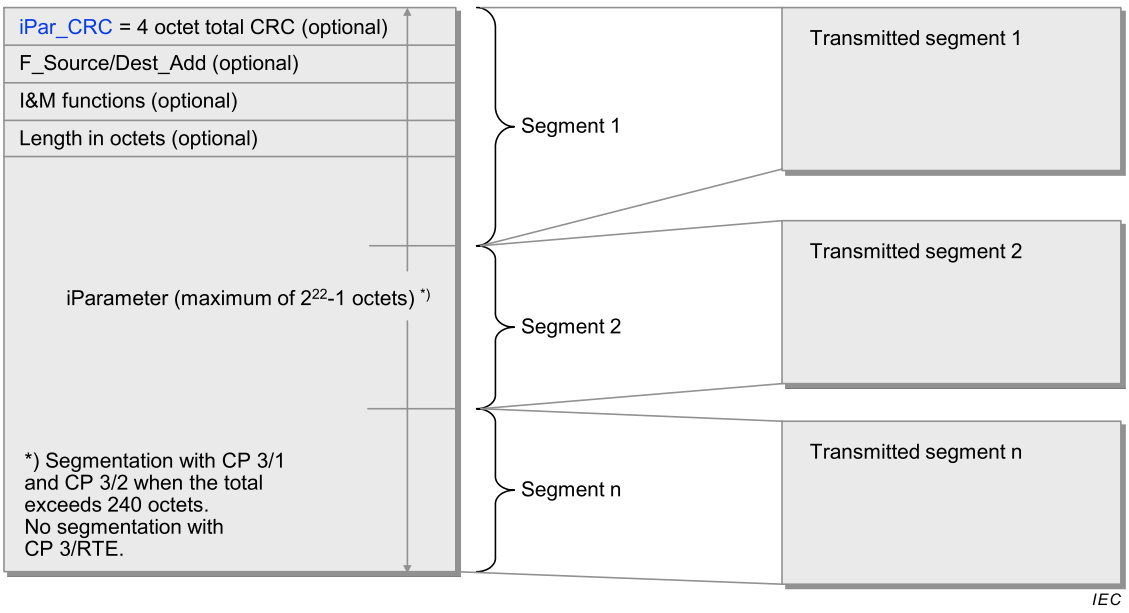


Figure 53 – iParameter block

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 [44] 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 IO 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-IO 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 [40] for IEC 61158 type 3 therefore defines keywords to structure and identify the F-Parameter block information of F-Modules shown in Figure 52. 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 16 are defined.

Table 16 – GSDL keywords for F-Parameters and F-IO structures

GSDL Keyword	Description
F_Ext_Module_Prm_Data_Len	The parameter associated with this keyword indicates the total length of the F_Prm-Block shown in Figure 52.
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 52. The position of an octet is indicated by an offset 0…3
F_Ext_Module_Prm_Data_Const (0)	Indicates the F_Prm_Block length including the F_iPar_CRC, e.g. 0x12
F_Ext_Module_Prm_Data_Const (1)	Identification of the F_Prm-Block = 5 (fix)
F_Ext_Module_Prm_Data_Const (2)	Slot of the F-Module
F_Ext_Module_Prm_Data_Const (3)	Reserved. Shall be set "0".
F_Ext_Module_Prm_Data_Ref (offset)	With the help of the parameter associated with this keyword a user selectable value at configuration time can be entered into one of the octets 0 to 13 of the F_Prm-Block shown in Figure 52. The position of an octet is indicated by an offset 4 to 16. The parameter is pointing to an ExtUserPrmData range definition within other parts of the GSD file

GSDL Keyword	Description
F_ParamDescCRC	The parameter associated with this keyword secures the safety-related parts of the F-Parameter descriptions within the GSD file See 8.3.3.3 for details on how to determine this CRC0 signature.
F_IO_StructureDescCRC	The parameter associated with this keyword secures the description of the F-IO data structure (cyclically transferred process values). See [40] 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) for IEC 61158 type 10 based on XML (see [43]).

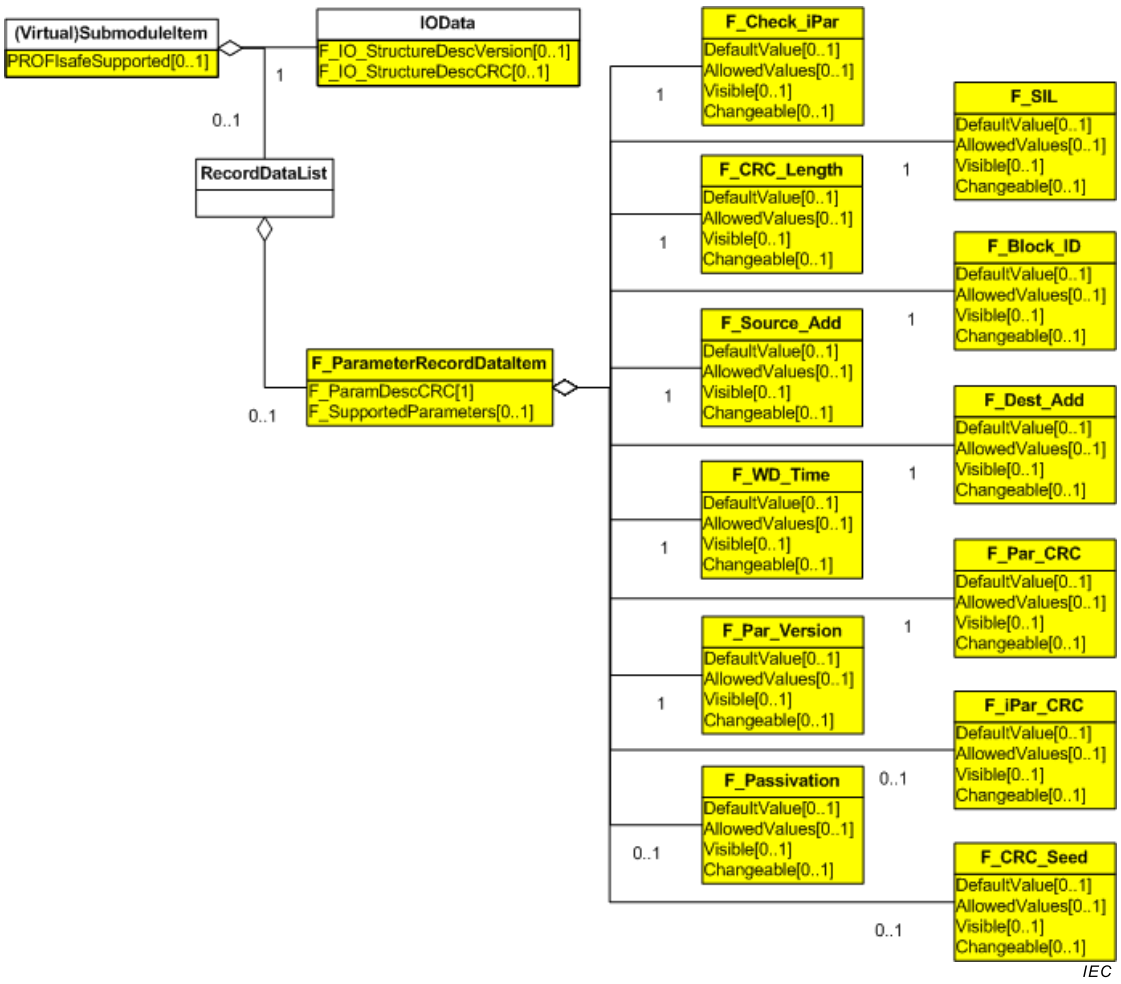


Figure 54 – F-Parameter extension within the GSDML specification

Figure 54 shows the extensions within the GSDML. The element "(Virtual)SubmoduleItem" provides the following attributes:

- "F_ParamDescCRC": This is the CRC signature (CRC0) of the F-Parameter description according to Figure 54.

- "F_SupportedParameters": Direct indication of the supported optional F-Parameters in the F-Parameter record (decoded information of "F_Block_ID"). For details see [43].

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

In GSDML, the F-Parameters F_CRC_Seed and F_Passivation are optional. They shall be present either both or none. Their presence indicates support of FSCP3/1 protocol according to this standard. To prevent engineering tools from stopping by the new F-Parameters, insert attribute RequiredSchemaVersion= ”V2.31” to the description of the F-Module.

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

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

Although there are multiple descriptions of the same F-Module in the GSD file, it is not necessary to have different IdentNumbers (see [69]).

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 IO 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 F_Par_CRC and iPar_CRC across safety parameters

Figure 23 is only showing the CRC1 signature across the F-Parameters that shall be involved in the CRC2 signature generating process. However, optionally there can be involved more CRC signatures as follows in 8.3.3.2.

In order to secure the F-Parameters, the engineering tool of the F-Host is generating the *F_Par_CRC* signature as described in 8.1.7. The CRC polynomial that shall be used is *0x4EAB*. The CRC signature is built across all F-Parameters in the octet order of Figure 52 excluding the optional F_iPar_CRC. Whenever bit 3 of the F-Parameter "F_Block_ID" is set to "1" the F_iPar_CRC signature shall be included at the beginning of the calculation as shown in Figure 55.

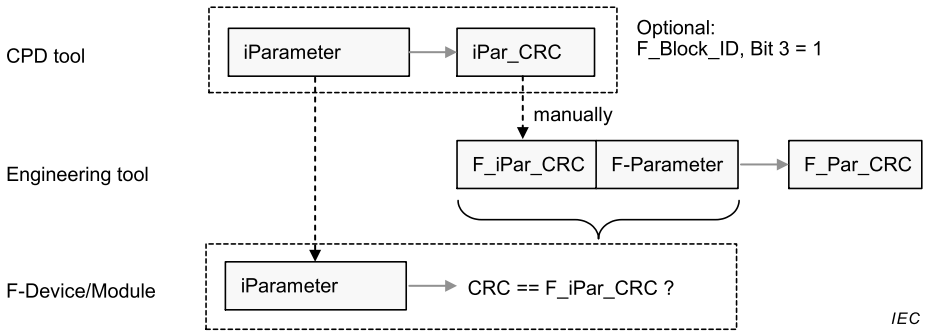


Figure 55 – F_Par_CRC signature including iPar_CRC

This procedure shall also be used for the calculation of CRC_FP (see 7.1.7) and CRC_FP+ (see 7.1.8).

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 (*0x4EAB*) that is used all over FSCP 3/1. Figure 56 describes the serialization and calculation algorithm.

Figure 56 – Algorithm to build CRC0

In case of a GSD file for an F-Slave (CP 3/1 or CP 3/2) the following GSDL annotation rules apply for the CRC0 signature calculation (see the example in Table 17 and Table 18):

- If an F-Parameter out of the set F_Check_SeqNr, F_Check_iPar, F_CRC_Length, F_CRC_Seed, F_Passivation, F_Block_ID is omitted in the GSD, a fixed value of zero is assumed and it shall not be included into the calculation of CRC0.
- The F_Ext_User_Prm_Data_Const keywords shall be ignored.

- In case the F-Parameters are described in a block structure form (see keywords Prm_Block_Structure_supp / ..._req), the F_Ext_User_Prm_Data_Ref keywords shall be ignored that point into the block header.
- The F_Ext_User_Prm_Data_Ref points to the ExtUserPrmData where the F-Parameter name, the data type, the default value and the permitted numerical values can be found.
- For F-Parameters with standardized names in addition to their numerical values, the Prm_Text_Ref points to the PrmText with these name definitions. The PrmTxt shall contain texts for all of the permitted values. Additional texts for unspecified values shall be ignored by engineering/configuration tools.

Table 17 – GSD example in GSDL notation

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

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

In case of a GSD file for an F-Device (CP 3/RTE) the following GSDML annotation rules apply for the CRC0 signature calculation (see the example in Figure 57 and Table 18):

- Some F-Parameters have standardized names with associated numerical values. In the GSDML notation only these names shall be used in the attributes “DefaultValue” and “AllowedValues”. The associated numerical values can be found in 8.1.

- If an F-Parameter out of the set F_Check_iPar, F_CRC_Length, F_Block_ID is set to invisible in the GSD, a fixed value of zero is assumed and it shall not be included into the calculation of CRC0.
- If an F-Parameter (or parts of its definition) is merely omitted from the GSD file, default values from the corresponding GSDML schema shall be used. Visible parameters shall always be included in the CRC0 calculation, regardless of whether their values are explicitly specified in a GSD file or supplemented from the schema.
- F_Check_SeqNr does not exist in the GSDML definition and thus shall not be included in the CRC0 calculation.
- F_Par_Version always shall be included in the CRC0 calculation although it has a fixed value of "1".
- The order of F-Parameters in element “F_ParameterRecordDataItem” corresponds with the order in the F-Parameter record, except for F_iPar_CRC.

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

Figure 57 – GSD example in GSDML notation

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

Table 18 – Serialized octet stream for the examples

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

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

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

Interpretation of the GSD file: Whenever the 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 IO data description (CRC7)

The F-IO 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 19 in the listed order (Version 2). The 32 bit CRC polynomial (*0xF4ACFB13*) shall be used to calculate the signature. Permitted data types for FSCP 3/1 are listed in 5.5.3. The previous version 1 of the IO data structure item set did not comprise the attribute VERSION and the data types Integer32 and Unsigned8+Unsigned8. Thus, no keyword 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 (*0x4EAB*), 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 19 – IO data structure items

Attribute name	Length	Description
VERSION	1 octet	Indicates a particular set of IO 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 × number of)
COUNT_PS_INPUT_CHANNELS_BOOL_MAX	2 octets	Input: Number of all bool channels (“used as bits”) in maximum mode (for example 1oo1 mode)
COUNT_PS_INPUT_BYTES_BOOL_MAX	2 octets	Input: Length of all bool DataItems (in octets) in maximum mode (for example 1oo1 mode)
COUNT_PS_INPUT_CHANNELS_INT	2 octets	Input: Number of all Integer16 DataItems
COUNT_PS_INPUT_CHANNELS_DINT	2 octets	Input: Number of all Integer32 DataItems

Attribute name	Length	Description
COUNT_PS_INPUT_CHANNELS_REAL	2 octets	Input: Number of all Float32 DataItems
OUT_ADDRESS_RANGE	2 octets	Length in octets of the whole IOData Output section (including F_MessageTrailer)
COUNT_PS_OUTPUT_BYTES_COMPOSITE	2 octets	Output: Length of all “Float32+Unsigned8” DataItems (5 × number of)
COUNT_PS_OUTPUT_BYTES_U8_U8	2 octets	Output: Length of all “Unsigned8+Unsigned8” DataItems (2 × number of)
COUNT_PS_OUTPUT_CHANNELS_BOOL	2 octets	Output: Number of all bool channels (“used as bits”)
COUNT_PS_OUTPUT_BYTES_BOOL	2 octets	Output: Length of all Bool DataItems (in octets)
COUNT_PS_OUTPUT_CHANNELS_INT	2 octets	Output: Number of all Integer16 DataItems
COUNT_PS_OUTPUT_CHANNELS_DINT	2 octets	Output: Number of all Integer32 DataItems
COUNT_PS_OUTPUT_CHANNELS_REAL	2 octets	Output: Number of all Float32 DataItems
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 contain example DataItem sections according to some F Channel driver types in 8.5.2 using the attributes described in Table 19. These example DataItem sections refer to F_CRC_Seed = 1.

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

NOTE F_Passivation =1 ("Channel") is only used in conjunction with [66], which contains additional examples

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 58. Table 19 contains a description of the variables.

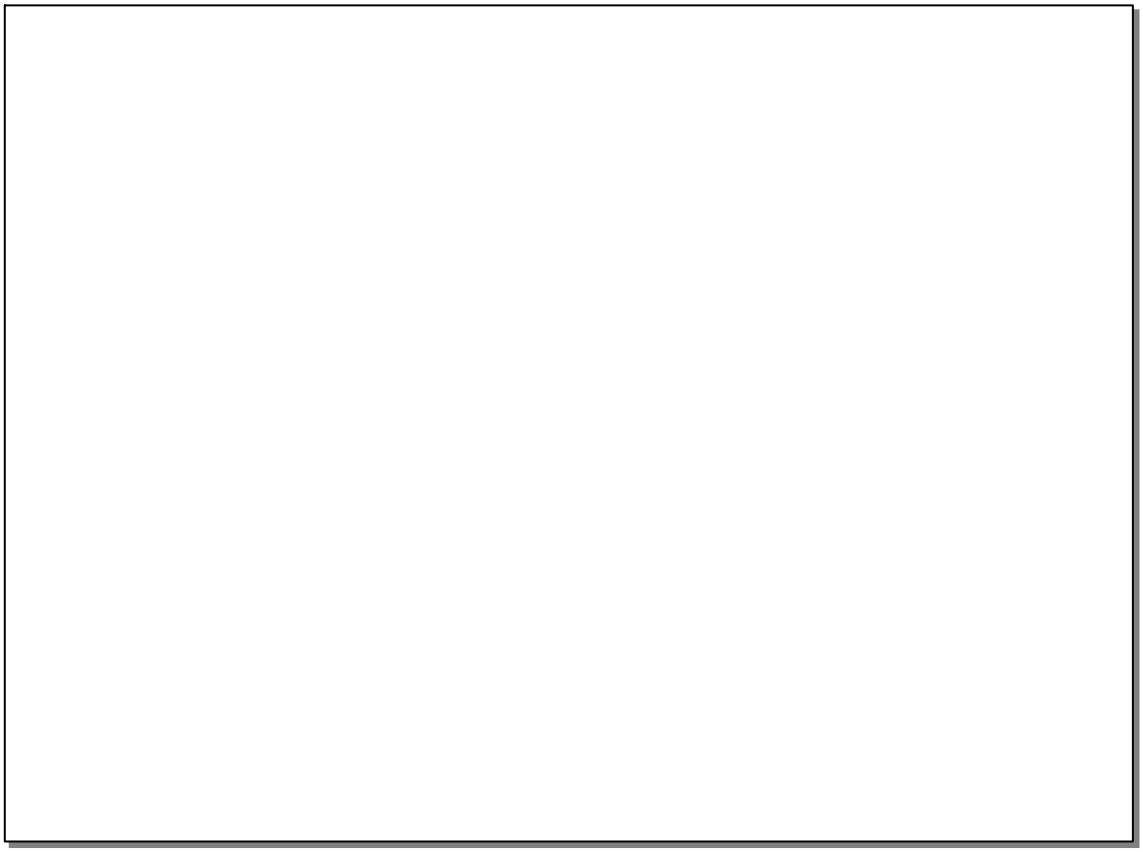


Figure 58 – DataItem section for F_IN_OUT_1

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 59.

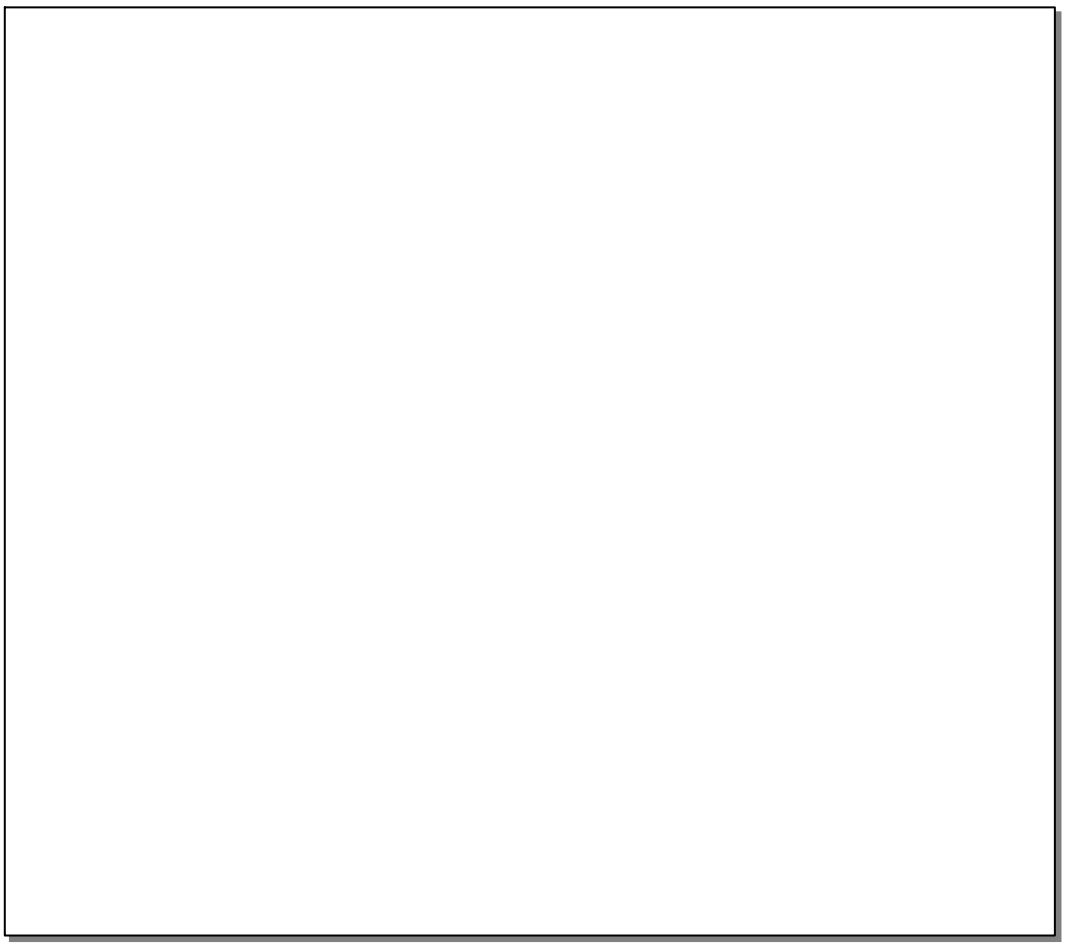


Figure 59 – DataItem section for F_IN_OUT_2

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 60.

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

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 60 – DataItem section for F_IN_OUT_5

8.4.2.5 F_IN_OUT_6

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

Output:
Setpoint (Float32 + Unsigned8)

The coding of the DataItem section for the F_IN_OUT_6 F_Channel_Driver example is shown in Figure 61. Table 19 contains a description of the variables.

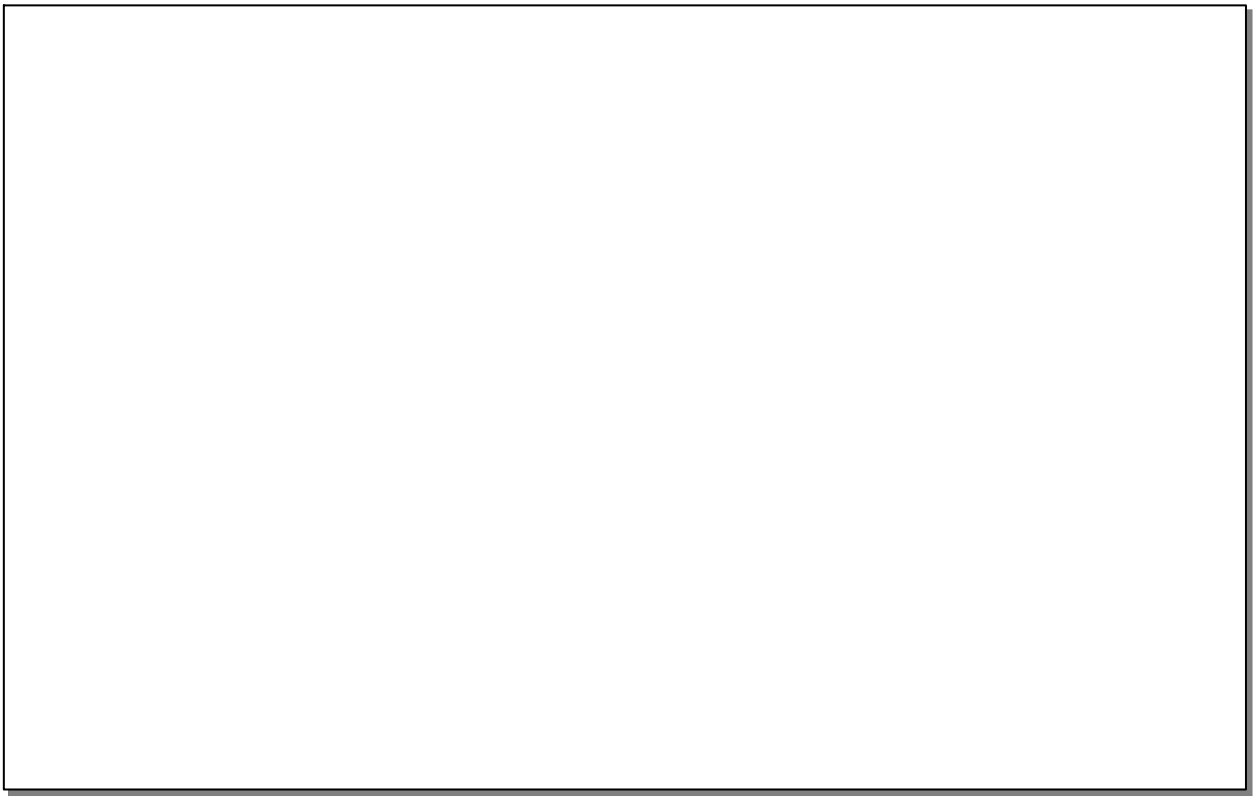


Figure 61 – DataItem section for F_IN_OUT_6

8.5 Data type information usage

8.5.1 F-Channel driver

The F-IO data cyclically transferred between an F-Device and an F-Host (Real-time Channel) need to be controlled by a user program.

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

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

Figure 62 illustrates such a programmer's view on "F-Channel driver" function blocks.

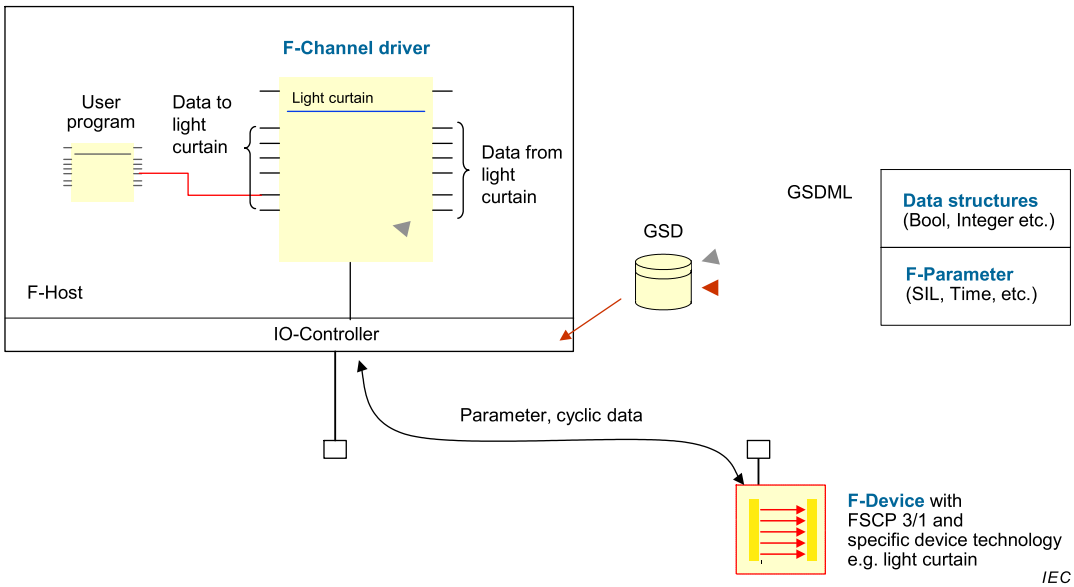


Figure 62 – F-Channel driver as "glue" between F-Device and user program

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, Integer32 variables if available. Then all floating-point variables if available.

Table 20 contains a list of sample F-Channel drivers. The drivers represent different F-Input and F-Output data structures according to the associated safety PDUs. The permitted data types for FSCP 3/1 are listed in 5.5.3. Thus, 32 Boolean values shall be mapped into data type Unsigned32 and 8 bit into the data type Unsigned8. See 8.4.2 for details.

Table 20 – 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 63 shows a layout example of an F channel host driver for a complex F-Device.

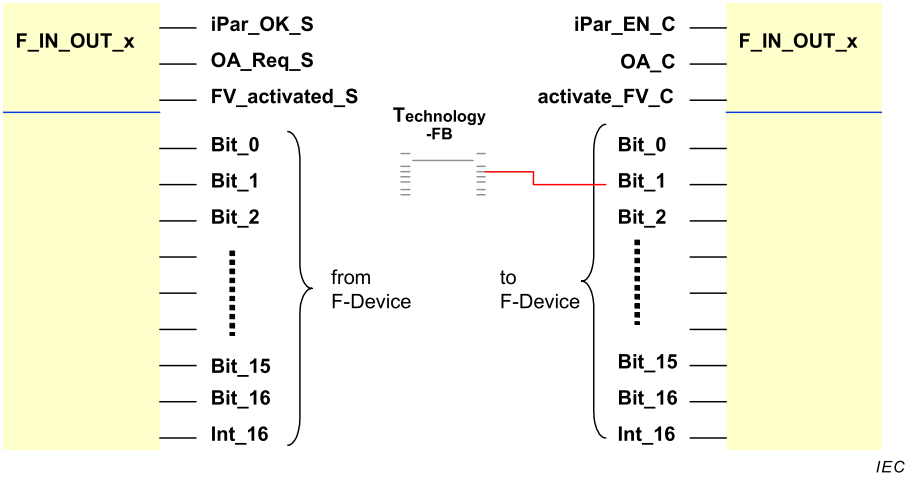


Figure 63 – Layout example of an F-Channel driver

The terms used in Figure 63 and the driver behaviors are specified below:

iPar_EN_C	iParametrization enabled
iPar_OK_S	iParametrization completed
OA_C	Operator Acknowledgment (for resumption after fault)
OA_Req_S	When fault (Timeout or CRC2) detected and removed
FV_activated_S	Fail-safe values activated by F-Device
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 63).

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

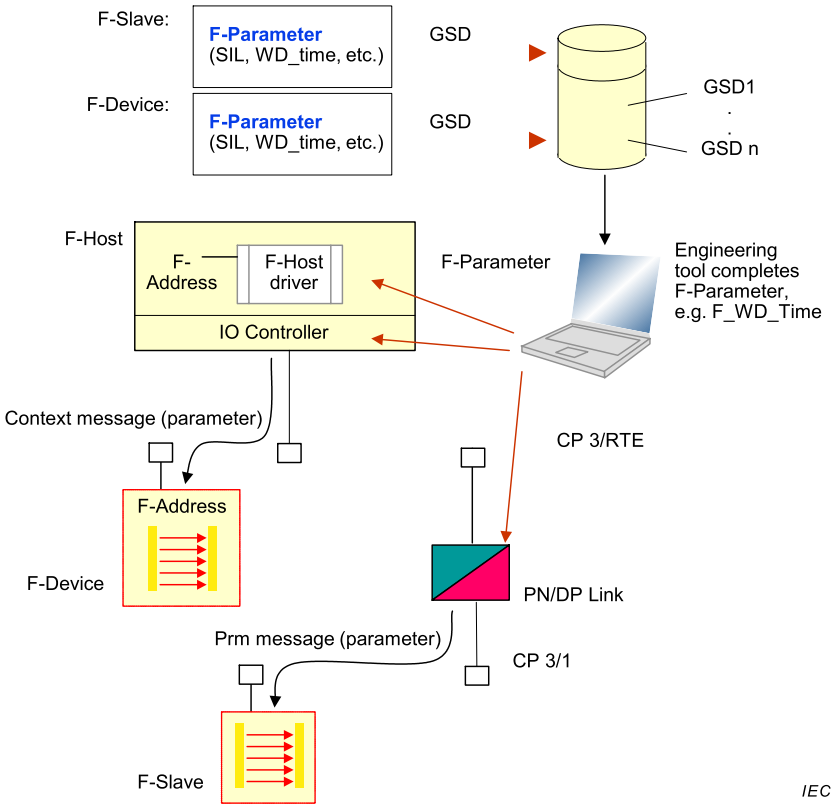


Figure 64 – F-Parameter assignment for simple F-Devices and F-Slaves

Simple F-Devices without iParameters can be supplied via the standard Context Message path. See IEC 61158-5-10, IEC 61158-6-10, and [50]. The total amount of F-Parameters hereby cannot exceed the upper limit of 234 octets (Figure 64).

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 65 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 (step 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

Table 35) across the fieldbus concurrently with the cyclic data communication. After parameterization and commissioning, the Proxy Function Block (Proxy FB) may be activated to upload the iParameters into the controller (step 2) where they are ready for download in case of device replacement for repair (step 3).

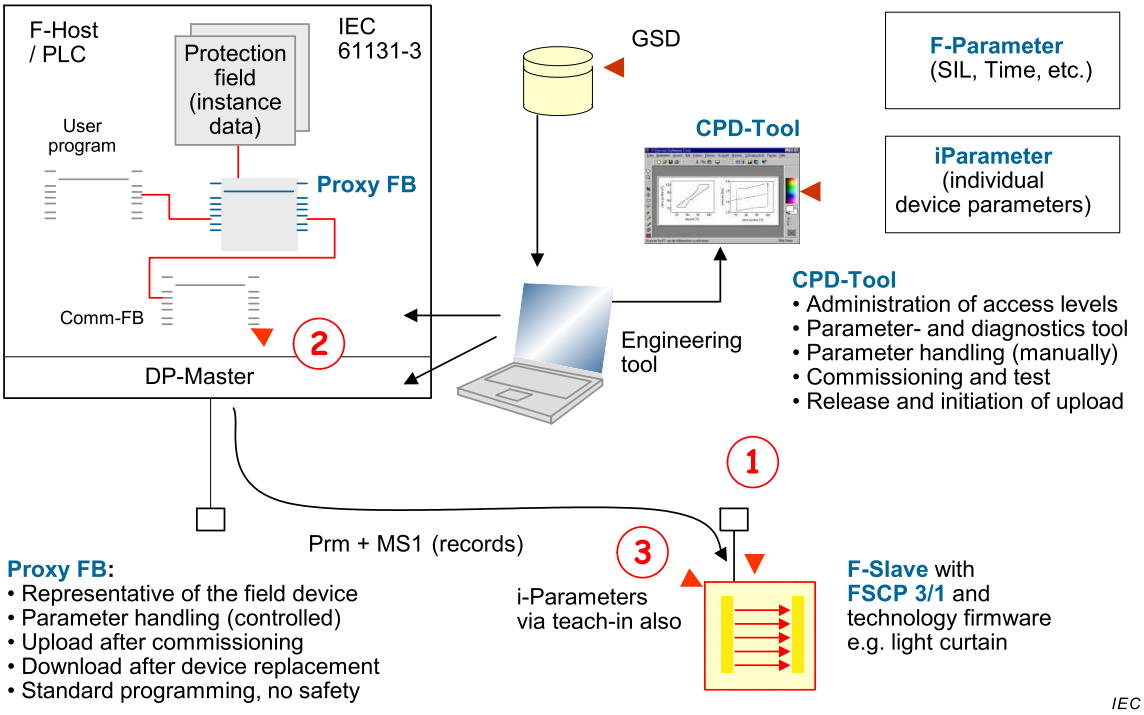


Figure 65 – F and iParameter assignment for complex F-Devices

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 65). The identification number of the actual iParameter data set shall be communicated cyclically within the F-IO data.

8.6.3 System integration requirements for iParameterization tools

Table 21 contains a list of requirements to be fulfilled by iParameterization procedures.

Table 21 – Requirements for iParameterization

No.	System requirement
R1	CPD-Tool to be designed for compatible personal computers or laptops and operating systems WINDOWS XP 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 favorite 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 octet order (the initial value shall not be zero). A manufacturer can use his own method to secure the iParameters as long as the criteria are fulfilled (iPar-Server, CPD-Tool)

Figure 66 illustrates the system aspects of the CPD-Tool-Integration.

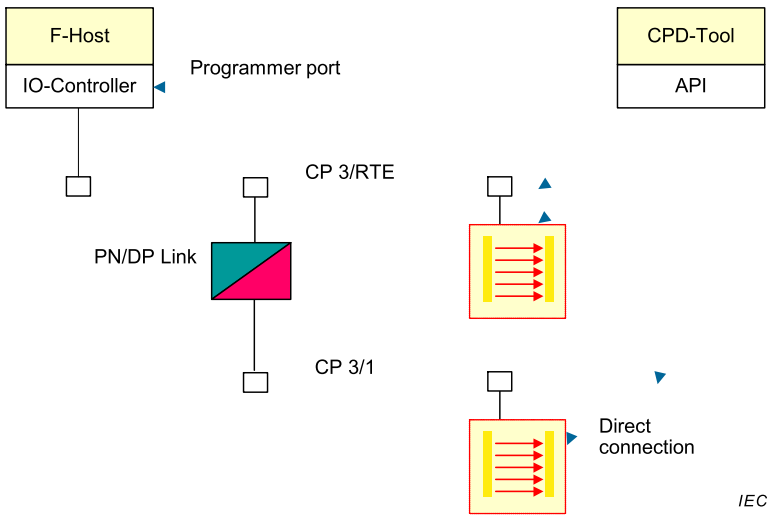


Figure 66 – System integration of CPD-Tools

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.

8.6.4 iPar-Server

8.6.4.1 General description and constraints

The iPar-Server concept is a specialized form of the more general Proxy-FB concept as pointed out in 8.3.1. It is the responsibility of F-Host manufacturers to provide this feature as stated in Table 35, be it realized within the non-safety part of an F-Host as the parameterization master or within a controlled subsystem such as a non-safety PLC or an industrial computer on the same network. [65] supersedes the non-safety-related part of the following specification.

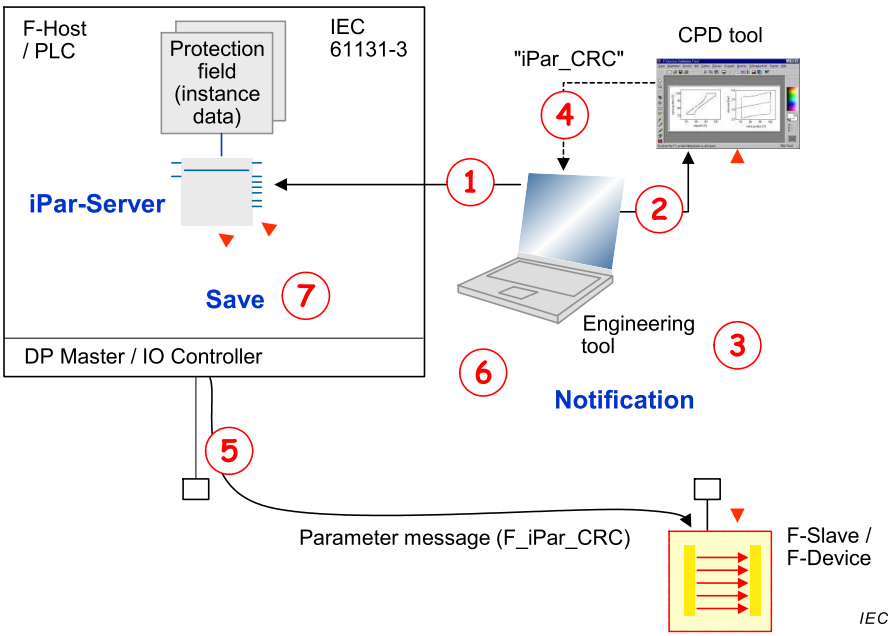


Figure 67 – iPar-Server mechanism (commissioning)

Figure 67 demonstrates the principle steps of the iPar-Server mechanism via an example. Together with the network configuration and F-Parameterization 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 uses the diagnosis means of CPF 3 (8.6.4.2 and [44]).

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

Figure 68 shows 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 uses the diagnosis means of CPF 3 (8.6.4.2 and [44]).

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

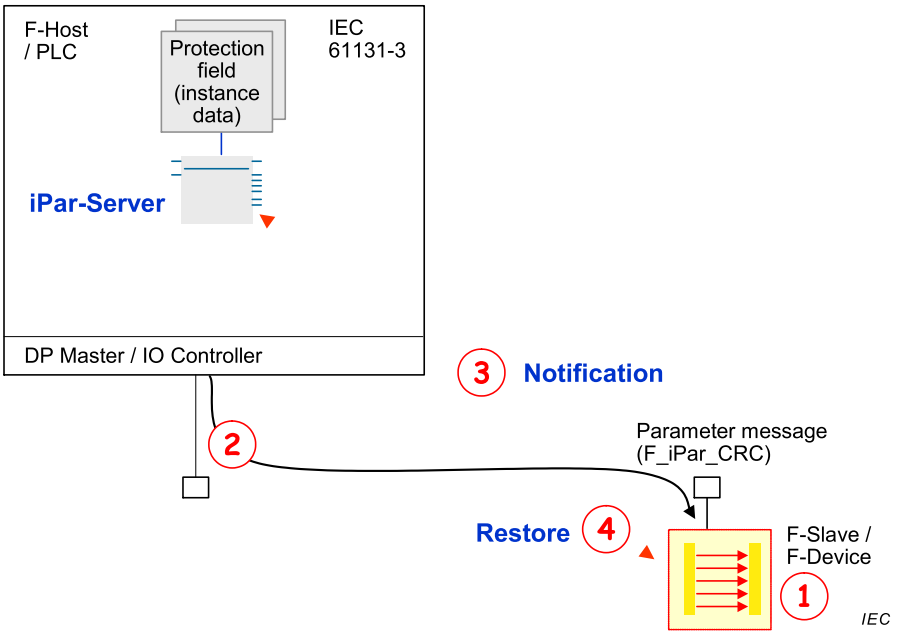


Figure 68 – iPar-Server mechanism (for example F-Device replacement)

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 53.
- 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 68).
- 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" shall only 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 visualization tool for maintenance interaction. Out of several different types on CP 3/1 and CP 3/2,

specified in IEC 61158-5-3, the preferred diagnosis information coding relates to the "Status Model" [45]. 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 IO does not have to know its deployment.

Figure 69 shows the iPar-Server request coding for CP 3/1 and CP 3/2.

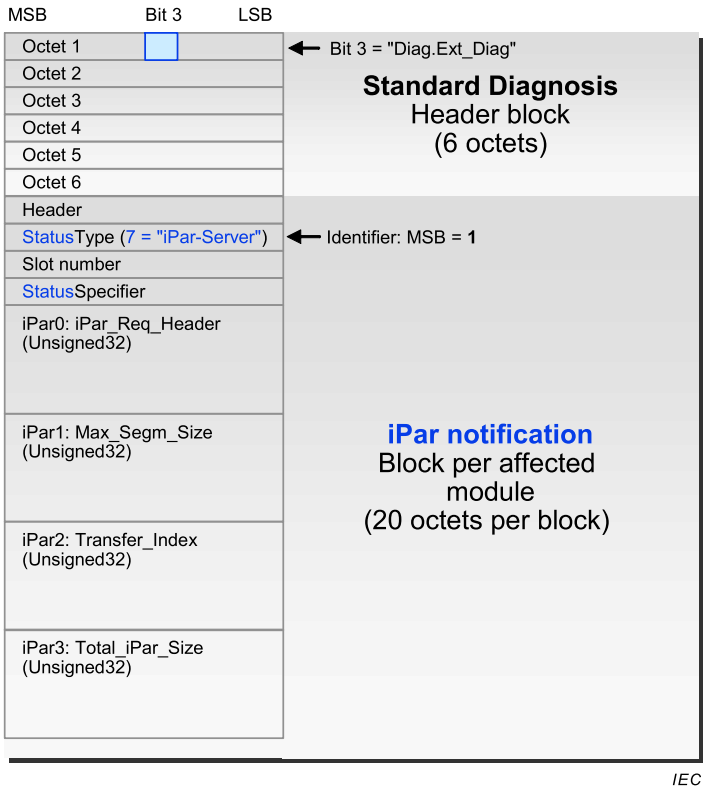


Figure 69 – iPar-Server request coding ("status model")

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 69. 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 22.

An F-Module within a remote IO always uses the coding of Figure 69 or an appropriate subset, whenever it can be deployed in a CP 3/1 or CP 3/RTE remote IO device. A remote IO shall only cast one notification at a time and thus save or restore iParameters F-Module by F-Module. Design hints for cases of diagnosis congestion (e.g. "Diag.Ext_Diag_Overflow") can be found in [45].

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

It is the task of the headstation of a remote IO device to transform the iPar-Server request coding into the appropriate format of the actual communication profile (Figure 69 or Figure 71).

Table 22 – Specifier for the iPar-Server Request

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

Reserved: See 3.3.

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

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

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

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.

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

The parameter "SR_Version" shall be set to 0x01. The parameter "N_Count" shall start with "1" and be changed with each notification (only in case of CP 3/1 and CP 3/2) until the value 15 and continued with "1" all over again. The parameter "SR_Type" shall be coded as shown in Figure 70.

7	6	5	4	3	2	1	0	
*	*	*	*	*	*	0	0	Reserved
*	*	*	*	*	*	0	1	Save (Upload)
*	*	*	*	*	*	1	0	Reserved
*	*	*	*	*	*	1	1	Restore (Download)
*	*	*	*	↑	↑			Reserved: See 3.3
*	*	*	0	*	*	*	*	Transfer per one read/write record
*	*	*	1	*	*	*	*	Segmented transfer per push/pull mechanism
↑	↑	↑						Reserved: See 3.3

Figure 70 – Coding of SR_Type

A possible realization of the counterpart within for example the non-safety part of an F-Host is specified in [44] and called RDIAG communication function block.

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 71 shows the iPar-Server request coding for CP 3/RTE.

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".

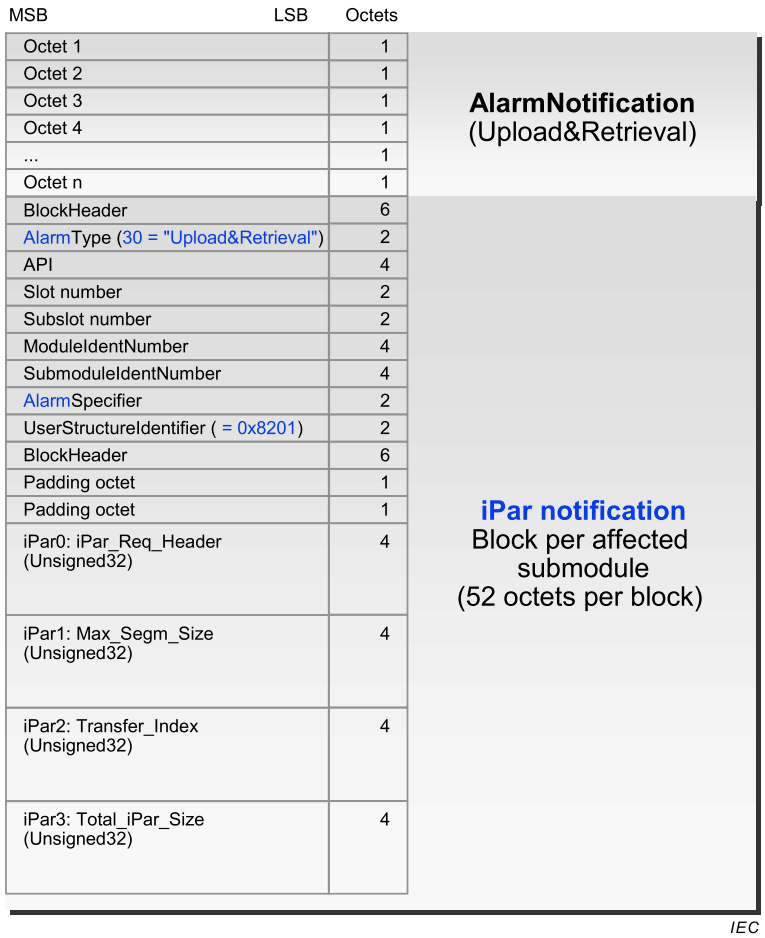


Figure 71 – iPar-Server request coding ("alarm model")

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 23 and Table 24). A possible realization of these two functions based on IEC 61131-3 programming languages is specified in [44] 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 23 – Structure of the Read_RES_PDU ("read record")

Structure of the Read_RES_PDU	Size	Coding	Notes	
Function_Num	1 octet	0x5E	Indicates "read", fix	Header
Slot_Number	1 octet	0 to 255	Location of module	
Index	1 octet	0 to 254	"Transfer_Index"	
Length of net data	1 octet	0 to 240	Length of iPar segment	
iParameter (segment)	n octets	-	n = 240 maximum per record	Data
NOTE Corresponding structures for CP 3/RTE can be found in [44].				

Table 24 – Structure of the Write_REQ_PDU ("write record")

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

For amounts of iParameters exceeding the record or buffer limit of a particular F-Slave/ F-Module an extended version of the "read record" and "write record" acyclic services can be used, specified in IEC 61158-5-3 as the so-called "Pull" and "Push" services (Table 25 and Table 26).

Table 25 – Structure of the Pull_RES_PDU ("Pull")

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

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

Table 26 – Structure of the Push_REQ_PDU ("Push")

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

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

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

An example for a standard parameter server is the "Upload&Retrieval" mechanism of CP 3/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 IO always uses an appropriate coding, whenever it can be deployed in a CP 3/1 or CP 3/RTE remote IO device. It is the task of the headstation of a remote IO device to transform the iParameter transfer coding into the appropriate format of the actual communication profile and back.

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

8.6.4.4 Protocol

Figure 72 shows the iPar-Server state diagram and Table 27 describes the iPar-Server states, transitions, and internal items. See 7.2.2 on general information about UML2 notation.

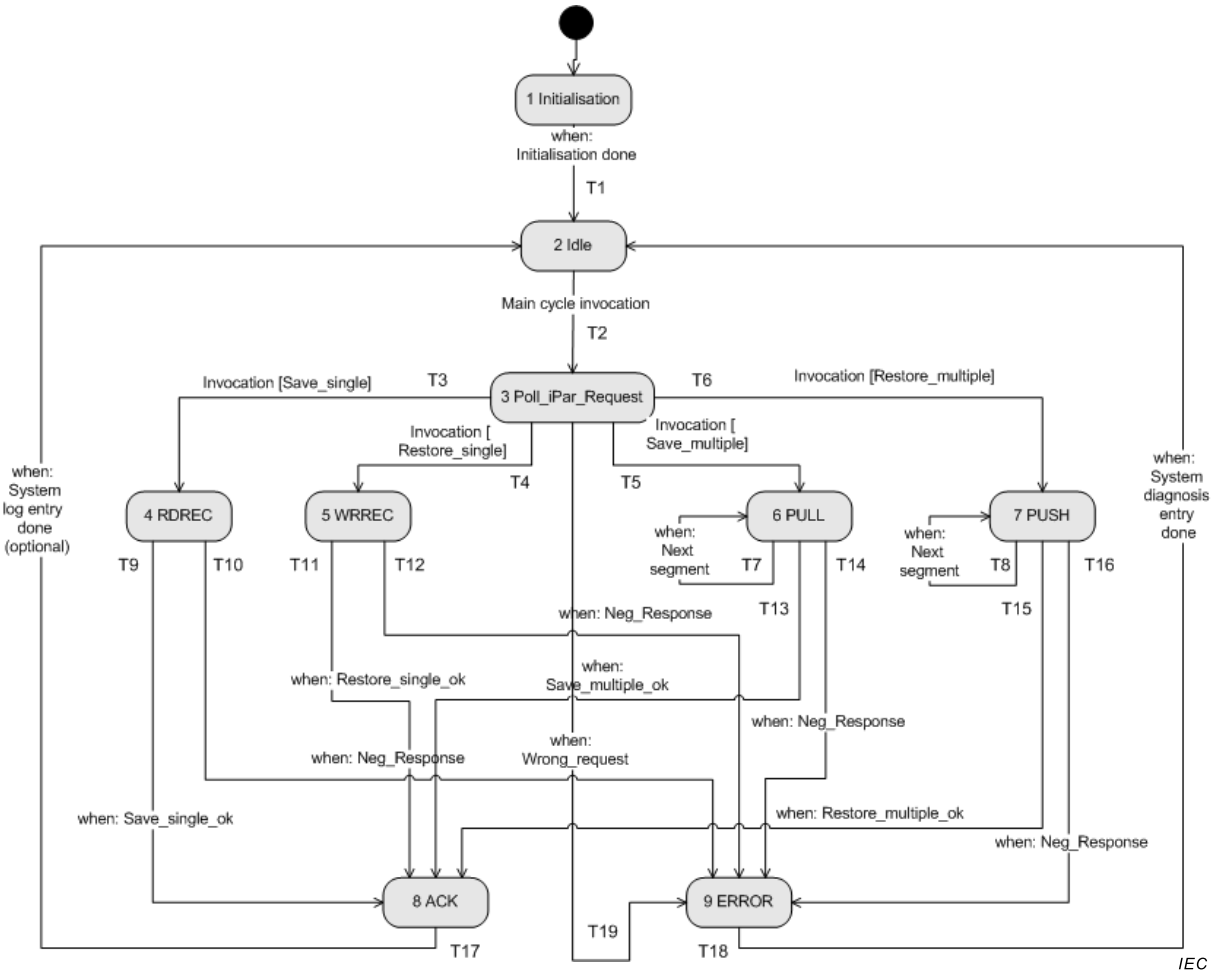


Figure 72 – iPar-Server state diagram

The terms used in Figure 72 are specified below:

Save_single	iPar-Server request to save (upload) an iParameter block per one single record (RDREC)

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

Table 27 – 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 [44] 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 [44] 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)

TRAN-SITION	SOURCE STATE	TARGET STATE	ACTION
T10	4	9	Start system diagnosis entry
T11	5	8	Start entry of a successful WRREC execution in the system log file (optional)
T12	5	9	Start system diagnosis entry
T13	6	8	Start entry of a successful POLL execution in the system log file (optional)
T14	6	9	Start system diagnosis entry
T15	7	8	Start entry of a successful PUSH execution in the system log file (optional)
T16	7	9	Start system diagnosis entry
T17	8	2	Go to sleep (idle)
T18	9	2	Go to sleep (idle)
T19	3	9	Start system diagnosis entry

8.6.4.5 iPar-Server management

The iPar-Server management measures to ensure authenticity, validity and data integrity of the iParameters are listed in Table 28. 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 28 – 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 parameterization
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

Item / phase	Clauses	Description
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
iPar-Server	-	An F-Module, F-Slave, or F-Device shall only 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 [40] and [43] 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 Acknowledgment requested" within the Control Byte (=1). This bit can be used to inform the user about three actions to start:

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

With compact 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 provide 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 [41].

9.3 Safety function response time

9.3.1 Model

A safety function may consist of several sensors such as a light curtain and E-Stop buttons, a safety control program within an F-Host, and an actuator such as a motor (Figure 73).

Each sensor has its own signal path and thus a particular typical response time (see blue dotted line in Figure 73).

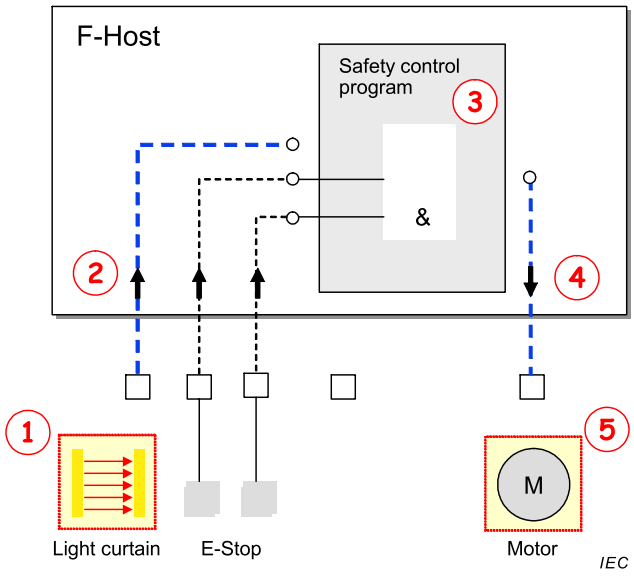


Figure 73 – Example safety function with a critical response time path

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 74. An example is used to show the principle, which can be adopted for the internal response time model of a complex device.

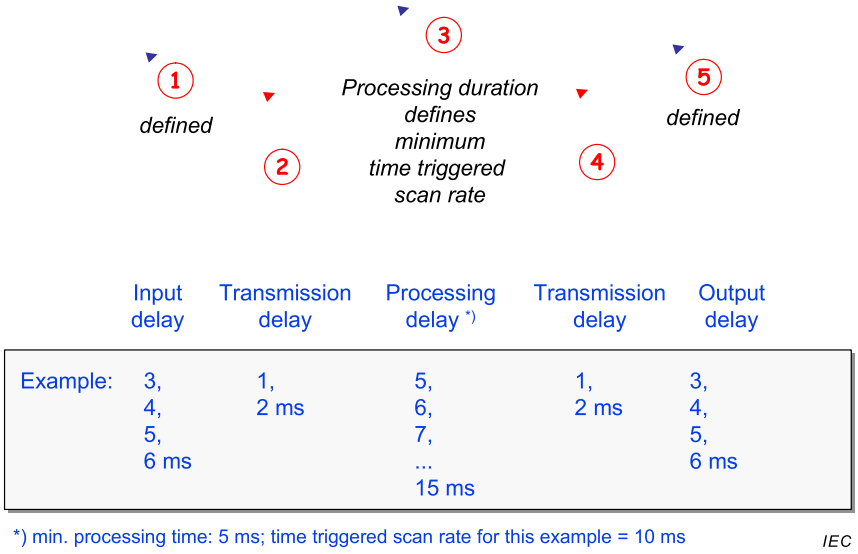


Figure 74 – Simplified typical response time model

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).

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

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

Figure 75 shows the frequency distributions of typical response times of the model for a time trigger of 10 ms, 20 ms and 30 ms.

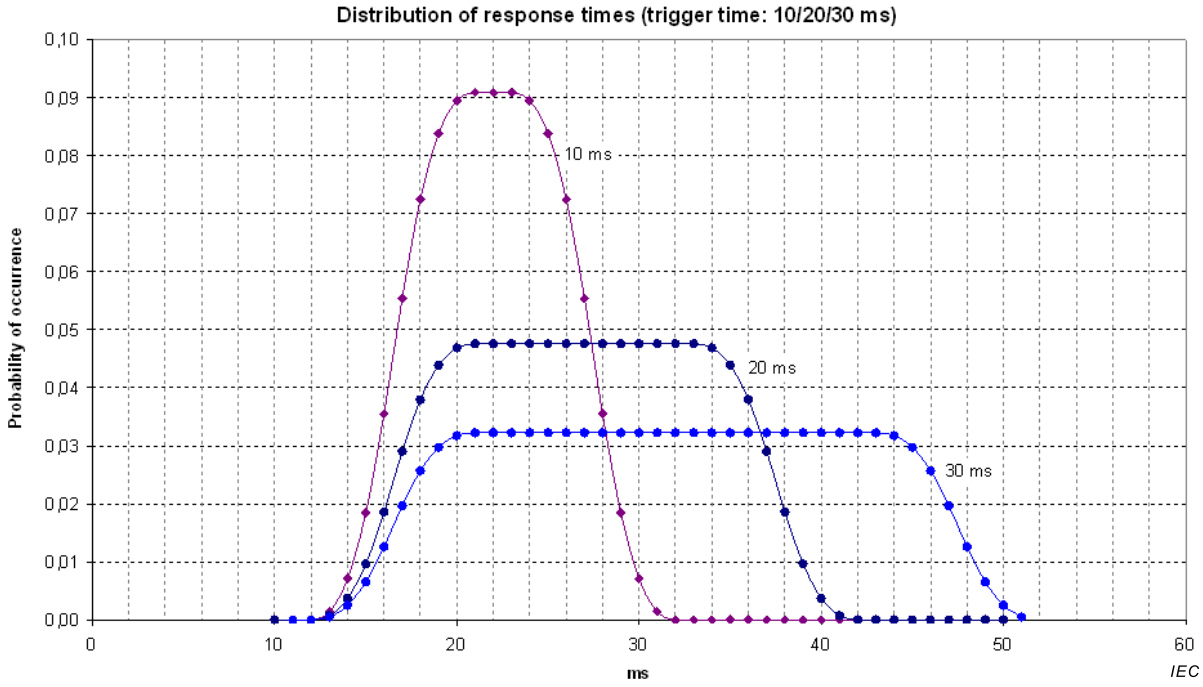


Figure 75 – Frequency distributions of typical response times of the model

9.3.2 Calculation and optimization

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

Figure 76 illustrates the context of the worst case delay times and the watchdog times.

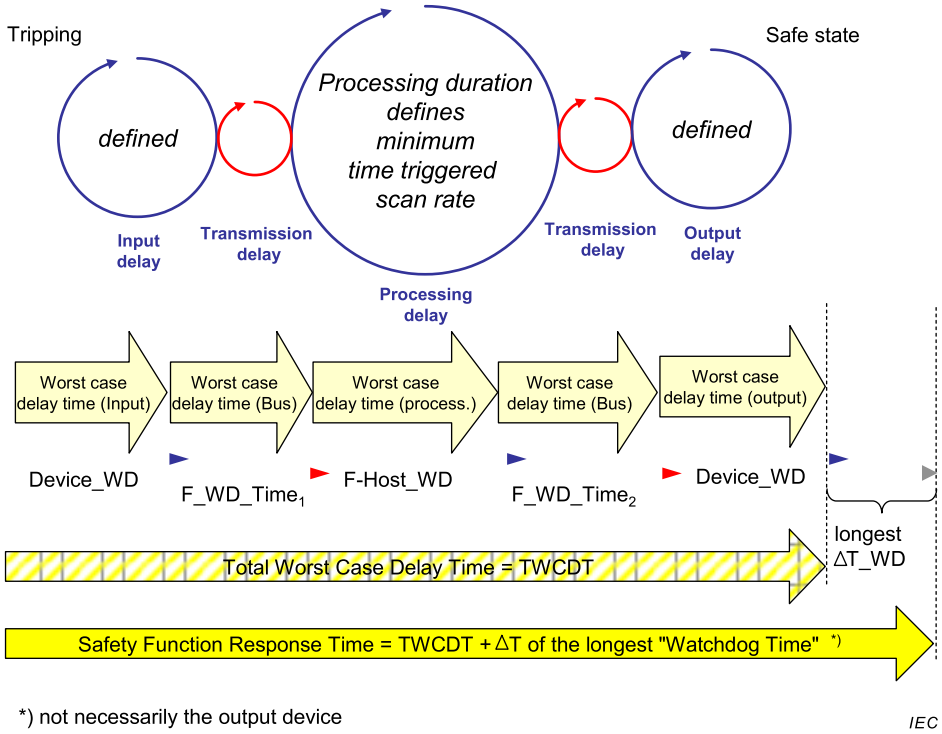


Figure 76 – Context of delay times and watchdog times

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 MNR and ending with the reaction on the expiration of the F_WD_Time. Following the particular expressions for the entities i:

- Input: $OFDT_{Input}$
- TD_1: $F\_WD\_Time_1 + WCDT_{TD1} + Tcy_{F\text{-}Host}$
- F-Host: $OFDT_{F\text{-}Host}$
- TD_2: $F\_WD\_Time_2 + WCDT_{TD2} + DAT_{Output}$
- Output: $OFDT_{Output}$

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

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

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

9.3.3 Adjustment of watchdog times for FSCP 3/1

The F-Parameter F_WD_Time determines the watchdog time for a FSCP 3/1 1:1 communication relationship (8.1.3). Figure 77 illustrates that the minimum watchdog time is composed of four timing sections (DAT – Bus – HAT – Bus).

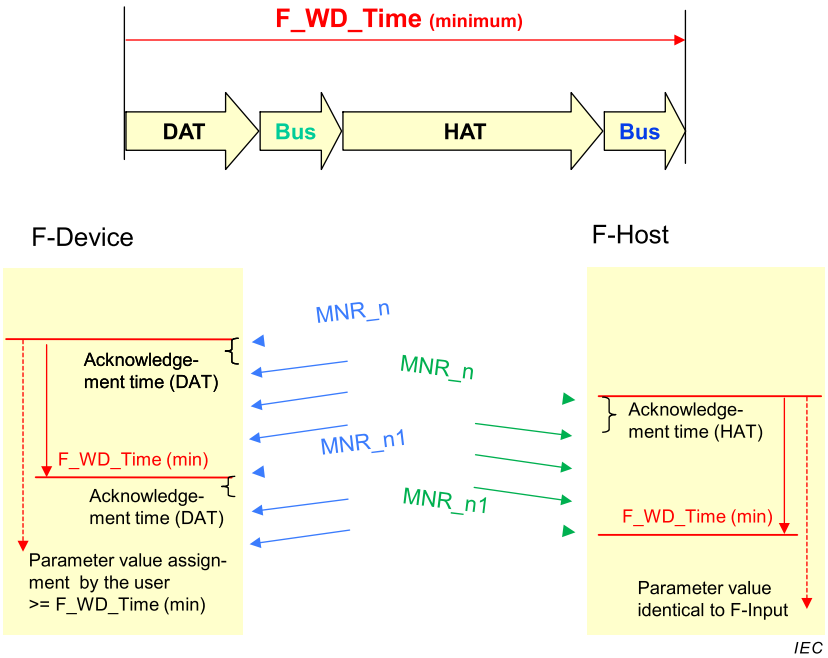


Figure 77 – Timing sections forming the FSCP 3/1 F_WD_Time

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

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

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 next MNR. The elapsed time for this operation is called "HAT = Host Acknowledgment 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 74 (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 – non-safety or safety – for its number of retries and if necessary to take appropriate measures such as correct application of the installation guidelines or usage of conformance tested devices (Clause 10). This will not only help to increase the availability but also provide short reaction times without nuisance trips (Figure 78).

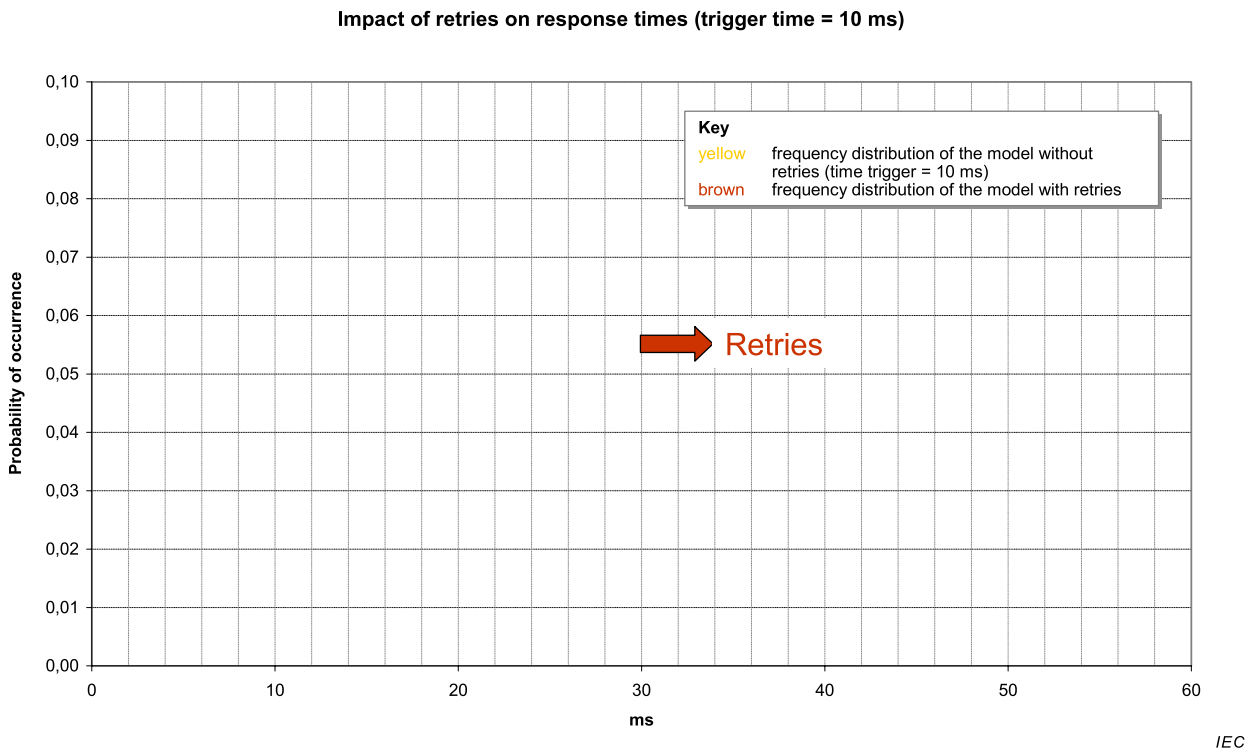


Figure 78 – Frequency distribution of response times with message retries

Figure 79 illustrates the retry mechanisms with CP 3/1, whereas Figure 80 illustrates 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.

