



BSI Standards Publication

Industrial communication networks — Profiles

Part 3-19: Functional safety fieldbuses — Additional specifications for CPF 19

National foreword

This British Standard is the UK implementation of EN IEC 61784-3-19:2024. It is identical to IEC 61784-3-19:2024.

The UK participation in its preparation was entrusted to Technical Committee GEL/65, Measurement and control.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

© The British Standards Institution 2024
Published by BSI Standards Limited 2024

ISBN 978 0 539 26876 8

ICS 25.040.40; 35.100.05

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 November 2024.

Amendments/corrigenda issued since publication

Date	Text affected
<hr/>	

English Version

Industrial communication networks - Profiles - Part 3-19:
Functional safety fieldbuses - Additional specifications for CPF
19
(IEC 61784-3-19:2024)

Réseaux de communication industriels - Profils - Partie 3-
19: Bus de terrain de sécurité fonctionnelle - Spécifications
supplémentaires pour CPF 19
(IEC 61784-3-19:2024)

Industrielle Kommunikationsnetze - Profile - Teil 3-19:
Funktional sichere Übertragung bei Feldbussen -
Zusätzliche Festlegungen für die
Kommunikationsprofilfamilie 19
(IEC 61784-3-19:2024)

This European Standard was approved by CENELEC on 2024-11-19. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and the United Kingdom.



European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

European foreword

The text of document 65C/1276/CDV, future edition 1 of IEC 61784-3-19, prepared by SC 65C "Industrial networks" of IEC/TC 65 "Industrial-process measurement, control and automation" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN IEC 61784-3-19:2024.

The following dates are fixed:

- latest date by which the document has to be implemented at national level by publication of an identical national standard or by endorsement (dop) 2025-11-30
- latest date by which the national standards conflicting with the document have to be withdrawn (dow) 2027-11-30

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

Any feedback and questions on this document should be directed to the users' national committee. A complete listing of these bodies can be found on the CENELEC website.

Endorsement notice

The text of the International Standard IEC 61784-3-19:2024 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following notes have to be added for the standard indicated:

IEC 61000-1-2	NOTE Approved as EN 61000-1-2
IEC 61000-6-7	NOTE Approved as EN 61000-6-7
IEC 61010-2-201	NOTE Approved as EN IEC 61010-2-201
IEC 61131-6	NOTE Approved as EN 61131-6
IEC 61158-1	NOTE Approved as EN IEC 61158-1
IEC 61158-5 (series)	NOTE Approved as EN 61158-5 (series)
IEC 61158-5-24	NOTE Approved as EN IEC 61158-5-24
IEC 61158-5-27	NOTE Approved as EN IEC 61158-5-27
IEC 61496 (series)	NOTE Approved as EN IEC 61496 (series)
IEC 61508-1	NOTE Approved as EN 61508-1
IEC 61508-4:2010	NOTE Approved as EN 61508-4:2010 (not modified)
IEC 61508-5	NOTE Approved as EN 61508-5
IEC 61784-1 (series)	NOTE Approved as EN IEC 61784-1 (series)
IEC 61784-2 (series)	NOTE Approved as EN IEC 61784-2 (series)

IEC 61784-3 (series) NOTE Approved as EN IEC 61784-3 (series)

IEC 61784-5 (series) NOTE Approved as EN IEC 61784-5 (series)

IEC 61800-5-2 NOTE Approved as EN 61800-5-2

IEC 61918 NOTE Approved as EN IEC 61918

IEC 62443 (series) NOTE Approved as EN IEC 62443 (series)

ISO 10218-1:2011 NOTE Approved as EN ISO 10218-1:2011 (not modified)

ISO 13849 (series) NOTE Approved as EN ISO 13849 (series)

ISO 13849-1:2023 NOTE Approved as EN ISO 13849-1:2023 (not modified)

Annex ZA (normative)

Normative references to international publications with their corresponding European publications

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

NOTE 1 Where an International Publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

NOTE 2 Up-to-date information on the latest versions of the European Standards listed in this annex is available here: www.cenelec.eu.