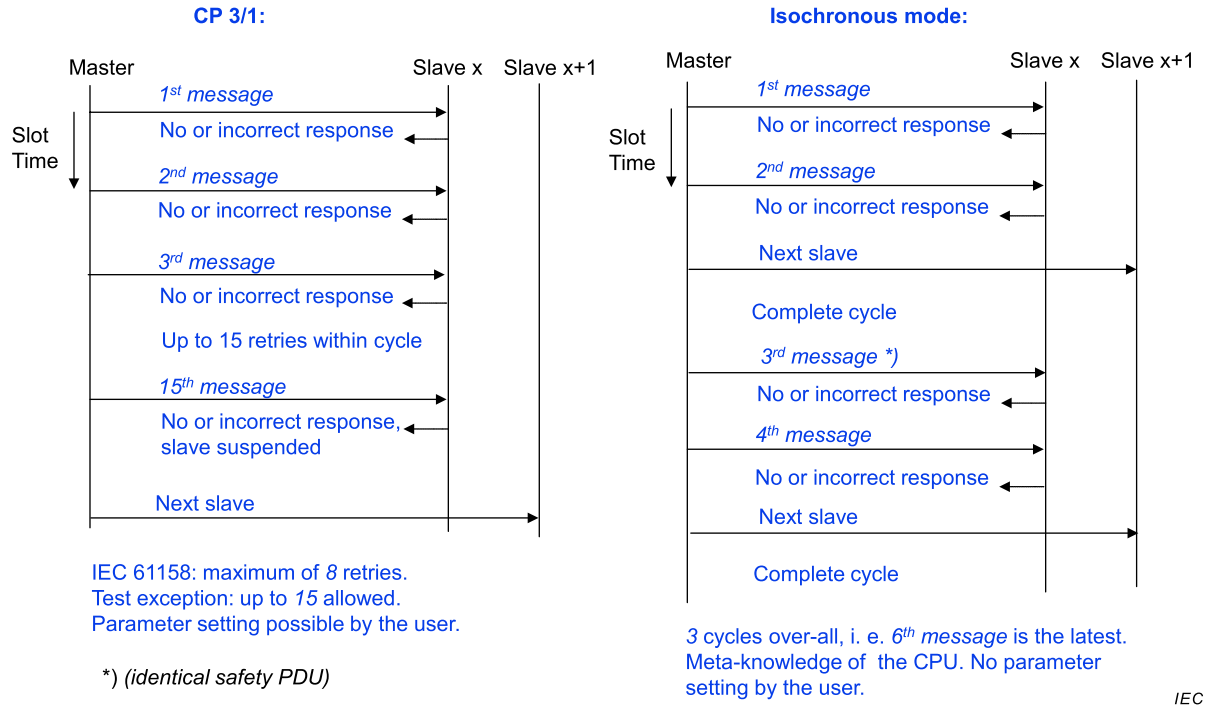


Figure 79 – Retries with CP 3/1

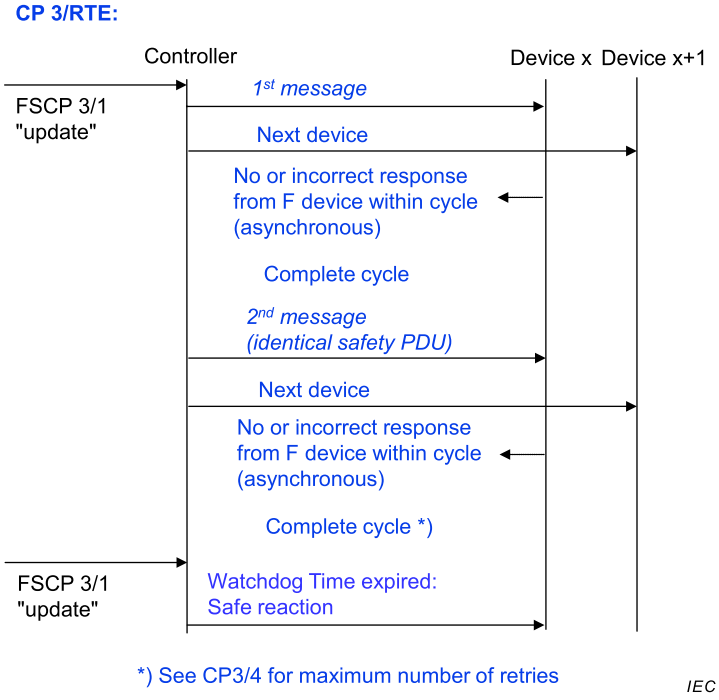


Figure 80 – Retries with CP 3/RTE

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 MNR and different process values can be received due to permuted messages in the black channel.

9.5 Constraints for the calculation of system characteristics

9.5.1 Probabilistic considerations

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

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

Figure 81 shows the diagrams of residual error probabilities for the 24-bit CRC generator polynomial. The calculated diagrams are for data lengths including the CRC signature.

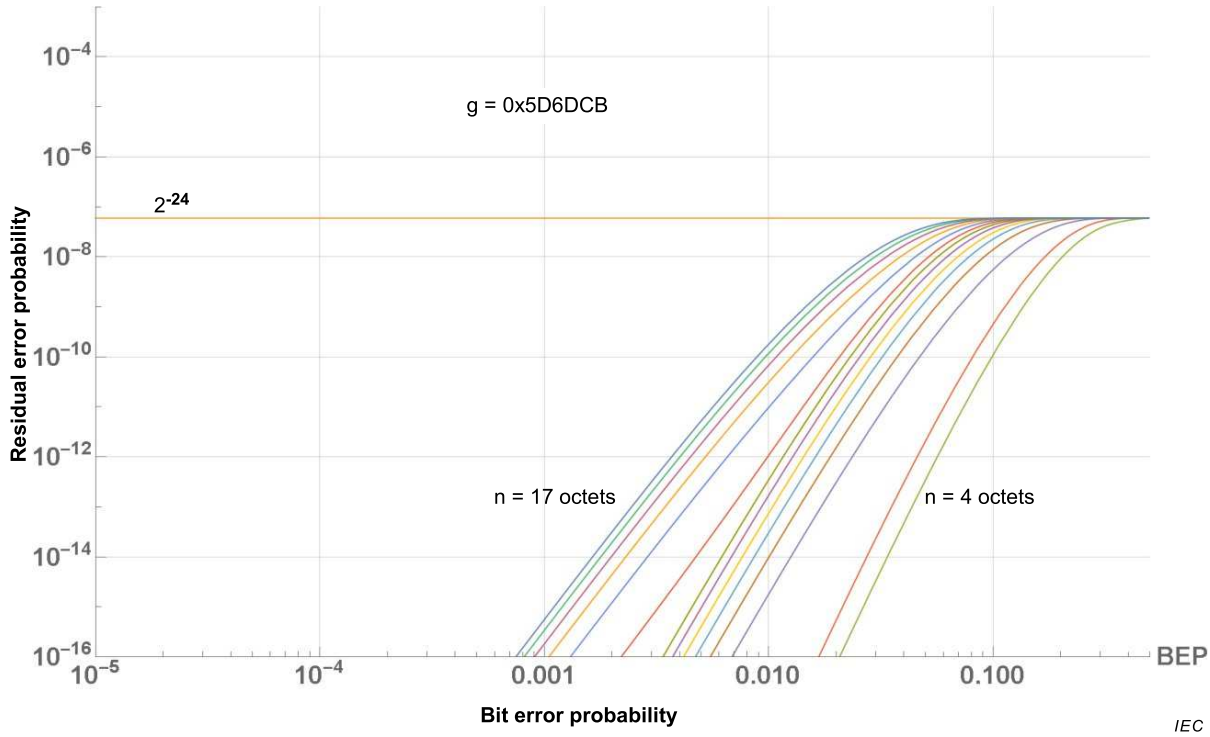


Figure 81 – Residual error probabilities for the 24-bit CRC polynomial

Figure 82 shows diagrams for the 32-bit CRC generator polynomial.

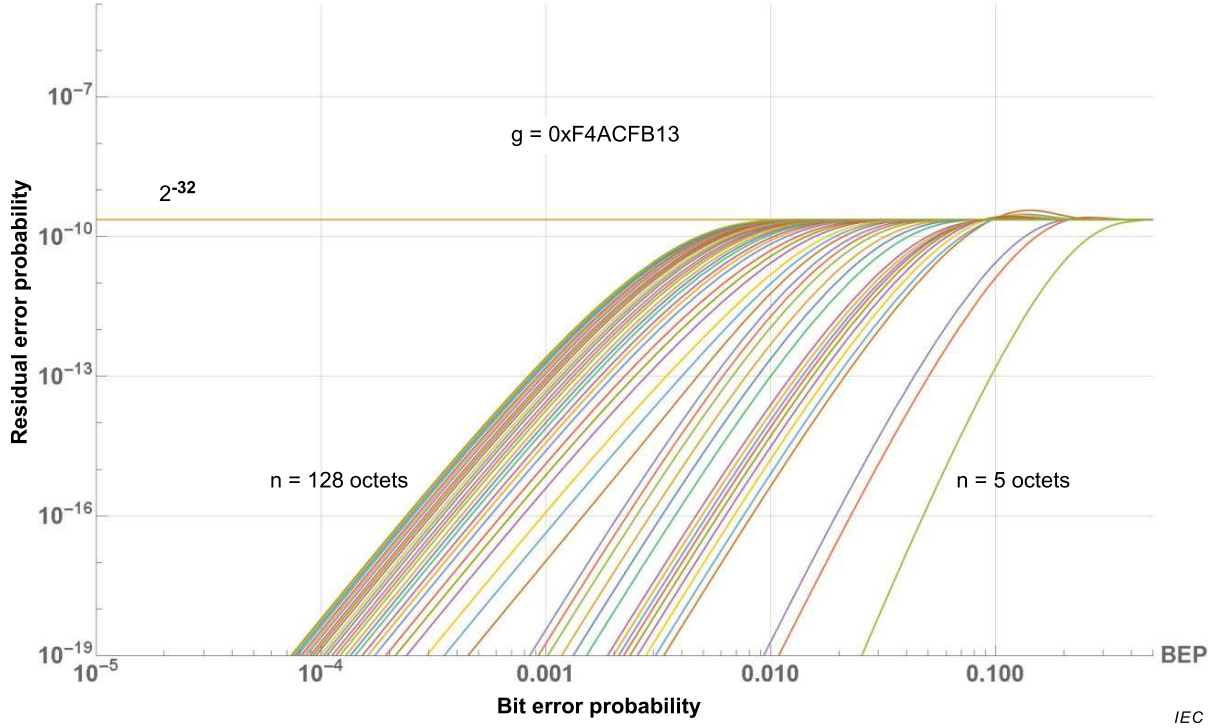


Figure 82 – Residual error probabilities for the 32-bit CRC polynomial

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

g = generator polynomial

n = bit length of data (including the CRC signature)

Summarizing reflections about any perturbing influences lead directly to Figure 83. The combination of the bus failure and error causes provides a (fictive) frequency of corrupted messages on the transmission system. The standard error detecting mechanisms of CP 3/RTE (1st Filter) detect every fault up to a certain level, thus only special bit patterns are reaching the safety layer mechanism. For the frequency of undetected corrupted messages the worst-case value of c = 1/T is taken, since the overall frequency of corrupted safety PDUs on the bus is continuously monitored.

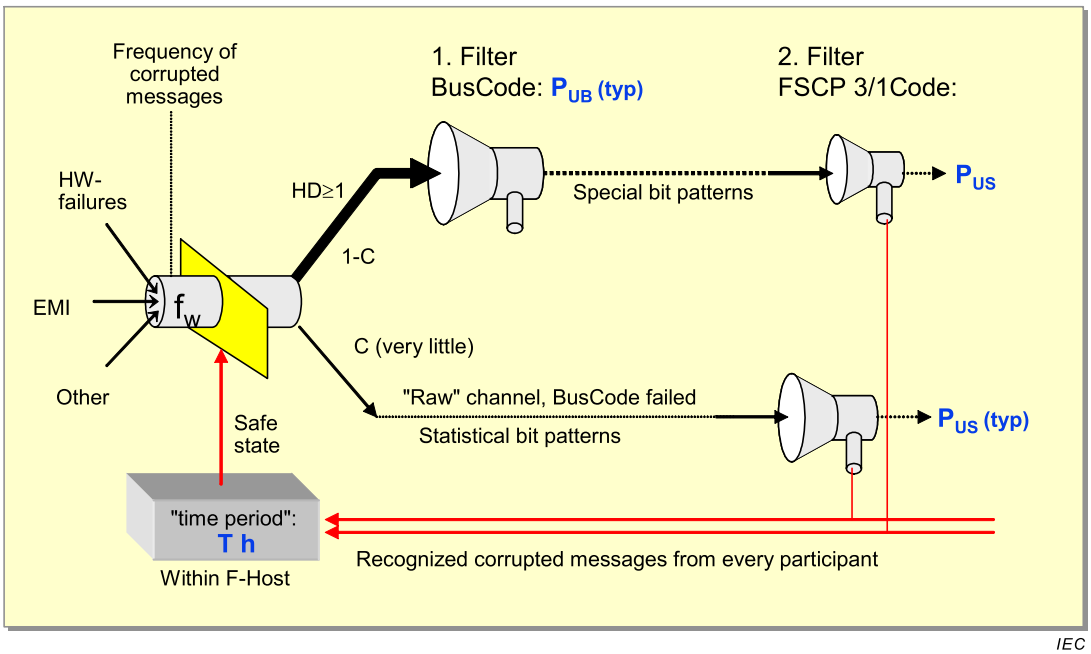


Figure 83 – Monitoring of corrupted messages

The terms used in Figure 83 are specified in Table 29:

Table 29 – Definition of terms in Figure 83

Term	Definition
fw	frequency of corrupted messages
EMI	electromagnetic interference
HD	hamming distance
c	frequency of occurrence
T	measurement period in hours (see 7.2.6)

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 assumptions

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

Generally:

- All devices provide electrical safety SELV/PELV and a CPF 3 conformance test report
- Safety devices 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 or IEC 61326-3-2

FSCP 3/1 protocol (V2-mode):

- Number of retries per channel type (see 9.3.5):
  No restrictions

- Number of safety-related message sinks per safety function:
  see Table 30
- Black Channel CRC polynomials:
  No restrictions
- Active buffering network elements:
  No restrictions; any switch permitted (see 7.3.9 and 5.4.2)
- Safety islands:
  Single port routers are not permitted as borders for a safety island (see 7.3.11)
- Octet-wise splitting of safety PDU:
  No restrictions
- Size of F-I/O data
  F_CRC_Seed =0: ≤ 12 octets
  F_CRC_Seed =1: ≤ 123 octets
- SIL-Monitor observation time:
  F_CRC_Seed =0: 100 h
  F_CRC_Seed =1: 10 h

9.5.3 Non safety related constraints (availability)

- Cyclic data exchange 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 function is only permitted, if there is no hazardous process state, and after an Operator Acknowledgment (OA_C).

9.6.2 Identification and maintenance functions

Identification and maintenance functions (I&M) define 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 [42]. 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. External write access to IM4 shall be denied.

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

9.7 Safety manual

According to IEC 61508-2, F-Host and F-Device suppliers shall provide a safety manual. In case of FSCP 3/1, the instructions, information and parameters of Table 30 shall be included.

Table 30 – 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 Codename ("F_S/D_Address")
Communication relationships per safety function (BP)	For the Basic Protocol: A maximum of 100 relationships is assumed for an average probability of a dangerous failure per hour (PFH) of 10^{-9} (SIL3). In case of more than 100 relationships, the PFH increases by $4*10^{-12}$ per additional relationship. Correspondingly, a maximum of 1000 relationships is assumed in case of SIL2. Additionally, the decision tree in Figure 84 shall be considered.	See Table 37
Programmable IO data router	F-Host (BP): Considerations against systematic loop-back configuration errors (see Figure 84)	Definitions [a]
	F-Host (LP and XP): No considerations	
Power supply	Requirements for electrical safety (PELV), ripple, noise, interrupts, etc. shall be defined	See [41] for country specific constraints such as current limitations
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 [41]
Electromagnetic immunity (EMI)	Applied tests and results (manufacturer declaration or test report from competent test laboratory)	According to IEC 61326-3-1 or -2 whatever is applicable or device specific standard such as IEC 61496 [7]; [41]
Isolation	Applied test voltages and duration at the fieldbus communication port	See [41]
Network components	Constraints on switches, router, and other network components	See 7.3.9, 7.3.11, 9.5.2, and 9.5.3
Installation	According to IEC 61918 and IEC 61784-5-3	See also [59]
Commissioning	Usage of the check list in IEC 61784-5-3 on for example proper addressing, retry checking, or signal quality	See also [60] and 9.9
iParameter	Verification of safety functions of F-Devices supporting the FSCP test mode shall include a check for 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 [33]
SIL monitor	Information for operators, similar to: "In case a request for manual Operator Acknowledgment caused by an associated diagnosis message (e.g. number 77 in table 3) has been perceived more than once within 100 hours it is highly recommended to call in the responsible service technician". Information for operators and service technicians: "This suggests a massive disturbance of the data transmission within the fieldbus system. Causes for this incident can be changes in the installation, corrosion of bus cable shields with connectors, and extreme electromagnetic interferences. Compliance with installation guidelines [61] or [48] should be checked, or an EMC expert (see Annex B for further guidance) should be called in.	See 7.2.6.1.

Item	Instruction and/or parameter	Remark
Security	Instructions on how to establish an adequate level of security defining security zones with security gates.	See 9.8, [41], [48]
Assessment and test reports	Safety assessment reports according IEC 61508 Interoperability and conformance test reports in order to grant CPF 3 conformance.	See Clause 10
a "Programmable IO data router" = A user can deliberately define the routing of IO data on the basis of logical addresses "Configurable router" = A user can select the routing of messages on the basis of network addresses (geographical addresses) with the help of an engineering tool		

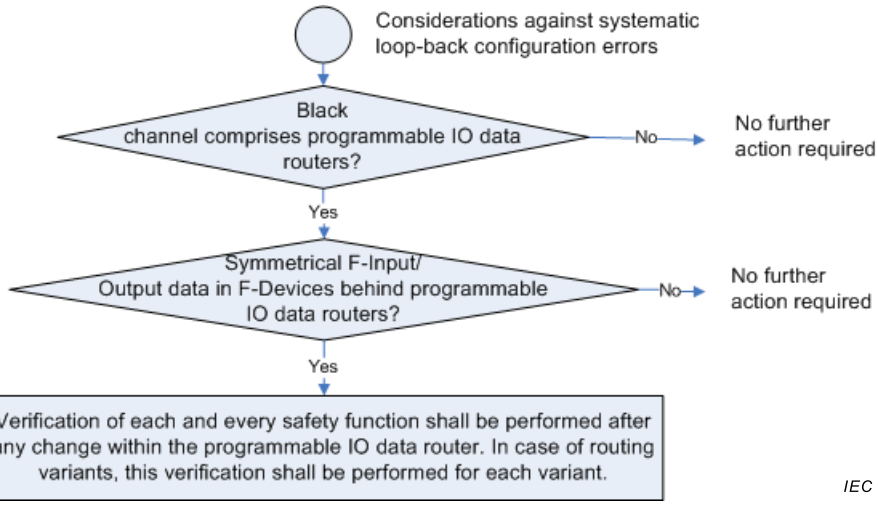


Figure 84 – Considerations against systematic loop-back configuration errors

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 [41]. 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

Figure 85 provides an overview of the security measures.

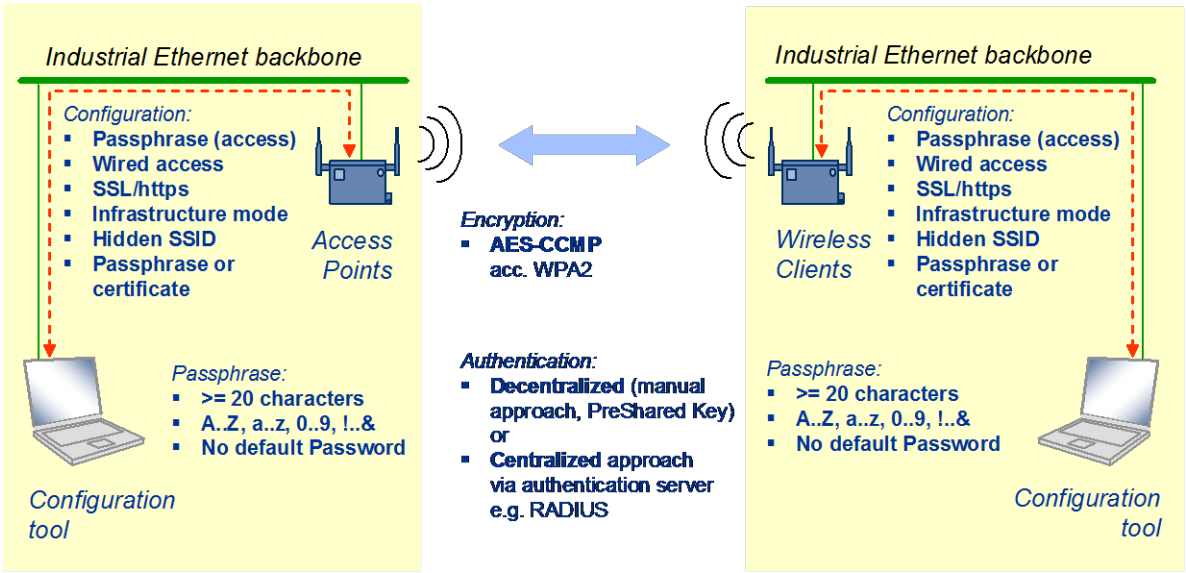


Figure 85 – Security for WLAN networks

The terms used in Figure 85 are specified in Table 31.

Table 31 – Definition of terms in Figure 85

Term	Definition
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 802.11 [29])
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

In order to secure the wireless network against these cases the measures in Table 32 shall be considered according to IEEE 802.11 [29] for industrial WLAN as pointed out in IEC 61784-2 for class A devices.

Table 32 – Security measures for WLAN (IEEE 802.11)

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	For authentication either *Shared Key* (= Preshared Secret) or *Certificates* are

No.	Item	Measure
	procedures	permitted
6	Quality of the pass-phrase for encryption	The length of the pass-phrase shall be ≥ 20 characters (see [29] 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) [29] 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 34 shall be considered according IEEE 802.15.1 [30] for Bluetooth as pointed out in IEC 61784-2 for class A devices. Figure 86 is providing an overview on the security measures.

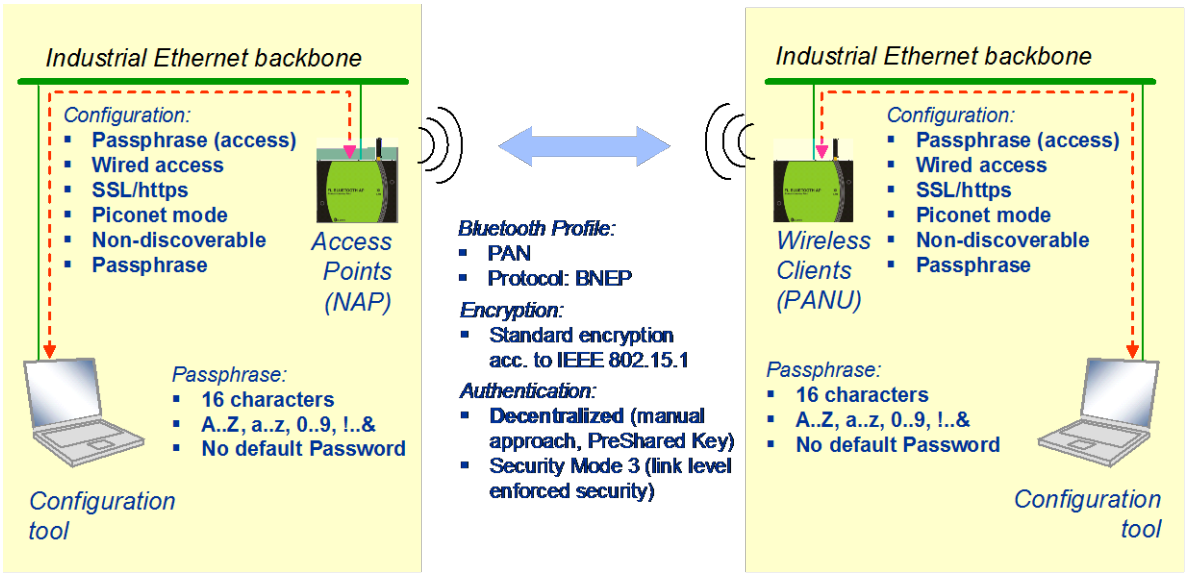


Figure 86 – Security for Bluetooth networks

The terms used in Figure 86 are specified in Table 33.

Table 33 – Definition of terms in Figure 86

Term	Definition
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 [30]
Wireless Client	Member station (slave) of a wireless piconet according IEEE 802.15.1

Table 34 – 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
3	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
4	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
5	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
6	Encryption of cyclic data communication (safety PDU)	Encryption according IEEE 802.15.1 is mandatory
7	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 [24]) 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 35.

Table 35 – F-Host conformance class requirements

Item	Factory Automation	Process Automation	Note
GSD-Support	V5.04 (PB-DP) of [40]; V2.31 (PN-IO) of [43] or later versions	ditto	Regarding F-Parameters only
Support of Channel-granular Passivation	Mandatory for F-Host (XP), see Table 37	ditto	–
"F_CRC_Seed" (see 8.1.5.2) supported	Mandatory for F-Host (XP), see Table 37	ditto	Previous "CRC1" corresponds to "CRC_FP" and shall be supported

Item	Factory Automation	Process Automation	Note
Loop-back check via Bit 7 in Status/ Control Byte	Mandatory for F-Host (LP) and (XP), see Table 37	ditto	Necessary for support of legacy F-Devices/F-Modules
Communication function blocks according IEC 61131-3	Minimum communication function block set is: RDIAG, RALRM [44]	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) [44]
Quantities (bit) of F-I/O data	Up to 64 bit (Bool) coded as Unsigned8, -16, -32	ditto	–
Quantities of F-I/O data (octets)	F_CRC_Seed = 0: up to12 octets F_CRC_Seed = 1: up to13 octets minimum required to support, 13th octet as qualifier; maximum of 123 octets permitted	ditto	Sizes of supported minimum data structures as shown for example in Figure 4, Figure 18, Figure 22, and Figure 25.
Data types	Unsigned8, -16, -32, Integer16, -32	all FSCP 3/1 data types: see Table 2	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: see [45] and [68]
Read and write record service	mandatory	mandatory	According CP 3/1, CP3/2, and CP/RTE
MS2 (F-Slave access)	Recommended	optional	According CP 3/1, CP3/2 Small CPUs may not be able to carry high traffic through load
F-Device access	Recommended	optional	According CP3/RTE
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 21	According to [58] or via tool interface that meets the requirements of Table 21	–
F_WD_Time_2	Optional for F-Host (XP)	Recommended for F-Host (XP)	See 8.1.4

The expanded protocol functions in this document require conformance considerations between three F-Host protocol versions (BP, LP, XP) and F-Devices/F-Modules according to IEC 61784-3-3 Edition 2 and this Edition 3.

Table 36 shows the main characteristics of the protocol versions.

Table 36 – Main characteristics of protocol versions

Protocol type	Characteristics
Basic protocol (BP)	- IEC 61784-3-3 Ed.2 - Restriction in Safety manual: Insert requirement in safety manual: See Table 30, "Communication relationships per safety function"
Loop-back extension (LP)	- IEC 61784-3-3 Ed.2 - F_CRC_Seed = 0 - Loop-back Bit 7
Expanded protocol (XP)	- IEC 61784-3-3 Ed.3 - F_CRC_Seed = 1

Table 37 specifies the requirements for the two F-Device/Module versions.

Table 37 – F-Host/F-Device conformance matrix

F-Host	F-Device/Module	
	according previous editions of this standard	**according to this standard**
according previous editions of this standard	**Basic protocol (BP)** - No change for F-Device and GSD (no F_CRC_Seed)	**Basic protocol (BP)** - F_CRC_Seed = 0
according to this standard	**Loop-back extension (LP)** - No change for F-Device and GSD	**Expanded protocol (XP)** - New GSD file - Qualifier for F-I/O data, see [66]

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.

10.2 Obligations

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

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

Annex A
(informative)

Additional information for functional safety communication profiles of CPF 3

A.1 Hash function calculation

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

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

```
void crc24_calc(unsigned char x, unsigned long * r)
  int i;
  for (i = 1; i <= 8; i++)
    if ((bool)(*r & 0x800000) != (bool)(x & 0x80))
      /* 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 seed values of r can be "0" (see 8.1.8), "1" (see 8.1.5.6, 8.1.7, 8.2) or "CRC_FP" = F_Par_CRC (see 8.1.5.6).

For this calculation Table A.1 is used.

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

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

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

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

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

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

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

```
r = crctab16 [((r >> 8) ^ *q++) & 0xff] ^ (r << 8)        (A.3)
```

For this calculation Table A.3 is used.

Table A.3 – The table "Crctab16" for 16 bit CRC signature calculations

CRC lookup table (0 to 255)							
0000	4EAB	9D56	D3FD	7407	3AAC	E951	A7FA
E80E	A6A5	7558	3BF3	9C09	D2A2	015F	4FF4
9EB7	D01C	03E1	4D4A	EAB0	A41B	77E6	394D
76B9	3812	EBEF	A544	02BE	4C15	9FE8	D143
73C5	3D6E	EE93	A038	07C2	4969	9A94	D43F
9BCB	D560	069D	4836	EFCC	A167	729A	3C31
ED72	A3D9	7024	3E8F	9975	D7DE	0423	4A88
057C	4BD7	982A	D681	717B	3FD0	EC2D	A286
E78A	A921	7ADC	3477	938D	DD26	0EDB	4070
0F84	412F	92D2	DC79	7B83	3528	E6D5	A87E
793D	3796	E46B	AAC0	0D3A	4391	906C	DEC7
9133	DF98	0C65	42CE	E534	AB9F	7862	36C9
944F	DAE4	0919	47B2	E048	AEE3	7D1E	33B5
7C41	32EA	E117	AFBC	0846	46ED	9510	DBBB
0AF8	4453	97AE	D905	7EFF	3054	E3A9	AD02
E2F6	AC5D	7FA0	310B	96F1	D85A	0BA7	450C
81BF	CF14	1CE9	5242	F5B8	BB13	68EE	2645
69B1	271A	F4E7	BA4C	1DB6	531D	80E0	CE4B
1F08	51A3	825E	CCF5	6B0F	25A4	F659	B8F2
F706	B9AD	6A50	24FB	8301	CDAA	1E57	50FC
F27A	BCD1	6F2C	2187	867D	C8D6	1B2B	5580
1A74	54DF	8722	C989	6E73	20D8	F325	BD8E
6CCD	2266	F19B	BF30	18CA	5661	859C	CB37
84C3	CA68	1995	573E	F0C4	BE6F	6D92	2339
6635	289E	FB63	B5C8	1232	5C99	8F64	C1CF
8E3B	C090	136D	5DC6	FA3C	B497	676A	29C1
F882	B629	65D4	2B7F	8C85	C22E	11D3	5F78
108C	5E27	8DDA	C371	648B	2A20	F9DD	B776
15F0	5B5B	88A6	C60D	61F7	2F5C	FCA1	B20A
FDFE	B355	60A8	2E03	89F9	C752	14AF	5A04
8B47	C5EC	1611	58BA	FF40	B1EB	6216	2CBD
6349	2DE2	FE1F	B0B4	174E	59E5	8A18	C4B3

This table contains 16 bit values in hexadecimal representation for each value (0 to 255) of the argument a in the function crctab16 [a]. The table should be used in ascending order from top left (0) to bottom right (255).

A.2 Example values for MonitoringNumbers (MNR)

Table A.4 shows the first four MNR values for two different Codename examples (see 7.1.5 and 7.1.6). The value for the variable Modifier is assumed to be "0".

Table A.4 – Values of CN_incrNR_64 and MNR for F-Host PDU

Codename 0x010001			Codename 0x010002		
Nr	CN_incrNR_64 [0]	MNR	Nr	CN_incrNR_64 [0]	MNR
0	-	CRC_FP+	0	-	CRC_FP+
1	0xCACFA720FA43BF62	0xCACFA720	1	0x444B59A4D64ABABB	0x444B59A4
2	0x174EE7E3C6063E8F	0x174EE7E3	2	0xE91C8E94EEA2B915	0xE91C8E94
3	0xE21E8F04C049FDF1	0xE21E8F04	3	0x2D67E839C4ED73D0	0x2D67E839
4	0xF96D76E886503C80	0xF96D76E8	4	0x168476CEB3902CE5	0x168476CE

A.3 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.

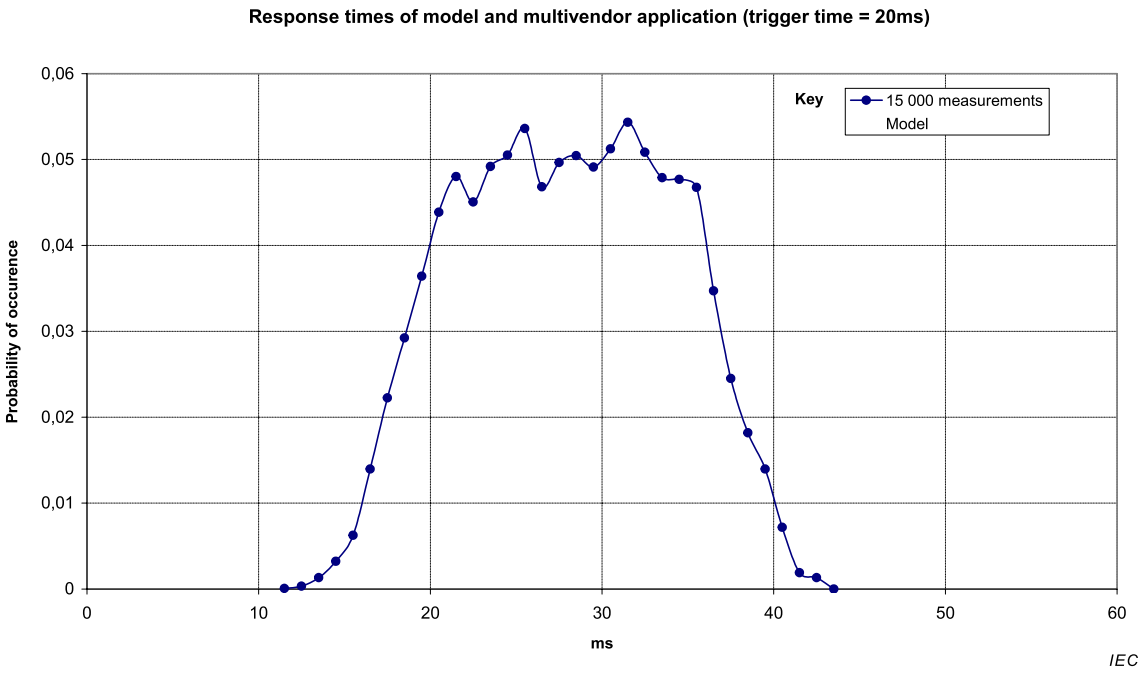


Figure A.2 – Comparison of the response time model and a real application

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.

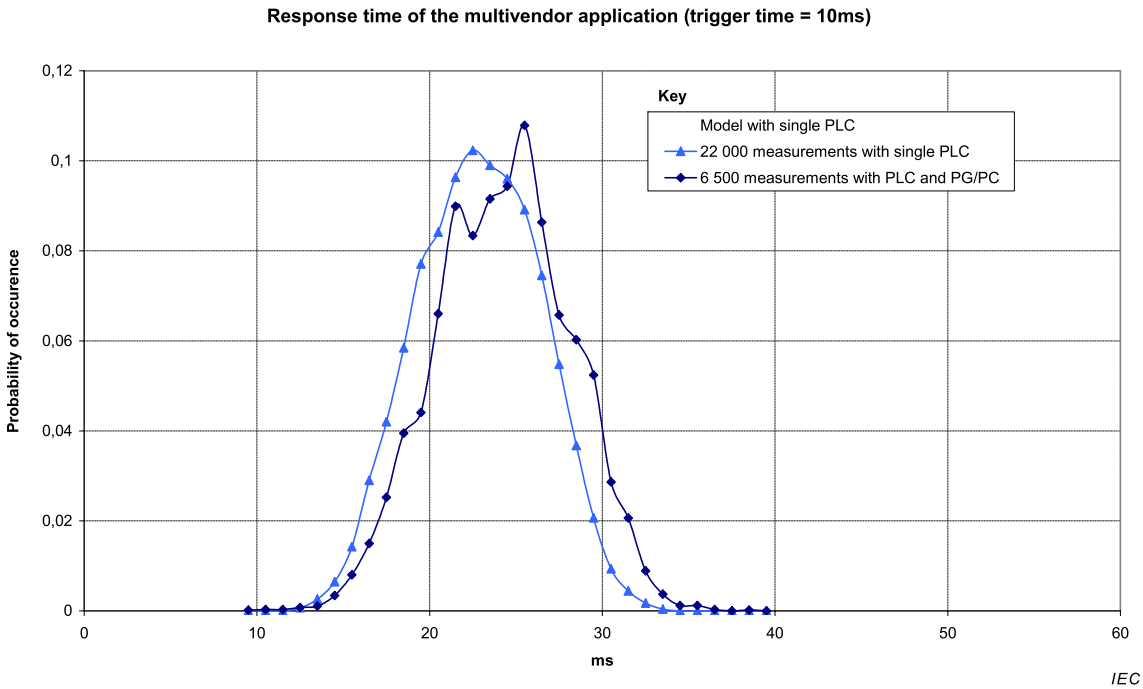


Figure A.3 – Frequency distribution of measured response times

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 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. 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 shows 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.

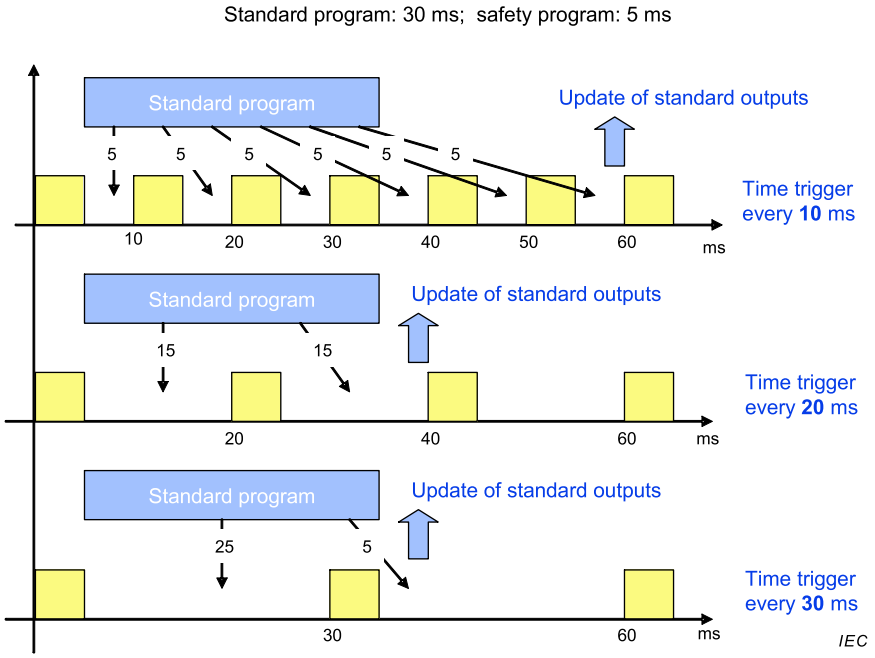


Figure A.4 – F-Host with standard and safety-related application programs

Annex B
(informative)

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

According to IEC rules, this standard does not make a statement on how to validate conformance. However, test and validation of compliance of FSCP 3/1 devices with IEC 61784-3-3 may be required by law.

Corresponding information relative to the test and compliance with this standard can be retrieved from the local National Committees of the IEC or from the relevant fieldbus organization.

NOTE For IEC 61784-3-3, the relevant fieldbus organization is PROFIBUS Nutzerorganisation e.V. (PNO), see www.profibus.com.

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 functional safety of electrical and electronic systems including equipment with regard to electromagnetic phenomena*

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

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

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

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

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

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

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

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

[12] IEC 61784-4[7], *Industrial communication networks – Profiles – Part 4: Secure communications for fieldbuses*

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

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

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

[16] IEC TR 62059-11:2002, *Electricity metering equipment – Dependability – Part 11: General concepts*

[17] IEC TR 62210:2003, *Power system control and associated communications – Data and communication security*

---

7 Proposed new work item under consideration.

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

[19] IEC TR 62685, *Industrial communication networks – Profiles – Assessment guideline for safety devices using IEC 61784-3 functional safety communication profiles (FSCPs)*

[20] ISO/IEC Guide 51:2014, *Safety aspects – Guidelines for their inclusion in standards*

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

[22] ISO/IEC 2382-16:1996, *Information technology – Vocabulary – Part 16: Information theory*

[23] ISO/IEC 7498-1, *Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model*

[24] ISO 10218-1, *Robots and robotic devices – Safety requirements for industrial robots – Part 1: Robots*

[25] ISO 12100, *Safety of machinery – General principles for design – Risk assessment and risk reduction*

[26] ISO 13849 (all parts), *Safety of machinery – Safety-related parts of control systems*

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

[28] ISO 15745-4, *Industrial automation systems and integration – Open systems application integration framework – Part 4: Reference description for Ethernet-based control systems*

[29] IEEE 802.11-2012, *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*

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

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

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

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

[34] ANDREW S. TANENBAUM, DAVID J. WETHERALL, *Computer Networks*, 5th Edition, Prentice Hall, N.J., ISBN-10: 01321269580, ISBN-13: 978-0132126953

[35] W. WESLEY PETERSON, EDWARD J. WELDON, Error-Correcting Codes, 2nd Edition 1972, MIT-Press, ISBN 0-262-16-039-0

[36] BRUCE P. DOUGLASS, *Doing Hard Time: Developing Real-Time Systems with UML, Objects, Frameworks, and Patterns,* 2011, Addison-Wesley, ISBN-10: 0321774930, ISBN-13: 978-0321774934

[37] NFPA79 (2012), *Electrical Standard for Industrial Machinery*

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

[39] 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

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

[41] PROFIBUS Guideline: *PROFIsafe – Environmental Requirements,* V2.6, June 2015. Order-No. 2.232

[42] PROFIBUS Profile Guideline, *Part 1: Identification & Maintenance Functions*, V1.2, October 2013. Order-No. 3.502

[43] PROFIBUS Guideline: *GSDML Specification for PROFINET IO*, Version 2.31, November 2013. Order-No. 2.352

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

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

[46] PROFINET Guideline: *PROFINET Cabling and Interconnection Technology,* Version 3.0.1, October 2011. Order-No. 2.252

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

[48] PROFINET Guideline: PROFINET Security, V2.0, November 2013. Order-No. 7.002

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

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

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

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

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

[54] 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 >

[55] 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 >

[56] 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 >

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

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

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

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

[61] PROFIBUS Guideline: *PROFIsafe Policy*, V1.5, July 2011. Order No. 2.282

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

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

[64] PI Specification: PROFINET IO: *Configure in Run for Distributed Control Systems*, V1.10, February 2015. Order-No. 7.112

[65] PROFIBUS Profile Guideline, *Part 4: iPar-Server*, V1.0.1, July 2011. Order-No. 3.532

[66] PI Specification: *Remote IO for Factory Automation*, V1.0, September 2012. Order-No. 3.242

[67] PI Specification: *PROFINET IO System Redundancy for Distributed Control Systems,* V1.10, February 2015. Order-No. 7.122

[68] PROFINET Guideline: *Diagnosis for PROFINET IO*, V1.0, November 2013. Order-No. 7.142

[69] PROFINET Guideline: *PROFINET IO Device Integration,* V1.0, December 2013. Order-No. 7.352

[70] PROFIBUS Guideline: *PROFIsafe – Test & Certification,* V2.2, Sep 2014. Order-No. 2.242

———————

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 Électrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC") Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.

Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.

4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.

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

Cette troisième édition annule et remplace la deuxième édition parue en 2010. Cette édition constitue une révision technique. Cette édition inclut les modifications techniques majeures suivantes par rapport à l'édition précédente:

- Mode V1 hérité supprimé de la présente édition de protocole;
- Extensions de protocoles afin d'assurer une protection contre les bouclages potentiels (extensions LP);
- Extensions de protocoles afin de conserver SIL3 pour les réseaux de sécurité avec de très nombreux participants (extensions XP) et le nouveau paramètre F "F_CRC_Seed" ultérieur;

- Introduction de MonitoringNumbers (MNR) aléatoires et disjoints basés sur le nom de code (Codename) outre les numéros consécutifs précédents;
- Dispositions concernant la passivation granulaire des canaux (Channel Granular Passivation) et le nouveau Paramètre F "F_Passivation" ultérieur;
- Extensions GSD dues aux nouveaux paramètres F;
- Notations selon la famille CP3 dans l'IEC 61158 (par exemple, contrôleur d'entrée-sortie);
- Types de messages de diagnostic supplémentaires;
- Diverses corrections d'erreurs et corrections de typographies;
- Documents mis à jour dans la bibliographie.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
65C/851/FDIS	65C/854/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à l'approbation de cette norme.

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

Une liste de toutes les parties de la série IEC 61784-3, publiées sous le titre général *Réseaux de communication industriels – Profils – Bus de terrain de sécurité fonctionnelle*, peut être consultée sur le site web de l'IEC.

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 l'IEC sous "http://webstore.iec.ch" dans les données relatives à la publication recherchée. À 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 garde 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.

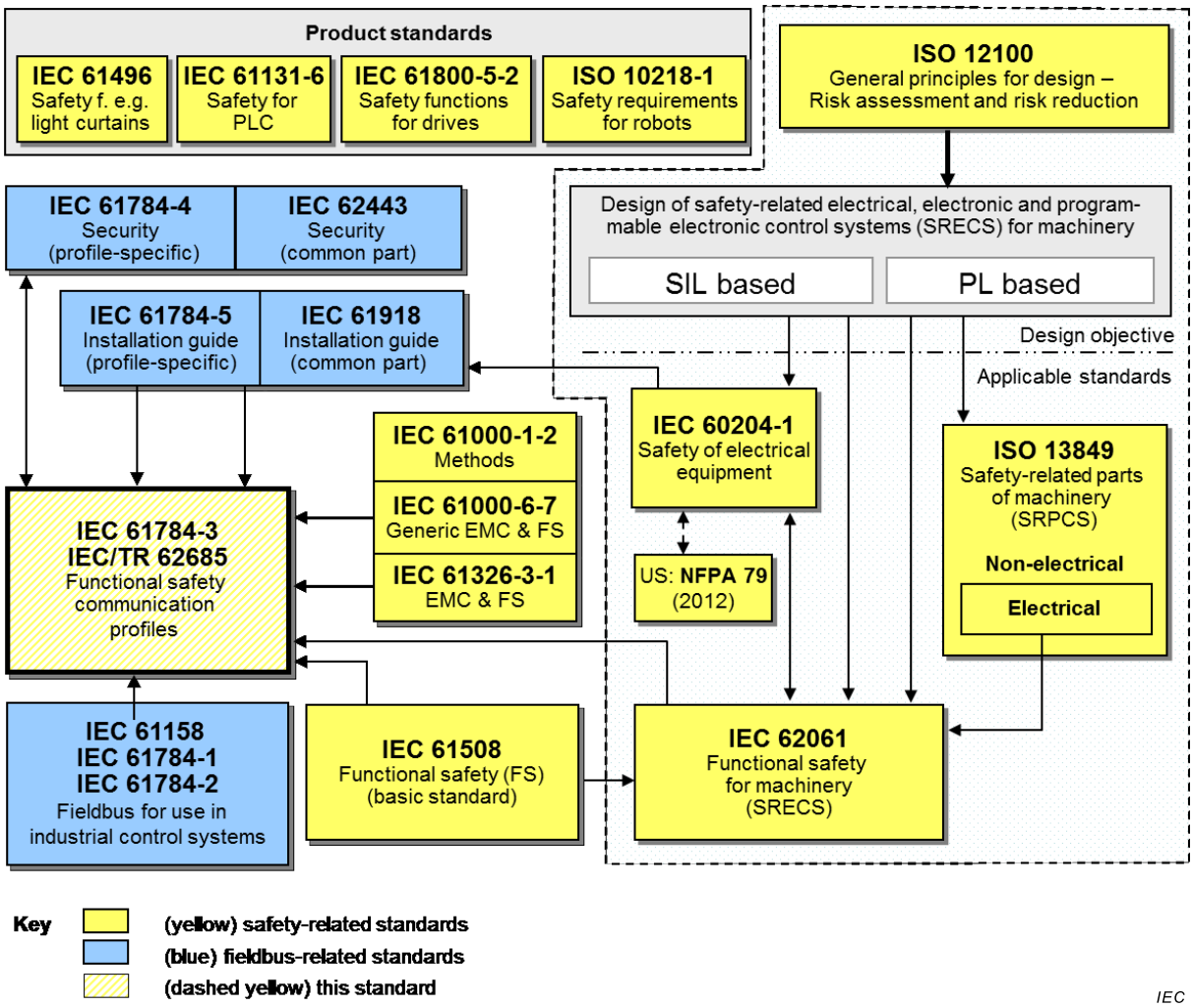
0 Introduction

0.1 Généralités

La norme IEC 61158 relative aux bus de terrain, ainsi que ses normes associées IEC 61784-1 et IEC 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, les améliorations des bus de terrain continuent à se développer, traitant des applications pour des domaines 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 IEC 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 l'IEC 61784-1, l'IEC 61784-2 et la série IEC 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.



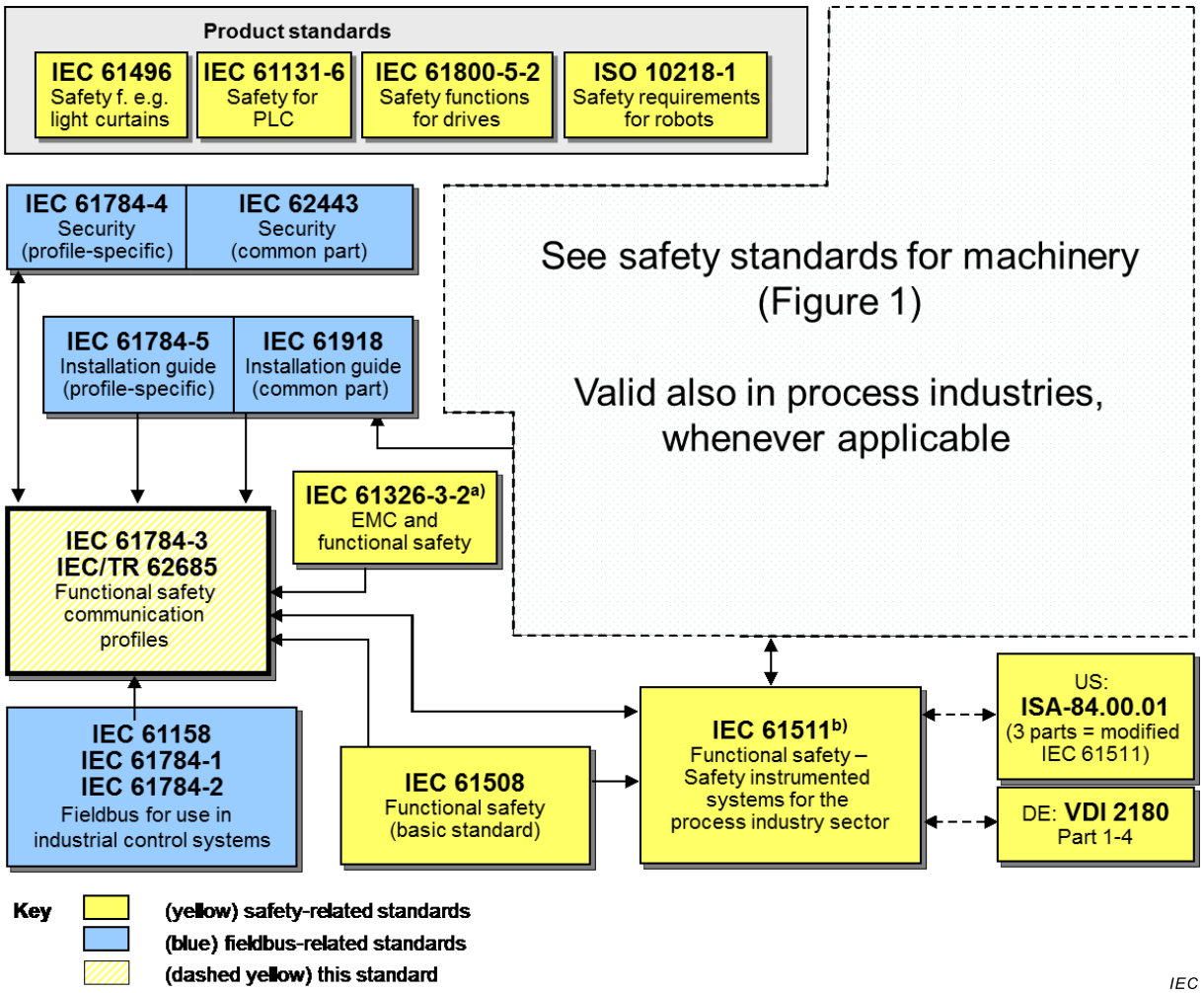
Anglais	Français
Product standards	Normes de produits
Safety function, e.g. light curtains	Fonction de sécurité, par exemple rideaux de lumière

Anglais	Français
Safety for PLC	Sécurité relative aux automates programmables
Safety functions for drives	Fonctions de sécurité applicables aux entraînements
Safety requirements for robots	Exigences de sécurité applicables aux robots
General principles for design – Risk assessment and risk reduction	Principes généraux de conception – Appréciation du risque et réduction du risque
Security (profile-specific)	Sûreté (spécifique au profil)
Security (common part)	Sûreté (partie commune)
Design of safety-related electrical, electronic and programmable electronic control systems (SRECS) 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)
Design objective	Objectif de conception
Applicable standards	Normes applicables
Methods	Méthodes
Generic EMC & FS	CEM & FS génériques
EMC & FS	CEM & FS
Safety of electrical equipment	Sécurité des équipements électriques
Safety-related parts of machinery (SRPCS)	Sécurité des machines – Parties des systèmes de commande relatives à la sécurité
Non-electrical	Non électrique
Electrical	Électrique
Functional safety communication profiles	Profils de communication de sécurité fonctionnelle
Fieldbus for use in industrial control systems	Bus de terrain pour utilisation dans des systèmes de commande industriels
Functional safety (FS) (basic standard)	Sécurité fonctionnelle (FS) (norme de base)
Functional safety for machinery (SRECS)	Sécurité fonctionnelle des machines
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

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

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

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



Anglais	Français
Product standards	Normes de produits
Safety function, e.g. light curtains	Fonction de sécurité, par exemple rideaux de lumière
Safety for PLC	Sécurité relative aux automates programmables
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
EMC and functional safety	CEM et sécurité fonctionnelle
Fieldbus for use in industrial control systems	Bus de terrain pour utilisation dans des systèmes de commande industriels
Functional safety (basic standard)	Sécurité fonctionnelle (norme de base)
Functional safety–safety instrumented systems for	Sécurité fonctionnelle – Systèmes instrumentés de

Anglais	Français
the process industry sector	sécurité pour le secteur des industries de transformation
3 parts = modified IEC 61511	3 parties = IEC 61511 modifiée
Part 1 –4	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 IEC 61326-3-1 ou IEC 61000-6-7.

[b] EN ratifiée.

Figure 2 – Relations entre l'IEC 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 IEC 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 (FSCP) retenu au sein du système – la mise en œuvre du profil de communication de sécurité fonctionnelle dans un appareil normal ne suffit pas à le qualifier d'appareil de sécurité.

La présente norme décrit:

– les principes de base de mise en œuvre des exigences de la série IEC 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;
– les profils de communication de sécurité fonctionnelle pour plusieurs familles de profils de communication dans les IEC 61784-1 et IEC 61784-2, y compris les extensions de la couche de sécurité aux sections relatives au service et aux protocoles de communication de la série IEC 61158.

0.2 Déclaration de droits de propriété

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

US 6907542	[SI]	System, device and method for determining the reliability of data carriers in a failsafe system network
US 6725419 DE 59910661.1 EP 1064590	[SI]	Automation system and method for operating an automation system

US 7808917 DE 50 2005 001 819.2 EP 1686732	[SI]	Method and system for transmitting telegrams
US 7640480 DE 50 2005 004 305.7 EP 1802019	[SI]	Detection of errors in the communication of data
EP 1921525	[SI]	Security-related system component e.g. guard door, for automation system of production system, has comparing unit comparing signatures for identity, where component supports security-related operation during sameness of signatures
EP 13172092.2	[SI]	Method and System for Detecting Errors when Transmitting Data from a Transmitter to at Least One Receiver

L'IEC ne prend pas position quant à la preuve, à la validité et à la portée de ces droits de propriété.

Le détenteur de ces droits de propriété a donné l'assurance à l'IEC qu'il consent à négocier des licences avec des demandeurs du monde entier, gratuitement ou à des termes et conditions raisonnables et non discriminatoires. À ce propos, la déclaration du détenteur des droits de propriété est enregistrée à l'IEC.

Des informations peuvent être demandées à:

[SI] Siemens Aktiengesellschaft
CT IP M&A
Otto-Hahn-Ring 6
81739 München
ALLEMAGNE

L'attention est d'autre part attirée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété intellectuelle autres que ceux identifiés ci-dessus. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et de ne pas avoir signalé leur existence.

L'ISO (www.iso.org/patents) et l'IEC (http://www.iec.ch/tctools/patent_decl.htm) maintiennent à disposition des bases de données en ligne des brevets relatifs à leurs normes. Les utilisateurs sont invités à les consulter pour obtenir les dernières informations relatives à ces brevets.

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 IEC 61784-3 spécifie une couche de communication relative à la sécurité (services et protocole) fondée sur la CPF 3 de l'IEC 61784-1 et les Types 3 et 10 de l'IEC 61784-2 (CP 3/1, CP 3/2, CP 3/4, CP 3/5 et CP 3/6) et de l'IEC 61158. Elle identifie les principes applicables aux communications de sécurité fonctionnelle définies dans l'IEC 61784-3, et appropriés à cette couche de communication de sécurité. Cette couche de communication de sécurité est destinée à être mise en œuvre uniquement sur les appareils de sécurité.

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

La présente partie[1] définit les mécanismes de transmission des messages relatifs à la sécurité entre les participants d'un réseau réparti, en utilisant la technologie de bus de terrain conformément aux exigences de la série IEC 61508[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 d'appareils 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 appareil normal ne suffit pas à le qualifier d'appareil de sécurité.

2 Références normatives

Les documents suivants sont cités en référence de manière normative, en intégralité ou en partie, dans le présent document et sont indispensables pour son application. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

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

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

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

---

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

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

IEC 61131-2:2007, *Automates programmables – Partie 2: Exigences et essais des équipements*

IEC 61131-3, *Automates programmables – Partie 3: Langages de programmation*

IEC 61158-2, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 2: Spécification et définition des services de la couche physique*

IEC 61158-3-3, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 3-3: Définition des services de la couche liaison de données – Éléments de type 3*

IEC 61158-4-3, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 4-3: Spécification du protocole de la couche liaison de données – Éléments de type 3*

IEC 61158-5-3, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 5-3: Définition des services de la couche application – Éléments de type 3*

IEC 61158-5-10, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 5-10: Définition des services de la couche application – Éléments de type 10*

IEC 61158-6-3, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 6-3: Spécification du protocole de la couche application – Éléments de type 3*

IEC 61158-6-10, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 6-10: Spécification du protocole de la couche application– Éléments de type 10*

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

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

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

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

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

IEC 61784-1, *Réseaux de communication industriels– Profils – Partie 1: Profils de bus de terrain*

IEC 61784-2, *Réseaux de communication industriels– Profils – Partie 2: Profils de bus de terrain supplémentaires pour les réseaux en temps réel basés sur l'ISO/CEI 8802-3*

IEC 61784-3:—[3], *Réseaux de communication industriels– Profils – Partie 3: Bus de terrain de sécurité fonctionnelle – Règles générales et définitions de profils*

IEC 61784-5-3, *Réseaux de communication industriels – Profils – Partie 5-3: Installation des bus de terrain – Profils d'installation pour CPF 3*

IEC 61918:2013, *Réseaux de communication industriels – Installation de réseaux de communication dans des locaux industriels*

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

IEC 62280:2014, *Applications ferroviaires – Systèmes de signalisation, de télécommunication et de traitement – Communication de sécurité dans les systèmes de transmission*

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

ISO 13849-1:2006, *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 relatives à la sécurité – Partie 2: Validation*

3 Termes, définitions, symboles, abréviations et conventions

3.1 Termes et définitions

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

NOTE Les définitions des termes eux-mêmes définis en 3.1 sont marquées en italique.

3.1.1 Termes et définitions communs

NOTE Ces termes et définitions communs sont issus de l'IEC 61784-3:—.

3.1.1.1
élément de réseau actif
élément de réseau contenant des composants actifs du point de vue électrique et/ou optique et permettant d'étendre le réseau

Note 1 à l'article: Les répéteurs et les commutateurs sont des exemples d'éléments de réseau actif.

[SOURCE: IEC 61918:2013, 3.1.2]

3.1.1.2
disponibilité
probabilité, pour un système automatisé, qu'il ne se produise pas de condition opérationnelle non satisfaisante, par exemple la perte de production, pendant une période donnée

3.1.1.3
probabilité d'erreurs sur les éléments binaires
Pe
probabilité de réception d'un bit donné avec la valeur incorrecte

[3] A publier.

3.1.1.4
canal noir
système de communication défini qui contient un ou plusieurs éléments sans preuve de conception ou de validation conformément à l'IEC 61508

Note 1 à l'article: Cette définition étend la signification habituelle du canal pour inclure le système qui contient le canal.

3.1.1.5
canal de communication
connexion logique entre deux points limites d'un *système de communication*

3.1.1.6
système de communication
ensemble de matériels, de logiciels et de supports de propagation qui permet la transmission de *messages* (ISO/IEC 7498-1, couche d'application) d'une application à une autre

3.1.1.7
connexion
liaison logique entre objets applicatifs au sein du même appareil ou d'appareils différents

3.1.1.8
contrôle de redondance cyclique
CRC
<valeur> donnée redondante déduite et enregistrée ou transmise simultanément d'un bloc de données afin de détecter toute corruption des données

<méthode> procédure utilisée pour calculer les données redondantes

Note 1 à l'article: Les termes "code CRC" et "signature CRC", ainsi que les étiquettes comme CRC1, CRC2, peuvent également être utilisés dans la présente norme pour se référer aux données redondantes.

Note 2 à l'article: Voir également [33], [34][4].

3.1.1.9
système de communication défini
canal défini
nombre fixe ou nombre maximal fixe d'éléments reliés par un système de communication à bus de terrain, dont les propriétés sont connues et fixées, par exemple les conditions d'installation, l'immunité électromagnétique, les éléments (actifs) de réseau industriel, et où le risque d'accès non autorisé est réduit à un niveau tolérable conformément au modèle de cycle de vie de l'IEC 62443, en utilisant par exemple des zones et des conduits

3.1.1.10
erreur
écart ou discordance entre une valeur ou une condition calculée, observée ou mesurée et la valeur ou la condition vraie, prescrite ou théoriquement correcte

Note 1 à l'article: Les erreurs peuvent être causées par des erreurs de conception du matériel/logiciel et/ou des informations altérées du fait d'un brouillage électromagnétique et/ou autres effets.

Note 2 à l'article: Les erreurs ne produisent pas nécessairement une *défaillance* ou une *anomalie*.

[SOURCE: IEC 61508-4:2010, 3.6.11, modifié – notes ajoutées]

4 Les chiffres entre crochets se réfèrent à la Bibliographie.

3.1.1.11
défaillance
cessation de l'aptitude d'une unité fonctionnelle à accomplir une fonction requise ou à fonctionner comme prévu

Note 1 à l'article: Une défaillance peut être causée par une *erreur* (problème de conception matérielle/logicielle ou rupture de message, par exemple).

[SOURCE: IEC 61508-4:2010, 3.6.4, modifié – notes et figures remplacées]

3.1.1.12
anomalie
condition anormale qui peut entraîner une réduction de capacité ou la perte de capacité d'une unité fonctionnelle à accomplir une fonction requise

Note 1 à l'article: L'IEC 60050-191:1990, 191-05-01, définit le terme "fault" (en français "panne") comme un état d'inaptitude à accomplir une fonction requise, en excluant l'inaptitude due à la maintenance préventive, à d'autres actions programmées ou à un manque de ressources extérieures.

[SOURCE: IEC 61508-4:2010, 3.6.1, modifié – référence à la figure supprimée]

3.1.1.13
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

3.1.1.14
système de bus de terrain
système qui utilise un *bus de terrain* avec des appareils reliés

3.1.1.15
trame
DLPDU
DÉCONSEILLÉ: trame
Data Link Protocol Data Unit (Unité de données de protocole de liaison de données)

3.1.1.16
séquence de contrôle de trame
FCS
données redondantes issues d'un bloc de données d'une DLPDU (trame), qui utilisent une fonction de hachage et enregistrées ou transmises avec le bloc de données, afin de déterminer l'altération des données

Note 1 à l'article: Une FCS peut être calculée à l'aide d'un CRC ou d'une autre fonction de hachage.

Note 2 à l'article: Voir également [33], [34].

Note 3 à l'article: L'abréviation «FCS» est dérivée du terme anglais développé correspondant «Frame Check Sequence».

3.1.1.17
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 à l'article: Les fonctions de hachage peuvent être utilisées pour déterminer l'altération des données.

Note 2 à l'article: Les fonctions de hachage communes incluent la parité, la somme de contrôle ou le CRC.

[SOURCE: IEC TR 62210:2003, 4.1.12, modifié – ajout de "habituellement" et de notes]

3.1.1.18
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

3.1.1.19
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

3.1.1.20
message
série ordonnée d'octets, destinée à communiquer des informations

[SOURCE: ISO/IEC 2382-16:1996, 16.02.01, modifié – caractère remplacé par octet]

3.1.1.21
déclenchement de nuisance
déclenchement parasite sans effet préjudiciable

Note 1 à l'article: Les erreurs anormales internes peuvent être générées dans des systèmes de communication, par exemple des systèmes de transmission par ondes radioélectriques, du fait d'un trop grand nombre de nouvelles tentatives en présence de perturbations.

3.1.1.22
essai périodique
essai périodique destiné à détecter les défaillances cachées dangereuses d'un *système relatif à la sécurité* de telle sorte que, lorsque nécessaire, une réparation peut rétablir le système dans une condition "comme neuf'' ou dans une condition aussi proche que possible de celle-ci

Note 1 à l'article: Un essai de validité est destiné à confirmer que l'état du système relatif à la sécurité garantit l'intégrité de sécurité spécifiée.

[SOURCE: IEC 61508-4:2010, 3.8.5, modifié – remplacement des quatre notes par une autre note]

3.1.1.23
niveau de performance
PL
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

Note 1 à l'article: L'abréviation «PL» est dérivée du terme anglais développé correspondant "performance level".

[SOURCE: ISO 13849-1:2006, 3.1.23, traduction française modifiée – amélioration]

3.1.1.24
très basse tension de protection
TBTP
circuit électrique dans lequel la tension ne peut pas dépasser 30 V eff. c.a., 42,4 V crête ou 60 V c.c. en conditions normales et en conditions de défaut isolé, sauf en conditions de défauts de terre dans d'autres circuits

Note 1 à l'article: Un circuit TBTP comprend un raccordement à un conducteur de protection. En l'absence de raccordement à un conducteur de protection, ou si une défaillance existe au niveau du raccordement, les tensions ne sont pas corrigées.

[SOURCE: IEC 61010-2-201:2013, 3.109, modifié – suppression de "circuit" dans le terme, et suppression de la seconde note à l'article]

3.1.1.25
redondance
existence de plusieurs moyens pour accomplir une fonction requise ou pour représenter des informations

[SOURCE: IEC 61508-4:2010, 3.4.6, modifié – exemple et notes supprimés]

3.1.1.26
fiabilité
probabilité pour qu'un système automatisé puisse accomplir une fonction requise, dans des conditions données, pendant un intervalle de temps donné (t1, t2)

Note 1 à l'article: 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 à l'article: Le terme "fiabilité" est aussi employé pour désigner l'aptitude caractérisée par cette probabilité.

Note 3 à l'article: Au cours de la période MTBF ou MTTF, la probabilité qu'un système automatisé exécute une fonction exigée dans les conditions données décroît.

Note 4 à l'article: La fiabilité diffère de la disponibilité.

[SOURCE: IEC TR 62059-11:2002, 3.17, modifié – utilisation des mots "un système automatisé" à la place de "une entité" et ajout de deux notes]

3.1.1.27
probabilité d'erreurs résiduelles
RP
probabilité de non-détection d'une erreur par les mesures de sécurité SCL

Note 1 à l'article: L'abréviation «RP» est dérivée du terme anglais développé correspondant «residual error probability».

3.1.1.28
taux d'erreurs résiduelles
taux statistique de défaut de détection d'erreurs par les mesures de sécurité SCL

3.1.1.29
risque
combinaison de la probabilité d'un dommage et de sa gravité

Note 1 à l'article: Pour plus d'informations sur ce concept, voir l'Annexe A de l'IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6, et Guide ISO/IEC 51:2014, définition 3.9, modifié – note différente]

3.1.1.30
canal de communication de sécurité
canal de communication qui débute au sommet de la SCL de la source et qui se termine au sommet de la SCL du collecteur

Note 1 à l'article: Le canal peut être modélisé sous la forme de deux SCL reliées par un canal noir, un système de communication défini ou un canal défini.

3.1.1.31
couche de communication de sécurité
SCL
couche de communication située au-dessus de la FAL qui comprend toutes les mesures supplémentaires nécessaires qui permettent d'assurer la transmission de données en toute sécurité conformément aux exigences de l'IEC 61508

Note 1 à l'article: L'abréviation «SCL» est dérivée du terme anglais développé correspondant «safety communication layer».

3.1.1.32
connexion de sécurité
connexion qui utilise le protocole de sécurité pour des transactions de communications

3.1.1.33
données de sécurité
données transmises par un réseau de sécurité qui utilise un protocole de sécurité

Note 1 à l'article: La couche de communication de sécurité ne garantit pas la sécurité des données proprement dites, mais uniquement la transmission en toute sécurité de ces dernières.

3.1.1.34
appareil de sécurité
appareil conçu conformément à l'IEC 61508 et qui met en œuvre le profil de communication de sécurité fonctionnelle

3.1.1.35
très basse tension de sécurité
TBTS
circuit électrique dans lequel la tension ne peut pas dépasser 30 V eff. c.a., 42,4 V crête ou 60 V c.c. en conditions normales et en conditions de défaut isolé, y compris en conditions de défauts de terre dans d'autres circuits

[SOURCE: IEC 61010-2-201:2013, 3.110, suppression de "circuit" dans le terme, et suppression de la note à l'article]

3.1.1.36
fonction de sécurité
fonction à réaliser par un système E/E/PE relatif à la sécurité ou par un dispositif externe de réduction de risque, prévue pour assurer ou maintenir un état de sécurité de l'EUC par rapport à un événement dangereux spécifique

[SOURCE: IEC 61508-4:2010, 3.5.1, modifié – références et exemples supprimés]

3.1.1.37
temps de réponse de la fonction de sécurité
temps écoulé dans le cas le plus défavorable à la suite de l'activation d'un capteur de sécurité relié à un bus de terrain, avant que ne soit atteint l'état de sécurité correspondant de ses actionneurs de sécurité, du fait d'erreurs ou de défaillances dans la fonction de sécurité

Note 1 à l'article: Ce concept, introduit dans l'IEC 61784-3:—, 5.2.4, est traité dans le cadre des profils de communication de sécurité fonctionnelle définis dans la présente partie.

3.1.1.38
niveau d'intégrité de sécurité
SIL
niveau discret (parmi quatre possibles) correspondant à une gamme de valeurs d'intégrité de sécurité, où le niveau 4 d'intégrité de sécurité possède le plus haut degré d'intégrité et le niveau 1 possède le plus bas

Note 1 à l'article: Les objectifs chiffrés de défaillance (voir l'IEC 61508-4:2010, 3.5.17) pour les quatre niveaux d'intégrité de sécurité sont indiqués dans les Tableaux 2 et 3 de l'IEC 61508-1:2010.

Note 2 à l'article: Les niveaux d'intégrité de sécurité sont utilisés pour spécifier les exigences concernant l'intégrité de sécurité des fonctions de sécurité à allouer aux systèmes E/E/PE relatifs à la sécurité.

Note 3 à l'article: Un niveau d'intégrité de sécurité (SIL) ne constitue pas une propriété d'un système, sous-système, élément ou composant. L'interprétation correcte de l'expression "système relatif à la sécurité à SIL n" (où

n est 1, 2, 3 ou 4) signifie que le système est potentiellement capable de prendre en charge les fonctions de sécurité avec un niveau d'intégrité de sécurité jusqu'à *n*.

Note 4 à l'article: L'abréviation «SIL» est dérivée du terme anglais développé correspondant «safety integrity level».

[SOURCE: IEC 61508-4:2010, 3.5.8, modifié — ajout de la Note 4]

3.1.1.39
mesure de sécurité
mesure permettant de contrôler les *erreurs* de communication éventuelles, qui est conçue et mise en œuvre conformément aux exigences de l'IEC 61508

Note 1 à l'article: Dans la pratique, plusieurs mesures de sécurité sont combinées pour atteindre le niveau d'intégrité de sécurité exigé.

Note 2 à l'article: Les *erreurs* de communication et les mesures de sécurité associées sont détaillées dans l'IEC 61784-3:2010, 5.3 et 5.4.

3.1.1.40
PDU de sécurité
SPDU
PDU transféré via le canal de communication de sécurité

Note 1 à l'article: Le SPDU peut comporter deux exemplaires ou plus des données de sécurité utilisant des structures de codage et des fonctions de hachage différentes, associées à des parties explicites de protections supplémentaires telles qu'une clé, un nombre de séquences ou un mécanisme de datation.

Note 2 à l'article: Les SCL redondantes peuvent fournir deux versions différentes du SPDU en vue de son insertion dans des champs séparés de la trame de bus de terrain.

Note 3 à l'article: L'abréviation «SPDU» est dérivée du terme anglais développé correspondant "safety PDU".

3.1.1.41
application relative à la sécurité
programmes conçus conformément à l'IEC 61508 pour satisfaire aux exigences SIL de l'application

3.1.1.42
système relatif à la sécurité
système qui exécute les *fonctions de sécurité* conformément à l'IEC 61508

3.1.1.43
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

3.1.1.44
déclenchement parasite
déclenchement provoqué par le système de sécurité sans injonction du processus

3.1.1.45
répartition uniforme
loi de probabilité où toutes les valeurs d'un ensemble fini sont susceptibles de se produire

Note 1 à l'article: Pour un champ de longueur binaire i, la probabilité d'occurrence d'une valeur particulière de champ est de 2^{-i} étant donné que la somme de toutes les probabilités d'occurrence est égale à 1.

3.1.2 CPF 3: Termes et définitions supplémentaires

3.1.2.1
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 1 à l'article: Instance d'*authentification de connexion* telle que présentée dans l'IEC 61784-3.

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

Note 1 à l'article: La configuration d'une communication de sécurité comprend la définition des connexions de sécurité et des paramètres F des entités de bus relatives à la sécurité d'une application relative à la sécurité particulière.

3.1.2.4
outil CPD
dans les ordinateurs de service connectés au bus de terrain, programme dédié aux besoins de la configuration, du paramétrage et du diagnostic d'appareils de terrain particuliers

3.1.2.5
cycle
intervalle d'exécution répétitive et continue d'une liste d'instructions ou d'une activité

3.1.2.6
point d'accès à l'appareil
DAP
élément permettant d'adresser un appareil d'entrée-sortie modulaire comme une entité

Note 1 à l'article: En règle générale, il s'agit d'une station de tête

Note 2 à l'article: L'abréviation «DAP» est dérivée du terme anglais développé correspondant «device access point».

3.1.2.7
temps d'acquittement de l'appareil
DAT
dans un appareil F, temps écoulé entre la réception d'un PDU de sécurité avec un nouveau *MonitoringNumber* dans le point d'accès à l'appareil et la génération, puis le renvoi au point d'accès de l'appareil, d'une réponse appropriée de PDU de sécurité

Note 1 à l'article: L'abréviation «DAT» est dérivée du terme anglais développé correspondant «device acknowledgment time».

3.1.2.8
pilote
module logiciel permettant d'analyser le matériel en fonction de l'application logicielle restante

3.1.2.9
à sécurité intégrée
F
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

Note 1 à l'article: Equivalent à sécurité fonctionnelle.

3.1.2.10
valeurs Failsafe
valeurs à sécurité intégrée
FV
valeurs remplaçant des valeurs de processus lorsque la fonction de sécurité est définie sur un état de sécurité intégrée

Note 1 à l'article: Dans la présente partie, les valeurs Failsafe (FV) doivent toujours être définies sur 0.

Note 2 à l'article: L'abréviation «FV» est dérivée du terme anglais développé correspondant «fail-safe values».

3.1.2.11
état de sécurité intégrée
mode opérationnel d'une fonction de sécurité ou d'un élément final (actionneur) qui, après des mesures techniques pertinentes, protège contre les dangers de manière déterministe ou en réduisant le risque à un niveau tolérable

Note 1 à l'article: Selon la fonction de sécurité particulière, la mise hors tension peut ne pas être la seule possibilité caractérisant un état de sécurité intégrée.

3.1.2.12
appareil 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

3.1.2.13
pilote F
logiciel assurant la gestion des PDU de sécurité à l'intérieur des hôtes F et des appareils F conformément aux spécifications FSCP 3/1

3.1.2.14
hôte F
unité de traitement de données permettant d'exécuter le protocole FSCP 3/1 et d'entretenir le canal noir

Note 1 à l'article: En règle générale, il s'agit d'un PLC ou d'un IPC équipé d'un système d'exploitation adéquat.

3.1.2.15
module F
dans un appareil 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 1 à l'article: Il s'agit en général d'un module d'entrée ou de sortie relatif à la sécurité.

3.1.2.16
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

3.1.2.17
réaction aux anomalies
indication d'un dysfonctionnement de communication en définissant les bits erronés dans les octets d'état et une réaction sécurisée automatique correspondante à l'intérieur des composants

Note 1 à l'article:

Dans une sortie F: Arrêt des sorties et/ou réaction sécurisée automatique de l'actionneur.

Dans le CPU F: Réaction possible du programme 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.

3.1.2.18
bloc de fonctions
FB
partie intégrée d'un programme permettant de traiter une fonctionnalité spécifique

Note 1 à l'article: L'abréviation «FB» est dérivée du terme anglais développé correspondant «function block».

3.1.2.19
temps d'acquittement de l'hôte
HAT
dans un hôte F, temps écoulé entre la réception d'un PDU de sécurité avec un certain *MonitoringNumber* et la génération, puis le renvoi au maître/contrôleur d'entrée-sortie, d'un PDU de sécurité approprié équipé d'un *MonitoringNumber* modifié

Note 1 à l'article: L'abréviation «HAT» est dérivée du terme anglais développé correspondant «host acknowledgment time».

3.1.2.20
contrôleur d'entrée-sortie
entité de communication active permettant à d'autres entités (des contrôleurs ou appareils d'entrée-sortie, par exemple) d'initier et de planifier des activités de communication CP 3/RTE

Note 1 à l'article: Dans CP 3/1, cette tâche correspond à une classe maître 1.

Note 2 à l'article: L'interface du contrôleur d'entrée-sortie est appelée FSPMCTL conformément à l'IEC 61158-5-10.

3.1.2.21
appareil 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 appareils d'entrée-sortie, par exemple)

Note 1 à l'article: Dans CP 3/1, cette tâche correspond à un esclave.

Note 2 à l'article: L'interface de l'appareil d'entrée-sortie est appelée FSPMDEV conformément à l'IEC 61158-5-10.

3.1.2.22
module d'entrée-sortie
sous-unité adressable d'entrée-sortie à l'intérieur d'un appareil d'entrée-sortie modulaire

3.1.2.23
superviseur d'entrée-sortie
station d'ingénierie permettant de lire et d'écrire des données sur un appareil d'entrée-sortie

Note 1 à l'article: Il est utilisé pour la mise en service et le diagnostic. À 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.

3.1.2.24
système d'entrée-sortie
contrôleur d'entrée-sortie et ses appareils d'entrée-sortie associés

3.1.2.25
iParamètre
paramètres d'appareil F individuels ou spécifiques à la technologie

Note 1 à l'article: Les coordonnées de la zone de protection d'un lecteur laser sont des iParamètres classiques.

3.1.2.26
serveur d'iParamètres
mécanisme normalisé permettant de stocker et d'extraire des paramètres d'appareil F individuels ou spécifiques à la technologie dans la partie standard d'un hôte F ou de son sous-système contrôlé

3.1.2.27
maître
homologue de communication CP 3/1 actif déclenchant des esclaves pour l'échange de données

Note 1 à l'article: Le terme "maître" est utilisé seul comme forme abrégée de "maître de classe 1".

3.1.2.28
MonitoringNumber
MNR
moyen permettant de garantir l'authenticité et l'ordre correct des PDU de sécurité transmis

Note 1 à l'article: Instance de *nombre de séquences* telle que présentée dans l'IEC 61784-3.

Note 2 à l'article: Le MonitoringNumber est protégé uniquement par la signature de CRC transmise.

Note 3 à l'article: L'abréviation «MNR» est dérivée du terme anglais développé correspondant «MonitoringNumber».

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

Note 1 à l'article: L'abréviation «PV» est dérivée du terme anglais développé correspondant «process values».

3.1.2.30
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 appareils de terrain auxquelles plusieurs contrôleurs peuvent accéder

Note 1 à l'article: 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 le *MonitoringNumber* (virtuel) dans l'hôte F et l'appareil F

3.1.2.33
bus de série universel
USB
norme de bus externe

Note 1 à l'article: USB remplace les ports série et parallèle. Il permet d'assurer une connexion directe et rapide entre les ordinateurs de service et les appareils de terrain.

Note 2 à l'article: L'abréviation «USB» est dérivée du terme anglais développé correspondant «universal serial bus».

3.1.2.34
mode V2
services et protocole FSCP 3/1 conformément à la présente partie

3.1.2.35
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

3.2 Symboles et abréviations

3.2.1 Symboles et abréviations communs

BSC	Binary Symmetric Channel (Canal symétrique binaire)	
CP	Communication profile (Profil de communication)	[IEC 61784-1/2]
CPF	Communication Profile Family (Famille de profils de communication)	[IEC 61784-1/2]
CRC	Contrôle de redondance cyclique	
DLL	Data Link LayerCouche de liaison de données	[ISO/IEC 7498-1]
DLPDU	Data Link Protocol Data Unit (Unité de données de protocole de liaison de données)	
CEM	Compatibilité électromagnétique	
EMI	Electromagnetic interference (Brouillage électromagnétique)	
EUC	Equipment Under Control (Équipement commandé)	[IEC 61508-4:2010]
E/E/PE	Électrique/électronique/électronique programmable	[IEC 61508-4:2010]
FAL	Fieldbus Application Layer (Couche application de bus de terrain)	[IEC 61158-5]
FCS	Frame Check Sequence (Séquence de contrôle de trame)	
FIT	Failure In Time (défaillance dans le temps) (équivaut à 10^{-9} de défaillance par heure)	
FS	Functional Safety (Sécurité fonctionnelle)	
FSCP	Functional Safety Communication Profile (Profil de communication de sécurité fonctionnelle)	
HD	Hamming Distance (Distance de Hamming)	
IACS	Industrial Automation and Control System (Automatisation industrielle et système de commande)	
MTBF	Mean Time Between Failures (Durée moyenne de bon fonctionnement)	
MTTF	Mean Time To Failure (Durée moyenne de fonctionnement avant défaillance)	
NSR	Non Safety Relared (Non relatif à la sécurité)	
PDU	Protocol Data Unit (Unité de données de protocole)	[ISO/IEC 7498-1]
Pe	Bit error probability (Probabilité d'erreurs sur les éléments binaires)	
TBTP	Très basse tension de protection	
PFD	Probability of dangerous Failure on Demand (Probabilité de défaillance dangereuse sur sollicitation)	[IEC 61508-4:2010]
PFH	Fréquence moyenne de défaillance dangereuse [h^{-1}] par heure	[IEC 61508-4:2010]
PhL	Physical Layer (Couche physique)	[ISO/IEC 7498-1]
PL	Performance Level (Niveau de performances)	[ISO 13849-1]
PLC	Programmable Logic Controller (Automate programmable)	
RP	Residual Error Probabilité (Probabilité d'erreurs résiduelles)	
SCL	Safety Communication Layer (Couche de communication de sécurité)	
TBTS	Très basse tension de sécurité	
SFRT	Safety Function Response Time (Temps de réponse de la fonction de	

	sécurité)	
SIL	Safety Integrity Level (Niveau d'intégrité de sécurité)	[IEC 61508-4:2010]
SIS	Safety Instrumented Systems (Systèmes de sécurité instrumentés)	
SL	Security Level (Niveau de sécurité)	[IEC 62443]
SMS	Security Management System (Système de gestion de sécurité)	[IEC 62443]
SPDU	Safety PDU (PDU de sécurité)	
SR	Safety Related (Relatif à la sécurité)	

3.2.2 CPF 3: Symboles et abréviations supplémentaires

AES-CCMP	Advanced Encryption Standard – Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
AP	Application process (Processus d'Application)
API	Application Process Identifier (Identifiant de processus d'application)
AR	Application Relationship (Relation d'application)
ASE	Application Service Element (Élément de service d'application)
ASIC	Application Specific Integrated Circuit (Circuit intégré à application spécifique)
C	Couverture
CGP	Channel-granular Passivation (Passivation granulaire des canaux)
CiR	Configure in Run (Configuration en cours)
CP 3/1	Communication profile (Profil de communication) communément appelé PROFIBUS DP[5]
CP 3/2	Communication profile (Profil de communication) communément appelé PROFIBUS PA
CP 3/RTE	Communication profile (Profil de communication) communément appelé PROFINET IO
CPU	Central Processing Unit (Unité centrale)
CR	Communication Relationship (Relation de communication)
CRC_FP	valeur de départ CRC2 à 16 bits de l'hôte F (du paramètre F = F_Par_CRC)
CRC_FP+	valeur CRC à 32 bits du paramètre F)
DAP	Device Access Point (Point d'accès à l'appareil)
DAT	Device Acknowledgement Time (Temps d'acquittement de l'appareil)
DP	Decentralized Peripherals (Périphériques décentralisés)
F	Identifiant des éléments sécurisés (à sécurité intégrée, sécurité fonctionnelle)
FB	Function Block (Bloc de fonctions)
FV	Fail-safe Values (Valeurs Failsafe)
GSD	General Station Description (Description générale de station) (fichier associé à l'appareil)
GSDL	General Station Description Language (Langage de description générale de station) (pour les appareils CP 3/1 et CP 3/2)
GSDML	General Station Description Markup Language (langage de balisage de description générale de station) (pour les appareils CP 3/RTE
HAT	Host Acknowledgement Time (Temps d'acquittement de l'hôte)
E-S	Entrée-sortie
LED	Light Emitting Diode (Diode Electroluminescente)
MNR	MonitoringNumber
PA	Process Automation (Automatisme industriel)
PN IO	PROFINET IO = CP 3/4 à 3/6 (PROFINET ES)
PSK	Pre-Shared Key (Clé préalablement partagée)
PV	Process Values (Valeurs de processus)

[5] Pour les déclarations d'appellation commerciale, voir l'Article 4.

RADIUS	Remote Authentication Dial In User Service	
S	*Standard*	
SR	(Functional) Safety-Related (Relatif à la sécurité (fonctionnelle))	
SSID	Service Set Identifier (Identifiant d'ensemble de service)	
UML	Unified Modeling Language (Langage de modélisation unifié)	[52]
USB	Universal Serial Bus (Bus de série universel)	[57]
VLAN	Virtual Local Area Network (Réseau local virtuel)	
WCDT	Worst Case Delay Time (Délai du cas le plus défavorable)	
WDTime	Watchdog Time (Temps de fonctionnement du chien de garde)	
WPA2	Wi-Fi Protected Access 2 (Accès Wi-Fi protégé 2)	[29]
XML	eXtensible Markup Language (langage de balisage extensible)	[54], [55], [56]

3.3 Conventions

La présente partie utilise la notation UML2 pour le tracé des diagrammes d'état et une forme condensée de diagrammes séquentiels [52]. Les tableaux de transition sont présentés conformément aux recommandations de l'IEC 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).

Dans la présente partie, 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).

Dans la présente partie, le bit réservé ("res") dans l'octet d'état/contrôle et les paramètres F doivent être nuls et ignorés par le récepteur de manière à éviter toute contrariété avec les versions futures des appareils FSCP 3/1.

Dans la présente partie, le calcul de la signature CRC ayant pour résultat une valeur 0 utilise la valeur 1 à la place.

Dans la présente partie, 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 Présentation générale de FSCP 3/1 (PROFIsafe™)

La famille de profils de communication 3 (communément appelée PROFIBUS™, PROFINET™[6]) définit des profils de communication sur la base du type 3 de l'IEC 61158-2, l'IEC 61158-3-3, l'IEC 61158-4-3, l'IEC 61158-5-3, l'IEC 61158-5-10, l'IEC 61158-6-3 et l'IEC 61158-6-10.

Les profils de base CP 3/1 et CP 3/2 sont définis dans l'IEC 61784-1; CP 3/4, CP 3/5 et CP 3/6 sont définis dans l'IEC 61784-2. Le profil de communication de sécurité fonctionnelle CPF 3 FSCP 3/1 (PROFIsafe™[6]) est basé sur les profils de base de CPF 3 spécifiés dans l'IEC 61784-1 et l'IEC 61784-2, et les spécifications de la couche de communication de sécurité définies dans la présente partie.

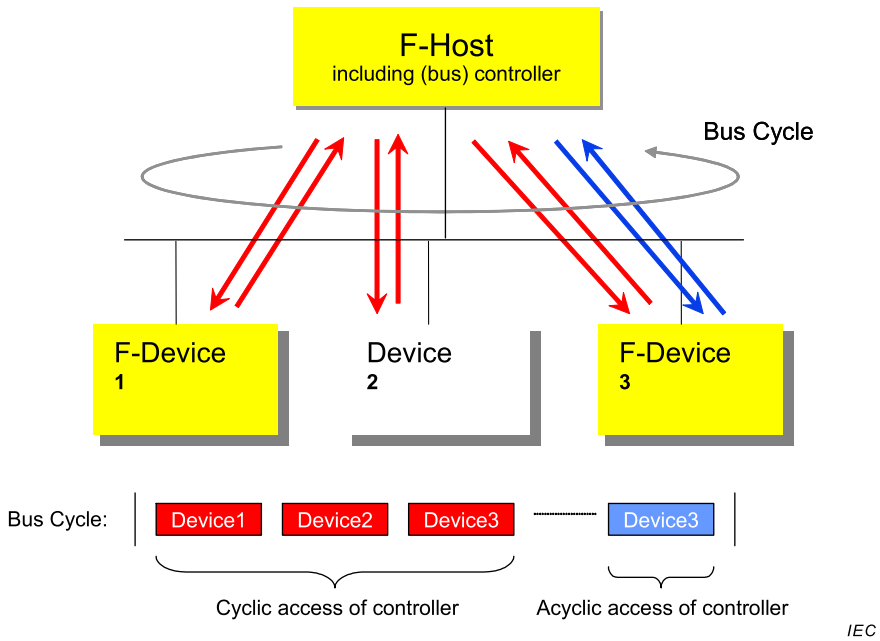
---

6 PROFIBUS™, PROFINET™ et PROFIsafe™ désignent les appellations commerciales de l'organisme sans but lucratif PROFIBUS Nutzerorganisation e.V. (PNO). Ces informations sont données pour des raisons de commodité des utilisateurs de la présente norme internationale et ne constituent en aucun cas un entérinement par l'IEC du titulaire de la marque ou de l'un 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 et la conformité aux conditions d'utilisation (essais et validation).

Le FSCP 3/1 est basé sur l'échange de données cycliques d'un contrôleur (de bus) avec ses appareils (de terrain) associés grâce à une relation de communication un-un (Figure 3). Un contrôleur peut utiliser toute combinaison d'appareils 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 appareils et les contrôleurs ou les superviseurs tels que les appareils 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:

– MonitoringNumber (MNR) (virtuel);
– contrôle du temps de fonctionnement du chien de garde avec acquittement;
– nom de code par relation de communication (le nom de code constitue la base du MNR); La direction est différenciée via l'élément complémentaire unique du MNR);
– contrôle de redondance cyclique pour l'intégrité des données.

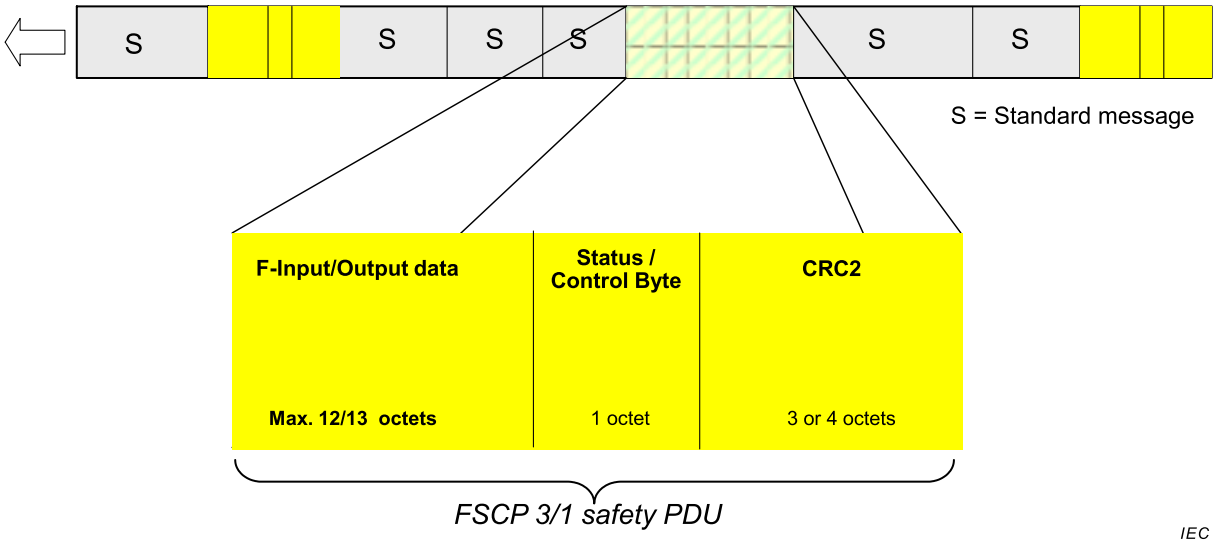


Anglais	Français
F-Host	Hôte F
Including (bus) controller	Y compris le contrôleur (bus)
Bus cycle	Cycle de bus
F-device	Appareil F
Device	Appareil
Cyclic access of controller	Accès cyclique du contrôleur
Acyclic access of controller	Accès acyclique du contrôleur

Figure 3 – Conditions préalables de communication de base pour le protocole FSCP 3/1

Le MonitoringNumber utilise une plage suffisamment grande pour sécuriser tout dysfonctionnement provoqué par les éléments de réseau de stockage des messages. Chaque appareil de sécurité renvoie un message 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 (et par des mesures supplémentaires de la direction source-collecteur) 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 cycliques (Figure 4).

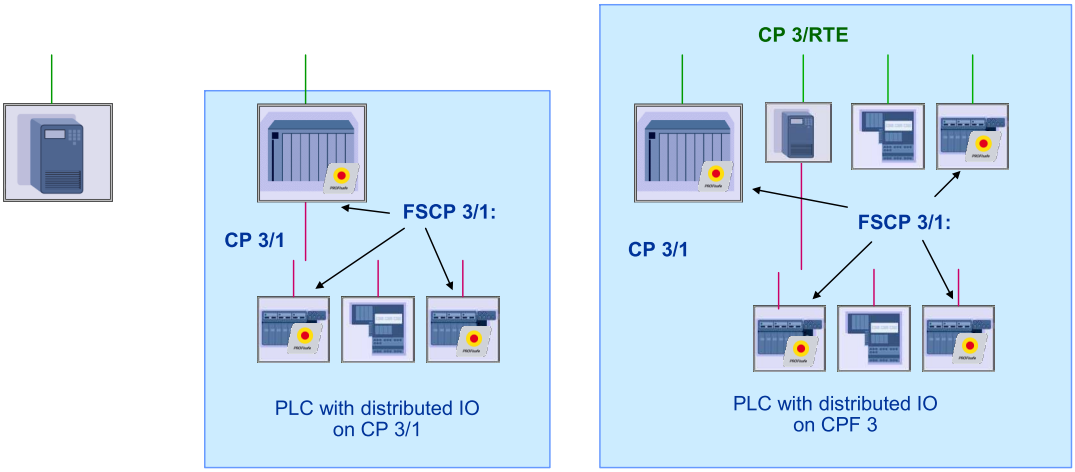


Anglais	Français
S = Standard message	S = Message standard
F-Input/Output data	Données d'entrée/sortie F
Status/Control Byte	Octet d'état/de contrôle
Max. 12/13 octets	12 ou 13 octets max.
3 or 4 octets	3 ou 4 octets
FSCP 3/1 safety PDU	PDU de sécurité FSCP 3/1

Figure 4 –Structure d'un PDU de sécurité FSCP 3/1

Le protocole FSCP 3/1 fournit le mode appelé V2. Le mode V2 spécifié dans la présente version couvre les développements récents des protocoles Ethernet / basé sur CP3/RTE tels que l'acheminement programmable des messages et des constatations scientifiques concernant les propriétés CRC.

La Figure 5 présente FSCP 3/1 dans le cadre d'architectures CP 3/1 et CP 3/RTE.



Anglais	Français
CP 3/4 to CP 3/6	CP 3/4 à CP 3/6
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
Island	Ilot

Figure 5 – Communication de sécurité avec CPF 3

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 comme nécessaire l'utilisation d'appareils de sécurité modernes (les lecteurs laser ou les appareils 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 en 5.5.3. Les paragraphes 6.1 à 6.3 dévoilent les services de l'hôte F et de l'appareil F, ainsi que les messages de diagnostic possibles de la couche de sécurité.

L'Article 7 commence par une présentation du PDU de sécurité (7.1) et se poursuit par une description des diagrammes d'état de l'hôte F et de l'appareil 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 l'IEC 61784-3:-, le paragraphe 7.3 présente les réactions du système en cas d'éventuels dysfonctionnements. D'autres fonctions du système (le démarrage de la couche de sécurité, par exemple) sont présentées en 7.4. La gestion de la couche des appareils de sécurité se concentre sur les paramètres F spécifiques à la communication de sécurité (8.1) et les iParamètres individuels spécifiques à l'appareil (8.2). Les exigences de traitement et de fourniture des paramètres F sont présentées en 8.3. Le paragraphe 8.4 aborde la sécurisation des structures de données

échangées entre les partenaires qui communiquent et entrant dans la configuration d'un appareil. Le paragraphe 8.5 explique comment les informations de structure de données peuvent être utilisées pour configurer les pilotes de canal F d'appareils 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 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 ([41], [70]).

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 satisfait aux exigences du document NE97 [53].

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 appareils standards et les appareils de sécurité doivent être en mesure d'utiliser le même canal de communication.

b) La communication de sécurité doit être conforme au niveau d'intégrité de sécurité SIL3 (voir l'IEC 61508) et au niveau PL e (voir l'ISO 13849-1).

c) La communication de sécurité doit utiliser un système de communication à un seul canal. La redondance peut uniquement être utilisée pour éventuellement augmenter la disponibilité.

d) La mise en œuvre du protocole de transmission de sécurité doit être limitée aux éléments finaux de communication (hôte F ou CPU F – appareil F et/ou module F).

e) La relation de communication entre un appareil 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 l'IEC 61326-3-1 ou l'IEC 61326-3-2 en l'absence de normes de produits particulières).

h) Les équipements de transmission (les contrôleurs, les ASIC, les liaisons, les coupleurs, etc.) ne doivent pas être modifiés (canal noir). Les fonctions de sécurité doivent être au-dessus de la couche OSI 7 (c'est-à-dire le profil, et pas de modifications ni d'améliorations apportées au protocole standard)

i) La communication de sécurité ne doit pas réduire le nombre d'appareils admis. Des restrictions peuvent apparaître pendant le mapping, dans le cas des applications CP 3/2, en raison des limitations de messages (voir CP 3/2 dans l'IEC 61784-1).

j) La communication de sécurité doit être conforme à NE97 [53] et satisfaire aux exigences de l'IEC 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 constituent un composant significatif du profil FSCP 3/1. La sélection dans le Tableau 1 des mesures de sécurité génériques figurant dans l'IEC 61784-3:2010, 5.5, est exigée pour FSCP 3/1.

Les mesures de sécurité doivent être traitées et surveillées dans une unité de sécurité.

Tableau 1 – Mesures déployées pour maîtriser les erreurs

Erreurs de communication	Mesures de sécurité			
	MonitoringNumber (virtuel) [a]	Temporisation avec réception [b]	Nom de code de l'émetteur et du récepteur [c]	Contrôle d'intégrité des données [d]
Corruption				X
Répétition non prévue		X		
Séquence incorrecte	X			
Perte	X	X		
Retard inacceptable		X		
Insertion	X		-	
Déguisement				X
Adressage	X		X	
Hors séquence	X			
Bouclage des messages	X [e]			

[a] Instance de «numéro de séquence» de l'IEC 61784-3.

[b] Instance de «délai» (Temporisation) et de «message de réaction» (Réception) de l'IEC 61784-3.

[c] Instance de «authentification de connexion» de l'IEC 61784-3.

d Instance de «assurance d'intégrité des données» de l'IEC 61784-3.

E En mode F_CRC_seed =0 via le bit d'état 7, en mode F_CRC_seed =1 via l'élément complémentaire unique du MNR

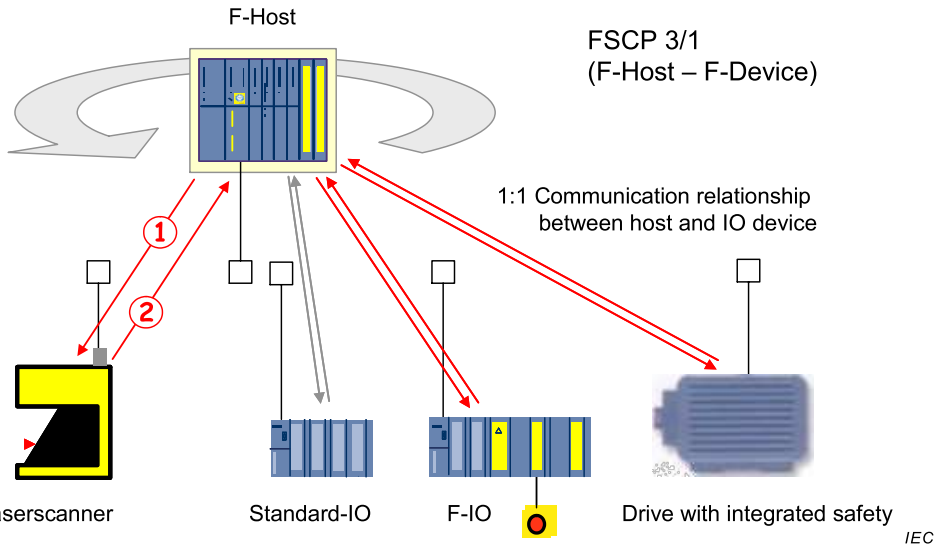
5.4 Structure de la couche de communication de sécurité

5.4.1 Principe des communications de sécurité FSCP 3/1

La communication de sécurité FSCP 3/1 repose sur l'expérience en matière de technique de signalisation ferroviaire, présentée dans les versions antérieures de l'IEC 62280.

Sur cette base, la communication de sécurité est assurée par

- un système de transmission standard (Figure 6), et
- un protocole de transmission de sécurité supplémentaire venant à l'appui de ce système de transmission standard.



Anglais	Français
(F-Host – F-Device)	(Hôte F – Appareil F)
1:1 Communication relationship between host and I/O device	Relation de communication 1:1 entre l'hôte et l'appareil d'entrée-sortie
Laser scanner	Lecteur laser
Standard-I/O	Entrée-sortie standard
F-I/O	Entrée-sortie F
Drive with integrated safety	Pilotage avec sécurité intégrée

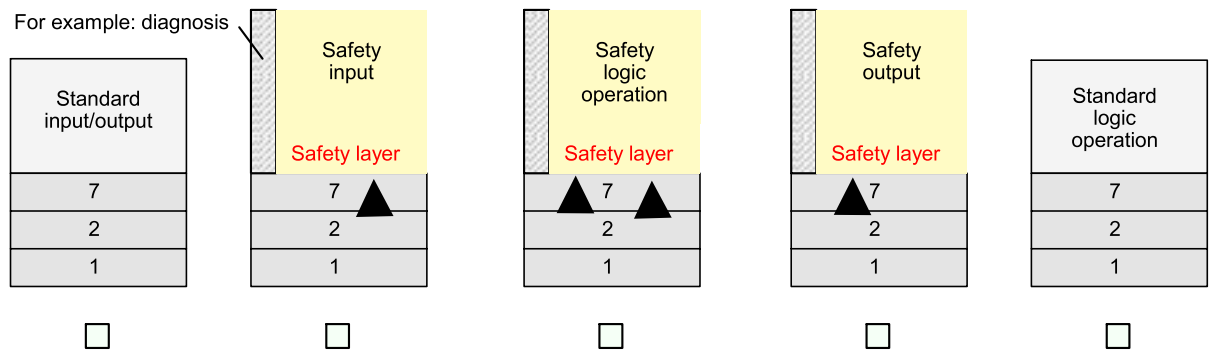
Figure 6 – Système de transmission CPF 3 standard

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 selon 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 anomalies/tous les dangers potentiels que le système de transmission standard est susceptible d'infiltrer, ou de maintien de la probabilité d'erreurs (anomalie) résiduelles sous une certaine limite. Il s'agit

- de dysfonctionnements aléatoires (en raison, par exemple, de l'impact des perturbations électromagnétiques 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 nécessaire de procéder à une évaluation de sécurité supplémentaire du «système de transmission standard» (canal noir).



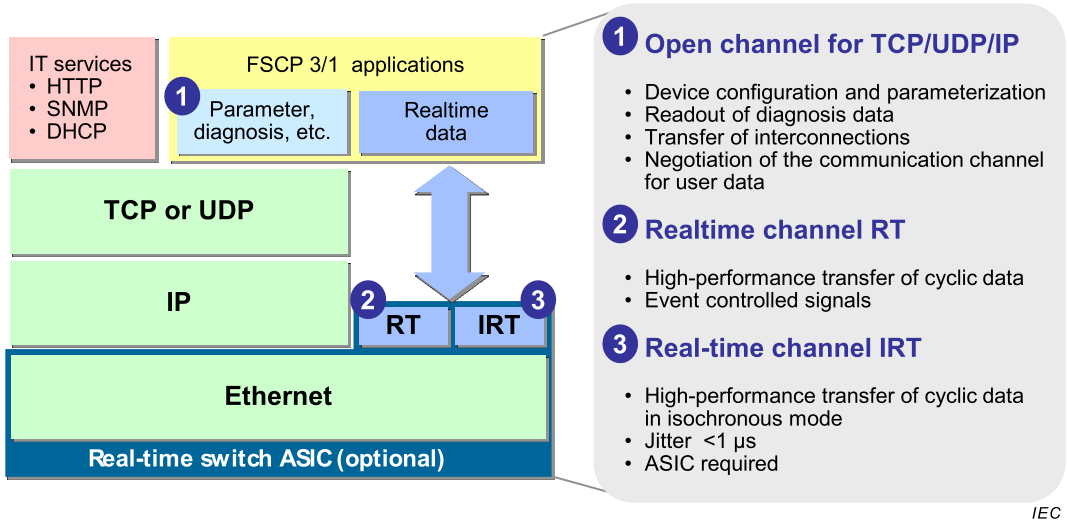
Anglais	Français
For example: diagnosis	Par exemple: diagnostic
Standard input/output	Entrée-sortie standard
Safety input	Entrée de sécurité
Safety layer	Couche de sécurité
Safety logic operation	Opération logique de sécurité
Safety output	Sortie de sécurité
Standard logic operation	Opération logique 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 related functions, e.g. diagnosis	Aucune fonction relative à la sécurité (diagnostic, par exemple)
FSCP 3/1: the safety related protocol comprises: addressing, watch-dog timing, MNR, signatures, etc.	FSCP 3/1: le protocole relatif à la sécurité comprend l'adressage, le temps de fonctionnement du chien de garde, le MNR, 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 relatives à la sécurité, 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 admissibles 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 à 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 l'IEC 61784-2), les autres services utilisent le canal dit ouvert via TCP/IP ou UDP.

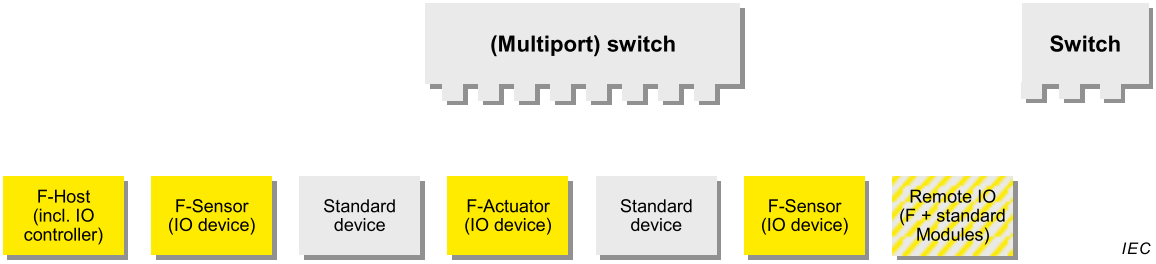


Anglais	Français
IT services	Service IT
FSCP 3/1 applications	Applications FSCO 3/1
Parameter, diagnosis, etc.	Paramètre, diagnostic, etc.
Realtime data	Données en temps réel
Open channel for TCP/UDP/IP	Canal ouvert pour TCP/UDP/IP
Device configuration and parameterization	Configuration et paramétrage de l'appareil
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
TCP or UDP	TCP ou UDP
Real-time switch ASIC (optional)	Switch-ASIC en temps réel (facultatif)
ASIC required	ASIC exigé

Figure 8 – Couches de communication de base

La Figure 9 représente la topologie (en étoile) classique d'un câblage CP 3/RTE possible, avec des commutateurs à plusieurs ports. Si un appareil tombe en panne, tout le système n'est pas arrêté. Toutefois, l'effort de câblage peut ne pas être favorable.

CP 3/RTE propose une variante grâce à Switch-ASIC, que chaque appareil peut intégrer dans son interface de communication. De cette façon, une topologie linéaire s'apparentant à CP 3/1 est possible.

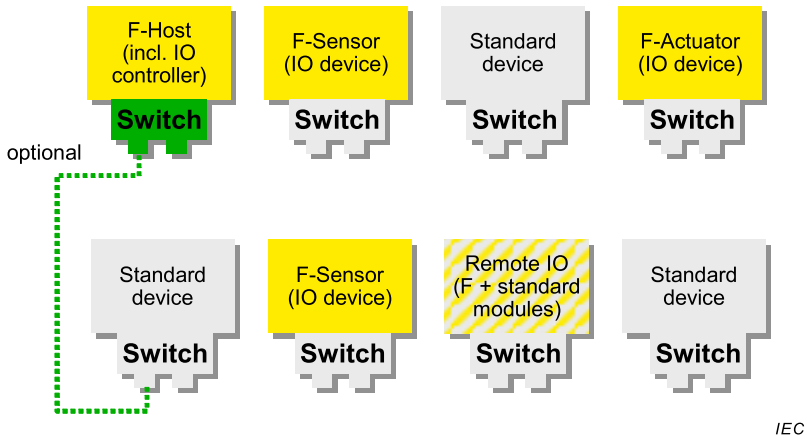


Anglais	Français
(Multiport) switch	Commutateur (à plusieurs ports)
Switch	Commutateur
F-Host (incl. IO controller)	Hôte F (y compris contrôleur d'entrée-sortie)
F-sensor (IO device)	Capteur F (appareil d'entrée-sortie)
Standard device	Appareil standard
F-Actuator (IO device)	Actionneur F (appareil d'entrée-sortie)
Remote IO (F + standard Modules)	Entrée-sortie distante (F + Modules standard)

Figure 9 – Structure de bus de commutateur à plusieurs ports

Pour éviter l'arrêt du système en cas de défaillance d'un appareil, une structure en anneau (voir Figure 10) est vivement recommandée. Toutefois, dans ce cas, il existe certaines restrictions:

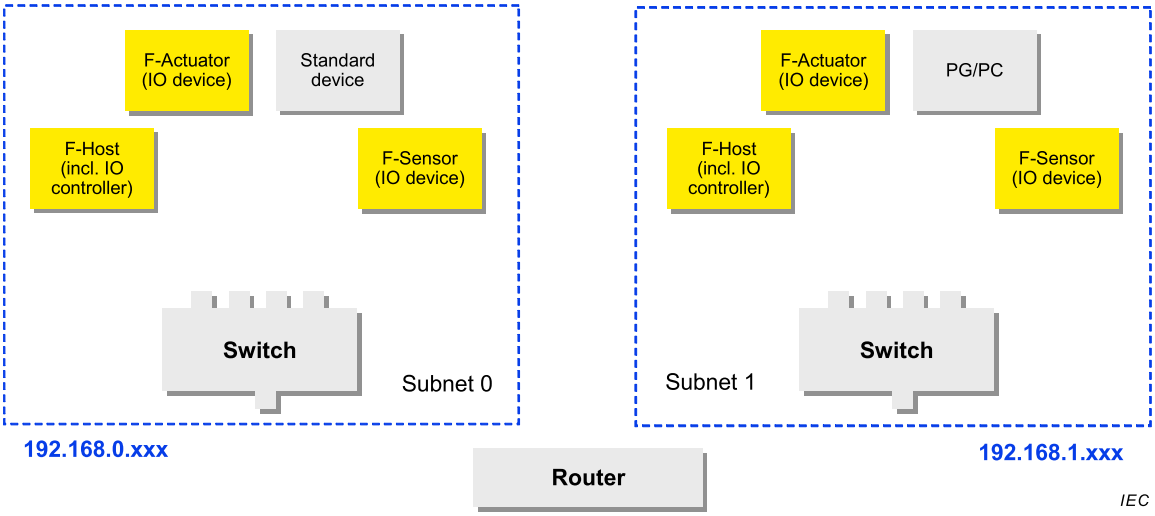
- Au moins un participant de l'anneau (l'hôte F dans la Figure 10) doit disposer d'une fonction de gestion de redondance afin de détecter toutes les interruptions et réorganiser la transmission vers les destinations.
- Dans ce cas, le temps de passage sur canal sémaphore de secours de la gestion du commutateur ne doit pas dépasser le temps minimal de fonctionnement du chien de garde d'un appareil F se trouvant dans le même îlot.



Anglais	Français
Switch	Commutateur
F-Host (incl. IO controller)	Hôte F (y compris contrôleur d'entrée-sortie)
F-sensor (IO device)	Capteur F (appareil d'entrée-sortie)
Standard device	Appareil standard
F-Actuator (IO device)	Actionneur F (appareil 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, car le protocole en temps réel (RT ou IRT) de la couche 2 ne peut pas aller au-delà de cet espace d'adresse IP (voir Figure 8). Il revient aux routeurs (couche OSI 3) de réacheminer les messages vers un niveau d'adresse IP (voir Figure 11). Par conséquent, les routeurs sont les limites naturelles des systèmes CP 3/RTE où RT_CLASS_UDP n'est ni admis ni pris en charge.



Anglais	Français
Switch	Commutateur
F-Host (incl. IO controller)	Hôte F (y compris contrôleur d'entrée-sortie)
F-sensor (IO device)	Capteur F (appareil d'entrée-sortie)
Standard device	Appareil standard
F-Actuator (IO device)	Actionneur F (appareil d'entrée-sortie)
Remote IO (F + standard Modules)	Entrée-sortie distante (F + Modules standard)
optional	facultatif
Subnet	Sous-réseau
Router	Routeur

Figure 11 – Croisement des limites du réseau avec les routeurs

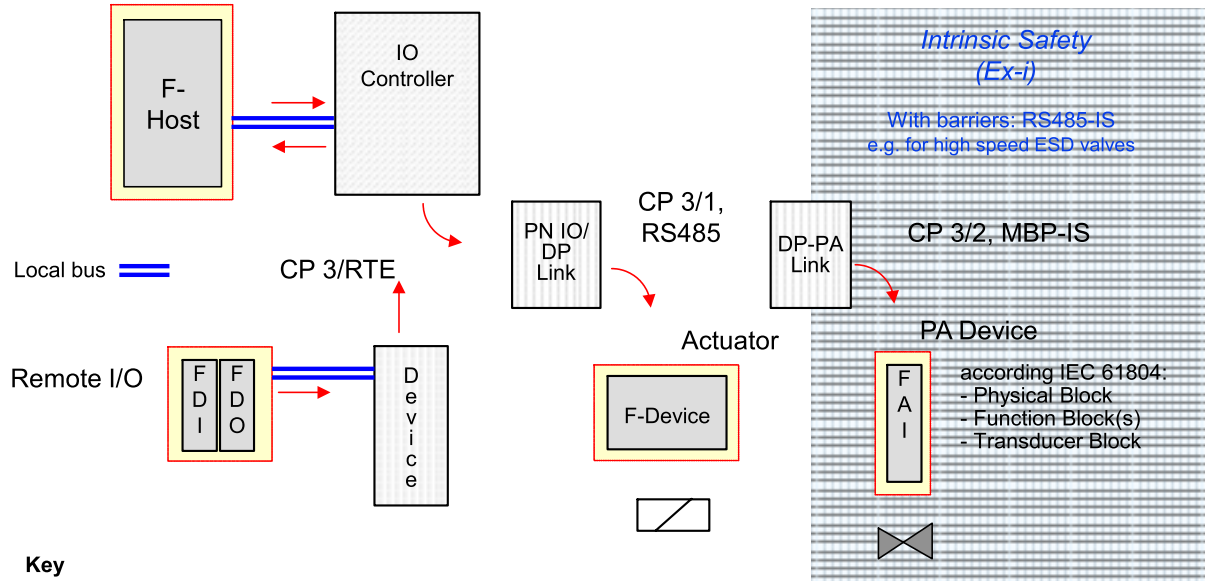
Les restrictions suivantes s'appliquent à FSCP 3/1.

- Réseau local sans fil autorisé. Toutefois, le caractère unique des noms de codes ("F_S/D_Addresses") doit être garanti à l'intérieur des îlots.
- Les routeurs à un seul port ne sont pas admis (7.3.11).

Lorsque des protocoles en temps réel croisent les routeurs, les noms de codes internes à l'ensemble du réseau doivent être exempts de toute ambiguïté et les vérifications du nom de code doivent identifier les relations non ambiguës et par des mesures supplémentaires les deux directions de transmission.

À l'inverse de la configuration d'un système de bus de terrain, la Figure 12 représente la structure de réseau possible, c'est-à-dire la mesure dans laquelle le profil de sécurité s'étend dans les unités individuelles. Par exemple, une entrée-sortie distante standard peut contenir un module F permettant de connecter un bouton d'arrêt d'urgence. Par conséquent, l'ensemble du canal de transmission FSCP 3/1 passe dans l'appareil d'entrée-sortie par le bus de fond de panier de l'hôte F via CP 3/RTE, 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.



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)

IEC

Anglais	Français
F-host	Hôte F
I/O controller	Contrôleur d'entrée-sortie
Intrinsic safety	Sécurité intrinsèque
With barriers	Avec barrières
e.g. for high speed ESD valves	Par exemple, pour soupapes ESD à grande vitesse
Local bus	Bus local
To	A
PN IO/DP link	Liaison PN ES/DP
DP-PA link	Liaison DP-PA
Remote I/O	Entrée-sortie distante
Actuator	Actionneur
Device	Appareil
F-device	Appareil F
PA device	Appareil PA
According IEC 61804	Conformément à l'IEC 61804
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 antidéflagrantes
High speed data transmission	Transmission de données grande vitesse
Special RS485 for explosion-proof areas	RS485 spécial pour zones antidéflagrantes
Safety digital input	Entrée numérique de sécurité
Safety digital output	Sortie numérique de sécurité
Safety analog input	Entrée analogique de sécurité
Device according process automation device model (IEC 61804)	Appareil conforme au modèle d'appareil d'automatisation industriel (IEC 61804)

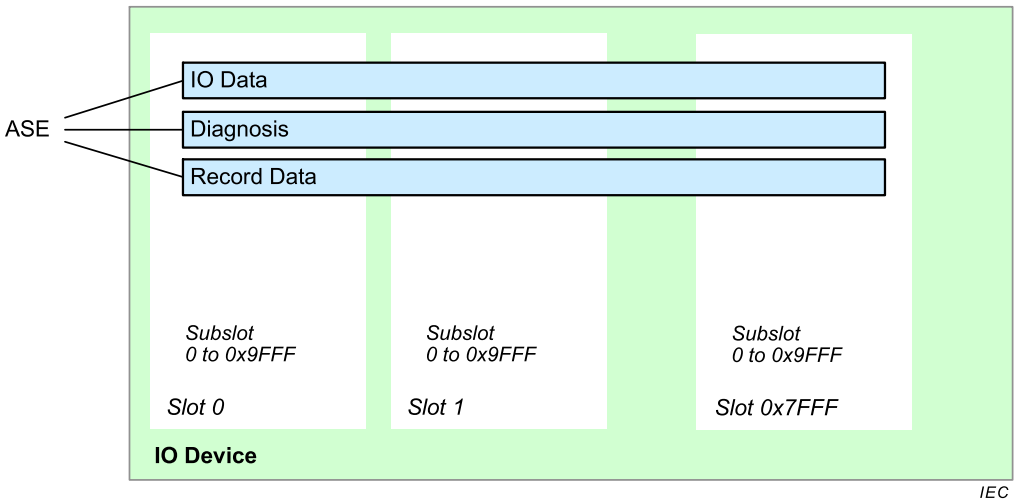
Figure 12 – Voies de transmission de sécurité complètes

5.5 Relations avec la FAL (et DLL, PhL)

5.5.1 Modèle d'appareil

Le CP 3/RTE, ainsi que le modèle d'appareil CP 3/1, considère la présence d'un ou de plusieurs processus d'application (AP) dans l'appareil. La Figure 13 représente la structure interne d'un processus d'application pour un appareil de terrain modulaire. Éventuellement, elle peut comporter plusieurs de ces processus d'application. Le processus d'application est divisé en autant d'intervalles et de sous-intervalles que nécessaire afin de représenter les entrées-sorties physiques de l'appareil. À l'inverse de CP 3/1, CP 3/RTE offre un niveau hiérarchique supplémentaire: les sous-intervalles.

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).



Anglais	Français
IO data	Données d'entrée-sortie
Diagnosis	Diagnostic
Record data	Données d'enregistrement
Subslot	Sous-intervalle
Slot	Intervalle
To	A
IO Device	Appareil ES

Figure 13 – Modèle d'appareil entrée-sortie

Le fabricant de l'appareil est chargé de la spécification (GSD) des modules F qui peuvent être insérés dans des intervalles ou des sous-intervalles.

5.5.2 Relations d'application et de communication

CP 3/RTE permet en général une entrée partagée. Étant donné que FSCP3/1 est basé sur des relations de communication 1:1, l'entrée partagée ne peut pas être utilisée pour la sécurité fonctionnelle.

5.5.3 Types de données

CPF 3 utilise les types de données de base figurant dans l'IEC 61158-5-10. Le Tableau 2 présente un nombre limité de types de données pour FSCP 3/1.

Tableau 2 – Types de données pour FSCP 3/1

Nom du type de données	Nombre d'octets
Integer16	2
Integer32	4
Unsigned8 (utilisé comme bits)	1
Unsigned16 (utilisé comme bits) [a]	2
Unsigned32 (utilisé comme bits) [a]	4
Float32	4
Unsigned8+Unsigned8	2
Float32+Unsigned8 (énuméré)	5
F_MessageTrailer4Byte	4
F_MessageTrailer5Byte	5
[a] Il est fortement recommandé d'utiliser à la place plusieurs Unsigned8	

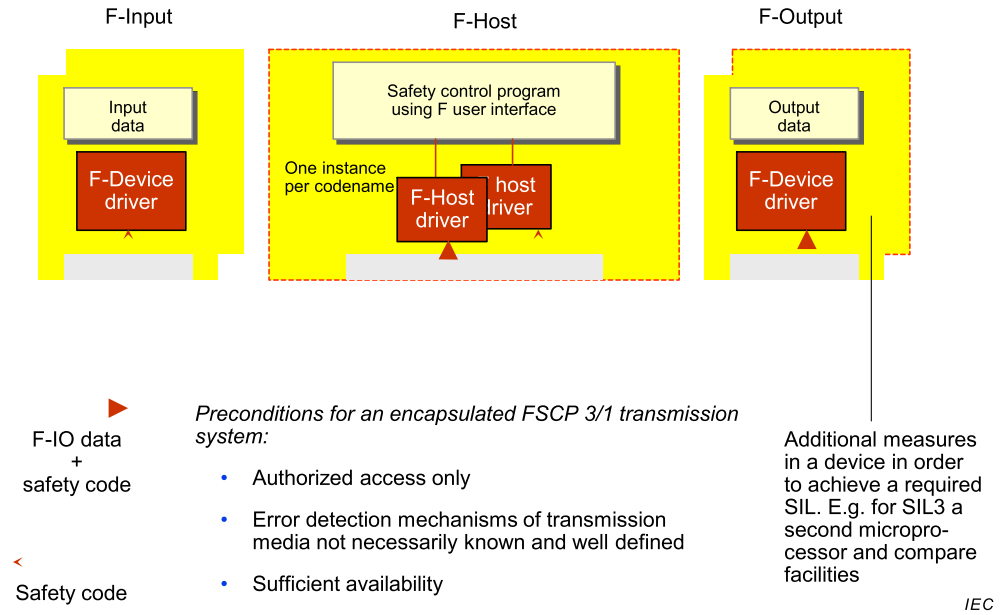
Les bits uniques doivent être codés dans un type de données Unsigned8, en raison de sa plus grande efficacité par comparaison avec le type de données booléen.

Voir [62] pour obtenir des informations générales relatives aux types de données et 8.4.1 pour le codage de sécurité fonctionnelle.

6 Services de la couche de communication de sécurité

6.1 Services de l'hôte F

La Figure 14 indique que chaque entrée et sortie F impliquent une gestion de PDU de sécurité (pilote F) afin de traiter le protocole FSCP 3/1. L'hôte F correspondant fonctionne avec une instance d'un pilote F pour chaque entrée ou sortie F, respectivement. Par conséquent, toutes les relations de type 1:1 entre une instance du pilote F et le partenaire correspondant dans un appareil F sont identifiées par un *Codename* unique (l'un des paramètres F).



Anglais	Français
F-input	Entrée F
F-host	Hôte F
F-output	Sortie F
Input data	Données d'entrée
Safety control program using F user interface	Programme de commande de sécurité utilisant l'interface utilisateur F
Output data	Données de sortie
F-device driver	Pilote de l'appareil 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 connus et bien définis
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 appareil afin d'atteindre un SIL exigé. Par exemple, pour SIL3, un second microprocesseur et des installations de comparaison

Figure 14 – 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 14 indiquent le transport de données cycliques entre les pilotes F: les suppléments de sécurité (Octet d'état ou de contrôle et CRC2) sont transférés de l'entrée F 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.

NOTE Il est possible que les appareils F/modules F fournissent des données de l'entrée et de la sortie F.

La gestion de PDU de sécurité et le paramétrage F sont des tâches des pilotes F à l'intérieur de l'hôte F et des appareils F. Ces tâches fournissent également les mesures venant à l'appui des fonctions de système supplémentaires "Configuration en cours" ("Configure in Run") (CiR) selon [64] et "Passivation granulaire des canaux" ("Channel-granular Passivation" basées sur [66].

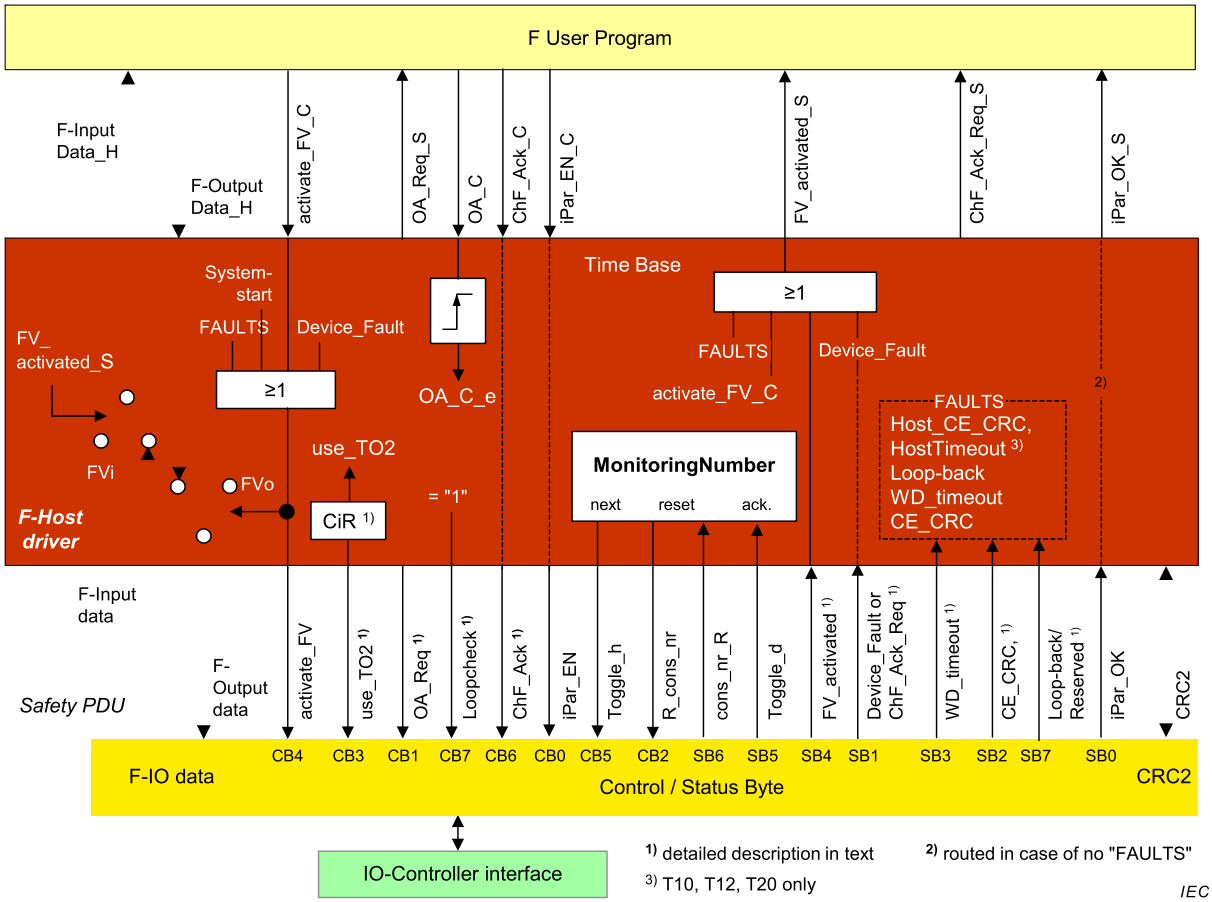
L'interface utilisateur F au niveau du programme de commande de sécurité est présentée à la Figure 15.

"Configuration en cours" (CiR) ou "Maintenance des systèmes de tolérance aux anomalies" ("Maintenance of Fault Tolerant Systems") selon [64] sont des activités planifiées qui doivent être contrôlées par du personnel autorisé uniquement. CiR doit être activée et désactivée uniquement par un opérateur. Elle ne doit pas être définie/réinitialisée via le "Programme utilisateur F"("F User Program").

La conception des parties relatives à la sécurité correspondantes de l'hôte F doit exclure toute activation involontaire de CiR, ainsi qu'assurer la désactivation de cette dernière à l'issue de la reconfiguration.

L'hôte F doit définir et réinitialiser "use_TO2" (CiR) pour tous les appareils F, affectant ainsi simultanément tous ces appareils.

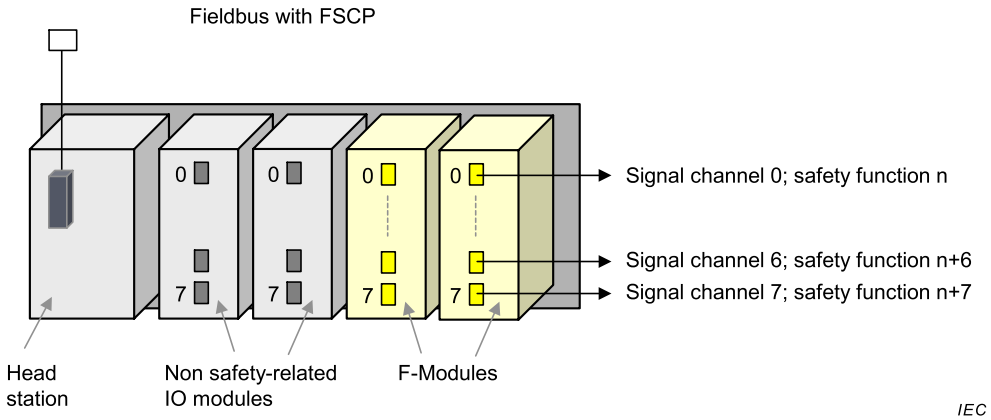
L'hôte F doit prolonger le temps de fonctionnement du chien de garde (principal) régulier (F_WD_Time) par un temps de fonctionnement de chien de garde secondaire (F_WD_Time_2) une seule fois uniquement (voir Figure 20, Figure 28, Figure 29, 7.2.6.2, 8.1.1, 8.1.4).



Anglais	Français
F user program	Programme utilisateur F
F-input	Entrée F
F-output	Sortie F
System start	Démarrage du système
Faults	Anomalies
Time base	Base de temps
F-host driver	Pilote d'hôte F
Next	suivant
Reset	Réinitialisation
Acknowledgement	Acquittement
Loop-back	Bouclage
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 d'anomalies

Figure 15 – Interface utilisateur F des instances du pilote de l'hôte F

Il est possible de constater la nécessité d'une "Passivation granulaire des canaux" en 5.4.2 et à la Figure 12. Le canal de transmission FSCP 3/1 atteint par exemple un module F d'un appareil d'entrée-sortie distant. Habituellement, le module F fournit plusieurs canaux de signalisation, avec un canal pour chaque capteur de sécurité comme présenté à la Figure 16. Chaque canal de signalisation peut être associé à une fonction de sécurité individuelle. En cas de défaillance d'un canal, le module F entraîne l'état de sécurité intégrée de toutes les fonctions de sécurité associées. L'option "Passivation granulaire des canaux" basée sur [66] permet un état de sécurité intégré individuel uniquement pour la fonction de sécurité soumise à l'influence du canal de signalisation défaillant.



Anglais	Français
Fieldbus with FSCP	Bus de terrain avec FSCP
Head station	Station de tête
Non safety-related IO modules	Modules ES non relatifs à la sécurité
F-Modules	Modules F
Signal channel safety function	Canal de signalisation; fonction de sécurité

Figure 16 – Motivation pour l'option "Passivation relative aux canaux" ("Channel-related Passivation")

Le programmeur dispose de plusieurs variables pour manipuler ces 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 63.

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 appareil F correspondant doit définir/réinitialiser cette variable (type: bit). Si la valeur 1 est attribuée à cette variable des appareils d'entrée (des capteurs, par exemple), le pilote fournit des valeurs Failsafe (0) au programme de commande F. Si la valeur 1 est attribuée à cette variable des appareils de sortie (des actionneurs, par exemple), le pilote envoie des valeurs Failsafe (0) à l'appareil et attribue la valeur 1 au bit 4 de l'octet de contrôle. Le concept de sécurité de l'appareil 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 appareil F correspondant doit évaluer cette variable (type: bit). Si la valeur 1 est attribuée à cette variable dans les appareils d'entrée, le pilote fournit des valeurs Failsafe (0) au programme de l'hôte F pour tous les canaux du module F. Voir [66].

Si la valeur 1 est attribuée à cette variable dans les appareils de sortie, des valeurs Failsafe 0 (comportement par défaut) ou une valeur spécifique à l'appareil de sortie F contrôlé par le signal «activate_FV» (= bit 4 de l'octet de contrôle) sont attribuées à tous les canaux du module F. Voir [66].

Cette variable (type: bit) représente le résultat d'un "OR" logique des signaux: Faults, activate_FV_C, FV_activated (SB4), Device_Fault/ ChF_Ack_Req, et Systemstart (implicite).

iPar_EN_C La valeur "1" attribuée à cette variable (type: bit) permet à un programme de commande F de commuter l'appareil 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 40). 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» (cas de mise en œuvre: F-Passivation =0) 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 définir/réinitialiser cette variable (type: bit). Si l'utilisateur attribue la valeur 1 à cette variable, il peut reprendre la fonction de sécurité après une réaction aux anomalies (spécifique à la fonction de sécurité) 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. Dans le cas où le pilote de l'hôte F ou un appareil F détecte une erreur de communication ou une anomalie de l'appareil F (F_Passivation = 0), les valeurs Failsafe sont activées. Ensuite, le pilote de l'appareil F définit la variable OA_Req_S (="1") dès que l'anomalie/l'erreur a été résolue et que l'acquittement de l'opérateur est possible. Après l'acquittement (OA_C = "1"), le pilote de l'appareil F réinitialise la variable de demande OA_Req_S (= "0").

ChF_Ack_C
(Acquittement de l'opérateur de canal) F_Passivation =1 (voir 8.1.6.2): Chaque programme de commande F doit définir/réinitialiser cette variable (type: bit). Si l'utilisateur attribue la valeur 1 à cette variable, il peut reprendre une fonction de sécurité après la correction de toute anomalie de canal de signalisation d'un appareil/module F à l'aide d'un programme utilisateur de l'hôte F. Ce signal peut être omis et représenté en revanche par le signal OA_C.

ChF_Ack_Req_S F_Passivation =1 (voir 8.1.6.2): Cette variable (type: bit) signale une demande d'acquittement en cas de défaillance d'au moins un des canaux d'entrée ou de sortie d'un appareil/module F. Le pilote de l'appareil F définit alors la variable ChF_Ack_Req (= "1") dès l'élimination de l'anomalie/erreur d'au moins un canal d'un appareil/module F. Après

l'acquittement (ChF_Ack = "1"), le pilote de l'appareil F réinitialise la variable de demande ChF_Ack_Req (= "0"). Ce signal peut fait l'objet d'une relation OR logique avec *OA_Req_S* et être présenté comme signal joint *OA_Req_S*.

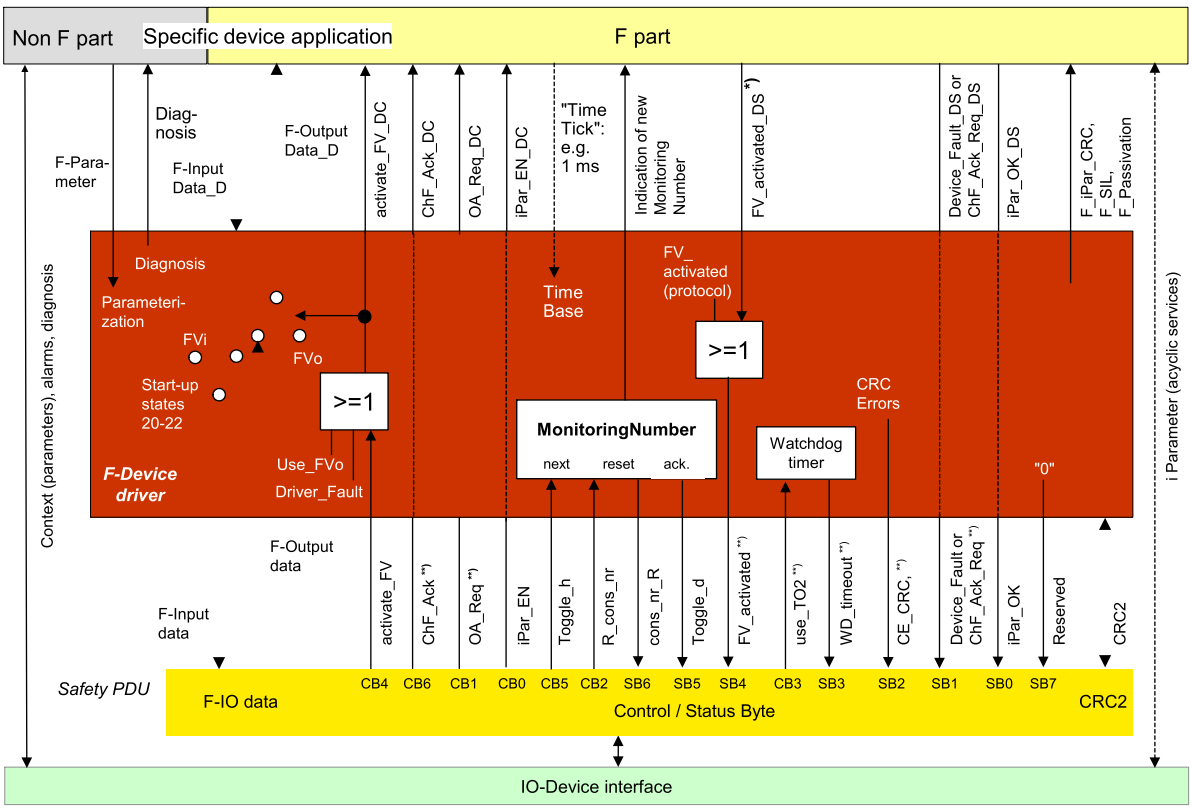
Valeurs d'entrée PVi Valeurs d'entrée de processus (←F-Input_Data_D, voir Figure 17)
FVi Valeurs d'entrée de sécurité intégrée, utilisées à la place de PVi pour F-Input_Data_D (Figure 17).

Valeurs de sortie PVo Valeurs de sortie de 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 de l'appareil F

La Figure 17 représente les caractéristiques du pilote de l'appareil F et son imbrication entre l'interface CP 3/RTE et la partie relative à la sécurité de l'application de l'appareil spécifique. Au cours de la phase de démarrage, la partie non relative à la sécurité de l'application de l'appareil spécifique reçoit les paramètres F et les transmet au pilote de l'appareil F. Le pilote lui-même, après avoir vérifié certains des paramètres F, transmet les paramètres «F_iPar_CRC» et «F_SIL» à la partie relative à la sécurité de l'application de l'appareil spécifique.

En règle générale, l'application de l'appareil spécifique offre une base de temps (1 ms) au pilote de l'appareil F afin d'alimenter les temporisateurs.



Anglais	Français
Non F part	Partie non F
Specific device application	Application d'appareil spécifique

Anglais	Français
F part	Partie F
F-parameter	Paramètre F
Diagnosis	Diagnostic
Indication of new MonitoringNumber	Indication d'un nouveau MonitoringNumber
Parameterization	Paramétrage
Time base	Base de temps
Protocol	Protocole
Start-up states	Le démarrage indique
Next	suivant
Reset	Réinitialisation
Acknowledgement	Acquittement
CRC errors	Erreurs CRC
F-Device driver	Pilote de l'appareil F
Watchdog timer	Temporisateur de chien de garde
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
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
IO-Device interface	Interface de l'appareil ES
Optional	facultatif

Figure 17 – Interfaces du pilote de l'appareil F

Le pilote de l'appareil F traite principalement les PDU de sécurité reçus ou transmis par l'intermédiaire de la relation de communication des données d'entrée-sortie 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 à CB6 (dans le cas où F_CRC_SEED =0: CB7 également). Certains de ces signaux sont transmis à l'interface d'application sans interaction. Un nouveau MonitoringNumber est indiqué afin de faciliter la mise en œuvre des sollicitations avec une durée suffisante (au moins un cycle FSCP 3/1 = deux MonitoringNumbers différents).

En retour, les PDU de sécurité sont préparés pour la transmission. Ils contiennent des octets d'état avec les bits d'état SB0 à SB6. L'un d'eux est transmis, le pilote 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.

Le MonitoringNumber est modifié lorsque l'état de "Toggle_h" change (0→1; 1→0). Le MonitoringNumber est réinitialisé (0) lorsque R_cons_nr = "1". Le MonitoringNumber en cours de modification change l'état de "Toggle_d" (0→1; 1→0). Le contrôle CRC est exécuté avec chaque PDU de sécurité reçu et envoyé (CRC2).

L'application de l'appareil spécifique dispose des variables suivantes. Les variables portent des noms similaires (en principe suivis d'une extension "DC" (contrôle de l'appareil) ou "DS" (état de l'appareil), comme les bits correspondants dans les octets d'état et de contrôle.

activate_FV_DC Cette variable relative à la sécurité indique que les données de sortie F sont des valeurs Failsafe (FV = 0). Elle peut être utilisée pour forcer les sorties d'un appareil F à être des valeurs Failsafe configurées ou intégrées.

FV_activated _DS Si la valeur 1 est attribuée à cette variable dans les appareils d'entrée, l'application de l'appareil fournit des valeurs Failsafe (0) au pilote FSCP 3/1 pour chaque valeur d'entrée. 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 appareils de sortie, des valeurs Failsafe sont attribuées à tous les canaux de sortie. Pour les appareils d'entrée et de sortie combinés, cette variable (type: bit) signale au moyen de la valeur "1" que l'application de l'appareil fournit des valeurs Failsafe (0) au pilote FSCP 3/1 pour tous les canaux d'entrée et de sortie, et que des valeurs Failsafe sont attribuées à chaque canal d'entrée et de sortie.

OA_Req_DC L'application de l'appareil F doit utiliser cette variable non relative à la sécurité pour indiquer localement la demande d'un acquittement de l'opérateur (*OA_C* dans l'hôte F), en général par l'intermédiaire d'une LED. La mise en œuvre est facultative pour les appareils F.

iPar_EN_DC Si la valeur 1 est attribuée à cette variable, cela indique une demande de paramétrage (l'appareil F a besoin de nouveaux iParamètres).

iPar_OK_DS Si la valeur 1 est attribuée à cette variable, de nouvelles valeurs iParamètre sont attribuées à l'appareil F (son application spécifique).

Device_Fault_DS ou *ChF_Ack_Req_DS* F_Passivation =0 (voir 8.1.6.2): Anomalie reconnue par l'application de l'appareil spécifique.
F_Passivation =1 (voir 8.1.6.2): L'anomalie reconnue par tout canal de signalisation d'un appareil/module F via le qualificatif (voir [66]) est corrigée et peut être acquittée.

ChF_Ack_DC F_Passivation =1 (voir 8.1.6.2): Le programme utilisateur de l'hôte F attribue la valeur "1" à cette variable. Cet acquittement confirme la correction de l'anomalie du ou des canaux de signalisation et l'évacuation de la zone de protection par le personnel.

6.3 Diagnostic

6.3.1 Génération d'alarme de sécurité

Compte tenu de la rapidité des cycles d'interrogation du programme 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 de l'appareil F (y compris le serveur d'iParamètres)

Afin de consigner les informations de diagnostic du pilote de l'appareil F FSCP 3/1 dans une interface homme/machine, le pilote les transmet à l'application de l'appareil 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 (Channel-Related-Diagnosis). La table de codage du champ «ChannelErrorType» définie dans l'IEC 61158-6-10 contient une gamme attribuée pour FSCP 3/1.

Le Tableau 3 présente les différents types d'informations de diagnostic de la couche de protocole FSCP 3/1 des appareils 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 ou défaut d'adaptation (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, F_WD_Time_2)
0x0044	68	Le paramètre «F_SIL» dépasse le niveau d'intégrité de sécurité (SIL) de l'application de l'appareil spécifique
0x0045	69	Le paramètre «F_CRC_Length» ne correspond pas aux valeurs générées
0x0046	70	La version de l'ensemble de paramètres F est incorrecte
0x0047	71	Données incohérentes dans le bloc de paramètres F reçu (erreur CRC1)
0x0048	72	Informations de diagnostic spécifique à l'appareil ou non spécifié, voir le manuel
0x0049	73	Temps de fonctionnement du chien de garde iParamètre de sauvegarde dépassé
0x004A	74	Temps de fonctionnement du chien de garde iParamètre de restauration dépassé
0x004B	75	iParamètres incohérents (erreur iParCRC)
0x004C	76	F_Block_ID non pris en charge
0x004D	77	Erreur de transmission: données incohérentes (erreur CRC2)
0x004E	78	Erreur de transmission: temporisation (F_WD_Time ou F_WD_Time_2 écoulé)
0x004F	79	Réservé: ne pas utiliser les numéros, ne pas évaluer les numéros

Les appareils/modules 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.

Les appareils F doivent le cas échéant utiliser ces types dans les messages de diagnostic. Toutefois, les messages de diagnostic peuvent contenir des informations récapitulatives pour plusieurs causes individuelles.

Les erreurs de transmission (codes 77 et 78) ne doivent pas engendrer l'engorgement de messages de diagnostic, par exemple lors de l'attente en premier lieu d'une communication PROFIsafe correcte avant de recevoir de nouveaux messages de diagnostic.

Il convient que le fabricant d'un appareil explique le mapping des causes individuelles avec un message de diagnostic particulier.

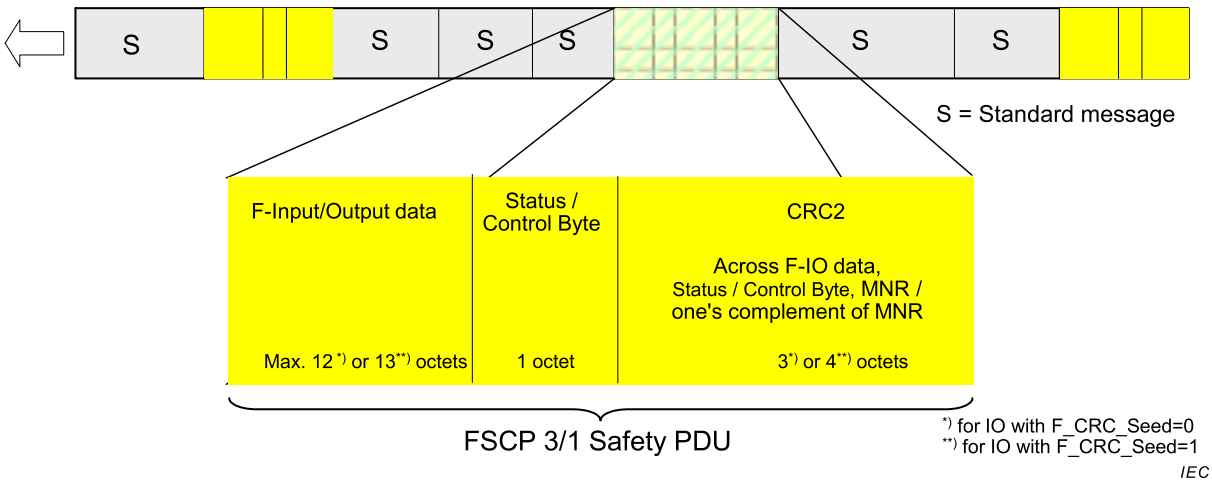
Des informations supplémentaires sont disponibles en [45] et [68].

7 Protocole de couche de communication de sécurité

7.1 Format PDU de sécurité

7.1.1 Structure PDU de sécurité

La Figure 18 représente la structure d'un PDU de sécurité unique 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 d'appareils d'entrée-sortie modulaires pour chaque module F, son propre PDU de sécurité, par exemple).



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-I/O data, Satus / Control Byte, MNR / one's complement of MNR	Parmi les données d'entrée-sortie F, octet de contrôle / d'état, MNR / élément complémentaire unique du MNR
Max. 12 or 13 octets	12 ou 13 octets maximum
3 or 4 octets	3 ou 4 octets
FSCP 3/1 safety PDU	PDU de sécurité FSCP 3/1
For IO with	Pour ES avec

Figure 18 – PDU de sécurité pour CPF 3

Outre les données d'entrée-sortie F (la Figure 18 indique le nombre minimal de données d'entrée-sortie F qu'un Hôte F doit prendre en charge), 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 7.1.9 donnent une description détaillée des éléments de la structure du PDU de sécurité.

7.1.2 Données d'entrée-sortie de sécurité

Les données d'entrée-sortie F des périphériques d'entrée-sortie F sont présentées dans cette section du PDU de sécurité. Le codage de type de données correspond à celui de CP 3/RTE et est défini dans l'ensemble du système dans l'IEC 61158-5-10. Le paragraphe 8.5.2 recommande et spécifie les types et structures de données normalisés pour plusieurs familles d'appareils de sécurité tels que les appareils d'entrée-sortie distants, rideaux de lumière, lecteurs laser, entraînements, etc.

Outre les appareils compacts, il existe des *appareils modulaires* avec des unités d'entrée-sortie et des sous-adresses standard (Figure 13). 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.

7.1.3 Octet d'état et de contrôle

Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
Res («0»)	Monitoring Number a été réinitialisé	Bit de basculement	Valeurs Failsafe (FV) activées	Défaut de communication: WD-timeout	Défaut de communication: CRC	Défaillance de l'appareil F ou du module F, ou défaillance du canal de module corrigée	De nouvelles valeurs iParamètre ont été attribuées à l'appareil F
-	cons_nr_R	Toggle_d	FV_activated	WD_timeout	CE_CRC	Device_Fault/ ChF_Ack_Req	iPar_OK

Figure 19 – Octet d'état

L'octet d'état présenté à la Figure 19 est présent dans chaque PDU de sécurité d'un sous-module CP 3/RTE transmis d'un appareil à son contrôleur (Figure 18).

– Le bit 0 est défini lorsque de nouvelles valeurs de paramètre sont attribuées à l'appareil F (son microprogramme technologique). Le nom de signal est iPar_OK.

– Le bit 1 avec F_Passivation = 0 doit être défini par le microprogramme technologique spécifique de l'appareil pour au moins deux (2) changements du MonitoringNumber, si un appareil/module F n'est pas capable de garantir la sécurité des données de processus à transmettre. Le nom de signal dans ce cas de mise en œuvre est "Device_Fault".

– Le bit 1 avec F_Passivation = 1 doit être défini par le microprogramme technologique spécifique de l'appareil si au moins un des canaux d'un appareil/module F est défini sur des valeurs Failsafe (FV) du fait de l'anomalie d'un canal de signalisation et si cette anomalie est éliminée (corrigée). Les contraintes de durée pour ce signal ne sont pas nécessaires. Une défaillance de l'appareil/module F (et non d'un seul canal) doit entraîner la commutation de tous les canaux sur l'état de sécurité intégrée et de tous les qualificatifs sur l'état "erreur". Le nom de signal dans ce cas de mise en œuvre est "ChF_Ack_Req". Voir [66].

– Le bit 2 est défini si l'appareil F reconnaît un défaut de communication F, c'est-à-dire si le MonitoringNumber est incorrect (détecté par une erreur CRC2) ou en cas de transgression de l'intégrité des données (erreur CRC). Ces informations binaires permettent à l'hôte F de dénombrer tous les messages erronés dans une période T définie et de déclencher un état de sécurité configuré du système si ce nombre dépasse une certaine limite (taux d'erreurs résiduelles maximal). Le nom de signal est CE_CRC. Voir également 9.5.1.

– Le bit 3 est défini si l'appareil F reconnaît un défaut de communication F, c'est-à-dire si le temps de fonctionnement du chien de garde de l'appareil F est dépassé. Le nom de signal est WD_timeout.

– Le bit 4 est défini par la couche de protocole FSCP 3/1 au démarrage et en cas d'erreur de communication (Figure 17 et 7.2). De plus, la partie F de l'application d'appareil spécifique peut également définir ce bit. Le nom de signal est FV_activated.

– Le bit 5 est un bit de basculement basé sur l'appareil indiquant le déclenchement de changement du MonitoringNumber virtuel dans l'hôte F. Le nom de signal est Toggle_d.

– Le bit 6 est défini lorsque l'appareil F a réinitialisé son MNR. Le nom de signal est "cons_nr_R" (issu de "consecutive number reset") ("nombre de réinitialisations consécutives").

– Le bit 7 est réservé (res) aux versions ultérieures de FSCP 3/1 et ainsi, par défaut, il doit être défini sur "0" afin de garantir un état défini pour une utilisation future et pour la "vérification de bouclage" ("Loop-back check) (voir 3.3).

Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
Réservé. ou vérification de bouclage ("1")	Acquittement de l'opérateur après correction de l'anomalie de canal	Bit de basculement	Valeurs Failsafe (FV) à activer	Utilisation de F_WD_Time_2 (chien de garde secondaire)	Réinitialisation de MonitoringNumber	Acquittement de l'opérateur demandé (indication)	Attribution d'iParamètre débloquée
Loopcheck	ChF_Ack	Toggle_h	activate_FV	Use_TO2	R_cons_nr	OA_Req	iPar_EN

Figure 20 – Octet de contrôle

L'octet de contrôle présenté à la Figure 20 est transmis du contrôleur d'entrée-sortie à l'appareil avec chaque PDU de sécurité d'un sous-intervalle (Figure 18).

– Le bit 0 est défini par l'application F dans un hôte F en cas de demande de paramétrage (l'appareil 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 l'appareil F l'utilise pour indiquer localement la demande d'acquittement d'un opérateur (OA_C), en général *par l'intermédiaire d'une LED* (9.1). Le nom de signal est OA_Req.

– Le bit 2 est défini lorsque l'hôte F détecte une erreur de communication, soit par l'octet d'état soit par lui-même. En conséquence, le MonitoringNumber virtuel de l'appareil F est réinitialisé (voir "RESETxD" en 7.1.5 et 7.1.6). Le bit 2 doit être réinitialisé après une erreur. Par la suite, le MNR reprend. Le nom de signal est "R_cons_nr" (issu de "Reset consecutive number") (Nombre de réinitialisations consécutives).

– Le bit 3 est défini lorsque le pilote de l'hôte F est informé, via l'entrée CiR (Figure 15), 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 d'un système de tolérance aux anomalies". Ceci indique à l'appareil F de prolonger le temps de fonctionnement du chien de garde F_WD_Time une seule fois uniquement par l'intermédiaire de F_WD_Time_2 (voir 6.1). Le nom de signal est "Use_TO2".

– Le bit 4 peut être utilisé pour forcer les sorties d'un appareil 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 changement du MonitoringNumber virtuel dans l'appareil F. Voir 7.1.4 pour plus de détails. Le nom de signal est Toggle_h.

– Le bit 6 est défini par l'application F dans un programme utilisateur de l'hôte F après correction d'au moins une anomalie de canal de signalisation d'un appareil/module F indiquée par le bit 1 (ChF_Ack_Req) de l'octet d'état et après que le personnel a quitté la zone de protection. Les PV sont activés. Voir [66]. Le nom de signal est "ChF_Ack".

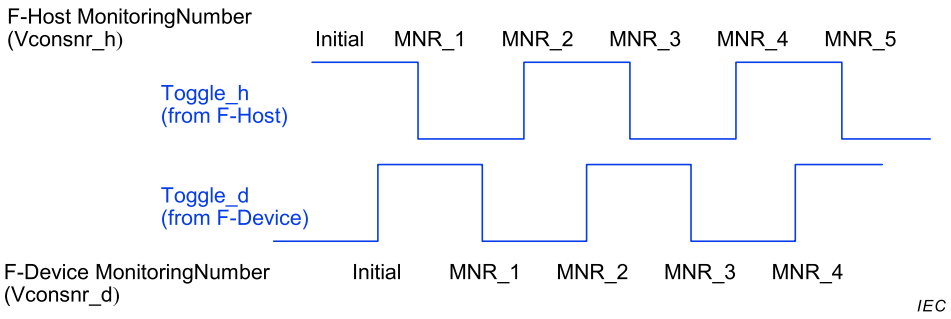
– Le bit 7 est défini sur "1" pour tous les appareils F/modules F dont les mises en œuvre sont conformes aux versions FSCP 3/1 antérieures à cette version (F_CRC_Seed =0). Dans la mesure où ces appareils F/modules F renvoient toujours les octets d'état avec Bit 7 = "0", un bouclage potentiel de messages peut être détecté par le pilote de l'hôte F si ce Bit 7 renvoie "1". Le nom de signal est "Loopcheck".

– Le bit 7 est défini sur "0" pour tous les appareils F/modules F avec une entrée GSD F_CRC_Seed =1 et réservés pour une utilisation future.

7.1.4 MonitoringNumber (Virtuel)

Le destinataire utilise le MonitoringNumber (MNR) pour s'assurer que l'émetteur et le canal de communication sont toujours actifs. Le MNR est utilisé dans un mécanisme d'acquittement pour surveiller les *temps de propagation* entre l'émetteur et le destinataire.

FSCP 3/1 ne transmet pas le MNR avec tous les PDU de sécurité. Il utilise un MNR virtuel à la place. Il est dit «virtuel» car il est invisible dans le PDU de sécurité. Cette approche s'appuie sur des MonitoringNumbers situés dans l'hôte F et l'appareil F, un bit de basculement de l'octet d'état et de l'octet de contrôle changeant le MNR approprié de manière synchrone (Figure 21).



Anglais	Français
F host	Hôte F
From F-host	De l'hôte F
From F-device	De l'appareil F
F device	Appareil F

Figure 21 – Fonction du bit de basculement

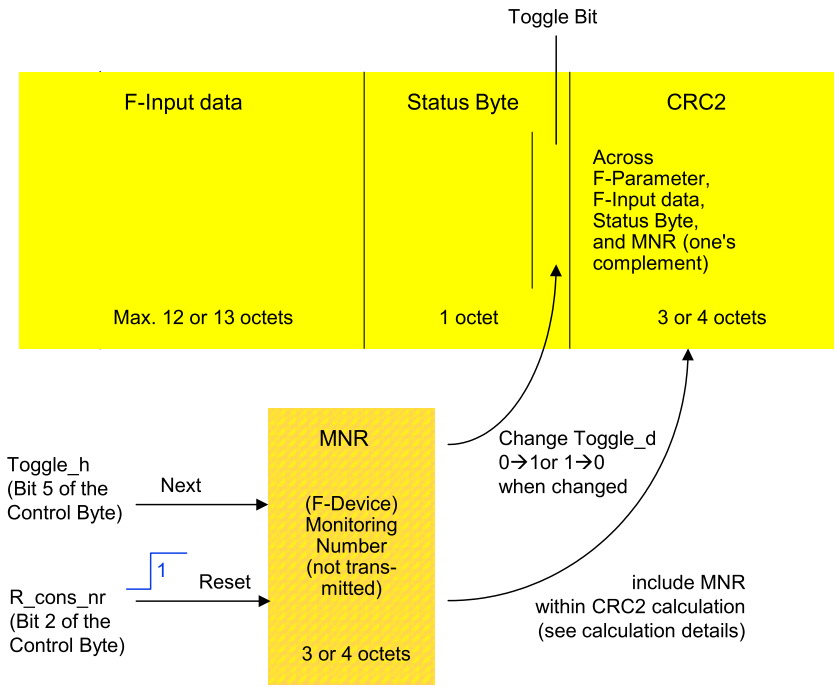
L'exactitude et la synchronisation des deux MNR indépendants sont vérifiées en intégrant les MonitoringNumbers dans le calcul CRC2. CRC2 est ensuite transmis avec tous les PDU de sécurité (Figure 22).

La partie transmise du MonitoringNumber (virtuel) est réduite à un bit de basculement, qui indique un changement du MNR local. Les MNR internes à l'hôte F et à l'appareil F sont modifiés à chaque extrémité des bits de basculement (0→1, 1→0).

La Figure 22 représente le mécanisme du MNR dans l'appareil F. Le MNR est réinitialisé lorsque l'hôte F envoie R_cons_nr = "1" dans l'octet de contrôle (voir 7.1.3).

Le mécanisme du MNR dans l'hôte F correspond à celui de l'appareil F. Toutefois, le MNR est réinitialisé à chaque fois qu'une anomalie se produit (en interne ou par l'octet d'état).

Le nom de ce mécanisme est "MNR" bien que deux procédures différentes sélectionnées par le paramètre F_CRC_Seed soient possibles.



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 MNR (one's complement)	Parmi paramètre F, données d'entrée F, octet d'état et MNR (élément complémentaire unique)
Max. 12 or 13 octets	12 ou 13 octets maximum
3 or 4 octets	3 ou 4 octets
Bit 5 of the Control Byte	Bit 5 de l'octet de contrôle
Next	Suivant
F-device	Appareil F
Monitoring Number (not transmitted)	Monitoring Number (non transmis)
Change Toggle_d 0-1 or 1-0 when changed	Faire passer Toggle_d 0-1 ou 1-0 lorsque modifié
Bit 2 of the Control Byte	Bit 2 de l'octet de contrôle
Reset	Réinitialisation
Include MNR within CRC2 calculation(see calculation details)	Inclure MNR dans le calcul de CRC2 (voir les détails du calcul)

Figure 22 – MonitoringNumber de l'appareil F

7.1.5 Mécanisme du MNR (virtuel)(F_CRC_Seed=0)

FSCP 3/1 utilise dans ce cas des *compteurs 24 bits* pour le MonitoringNumber. Ainsi, dans un mode cyclique, le MonitoringNumber part de 1 à 0xFFFFFF, revenant à 1 à la fin (voir Tableau 4 et Tableau 5). La valeur de compteur est représentée par MNR.

Tableau 4 – MonitoringNumber du PDU d'un hôte F

MACRO	ACTION (Pseudo code)
INITIALxH	old_MNR = 0xFFFFF0; MNR=0xFFFFF0;
RESETxH	R_cons_nr =1; MNR=0;
RUNxH	R_cons_nr =0, old_MNR = MNR; **si** MNR=0xFFFFFF **alors** MNR=1, **sinon** MNR= MNR +1;

Tableau 5 – MonitoringNumber du PDU d'un appareil F

MACRO	ACTION (Pseudo code)
INITIALxD	MNR=0xFFFFF0;
RESETxD	cons_nr_R =1; MNR=0;
RUNxD	cons_nr_R =0 **si** MNR=0xFFFFFF **alors** MNR=1, **sinon** MNR= MNR +1;

7.1.6 Mécanisme du MNR (virtuel)(F_CRC_Seed=1)

FSCP 3/1 fournit une procédure étendue activée par l'intermédiaire de l'entrée GSD "F_CRC_Seed" =1 (voir 8.1.5.2). Il permet la compatibilité avec l'IEC 65C/747/CD:2013, plus particulièrement avec le modèle par défaut d'une transmission implicite.

Cette procédure répartit l'utilisation de MonitoringNumber en deux phases. La première phase est caractérisée comme démarrage du système (system start) (INITIALx) ou en cas d'anomalie et tant que le bit 2 (R_cons_nr) dans l'octet de contrôle est défini sur "1" (RESETx). La deuxième phase est caractérisée comme communication cyclique. "CRC_FP+" est la signature CRC 32 bits (*0xF4ACFB13*) qui inclut les mêmes paramètres F que "CRC_FP" (voir Tableau 6 et Tableau 7).

Tableau 6 – MonitoringNumber du PDU d'un hôte F

MACRO	ACTION (Pseudo code)
INITIALxH	old_MNR = CRC_FP+; MNR=CRC_FP+; CRC2 = CRC2 (calculé selon 7.1.8) XOR Modifier; CN_incrNR_64 [1] = 0x5851F42D4C957F2D * Codename; SwapHL = shl (CN_incrNR_64 [1], 32) + shr (CN_incrNR_64 [1], 32); CN_incrNR_64 [2] = 0xAB16D2792302FE5A * (SwapHL + Modifier) +1;
RESETxH	R_cons_nr =1; MNR=CRC_FP+; CRC2 = CRC2 (calculé selon 7.1.8) XOR Modifier; CN_incrNR_64 [1] = 0x5851F42D4C957F2D * Codename; SwapHL = shl (CN_incrNR_64 [1], 32) + shr (CN_incrNR_64 [1], 32); CN_incrNR_64 [2] = 0xAB16D2792302FE5A * (SwapHL + Modifier) +1;
RUNxH	R_cons_nr =0; old_MNR = MNR; CN_incrNR_64 [0] = CN_incrNR_64 [1] + CN_incrNR_64 [2]; CN_incrNR_64 [2] = CN_incrNR_64 [1]; CN_incrNR_64 [1] = CN_incrNR_64 [0]; MNR= valeur significative 32 bits de CN_incrNR_64 [0];

Tableau 7 – MonitoringNumber du PDU d'un appareil F

MACRO	ACTION (Pseudo code)
INITIALxD	MNR = élément complémentaire unique de CRC_FP+; CN_incrNR_64 [1] = 0x5851F42D4C957F2D * Codename; SwapHL = shl (CN_incrNR_64 [1], 32) + shr (CN_incrNR_64 [1], 32); Modifier = reçu CRC2 XOR calculé CRC2 selon 7.1.8; pas de vérification CRC2 à l'état 22; CN_incrNR_64 [2] = 0xAB16D2792302FE5A * (SwapHL + Modifier) +1;
RESETxD	cons_nr_R =1; MNR= élément complémentaire unique de CRC_FP+; CN_incrNR_64 [1] = 0x5851F42D4C957F2D * Codename; SwapHL = shl (CN_incrNR_64 [1], 32) + shr (CN_incrNR_64 [1], 32); Modifier = reçu CRC2 XOR calculé CRC2 selon 7.1.8; pas de vérification CRC2 aux états 22, 25, et 28; CN_incrNR_64 [2] = 0xAB16D2792302FE5A * (SwapHL + Modifier) +1;

RUNxD	cons_nr_R =0;
	old_MNR = MNR;
	CN_incrNR_64 [0] = CN_incrNR_64 [1] + CN_incrNR_64 [2];
	CN_incrNR_64 [2] = CN_incrNR_64 [1];
	CN_incrNR_64 [1] = CN_incrNR_64 [0];
	
	MNR= "élément complémentaire unique" d'une valeur significative 32 bits de CN_incrNR_64 [0];

L'instruction shl (x,n) est un décalage à gauche de la valeur x du bit n logique, l'instruction shr (x,n) est un décalage à droite de la valeur x du bit n logique.

CN_incrNR_64 [0], CN_incrNR_64 [1], CN_incrNR_64 [2] et SwapHL sont des variables unsigned 64 bits. CRC_FP+, CRC2 et Modifier sont des variables unsigned 32 bits.

Modifier est une valeur générée par l'hôte F pour utilisation ultérieure, qui détermine une nouvelle initialisation. Lorsque les macros de l'appareil F, INITIALxD et/ou RESETxD, sont exécutées plusieurs fois, elles ne peuvent pas être censées comporter la même valeur. Cependant, dans la présente édition, la valeur "0" est toujours utilisée dans les macros de l'hôte F, INITIALxH et RESETxH.

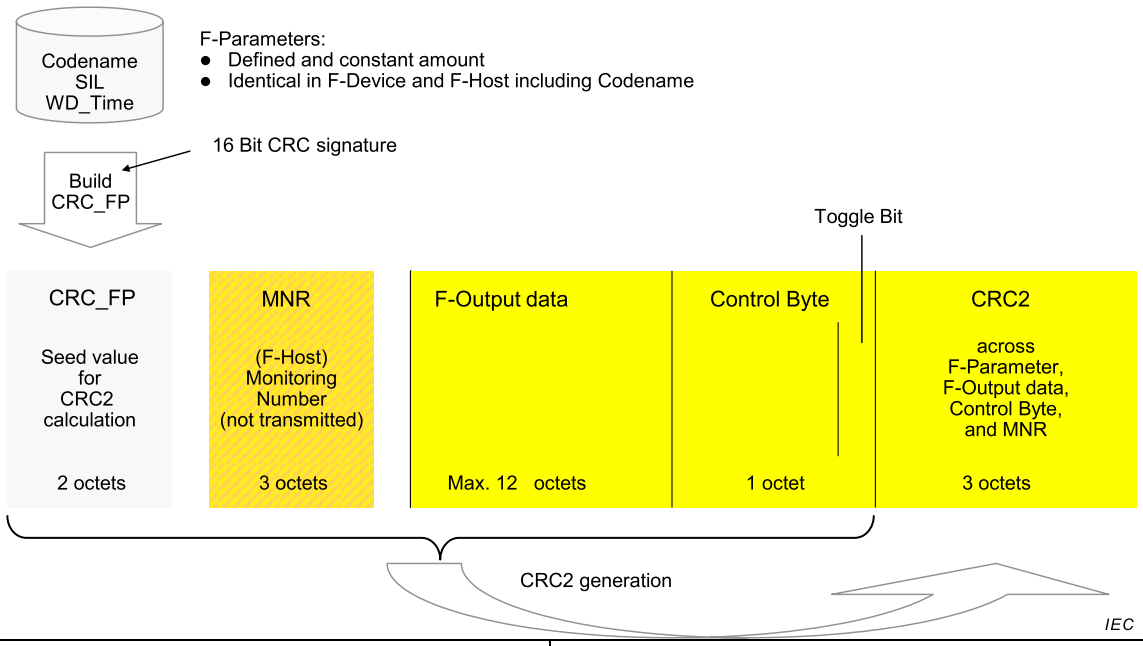
Un exemple des 5 premières valeurs des MonitoringNumbers est présenté dans le Tableau A.4. Le MonitoringNumber est une valeur 32 bits. L' "élément complémentaire unique" ("one's complement") sert à différencier les PDU de sécurité de l'hôte F des PDU de sécurité de l'appareil F afin de détecter une erreur de bouclage.

Pour le nom de code, voir 8.1.2.

7.1.7 Signature CRC2 (F_CRC_Seed=0)

Dans le cas où F_CRC_Seed = 0, les principes suivants s'appliquent: Une fois les paramètres F (relation source-destination ou nom de code, SIL, temps de fonctionnement du chien de garde, etc.) transmis à l'appareil F, les paramètres identiques sont utilisés dans une procédure identique dans l'hôte F et l'appareil F/module F pour produire une signature CRC_FP en tant que valeur de départ pour le calcul de CRC2 à transfert cyclique. Pour plus d'informations relatives à la conception de ce CRC_FP, voir 8.3.3.2. Cette signature CRC_FP, les données d'entrée-sortie F, l'octet d'état ou de contrôle et le MNR correspondant sont utilisés pour générer une autre signature CRC2 à 3 octets dans l'hôte F (voir Figure 23).

Dans l'appareil F, la signature CRC2 identique est générée et les signatures sont comparées. Les transferts cycliques consécutifs exigent uniquement une comparaison (qui peut être très rapide) de signature CRC2.

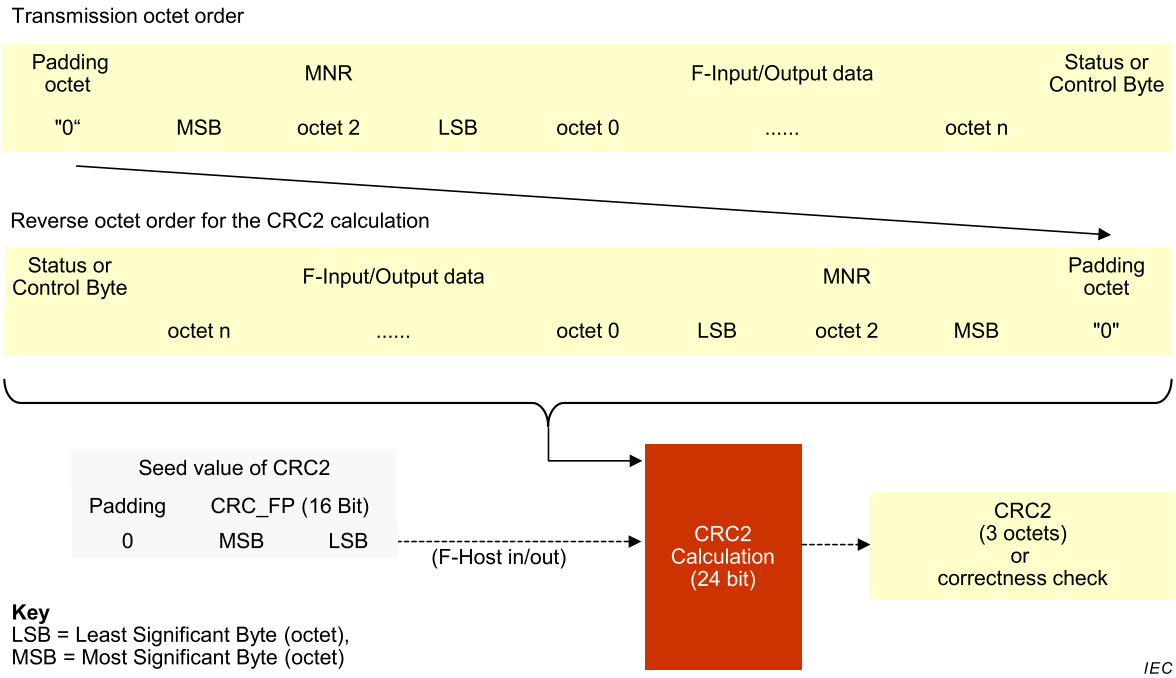


Anglais	Français
Codename	Nom de code
F-parameters	Paramètres F
Defined and constant amount	Quantité définie et constante
Identical in F-device and F-host including Codename	Identique dans appareil F et hôte F, y compris le nom de code
16 bit CRC signature	Signature CRC 16 bits
Build	Construire
Toggle bit	Bit de basculement
F-Output data	Données de sortie F
Control byte	Octet de contrôle
Seed value for CRC2 calculation	Valeur de départ pour le calcul de CRC2
(F-host) MonitoringNumber (not transmitted)	MonitoringNumber (hôte F) (non transmis)
Across F-Parameter, F-Output data, Control Byte and MNR	Parmi paramètre F, données de sortie F, octet d'état et MNR
Max. 12 octets	12 octets maximum
CRC2 generation	Génération de CRC2

Figure 23 – Génération de signature CRC2 de l'hôte F (F_CRC_Seed=0)

Toutes les modifications apportées aux paramètres F stockés doivent être détectées et provoquer un état de sécurité de l'appareil F. Les mécanismes de détection dépendent de la mise en œuvre individuelle des appareils F, et ne font pas l'objet de la présente partie.

Pour faciliter la détection des erreurs, même en présence de polynômes CRC identiques à l'intérieur du canal noir et de la couche de sécurité, le calcul de la signature CRC2 intègre les octets de la Figure 23 dans l'ordre inverse (voir Figure 24).



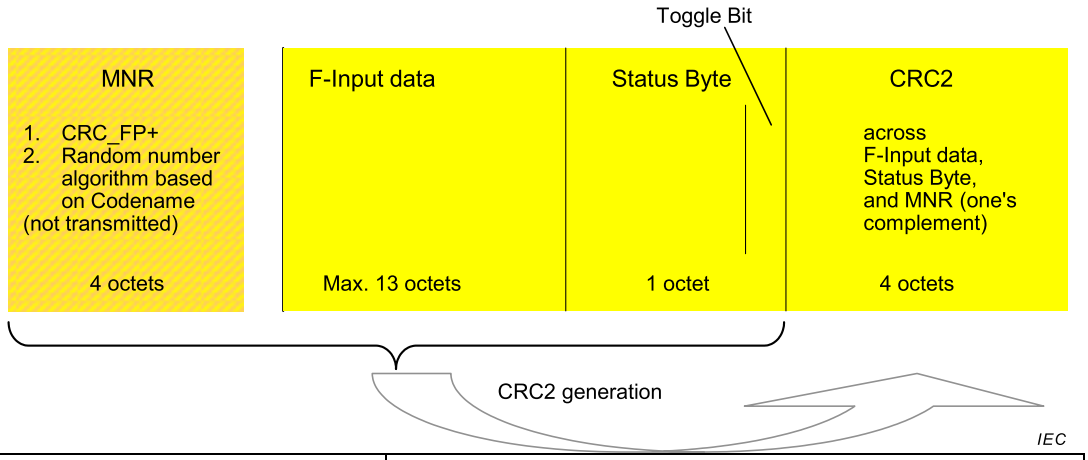
Anglais	Français
Transmission octet order	Ordre de transmission des octets
Padding octet	Octet de remplissage
F-input/output data	Données d’entrée-sortie F
Status or control byte	Octet d’état ou de contrôle
Reverse octet order for the CRC2 calculation	Ordre inverse des octets pour le calcul de CRC2
Seed value of CRC2	Valeur de départ de CRC2
F-host in/out	Entrée/sortie hôte F
CRC 2 calculation	Calcul de CRC2
CRC2 (3 octets) or correctness check	CRC2 (3 octets) ou vérification de l’exactitude
Key	Légende
LSB = Least Significant Byte (octet)	Octet de poids faible
MSB = Most Significant Byte (octet)	Octet de poids fort

Figure 24 – Détails du calcul de la signature CRC2 (F_CRC_Seed=0)

Le polynôme générateur *0x5D6DCB* doit être utilisé pour la signature CRC2 24 bits. Pour éviter qu’un PDU de sécurité ne porte qu’un 0, une exception est faite dans ce cas particulier: la valeur 1 est attribuée à CRC2 au lieu de la valeur 0 (voir 3.3).

7.1.8 Signature CRC2 (F_CRC_Seed=1)

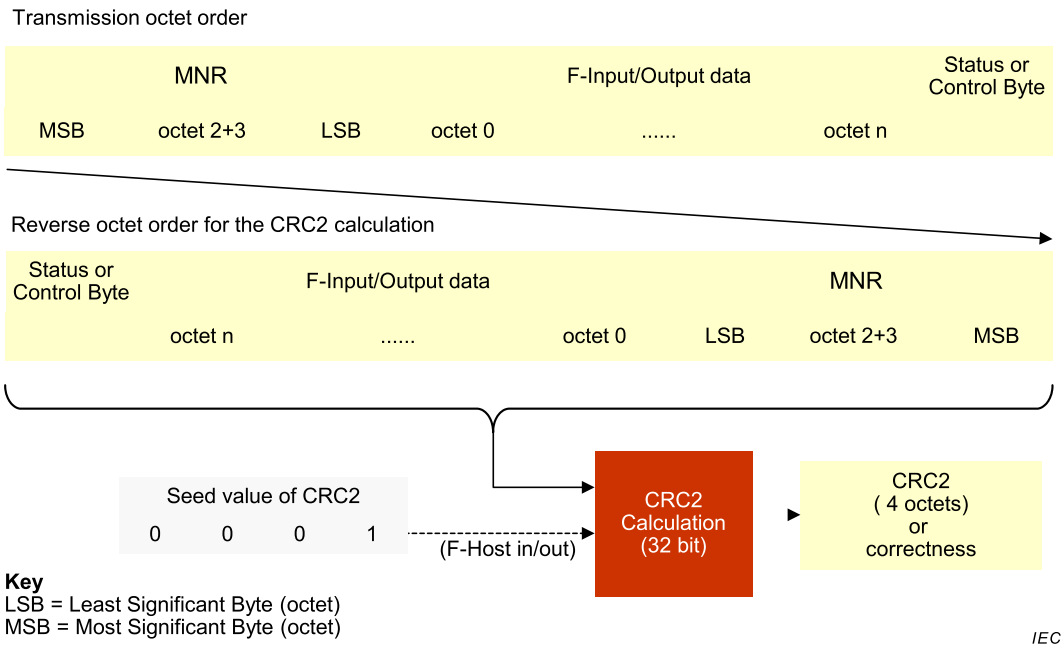
Dans le cas où F_CRC_Seed = 1, la première valeur de MNR est le CRC_FP+ du paramètre F, les MNR suivants constituent une séquence basée sur le nom de code.



Anglais	Français
Toggle bit	Bit de basculement
F-input data	Données d'entrée F
Status byte	Octet d'état
Random number algorithm based on Codename (not transmitted)	Algorithme de nombres aléatoires basé sur le nom de code (non transmis)
Across F-Input data, Status Byte and MNR (one's complement)	Parmi données d'entrée F, octet d'état et MNR (élément complémentaire unique)
Max. 13 octets	13 octets maximum
CRC2 generation	Génération de CRC2

Figure 25 – Calcul de signature CRC2 (F_CRC_Seed=1)

Le calcul de la signature CRC2 inclut les octets dans l'ordre inverse (voir Figure 26).



Anglais	Français
Transmission octet order	Ordre de transmission des octets
F-input/output data	Données d'entrée-sortie F
Status or control byte	Octet d'état ou de contrôle

Anglais	Français
Reverse octet order for the CRC2 calculation	Ordre inverse des octets pour le calcul de CRC2
Seed value of CRC2	Valeur de départ de CRC2
F-host in/out	Entrée/sortie hôte F
CRC 2 calculation	Calcul de CRC2
CRC2 (4 octets) or correctness check	CRC2 (4 octets) ou exactitude
Key	Légende
LSB = Least Significant Byte (octet)	Octet de poids faible
MSB = Most Significant Byte (octet)	Octet de poids fort

Figure 26 – Détails du calcul de la signature CRC2 (F_CRC_Seed=1)

Le pilote de l'hôte F utilise la même procédure de calcul de signature CRC2 présentée à la Figure 26 pour vérifier l'exactitude du PDU de sécurité de l'appareil F, y compris l'octet d'état, les données d'entrée F et l'élément complémentaire unique du MNR.

Le polynôme générateur *0xF4ACFB13* doit être utilisé pour la signature CRC2 32 bits. Pour éviter qu'un PDU de sécurité ne porte qu'un 0, une exception est faite dans ce cas particulier: la valeur 1 est attribuée à CRC2 au lieu de la valeur 0 (voir 3.3).

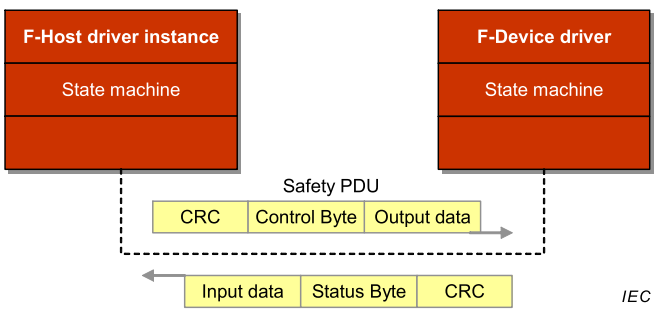
7.1.9 Données d'entrée-sortie autres que de sécurité

Des données d'entrée-sortie autres que de sécurité ne peuvent pas être ajoutées à un PDU de sécurité. Pour les appareils F compacts, cela peut être effectué en attribuant des identifications d'intervalle ou de sous-intervalles virtuelles séparées. Les modules F des appareils modulaires sont capables d'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 de chaque couche de sécurité d'un hôte F et d'un appareil F repose sur un diagramme d'états finis. Ses modes de fonctionnement sont définis au moyen des diagrammes d'états et des diagrammes séquentiels définis en 7.2.2 et 7.2.3. La Figure 27 présente un modèle simplifié de la communication de sécurité. Un chronogramme particulier présenté en 7.2.5 représente les conséquences d'une anomalie du signal de réinitialisation du MNR. La surveillance des temps de passage du PDU de sécurité est décrite en 7.2.6.



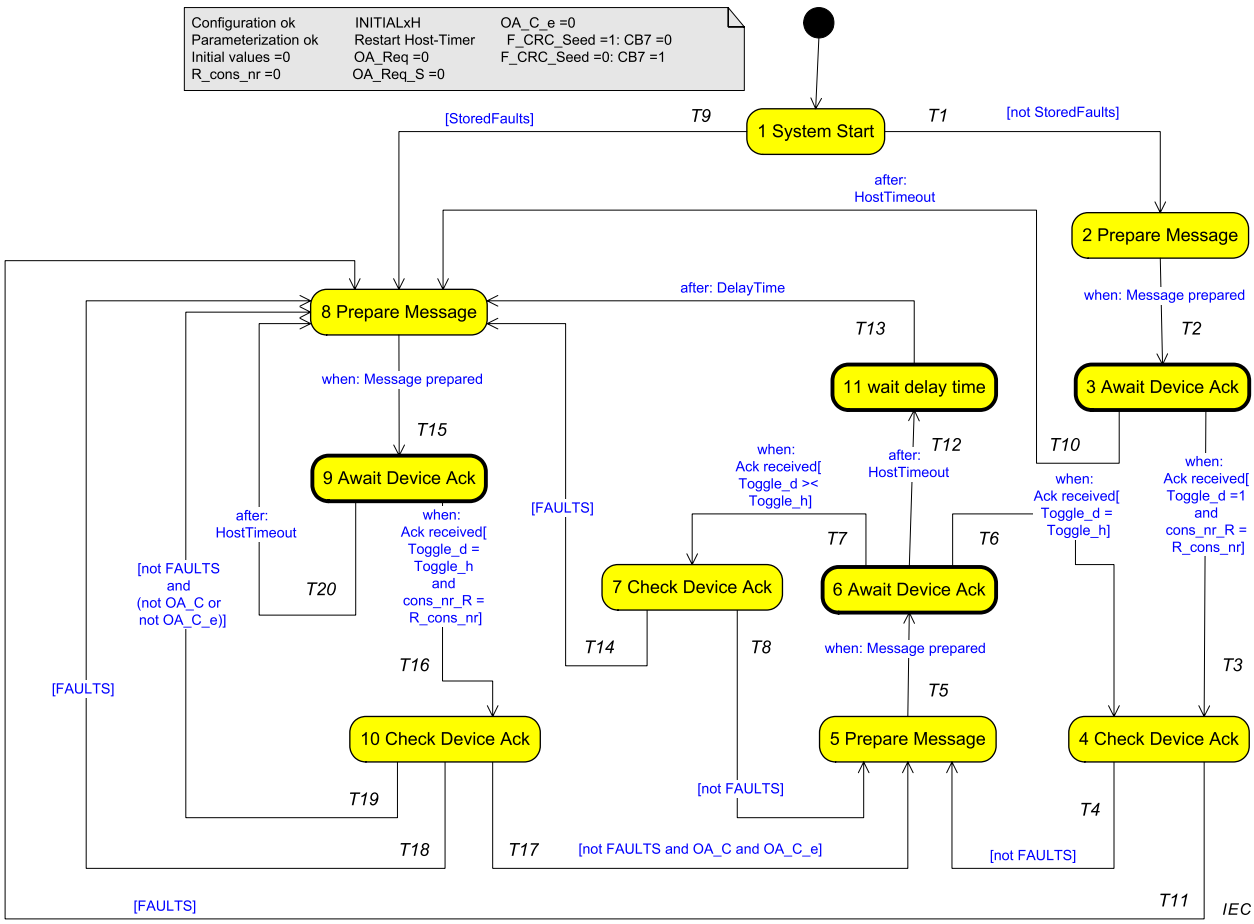
Anglais	Français
F-host driver instance	Instance de pilote d'hôte F
State machine	Diagramme d'états
F-device driver	Pilote d'appareil F
Safety PDU	PDU de sécurité
Control byte	Octet de contrôle

Anglais	Français
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 représente le diagramme d'états de l'hôte F, et le Tableau 9 décrit les états, les transitions et les éléments internes de l'hôte F. Les diagrammes suivent la notation UML2.



Anglais	Français
Parameterization	Paramétrage
Initial values	Valeurs initiales
Restart host timer	Redémarrer le temporisateur de l'hôte

Figure 28 – Diagramme d'états de l'hôte F

Les termes utilisés dans la Figure 28 sont spécifiés dans le Tableau 8.

Tableau 8 – Définition des termes utilisés dans le diagramme d'états de l'hôte F

Terme	Définition
Initial values (Valeurs initiales)	Valeurs du PDU de sécurité =0
HostTimeout	L'hôte F reconnaît une temporisation locale lorsqu'il attend un acquittement de l'appareil F dans F_WD_Time. Cette HostTimeout doit être étendue une seule fois par F_WD_Time_2 dans le cas où "use_TO2" = 1 (F_WD_Time + F_WD_Time_2), similaire à l'appareil F (voir 6.1, 8.1.4).
Host_CE_CRC	L'hôte F reconnaît l'anomalie CRC lors de l'analyse du PDU de sécurité reçu
Device_Fault	F_Passivation =0 (voir 8.1.6.2): l'appareil F a signalé une anomalie à l'hôte; bit d'état 1 =1.
CE_CRC	L'appareil 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	L'appareil F a signalé une anomalie de temporisation à l'hôte F; bit d'état 3 =1
INITIALxH	Macro, voir 7.1.5 et 7.1.6
FAULTS	Cette variable est vraie (=1) si l'un des bits suivants est défini: - SB2 (CE_CRC) - SB3 (WD_timeout) - SB7 (Status Byte, Bit7), if F_CRC_Seed =0 - Host_CE_CRC
StoredFaults	Cette variable est vraie (=1) si l'un des bits FAULTS et/ou HostTimeout avait été stocké au moment de l'arrêt
Ack received (acquittement reçu)	Tout nouveau PDU de sécurité reçu; ignorer le PDU de sécurité avec toutes les valeurs = 0

Les transitions sont supprimées si un événement se produit (la réception d'un message, par exemple). Si plusieurs transitions sont possibles, les protections [conditions] définissent la transition à supprimer.

Les états 4, 7 et 10 (Vérification de l'acquittement de l'appareil) sont appelés états de changement conformément à UML2 sans événement «externe». Les transitions correspondantes sont supprimées après évaluation des valeurs internes.

Le diagramme est composé d'états d'activité et d'action. Les états d'activité sont encadrés par des lignes en gras, et les états d'action par des lignes minces. Les états d'activité peuvent être interrompus par de nouveaux événements, ce qui n'est pas le cas des états d'action. Les événements qui composent un état d'action (les délais, les messages reçus ou les acquittements de l'opérateur, par exemple) sont différés jusqu'à l'état d'activité suivant.

Tableau 9 – États et transitions de l'hôte F

NOM D'ÉTAT	DESCRIPTION DE L'ÉTAT
1 System Start (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 Prepare Message (Préparation du message)	Préparation d'un PDU de sécurité régulier pour l'appareil F
3 Await Device Ack (Attente de l'acquittement de l'appareil)	La couche de sécurité attend le PDU de sécurité régulier suivant provenant de l'appareil F (Acquittement).
4 Check Device Ack (Vérification de l'acquittement de l'appareil)	Vérification du PDU de sécurité reçu pour une erreur *CRC* (Host_CE_CRC) comprenant le MNR virtuel, et pour les anomalies potentielles *de l'*appareil *F* dans l'octet d'état (WD_timeout, CE_CRC)
5 Prepare Message (Préparation du message)	Préparation d'un PDU de sécurité régulier pour l'appareil F
6 Await Device Ack (Attente de l'acquittement de l'appareil)	La couche de sécurité attend le PDU de sécurité régulier suivant provenant de l'appareil F (Acquittement)
7 Check Device Ack (Vérification de l'acquittement de l'appareil)	Vérification du PDU de sécurité reçu pour une erreur *CRC* (Host_CE_CRC) comprenant l'ancien (old_MNR) MNR virtuel, et pour les anomalies potentielles *de* l'appareil *F* dans l'octet d'état (WD_timeout, CE_CRC)
8 Prepare Message (Préparation du message)	Préparation d'un PDU de sécurité pour l'appareil F (traitement des exceptions)
9 Await Device Ack (Attente de l'acquittement de l'appareil)	La couche de sécurité attend le PDU de sécurité irrégulier suivant provenant de l'appareil F (Acquittement)
10 Check Device Ack (Vérification de l'acquittement de l'appareil)	Vérification du PDU de sécurité reçu pour une erreur *CRC* (Host_CE_CRC) comprenant le MNR virtuel, et pour les anomalies potentielles de l'appareil *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 Wait delay time (Délai d'attente)	Cet état permet d'éviter le stockage d'une anomalie de temporisation en cas d'arrêt occasionnel du système, ce qui engendrerait une demande d'acquittement de l'opérateur à la prochaine mise sous tension. Un délai d'attente de 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	RUNxH Toggle_h = not Toggle_h, **if** FV_activated =1 or activate_FV_C =1 or Device_Fault [b] =1 **then** use FVi, FV_activated_S =1 **else** use PVi, FV_activated_S =0 **if** activate_FV_C =1 or Device_Fault [b] =1 **then** use FVo, activate_FV =1 **else** use PVo, activate_FV =0 iPar_OK_S =iPar_OK
T5	5	6	send safety PDU
T6	6	4	restart host-timer
T7	6	7	-
T8	7	5	**if** FV_activated =1 or activate_FV_C =1 or Device_Fault [b] =1 **then** use FVi, FV_activated_S =1 **else** use PVi, FV_activated_S =0 **if** activate_FV_C =1 or Device_Fault [b] =1 **then** use FVo, activate_FV =1 **else** use PVo, activate_FV =0 iPar_OK_S =iPar_OK

TRAN-SITION	ETAT SOURCE	ETAT CIBLE	ACTION
T9[a]	1	8	use FV, activate_FV =1, FV_activated_S =1, Toggle_h =1, RESETxH
T10	3	8	restart host-timer, store faults, use FV, activate_FV =1, FV_activated_S =1, Toggle_h = not Toggle_h, RESETxH
T11	4	8	store faults, use FV, activate_FV =1, FV_activated_S =1, Toggle_h = not Toggle_h, RESETxH
T12	6	11	use FV, activate_FV =1, FV_activated_S =1, RESETxH
T13	11	8	store faults, Toggle_h = not Toggle_h, restart host-timer
T14	7	8	restart host-timer, store faults, use FV, activate_FV =1, FV_activated_S =1, Toggle_h = not Toggle_h, RESETxH
T15	8	9	send safety PDU
T16	9	10	restart host-timer
T17	10	5	reset stored faults, OA_Req_S =0, OA_Req =0, OA_C_e =0, Toggle_h = not Toggle_h, RUNxH if FV_activated =1 or activate_FV_C =1 or Device_Fault [b] =1 then use FVi, FV_activated_S =1 else use PVi, FV_activated_S =0 if activate_FV_C =1 or Device_Fault [b] =1 then use FVo, activate_FV =1 else use PVo, activate_FV =0 iPar_OK_S =iPar_OK
T18	10	8	store faults, OA_Req =0, OA_Req_S =0, OA_C_e =0, use FV, activate_FV =1, FV_activated_S =1, Toggle_h = not Toggle_h, RESETxH
T19	10	8	OA_Req_S =1, OA_Req =1, if OA_C =0 then OA_C_e =1 use FV, activate_FV =1, FV_activated_S =1, Toggle_h = not Toggle_h, RUNxH
T20	9	8	store faults, OA_Req =0, OA_Req_S =0, OA_C_e =0, use FV, activate_FV =1, FV_activated_S =1, Toggle_h = not Toggle_h, RESETxH restart host-timer

a Voir STATE DESCRIPTION de STATE 1. L'énoncé "store faults" ("stocker les anomalies") dans les transitions peut être omis si T9 n'est pas mis en œuvre.

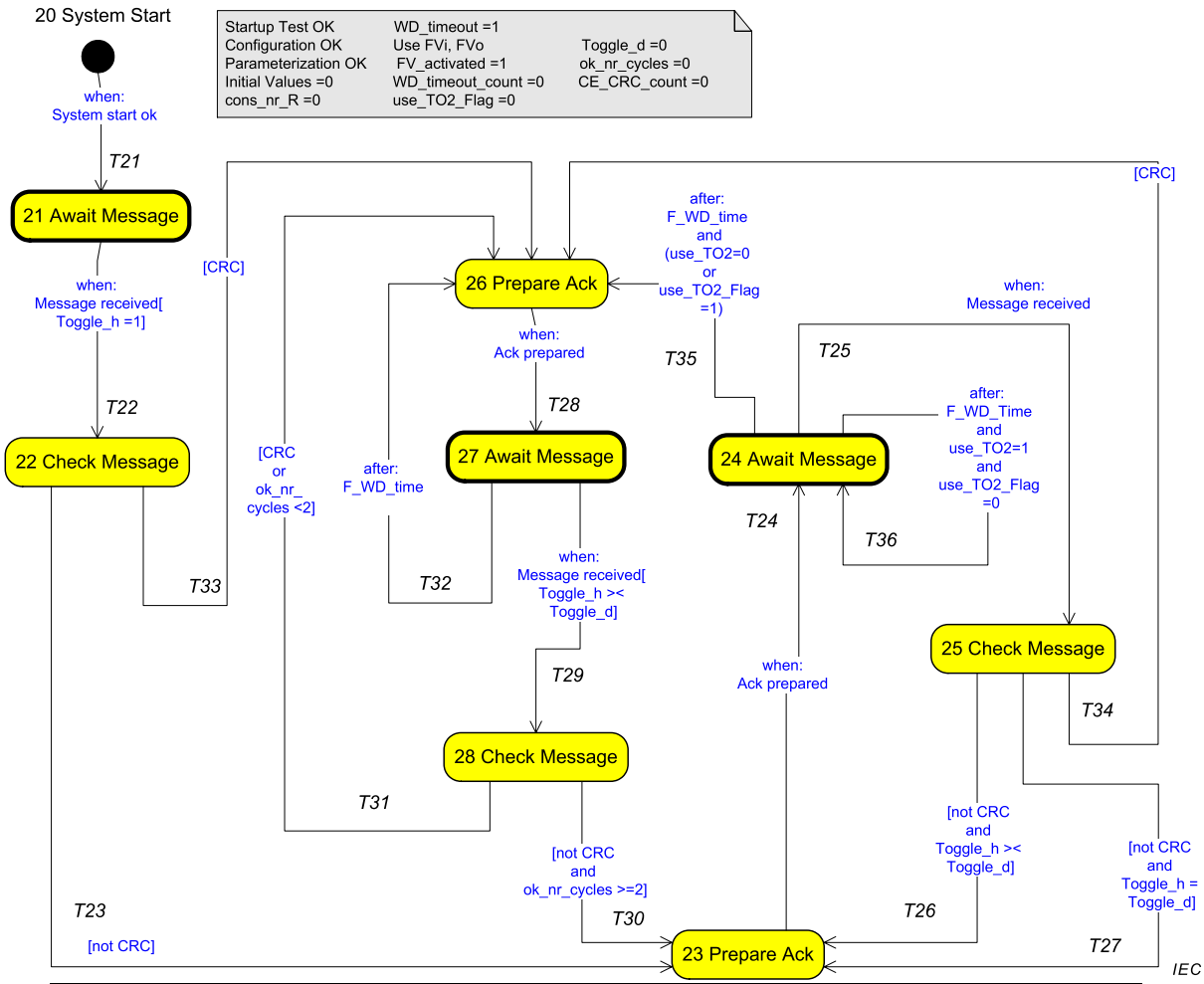
b L'anomalie de l'appareil n'est pas prise en considération dans l'opération logique si Passivation F =1.

ÉLÉMENTS INTERNES	TYPE	DÉFINITION
RESETxH	Macro	Voir 7.1.5 et 7.1.6
RUNxH	Macro	Voir 7.1.5 et 7.1.6

ÉLÉMENTS INTERNES	TYPE	DÉFINITION
MNR	Variable	MNR représente le MonitoringNumber local dans l'instance de pilote de l'hôte F. Il n'est pas transmis à son homologue de l'appareil F, mais synchronise en revanche ces homologues par l'intermédiaire d'un bit de basculement de l'octet de contrôle. Le MNR réel est intégré dans le calcul de CRC2 et ainsi vérifié par rapport aux anomalies de transmission.
old_MNR	Variable	Valeur précédente du MNR local actuel. Il est nécessaire de stocker cette valeur précédente du MNR.
DelayTime	Temporisateur	Ce délai d'attente permet de couvrir le temps de stabilisation à la mise hors tension de l'ensemble du système. Le fabricant de l'hôte/du système est chargé de définir ce paramètre.
host-timer	Temporisateur	Ce temporisateur permet de vérifier si le PDU de sécurité valide suivant provenant de l'appareil 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 peut annuler des états de sécurité en activant définitivement le signal OA_C.
faults	Drapeaux	Tant qu'un acquittement de l'opérateur (OA_C) n'a pas été reçu, un stockage permanent du bit FAULT (voir Tableau 8) dans l'hôte F uniquement est exigé (et pas dans l'appareil F
	État d'activité	Dans ces états d' «activité» qu'il est possible d'interrompre, l'hôte attend de nouvelles entrées (une temporisation ou un acquittement, par exemple) [34].
	État d'action	Dans ces états d' «action» qu'il est impossible d'interrompre, les événements (temporisation, message reçu ou acquittement de l'opérateur, par exemple) sont différés jusqu'à l'état d' «activité» suivant [34].

7.2.3 Diagramme d'états de l'appareil F

La Figure 29 représente le diagramme d'états de l'appareil F, et le Tableau 11 décrit les états, les transitions et les éléments internes. Les diagrammes suivent la notation UML2.



Anglais	Français
Parameterization	Paramétrage
Initial values	Valeurs initiales
Startup test	Essai de démarrage

Figure 29 – Diagramme d'états de l'appareil F

Les termes utilisés dans la Figure 29 sont spécifiés dans le Tableau 10.

Tableau 10 – Définition des termes utilisés dans la Figure 29

Terme	Définition
[Toggle_h = Toggle_d]	notation UML d'une condition (protection) pour supprimer la transition. Dans ce cas, elle signifie: La valeur du bit Toggle_h n'a pas changé ("pas de basculement")
[Toggle_h >< Toggle_d]	La valeur du bit Toggle_h a changé ("basculement")
[CRC]	L'appareil F reconnaît l'anomalie CRC (erreur de communication et/ou de MNR)
F_WD_Time	Temps de fonctionnement du chien de garde défini par le paramètre F "F_WD_Time"
use_TO2	CB3 de l'octet de contrôle 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 de l'appareil F
Message received (Message reçu)	Tout nouveau PDU de sécurité reçu; ignorer le PDU de sécurité avec toutes les valeurs = 0
INITIALxD	Macro voir 7.1.5 et 7.1.6

Tableau 11 – États et transitions de l'appareil F

NOM D'ÉTAT	DESCRIPTION DE L'ÉTAT
20 System Start (Démarrage du système)	État initial de l'appareil lors de la mise sous tension. Lors de la mise sous tension, la valeur de l'appareil F de sortie est 0. Immédiatement après le paramétrage F, les valeurs Failsafe sont définies. Lors de la mise sous tension, l'appareil F d'entrée envoie 0. Immédiatement après le paramétrage F, il envoie des valeurs de processus.
21 Await Message (Attente de message)	La couche de sécurité attend le PDU de sécurité suivant provenant de l'hôte F
22 Check Message (Vérification de message)	Vérification du PDU de sécurité reçu pour l'erreur CRC, y compris le MNR virtuel
23 Prepare Ack (Préparation de l'acquittement)	Préparation d'un PDU de sécurité régulier pour l'hôte F (Acquittement)
24 Await Message (Attente de message)	La couche de sécurité attend le PDU de sécurité régulier suivant provenant de l'hôte F
25 Check Message (Vérification de message)	Vérification du PDU de sécurité reçu pour l'erreur CRC, y compris le MNR virtuel
26 Prepare Ack (Préparation de l'acquittement)	Préparation d'un PDU de sécurité pour l'hôte F (Acquittement avec bits erronés)
27 Await Message (Attente de message)	La couche de sécurité attend le PDU de sécurité suivant provenant de l'hôte F (traitement des exceptions)
28 Check Message (Vérification de message)	Vérification du PDU de sécurité reçu pour l'erreur *CRC*, y compris le MNR virtuel

TRAN-SITION	ETAT SOURCE	ETAT CIBLE	ACTION
T21	20	21	-
T22	21	22	**if** R_cons_nr =1 **then** RESETxD **else** INITIALxD
T23	22	23	use PVi, FVo, FV_activated =1, CE_CRC =0, WD_timeout =0, Toggle_d = Toggle_h, restart device-timer, ok_nr_cycles =ok_nr_cycles +1
T24	23	24	send safety PDU
T25	24	25	**if** Toggle_h >< Toggle_d **then** restart device-timer **if** R_cons_nr =1 and activate_FV =1 **then** RESETxD **else** RUNxD
T26	25	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 **if** use_TO2 =0 **then** use_TO2_Flag =0
T27	25	23	Use PVi, Toggle_d = Toggle_h, **if** ok_nr_cycles <4 **then** use FVo, FV_activated =1 **else** use PVo, FV_activated =0 **if** activate_FV =1 **then** use FVo

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

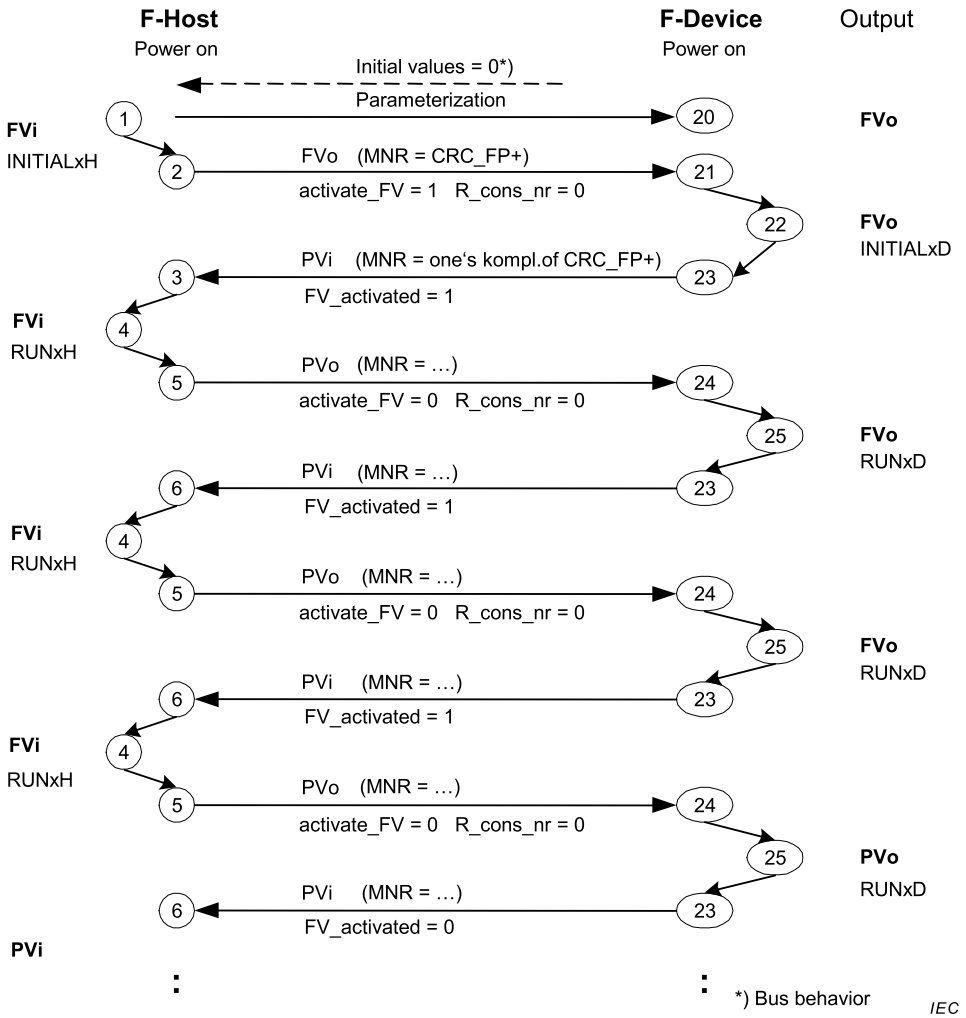
ÉLÉMENTS INTERNES	TYPE	DÉFINITION
RESETxD	Macro	Voir 7.1.5 et 7.1.6
RUNxD	Macro	Voir 7.1.5 et 7.1.6
MNR	Variable	MNR représente le MNR local réel dans l'appareil F. Il n'est pas transmis à son homologue dans l'hôte F, mais est synchronisé en revanche avec ces homologues par l'intermédiaire d'un bit de basculement de l'octet de contrôle. Cela signifie qu'il change à chaque fois que l'état du bit de basculement de l'octet de contrôle (Toggle_h) change de 0 → 1 ou de 1 → 0.

ÉLÉMENTS INTERNES	TYPE	DÉFINITION
ok_nr_cycles	Compteur	Lors du démarrage et après une anomalie, l'appareil F doit définir FVo et «FV_activated = 1» pendant au moins 3 cycles. Ce compteur incrémentiel est chargé de compter ces cycles de 0 à 3.
CE_CRC_count	Compteur	Ce compteur décrémentiel permet de s'assurer que le bit «CE_CRC» de l'octet d'état est défini pour au moins 1 cycle ou 2 cycles au maximum. La plage de valeurs est comprise entre 0 et 1.
WD_timeout_count	Compteur	Ce compteur décrémentiel permet de s'assurer que le bit «WD_timeout» de l'octet d'état est défini pour au moins 1 cycle ou 2 cycles au maximum. La plage de valeurs est comprise entre 0 et 1.
device-timer	Temporisateur	Ce temporisateur permet de vérifier si le PDU de sécurité valide suivant est arrivé à temps. Le paramètre F " F_WD_Time" permet de définir ce temps de fonctionnement du chien de garde. La plage de valeurs est comprise entre 0 et 65 535 ms.

7.2.4 Diagrammes séquentiels

Les Figure 30 à Figure 35 représentent les messages d'interaction de l'hôte F et de l'appareil F pendant la phase de démarrage. Trois phases sont présentées: lors du démarrage, les deux partenaires, l'hôte F ou l'appareil F commute 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 l'appareil F.

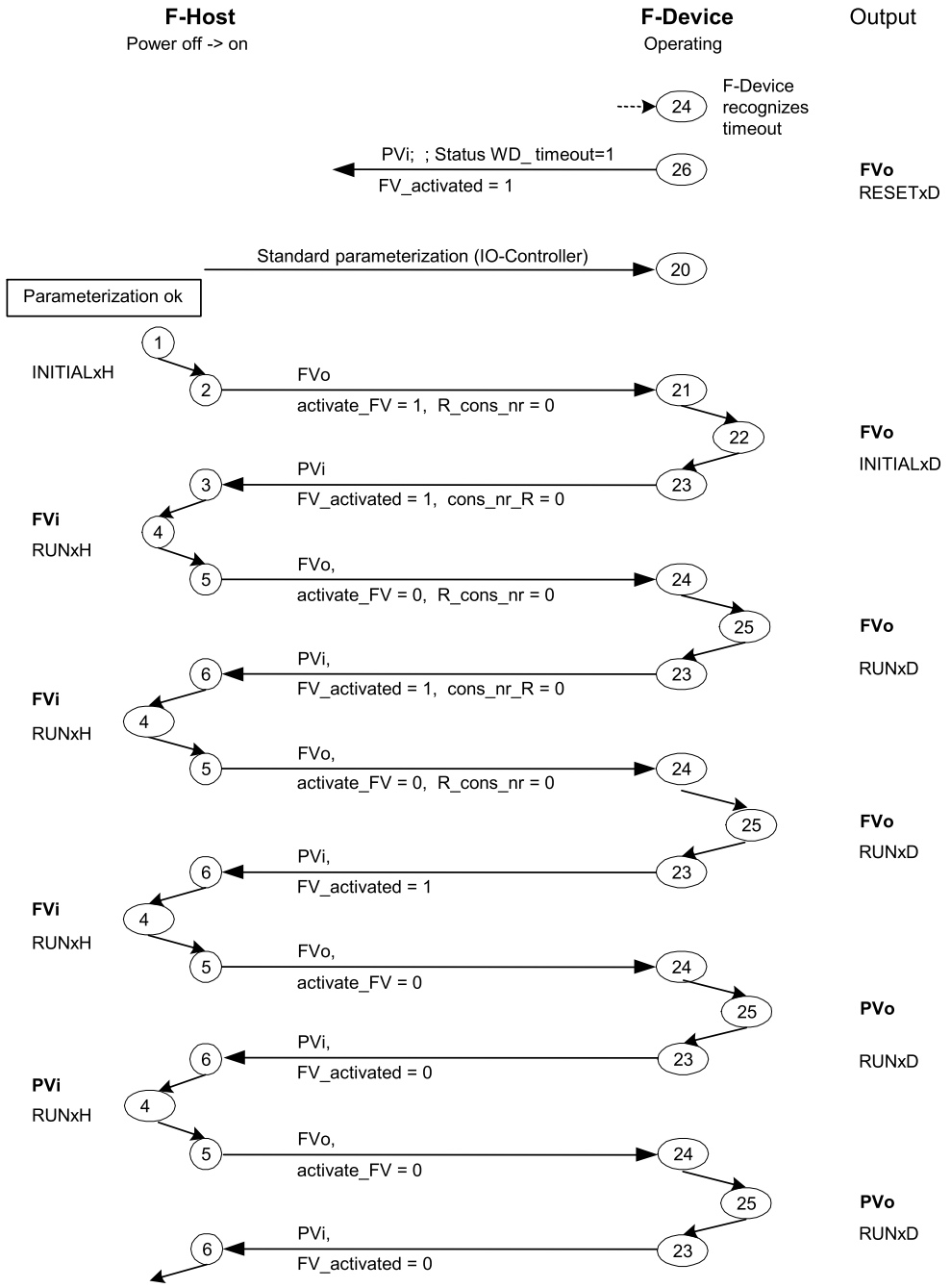
La Figure 30 présente le début régulier des transmissions de PDU de sécurité entre l'hôte F et l'appareil F après mise sous tension. Une séquence possible des MonitoringNumbers est présentée au Tableau A.4



Anglais	Français
F-host	Hôte F
Power on	Sous tension
F-device	Appareil F
Output	Sortie
Initial values	Valeurs initiales
Parameterization	Paramétrage
Bus behavior	Comportement du bus

Figure 30 – Interaction de l'hôte F et de l'appareil F pendant le démarrage

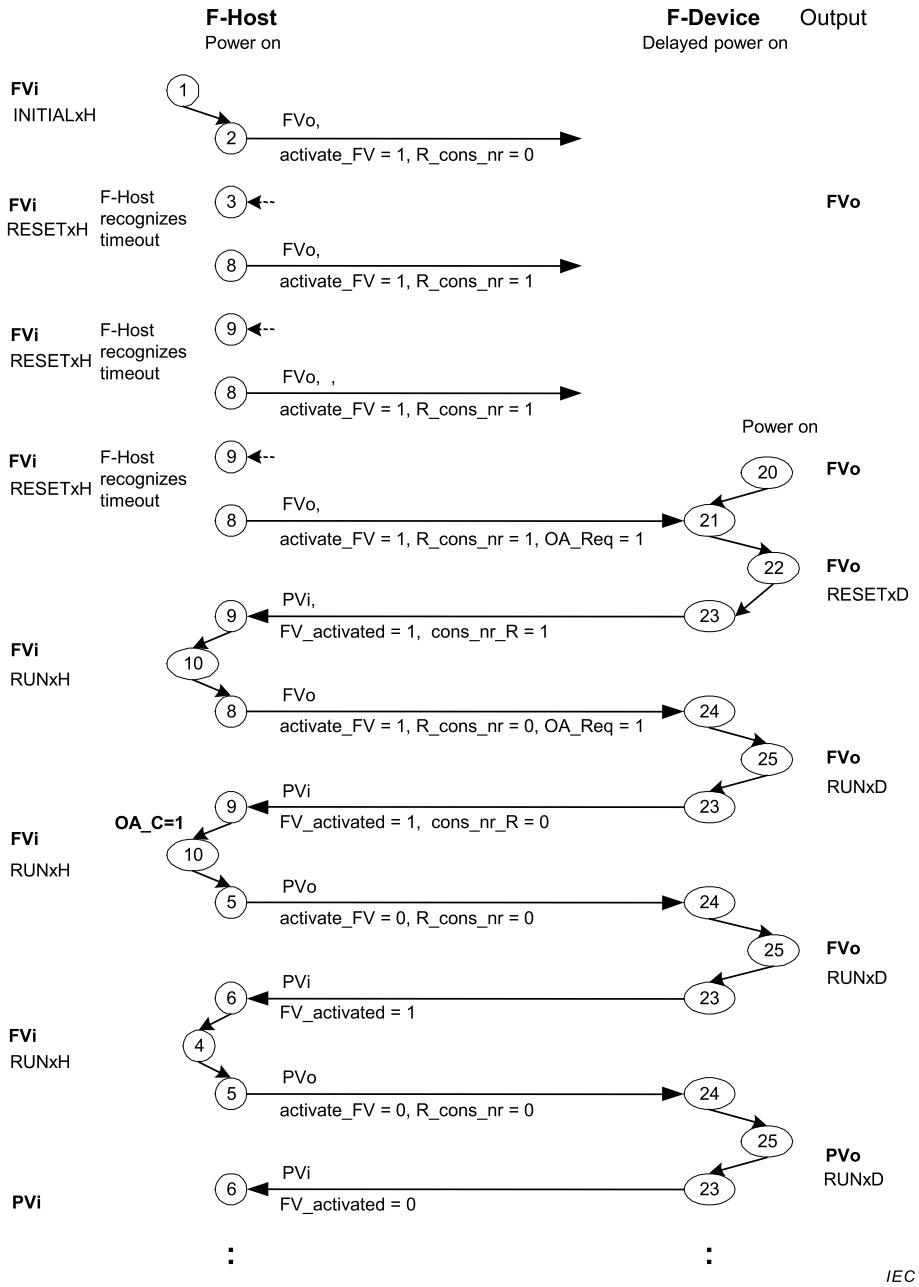
La Figure 31 présente un exemple d'attribution de paramètre F dans le cas où l'appareil F fonctionne déjà et où l'hôte F passe de la mise hors tension à la mise sous tension.



Anglais	Français
Anglais	Français
F-host	Hôte F
Power off -> on	hors tension -> sous tension
F-device	Appareil F
Output	Sortie
Operating	En fonctionnement
Parameterization	Paramétrage
F-device recognizes timeout	L'appareil F reconnaît la temporisation
Status	État
Standard parameterization (IO controller)	Paramétrage standard (contrôleur d'entrée-sortie)

Figure 31 – Interaction de l'hôte F et de l'appareil F pendant la mise hors tension → sous tension de l'hôte F

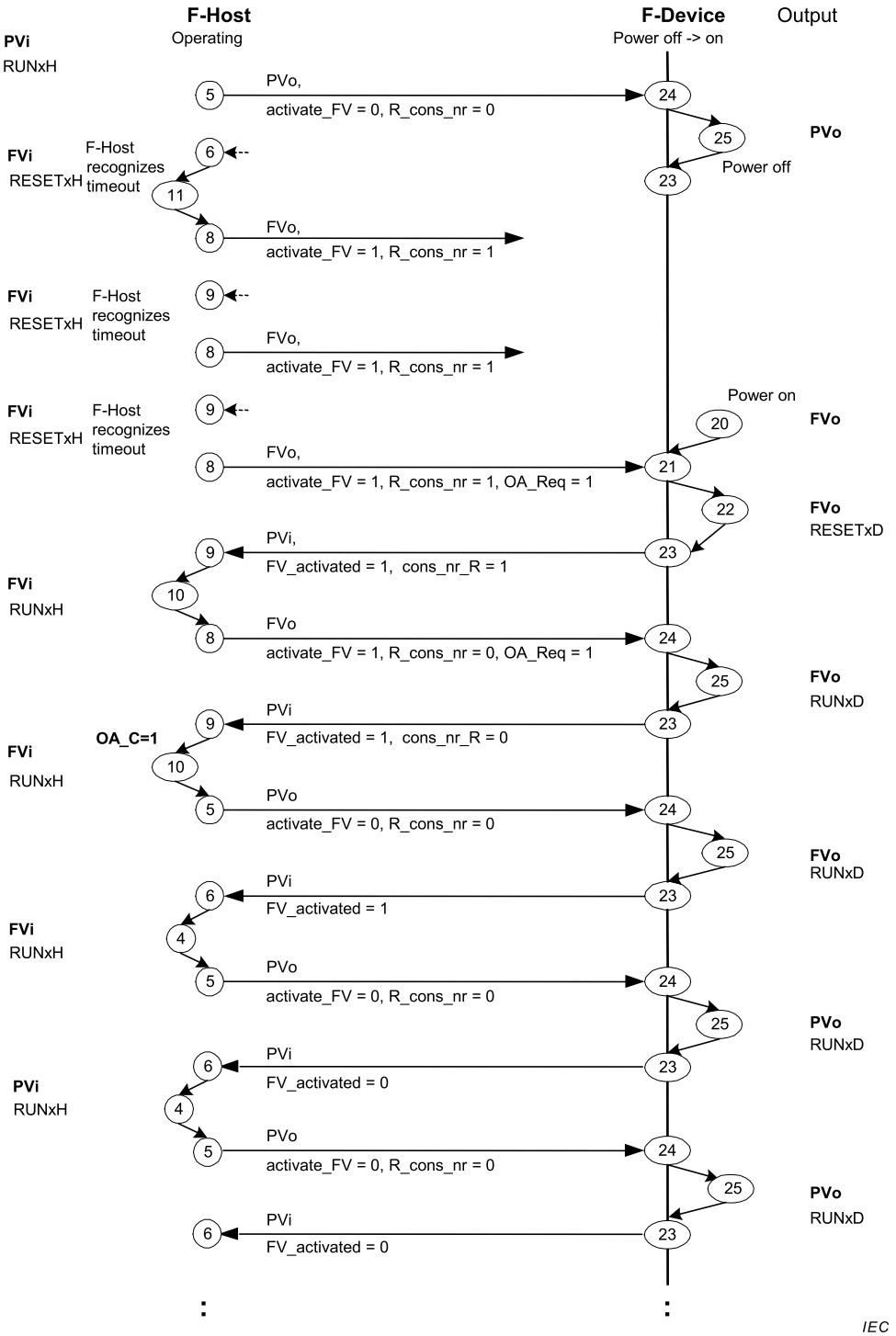
La Figure 32 présente un exemple d'attribution de paramètre F dans le cas où l'hôte F fonctionne déjà et où l'appareil F commute la mise sous tension après un report.



Anglais	Français
Anglais	Français
F-host	Hôte F
Delayed power on	mise sous tension retardée
F-device	Appareil F
Output	Sortie
Power on	Sous tension
F-host recognizes timeout	L'hôte F reconnaît la temporisation

Figure 32 – Interaction de l'hôte F et de l'appareil F pendant un report de mise sous tension

La Figure 33 correspond à la Figure 32. Elle représente le cas où l'hôte F fonctionne déjà et où l'appareil F commute la mise hors tension, puis après un report, commute à nouveau la mise sous tension.

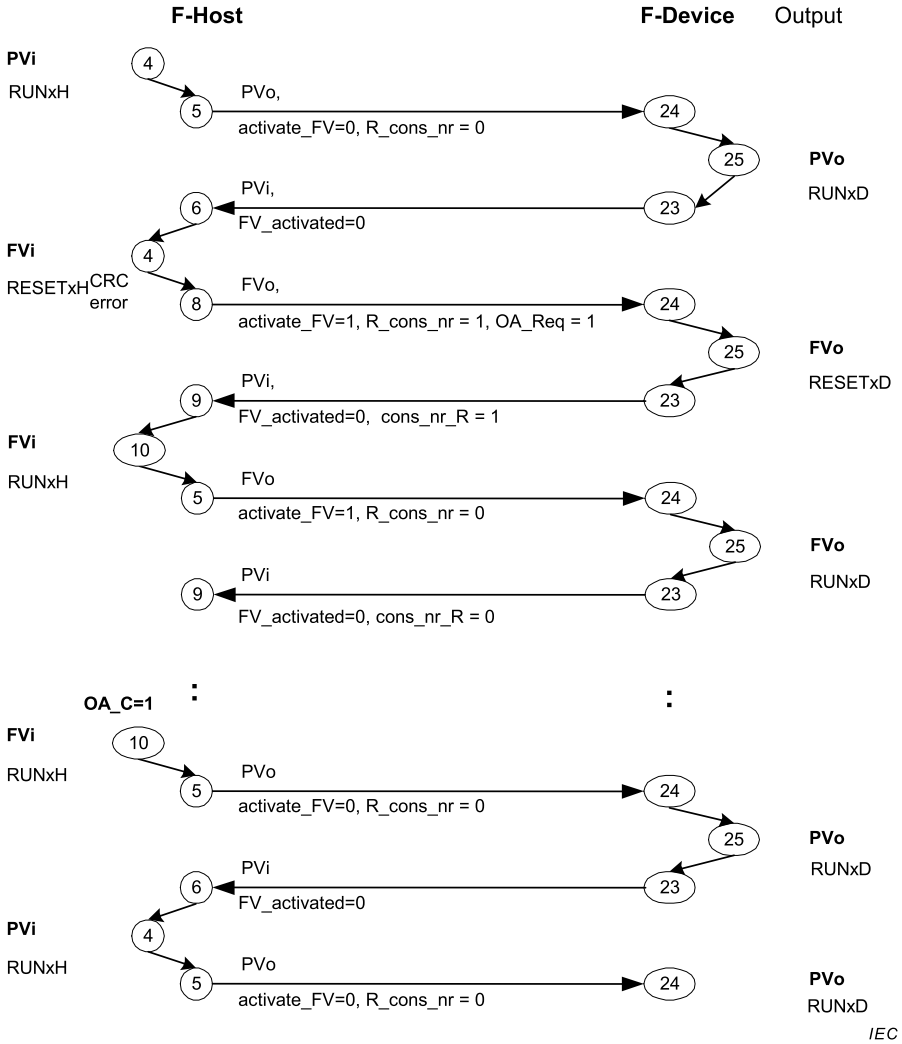


Anglais	Français
F-host	Hôte F
Power off -> on	hors tension -> sous tension
F-device	Appareil F
Output	Sortie
Operating	En fonctionnement

Anglais	Français
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 de l'appareil F pendant la mise hors tension→ sous tension

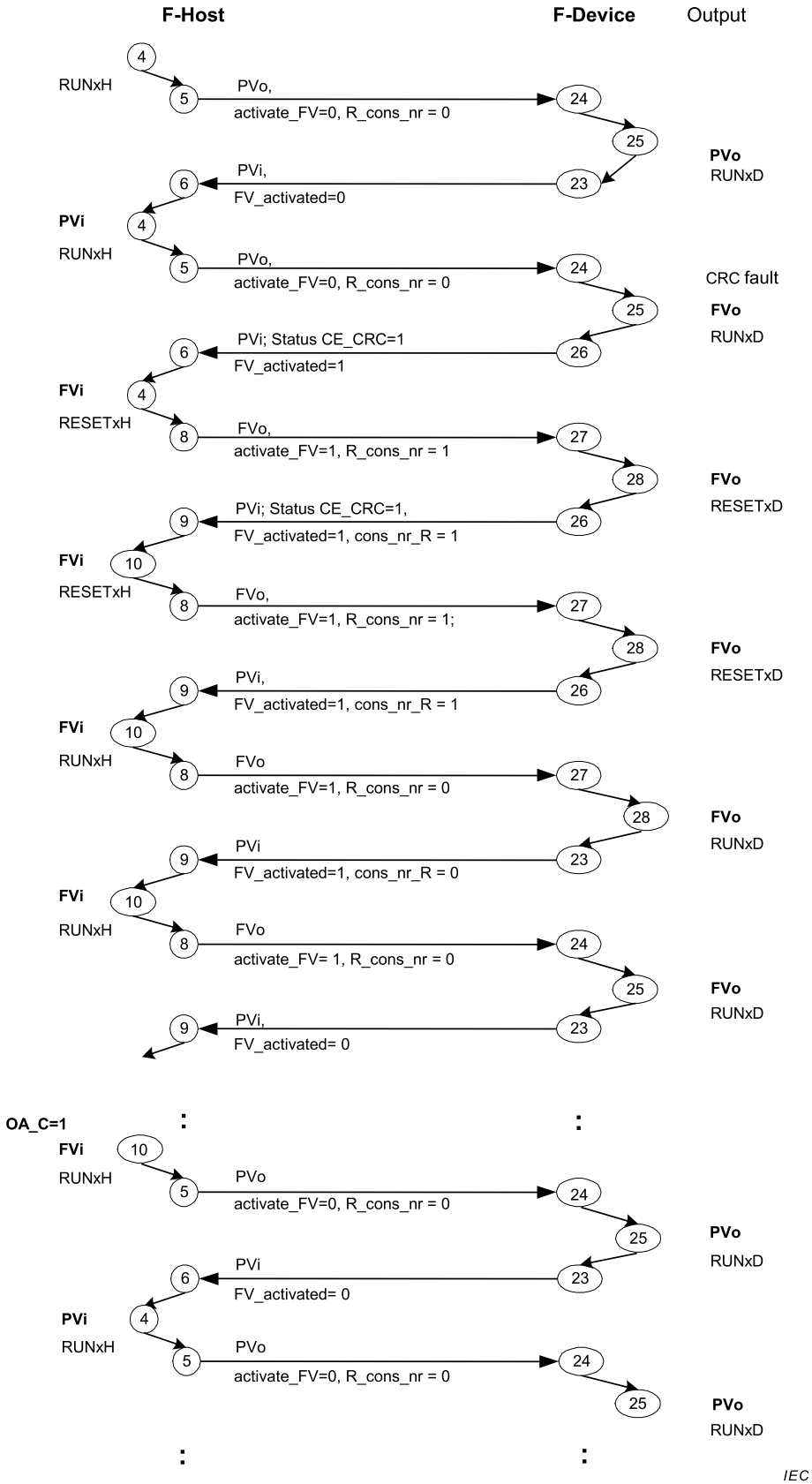
La Figure 34 présente les messages d'interaction entre l'hôte F et l'appareil F lorsque des anomalies CRC sont détectées du côté de l'hôte F.



Anglais	Français
F-host	Hôte F
F-device	Appareil F
Output	Sortie
CRC error	Erreur CRC

Figure 34 – Interaction de l'hôte F et de l'appareil F lorsque l'hôte reconnaît une erreur CRC

La Figure 35 présente les messages d'interaction entre l'hôte F et l'appareil F lorsque des anomalies CRC sont détectées du côté de l'appareil F.



Anglais	Français
F-host	Hôte F
F-device	Appareil F
Output	Sortie

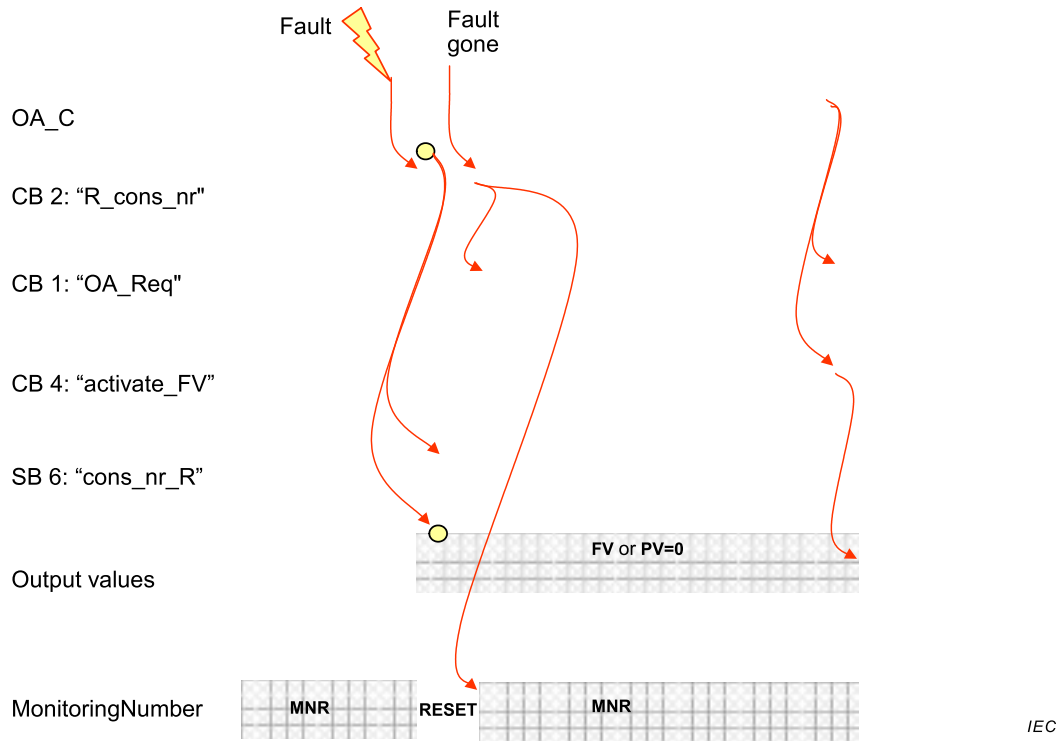
Anglais	Français
CRC fault	Anomalie CRC

Figure 35 – Interaction de l'hôte F et de l'appareil F lorsque l'appareil reconnaît une erreur CRC

7.2.5 Chronogramme de réinitialisation d'un MonitoringNumber

La Figure 36 présente les conséquences d'un défaut de communication F sur le Monitoring-Number et les éléments dépendants.

Après une anomalie, le bit 2 ("R_cons_nr") et le bit 4 ("activate_FV") de l'octet de contrôle sont définis (=1). Par conséquent, le MNR est réinitialisé et les valeurs de sortie d'un appareil de sortie F sont définies sur "FVo".



Anglais	Français
Fault	Anomalie
Fault gone	Anomalie résolue
Output values	Valeurs de sortie
Or	Ou
RESET	REINITIALISATION

Figure 36 – Impact du signal de réinitialisation du MNR

Au même moment, l'hôte F envoie le signal "OA_Req" en tant que bit 1 de l'octet de contrôle à l'appareil F. Ce signal peut être utilisé pour indiquer à l'utilisateur, via la LED (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 MNR reprend sa valeur par défaut (R_cons_nr = 0);
- le MNR redémarre.

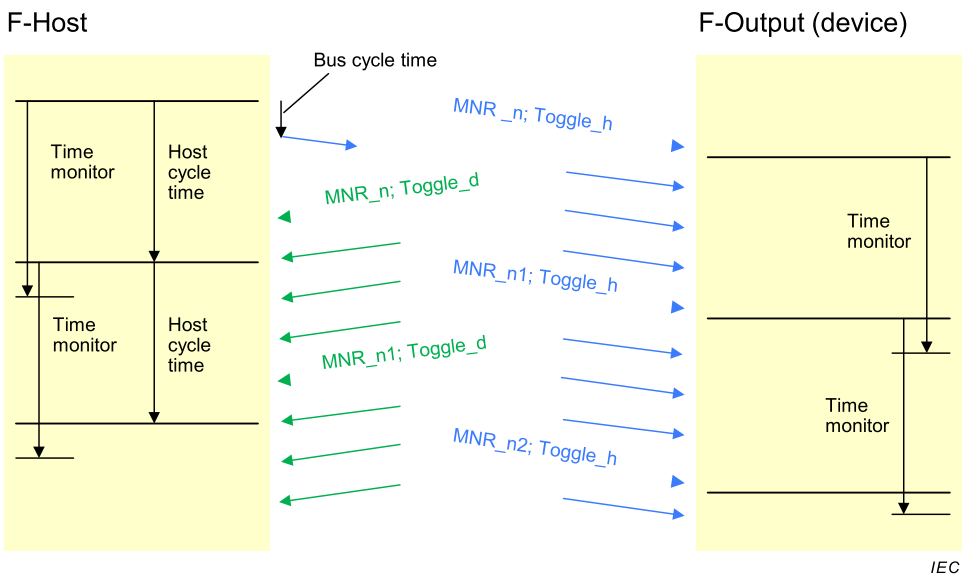
Immédiatement après un acquittement de l'opérateur (OA_C = 1), les actions ci-dessous se déroulent:

- la demande d'un acquittement de l'opérateur reprend sa valeur par défaut (OA_Req = 0);
- la demande d'activation d'un état de sortie de sécurité 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

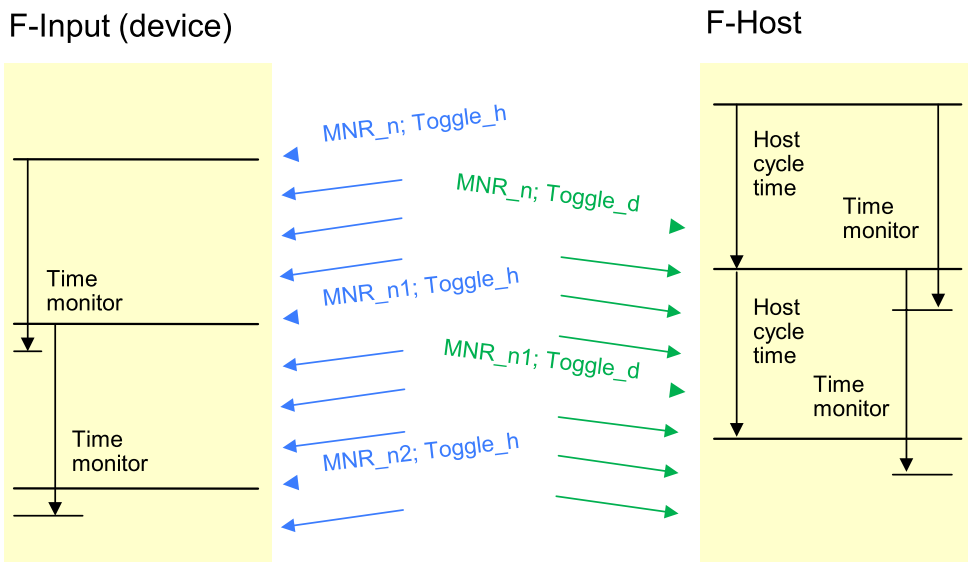
La Figure 37 explique comment le pilote F utilise les communications CP 3/RTE sous-jacentes et la manière dont certains temps de surveillance sont définis. Signification des flèches courtes: dans CP 3/RTE, le contrôleur d'entrée-sortie envoie le même PDU de sécurité à l'appareil F plus fréquemment que le pilote F ne génère un nouveau PDU de sécurité dans la durée de cycle de l'hôte F. En retour, l'appareil F envoie le PDU de sécurité (acquittement) au contrôleur d'entrée-sortie plus fréquemment que le pilote F de l'appareil F ne génère un nouveau PDU de sécurité.



Anglais	Français
F-host	Hôte F
F-output (device)	Sortie F (appareil)
Bus cycle time	Durée de cycle du bus
Time monitor	Surveillance de la durée
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 présente la surveillance de la durée dans l'hôte F et un appareil de sortie F. La Figure 38 présente la surveillance de la durée dans l'appareil d'entrée F et l'hôte F. Les flèches courtes dans les Figures représentent les PDU de FSCP 3/1 comportant le MNR (virtuel) en cours de validité, mais avec d'éventuelles valeurs de processus différentes.



Anglais	Français
F-host	Hôte F
F-input (device)	Entrée F (appareil)
Host cycle time	Durée de cycle de l'hôte
Time monitor	Surveillance de la durée

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 MNR initial virtuel (voir 7.1.5 et 7.1.6).

Cycle de protocole F

Une entrée/sortie F renvoie un PDU de sécurité à l'hôte F avec le même MNR 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).

Surveillance du temps de fonctionnement (Chien de garde)

L'arrivée d'un nouveau PDU de sécurité correct dans l'appareil F dans le temps de fonctionnement du chien de garde est surveillée. Cette vérification peut être réalisée aussi souvent que nécessaire, mais au moins une fois à l'issue de l'intervalle de temps de surveillance. À 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 MNR

Un nouveau PDU de sécurité correct se caractérise par le fait que le MNR virtuel au moins passe au MNR virtuel suivant et que tout le reste du PDU de sécurité n'a pas été modifié ou l'a été de manière erronée. Cela signifie qu'un changement incorrect du MNR virtuel est reconnu

directement par CRC2. Cela se traduit alors par une réaction aux anomalies.

Répétition des *PDU de sécurité*

La répétition d'un PDU de sécurité complet n'est pas prise en charge si un nouveau PDU de sécurité correct n'a pas été reçu dans l'intervalle du temps de fonctionnement du chien de garde.

Appareil de surveillance SIL

Chaque message corrompu de toutes les transmissions relatives à une fonction de sécurité (CRC et anomalie MNR virtuelle) est compté pendant une période de temps de l'appareil de surveillance SIL configurable (T). Les valeurs Failsafe sont définies lorsque plusieurs anomalies de ce type se produisent. En d'autres termes, un message corrompu détecté peut être toléré (*variante A*). Ainsi, la préaffectation correspond à un "message corrompu" au démarrage du système. Les cas dans lesquels l'ensemble du PDU du message = "0" (au démarrage, par exemple) ne doit pas être compté.

En réalité, il peut être démontré que le comptage reste effectivement toujours nul. Cela explique la nécessité d'optimiser la complexité donnant la *variante B*, où la période de temps (T) de l'appareil de surveillance SIL est infinie. Dans ce cas, le diagramme d'états simplifié de l'hôte F de la Figure 28 doit être pris en compte lorsque les PDU de sécurité corrompus détectés ne sont pas tolérés et donnent toujours lieu à un état de sécurité.

À chaque fois qu'un message corrompu est détecté de manière inattendue pendant la production ou l'exploitation, l'opérateur responsable joue le rôle d'appareil de surveillance SIL et peut tolérer et acquitter l'indication. Dans le cas d'indications fréquentes à plus de deux reprises au moins par temps de l'appareil de surveillance SIL, il convient d'effectuer une vérification de l'installation (par exemple, perturbations électromagnétiques), du volume de trafic de réseau ou de la qualité de transmission.

Il revient au fabricant de l'hôte F de mettre en œuvre la variante A. Toutefois, une réalisation détaillée n'est pas présentée ici afin de permettre des adaptations individuelles aux environnements système particuliers. L'appareil de surveillance SIL doit uniquement être mis en œuvre dans l'hôte F.

Période de temps de l'appareil de surveillance SIL (T)

La période de temps T de l'appareil de surveillance SIL est une valeur constante intégrant la dimension horaire (h) résultant du SIL demandé et de la longueur CRC configurée (9.5.1). Le Tableau 12 spécifie les temps de l'appareil de surveillance SIL.

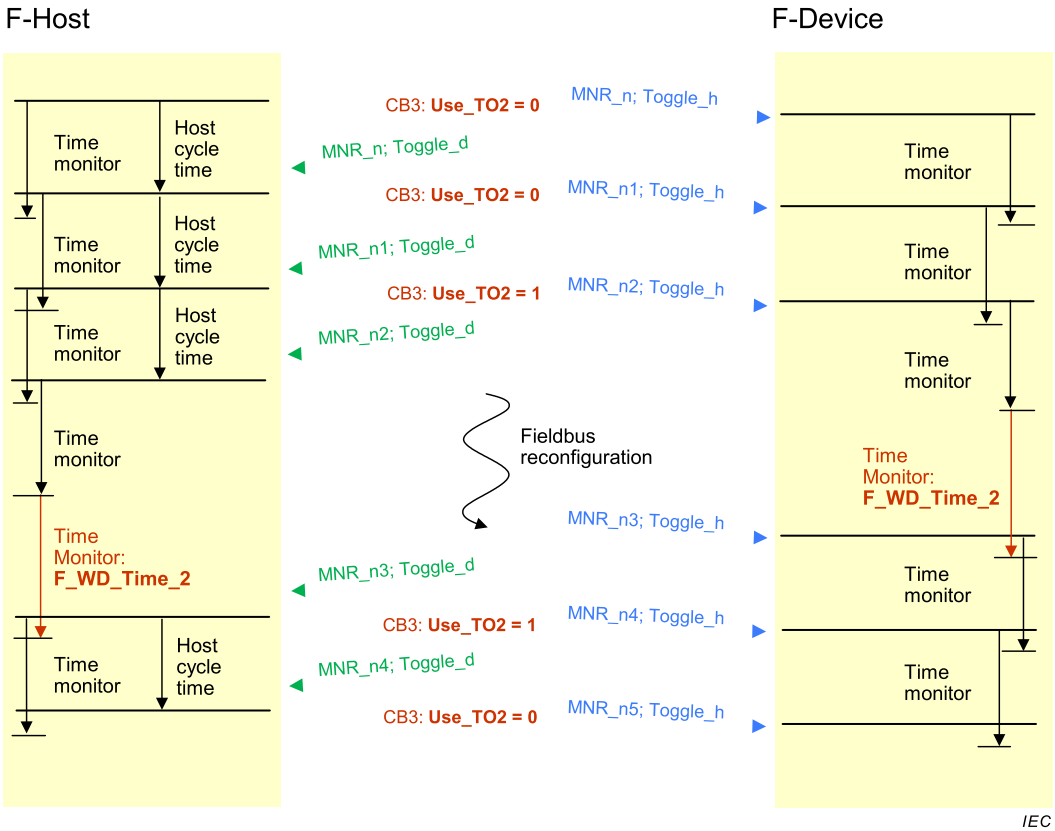
Tableau 12 – Temps de l'appareil de surveillance SIL

SIL	Période de temps (h) protocole BP, LP	Période de temps protocole XP
3	> 100	> 10
2	> 10	> 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» [64] ou la «maintenance des systèmes de tolérance aux pannes», un certain temps est nécessaire à la mise à jour des appareils concernés. En règle générale, ce temps de mise à jour est plus long que le temps

de fonctionnement du chien de garde principal régulier (F_WD_Time) défini pour une application de sécurité. Afin d'éviter des déclenchements de nuisance, le pilote de l'hôte F peut utiliser uniquement une seule fois (voir Figure 41) un temps de fonctionnement du chien de garde secondaire (F_WD_Time_2) pour étendre le temps de fonctionnement du chien de garde principal de ces cas présentés à la Figure 39.



Anglais	Français
F-host	Hôte F
F-Device	Appareil F
Time monitor	Surveillance de la durée
Host cycle time	Durée de cycle de l'hôte
Fieldbus reconfiguration	Reconfiguration du bus de terrain

Figure 39 – Temps de fonctionnement étendu du chien de garde à la demande

L'hôte F doit définir et réinitialiser le bit 3 (Use_TO2 de l'octet de contrôle pour tous les appareils F, affectant ainsi simultanément tous ces appareils (voir 6.1).

7.3 Réaction en cas de dysfonctionnement

7.3.1 Répétition indésirable

Déclaration: «Le dysfonctionnement d'un appareil de bus génère d'anciens PDU de sécurité obsolètes répétés au moment inopportun, ce qui risque de gêner dangereusement le destinataire (l'appareil de sûreté est signalé comme étant fermé alors qu'il a déjà été ouvert, par exemple).»

Solution palliative: Les données internes au canal noir 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 (sollicitation)

d'urgence peut donc correspondre à un *temps de fonctionnement du chien de garde (voir 9.3.3)*.

NOTE «Déclaration» fait référence aux dysfonctionnements correspondants dans l'article «erreurs de communication» de l'IEC 61784-3:-.

7.3.2 Perte

Déclaration: «Le dysfonctionnement d'un appareil de bus supprime un PDU de sécurité (demande d' "arrêt technique de sécurité", par exemple)».

Solution palliative: Les informations perdues sont découvertes par une modification et un examen rigoureux du MNR et/ou du temps de fonctionnement du chien de garde de la couche de communication de sécurité du destinataire respectif.

7.3.3 Insertion

Déclaration: «Le dysfonctionnement d'un appareil de bus insère un PDU de sécurité (désélection de l' "arrêt technique de sécurité", par exemple)».

Solution palliative: En raison d'une attente d'un MNR rigoureusement séquentiel, le destinataire détecte un PDU de sécurité inséré.

7.3.4 Séquence incorrecte

Déclaration: «Le dysfonctionnement d'un appareil de bus modifie la séquence du PDU de sécurité. Exemple: Avant de procéder à l'arrêt technique de sécurité, l'opérateur souhaite sélectionner la vitesse limitée de sécurité. Si ces PDU de sécurité ne sont pas clairs, la machine fonctionne au lieu de s'arrêter.»

Solution palliative: En raison d'une attente d'un MNR rigoureusement séquentiel, le destinataire reconnaît une séquence incorrecte.

7.3.5 Corruption des données de sécurité

Déclaration: «Le dysfonctionnement d'un appareil de bus ou de la liaison de transmission perturbe les PDU de sécurité.»

Solution palliative: La signature CRC2 reconnaît une perturbation des données entre l'émetteur et le destinataire.

La signature CRC2 est générée par l'intermédiaire des paramètres F respectivement, des données d'entrée-sortie F, du MNR virtuel et de l'octet de contrôle/d'état (voir 7.1.7, 7.1.8, Figure 24 et Figure 26).

7.3.6 Délai inacceptable

Déclaration: "*1*. Le volume d'échange de données opérationnelles dépasse la capacité de la liaison de communication. *2*. Un appareil de bus provoque une situation de surcharge en simulant des PDU de sécurité incorrects, causant le retard ou l'empêchement d'un service appartenant au PDU de sécurité.»

Solution palliative:

- Le bit de basculement dans l'octet de contrôle et l'octet d'état (voir 7.1.3).
- 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 appareil de bus provoque le mélange des PDU de sécurité, des PDU de sécurité mal acheminés et des PDU qui ne sont pas de sécurité".

Solution palliative: Le destinataire détecte les PDU (de sécurité) des émetteurs avec une authenticité incorrecte par l'intermédiaire de la signature CRC2. Il est possible d' exclure la possibilité qu'un émetteur non relatif à la sécurité ou non autorisé soit capable de générer un PDU de sécurité FSCP 3/1 attendu avec le CRC2 correct.

7.3.8 Adressage

Principe d'authentification de connexion sécurisée:

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 la connexion étant donné que le nom de code et la direction sont inclus dans le CRC via MNR (voir 7.1.7, 7.1.8 et 7.3.10).

Le nom de code ("F_S/D_Address") peut être soigneusement sélectionné dans les appareils individuels selon l'une des méthodes suivantes:

– codage du commutateur dans l'unité correspondant au nom de code;
– un paramétrage unique d'appareil par un logiciel qui exige une vérification si le bon appareil a été adressé. L'opération doit être répétée lorsque cette unité est remplacée;
– mécanismes d'adressage indépendants de l'adressage CPF 3.

Le sabotage n'est pas pris en compte.

7.3.9 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 appareil de bus provoque une situation de surcharge en simulant des messages incorrects, causant le retard ou l'empêchement d'un service appartenant aux PDU de sécurité intégrés.»

Voir la Figure 9 et la Figure 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 lorsque l'émetteur a déjà été arrêté. Le Tableau 13 contient une liste des anomalies de commutation possibles et leurs solutions palliatives visant à assurer une sécurité suffisante.

Tableau 13 – Solutions aux anomalies de commutation

Type d'anomalie	Détection et maîtrise
Données perturbées	Signature CRC (24/32 bits)
Mauvaise destination	Nom de code (2 x 16 bits)
Perte de message de sécurité	MonitoringNumber (24/32 bits) et temporisation
Message en double	MonitoringNumber (24/32 bits)
Message retardé	Temporisation
Retransmission des messages stockés avec moins de 3 PDU de sécurité consécutifs en série. L'hôte F n'est plus connecté.	MonitoringNumber (24/32 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.	MonitoringNumber (24/32 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 MNR. L'appareil F reconnaît une anomalie MNR et définit des valeurs Failsafe (FV).

– Un seul message de la mémoire tampon de commutation est retransmis et comporte un PDU de sécurité avec le bon MNR. Cette anomalie est détectée à cause du MNR à 24/32 bits et du fait que le redémarrage de l'appareil de sortie F nécessite 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 MNR, la séquence de ce message commençant dans le temps de fonctionnement du chien de garde de sécurité. Cette anomalie est détectée à cause du MNR à 24/32 bits et du fait que le redémarrage de l'appareil de sortie F nécessite un OA_C = 1 (Acquittement de l'opérateur).

7.3.10 Bouclage

Déclaration: "La fonction d'acheminement programmable d'un appareil de bus réachemine de manière involontaire un message de l'hôte F vers ce même hôte, qui attend un PDU de sécurité de même longueur".

Solution palliative:

F_CRC_Seed = 0: L'hôte F vérifie le bouclage via le bit 7 de l'octet d'état (voir Figure 19) et l'appareil de sortie F détecte le bouclage via la temporisation;

F_CRC_Seed= 1: Le calcul de la signature CRC2 de et vers l'hôte F utilise différents algorithmes MNR (élément complémentaire unique).

7.3.11 Limites du réseau et routeur

Déclaration: "1. Le volume d'échange de données opérationnelles dépasse la capacité de la liaison de communication. *2* Un appareil de bus provoque une situation de surcharge en simulant des messages incorrects, causant le retard ou l'empêchement d'un service appartenant aux PDU de sécurité intégrés."

Pour les réseaux CP 3/RTE équipés de routeurs, la Figure 11 et les explications correspondantes s'appliquent. Un système de ce type composé de sous-réseaux connectés par des routeurs est considéré pour les considérations ci-dessous. Ces considérations démontrent qu'une seule erreur ne peut être à l'origine de la transmission inappropriée d'un PDU de sécurité vers le mauvais appareil F, ni de son passage à un état dangereux.

Le routeur connecte deux sous-réseaux ou plus sur des niveaux de couche 3. Chaque hôte F et appareil 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 14 contient une liste des types d'anomalie et des contraintes liées à une opération de routeur pour obtenir un niveau de sécurité suffisant.

Tableau 14 – Limites du réseau de sécurité

Type d'anomalie	Conséquences	Détection et maîtrise
Le routeur ne détient pas la bonne adresse d'un appareil F	Le routeur reçoit un message pour cet appareil F particulier. Résultat: cible introuvable.	Temporisation de l'appareil F
Deux appareils 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) Appareil F du sous-réseau 0 introuvable dans le sous-réseau 0 2) Impossible d'atteindre l'appareil F du sous-réseau 0 dans le sous-réseau 1 3) Impossible d'atteindre l'appareil F du sous-réseau 1 dans le sous-réseau 0 4) Appareil F du sous-réseau 1 correct dans le sous-réseau 1	Par CP 3/RTE standard
Deux appareils 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) Appareil F 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 changement des paramètres lors de l'exécution

7.4.1 Procédure de démarrage standard

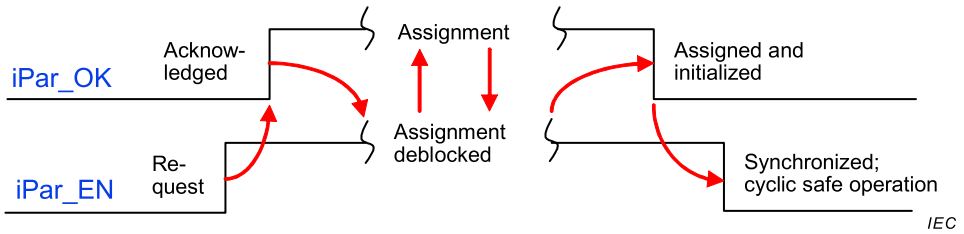
Le démarrage des appareils/modules F est indépendant du profil CP 3/RTE standard. Les couches de sécurité de l'hôte F et de l'appareil F commencent d'elles-mêmes à chaque établissement de la communication CP 3/RTE. Les éléments déjà exécutés des couches de sécurité et leurs paramètres F spéciaux sont intégrés dans le processus normal de configuration et de paramétrage («Contexte») de CP 3/RTE. Toutes les répétitions des éléments du paramètre F portant des valeurs identiques lors de l'exécution doivent être ignorées et les valeurs qui s'écartent doivent être rejetées ou doivent générer un état de sécurité.

Voir le document [50], l'IEC 61158-5-10 et l'IEC 61158-6-10 pour des informations relatives aux séquences de démarrage d'un contrôleur d'entrée-sortie et de ses appareils d'entrée-sortie, qui font partie intégrante des appareils F.

7.4.2 Déblocage de l'attribution d'iParamètres

En raison d'un message de diagnostic de l'appareil F nécessitant des iParamètres supplémentaires (8.2) ou après une demande externe, l'hôte F définit le bit 0 («Attribution d'iParamètres débloquée» = "iPar_EN") 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), l'appareil F/module F reçoivent les iParamètres et procèdent à un acquittement à la fin en définissant le bit 0 («De nouvelles valeurs iParamètre ont été attribuées à l'appareil F» ="iPar_OK") dans l'octet d'état de son PDU de sécurité suivant (Figure 40).

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 40 est un exemple d'application possible.



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 40 – Déblocage de l'attribution d'iParamètres 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 appareils 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 [40] et [43]). De plus, les paramètres F exigés 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 l'appareil/module F (valeur par défaut dans le fichier GSD: temps de traitement maximal de l'appareil/module F)
- F_WD_Time_2 — Temps de fonctionnement du chien de garde secondaire dans les appareils/modules F conçus pour la «configuration en cours» ou la «maintenance des systèmes de tolérance aux anomalies". L'outil de développement calcule et définit la valeur (avec des réserves pour les sessions "CiR" futures) lors de la mise en service (7.2.6.2)
- F_Prm_Flag1 + 2 — Octets du paramètre contenant plusieurs paramètres de gestion de profil
  - F_Check_SeqNr — Mode V2: le MNR est toujours inclus dans le calcul de CRC2
  - F_Check_iPar — Utilisation spécifique au fabricant dans des systèmes homogènes
  - F_SIL — Vérification: SIL configuré = SIL utilisé ?
  - F_CRC_Length — Longueur de signature CRC2
  - F_CRC_Seed — Utilisation de différentes règles pour la valeur de départ CRC et le MNR pour le calcul de la signature CRC2 (voir Figure 47)
  - F_Passivation — Appareil/Module F ou Passivation granulaire des canaux [66]

  - F_Block_ID — Identification du type de blocage de paramètre
  - F_Par_Version — Numéro de version des paramètres F/du mode opérationnel FSCP 3/1
- F_iPar_CRC — Valeur du calcul de la signature CRC d'iParamètres, au moins manuellement transférée d'un outil CPD vers l'outil de développement
- F_Par_CRC — Calcul de la signature CRC des paramètres F afin de sécuriser le transfert entre l'hôte F et l'appareil F

8.1.2 F_Source/Destination_Address (Nom de code)

Les noms de codes des relations de communication de sécurité 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 où le UDP RT CLASS n'est pas admis ou pas pris en charge (5.4.2). En local, chaque appareil 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). La relation est soigneusement stockée dans les appareils F, fait partie intégrante de l'ensemble de paramètres F et, par conséquent, est vérifiée 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*. En règle générale, elles sont représentées à partir de l'hôte F (comme source) et de l'appareil F (comme destination) pendant la configuration (7.3.7). Les adresses *0* et *0xFFFF* doivent être *exclues*.

Le paramètre est composé de deux parties: "F_Source_Add" et "F_Dest_Add", chacune appartenant au type de données Unsigned16. Le Tableau 15 spécifie l'ordre des octets du nom de code (F_Source/Destination_Address).

Tableau 15 – Ordre des octets de nom de code

Nom de code			
Octet de poids fort	octet	octet	Octet de poids faible
F_Source_Address		**F_Dest_Address**	
Octet de poids fort	Octet de poids faible	Octet de poids fort	Octet de poids faible

8.1.3 F_WD_Time (temps de fonctionnement du chien de garde F)

En local, chaque appareil 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 MNR.

Ce paramètre F_WD_Time est codé comme suit: Unsigned16. Base de temps: *1 ms*. La plage de valeurs est comprise entre 1 et 65 535.

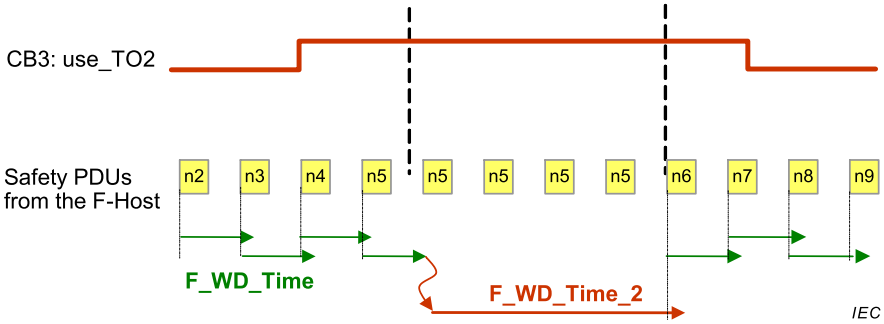
Voir 9.3.3 pour plus de détails sur la manière dont ces temps de fonctionnement du chien de garde s'intègrent dans l'ensemble de la définition des temps de réponse de la fonction de sécurité (SFRT) et sur la manière de les déterminer.

Le fabricant d'un appareil F attribue le temps maximal d'acquittement de l'appareil (DAT) à la valeur par défaut du paramètre F_WD_Time dans le fichier GSD. Un outil de développement 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 paramètre F peut être éventuellement utilisé pour étendre le F-WD_Time régulier d'un temps de fonctionnement F_WD_Time_2 supplémentaire via le bit 3 de l'octet de contrôle tel que démontré à la Figure 41 (MNR "n5"). Ce temps supplémentaire est exigé pour la mise à jour de la configuration des appareils/modules F.



Anglais	Français
Safety PDUs from the F-Host	PDU de sécurité de l'hôte F

Figure 41 – Effet de F_WD_Time_2

Le paramètre F_WD_Time_2 est codé comme suit: Unsigned16. Base de temps: *1 ms*. La plage de valeurs est comprise entre 1 et 65 535. CB3 = 1 ("use_TO2") est un indicateur destiné aux appareils F pour l'activation du temps de fonctionnement F_WD_Time_2 une seule fois uniquement. Le temps de fonctionnement F_WD_Time normal démarre immédiatement après la réception du PDU de sécurité suivant avec un nouveau MNR. Préalablement à un redémarrage du temps de fonctionnement F_WD_Time_2, l'hôte F doit réinitialiser CB3 après écoulement de F_WD_Time_2.

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 42:

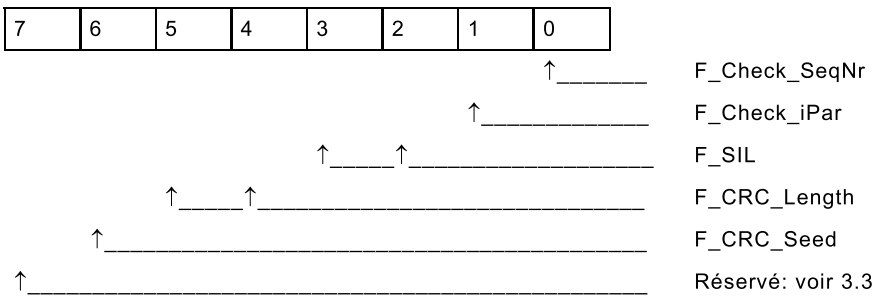


Figure 42 – F_Prm_Flag1

8.1.5.2 F_Check_SeqNr (MNR dans CRC2)

Ce paramètre détermine si le MNR doit ou non être inclus dans la signature CRC2 (voir Figure 43). 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

7	6	5	4	3	2	1	0

0 = Pas de vérification (inutile en mode V2; la notation dans GSD doit être «NoCheck»)

1 = Vérification (inutile en mode V2; la notation dans GSD doit être «Check»)

Figure 43 – 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. Ce paramètre est réservé au fabricant dans les systèmes homogènes. Il n'est pas lié au mécanisme de serveur d'iParamètres.

Il est codé comme suit: Bit 1 de l'octet de paramètre "F_Prm_Flag1" (voir Figure 44).

7	6	5	4	3	2	1	0

0 = Pas de vérification (la notation dans GSD doit être «NoCheck»)

1 = Vérification (utilisation spécifique au fabricant; la notation dans GSD doit être «Check»)

Figure 44 – 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 de sécurité. Les différentes fonctions de sécurité utilisant la communication de sécurité peuvent exiger différents niveaux d'intégrité de sécurité (SIL 1 à SIL 3). Les appareils F sont capables de comparer le SIL qui leur a été attribué au SIL configuré (F_SIL). Si le niveau d'intégrité de sécurité est supérieur à celui de l'appareil/module F configuré, une valeur est attribuée au bit d'état de la «défaillance de l'appareil», ce qui déclenche une réaction d'état de sécurité. Il existe quatre phases différentes: SIL 1 à SIL 3, NoSIL (voir Figure 45).

Il est codé comme suit: Bits 2 et 3 de l'octet de paramètre F_Prm_Flag1.

7	6	5	4	3	2	1	0

0 0 = SIL 1 (la notation dans GSD doit être «SIL1»)

0 1 = SIL 2 (la notation dans GSD doit être «SIL2»)

1 0 = SIL 3 (la notation dans GSD doit être «SIL3»)

1 1 = Pas de SIL (la notation dans GSD doit être «NoSIL»): dans les appareils d'automatisme industriel, par exemple

Figure 45 – F_SIL

8.1.5.5 F_CRC_Length (longueur de la signature CRC2)

Selon le paramètre F_CRC_Seed, une signature CRC2 de 3 ou 4 octets est exigée (voir Figure 46). 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; la notation dans GSD doit être «3-Byte-CRC»)
		0	1					=	Cette attribution de paramètre ne doit pas être utilisée pour les nouveaux développements
		1	0					=	Signature CRC2 à 4 octets; la notation dans GSD doit être «4-Byte-CRC»)
		1	1					=	Réservé

Figure 46 – F_CRC_Length

8.1.5.6 F_CRC_Seed (Valeur initiale pour CRC2)

Avec F_CRC_Seed =0, l'appareil/module F indique l'utilisation de CRC_FP (16 bits) comme valeur de départ et d'un compteur en tant que MNR pour une intégration dans le calcul de la signature CRC2 (voir 7.1.5 et 7.1.7) selon les versions de protocole précédentes.

Avec F_CRC_Seed =1, l'appareil/module F indique l'utilisation de la valeur “1” comme valeur de départ, le protocole CRC-FP+, et le MonitoringNumber virtuel établi sur le nom de code pour une intégration dans la signature CRC2 (voir 7.1.6 et 7.1.8).

L'outil de développement d'un hôte F ajuste son pilote selon cette entrée. Le paramètre est distribué à l'appareil/module F au cours du démarrage.

Il est codé comme suit (voir Figure 47): Bit 6 de l’octet de paramètre F_Prm_Flag1

7	6	5	4	3	2	1	0		
	0							=	CRC-FP en tant que valeur de départ et compteur (la notation dans GSD est "CRC-Seed16")
	1							=	"1" en tant que valeur de départ et CRC-FP+/MNR (la notation dans GSD est "CRC-Seed24/32"

Figure 47 – F_CRC_Seed

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 8.1.6.3 à 8.1.6.4 décrivent les caractéristiques de l’octet du paramètre F_Prm_Flag2. Sa structure est présentée dans la Figure 48.

7	6	5	4	3	2	1	0	
							↑_____	F_Passivation
					↑_____	↑_____		Réservé: voir 3.3
		↑_____	↑_____	↑_____				F_Block_ID
↑_____	↑_____							F_Par_Version

Figure 48 – F_Prm_Flag2

8.1.6.2 F_Passivation

Les indications données en 6.1 et à la Figure 16 décrivent le concept de passivation granulaire des canaux (CGP) par opposition à la passivation complète des appareils/modules F. Un outil de développement de l'hôte F définit ce paramètre sur "0" lorsqu'un hôte F ne prend pas en charge la CGP (voir Figure 49). Un appareil/module F qui prend en charge la CGP doit vérifier ce paramètre "F_Passivation".

7	6	5	4	3	2	1	0		
							0	=	Passivation de l'appareil/module F du fait de "Device_Fault" (la notation dans GSD doit être "Device/Module")
							1	=	Passivation granulaire des canaux (CGP) du fait d'anomalies de canal de signalisation individuel en utilisant le modèle de qualificatif de [66] (la notation dans GSD doit être "Channel")

Figure 49 – F_Passivation

8.1.6.3 F_Block_ID (identification du type de paramètres)

Pour distinguer les paramètres des modes FSCP 3/1 ultérieurs, l'identification du type de paramètre "F_Block_ID" est codée de la manière suivante: Bits 3, 4 et 5 de l'octet de paramètre "F_Prm_Flag2" (voir Figure 50). Il est obligatoire pour permettre à la couche de sécurité de vérifier F_Block_ID.

7	6	5	4	3	2	1	0		
		0	0	0				=	No F_WD_Time_2, no F_iPar_CRC
		0	0	1				=	No F_WD_Time_2, F_iPar_CRC
		0	1	0				=	F_WD_Time_2, no F_iPar_CRC
		0	1	1				=	F_WD_Time_2, F_iPar_CRC
		1	0	0				=	Réservé
		1	0	1				=	Réservé
		1	1	0				=	Réservé
		1	1	1				=	Réservé

Figure 50 – F_Block_ID

8.1.6.4 F_Par_Version (numéro de version de l'ensemble de paramètres F)

Ce compteur de versions a pour objet d'identifier les nouvelles versions d'un mode opérationnel à l'intérieur de la couche de sécurité. L'appareil F doit répondre par un message de diagnostic spécifique à l'appareil dans le cas où la version demandée de la couche de sécurité ne correspond pas à celle mise en œuvre (voir 6.3.2 et Figure 51). 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							=	Mode V1 hérité, qui ne doit pas être utilisé pour de nouvelles mises en œuvre (la notation dans GSD doit être "V1-mode")
0	1							=	Valide pour le mode V2 (la notation dans GSD doit être "V2-mode")
1	0							=	Réservé
1	1							=	Réservé

Figure 51 – F_Par_Version

8.1.7 F_iPar_CRC (valeur d'iPar_CRC dans iParamètres)

L'outil CPD d'un appareil F particulier calcule une signature CRC (iPar_CRC) entre tous les iParamètres lorsque la session de paramétrage et de mise en service a abouti. Si le résultat du calcul est "0", la valeur doit être définie sur "1". La valeur de départ CRC recommandée pour ce calcul est "1". La valeur au format *hexadécimal* doit être transférée au moins manuellement à l'outil de développement et attribuée au champ d'entrée "F_iPar_CRC".

Ce paramètre est transmis à l'appareil F lors du démarrage et est utilisé dans le cadre d'un contrôle de cohérence iParamètre dans l'appareil F avant de commencer une opération de

sécurité normale. En "mode d'essai FSCP" (8.6.4.5) d'un appareil F, la valeur "0" doit être attribuée à ce paramètre. Dans ce cas, l'appareil F ignore le contrôle de cohérence. À chaque fois que l'appareil F reconnaît une discordance entre la signature iPar_CRC calculée en local et la valeur de F_iPar_CRC, il doit définir des valeurs Failsafe (FV).

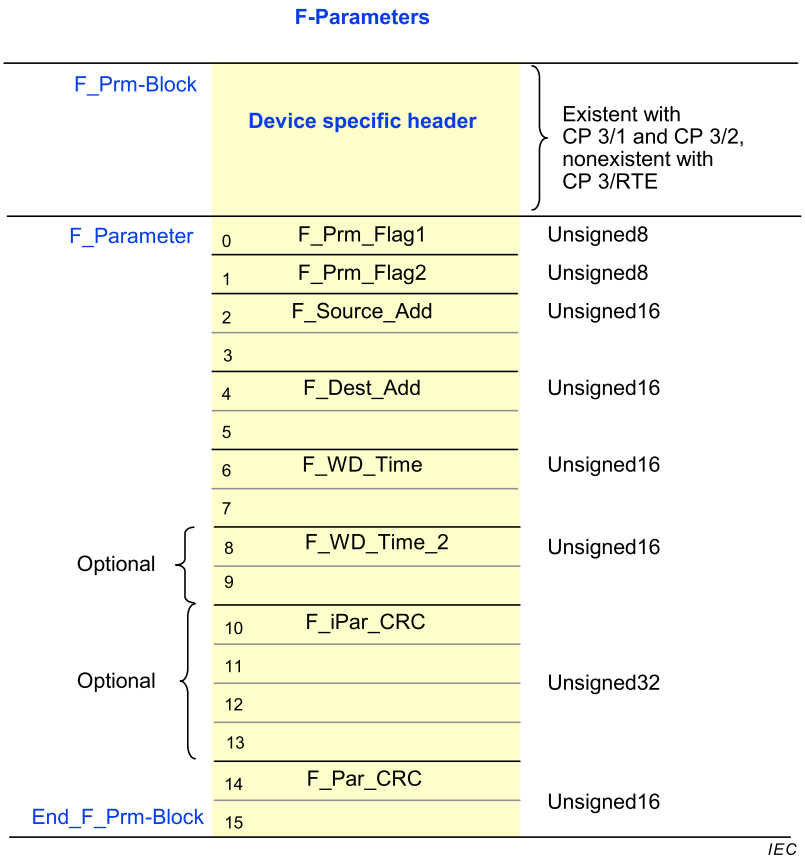
Ce paramètre est facultatif. Le bit 3 du paramètre F «F_Prm_Flag2» indique sa présence. Il est codé comme suit: Unsigned32

8.1.8 Calcul de F_Par_CRC (entre les paramètres F)

L'outil de développement génère cette signature CRC entre les paramètres F. La valeur de départ pour cette signature CRC est "0". Voir 8.3.3.2 pour plus de détails sur l'ordre des paramètres F qui doivent être utilisés pour générer cette signature CRC. Le polynôme générateur CRC 16 bits (*0x4EAB*) est utilisé.

Il est codé comme suit: Unsigned16.

8.1.9 Structure de l'objet de données d'enregistrement du paramètre F



Anglais	Français
F-parameters	Paramètres F
Device specific header	En-tête spécifique à l'appareil
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 52 – Paramètre F

La Figure 52 représente la structure du bloc de paramètres F dans un objet de données d'enregistrement CP 3/RTE. L'ordre des octets est conforme au protocole CP 3/RTE

standard. Les éléments suivants s'appliquent aux appareils F modulaires: Pour chaque module F, un bloc de paramètres F est inséré dans le message de contexte (Figure 13). Le module F peut être alloué à l'appareil F via le numéro de sous-intervalle.

8.2 iParamètre et iPar_CRC

Les appareils F sont de plus en plus équipés de fonctions intelligentes qui exigent l'attribution de nombreuses valeurs de paramètre d'appareil F individuelles. Ces paramètres relatifs à la sécurité sont appelés iParamètres. En particulier, si un appareil 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 la 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.

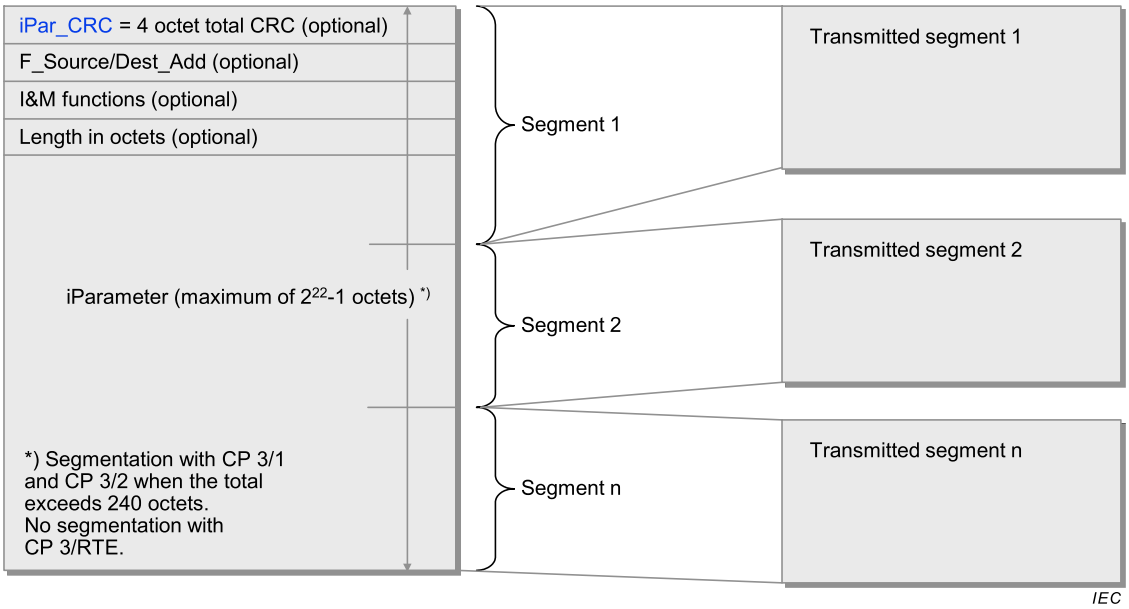
La Figure 53 présente une proposition de structure de grandes quantités d'iParamètres aux fins de téléchargement amont et aval des données. La limite supérieure absolue des iParamètres est de 2^{22}-1 octets, la limite inférieure étant de 4 octets. Par conséquent, une segmentation est exigée avec CP 3/1 lorsque le total dépasse 240 octets comme présenté à la Figure 53. Aucune segmentation n'est exigée avec CP 3/RTE.

La signature CRC ("iPar_CRC") doit être calculée entre les iParamètres (Figure 53) à l'aide d'un polynôme CRC approprié, et intégrée dans l'iPar_CRC à 4 octets au format hexadécimal, puis affichée dans l'outil CPD. Si le résultat du calcul est "0", la valeur doit être définie sur "1". La valeur de départ CRC recommandée pour ce calcul est "1". L'introduction de la valeur iPar_CRC dans les iParamètres comme présenté à la Figure 53 est facultative. Aucune preuve de sécurité du taux d'erreurs résiduelles suffisant n'est exigée lors de l'utilisation du polynôme CRC à 32 bits FSCP 3/1.

La relation F_source/destination (nom de code) permet de vérifier la remise au destinataire configuré. L'introduction dans les iParamètres comme présenté à la Figure 53 est facultative.

Les fonctions d'identification et de maintenance (I&M) sont obligatoires pour tous les appareils CPF 3. Elles fournissent des codes permettant d'identifier le type et la version d'un appareil/module particulier. L'introduction de ce type d'informations dans l'ensemble d'iParamètres peut être utilisée pour vérifier la validité d'un appareil de remplacement avec ses propres fonctions I&M. L'introduction dans les iParamètres comme présenté à la Figure 53 est facultative. Les fabricants d'appareils peuvent utiliser leurs codages personnels.

La longueur du bloc iParamètre peut être utile à l'organisation efficace des processus de téléchargement amont et aval des données dans les appareils. L'introduction dans les iParamètres comme présenté à la Figure 53 est facultative.



Anglais	Français
4 octet total CRC	CRC total de 4 octets
(optional)	(facultatif)
Transmitted segment	Segment transmis
I&M functions	Fonctions I&M
Length in octets	Longueur en octets
iParameter (maximum of 2^{22}- 1 octets)	iParamètre (maximum de 2^{22}- 1 octets)
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 53 – 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 iParamètres des appareils F en raison des nombreuses manipulations des appareils de terrain dans les industries de fabrication et de transformation. L'un des principaux objectifs consiste à maintenir la stabilité d'un petit ensemble défini de paramètres F (niveau de communication) entre tous les appareils F et à fournir des interfaces d'iParamétrage afin de limiter la dépendance entre le fabricant du système et celui de l'appareil et donc, à 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 [44] et le fabricant de l'appareil 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 présenté ici. À 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 spécifié en 8.6.4.

Le petit ensemble de paramètres F identiques des différents appareils 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 ainsi 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 paramètres F est compilé et stocké 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 n'est donc pas transféré vers l'appareil 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 appareils orientés module physique ou virtuel. Par conséquent, la spécification du langage de description générale de station (General Station Description Language ou GSDL) [40] pour le type 3 défini dans l'IEC 61158 définit les mots clés visant à structurer et identifier les informations de bloc de paramètres F des modules F présentés à la Figure 52. Les sélections de valeurs possibles du paramètre F se trouvent dans un fichier de description générale de station (GSD associé à un esclave F du module F pour lequel il est conçu. Les mots clés ci-dessous du Tableau 16 sont définis.

Tableau 16 – 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 52.
F_Ext_Module_Prm_Data_Const (décalage)	À 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 52. 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)	À l'aide du paramètre associé à ce mot clé, une valeur sélectionnable par l'utilisateur au moment de la configuration peut être entrée dans l'un des octets 0 à 13 du bloc F_Prm présenté dans la Figure 52. La position d'un octet est indiquée par un décalage 4 à 16. Le paramètre pointe vers une définition de plage ExtUserPrmData dans les autres parties du fichier GSD
F_ParamDescCRC	Le paramètre associé à ce mot clé protège les parties relatives à la sécurité des descriptions du paramètre F dans le fichier GSD. Voir 8.3.3.3 pour plus 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 [40] et 8.4.1 pour plus de 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

Mot clé GSDL	Description
	indiquant une signature CRC7 32 bits. Si cet attribut est absent, la valeur 1 est considérée 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 appareil F particulier sont définis à l'aide de son fichier GSD. La description est fournie en langage de balisage de description générale de station (GSDML) pour le type 10 défini dans l'IEC 61158, basé sur le langage XML (voir [43]).

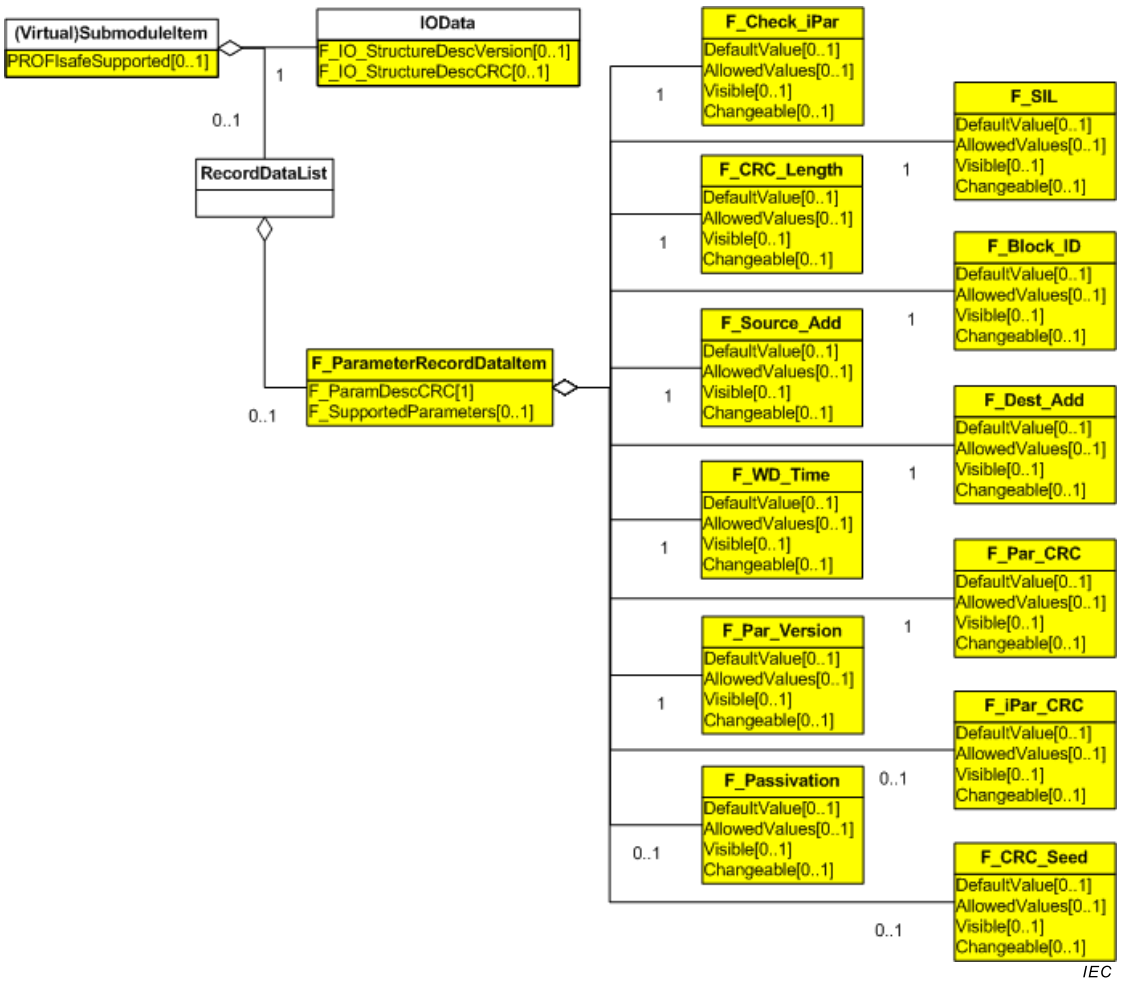


Figure 54 – Extension du paramètre F dans la spécification GSDML

La Figure 54 représente les extensions en langage GSDML. L'élément "(Virtual)SubmoduleItem" fournit les attributs suivants:

- "F_ParamDescCRC": Il s'agit de la signature CRC (CRC0) de la description du paramètre F selon la Figure 54.
- "F_SupportedParameters": Indication directe des paramètres F facultatifs pris en charge dans l'enregistrement de ces mêmes paramètres (information décodée de "F_Block_ID"). Pour plus de détails, voir [43].

Le "F_IO_StructureDescCRC" de l'élément "IOData" protège les formats des données d'entrée F et de sortie F. La "F_IO_StructureDescVersion" indique la version d'une structure de données d'entrée-sortie F (voir 8.3.3).

Dans le langage GSDML, les paramètres F F_CRC_Seed et F_Passivation sont facultatifs. Les deux paramètres doivent être présents ou aucun de ces deux paramètres ne doit être présent. Leur présence indique la prise en charge du protocole FSCP3 conformément à la présente norme. Pour empêcher l'interruption des outils de développement par la présence des nouveaux paramètres F, intégrer l'attribut RequiredSchemaVersion= "V2.31" à la description du module F.

En cas de rétrocompatibilité avec les versions de protocole précédentes, un module F doit être décrit une seconde fois dans le fichier GSD sans F_CRC_Seed et F_Passivation, mais avec F_CRC_Length=3-Byte-CRC à la place de 4-Byte-CRC.

Les modules F qui prennent en charge les deux paramétrages de F_Passivation exigent également des ensembles séparés de descriptions dans le fichier GSD en raison des différents formats de données d'entrée-sortie avec ou sans qualificatifs.

Bien que le fichier GSD comporte plusieurs descriptions du même module F, il n'est pas nécessaire qu'il contienne différents IdentNumbers (voir [69]).

8.3.3 Protection des paramètres de sécurité et des données GSD

8.3.3.1 Généralités

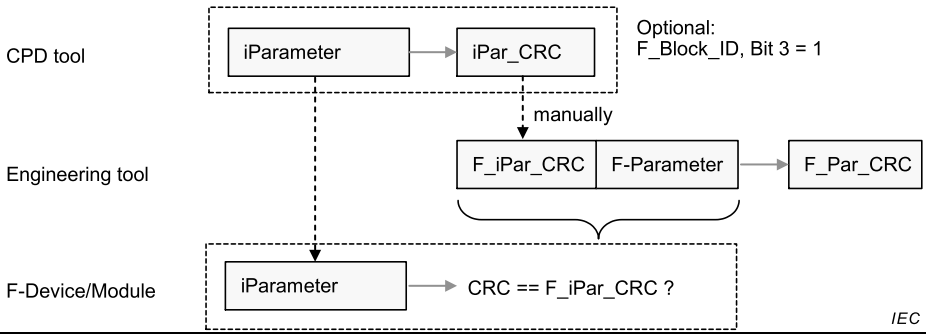
Il est essentiel pour la sécurité du système de protéger les paramètres de sécurité de la couche de sécurité (paramètres F) et de la technologie de sécurité de l'appareil F (iParamètres), ainsi que les structures de données d'entrée-sortie de sécurité configurées. Cette protection est assurée par les signatures CRC, leur stockage définitif dans l'appareil F et l'hôte F et une comparaison régulière des signatures CRC.

Pour éviter que l'outil de développement n'utilise des données de description d'appareil perturbées (GSD), les parties relatives à la sécurité qui le composent sont également protégées par signature CRC.

8.3.3.2 F_Par_CRC et iPar_CRC entre les paramètres de sécurité

La Figure 23 représente uniquement la signature CRC1 des paramètres F qui doivent être concernés par le processus de génération de signature CRC2. Toutefois, d'autres signatures CRC peuvent éventuellement être concernées, comme indiqué ci-après en 8.3.3.2.

Pour protéger les paramètres F, l'outil technique de l'hôte F génère la signature *F_Par_CRC* comme décrit en 8.1.7. Le polynôme CRC qui doit être utilisé est *0x4EAB*. La signature CRC est conçue entre tous les paramètres F dans l'ordre des octets indiqué dans la Figure 52, à l'exclusion de F_iPar_CRC facultatif. À chaque fois que la valeur 1 est attribuée au bit 3 du paramètre F «F_Block_ID», la signature F_iPar_CRC doit être placée au début du calcul comme présenté à la Figure 55.



Anglais	Français
Optional	Facultatif
CPD tool	Outil CPD
IParameter	IParamètre
Engineering tool	Outil de développement
Manually	Manuellement
F-parameter	Paramètre F
F-device/module	Appareil/module F

Figure 55 – Signature F_Par_CRC incluant iPar_CRC

Cette procédure doit également être utilisée pour le calcul de CRC_FP (voir 7.1.7) et de CRC_FP+ (voir 7.1.8).

8.3.3.3 CRC0 entre les données GSD

Pour s'assurer que les paramètres relatifs à la sécurité de l'appareil F ne changent pas de manière inaperçue au cours du cycle de vie d'un support de stockage et peuvent être lus en toute sécurité dans l'outil de configuration, ces paramètres sont tous protégés par signature CRC. Le paramètre "F_ParamDescCRC" contient une signature CRC à 2 octets (CRC0) générée à l'aide du même polynôme CRC 16 bits (*0x4EAB*) que celui utilisé avec l'ensemble du protocole FSCP 3/1. La Figure 56 décrit l'algorithme de sérialisation et de calcul.

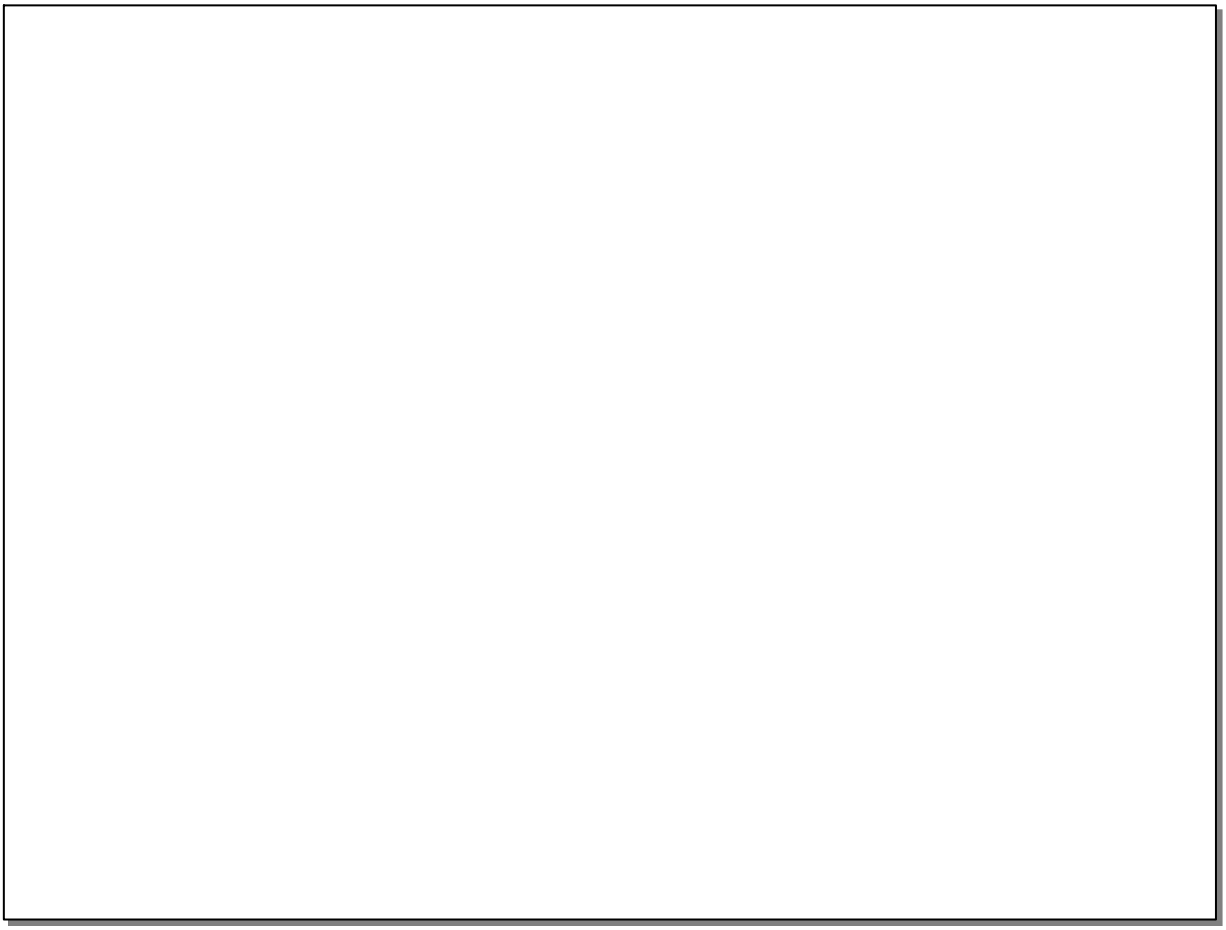


Figure 56 – Algorithme de génération de CRC0

Dans le cas d'un fichier GSD dédié à un esclave F (CP 3/1 ou CP 3/2), les règles d'annotation GSDL suivantes s'appliquent pour le calcul de la signature CRC0 (voir l'exemple du Tableau 17 et du Tableau 18):

- Si un paramètre F non inclus dans l'ensemble F_Check_SeqNr, F_Check_iPar, F_CRC_Length, F_CRC_Seed, F_Passivation, F_Block_ID est omis dans le fichier GSD, une valeur fixe nulle est considérée et ce paramètre ne doit pas être inclus dans le calcul de CRC0.
- Les mots clés F_Ext_User_Prm_Data_Const doivent être ignorés.
- Dans le cas où les paramètres F sont décrits sous une forme de structure de bloc (voir les mots clés Prm_Block_Structure_supp / ..._req), les mots clés F_Ext_User_Prm_Data_Ref dirigés vers l'en-tête de bloc doivent être ignorés.
- Le mot clé F_Ext_User_Prm_Data_Ref est dirigé vers les ExtUserPrmData où le nom des paramètres F, le type de données, la valeur par défaut et les valeurs numériques admises peuvent être déterminés.
- Pour les paramètres F comportant des noms normalisés outre leurs valeurs numériques, le mot clé Prm_Text_Ref est dirigé vers le PrmText avec ces définitions de noms. Le PrmTxt doit contenir des textes pour toutes les valeurs admises. Les outils de développement/configuration doivent ignorer les textes supplémentaires propres aux valeurs non spécifiées.

Tableau 17 – Exemple de GSD dans la notation GSDL

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

Pour obtenir des modèles de fichier GSD pour les esclaves F (CP 3/1 ou CP 3/2), s'adresser aux organismes de bus de terrain.

Dans le cas d'un fichier GSD dédié à un appareil F (CP 3/RTE), les règles d'annotation GSDML suivantes s'appliquent pour le calcul de la signature CRC0 (voir l'exemple de la Figure 57 et du Tableau 18):

- Certains paramètres F comportent des noms normalisés avec des valeurs numériques associées. Dans la notation GSDML, seuls ces noms doivent être utilisés dans les attributs "DefaultValue" et "AllowedValues". Il est possible de trouver les valeurs numériques associées en 8.1.
- Si un paramètre F non inclus dans l'ensemble F_Check_iPar, F_CRC_Length, F_Block_ID est défini comme invisible dans le fichier GSD, une valeur fixe nulle est considérée et ce paramètre ne doit pas être inclus dans le calcul de CRC0.
- Si un paramètre F (ou des éléments de sa définition) est purement omis du fichier GSD, les valeurs par défaut issues du schéma GSDML correspondant doivent être utilisées. Les paramètres visibles doivent être toujours inclus dans le calcul de CRC0, indépendamment du fait que leurs valeurs soient spécifiées de manière explicite dans un fichier GSD ou qu'elles complètent le schéma.

- F_Check_SeqNr n'existe pas dans la définition de la notation GSDML et ne doit ainsi pas être inclus dans le calcul de CRC0.
- F_Par_Version doit toujours être inclus dans le calcul de CRC0 bien qu'il ait une valeur fixe de "1".
- L'ordre des paramètres F dans l'élément “F_ParameterRecordDataItem” correspond à l'ordre de l'enregistrement des paramètres F, sauf pour F_iPar_CRC.

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

Figure 57 – Exemple de GSD dans la notation GSDML

Pour obtenir des modèles de fichier GSD pour les appareils F (CP 3/RTE), s’adresser aux organismes de bus de terrain.

Tableau 18 – Flux d'octets sérialisé pour les exemples

Contenu GSD	Flux d'octets sérialisé pour le calcul de CRC0
“F_SIL” Type=BitArea, Décalage=2 Valeur par défaut=2 (SIL3) “SIL1”, 0 (énumération) “SIL2”, 1 “SIL3”, 2	0x46, 0x5F, 0x53, 0x49, 0x4C, 0x00, 0x02, 0x02, 0x00, 0x53, 0x49, 0x4C, 0x31, 0x00, 0x00, 0x53, 0x49, 0x4C, 0x32, 0x01, 0x00, 0x53, 0x49, 0x4C, 0x33, 0x02, 0x00,
“F_CRC_Length” Type=BitArea, Décalage=4 Valeur par défaut=2 (4-Byte-CRC) Min=2, Max=2 (plage)	0x46, 0x5F, 0x43, 0x52, 0x43, 0x5F, 0x4C, 0x65, 0x6E, 0x67, 0x74, 0x68, 0x00, 0x04, 0x02, 0x00, 0x02, 0x00, 0x02, 0x00,
“F_CRC_Seed” Type=Bit, Décalage=6 Valeur par défaut=1 (CRC_Seed24/32) Min=1, Max=1 (plage)	0x46, 0x5F, 0x43, 0x52, 0x43, 0x5F, 0x53, 0x65, 0x65, 0x64, 0x00, 0x06, 0x01, 0x00, 0x01, 0x00, 0x01, 0x00,
“F_Passivation” Type=Bit, Décalage=0 Valeur par défaut=0 (Appareil/Module) Min=0, Max=0 (plage)	0x46, 0x5F, 0x50, 0x61, 0x73, 0x73, 0x69, 0x76, 0x61, 0x74, 0x69, 0x6F, 0x6E, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
“F_Block_ID” Type=BitArea, Décalage=3 Valeur par défaut=0 Min=0, Max=0	0x46, 0x5F, 0x42, 0x6C, 0x6F, 0x63, 0x6B, 0x5F, 0x49, 0x44, 0x00, 0x03, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
“F_Par_Version” Type=BitArea, Décalage=6 Valeur par défaut=1 (V2-mode) Min=1, Max=1	0x46, 0x5F, 0x50, 0x61, 0x72, 0x5F, 0x56, 0x65, 0x72, 0x73, 0x69, 0x6F, 0x6E, 0x00, 0x06, 0x01, 0x00, 0x01, 0x00, 0x01, 0x00,
“F_Source_Add” Type=Unsigned16 Valeur par défaut=1 Min=1, Max=65534	0x46, 0x5F, 0x53, 0x6F, 0x75, 0x72, 0x63, 0x65, 0x5F, 0x41, 0x64, 0x64, 0x02, 0x00, 0x01, 0x00, 0x01, 0x00, 0xFE, 0xFF,
“F_Dest_Add” Type=Unsigned16 Valeur par défaut=1 Min=1, Max=65534	0x46, 0x5F, 0x44, 0x65, 0x73, 0x74, 0x5F, 0x41, 0x64, 0x64, 0x02, 0x00, 0x01, 0x00, 0x01, 0x00, 0xFE, 0xFF,
“F_WD_Time” Type=Unsigned16 Valeur par défaut =500 Min=10, Max=2000	0x46, 0x5F, 0x57, 0x44, 0x5F, 0x54, 0x69, 0x6D, 0x65, 0x02, 0x00, 0xF4, 0x01, 0x0A, 0x00, 0xD0, 0x07,
“F_Par_CRC” Type=Unsigned16 Valeur par défaut=21211 Min=0, Max=65535	0x46, 0x5F, 0x50, 0x61, 0x72, 0x5F, 0x43, 0x52, 0x43, 0x02, 0x00, 0xDB, 0x52, 0x00, 0x00, 0xFF, 0xFF

La signature CRC0 résultante 56313 (décimale) ou 0xDBF9 (hexadécimale) doit être saisie dans l'attribut F_ParamDescCRC.

Interprétation du fichier GSD: 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 19 dans l’ordre indiqué (Version 2). Le polynôme CRC à 32 bits

(*0xF4ACFB13*) doit être utilisé pour calculer la signature. Les types de données admis pour FSCP 3/1 figurent en 5.5.3. La précédente version 1 de l'ensemble d'éléments de structure de données d'entrée-sortie ne contenait pas l'attribut VERSION, ni les types de données Integer32 et Unsigned8+Unsigned8. Par conséquent, aucun mot clé 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 (*0x4EAB*), et la longueur de la signature CRC7 est de 2 octets.

Le paramètre "F_IO_StructureDescCRC" n'est pas transmis à l'appareil F lors du démarrage. L'outil de développement peut utiliser ce mécanisme pour assurer une configuration correcte.

Tableau 19 – Éléments de structure de données d'entrée-sortie

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 DataItems ''Float32+Unsigned8'' (5 × nombre de)
COUNT_PS_INPUT_BYTES_U8_U8	2 octets	Entrée: longueur de tous DataItems ''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 DataItems booléens (en octets) en mode maximal (mode 1oo1, par exemple)
COUNT_PS_INPUT_CHANNELS_INT	2 octets	Entrée: nombre de tous les DataItems Integer16
COUNT_PS_INPUT_CHANNELS_DINT	2 octets	Entrée: nombre de tous les DataItems Integer32
COUNT_PS_INPUT_CHANNELS_REAL	2 octets	Entrée: nombre de tous les DataItems 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 DataItems 'Float32+Unsigned8'' (5 × nombre de)
COUNT_PS_OUTPUT_BYTES_U8_U8	2 octets	Sortie: longueur de tous les DataItems ''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 DataItems booléens (en octets)
COUNT_PS_OUTPUT_CHANNELS_INT	2 octets	Sortie: nombre de tous les DataItems Integer16
COUNT_PS_OUTPUT_CHANNELS_DINT	2 octets	Sortie: nombre de tous les DataItems Integer32
COUNT_PS_OUTPUT_CHANNELS_REAL	2 octets	Sortie: nombre de tous les DataItems 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 19. Ces exemples de sections DataItem font référence à F_CRC_Seed = 1.

Les types de données admis pour FSCP 3/1 figurent en 5.5.3.

NOTE F_Passivation =1 ("Canal") est utilisé uniquement conjointement à [66], qui contient des exemples supplémentaires

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 à la Figure 58. Le Tableau 19 contient une description des variables.

Figure 58 – 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 à la Figure 59.

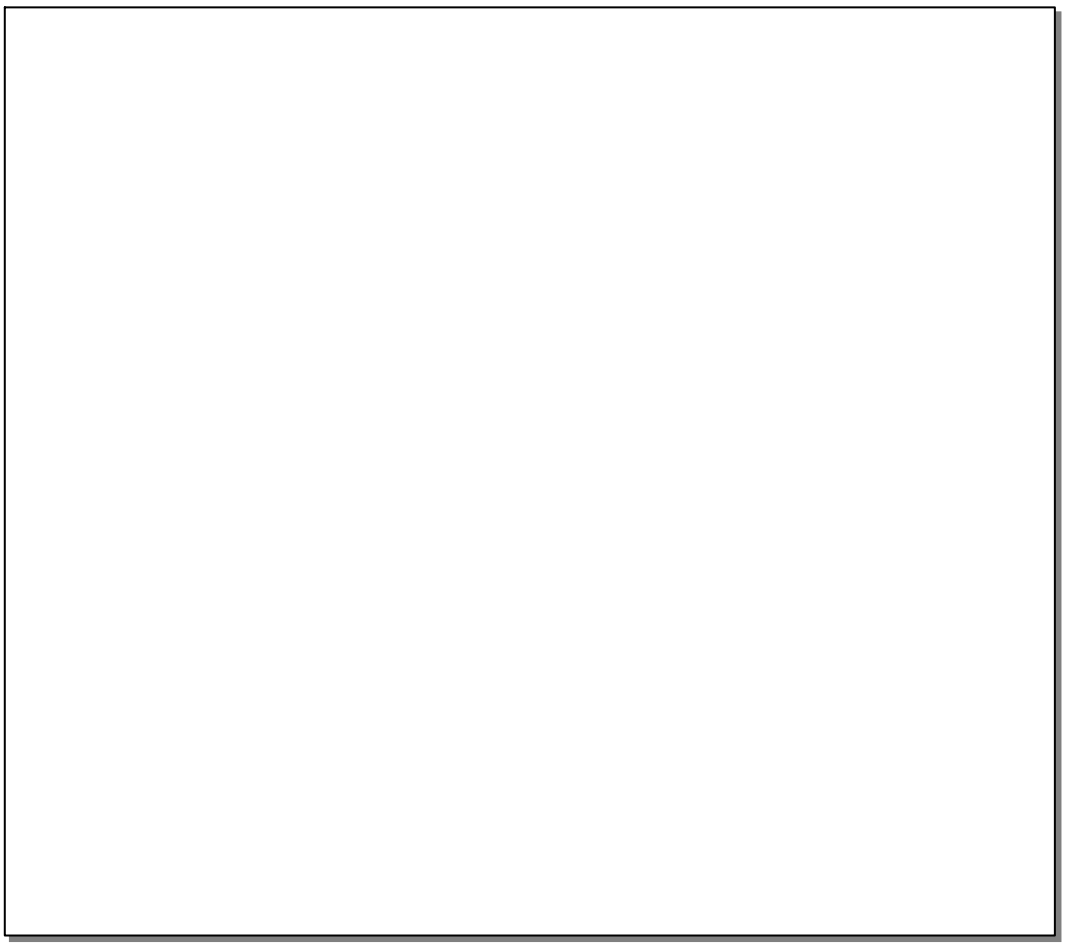


Figure 59 – Section DataItem de F_IN_OUT_2

8.4.2.4 F_IN_OUT_5

Entrée: Composite (Float32+Unsigned8) Le codage de l'exemple F_IN_OUT_5 F_Channel_Driver est présenté à la Figure 60.

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

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 60 – Section DataItem de F_IN_OUT_5

8.4.2.5 F_IN_OUT_6

Entrée:
Relecture (Float32 + Unsigned8),
Revérification (Unsigned8 + Unsigned8 + Unsigned8)

Sortie:
Point de consigne (Float32+Unsigned8)

Le codage de la section DataItem de l'exemple F_IN_OUT_6 F_Channel_Driver est présenté à la Figure 61. Le Tableau 19 contient une description des variables.

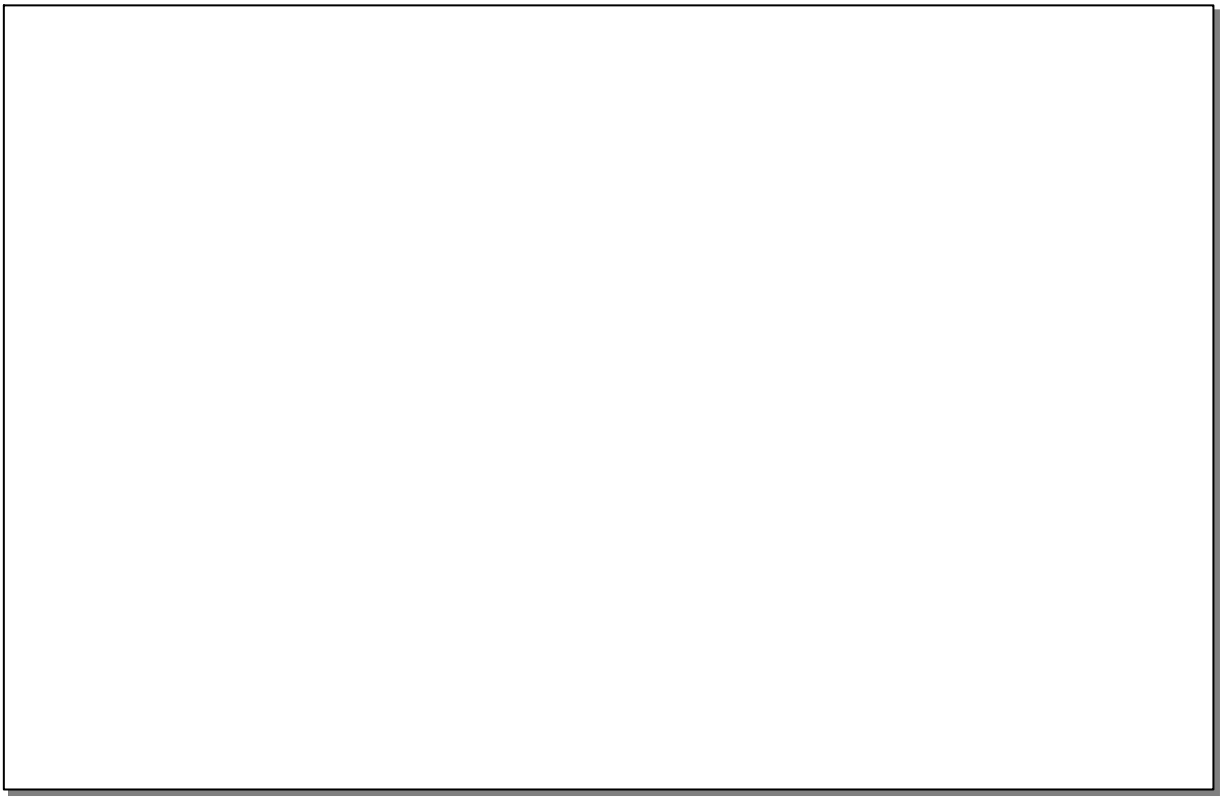


Figure 61 – Section DataItem de F_IN_OUT_6

8.5 Utilisation des informations de type de données

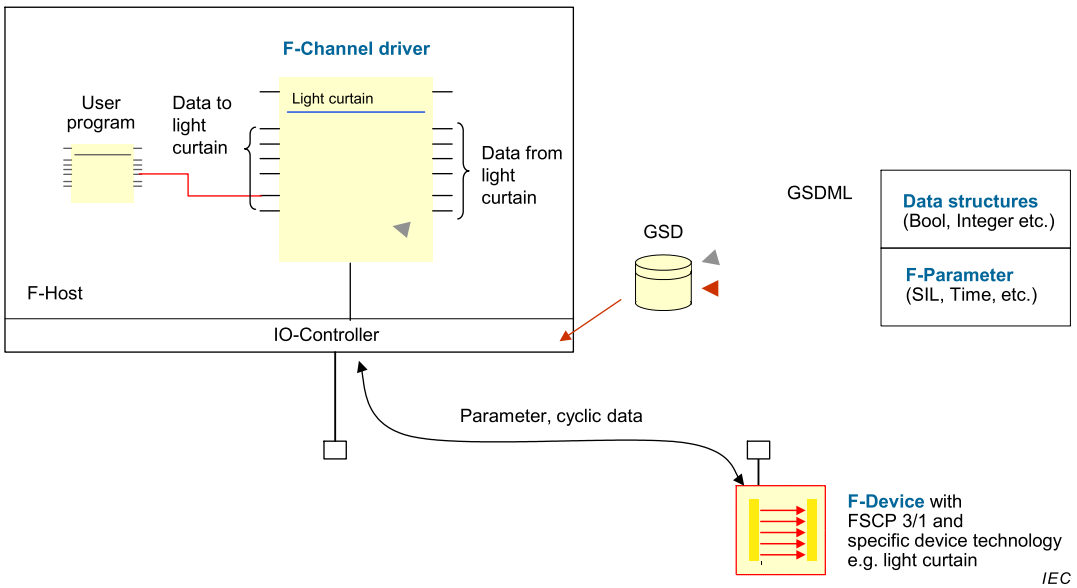
8.5.1 Pilote de canal F

Il est nécessaire que les données d'entrée-sortie F transférées de manière cyclique entre un appareil F et un hôte F (canal en temps réel) soient contrôlées par un programme utilisateur.

Habituellement, un programmeur attend des variables d'entrée ou de sortie discrètes adressables logiquement (par exemple, dans le cas du langage de programmation "logique d'échelle") qui correspondent directement à une image communément appelée image de processus.

Dans le cas d'appareils F plus complexes, le programmeur attend des blocs de fonctions appropriés ("pilote de canal F") dans les bibliothèques de son outil de programmation, qu'il peut intégrer dans le programme client.

La Figure 62 représente cette vue des blocs de fonctions «pilote de canal F» du programmeur.



Anglais	Français
F-channel driver	Pilote de canal F
User program	Programme utilisateur
Data to light curtain	Données vers le rideau de lumière
Light curtain	Rideau de lumière
Data from light curtain	Données provenant du rideau de lumière
F-host	Hôte F
IO-controller	Contrôleur d'entrée-sortie
Data structures (bool, integer, etc.)	Structures de données (valeur booléenne, entier, etc.)
F-Parameter (SIL, time, etc.)	Paramètre F (SIL, durée, etc.)
Parameter, cyclic data	Paramètre, données cycliques
F-device with FSCP 3/1 and specific device technology e.g. light curtain	Appareil F avec FSCP 3/1 et technologie d'appareil spécifique, par exemple, rideau de lumière

Figure 62 – Pilote de canal F en tant que «colle» entre l'appareil F et le programme utilisateur

8.5.2 Règles pour les pilotes de canal F standard

Une prise en charge générale des systèmes à partir de tous les types d'hôte F peut être assurée en respectant les règles suivantes de conception des structures de données F transmises de manière cyclique:

- La structure de données doit être décrite dans la section IODataSection du fichier GSD. Voir la description détaillée en 8.3.2.
- Une structure de données composée doit être présentée dans l'ordre suivant: Tous les types mixtes de Float32 + Unsigned8 en premier, le cas échéant. Ensuite, toutes les variables Unsigned8, Unsigned16, Unsigned32, le cas échéant. Puis toutes les variables Integer16, Integer32, le cas échéant. Enfin, toutes les variables à virgule flottante, le cas échéant.

Le Tableau 20 contient une liste de modèles de pilote de canal F. Les pilotes représentent différentes structures de données d'entrée F et de sortie F en fonction des PDU de sécurité associés. Les types de données admis pour FSCP 3/1 figurent en 5.5.3. Par conséquent, 32 valeurs booléennes et 8 bits doivent être mis en correspondance respectivement dans le type de données Unsigned32 et le type de données Unsigned8. Voir 8.4.2 pour plus de détails.

Tableau 20 – Modèle de pilotes de canal F

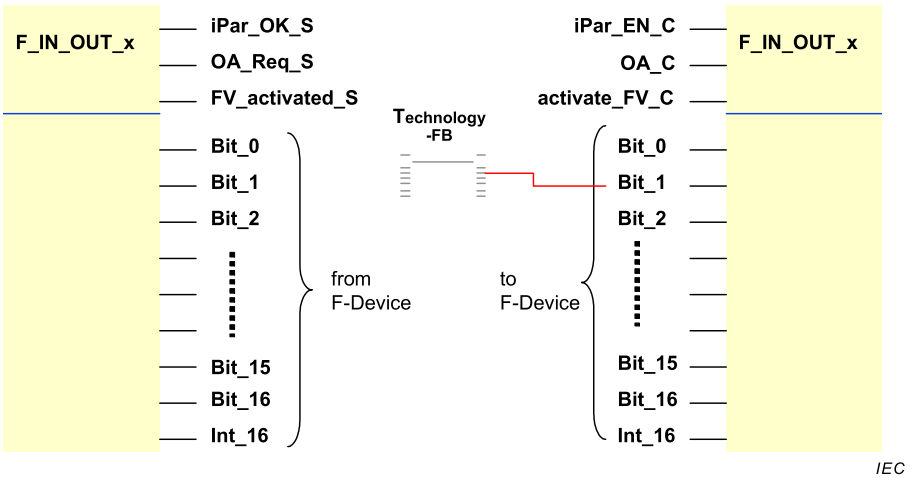
Configuration du pilote de canal F[a]	Entrée F (depuis l'appareil)	Sortie F (vers l'appareil)	Remarques
F_IN_OUT_1	32 valeurs booléennes,	32 valeurs booléennes,	Rideaux de lumière, par exemple
F_IN_OUT_2	16 valeurs booléennes, 1 Integer16	16 valeurs booléennes, 1 Integer16	Lecteurs laser, par exemple
F_IN_OUT_5	1 Float32, Unsigned8 (8 bits «Qualificatifs»)		Transmetteur de pression, par exemple
F_IN_OUT_6	«Readback»: 1 Float32, 8 bits «Checkback»: 24 bits	«Setpoint»: 1 Float32, 8 bits	Soupape pneumatique, par exemple
[a] La numérotation n'indique pas nécessairement différents pilotes. Il peut s'agir d'un pilote paramétré à l'aide des informations GSD.			

Contraintes:

- la valeur 0 doit être attribuée aux bits inutilisés;
- les indications d'état et d'anomalie d'un appareil F doivent être définies dans la structure de données d'entrée, le cas échéant (un qualificatif, par exemple).

8.5.3 Recommandations relatives aux pilotes de canal F

La Figure 63 donne un exemple de présentation d'un pilote hôte de canal F d'un appareil F complexe.



Anglais	Français
Technology-FB	Technologie- FB
From F-device	En provenance de l'appareil F
To F-device	Vers l'appareil F

Figure 63 – Exemple de présentation d'un pilote de canal F

Les termes utilisés dans la Figure 63 et les comportements du pilote sont spécifiés ci-dessous:

iPar_EN_C	iParamétrage activé
iPar_OK_S	iParamétrage terminé
OA_C	Acquittement de l'opérateur (pour reprise après anomalie)
OA_Req_S	En cas de détection et de suppression d'anomalie

	(temporisation ou CRC2)
FV_activated_S	Valeurs Failsafe activées par l'appareil F
activate_FV_C	Valeurs Failsafe à activer dans l'appareil F
Comportement fixe du pilote de canal F	Valeur Failsafe sur «0»

Outre les structures de données spécifiques à l'appareil, le programmeur dispose d'autres signaux FSCP 3/1 supplémentaires. Voir 7.1.3 «Octet d'état et de contrôle» et 6.1 pour obtenir des informations détaillées relatives aux signaux mentionnés ci-dessus.

Pour des raisons de performance, le pilote de canal F peut être divisé en deux blocs de fonctions, l'un pour les entrées et l'autre pour les sorties (Figure 63).

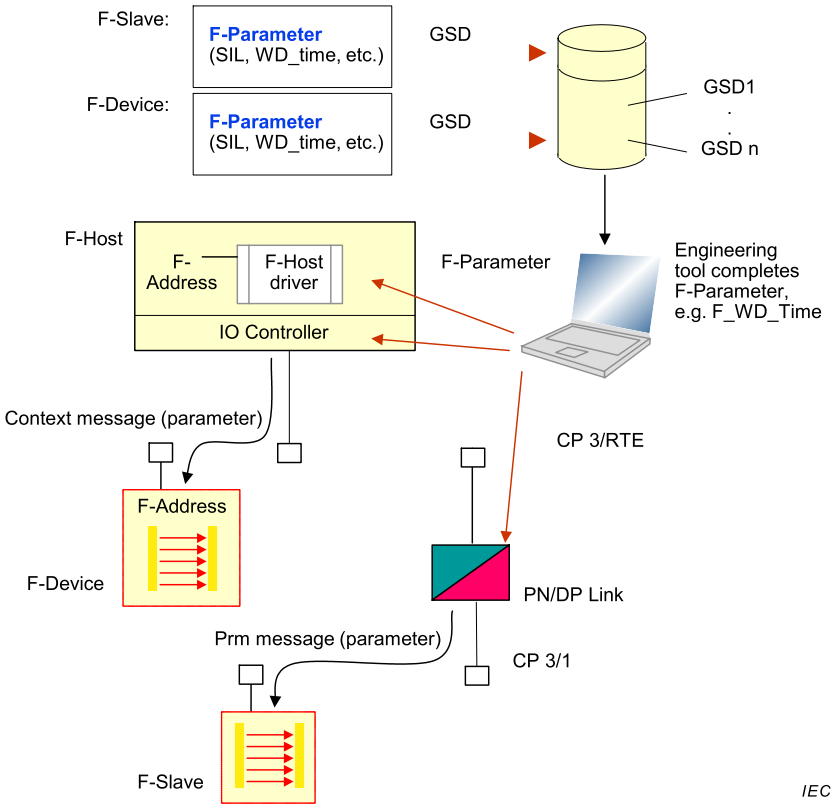
Il s'agit d'un comportement fixe des pilotes de canal F par rapport aux valeurs Failsafe: si la structure de données est composée du bit (Unsigned8), Integer16, Float32 ou Float32 + Unsigned8, chaque valeur est définie sur 0.

Si les actionneurs ne peuvent admettre FV = "0", d'autres valeurs peuvent être mises en œuvre de manière figée dans le code ou par l'intermédiaire d'iParamètres. Les programmes utilisateur peuvent activer ces valeurs Failsafe spécifiques à l'appareil avec le bit 4 de l'octet de contrôle (voir 7.1.3).

Si les capteurs ne peuvent admettre FV = "0", une logique de programme utilisateur supplémentaire peut les transformer en valeurs individuelles à l'aide de l'entrée "activate_ FV_C" du pilote de canal F.

8.6 Mécanismes d'attribution de paramètres de sécurité

8.6.1 Attribution du paramètre F



Anglais	Français
F-slave	Esclave F
F-parameter	Paramètre F
F-device	Appareil F
F-host	Hôte F
F-address	Adresse F
F-host driver	Pilote d'hôte F
IO controller	Contrôleur d'entrée-sortie
Engineering tool completes F-Parameter, e.g …	L'outil de développement complète le paramètre F, par exemple …
Context message (parameter)	Message de contexte (paramètre)
To	A
PN/DP link	Liaison PN/DP
Prm message (parameter)	Message Prm (paramètre)
F-slave	Esclave F

Figure 64 – Attribution du paramètre F pour de simples appareils F et esclaves F

De simples appareils F sans iParamètres peuvent être fournis par l'intermédiaire du chemin de message de contexte standard. Voir l'IEC 61158-5-10, l'IEC 61158-6-10 et [50]. La quantité totale de paramètres F ne peut pas dépasser ici la limite supérieure de 234 octets (Figure 64).

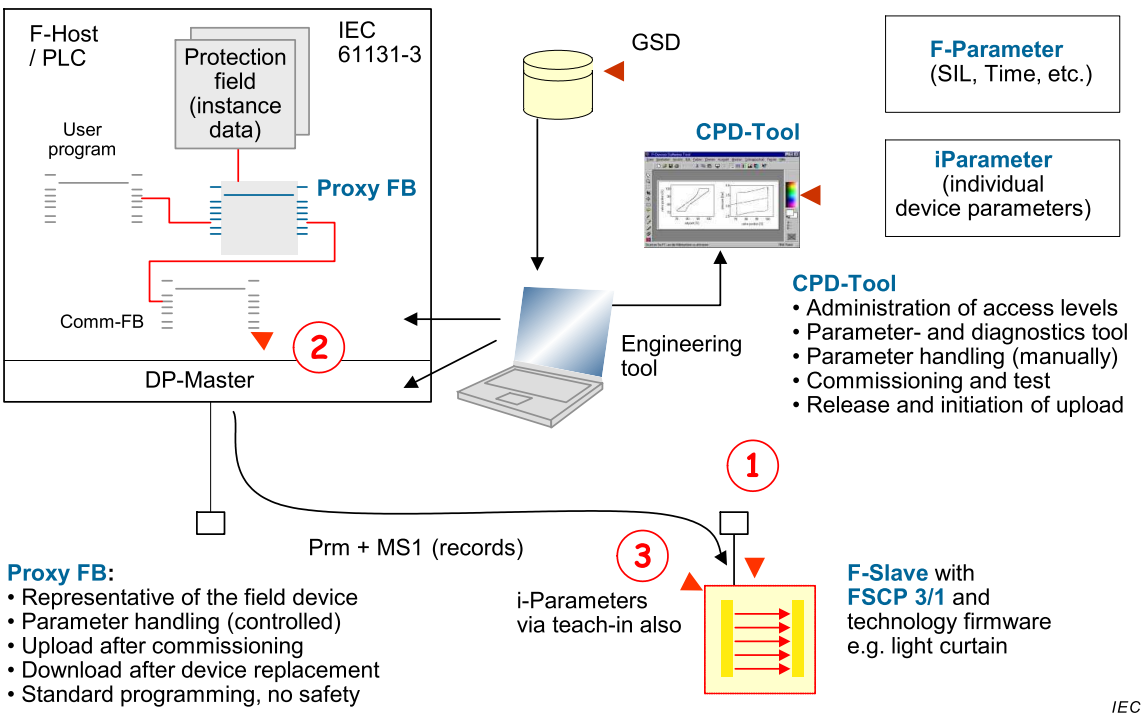
8.6.2 Attribution générale d'iParamètres

Pour les appareils complexes comportant des iParamètres, une décision (de sécurité) doit être prise quant à savoir si une attribution de démarrage automatique est préférable à une attribution séparée à partir d'un outil CPD dédié pour l'appareil F particulier, comme le demande l'IEC 62061. Dans chaque cas, l'hôte F doit débloquer uniquement l'attribution en l'absence d'état de processus dangereux (7.4.2). Principalement, il existe deux méthodes qui peuvent s'avérer complémentaires:

- attribution de la valeur iParamètre par l'intermédiaire de blocs de fonctions proxy particuliers dans un hôte F et un ensemble de données iParamètre approprié;
- attribution de la valeur iParamètre grâce à un outil CPD dédié par l'intermédiaire d'un superviseur d'entrée-sortie (outil de développement/PC).

CPF 3 offre une plate-forme de communication standard pour les programmes de commande grâce aux *blocs de fonctions de communication* conformément à l'IEC 61131-3 et aux *blocs de fonctions proxy* conformément à l'IEC 61131-3, en particulier le langage de programmation ST (Structured Text – Texte structuré), prenant donc en charge le premier. Les fabricants d'appareils F ont la possibilité de fournir des logiciels de commande mobiles pour leurs appareils.

La Figure 65 présente un exemple d'utilisation des normes CPF 3 pour assurer une prise en charge très pratique et très souple des appareils F par le système. L'outil CPD dédié du fabricant d'appareils communique (étape 1) avec son appareil F (ici: le rideau de lumière) sur une liaison directe et séparée (USB, par exemple) ou par l'intermédiaire de services acycliques = Données d'enregistrement de lecture/d'écriture (voir Tableau 35) sur le bus de terrain simultanément avec la communication de données cycliques. Après le paramétrage et la mise en service, le bloc de fonctions proxy (FB proxy) peut être activé pour télécharger en amont les iParamètres dans le contrôleur (étape 2) d'où ils peuvent être téléchargés en aval en en cas de remplacement de l'appareil pour réparation (étape 3).



Anglais	Français
F-host/PLC	Hôte F/PLC
Protection field (instance data)	Champ de protection (données d'instance)
User program	Programme utilisateur

Anglais	Français
Proxy FB	FB proxy
CPD tool	Outil CPD
F-parameter (SIL, Time, etc.)	Paramètre F (SIL, durée, etc.)
iParameter (individual device parameters)	iParamètre (paramètres d'appareil individuel)
Engineering tool	Outil de développement
Comm-FB	FB comm
DP master	Maître DP
(records)	(enregistrements)
Administration of access levels Parameter- and diagnostics tool Parameter handling (manually) Commissioning and test Release and initiation of upload	Administration des niveaux d'accès outil de paramètre et de diagnostic traitement des paramètres (manuellement) mise en service et essai déclenchement et initiation du téléchargement amont
Representative of the field device Parameter handling (controlled) Upload after commissioning Download after device replacement Standard programming, no safety	Représentatif de l'appareil de terrain traitement des paramètres (contrôlé) téléchargement amont après mise en service téléchargement aval après remplacement de l'appareil programmation standard, pas de sécurité
IParameters via teach-in also	IParamètres via teach-in également
F-slave with FSCP 3/1 and technology firmware, e.g. light curtain	Esclave F avec FSCP 3/1 et micrologiciel technologique, par exemple rideau de lumière

Figure 65 – Attribution de paramètre F et d'iParamètre pour les appareils F complexes

Par l'intermédiaire des attributions d'iParamètre dynamiques commandées par programme, les programmes de recette peuvent permettre de résoudre les exigences de flexibilité renforcée dans les secteurs actuels de la fabrication. Par conséquent, plusieurs ensembles de données différents présentant des coordonnées de zones de détection des rideaux de lumière («effacement»), par exemple, peuvent être attribués l'un après l'autre (Figure 65). Le numéro d'identification de l'ensemble de données iParamètre réel doit être communiqué de manière cyclique dans les données d'entrée-sortie F.

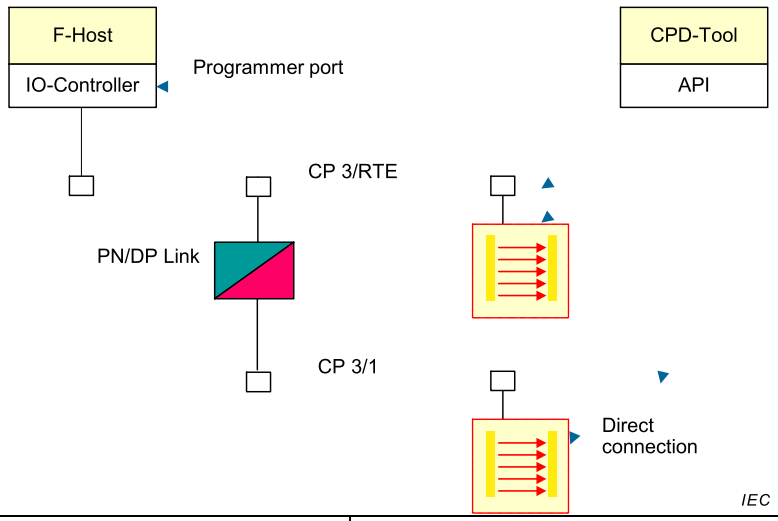
8.6.3 Exigences d'intégration de système des outils d'iParamétrage

Le Tableau 21 contient une liste des exigences que les procédures d'iParamétrage sont tenues de satisfaire.

Tableau 21 – Exigences pour l'iParamétrage

N°	Exigences système
R1	Outil CPD à concevoir pour les ordinateurs personnels ou portables compatibles et les systèmes d'exploitation WINDOWS XP ou ultérieurs
R2	Il convient d'exécuter simultanément plusieurs outils CPD ou instances de ces outils
R3	CP 3/1: les tableaux d'interface de classe maître 2 doivent fournir une API uniforme (interface d'un programmeur d'application) de manière à pouvoir configurer, puis exécuter les outils CPD sur des marques différentes
R4	CP 3/RTE: l'interface du superviseur d'entrée-sortie doit être définie de manière à pouvoir utiliser les services «acycliques» de CP 3/RTE pour un appareil F directement connecté à un réseau CP 3/RTE
R5	CPF 3: l'interface du superviseur d'entrée-sortie doit être définie de manière à pouvoir utiliser les services "acycliques" de CP 3/RTE pour un appareil F directement connecté à un réseau CP 3/RTE ou par l'intermédiaire d'un "Lien" à un esclave F connecté à un réseau CP 3/1 "auxiliaire" (initier, lire et écrire des enregistrements, etc.)
R6	Il convient que les connexions R4 et R5 soient possibles via le port des programmeurs de l'hôte F également
R7	Il convient que les "liens PN/DP" soient possibles en tant qu'appareil autonome ou intégré dans un contrôleur
R8	Indication d'interface de bus de terrain: un appareil F doit indiquer son type d'interface de bus de terrain. Inutile si une API uniforme (voir R3) est définie et qu'elle est adaptée aux communications acycliques CPF 3
R9	Chemin vers la base de données du projet en tant que paramètre "Invocation" ou utilisation d'une interface d'outil de développement intégrée pour stocker les données de l'appareil F dans cette base de données de projet globale. Il convient de pouvoir procéder à la définition automatique de la version des ensembles de données iParamètre
R10	Il convient de définir le nom de la station/adresse en tant que paramètre "Invocation"
R11	Il convient de définir le chemin au fichier GSD en tant que paramètre "Invocation"
R12	Il convient de définir le support en plusieurs langues en tant que paramètre «Invocation». Outil de développement hôte de définition de la langue par défaut sur invocation
R13	Il convient que l'autorisation (rôles et droits d'accès) soit héritée de l'outil de développement hôte vers l'outil CPD sur invocation
R14	Téléchargement aval d'iParamètres sur l'appareil F: il convient de définir le flux d'octets d'iParamètres de manière à pouvoir le stocker dans le contrôleur d'entrée-sortie et de le transférer sur l'appareil F lors du paramétrage général. Le bloc de fonctions proxy est toujours la solution préférée pour FSCP 3/1
R15	Version: les API (voir R3 et R4) doivent fournir un numéro de version de sorte que les outils CPD puissent automatiquement s'ajuster
R16	Impression: il convient de pouvoir «contrôler à distance» les outils CPD individuels à partir de l'outil de développement hôte pour l'impression par lots ou pour fournir l'impression dans un format normalisé (HTML, par exemple) à l'outil de développement hôte
R17	Téléchargement amont et aval d'iParamètres: il convient de pouvoir «contrôler à distance» les outils CPD dédiés à partir de l'outil de développement hôte pour «l'iParamétrage» par lots ou pour fournir les iParamètres dans un format normalisé à l'outil de développement hôte (voir R14)
R18	Il convient d'activer l'outil CPD pour soumettre des noms de symbole par défaut ("OSSD1", par exemple) à l'outil de développement hôte et obtenir en retour les noms de symbole finaux attribués du projet en cas de diagnostic. La soumission de noms de symbole par défaut est possible avec le fichier GSD de CP 3/RTE
R19	Pour assurer l'indépendance vis-à-vis du canal noir sous-jacent, le même principe de protection de la transmission des données iParamètre que celui de l'échange de données cycliques (voir la Figure 26 et l'article connexe) doit être utilisé, c'est-à-dire que le calcul d'iPar CRC32 doit avoir lieu dans l'ordre inverse des octets (la valeur initiale ne doit pas être nulle). Un fabricant peut utiliser sa méthode personnelle de protection des iParamètres tant que les critères sont satisfaits (serveur d'iParamètres, outil CPD)

La Figure 66 représente les aspects du système liés à l'intégration de l'outil CPD.



Anglais	Français
F-host	Hôte F
IO controller	Contrôleur d'entrée-sortie
Programmer port	Port du programmeur
CPD tool	Outil CPD
To	à
PN/DP link	Liaison PN/DP
Direct connection	Connexion directe

Figure 66 – Intégration système des outils CPD

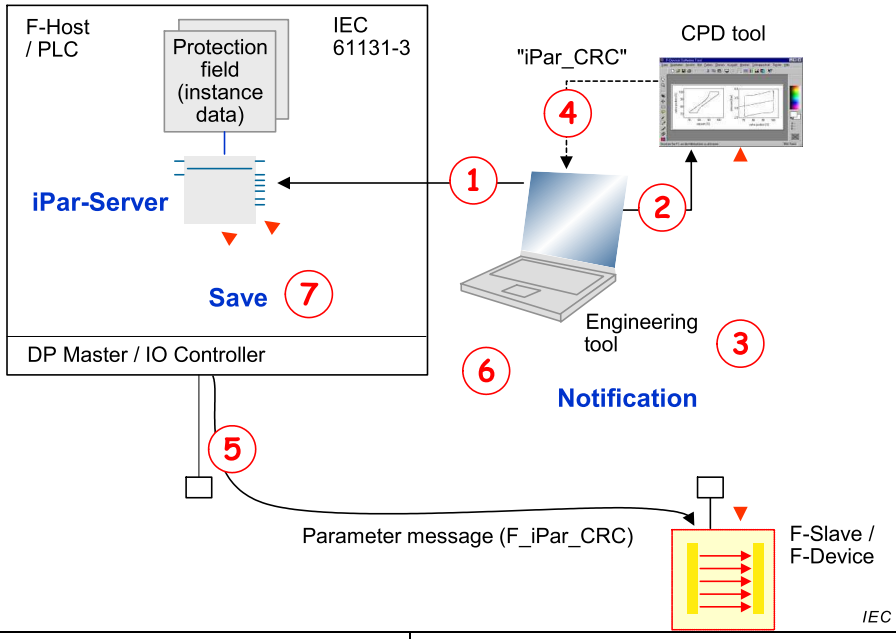
L'outil CPD peut être connecté:

- à l'appareil F directement (USB, RS232, par exemple);
- à l'hôte F par l'intermédiaire d'un port du programmeur;
- à CP 3/RTE et à CP 3/1 par une liaison; ou
- à CP 3/1 ou CP 3/2.

8.6.4 Serveur d'iParamètres

8.6.4.1 Description générale et contraintes

Le concept de serveur d'iParamètres est une forme particulière du concept plus général de bloc de fonctions proxy énoncé en 8.3.1. Il revient aux fabricants d'hôtes F d'assurer cette fonction comme indiqué dans le Tableau 35, que ce soit au sein de la partie non relative à la sécurité d'un hôte F (le maître de paramétrage, par exemple) ou dans un sous-système contrôlé (un PLC non relatif à la sécurité ou un ordinateur industriel participant au même réseau, par exemple). [65] remplace la partie non relative à la sécurité de la spécification suivante.



Anglais	Français
F-host	Hôte F
Protection field (instance data)	Champ de protection (données d'instance=
CPD-tool	Outil CPD
iPar-Server	Serveur d'iParamètres
Engineering-tool	Outil de développement
Save	Sauvegarde
Notification	Avis
Parameter message	Message de paramètre
F-slave/F-device	Esclave F/appareil F
DP-master	Maître DP
IO controller	Contrôleur ES

Figure 67 – Mécanisme de serveur d'iParamètres (mise en service)

La Figure 67 représente par un exemple les grandes étapes du mécanisme de serveur d'iParamètres. Parallèlement à la configuration du réseau et au paramétrage F d'un esclave F/appareil F, une fonction iPar-Server associée est instanciée (étape 1).

L'esclave F/appareil F est capable de passer en mode d'échange de données tout en utilisant un état de sécurité (FV). Un outil CPD associé peut être lancé, à partir de l'outil de développement, par une interface appropriée (étape 2), diffusant au moins l'adresse de nœud de l'appareil configuré.

Le paramétrage, la mise en service, les essais, etc. peuvent être exécutés à l'aide de l'outil CPD (étape 3).

La signature iPar_CRC est ensuite calculée et affichée au format hexadécimal pour au moins copier-coller cette valeur dans le champ d'entrée "F_iPar_CRC" de la partie configuration de l'outil de développement (étape 4).

Il est nécessaire de redémarrer l'esclave F/appareil F pour lui transférer le paramètre "F_iPar_CRC" (étape 5).

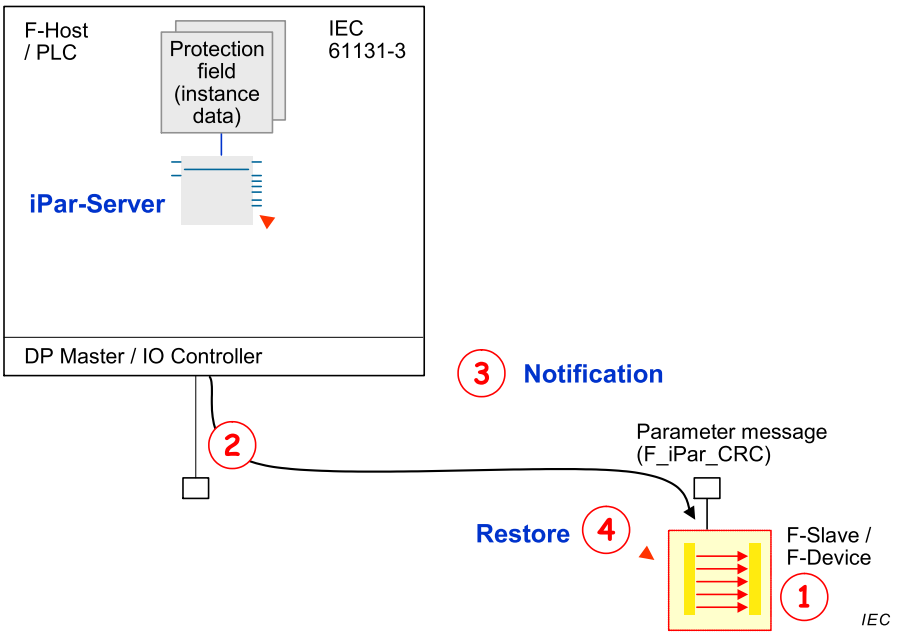
Après une dernière vérification et diffusion, l'esclave F/appareil F est autorisé à émettre un avis de téléchargement amont (étape 6) vers son instance iPar-Server. Il utilise ainsi le mécanisme de diagnostic de CPF 3 (8.6.4.2 et [44]).

Le serveur d'iParamètres interroge les informations de diagnostic pour interpréter la demande (R) et établir le processus de téléchargement amont (étape 7) qui stocke les iParamètres sous forme de données d'instance dans l'hôte du serveur d'iParamètres.

La Figure 68 représente la deuxième partie du mécanisme de serveur d'iParamètres. En cas de remplacement d'un esclave F/appareil F défectueux (étape 1), l'esclave F/appareil F reçoit ses paramètres F, dont "F_iPar_CRC" (étape 2), au démarrage.

Sachant que les iParamètres sont normalement absents d'un esclave F/appareil F de remplacement ou non rémanent, celui-ci émet un avis de téléchargement aval (étape 3) vers son instance iPar-Server. Il utilise ainsi le mécanisme de diagnostic de CPF 3 (8.6.4.2 et [44]).

Le serveur d'iParamètres interroge les informations de diagnostic pour interpréter la demande (R) et établir le processus de téléchargement aval (étape 4). Par ce transfert, l'esclave F/appareil F est capable d'assurer cette fonction d'origine sans autres outils de développement ou CPD.



Anglais	Français
F-host	Hôte F
Protection field (instance data)	Champ de protection (données d'instance=
DP-master	Maître DP
IO controller	Contrôleur ES
Notification	Avis
Parameter message	Message de paramètre
F-slave/F-device	Esclave F/appareil F
Restore	restauration

Figure 68 – Mécanisme de serveur d'iParamètres (remplacement de l'appareil F, par exemple)

Les contraintes suivantes ont été identifiées pour le mécanisme du serveur d'iParamètres.

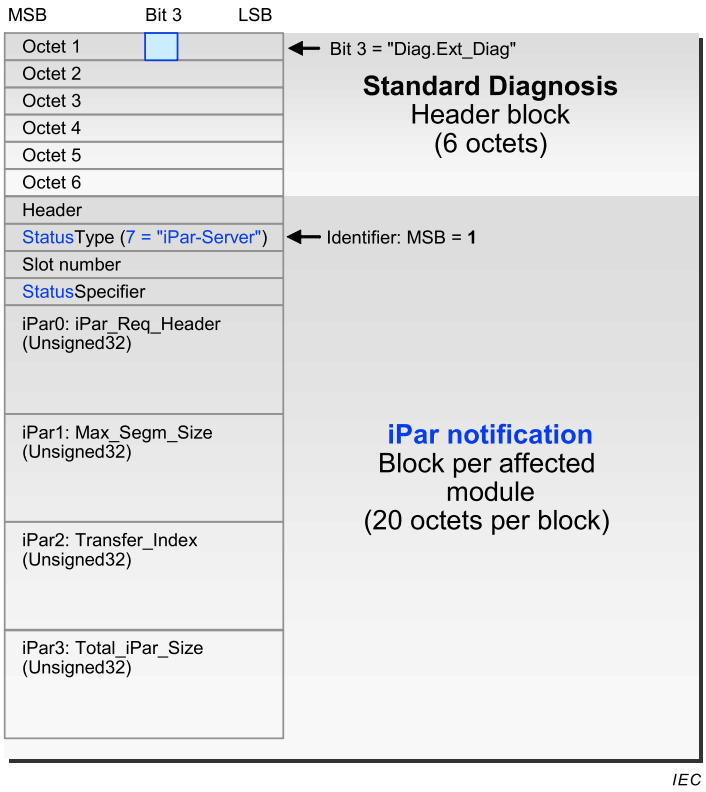
- Chaque instance iPar-Server doit prendre en charge au moins 2^{15}-1 octets d'iParamètres par F_source/Destination_Address (appareil/sous-module/module).
- Les iParamètres sont stockés sous la forme d'un bloc fixe de données tel que présenté à la Figure 53.
- Le serveur d'iParamètres n'est pas sécurisé. Il peut être mis en œuvre ou lancé dans un hôte standard ou dans la partie standard d'un hôte F (Figure 68).
- Il est de la responsabilité du fabricant de l'esclave F/appareil F de faire en sorte que l'ensemble d'iParamètres téléchargé corresponde, par exemple, au type et à la version corrects de l'appareil de remplacement.
- Un module F/esclave F/appareil F doit uniquement lancer une demande de serveur d'iParamètres lorsque le canal noir assure la remise de l'avis.
- Une répétition est admise à chaque tentative de restauration qui n'a pas abouti. La fonction de sécurité associée reste à l'état de sécurité (FV).
- La restauration doit uniquement être exécutée au démarrage du système/appareil F.

8.6.4.2 Avis

Le seul mécanisme standard permettant à un esclave F/module F d'émettre un avis au serveur d'iParamètres des réseaux de type CPF 3 repose sur un message de diagnostic. Toutefois, à l'inverse du contexte de diagnostic standard, il n'est pas utile de propager les informations pour permettre au serveur d'iParamètres d'émettre un avis à l'intention d'un outil de visualisation pour une interaction de maintenance. Parmi les différents types de CP 3/1 et CP 3/2, spécifiés dans l'IEC 61158-5-3, le codage préférentiel des informations de diagnostic s'appuie sur le «Modèle d'état» [45]. Pour éviter les conflits avec les types déjà existants, un nouveau type d'état «Demande de serveur d'iParamètres» (type = 7) a été défini dans une gamme déjà réservée.

NOTE Le type «Mise à jour d'alarme» (type = 6) n'a pas été choisi, puisqu'il donne généralement lieu à l'affichage des informations d'alarme et s'appuie sur une autre sémantique. L'un des objectifs de FSCP 3/1 consiste à coder les deux types de message de diagnostic pour CP 3/1, CP 3/2 et CP 3/RTE de manière aussi proche que possible, de sorte qu'un module F d'une entrée-sortie distante ne soit pas obligé de connaître son déploiement.

La Figure 69 représente le codage de la demande de serveur d'iParamètres pour CP 3/1 et CP 3/2.



Anglais	Français
MSB	Octet de poids fort
LSB	Octet de poids faible
Standard diagnosis – Header block	Diagnostic standard – bloc d'en-tête
Header	En-tête
Identifier	Identifiant
Slot number	Numéro d'intervalle
IPar notification – Block per affected module (20 octets per block)	Avis iPar – bloc par module affecté (20 octets par bloc)

Figure 69 – Codage de la demande de serveur d'iParamètres («modèle d'état»)

Chaque codage de la «demande de serveur d'iParamètres» commence par les six octets obligatoires du bloc de diagnostic standard. Le drapeau "Diag.ext.diag" (bit 3 du premier octet) ne doit pas être impacté, étant donné qu'aucune LED ne doit s'allumer si aucun défaut n'est à signaler. Les quatre octets suivants suivent le codage standard décrit dans l'IEC 61158-5-3 et dans la Figure 69. Le type d'état est la nouvelle «Demande de serveur d'iParamètres» (7). La valeur du spécificateur d'état doit être 0. Le corps de la «Demande de serveur d'iParamètres» contient les spécificateurs définis dans le Tableau 22.

Un module F d'une entrée-sortie distante utilise toujours le codage de la Figure 69 ou un sous-ensemble approprié, à chaque fois qu'il est possible de le déployer dans un appareil d'entrée-sortie distant CP 3/1 ou CP 3/RTE. Une entrée-sortie distante doit uniquement émettre un avis à la fois et donc sauvegarder ou restaurer les iParamètres module F par module F. Des conseils de conception en cas de problème de diagnostic ("Diag.Ext_Diag_Overflow", par exemple) sont disponibles en [45].

NOTE Le codage du transfert d'informations entre un module et sa station de tête n'est pas normalisé.

Il revient à la station de tête d'un appareil d'entrée-sortie distant de transformer le codage de la demande de serveur d'iParamètres dans le format approprié du profil de communication réel (Figure 69 ou Figure 71).

Tableau 22 – Spécificateur de la demande de serveur d'iParamètres

Spécificateur d'iParamètre	Nom	Octet 3	Octet 2	Octet 1	Octet 0	Définition
iPar0	iPar_Req_Header	SR_Version	Réservé	N_Count	SR_Type	Type de demande de serveur d'iParamètres (Unsigned32)
iPar1	Max_Segm_Size	0x00h	0x00h	0x00h	0 à 234	Taille de réseau maximale admise d'un segment, en octets (Unsigned32)
iPar2	Transfer_Index	0x00h	0x00h	0x00h	0 à 254 (255)	Indice de transfert d'enregistrement lecture/écriture (Unsigned32)
iPar3	Total_iPar_Size					Longueur totale des octets d'iParamètre (Unsigned32)

Réservé: Voir 3.3

Avec CP 3/RTE, le paramètre ''Max_Segm_Size'' peut contenir plus de 234 octets. Il peut contenir jusqu'à 2^{22}-1 octets compte tenu des restrictions FSCP 3/1.

Un ''Transfer_Index'' de 255 peut entrer en conflit avec d'autres services (un CALL des fonctions I&M, par exemple).

Le paramètre ''Transfer_Index'' peut contenir plus de 255 octets avec CP 3/RTE: il peut en contenir jusqu'à 65 535.

Un appareil de remplacement peut ne pas connaître la taille exacte de l'iParamètre de son prédécesseur. Dans ce cas, l'avis de restauration peut contenir ''Total_iPar_Size = 0'', ce qui signifie que le serveur d'iParamètres va télécharger en aval l'ensemble de données d'iParamètre.

N_Count est un compteur de séquence pour les avis (CP 3/1 et CP 3/2 uniquement), comptant en boucle de 1 à 15.

La valeur 0x01 doit être attribuée au paramètre "SR_Version". Le paramètre "N_Count" doit commencer par 1 et être modifié à chaque avis (uniquement dans les cas de CP 3/1 et CP 3/2) jusqu'à la valeur 15, puis recommencer à 1. Le paramètre "SR_Type" doit être codé comme présenté à la Figure 70.

7	6	5	4	3	2	1	0	
*	*	*	*	*	*	0	0	Réservé
*	*	*	*	*	*	0	1	Sauvegarder (Téléchargement amont)
*	*	*	*	*	*	1	0	Réservé
*	*	*	*	*	*	1	1	Restaurer (Téléchargement aval)
*	*	*	*	↑	↑			Réservé: Voir 3.3
*	*	*	0	*	*	*	*	Transfert par un enregistrement lecture/écriture
*	*	*	1	*	*	*	*	Transfert segmenté par mécanisme push/pull
↑	↑	↑						Réservé: Voir 3.3

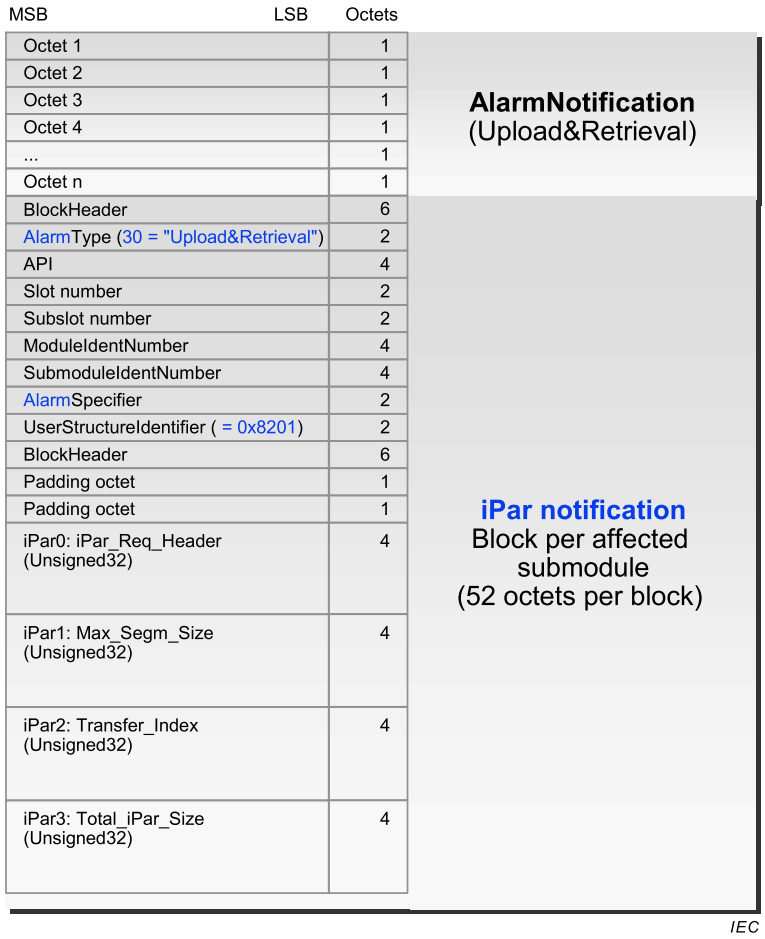
Figure 70 – Codage de SR_Type

Une réalisation possible de l'homologue dans la partie non relative à la sécurité de l'hôte F, par exemple, est spécifiée en [44] et appelée bloc de fonctions de communication RDIAG.

Le codage préférentiel des informations de diagnostic sur CP 3/RTE du serveur d'iParamètres s'appuie sur le «Modèle d'alarme» et sur l'alarme «Upload&Retrieval» standard définis dans l'IEC 61158-5-10 et l'IEC 61158-6-10. La Figure 71 représente le codage de la demande de serveur d'iParamètres pour CP 3/RTE.

Après l'envoi d'une demande de serveur d'iParamètres, l'appareil F/module F attend 2^{18} ms (environ 4,4 minutes) le service de sauvegarde ou de restauration à exécuter intégralement. À l'expiration de ce délai, il lance un message de diagnostic approprié selon 6.3.2.

En cas de demande de serveur d'iParamètres pour un service de restauration et si aucun iParamètre n'est stocké, le serveur d'iParamètres doit envoyer un enregistrement de longueur "0".



Anglais	Français
MSB	Octet de poids fort
LSB	Octet de poids faible
Upload&retrieval	Téléchargement amont & extraction
Slot number	Numéro d'intervalle
Subslot number	Numéro de sous-intervalle
Padding octet	Octet de remplissage
IPar notification – Block per affected submodule (52 octets per block)	Avis iPar – bloc par sous-module affecté (52 octets par bloc)

Figure 71 – Codage de la demande de serveur d'iParamètres («modèle d'alarme»)

8.6.4.3 Services

Le serveur d'iParamètres est un petit programme qui est appelé à chaque cycle principal (dans la partie non relative à la sécurité d'un hôte F, par exemple). Il interroge les informations de diagnostic des esclaves F/modules F particuliers, en recherchant l'un des deux types de demande «Sauvegarde» et «Restauration». Pour exécuter ces demandes, il utilise les services acycliques standards de "read record" ("lecture d'enregistrement") et de

"write record" ("écriture d'enregistrement") définis dans l'IEC 61158-5-3. Pour les petites quantités d'iParamètres, une version non segmentée ordinaire par "read record" et "write record" est suffisante (Tableau 23 et Tableau 24). Une réalisation possible de ces deux fonctions reposant sur les langages de programmation de l'IEC 61131-3 est présentée en [44] et appelée bloc de fonctions de communication RDREC et WRREC. Il est vivement recommandé aux systèmes de l'hôte F de fournir ces blocs de fonctions dans la bibliothèque se trouvant dans sa partie non relative à la sécurité.

Tableau 23 – Structure de Read_RES_PDU («read record»)

Structure de Read_RES_PDU	Taille	Codage	Remarques	
Function_Num	1 octet	0x5E	Indique "read", fixe	En-tête
Slot_Number	1 octet	0 à 255	Emplacement du module	
Indice	1 octet	0 à 254	Transfer_Index	
Longueur des données de réseau	1 octet	0 à 240	Longueur du segment iPar	
iParamètre (segment)	n octets	-	N = 240 par enregistrement au maximum	Données
NOTE Les structures correspondantes de CP 3/RTE sont disponibles en [44].				

Tableau 24 – Structure de Write_REQ_PDU («write record»)

Structure de Write_REQ_PDU	Taille	Codage	Remarques	
Function_Num	1 octet	0x5F	Indique "write", fixe	En-tête
Slot_Number	1 octet	0 à 255	Emplacement du module	
Indice	1 octet	0 à 254	Transfer_Index	
Longueur des données de réseau	1 octet	0 à 240	Longueur du segment iParamètre	
iParamètre	n octets	-	n = 240 maximum	Données

Pour les quantités d'iParamètres dépassant la limite d'enregistrement ou de mémoire tampon d'un esclave F/module F particulier, une version étendue des services acycliques "read record" ("lecture d'enregistrement") et "write record" ("écriture d'enregistrement") peut être utilisée. Elle est présentée dans l'IEC 61158-5-3 sous le nom services "Pull-Push" (Tableau 25 et Tableau 26).

Tableau 25 – Structure de Pull_RES_PDU («Pull»)

Structure de Pull_RES_PDU	Taille	Codage	Remarques	
Function_Num	1 octet	0x5E	Indique "Read", fixe	**En-tête**
Slot_Number	1 octet	0 à 255	Emplacement du module	
Indice	1 octet	0 à 254 (255)	Transfer_Index [a]	
Longueur des données de réseau	1 octet	0 à 240	Longueur du segment iPar + en-tête de région de chargement	
Extended_Function_Num	1 octet	0x02	Indique «Pull»	Région de chargement
Options	1 octet	Unsigned8	Contrôle du flux, voir 6.2.17.2 de l'IEC 61158-5-3	
Sequence_Number	4 octets	Unsigned32	...du segment iPar en cours	
iParamètre (segment)	n octets	Chaîne d'octets	n = 234 par enregistrement au maximum	Données

[a] Un Transfer_Index de 255 est dans ce cas conforme à l'IEC 61158-5-3. Toutefois, les conflits d'accès avec d'autres services (un service CALL des fonctions I&M, par exemple) doivent être pris en compte dans la phase de conception et de mise en œuvre. Tous les autres indices peuvent être utilisés pour les services «Pull» et «Push».

Tableau 26 – Structure de Push_REQ_PDU («Push»)

Structure de Push_REQ_PDU	Taille	Codage	Remarques	
Function_Num	1 octet	0x5F	Indique "Write", fixe	En-tête
Slot_Number	1 octet	0 à 255	Emplacement du module	
Indice	1 octet	0 à 254 (255)	Transfer_Index [a]	
Longueur des données de réseau	1 octet	0 à 240	Longueur du segment iPar + en-tête de région de chargement (Load Region)	
Extended_Function_Num	1 octet	0x01	Indique «Push»	Région de chargement
Options	1 octet	Unsigned8	Contrôle du flux, voir 6.2.17.2 de l'IEC 61158-5-3	
Sequence_Number	4 octets	Unsigned32	…du segment iPar en cours	
iParamètre (segment)	n octets	Chaîne d'octets	n = 234 par enregistrement au maximum	Données

[a] Un ''Transfer_Index'' de 255 est dans ce cas conforme à l'IEC 61158-5-3. Toutefois, les conflits d'accès avec d'autres services (un service CALL des fonctions I&M, par exemple) doivent être pris en compte dans la phase de conception et de mise en œuvre. Tous les autres indices peuvent être utilisés pour les services «Pull» et «Push».

Un hôte F ou un système associé non relatif à la sécurité peut offrir au serveur d'iParamètres un mécanisme totalement masqué pour l'utilisateur ou se présentant sous la forme d'un ensemble de fonctions de bibliothèque à configurer pour un projet particulier.

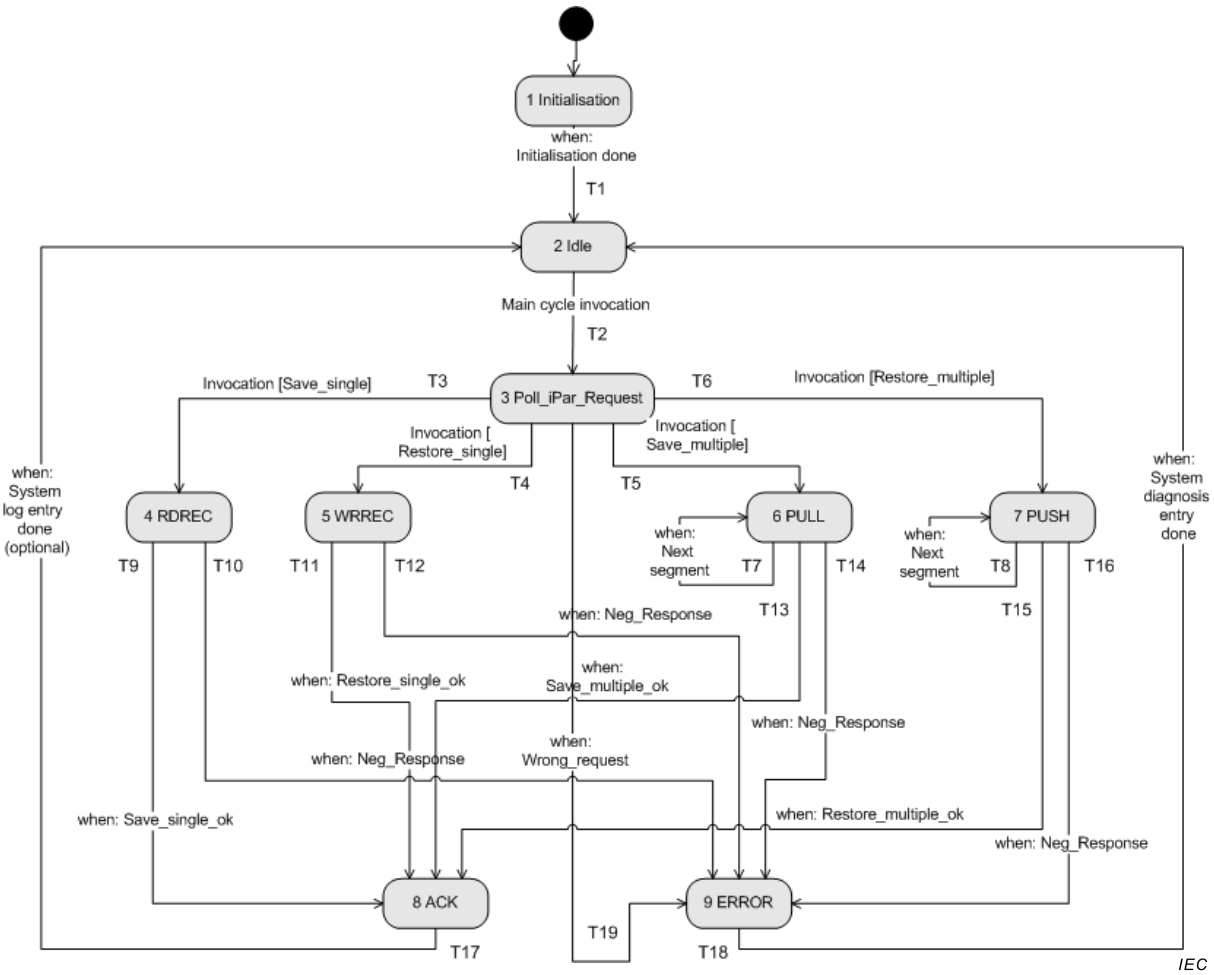
Le mécanisme de téléchargement aval et d'extraction (Upload&Retrieval) de CP 3/RTE défini dans l'IEC 61158-5-10, l'IEC 61158-6-10 et l'IEC 61784-2 (CP 3/RTE) est un exemple de serveur de paramètres standard.

Un module F d'une entrée-sortie distante utilise toujours un codage approprié, à chaque fois qu'il peut être déployé dans un appareil d'entrée-sortie distant CP 3/1 ou CP 3/RTE. Il revient à la station de tête d'un appareil d'entrée-sortie distant de transformer le codage du transfert d'iParamètre dans le format approprié du profil de communication réel, et inversement

Les indices des enregistrements des services "Save" (= téléchargement amont) ou "Restore" (= récupération, téléchargement aval) peuvent être différents. Il est également possible pour un service "Restore" de lire une plus petite quantité de données que celle préalablement sauvegardée. Ces données sauvegardées peuvent contenir des informations de contrôle (type d'appareil, longueur des données, signature CRC, par exemple) en plus de l'iParamètre. Le téléchargement aval d'un court enregistrement avec les informations de contrôle permet de vérifier l'intégrité et l'actualité des données sans compromettre les performances.

8.6.4.4 Protocole

La Figure 72 et le Tableau 27 présentent respectivement le diagramme d'états du serveur d'iParamètres et les états, transitions et éléments internes du serveur d'iParamètres. Voir 7.2.2 pour obtenir des informations générales relatives à la notation UML2.



Anglais	Français
Main cycle invocation	Appel du cycle principal
Invocation	Appel
System log entry (optional)	Entrée du journal système (facultatif)
System diagnosis entry	Entrée de diagnostic du système
Next segment	Segment suivant

Figure 72 – Diagramme d'états du serveur d'iParamètres

Les termes utilisés dans la Figure 72 sont spécifiés ci-dessous:

Save_single	Demande du serveur d'iParamètres pour sauvegarder (exporter) un bloc d'iParamètres par enregistrement simple (RDREC)
Restore_single	Demande du serveur d'iParamètres pour restaurer (importer) un bloc d'iParamètres par enregistrement simple (WRREC)
Save_multiple	Demande du serveur d'iParamètres pour sauvegarder (exporter) un bloc d'iParamètres plus important par enregistrements multiples (PULL)
Restore_multiple	Demande du serveur d'iParamètres pour restaurer (importer) un bloc d'iParamètres plus important par enregistrements multiples (PUSH)
System log entry (Entrée du journal système)	Toutes les actions de sauvegarde et de restauration qui ont abouti peuvent être enregistrées dans un fichier journal du serveur d'iParamètres (facultatif)

System diagnosis entry (Entrée de diagnostic du système)	Toutes les actions de sauvegarde et de restauration qui n'ont pas abouti doivent être signalées par un diagnostic du système.
Neg_Response	À chaque fois qu'une fonction du système (RDREC, WRREC, PULL ou PUSH, par exemple) s'arrête avec une erreur, le serveur d'iParamètres doit créer une entrée de diagnostic du système
Incorrect_request	À chaque fois que le serveur d'iParamètres détecte un type de demande erroné ou l'absence de réaction de l'une des fonctions système appelées, il doit arrêter l'action et créer une entrée de diagnostic du système

Tableau 27 – États et transitions du serveur d'iParamètres

NOM D'ÉTAT	DESCRIPTION DE L'ÉTAT
1 Initialisation	État de démarrage à froid; si défini, initialiser les sorties
2 Repos	État de repos, pas d'action
3 Poll_iPar_Request	Dans le cadre de l'appel du cycle principal ou d'une activité analogue dans un sous-système contrôlé, la demande du serveur d'iParamètres est interprétée dans le corps des informations de diagnostic, et le service système correspondant doit être lancé. En cas d'erreur, l'état ERROR doit être entré
4 RDREC	Dans cet état, la fonction système RDREC conforme à [44] ou une fonction analogue doit être appelée afin d'exécuter une fonction de lecture selon le CP 3/1 ou le CP 3/2 de l'IEC 61158-5-3
5 WRREC	Dans cet état, la fonction système WRREC conforme à [44] ou une fonction analogue doit être appelée afin d'exécuter une fonction d'écriture selon le CP 3/1 ou le CP 3/2 de l'IEC 61158-5-3
6 PULL	Dans cet état, la fonction système PULL doit être appelée pour exécuter une fonction de lecture multiple grâce à «Extended_Function_Num = 0x02» selon le CP 3/1 ou le CP 3/2 de l'IEC 61158-5-3
7 PUSH	Dans cet état, la fonction système PUSH doit être appelée pour exécuter une fonction d'écriture multiple grâce à «Extended_Function_Num = 0x01» selon le CP 3/1 ou le CP 3/2 de l'IEC 61158-5-3
8 ACK	Dans cet état, toutes les actions de sauvegarde et de restauration qui ont abouti peuvent être enregistrées dans un «fichier journal du serveur d'iParamètres du système» (facultatif)
9 ERROR	Dans cet état, à chaque fois qu'une fonction du système (RDREC, WRREC, PULL ou PUSH, par exemple) s'arrête avec une erreur, ou en cas de demande erronée, le serveur d'iParamètres doit créer une entrée de diagnostic du système

TRAN-SITION	ETAT SOURCE	ETAT CIBLE	ACTION
T1	1	2	-
T2	2	3	Appel du cycle principal (ou d'un événement analogue dans un sous-système contrôlé)
T3	3	4	Appel de la fonction RDREC pour le téléchargement amont d'un seul bloc d'iParamètres
T4	3	5	Appel de la fonction WRREC pour le téléchargement aval d'un seul bloc d'iParamètres
T5	3	6	Appel de la fonction POLL pour le téléchargement amont multiple d'un bloc d'iParamètres plus important segmenté
T6	3	7	Appel de la fonction PUSH pour le téléchargement aval multiple d'un bloc d'iParamètres plus important segmenté
T7	6	6	Début de la lecture du segment suivant
T8	7	7	Début de l'écriture du segment suivant
T9	4	8	Début de l'entrée d'une exécution RDREC qui a abouti dans le fichier journal du système (facultatif)
T10	4	9	Début de l'entrée de diagnostic du système

TRAN-SITION	ETAT SOURCE	ETAT CIBLE	ACTION
T11	5	8	Début de l'entrée d'une exécution WRREC qui a abouti dans le fichier journal du système (facultatif)
T12	5	9	Début de l'entrée de diagnostic du système
T13	6	8	Début de l'entrée d'une exécution POLL qui a abouti dans le fichier journal du système (facultatif)
T14	6	9	Début de l'entrée de diagnostic du système
T15	7	8	Début de l'entrée d'une exécution PUSH qui a abouti dans le fichier journal du système (facultatif)
T16	7	9	Début de l'entrée de diagnostic du système
T17	8	2	Mise en veille (repos)
T18	9	2	Mise en veille (repos)
T19	3	9	Début de l'entrée de diagnostic du système

8.6.4.5 Gestion du serveur d'iParamètres

Les mesures de gestion du serveur d'iParamètres visant à garantir l'authenticité, la validité et l'intégrité des données des iParamètres sont présentées dans le Tableau 28. Le module F, l'esclave F ou l'appareil F est chargé de fournir les mesures de sécurité pour les mécanismes de sauvegarde et de restauration. Le serveur d'iParamètres ne fait que stocker les iParamètres sous la forme de flux d'octets et peut également faire office de serveur de paramètres standard pour les appareils non relatifs à la sécurité.

Tableau 28 – Mesures de gestion du serveur d'iParamètres

Élément/Phase	Articles /Para-graphes	Description
F_S/D_Address	8.1.2 7.3.7 9.1	L'utilisation de F_Source/Destination_Address ou de F_S/D_Address abrégé est une condition préalable à la garantie d'authenticité des iParamètres sauvegardés et restaurés. Il n'est pas utile d'inclure F_S/D_Address dans le calcul iPar_CRC ou dans le bloc d'iParamètres. La remise correcte de F_iPar_CRC est déjà protégée par F_S/D_Address, de manière à pouvoir détecter un bloc d'iParamètres remis par erreur en comparant son iPar_CRC au F_iPar_CRC. Si F_S/D_Address est défini par un commutateur de codage, l'appareil de remplacement doit être ajusté au F_S/D_Address d'origine avant un redémarrage. Si F_S/D_Address est attribué à l'aide d'un outil CPD, le fabricant de l'appareil est chargé de fournir les moyens d'ajuster le F_S/D_Address d'origine avant un redémarrage
Démarrage	8.1.7 8.6.3 9.1	Après le démarrage, le module F, l'esclave F ou l'appareil F reçoit les paramètres F afin d'établir une communication CPF 3 (échange de données cycliques). La valeur préalablement établie de F_iPar_CRC est "0", ce qui permet de garantir l'état de sécurité de l'appareil et de s'assurer qu'il envoie des valeurs Failsafe (FV). La LED (verte) clignote à 2 Hz
Mise en service	-	Dans cette phase, l'appareil peut être configuré et paramétré à l'aide d'un outil CPD directement connecté ou utilisant des services de communication acycliques (MS2, par exemple). Le fabricant de l'appareil et de l'outil CPD correspondant est chargé de garantir la sécurité du paramétrage sur les canaux de communication standard et de définir la sécurité de l'appareil en mode d'essai FSCP
iPar_CRC / F_iPar_CRC	8.2 8.3.3.2	L'utilisation d'iPar_CRC et de son homologue F_iPar_CRC transmis de diverses manières est une condition préalable à la garantie d'intégrité des données des iParamètres sauvegardés et restaurés. Si la signature iPar_CRC calculée de l'outil CPD prend la valeur "0", elle doit être définie sur "1". Cela s'applique également au calcul de la signature iPar_CRC dans le module F, l'esclave F ou l'appareil F avant la comparaison à la valeur F_iPar_CRC provenant du paramétrage du démarrage

Élément/Phase	Articles /Para-graphes	Description
Propagation manuelle	8.1.7	L'iPar_CRC est calculé dans l'outil CPD en toute sécurité et doit être affiché au format hexadécimal. L'utilisateur peut alors transférer manuellement cette valeur dans le champ d'entrée ''F_iPar_CRC'' de l'outil de développement. Ce transfert peut être automatique si la sécurité est suffisante
Fonctions I&M	8.2	La validité d'un ensemble (bloc) d'iParamètres particulier d'un appareil remplaçant un autre appareil défectueux peut être vérifiée par exemple par les fonctions d'identification et de maintenance (I&M) «numéro de commande», «remise matérielle» et «remise logicielle». Il revient au fabricant de l'appareil de choisir les bonnes informations afin de garantir la validité
Vérification	-	En règle générale, la phase d'attribution d'iParamètres est finalisée par une étape particulière d'essai et de vérification, suivie d'une action de déconnexion et de reconnexion de l'appareil, ce qui provoque un démarrage et la transmission du F_iPar_CRC correct
Serveur d'iParamètres	-	Un module F, un esclave F ou un appareil F ne doit lancer qu'une seule demande de serveur d'iParamètres après un paramétrage de démarrage réussi (paramètres F)
Voyants LED	9.1	Tant que le module F, l'esclave F ou l'appareil F n'a pas sauvegardé ses iParamètres ou qu'il est toujours en mode d'essai FSCP, il doit indiquer cet état par les voyants LED décrits en 9.1. Dans ce cas, la fréquence de clignotement doit être de 2 Hz

8.6.4.6 Taille de l'iParamètre dans le fichier GSD

Un module F, un esclave F ou un appareil F peut indiquer la taille maximale de ses iParamètres grâce à l'entrée de mot clé "Max_iParamètre_Size" de son fichier GSD ("Max_iParameterSize" dans le fichier GSDML). Voir [40] et [43] pour plus de détails.

9 Exigences système

9.1 Voyants et commutateurs

En cas d'anomalie qui peut être liée à un appareil F particulier, l'hôte F définit le bit de contrôle 1 «Acquittement de l'opérateur demandé» de l'octet de contrôle (=1). Ce bit permet d'informer l'utilisateur que trois actions vont démarrer:

– contrôle de l'équipement et, le cas échéant, sa réparation ou son remplacement;
– vérification de la fonction de sécurité;
– acquittement de l'opérateur (OA_C).

Avec les appareils F compacts, il est vivement recommandé d'utiliser un voyant LED (la LED de bus bicolore existant, par exemple) qui clignote en vert à 0,5 Hz (= communication de bus ok, mais OA_C demandé). Avec les appareils modulaires, il convient d'utiliser une LED «d'opération de sécurité» dont dispose en général chaque module et clignotant en vert à 0,5 Hz (= communication de sécurité ok, mais OA_C exigé). La mise en œuvre est *facultative* pour les appareils F.

En *mode d'essai FSCP* ou tant que le module F, l'esclave F ou l'appareil F n'a pas procédé à la sauvegarde de ses iParamètres, le voyant LED ou la LED «d'opération de sécurité» doit indiquer cet état en clignotant en vert à 2 Hz.

Les paragraphes 7.3.7 et 8.1.2 donnent des informations sur la manière d'entrer la F_S/D_Address des appareils F grâce aux commutateurs.

9.2 Lignes directrices d'installation

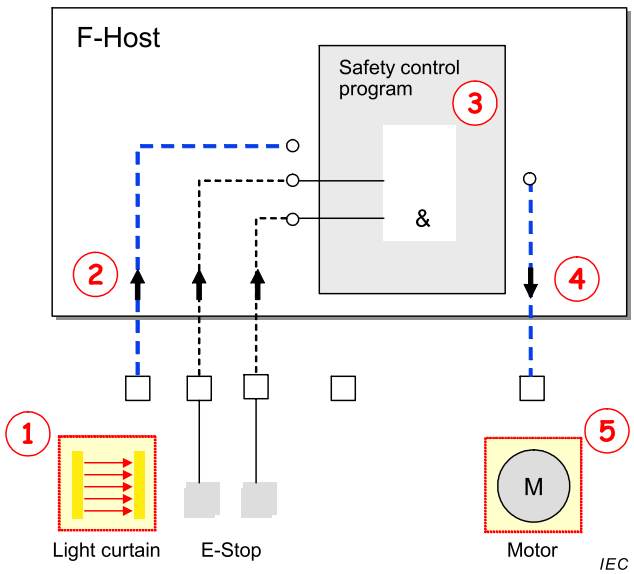
Les lignes directrices d'installation de l'IEC 61918 et les modifications spécifiques à la CPF 3 de l'IEC 61784-5-3 doivent s'appliquer. Des informations supplémentaires sont disponibles en [41].

9.3 Temps de réponse de la fonction de sécurité

9.3.1 Modèle

Une fonction de sécurité peut être composée de plusieurs capteurs (des rideaux de lumière et des boutons d'arrêt d'urgence, par exemple), d'un programme de commande de sécurité intégré à l'hôte F et d'un actionneur (un moteur, par exemple) (Figure 73).

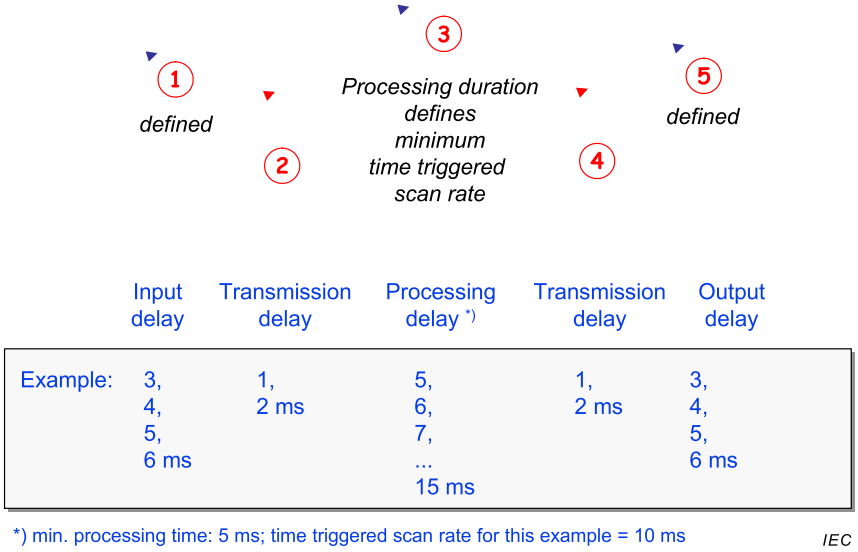
Chaque capteur détient son propre chemin de signal, et donc un temps de réponse classique particulier (voir la ligne pointillée bleue à la Figure 73).



Anglais	Français
F-host	Hôte F
Safety control program	Programme de commande de sécurité
Light curtain	Rideau de lumière
Motor	Moteur
E-stop	Arrêt d'urgence

Figure 73 – Exemple de fonction de sécurité avec chemin de temps de réponse critique

Ce temps de réponse classique est composé de plusieurs valeurs de temps individuelles, notamment des temps de transfert de bus (voir le modèle simplifié de temps de réponse classique de la Figure 74). Un exemple représente ce principe, qui peut être adopté pour le modèle de temps de réponse interne d'un appareil complexe.



Anglais	Français
Defined	Défini
Processing duration defines minimum time triggered scan rate	La durée du traitement définit la fréquence minimale de balayage déclenché par le temps
Input delay	Délai d'entrée
Transmission delay	Délai de transmission
Processing delay	Délai de traitement
Output delay	Délai de sortie
Example	Exemple
Min. processing time: 5ms; time triggered scan rate for this example = 10ms …	Temps min. de traitement: 5 ms; fréquence de balayage déclenché par le temps pour cet exemple = 10 ms

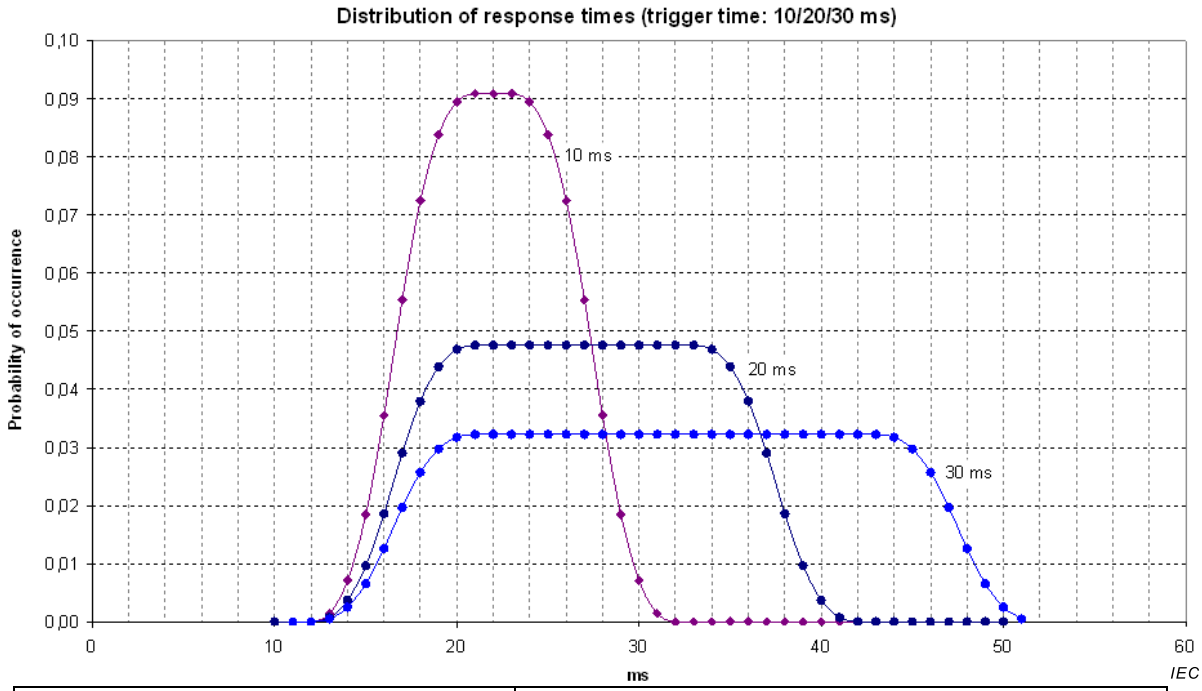
Figure 74 – Modèle simplifié de temps de réponse classique

L'exemple représente un chemin de signal composé d'un capteur, du transfert de bus vers l'hôte F, du traitement de l'hôte F, d'un autre transfert de bus vers l'appareil de sortie et de l'appareil de sortie (élément final).

Tous ces éléments présentent des délais minimaux (= traitement) et maximaux (= traitement + attente). Le délai réel peut être la durée (ou intervalle de temps) entre ces valeurs.

Dans ce modèle, l'hôte F est considéré être un contrôleur combiné pour les programmes standard et de sécurité. Le programme de sécurité est exécuté à un niveau de programme distinct déclenché par le temps et peut nécessiter un temps de traitement de 5 ms. Dans ce cas, la période de temps du déclencheur est de 10 ms, ce qui donne lieu à un délai de traitement compris entre 5 ms au minimum et 15 ms au maximum. Au total, le délai de cette fonction de sécurité est compris entre 13 ms au minimum et 31 ms au maximum.

La Figure 75 présente les distributions de fréquence des temps de réponse classiques du modèle pour une période de temps de déclencheur de 10 ms, 20 ms et 30 ms.



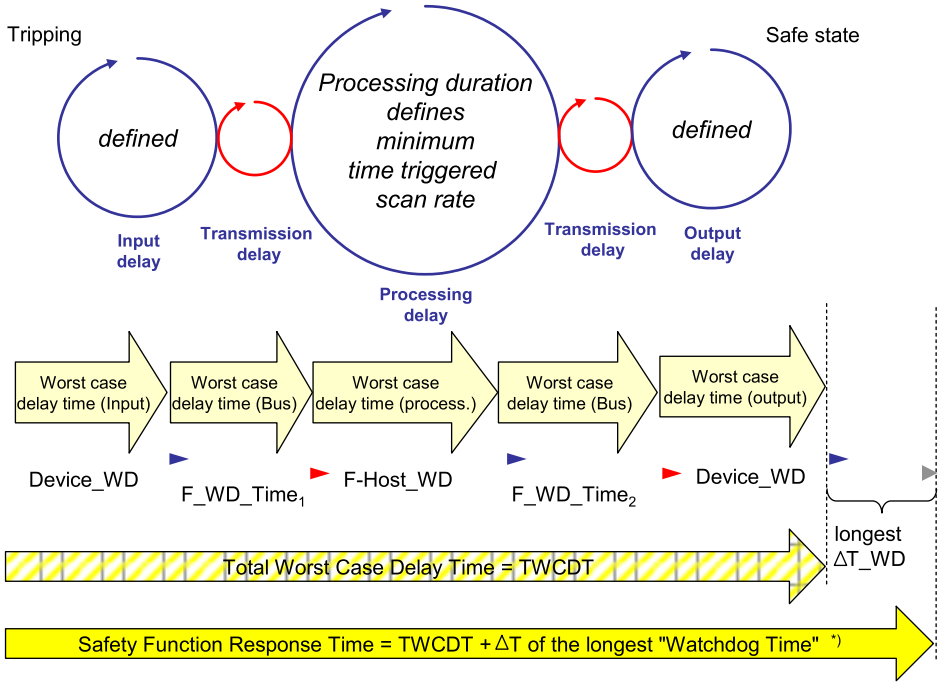
Anglais	Français
Distribution of response time (trigger time)	Distribution des temps de réponse (temps de déclencheur)
Probability of occurrence	Probabilité d'occurrence

Figure 75 – Distributions de fréquence des temps de réponse classiques du modèle

9.3.2 Calcul et optimisation

Le modèle des temps de réponse classiques de 9.3.1 permet de définir le temps de réponse de la fonction de sécurité. Chacun des cycles du modèle peut varier entre le délai du cas le plus favorable et le délai du cas le plus défavorable ($WCDT_i$). Pour des raisons de sécurité, chaque cycle comporte son temporisateur de chien de garde superposé ($WDTime_i$), ce qui implique d'activer l'état de sécurité à chaque fois qu'une anomalie ou une erreur se produit dans cette entité particulière.

La Figure 76 représente le contexte des délais du cas le plus défavorable et des temps de fonctionnement du chien de garde.



Anglais	Français
Tripping	Déclenchement
Safe state	État de sécurité
Defined	Défini
Processing duration defines minimum time triggered scan rate	La durée du traitement définit la fréquence minimale de balayage déclenché par le temps
Input delay	Délai d'entrée
Transmission delay	Délai de transmission
Processing delay	Délai de traitement
Output delay	Délai de sortie
Worst case delay time	Délai du cas le plus défavorable
(input)	(entrée)
(process)	(processus)
(output)	(sortie)
Total worst case delay time	Délai total du cas le plus défavorable
Longest	Le plus long
Safety function Response Time = TWCDT + ΔT of the longest "Watchdog Time"	Temps de réponse de la fonction de sécurité = … du plus long «temps de fonctionnement du chien de garde»
Not necessarily the output device	Pas nécessairement l'appareil de sortie

Figure 76 – Contexte de délais et de temps de fonctionnement du chien de garde

Pour calculer le temps de réponse de la fonction de sécurité, une erreur ou une anomalie doit être considérée dans l'entité concernée du chemin de signal, contribuant à la différence de temps maximale entre le délai du cas le plus défavorable et son temps de fonctionnement du chien de garde (WDTime). L'équation correspondante (1) est présentée ci-dessous:

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

Où

SFRT Temps de réponse de la fonction de sécurité

TD Délai de transmission

$WCDT_i$ Délai du cas le plus défavorable de l'entité i

$WDTime_i$ Le WDTime est égal au délai qui sépare la réception d'un PDU de sécurité équipé d'un nouveau MNR et la réaction après l'expiration de F_WD_Time. Les expressions particulières pour les entités i sont les suivantes:

– Entrée: $OFDT_{Input}$

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

– Hôte F: $OFDT_{F\text{-}Host}$

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

– Sortie: $OFDT_{Output}$

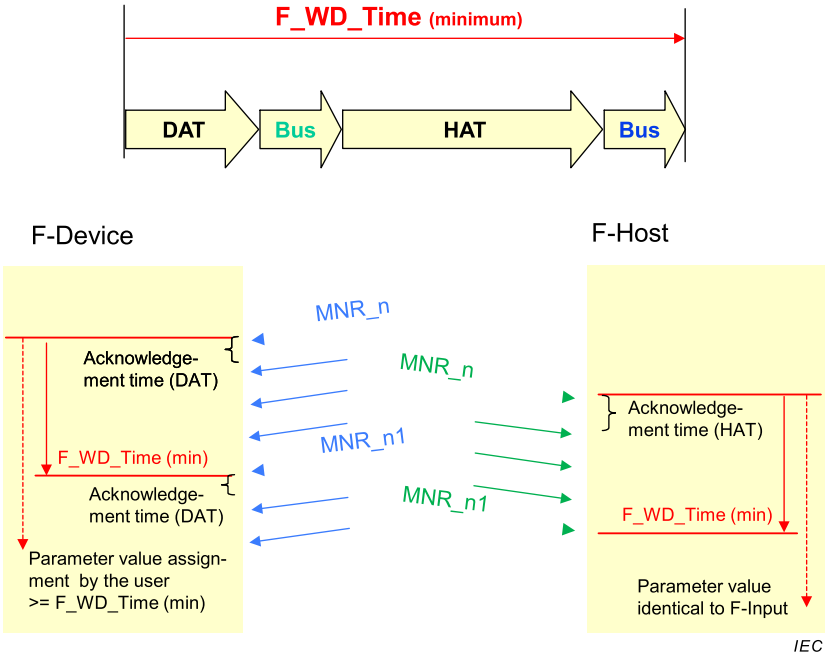
OFDT Délai d'une anomalie d'une entité, c'est-à-dire le délai du cas le plus défavorable en cas d'anomalie dans l'entité

$Tcy_{F\text{-}Host}$ Durée de cycle de l'hôte F

Les fabricants de systèmes doivent fournir leur méthode de calcul individuelle adaptée, le cas échéant.

9.3.3 Ajustement des temps de fonctionnement du chien de garde pour FSCP 3/1

Le paramètre F F_WD_Time détermine le temps de fonctionnement du chien de garde dans le cadre d'une relation de communication 1:1 de FSCP 3/1 (8.1.3). La Figure 77 indique que le temps de fonctionnement minimal du chien de garde est composé de quatre sections de temporisation (DAT – Bus – HAT – Bus).



Anglais	Français
F-device	Appareil F
F-host	Hôte F
Acknowledgement time	Temps d'acquittement
Parameter value assignment by the user	Attribution de valeur de paramètre par l'utilisateur
Parameter value identical to F-Input	Valeur de paramètre identique à l'entrée F

Figure 77 – Sections de temporisation formant le F_WD_Time de FSCP 3/1

À chaque fois que le pilote F (6.2) d'un appareil F compact ou du module F d'un appareil modulaire détecte un PDU de sécurité (trame FSCP 3/1) équipé d'un nouveau MNR, il redémarre le temporisateur du chien de garde. Ensuite, il traite le protocole FSCP 3/1 en prenant les *valeurs de processus actuellement disponibles*, puis prépare un nouveau PDU de sécurité. Le temps écoulé pour cette opération est appelé "DAT = Device Acknowledgement Time (Temps d'acquittement de l'appareil)".

NOTE Dans le cas d'un appareil F modulaire, le DAT comprend les temps de transfert interne sur le bus de fond de panier.

Le transfert du nouveau PDU de sécurité vers l'hôte F caractérise la section de temporisation suivante (Bus). Dès que le pilote F de l'hôte F reçoit le nouveau PDU de sécurité, il redémarre le temporisateur de son chien de garde et traite le protocole FSCP 3/1. Il génère un PDU de sécurité équipé du MNR suivant. Le temps écoulé pour cette opération est appelé "HAT = Host Acknowledgement Time (Temps d'acquittement de l'hôte)". Le transfert du PDU de sécurité vers l'appareil F caractérise la dernière section de temporisation (Bus).

Le temps de fonctionnement du chien de garde qui doit être attribué au paramètre F est plus long que le *temps minimal de fonctionnement du chien de garde* afin de s'assurer qu'un événement d'urgence a été détecté.

Selon 8.1.3, la valeur à attribuer à F_WD_Time dans l'exemple de la Figure 74 (Temps de déclencheur = 10 ms) serait de 2 x transmission de bus (2 × 2 ms) plus le DAT de l'appareil (6 ms) et de l'hôte F (15 ms): F_WD_Time = 4 ms + 6 ms + 15 ms = 25 ms. L'ajustement d'un temps de fonctionnement plus court du chien de garde n'a aucun impact sur la sécurité du système. Il peut provoquer des déclenchements de nuisance et affecter ainsi sa disponibilité.

La possibilité qu'un appareil puisse étendre les temps de transfert de bus en cas de message de diagnostic doit également être prise en compte pour réserver l'allocation de temps nécessaire au cours des ajustements du temporisateur du chien de garde. L'influence des appareils de supervision supplémentaires (ou classe maître 2 dans CP 3/1) sur les temps de réponse est négligeable comme présenté à la Figure A.3. D'autres influences sont décrites en 9.3.5.

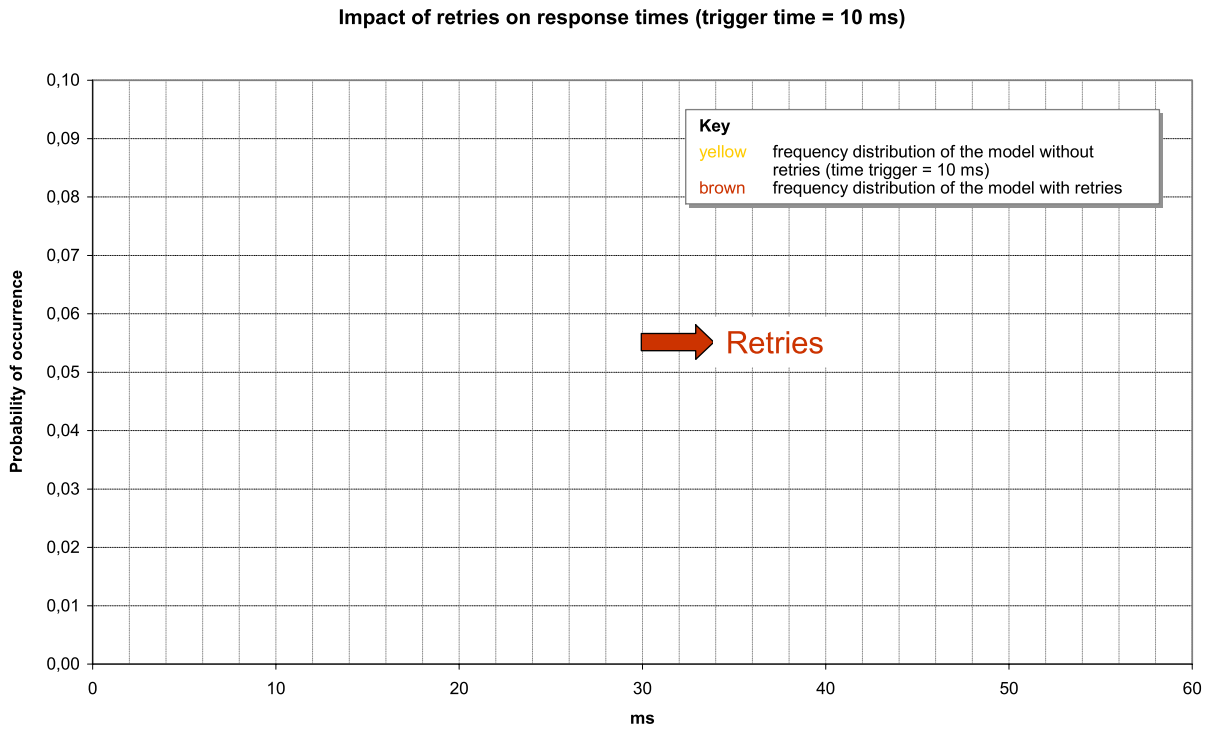
L'équation (1) de 9.3.2 est valide dans le cas où les temporisations de DAT, HAT et des transmissions de bus peuvent être garanties. Une valeur sensiblement supérieure à la somme DAT + HAT + 2 x temps de transmission de bus doit être attribuée au paramètre F F_WD_Time principal. Il est vivement recommandé de faire en sorte que la différence entre la valeur de paramètre attribuée et cette somme ne dépasse pas 30 %. Les fabricants de systèmes peuvent ajuster cette règle en fonction de leurs besoins particuliers.

9.3.4 Prise en charge de l'outil de développement

Il convient que les outils de développement permettent d'estimer déjà les temps de réponse de la fonction de sécurité, lors de la phase de planification pour prendre en charge le dimensionnement des distances dans la conception mécanique, et lors de la phase de mise en service pour prendre en charge l'attribution des paramètres du chien de garde.

9.3.5 Relances (répétition des messages)

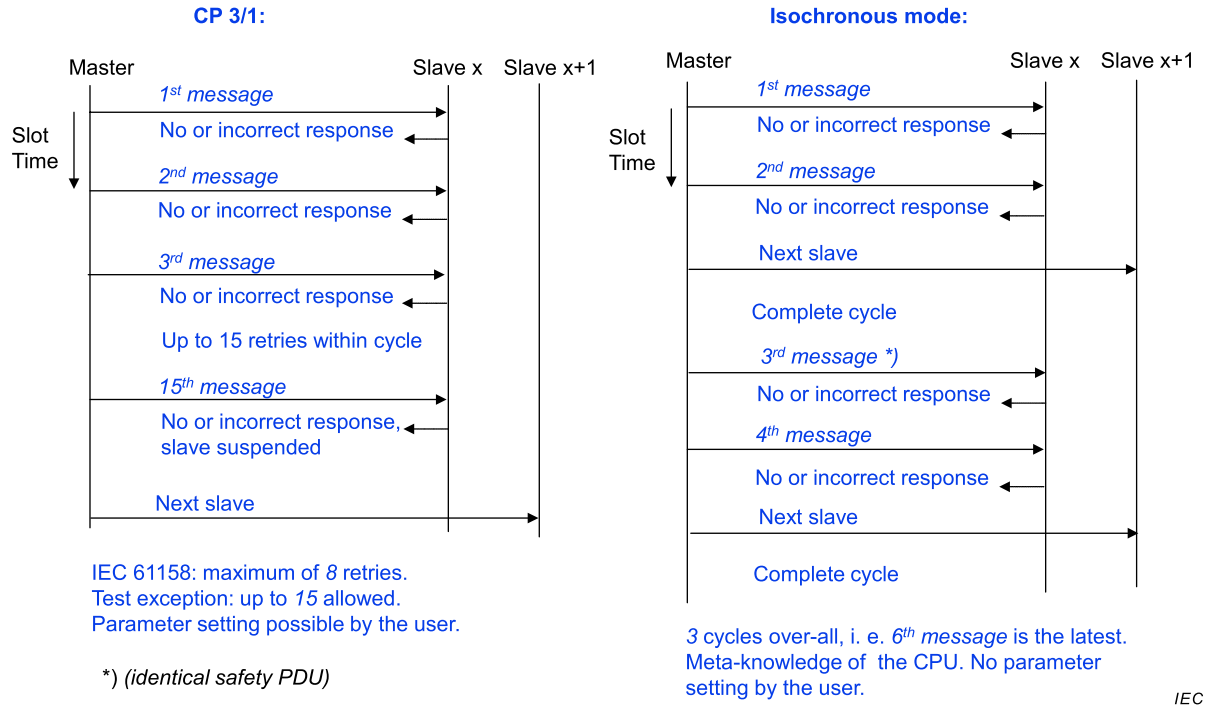
En cas de perturbations électromagnétiques extrêmes ou de non-conformité des appareils aux normes de bus de terrain en matière de bruits électriques inacceptables sur les voies de communication de données, les systèmes de bus de terrain tendent à utiliser des mécanismes de relance pour augmenter la disponibilité. Lors de la phase de mise en service, il est de bonne pratique d'ingénierie de vérifier chaque connexion au niveau de tous les appareils (non relatifs à la sécurité ou de sécurité) pour déterminer leurs nombres de relances et, le cas échéant, de prendre les mesures qui s'imposent (application correcte des lignes directrices d'installation ou utilisation d'appareils dont la conformité a été soumise à essai, par exemple) (Article 10). Cela ne permet pas uniquement d'augmenter la disponibilité, mais également d'assurer des temps de réaction courts sans déclenchement de nuisance (Figure 78).



Anglais	Français
Probability of occurrence	Probabilité d'occurrence
Impact of retries on response times (trigger time = 10 ms)	Impact des relances sur les temps de réponse (temps de déclencheur = 10 ms)
Key	Légende
Yellow	Jaune
Brown	Brun
Frequency distribution of the model without retries (time trigger = 10 ms)	Distribution de fréquence du modèle sans relance (temps de déclencheur = 10 ms)
Frequency distribution of the model with retries	Distribution de fréquence du modèle avec relances
Retries	Relances

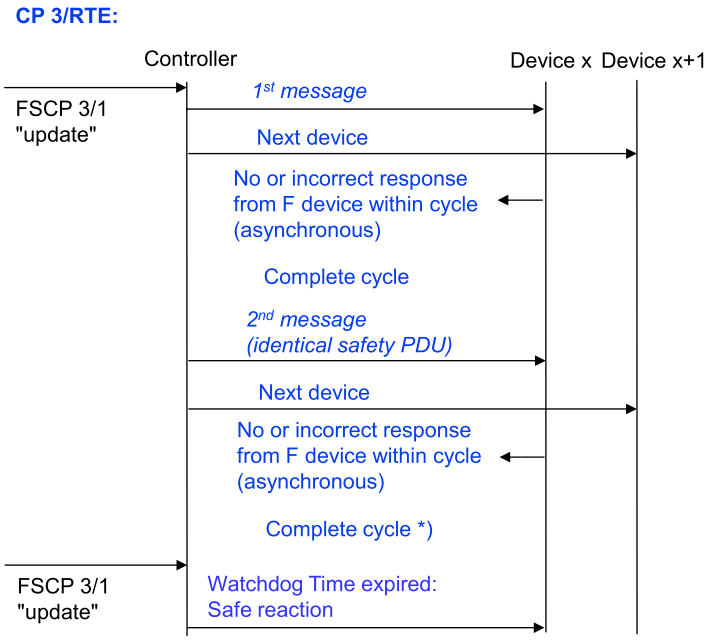
Figure 78 – Distribution de fréquence des temps de réponse avec relances de message

La Figure 79 représente les mécanismes de relance avec CP 3/1, alors que la Figure 80 représente les mécanismes de relance pour CP 3/RTE. Pour évaluer la sécurité, il peut s'avérer également nécessaire de connaître le comportement de relance des canaux noirs.



Anglais	Français
Master	Maître
Isochronous mode	Mode isochrone
Slave	Esclave
Slot time	Créneau horaire
1st message	1er message
No or incorrect response	Aucune réponse ou réponse incorrecte
2nd message	2e message
Next slave	Esclave suivant
3rd message	3e message
Complete cycle	Cycle complet
Up to 15 retries within cycle	Jusqu'à 15 relances au cours du cycle
15th message	15e message
Slave suspended	Esclave interrompu
IEC 61158: maximum of 8 retries. Test exception: up to 15 allowed. Parameter setting possible by the user.	IEC 61158: 8 relances au maximum Exception d'essai: jusqu'à 15 admises Réglage des paramètres possible par l'utilisateur
(identical safety PDU)	(PDU de sécurité identique)
3 cycles over-all, i.e 6th message is the latest. Meta-knowledge of the CPU. No parameter setting by the user.	3 cycles sur l'ensemble, c'est-à-dire le 6e message est le dernier. Méta-connaissance du CPU. Aucun réglage de paramètre par l'utilisateur

Figure 79 – Relances avec CP 3/1



Anglais	Français
To	à
Controller	Contrôleur
Device	Appareil
1st message	1er message
No or incorrect response	Aucune réponse ou réponse incorrecte
2nd message	2e message
Next device	appareil suivant
«update»	«mise à jour»
From F device within cycle	Depuis l'appareil F au cours du cycle
(asynchronous)	(asynchrone)
Complete cycle	Cycle complet
Watchdog time expired: Safe reaction	Temps de fonctionnement du chien de garde expiré: réaction sécurisée
(identical safety PDU)	(PDU de sécurité identique)
See CP3/4 for maximum number of retries	Voir CP 3/4 pour le nombre maximal de relances

Figure 80 – Relances avec CP 3/RTE

9.4 Durée des sollicitations

En règle générale, les «sollicitations de réaction sécurisée» proviennent, par exemple, des rideaux de lumière, des appareils d'arrêt automatique de sécurité, des appareils de commande bimanuelle, des appareils d'arrêts d'urgence et analogues. Ces signaux

– doivent être au moins aussi longs, ou plus longs, que le temps de sécurité de processus ou que la temporisation FSCP 3/1 (F_WD_Time) respectivement;

– peuvent être plus courts que le temps de sécurité de processus ou que la temporisation FSCP 3/1 (F_WD_Time) respectivement; Dans ce cas, une réaction sécurisée est possible. Exemple: une mouche qui traverse un rideau de lumière.

Dans le F_WD_Time, des PDU de sécurité portant le même MNR et des valeurs de processus différentes peuvent être reçus après la permutation des messages dans le canal noir.

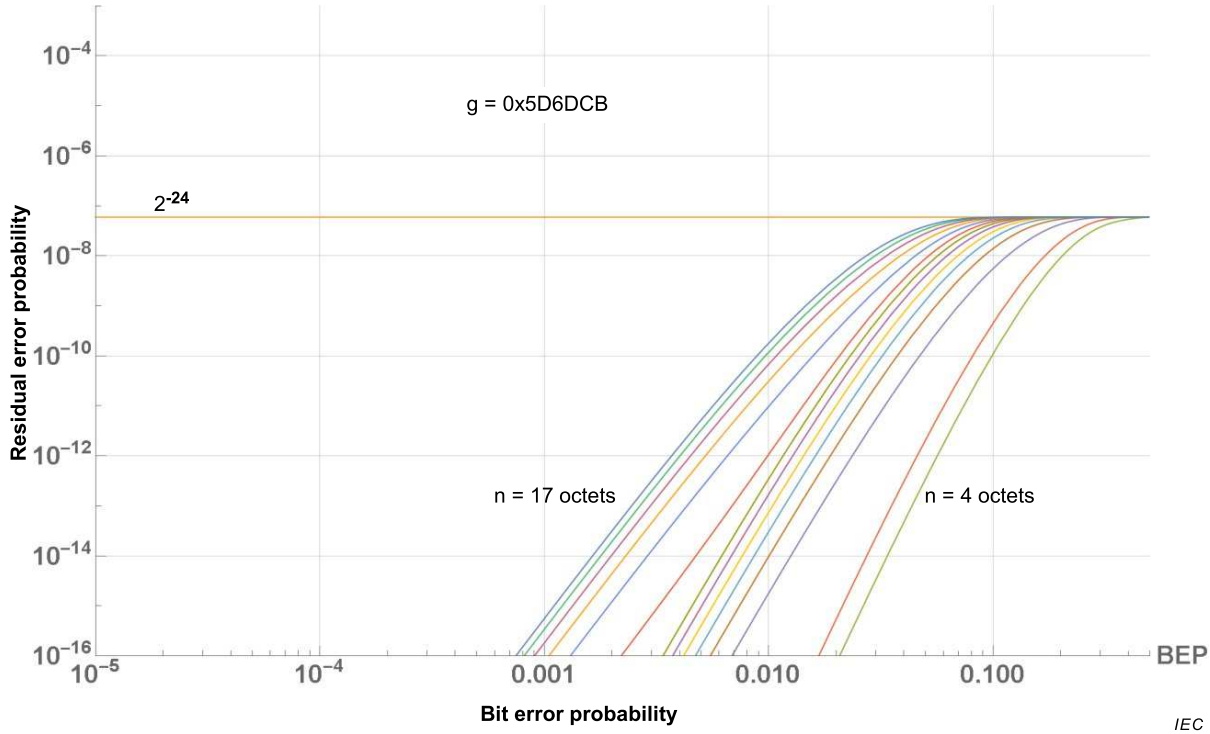
9.5 Contraintes liées au calcul des caractéristiques des systèmes

9.5.1 Considérations probabilistes

Le mécanisme de contrôle de l'intégrité des données du protocole FSCP 3/1 est indépendant des mécanismes du système de communication sous-jacent, qui est alors appelé «canal noir». Par conséquent, il peut également être utilisé pour les canaux de communication de fond de panier.

Conformément à l'IEC 62280-1, «l'exactitude» des polynômes générateurs CRC utilisés doit être démontrée. Cela implique de calculer la probabilité d'erreurs résiduelles en fonction de la probabilité d'erreurs sur les bits d'un polynôme particulier, ici pour les versions 24 bits (*0x5D6DCB*), et 32 bits (*0xF4ACFB13*).

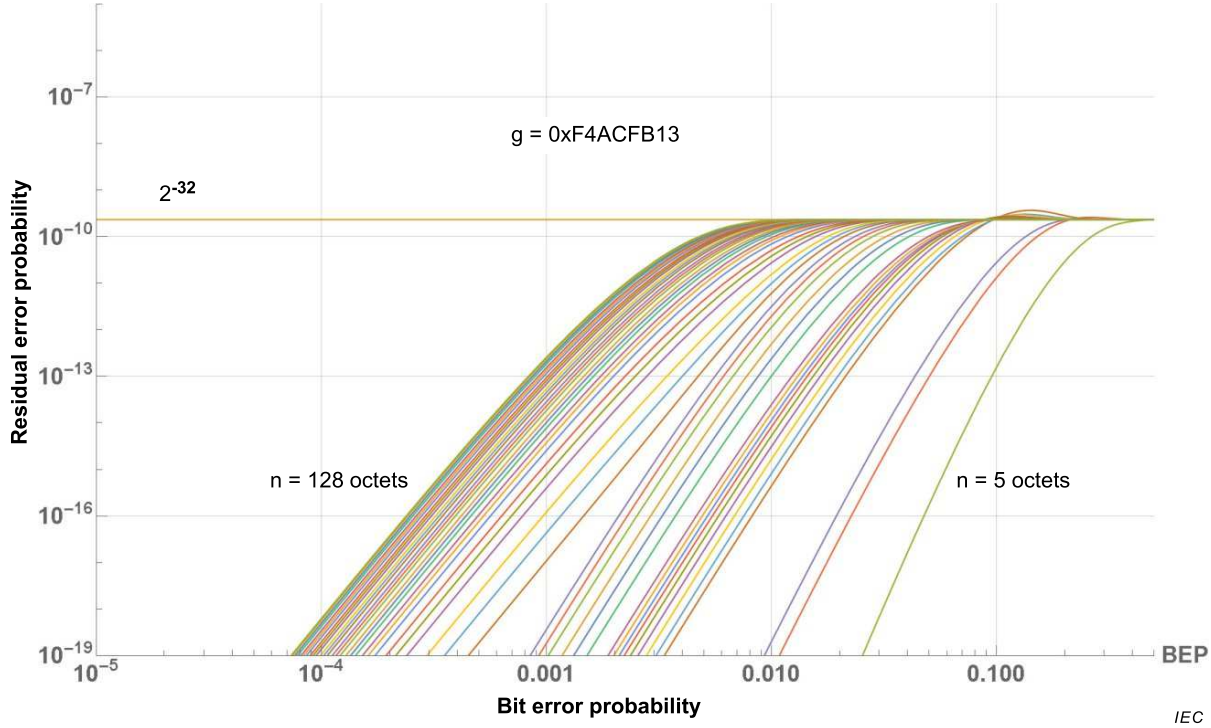
La Figure 81 présente les diagrammes de probabilités d'erreurs résiduelles d'un polynôme générateur CRC 24 bits. Les diagrammes calculés portent sur les longueurs de données incluant la signature CRC.



Anglais	Français
Residual error probability	Probabilité d'erreurs résiduelles
Red	Rouge
Black	Noir
Cyan	Cyan
Blue	Bleu
Bit error probability	Probabilité d'erreurs sur les bits
Bytes	Octets

Figure 81 – Probabilités d'erreurs résiduelles du polynôme CRC 24 bits

La Figure 82 représente les diagrammes du polynôme générateur CRC 32 bits.



Anglais	Français
Residual error probability	Probabilité d'erreurs résiduelles
Bit error probability	Probabilité d'erreurs sur les bits

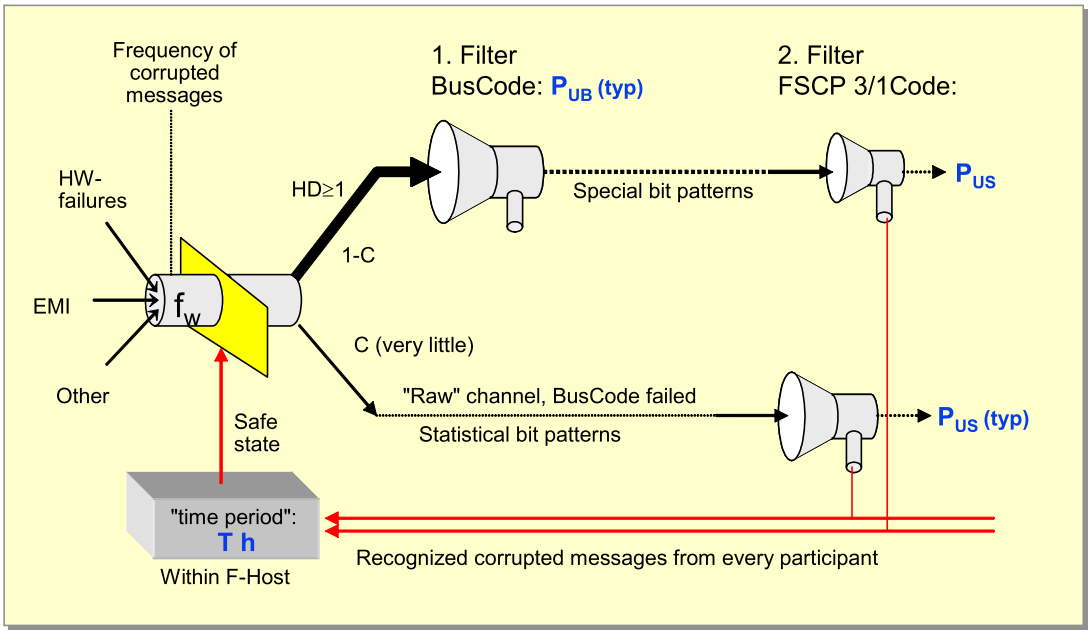
Figure 82 – Probabilités d'erreurs résiduelles du polynôme CRC 32 bits

Les termes utilisés dans la Figure 81 et la Figure 82 sont spécifiés ci-dessous:

g = polynôme générateur *0xF4ACFB13*

n = longueur de bit des données (incluant la signature CRC)

La Figure 83 récapitule les réflexions relatives aux influences perturbatrices. La combinaison des causes d'anomalie de bus et d'erreur donne une fréquence (fictive) de messages corrompus sur le système de transmission. Les mécanismes standard de détections d'erreurs de CP 3/RTE (1er filtre) reconnaissent toutes les anomalies jusqu'à un certain niveau. Par conséquent, seuls les profils binaires particuliers atteignent le mécanisme de couche de sécurité. Pour la fréquence des messages corrompus non détectés, la valeur la plus défavorable de c = 1/T est prise, étant donné que la fréquence globale des PDU de sécurité corrompus sur le bus est contrôlée en permanence.



Anglais	Français
Frequency of corrupted messages	Fréquence des messages corrompus
Filter	Filtre
HW-failures	Défaillances matérielles
Special bit patterns	Profils binaires spéciaux
Other	Autre
(Very little)	(très faible)
Safe state	État de sécurité
«raw» channel, BusCode failed	Canal «brut», BusCode défectueux
Statistical bit patterns	Profils binaires statistiques
«time period»	«durée»
Within F-host	Dans l'hôte F
Recognized corrupted messages from every participant	Messages corrompus reconnus provenant de chaque participant

Figure 83 – Surveillance des messages corrompus

Les termes utilisés dans la Figure 83 sont spécifiés dans le Tableau 29:

Tableau 29 – Définition des termes utilisés dans la Figure 83

Terme	Définition
fw	fréquence des messages corrompus
EMI	perturbation électromagnétique
HD	distance de Hamming
c	fréquence d'occurrence
T	période de mesure en heures (voir 7.2.6)

En cas de défaillance des mécanismes de sécurité des couches d'entrée-sortie CP 3/1 et CP 3/RTE standard (très faible probabilité), les messages corrompus contenant des profils binaires statistiques atteignent alors le mécanisme de la couche de sécurité.

Ce protocole FSCP 3/1 permet un contrôle simple de tous les PDU de sécurité corrompus de l'hôte F et, par l'intermédiaire de l'octet d'état, du PDU de sécurité d'acquittement d'un appareil F.

9.5.2 Hypothèses relatives à la sécurité

Les conditions aux limites et les hypothèses liées aux évaluations et calculs de sécurité des taux d'erreurs résiduelles sont présentées ici.

En règle générale:

- Tous les appareils offrent une sécurité électrique TBTS/TBTP et un rapport d'essai de conformité CPF 3
- Les appareils de sécurité sont prévus pour évoluer dans un environnement industriel normal conformément à l'IEC 61000-6-2 ou à l'IEC 61131-2 et offrent une immunité plus importante conformément à l'IEC 61326-3-1 ou à l'IEC 61326-3-2

Protocole FSCP 3/1 (mode V2):

- Nombre de relances par type de canal (voir 9.3.5):
  Aucune restriction
- Nombre de collecteurs de messages relatifs à la sécurité par fonction de sécurité:
  voir Tableau 30
- Polynômes CRC du canal noir:
  Aucune restriction
- Mise en mémoire tampon active des éléments de réseau:
  Aucune restriction; tous les commutateurs sont admis (voir 7.3.9 et 5.4.2)
- Îlots de sécurité:
  Les routeurs à un seul port ne sont pas admis comme limites d'un îlot de sécurité (voir 7.3.11)
- Fractionnement du PDU de sécurité au niveau de l'octet:
  Aucune restriction
- Taille des données d'entrée-sortie F
  F_CRC_Seed =0: ≤ 12 octets
  F_CRC_Seed =1: ≤ 123 octets
- Durée d'observation de l'appareil de surveillance SIL:
  F_CRC_Seed =0: 100 h
  F_CRC_Seed =1: 10 h

9.5.3 Contraintes non relatives à la sécurité (disponibilité)

- Échange de données cycliques entre les hôtes et les appareils de terrain au cours d'une période définie (signe de vie)
- Remise garantie de tous les PDU de sécurité au niveau de la couche de sécurité (intégrité des données)

En règle générale:

– CP 3/1: Pas de dérivation (lignes secondaires)

– CP 3/RTE: Un seul hôte F par sous-module

– Les commutateurs Ethernet doivent être adaptés à l'environnement industriel standard tel que défini par exemple dans l'IEC 61131-2

Les appareils standards et de sécurité peuvent partager la même source d'alimentation 24V

9.6 Maintenance

9.6.1 Mise en service/remplacement du module F

Les modules F peuvent être remplacés pendant le fonctionnement du système. Seul le redémarrage de la fonction de sécurité correspondante est admis, en l'absence d'état de processus dangereux, et après acquittement de l'opérateur (OA_C).

9.6.2 Fonctions d'identification et de maintenance

Les fonctions d'identification et de maintenance (I&M) définissent un ensemble de paramètres d'un appareil F afin d'identifier les types d'appareils et les appareils individuels par l'intermédiaire d'un réseau CPF 3 et de prendre en charge sa maintenance [42]. Ces fonctions peuvent être utilisées pour prendre en charge l'iParamétrage défini en 8.2. Les appareils/modules F doivent mettre en œuvre l'ensemble obligatoire de fonctions I&M. De plus, ils doivent entrer une signature dans le champ IM4 (signature), indiquant la configuration et l'état de paramétrage de la sécurité de l'appareil/module F, si cette signature n'a pas déjà été intégrée dans celle du projet global de l'hôte F. Un accès en écriture externe dans le champ IM4 doit être refusé.

La fonction "Réinitialisation aux réglages usine" ("Reset to factory settings") du protocole CP 3/RTE ne doit pas réinitialiser les iParamètres, y compris le mot de passe d'accès et le champ IM4, sur les valeurs par défaut.

9.7 Manuel de sécurité

Conformément à l'IEC 61508-2, les fournisseurs de l'hôte F et de l'appareil F doivent fournir un manuel de sécurité. Dans le cas de FSCP 3/1, les instructions, informations et paramètres du Tableau 30 doivent être inclus.

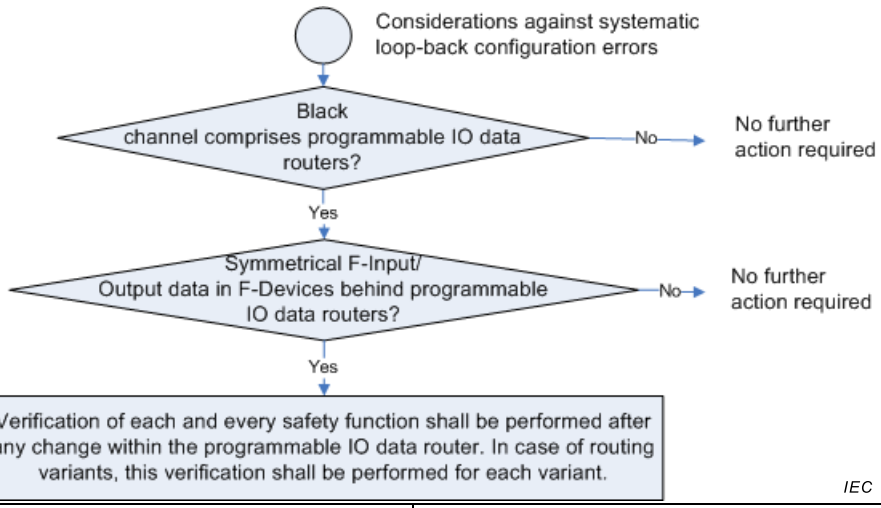
Tableau 30 – Informations à inclure dans le manuel de sécurité

Élément	Instruction et/ou paramètre	Remarque
Traitement de la sécurité	Instructions sur la manière de configurer, paramétrer, mettre en service, soumettre à essai et verrouiller la sécurité de cet appareil conformément à l'IEC 61508	Voir 9.1 (LED) et 7.3.7 Nom de code ("F_S/D_Address")
Relations de communication par fonction de sécurité (BP)	Pour le protocole de base: Un nombre maximum de 100 relations est considéré pour une probabilité moyenne d'une défaillance dangereuse par heure (PFH) de 10^{-9} (SIL3). Dans le cas d'un nombre supérieur à 100 relations, la PFH augmente de $4*10^{-12}$ par relation supplémentaire. De la même manière, un nombre maximum de 1 000 relations est considéré dans le cas de SIL2. De plus, l'arbre de décision de la Figure 84 doit être pris en considération.	Voir Tableau 37
Routeur de données ES programmable	Hôte F (BP): Considérations par rapport à des erreurs de configuration de bouclage systématiques (voir Figure 84)	Définitions [a]
	Hôte F (LP et XP): Aucune considération	
Alimentation	Des exigences relatives à la sécurité électrique (TBTP), à l'ondulation, au bruit, aux interruptions, etc. doivent être définies	Voir [41] pour connaître les contraintes spécifiques au pays (les limitations de courant, par exemple)
Sécurité électrique	Tous les appareils de réseau utilisés conjointement avec cet appareil doivent satisfaire aux exigences de l'IEC 61010-1 ou de l'IEC 61131-2 (TBTP, par exemple)	Voir [41]
Immunité électromagnétique (IEM)	Essais et résultats appliqués (déclaration du fabricant ou rapport d'essai provenant d'un laboratoire d'essai compétent)	Conformément à l'IEC 61326-3-1 ou -2, selon celle qui s'applique, ou norme spécifique à l'appareil (IEC 61496 [7]; [41], par exemple)

Élément	Instruction et/ou paramètre	Remarque
Isolation	Tensions d'essai appliquées et durée au niveau du port de communication du bus de terrain	Voir [41]
Composants de réseau	Contraintes sur les commutateurs, le routeur et d'autres composants de réseau	Voir 7.3.9, 7.3.11, 9.5.2 et 9.5.3
Installation	Conformément à l'IEC 61918 et à l'IEC 61784-5-3	Voir également [59]
Mise en service	Utilisation de la liste de contrôle de l'IEC 61784-5-3 relative, par exemple, à l'adressage correct, au contrôle de relance ou à la qualité du signal	Voir également [60] et 9.9
iParamètre	La vérification des fonctions de sécurité des appareils F prenant en charge le mode d'essai FSCP doit permettre de vérifier si une valeur supérieure à 0 a été attribuée à F_iPar_CRC.	Voir 8.6.4.5
Maintenance	Conditions et procédure de remplacement des pièces. Identification	Voir 9.6
Cycle de vie	Valeur(s) de paramètre d'intervalle d'essai de validité	Conformément à l'IEC 61508
Temps de réponse	Valeurs de paramètres pour DAT, WCDT, WDTime	Voir 9.3.2 et 9.3.3
Sécurité des machines (électrique)	Valeurs de paramètre pour la revendication du SIL, PFH (probabilité de défaillance par heure)	Conformément à l'IEC 62061
Sécurité des machines (non électrique)	Valeurs de paramètre pour PL (niveau de performance), MTTFd (Temps moyen entre défaillances dangereuses)	Conformément à l'ISO 13849-1
Sécurité d'automatisation de processus	Valeurs de paramètre pour la revendication du SIL, PFD (probabilité de défaillance sur sollicitation), possibilités d'interconnexion pour obtenir un SIL plus élevé	Conformément à l'IEC 61511 et à [33]
Appareil de surveillance SIL	Information pour les opérateurs, analogue à: "Dans le cas où une demande d'acquittement manuel de l'opérateur provoquée par un message de diagnostic associé (par exemple, le nombre 77 dans le Tableau 3) a été réceptionnée plus d'une fois dans une période de 100 heures, il est vivement recommandé d'appeler le technicien de service responsable". Information pour les opérateurs et les techniciens de service: "Cela pose le principe d'une perturbation importante de la transmission des données dans le système de bus de terrain. Les causes à l'origine de cet incident peuvent être des changements au niveau de l'installation, la corrosion des blindages de câbles de bus avec raccords et des perturbations électromagnétiques extrêmes. Il convient de vérifier la conformité avec les lignes directrices d'installation [61] ou [48], ou il convient d'appeler un spécialiste CEM (voir Annexe B pour un guide supplémentaire).	Voir 7.2.6.1.
Sécurité	Instructions sur la manière d'établir un niveau pertinent de sécurité en définissant des zones de sécurité équipées de portes de sécurité.	Voir 9.8, [41],[48]
Rapports d'évaluation et d'essai	Rapports d'évaluation de la sécurité conformément à l'IEC 61508 Interopérabilité et rapports d'essai de conformité afin d'octroyer la conformité CPF 3	Voir Article 10

[a] "Routeur de données ES programmable" = Un utilisateur peut délibérément définir le cheminement des données ES sur la base des adresses logiques

"Routeur configurable" = Un utilisateur peut sélectionner le cheminement des messages sur la base des adresses de réseau (adresses géographiques) à l'aide d'un outil de développement



Anglais	Français
Considerations against systematic loop-back configuration errors	Considérations par rapport aux erreurs de configuration de bouclage systématiques
Black channel comprises programmable IO data routers ?	Le canal noir comporte-t-il des routeurs de données ES programmables ?
No	Non
No further action required	Aucune autre action exigée
Yes	Oui
Symmetrical F-input/Output data in F-Devices behind programmable IO data routers?	Les appareils F derrière les routeurs de données ES programmables contiennent-ils des données d'entrée/sortie F symétriques?
Verification of each and every safety function shall be performed after any change within the programmable IO data router. In case of routing variants, this verification shall be performed for each variant.	Toutes les fonctions de sécurité doivent être vérifiées après tout changement au niveau du routeur de données programmable. Dans le cas de variantes de cheminement, cette vérification doit être effectuée pour chaque variante.

Figure 84 – Considérations par rapport aux erreurs systématiques de configuration de bouclage

9.8 Canaux de transmission sans fil

9.8.1 Approche du canal noir

Les canaux de transmission sans fil sont classés comme faisant partie intégrante du canal noir et, à ce titre, il n'est pas utile d'évaluer leur sécurité étant donné que FSCP 3/1 est approuvé pour une probabilité d'erreurs sur les bits de 10^{-2}.

9.8.2 Disponibilité

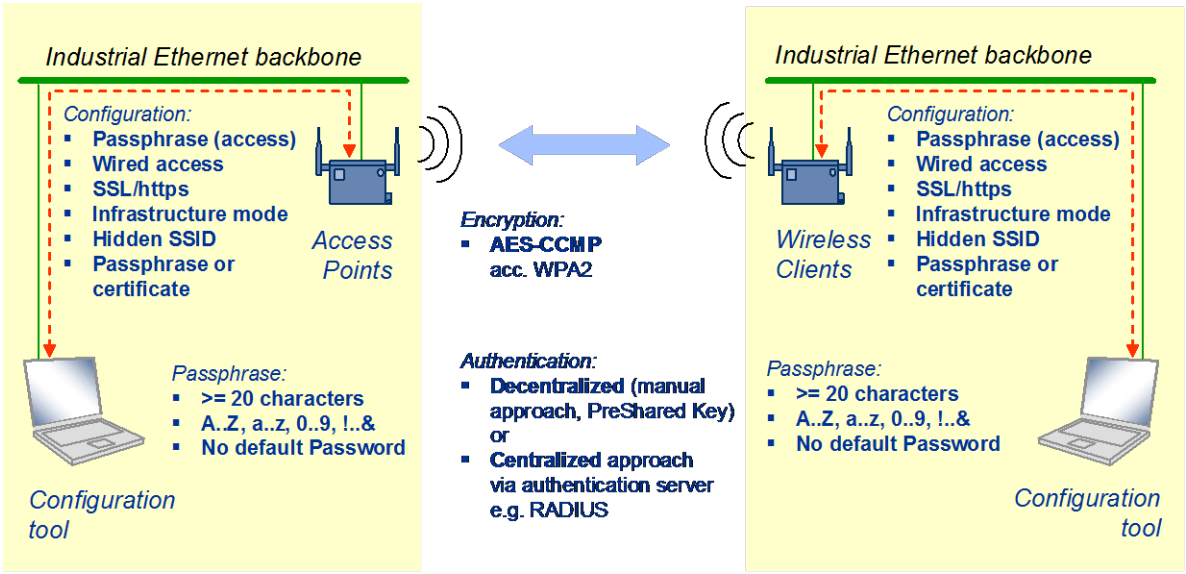
L'un des défis majeurs de la transmission sans fil est sa disponibilité. L'utilisateur doit mettre en place des mesures appropriées pour garantir une disponibilité suffisante en cas d'itinérance, de surtemps ou de coupure de communication en raison de réflexions, d'interférences ou d'autres causes de déclenchement de nuisances. Les déclenchements de nuisances peuvent donner lieu à l'arrêt ou au retrait de l'équipement de sécurité (mauvaise utilisation prévisible).

9.8.3 Mesures de sécurité

Avant de déployer une application de sécurité avec FSCP 3/1 et des composants sans fil, les menaces dangereuses (écoutes illicites ou manipulation de données, par exemple) doivent être évaluées comme énoncé en [41]. En l'absence de menace, aucune mesure de sécurité n'est nécessaire. Les menaces possibles peuvent être évaluées de deux manières:

- Modifications délibérées des paramètres des appareils F et des programmes de sécurité
- Attaques portées sur la communication cyclique (simulation de la communication de sécurité, par exemple)

La Figure 85 présente les mesures de sécurité.



Anglais	Français
Industrial Ethernet backbone	Épine dorsale Ethernet industrielle
Passphrase (access)	Phrase-passe (accès)
Wired access	Accès filaire
Infrastructure mode	Mode infrastructure
Hidden SSD	SSD masqué
Passphrase or certificate	Phrase-passe ou certificat
Access points	Points d'accès
Wireless clients	Clients sans fil
Encryption	Chiffrement
20 characters	20 caractères
No default password	Pas de mot de passe par défaut
Configuration tool	Outil de configuration
Authentication: Decentralized (manual approach, PreShared Key) or	Authentification: Décentralisée (approche manuelle, clé préalablement partagée) ou
Centralized approach via authentication server e.g. RADIUS	Approche centralisée (approche par serveur d'authentification, par exemple RADIUS)

Figure 85 – Sécurité des réseaux WLAN

Les termes utilisés dans la Figure 85 sont spécifiés dans le Tableau 31.

Tableau 31 – Définition des termes utilisés dans la Figure 85

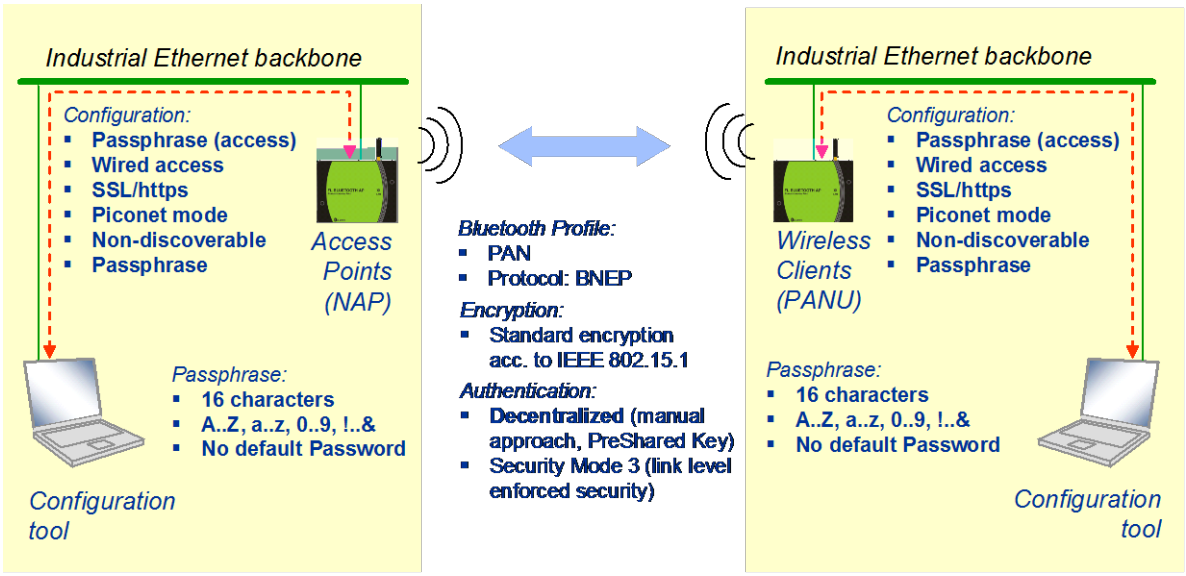
Terme	Définition
AES-CCMP	Advanced Encryption Standard – Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
RADIUS	Remote Authentication Dial In User Service
SSID	Service Set Identifier (Identifiant d'ensemble de services)
SSL	Secure Sockets Layer
WPA2	Wi-Fi Protected Access 2 (correspond à l'IEEE 802.11 [29])
Point d'accès	Station de coordination d'un ensemble de services sans fil conformément à l'IEEE 802.11
Client sans fil	Station appartenant à un ensemble de services sans fil conformément à l'IEEE 802.11

Pour protéger le réseau sans fil contre ce type de cas, les mesures indiquées au Tableau 32 doivent être prises en compte conformément à l'IEEE 802.11 [29] pour les réseaux locaux sans fil industriels énoncés dans l'IEC 61784-2 pour les appareils de classe A.

Tableau 32 – Mesures de sécurité d'un réseau WLAN (IEEE 802.11)

N°	Élément	Mesure
1	Administration du point d'accès sans fil et du client sans fil	Seul l'accès filaire est autorisé par SSL ou https. Le mot de passe/la phrase-passe d'administration ne doit pas être celui/celle par défaut
2	Qualité de la phrase-passe pour d'administration	La phrase-passe doit contenir au moins 20 caractères. Il doit s'agir d'un mélange de caractères alphabétiques, de caractères numériques et de signes spéciaux
3	Modes opérationnels	Seul le *Mode d'infrastructure* est autorisé. Le *Mode ad hoc* ne doit pas être déployé
4	Approches d'authentification	L'Approche décentralisée (déploiement manuel des clés d'authentification) ou l'Approche centralisée (serveur d'authentification dédié, comme RADIUS, par exemple) sont autorisées. En présence d'un serveur d'authentification central avec itinérance, les temps de transfert doivent être plus courts que les durées de cycle
5	Procédures d'authentification	Pour l'authentification, la *Clé partagée* (= Secret préalablement partagé) ou les *Certificats* sont autorisés
6	Qualité de la phrase-passe pour le chiffrement	La phrase-passe doit contenir au moins 20 caractères (voir [29] H.4 Suggested pass-phrase-to PSK mapping). Il doit s'agir d'un mélange de caractères alphabétiques, de caractères numériques et de signes spéciaux
7	Chiffrement de la communication de données cycliques (PDU de sécurité)	AES-CCMP (conformément à WPA2*)* [29] doit être déployé sous la forme d'un algorithme de chiffrement.
8	SSID masqué	Le point d'accès sans fil doit être configuré de manière à masquer le SSID. Le SSID déployé ne doit pas être le SSID par défaut
NOTE 1 Il convient que la longueur de la phrase-passe soit acceptable étant donné que les mots de passe ou les phrases-passe doivent être entrés une seule fois pendant une session de mise en service. NOTE 2 Le chiffrement de la communication de données cycliques assure la protection contre la manipulation des données.		

Pour protéger le réseau sans fil, les mesures indiquées au Tableau 34 doivent être prises en compte conformément à l'IEEE 802.15.1 [30] pour les réseaux Bluetooth énoncés dans l'IEC 61784-2 pour les appareils de classe A. La Figure 86 présente les mesures de sécurité.



Anglais	Français
Industrial Ethernet backbone	Épine dorsale Ethernet industrielle
Passphrase (access)	Phrase-passe (accès)
Wired access	Accès filaire
Piconet mode	Mode picoréseau
Non-discoverable	Non détectable
Bluetooth profile	Profil bluetooth
Protocol	Protocole
Standard encryption acc. To IEEE 802.15.1	Chiffrement standard conformément à l'IEEE 802.15.1
Access points	Points d'accès
Wireless clients	Clients sans fil
Encryption	Chiffrement
16 characters	16 caractères
No default password	Pas de mot de passe par défaut
Configuration tool	Outil de configuration
Authentication: Decentralized (manual approach, Preshared Key) …	Authentification: Décentralisée (approche manuelle, clé préalablement partagée)
Security mode 3 (link level enforced security)	Mode de sécurité 3 (sécurité renforcée au niveau de la liaison)

Figure 86 – Sécurité des réseaux Bluetooth

Les termes utilisés dans la Figure 86 sont spécifiés dans le Tableau 33.

Tableau 33 – Définition des termes utilisés dans la Figure 86

Terme	Définition
SSL	Secure Sockets Layer
PAN	Personal Area Network (Réseau personnel)
BNEP	Bluetooth Network Encapsulation Protocol
NAP	Network Access Point (Point d'accès au réseau)
PANU	Personal Area Network User (Utilisateur du réseau personnel)
Point d'accès	Station de coordination (maître) d'un picoréseau sans fil conformément à l'IEEE 802.15.1 [30]
Client sans fil	Station (esclave) appartenant à un picoréseau sans fil conformément à l'IEEE 802.15.1

Tableau 34 – Mesures de sécurité pour Bluetooth (IEEE 802.15.1)

N°	Élément	Mesure
1	Administration du point d'accès sans fil et du client sans fil	Seul l'accès filaire est autorisé par SSL ou https. Le mot de passe/la phrase-passe d'administration ne doit pas être celui/celle par défaut
2	Qualité de la phrase-passe pour d'administration	La phrase-passe doit contenir au moins 16 caractères. Il doit s'agir d'un mélange de caractères alphabétiques, de caractères numériques et de signes spéciaux
3	Modes opérationnels	Les appareils doivent fonctionner en mode picoréseau de base, c'est-à-dire que chacun d'eux doit uniquement communiquer dans un seul picoréseau. Les réseaux éclatés ne doivent pas être déployés
4	Approches d'authentification	Les appareils Bluetooth doivent utiliser le mode de sécurité 3 (sécurité renforcée au niveau de la liaison) défini comme obligatoire dans l'IEEE 802.15.1. L'authentification est assurée dans une approche décentralisée à l'aide d'une phrase-passe (PIN). Les appareils ne permettant pas de modifier la phrase-passe ou fonctionnant uniquement en mode de sécurité 1 (pas de sécurité) ou 2 (sécurité au niveau du service) ne sont pas autorisés
5	Qualité de la phrase-passe pour le chiffrement	La phrase-passe doit contenir au moins 16 caractères. Il doit s'agir d'un mélange de caractères alphabétiques, de caractères numériques et de signes spéciaux
6	Chiffrement de la communication de données cycliques (PDU de sécurité)	Le chiffrement conforme à l'IEEE 802.15.1 est obligatoire
7	Possibilité de reconnaissance	Le point d'accès sans fil et les clients doivent être configurés de manière à ne pas être reconnus

NOTE 1 Il convient que la longueur de la phrase-passe soit acceptable étant donné que les mots de passe ou les phrases-passe doivent être entrés une seule fois pendant une session de mise en service.

NOTE 2 Le chiffrement de la communication de données cycliques assure la protection contre la manipulation des données.

9.8.4 Applications fixes et mobiles

Deux types d'application de sécurité doivent être considérés: les applications de sécurité «fixes», se caractérisant par des emplacements et des mouvements bien définis, et les applications de sécurité «mobiles».

Les applications fixes ne font l'objet d'aucune contrainte et évaluation particulières (systèmes de vidage et de remplissage tournants, par exemple).

Le déploiement mobile des composants sans fil fait l'objet de défis supplémentaires. En particulier, l'allocation univoque des fonctions de sécurité aux éléments finaux dangereux (comme les robots, par exemple (voir l'ISO 10218-1 [24]) doit être garantie.

9.9 Classes de conformité

Les fabricants d'appareils F s'appuient sur un ensemble minimum de fonctions que leurs homologues (hôte F) doivent prendre en charge en plus de la conformité au protocole FSCP 3/1. Les fonctions exigées figurent dans le Tableau 35.

Tableau 35 – Exigences de classe de conformité de l'hôte F

Élément	Automatisation des usines	Automatisme industriel	Remarque
Prise en charge GSD	V5.04 (PB-DP) de [40]; V2.31 (PN-IO) de [43]ou versions ultérieures	idem	Relatif aux paramètres F uniquement
Prise en charge de la passivation granulaire des canaux	Obligatoire pour l'hôte F (XP), voir Tableau 37	Idem	-
''F_CRC_Seed'' (voir 8.1.5.2) pris en charge	Obligatoire pour l'hôte F (XP), voir Tableau 37	Idem	Le ''CRC1'' précédent correspond à ''CRC_FP'' et doit être pris en charge
Vérification de bouclage par l'intermédiaire du bit 7 dans l'octet d'état/contrôle	Obligatoire pour l'hôte F (LP) et (XP), voir Tableau 37	Idem	Nécessaire pour la prise en charge des appareils F/modules F hérités
Blocs de fonctions de communication conformément à l'IEC 61131-3	L'ensemble minimal de blocs de fonctions de communication est: RDIAG, RALRM [44]	idem	La prise en charge de MS1 est une condition préalable. Facultatif pour les autres profils d'application: GETIO_PART, SETIO_PART
Serveur d'iParamètres	Les fabricants de systèmes doivent fournir les services de ''serveur d'iParamètres'' avec au moins 2^{15} octets	idem	Il est vivement recommandé aux fabricants de systèmes de fournir les blocs de fonctions de communication RDREC, WRREC, RDIAG (RALRM) [44]
Quantités (bit) de données d'entrée-sortie F	64 bits (Bool) maximum codés en Unsigned8, -16, -32	idem	-
Quantités (octets) de données d'entrée-sortie F	F_CRC_Seed = 0: 12 octets maximum F_CRC_Seed = 1: jusqu'à 13 octets minimum exigés pour la prise en charge, 13e octet en tant que qualificatif, 123 octets au maximum admis	idem	Tailles des structures de données minimales prises en charge comme représenté dans l'exemple dans la Figure 4, la Figure 18, la Figure 22 et la Figure 25
Types de données	Unsigned8, -16, -32, Integer16, -32	tous les types de données FSCP 3/1: voir Tableau 2	les règles FSCP 3/1 pour les pilotes de canal F doivent être respectées
Interface du pilote de l'hôte F	Tous les signaux	Tous les signaux	-
Diagnostic	Vivement recommandé: messages d'erreur de la couche de sécurité (6.3.2)	Vivement recommandé: messages d'erreur de la couche de sécurité (6.3.2)	Documentation recommandée: voir [45] et [68]
Service d'enregistrement lecture et écriture	obligatoire	obligatoire	Conformément à CP 3/1, CP 3/2 et CP/RTE

Élément	Automatisation des usines	Automatisme industriel	Remarque
MS2 (accès de l'esclave F)	Recommandé	facultatif	Conformément à CP 3/1, CP 3/2 Les petites CPU peuvent ne pas être en mesure de supporter une charge de trafic élevé
Accès de l'appareil F	Recommandé	facultatif	Conformément à CP3/RTE
Revendication du SIL	3 (dans les zones d'application spéciales, telles que la CNC: minimum 2)	3	-
Intégration d'outils, paramétrage	Interface d'outil satisfaisant aux exigences du Tableau 21	Selon [58] ou par l'intermédiaire de l'interface d'outil satisfaisant aux exigences du Tableau 21	-
F_WD_Time_2	Facultatif pour l'hôte F (XP)	Recommandé pour l'hôte F (XP)	Voir 8.1.4

Les fonctions de protocole étendues décrites dans le présent document exigent des considérations de conformité entre trois versions de protocole de l'hôte F (BP, LP, XP) et les appareils F/modules F conformément à l'IEC 61784-3-3 Édition 2 et la présente Édition 3.

Le Tableau 36 présente les principales caractéristiques des versions de protocole.

Tableau 36 – Principales caractéristiques des versions de protocole

Type de protocole	Caractéristique
Protocole de base (BP)	- IEC 61784-3-3 Ed. 2 - Restriction du manuel de sécurité: Intégrer une exigence dans le manuel de sécurité: Voir Tableau 30, "Relations de communication par fonction de sécurité"
Extension de bouclage (LP)	- IEC 61784-3-3 Ed. 2 - F_CRC_Seed = 0 - Bit de bouclage 7
Protocole étendu (XP)	- IEC 61784-3-3 Ed. 3 - F_CRC_Seed = 1

Le Tableau 37 spécifie les exigences concernant les deux versions d'appareil/module F.

Tableau 37 – Matrice de conformité de l'hôte/appareil F

Hôte F	Appareil/Module F	
	selon les éditions précédentes de la présente norme	**selon la présente norme**
selon les éditions précédentes de la présente norme	**Protocole de base (BP)** - Pas de changement pour l'appareil F et GSD (pas de F_CRC_Seed)	**Protocole de base (BP)** - F_CRC_Seed = 0
selon la présente norme	**Extension de bouclage (LP)** - Pas de changement pour l'appareil F et GSD	**Protocole étendu (XP)** Nouveau fichier GSD - Qualificatif pour les données d'entrée-sortie F, voir [66]

10 Évaluation

10.1 Politique de sécurité

Pour éviter tout malentendu, faux espoir et faute lourde des fabricants et fournisseurs d'appareils FSCP 3/1 concernant les développements et applications relatifs à la sécurité, ce qui suit doit être respecté et expliqué dans les formations, séminaires, ateliers et conseils.

- Tous les appareils ne sont pas automatiquement destinés aux applications relatives à la sécurité en utilisant simplement la communication de bus de terrain et une couche de communication de sécurité.
- Pour qu'un produit puisse être utilisé dans le cadre d'applications relatives à la sécurité, les processus de développement appropriés conformes aux normes de sécurité doivent être respectés (voir l'IEC 61508, l'IEC 61511, l'IEC 60204-1, l'IEC 62061 et l'ISO 13849-2) et/ou une évaluation doit être réalisée par un organisme compétent.
- Le fabricant d'un produit de sécurité est responsable de la mise en œuvre correcte de la technologie de couche de communication de sécurité, de l'exactitude et de l'exhaustivité de la documentation et des informations du produit.
- Les informations importantes supplémentaires relatives aux rectificatifs réels après des demandes de modification conclues doivent être prises en compte pour la mise en œuvre et l'évaluation.

10.2 Obligations

Il est de règle d'accepter les normes de sécurité internationales (ratifiées) de manière globale. Toutefois, compte tenu du rapport entre la technologie de sécurité dans le secteur de l'automatisation et la sécurité au travail et les garanties concomitantes d'un pays, la reconnaissance des règles énoncées ici reste un droit souverain. Les «Autorités» nationales décident de la reconnaissance des rapports d'évaluation.

NOTE Il peut s'agir, par exemple de l'IFA (Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung / BG – Institut de la sécurité et de la santé au travail de l'assurance sociale contre les accidents corporels) en Allemagne, de la HSE (Health and Safety Executive) au Royaume-Uni, de FM (Factory Mutual / Property Insurance and Risk Management Organization), de l'UL (Underwriters Laboratories Inc./ Product Safety Testing and Certification Organization) ou de l'INRS (Institut National de Recherche et de Sécurité) en France.

Pour FSCP 3/1, les règles d'évaluation de l'IEC 61784-3 s'appliquent.

Annexe A
(informative)

Informations supplémentaires pour les profils de communication de sécurité fonctionnelle de CPF3

A.1 Calcul de la fonction de hachage

La procédure de la Figure A.1 permet de détecter 99,999 994 % des erreurs totales qui se produisent après la modification des données. Elle permet également de détecter les erreurs séquentielles, le contrôle de signature tenant compte de la séquence des mots.

Pour la signature CRC 24 bits, la valeur *0x5D6DCB* fait office de polynôme générateur. Le nombre de bits de données peut être pair ou impair. La valeur générée après le dernier octet correspond à la signature CRC transférée.

```
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 – Procédure «C» classique de contrôle de redondance cyclique

La variante optimisée au démarrage du calcul de la signature CRC exige sensiblement plus d'espace mémoire. La fonction correspondante (A.1) en langage de programmation C pour les calculs de la signature CRC 24 bits à l'aide des tables de conversion est indiquée ci-dessous:

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

où

- r représente le résultat de la signature CRC 24 bits
- q représente le pointeur vers la valeur réelle de l'octet qui nécessite un calcul CRC. Après lecture de cette valeur, le pointeur doit être incrémenté pour l'octet suivant via q++.
- Les valeurs de départ de r peuvent être "0" (voir 8.1.8), "1" (voir 8.1.5.6, 8.1.7, 8.2) ou "CRC_FP" = F_Par_CRC (voir 8.1.5.6).

Pour ce calcul, le Tableau A.1 est utilisé.

Tableau A.1 – Tableau "Crctab24" de calculs de la signature CRC 24 bits

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

Ce tableau contient des valeurs 24 bits pour chaque valeur (0 à 255) de l'argument a de la fonction crctab24 [a]. Il convient d'utiliser ce tableau dans l'ordre croissant du haut à gauche (0) vers le bas à droite (255).

La fonction correspondante (A.2) en langage de programmation C pour les calculs de la signature CRC 32 bits à l'aide des tables de conversion est indiquée ci-dessous:

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

Pour ce calcul, le Tableau A.2 est utilisé.

Tableau A.2 – Tableau "Crctab32" de calculs de la signature CRC 32 bits

Table de conversion CRC (0 à 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

Ce tableau contient des valeurs 32 bits en représentation hexadécimale pour chaque valeur (0 à 255) de l'argument a de la fonction crctab32 [a]. Il convient d'utiliser ce tableau dans l'ordre croissant du haut à gauche (0) vers le bas à droite (255).

La fonction correspondante (A.3) en langage de programmation C pour le calcul de la signature (16 bits) F_Par_CRC (voir 8.1.8) à l'aide des tables de conversion est indiquée ci-dessous:

```
r = crctab16 [((r >> 8) ^ *q++) & 0xff] ^ (r << 8)        (A.3)
```

Pour ce calcul, le Tableau A.3 est utilisé.

Tableau A.3 – Tableau "Crctab16" de calculs de la signature CRC 16 bits

Table de conversion CRC (0 à 255)							
0000	4EAB	9D56	D3FD	7407	3AAC	E951	A7FA
E80E	A6A5	7558	3BF3	9C09	D2A2	015F	4FF4
9EB7	D01C	03E1	4D4A	EAB0	A41B	77E6	394D
76B9	3812	EBEF	A544	02BE	4C15	9FE8	D143
73C5	3D6E	EE93	A038	07C2	4969	9A94	D43F
9BCB	D560	069D	4836	EFCC	A167	729A	3C31
ED72	A3D9	7024	3E8F	9975	D7DE	0423	4A88
057C	4BD7	982À	D681	717B	3FD0	EC2D	A286
E78A	A921	7ADC	3477	938D	DD26	0EDB	4070
0F84	412F	92D2	DC79	7B83	3528	E6D5	A87E
793D	3796	E46B	AAC0	0D3A	4391	906C	DEC7
9133	DF98	0C65	42CE	E534	AB9F	7862	36C9
944F	DAE4	0919	47B2	E048	AEE3	7D1E	33B5
7C41	32EA	E117	AFBC	0846	46ED	9510	DBBB
0AF8	4453	97AE	D905	7EFF	3054	E3A9	AD02
E2F6	AC5D	7FA0	310B	96F1	D85A	0BA7	450C
81BF	CF14	1CE9	5242	F5B8	BB13	68EE	2645
69B1	271À	F4E7	BA4C	1DB6	531D	80E0	CE4B
1F08	51A3	825E	CCF5	6B0F	25A4	F659	B8F2
F706	B9AD	6A50	24FB	8301	CDAA	1E57	50FC
F27A	BCD1	6F2C	2187	867D	C8D6	1B2B	5580
1A74	54DF	8722	C989	6E73	20D8	F325	BD8E
6CCD	2266	F19B	BF30	18CA	5661	859C	CB37
84C3	CA68	1995	573E	F0C4	BE6F	6D92	2339
6635	289E	FB63	B5C8	1232	5C99	8F64	C1CF
8E3B	C090	136D	5DC6	FA3C	B497	676A	29C1
F882	B629	65D4	2B7F	8C85	C22E	11D3	5F78
108C	5E27	8DDA	C371	648B	2A20	F9DD	B776
15F0	5B5B	88A6	C60D	61F7	2F5C	FCA1	B20A
FDFE	B355	60A8	2E03	89F9	C752	14AF	5A04
8B47	C5EC	1611	58BA	FF40	B1EB	6216	2CBD
6349	2DE2	FE1F	B0B4	174E	59E5	8A18	C4B3

Ce tableau contient des valeurs 16 bits en représentation hexadécimale pour chaque valeur (0 à 255) de l'argument a de la fonction crctab16 [a]. Il convient d'utiliser ce tableau dans l'ordre croissant du haut à gauche (0) vers le bas à droite (255).

A.2 Exemples de valeurs pour les MonitoringNumbers (MNR)

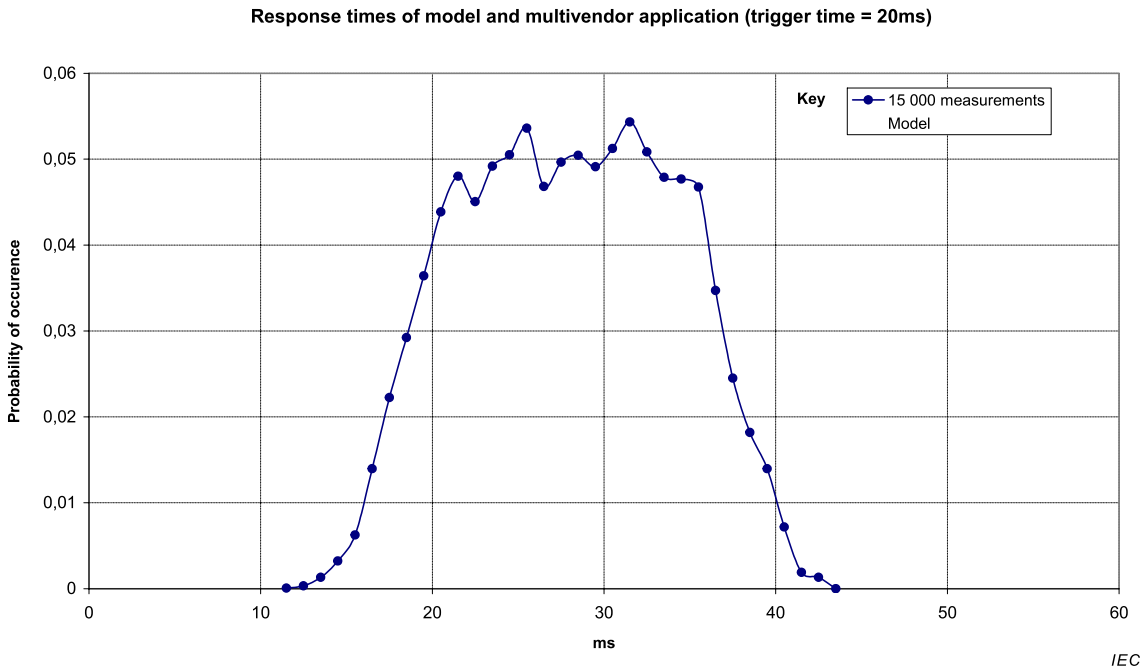
Le Tableau A.4 présente les quatre premières valeurs MNR pour deux exemples différents de nom de code (voir 7.1.5 et 7.1.6). La valeur de la variable Modifier est censée être de «0».

Tableau A.4 – Valeurs de CN_incrNR_64 et de MNR pour le PDU de l'hôte F

Nom de code 0x010001			Nom de code 0x010002		
Nr	CN_incrNR_64 [0]	MNR	Nr	CN_incrNR_64 [0]	MNR
0	-	CRC_FP+	0	-	CRC_FP+
1	0xCACFA720FA43BF62	0xCACFA720	1	0x444B59A4D64ABABB	0x444B59A4
2	0x174EE7E3C6063E8F	0x174EE7E3	2	0xE91C8E94EEA2B915	0xE91C8E94
3	0xE21E8F04C049FDF1	0xE21E8F04	3	0x2D67E839C4ED73D0	0x2D67E839
4	0xF96D76E886503C80	0xF96D76E8	4	0x168476CEB3902CE5	0x168476CE

A.3 Mesurages du temps de réponse

Un modèle simplifié de temps de réponse classiques est présenté en 9.3.1. La coïncidence entre ce modèle et une application multifournisseurs réelle pour 15 000 mesurages sur échantillon est indiquée dans la Figure A.2. Dans ce cas, la vitesse de transmission des données était de 1,5 Mbit/s et l'hôte F exécutait l'application (le programme) relative à la sécurité toutes les 20 ms restantes.

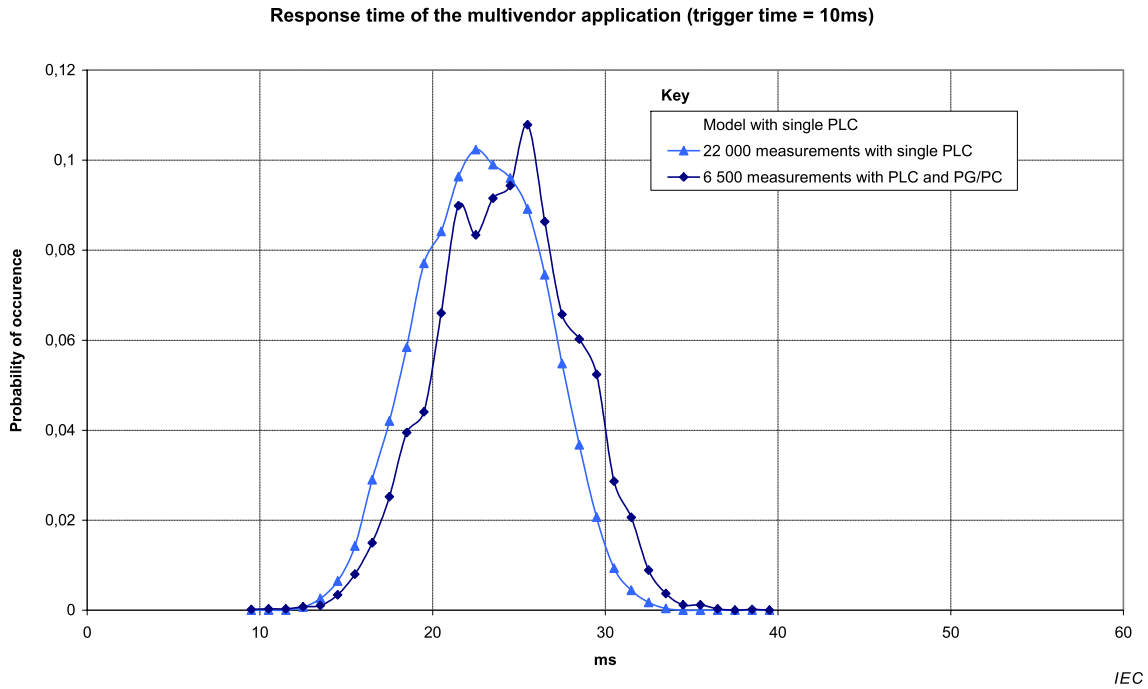


Anglais	Français
Response times of model and multivendor application (trigger time = 20 ms)	Temps de réponse du modèle et de l'application multifournisseurs (temps de déclencheur = 20 ms))
Probability of occurrence	Probabilité d'occurrence
Key	Légende
15 000 measurements	15 000 mesurages
Model	modèle

Figure A.2 – Comparaison du modèle de temps de réponse et d'une application réelle

D'autres ordinateurs (les programmeurs ou écrans de diagnostic utilisant l'accès acyclique au réseau (Figure 3), par exemple) ont peu, voire aucun, impact sur les temps de réponse si le réseau est configuré selon les recommandations du fabricant.

La Figure A.3 présente la distribution de fréquence des temps de réponse d'une application multifournisseurs CP 3/1 et FSCP 3/1 réelle à 1,5 Mbit/s et 2 situations de contrainte différentes.



Anglais	Français
Response times of the multivendor application (trigger time = 10 ms)	Temps de réponse de l'application multifournisseurs (temps de déclencheur = 10 ms)
Probability of occurrence	Probabilité d'occurrence
Key	Légende
22 000 measurements with single PLC	22 000 mesurages avec un seul PLC
6 500 measurements with PLC and PG/PC	6 500 mesurages avec PLC et PG/PC
Model with single PLC	Modèle à un seul PLC

Figure A.3 – Distribution de fréquence des temps de réponse mesurés

Les couleurs utilisées dans la Figure A.3 sont spécifiées ci-dessous:

cyan Modèle à un seul PLC (CPU)

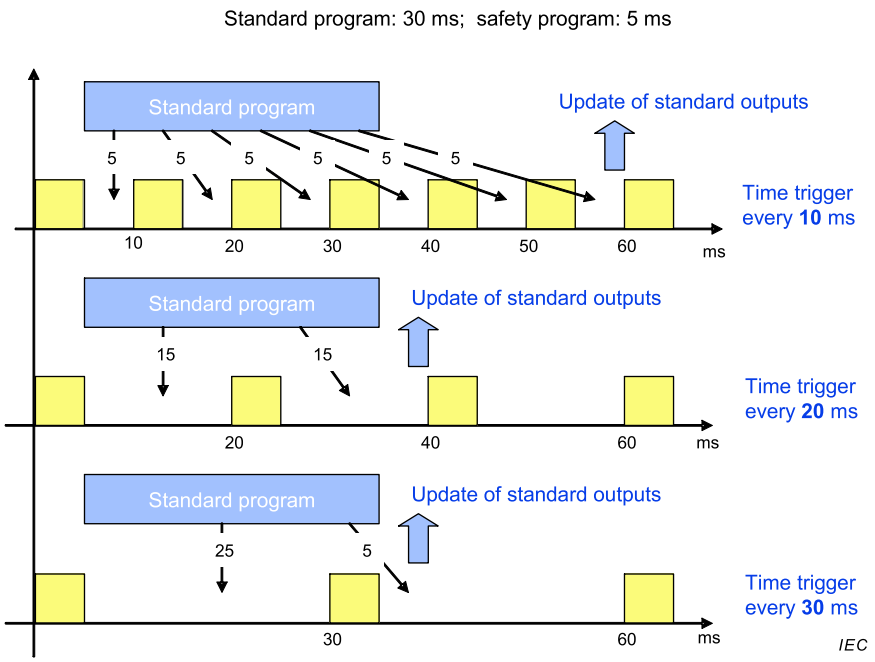
bleu 22 000 mesurages de temps de réponse avec une application multifournisseurs et un seul PLC (hôte F)

bleu foncé 6 500 mesurages de temps de réponse avec une application multifournisseurs utilisant un seul PLC (hôte F), plus un programmeur (classe maître 2) pour la fonction «état du programme cyclique» ("cyclic program status"), plus un écran de diagnostic supplémentaire (seconde classe maître 2) pour la fonction «état du rideau de lumière cyclique» ("cyclic light curtain status")

La courbe bleue représente 22 000 mesurages réalisés avec un PLC de sécurité autonome. La courbe bleue foncée représente 6 500 mesurages réalisés avec le même PLC de sécurité, un programmeur supplémentaire (PG) affichant régulièrement l'état du programme et un écran de diagnostic (PC) affichant régulièrement l'état des faisceaux d'un rideau de lumière. Le PG et le PC communiquaient tous deux par l'intermédiaire des services acycliques de CP 3/1 (classe maître 2).

Cela démontre que, comme prévu, deux appareils supplémentaires de surveillance ont peu, voire aucun, impact sur les temps de réponse. Les courbes s'apparentent à une distribution en cloche avec un temps de réaction compris entre 13 ms et 35 ms et un temps de réaction moyen de 24 ms. L'hôte F du modèle partage le même CPU pour les programmes standard et de sécurité. Ces deux programmes sont exécutés à différents niveaux du système d'exploitation afin de séparer de manière logique le programme d'application relatif à la sécurité et le programme standard.

La Figure A.4 présente des exemples de différentes segmentations du programme standard pour plusieurs valeurs de déclencheur. Elle démontre qu'une modification d'une partie du programme standard n'a aucun impact sur l'exécution du programme de sécurité. Toutefois, il peut être important de compenser la mise à jour des sorties standard et des sorties de sécurité s'il s'avère nécessaire d'utiliser des signaux provenant de l'autre partie pour répondre à des besoins de coordination.



Anglais	Français
Standard program	Programme standard
Safety program	Programme de sécurité
Update of standard outputs	Actualisation des sorties standard
Time trigger every 10/20 ms	Déclencheur temporel toutes les 10/20 ms

Figure A.4 – Hôte F avec programmes d'application standard et programmes d'application relatifs à la sécurité

Annexe B
(informative)

Informations pour l'évaluation des profils de communication de sécurité fonctionnelle de CPF 3

Selon les règles de l'IEC, la présente norme n'énonce pas les conditions de validation de la conformité. Toutefois, les essais et validation de conformité des appareils FSCP 3/1 à l'IEC 61784-3-3 peuvent être exigés par la loi.

L'information correspondante relative aux essais et à la conformité à la présente norme peut être obtenue auprès des comités nationaux locaux de l'IEC ou de l'organisation de bus de terrain compétente.

Note Pour l'IEC 61784-3-3, l'organisation de bus de terrain compétente est PROFIBUS Nutzerorganisation e.V. (PNO), see www.profibus.com.

Bibliographie

[1] IEC 60050 (toutes les parties), *Vocabulaire Électrotechnique International*

NOTE Voir également le dictionnaire multilingue de l'IEC – Électricité, électronique et télécommunications (disponible sur CD-ROM et à l'adresse <http://www.electropedia.org>).

[2] IEC 60870-5-1, *Matériels et systèmes de téléconduite – Cinquième partie: Protocoles de transmission – Section un: Formats de trames de transmission*

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

[4] IEC 61000-6-7, *Compatibilité électromagnétique (CEM) – Partie 6-7: Normes génériques – Exigences d'immunité pour les équipements visant à exercer des fonctions dans un système lié à la sécurité (sécurité fonctionnelle) dans des sites industriels*

[5] IEC 61131-6, *Automates programmables – Partie 6: Sécurité fonctionnelle*

[6] IEC 61158 (toutes parties), *Réseaux de communication industriels – Spécifications des bus de terrain*

[7] IEC 61496 (toutes les parties), *Sécurité des machines – Équipements de protection électro-sensibles*

[8] IEC 61508-1:2010, *Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité – Partie 1: Exigences générales*

[9] IEC 61508-4:2010, *Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité – Partie 4: Définitions et abréviations*

[10] IEC 61508-5:2010, *Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité – Partie 5: Exemples de méthodes de détermination des niveaux d'intégrité de sécurité*

[11] IEC 61508-6:2010, *Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité – Partie 6: Lignes directrices pour l'application de la CEI 61508-2 et de la CEI 61508-3*

[12] IEC 61784-4[7], *Industrial communication networks – Profiles – Part 4: Secure communications for fieldbuses* (disponible en anglais seulement)

[13] IEC 61784-5 (toutes les parties), *Réseaux de communication industriels – Profils – Partie 5: Installation des bus de terrain – Profils d'installation pour CPF x*

[14] IEC 61800-5-2, *Entraînements électriques de puissance à vitesse variable – Partie 5-2: Exigences de sécurité – Fonctionnelle*

[15] IEC 61804 (toutes les parties), *Blocs fonctionnels (FB) pour les procédés industriels*

[16] IEC TR 62059-11:2002, *Équipements de comptage de l'électricité – Sûreté de fonctionnement – Partie 11: Concepts généraux*

[17] IEC TR 62210:2003, *Power system control and associated communications – Data and communication security* (disponible en anglais seulement)

7 Proposition d'un nouveau sujet d'étude à l'étude.

[18] IEC 62443 (all parts), *Réseaux industriels de communication – Sécurité dans les réseaux et les systèmes*

[19] IEC TR 62685, *Réseaux de communication industriels – Profils – Lignes directrices pour l'évaluation des appareils de sécurité utilisant les profils de communication pour la sécurité fonctionnelle (FSCP) de la CEI 61784-3*

[20] Guide ISO/IEC 51:2014, *Aspects liés à la sécurité – Principes directeurs pour les inclure dans les normes*

[21] ISO/IEC 2382-14, *Technologies de l'information – Vocabulaire – Partie 14: Fiabilité, maintenabilité et disponibilité*

[22] ISO/IEC 2382-16:1996, *Technologies de l'information – Vocabulaire – Partie 16: Théorie de l'information*

[23] ISO/IEC 7498-1, *Information Technology – Open Systems Interconnection – Basic Reference Model: The Basic Model* (disponible en anglais seulement)

[24] ISO 10218-1, *Robots et dispositifs robotiques – Exigences de sécurité pour les robots industriels – Partie 1: Robots*

[25] ISO 12100, *Sécurité des machines – Principes généraux de conception – Appréciation du risque et réduction du risque*

[26] ISO 13849 (toutes les parties), *Sécurité des machines – Parties des systèmes de commande relatives à la sécurité*

[27] 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* (disponible en anglais seulement)

[28] 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* (disponible en anglais seulement)

[29] IEEE 802.11-2012, *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*

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

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

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

[33] VDI/VDE-Richtlinien 2180, *Part 1-4: 2006, Safeguarding of industrial process plants by means of process control engineering,* (en allemand)

[34] ANDREW S. TANENBAUM, DAVID J. WETHERALL, *Computer Networks*, 5th Edition, Prentice Hall, N.J., ISBN-10: 01321269580, ISBN-13: 978-0132126953

[35] W. WESLEY PETERSON, EDWARD J. WELDON, *Error-Correcting Codes*, 2nd Edition 1972, MIT-Press, ISBN 0-262-16-039-0

[36] BRUCE P. DOUGLASS, *Doing Hard Time: Developing Real-Time Systems with UML, Objects, Frameworks, and Patterns*, 2011, Addison-Wesley, ISBN-10: 0321774930, ISBN-13: 978-0321774934

[37] NFPA79 (2012), *Electrical Standard for Industrial Machinery*

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

[39] 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

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

[41] PROFIBUS Guideline: *PROFIsafe – Environmental Requirements,* V2.6, June 2015. Order-No. 2.232

[42] PROFIBUS Profile Guideline, *Part 1: Identification & Maintenance Functions*, V1.2, October 2013. Order-No. 3.502

[43] PROFIBUS Guideline: *GSDML Specification for PROFINET IO*, Version 2.31, November 2013. Order-No. 2.352

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

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

[46] PROFINET Guideline: *PROFINET Cabling and Interconnection Technology,* Version 3.0.1, October 2011. Order-No. 2.252

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

[48] PROFINET Guideline: *PROFINET Security*, V2.0, November 2013. Order-No. 7.002

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

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

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

[52] Object Management Group, *Unified Modeling Language: Superstructure*, Version 2.0; Formal/05-07-04; disponible à l'adresse < www.omg.com >

[53] NAMUR, *NE97 – Fieldbus for safety-related uses*, 2003; disponible à l'adresse < www.namur.de >

[54] REC-xml-20081126, *Extensible Markup Language (XML) 1.0 (Fifth Edition)* – W3C Recommendation 26 November 2008,
disponible à l'adresse < www.w3.org/TR/2008/REC-xml-20081126 >

[55] REC-xmlschema-1-20041028, *XML Schema Part 1: Structures (Second Edition)* – W3C Recommendation 28 October 2004,
disponible à l'adresse < www.w3.org/TR/2004/REC-xmlschema-1-20041028 >

[56] REC-xmlschema-2-20041028, *XML Schema Part 2: Datatypes (Second Edition)* – W3C Recommendation 28 October 2004,
disponible à l'adresse < www.w3.org/TR/2004/REC-xmlschema-2-20041028 >

[57] USB Implementers Forum, Inc , *Universal Serial Bus Revision 2.0 specification,* disponible à l'adresse < http://www.usb.org/developers/docs >

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

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

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

[61] PROFIBUS Guideline: *PROFIsafe Policy,* V1.5, July 2011. Order No. 2.282

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

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

[64] PI Specification: *PROFINET IO: Configure in Run for Distributed Control Systems,* V1.10, February 2015. Order-No. 7.112

[65] PROFIBUS Profile Guideline, *Part 4: iPar-Server*, V1.0.1, July 2011. Order-No. 3.532

[66] PI Specification: *Remote IO for Factory Automation,* V1.0, September 2012. Order-No. 3.242

[67] PI Specification: *PROFINET IO System Redundancy for Distributed Control Systems*, V1.10, February 2015. Order-No. 7.122

[68] PROFINET Guideline: *Diagnosis for PROFINET IO,* V1.0, November 2013. Order-No. 7.142

[69] PROFINET Guideline: *PROFINET IO Device Integration,* V1.0, December 2013. Order-No. 7.352

[70] PROFIBUS Guideline: *PROFIsafe – Test & Certification,* V2.2, Sep 2014. Order-No. 2.242

———————

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

3, rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

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