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
IEC 61131-2	-	Industrial-process measurement and control - Programmable controllers - Part 2: Equipment requirements and tests	EN 61131-2	-
IEC 61158	series	Industrial communication networks - Fieldbus specifications	EN IEC 61158	series
IEC 61158-6-24	-	Industrial communication networks - Fieldbus specifications - Part 6-24: Application layer protocol specification - Type 24 elements	EN IEC 61158-6-24	-
IEC 61158-6-27	-	Industrial communication networks - Fieldbus Specifications Part 6-27: Application layer protocol specification - Type 27 elements	EN IEC 61158-6-27	-
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	EN 61326-3-1	-
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	EN IEC 61326-3-2	-
IEC 61508	series	Functional safety of electrical/electronic/programmable electronic safety-related systems	EN 61508	series
IEC 61511	series	Functional safety - Safety instrumented systems for the process industry sector	EN 61511	series

IEC 61784-1-19	2023	Industrial networks - Profiles - Part 1-19: Fieldbus profiles - Communication Profile Family 19	EN IEC 61784-1-19 2023
IEC 61784-2-19	2023	Industrial networks - Profiles - Part 2-19: Additional real-time fieldbus profiles based on ISO/IEC/IEEE 8802-3 - CPF 19	EN IEC 61784-2-19 2023
IEC 61784-3	-	Industrial communication networks - Profiles - Part 3: Functional safety fieldbuses - General rules and profile definitions	EN IEC 61784-3 -
IEC 61784-5-19	-	Industrial networks - Profiles - Part 5-19: Installation of fieldbuses - Installation profiles for CPF 19	EN IEC 61784-5-19 -
IEC 62061	-	Safety of machinery - Functional safety of safety-related control systems	EN IEC 62061 -

CONTENTS

FOREWORD.....	6
INTRODUCTION.....	8
1 Scope.....	10
2 Normative references	10
3 Terms, definitions, symbols, abbreviated terms and conventions	11
3.1 Terms and definitions.....	11
3.1.1 Common terms and definitions.....	11
3.1.2 CPF 19: Additional terms and definitions	15
3.2 Symbols and abbreviated terms	15
3.2.1 Common symbols and abbreviated terms.....	15
3.2.2 CPF 19: Additional symbols and abbreviated terms	16
3.3 Conventions.....	16
4 Overview of FSCP 19 (MECHATROLINK Safety)	16
5 General	17
5.1 External documents providing specifications for the profile	17
5.2 Safety functional requirements	17
5.3 Safety measures	17
5.3.1 General	17
5.3.2 Sequence number.....	18
5.3.3 Time expectation	19
5.3.4 Connection ID.....	21
5.3.5 CRC calculation.....	21
5.3.6 Redundancy with cross checking	22
5.4 Safety communication layer structure.....	25
5.5 Relationships with FAL (and DLL, PhL).....	26
5.5.1 General	26
5.5.2 Data types	26
6 Safety communication layer services	26
6.1 Service description	26
6.1.1 S_CONNECT_START.....	26
6.1.2 S_CONNECT_CONF	28
6.1.3 S_PRM_SET	31
6.1.4 S_PRM_APPLY	33
6.1.5 S_SAFE_DATA.....	34
6.1.6 S_DISCONNECT	35
6.1.7 S_FAIL_SAFE	36
6.1.8 S_NOP	37
7 SCL protocol	38
7.1 SPDU format.....	38
7.1.1 SPDU structure.....	38
7.1.2 Connection ID.....	39
7.1.3 Sequence number.....	39
7.1.4 Command	39
7.1.5 State number	40
7.1.6 CRC	40
7.1.7 Redundant data	40

7.2	Safety FAL service protocol machine	40
7.2.1	State transition of safety master	40
7.2.2	State transition of safety slave	47
7.3	Behaviour description	53
7.3.1	Connection establishment	53
7.3.2	Safety data sending/receiving sequence	60
7.3.3	Disconnect safety channel	64
8	SCL management	65
8.1	Parameter definitions	65
8.1.1	General	65
8.1.2	T_Watchdog	65
8.1.3	T_Response	65
8.1.4	Master_Connection_Key	66
8.1.5	Slave_Connection_Key	66
8.1.6	Connection_Id	66
8.1.7	Master_Sequence_Number	66
8.1.8	Extended_Master_Sequence_Number	66
8.1.9	Slave_Sequence_Number	66
8.1.10	Extended_Slave_Sequence_Number	66
8.1.11	Node_Address	66
8.1.12	Device_Info (structure)	67
8.1.13	Output_Data_Length	67
8.1.14	Input_Data_Length	67
8.1.15	Output_User_Data_Length	67
8.1.16	Input_User_Data_Length	67
8.1.17	Stop_Safety_Loop	67
8.1.18	Stop_Safety_Loop_Oth	68
9	System requirements	69
9.1	Indicators and switches	69
9.1.1	General	69
9.1.2	Safety connection LED	70
9.2	Installation guidelines	70
9.3	Safety function response time	70
9.3.1	System response time	70
9.3.2	FSCP 19 response time	71
9.4	Duration of demands	72
9.5	Constraints for calculation of system characteristics	72
9.5.1	Number of stations	72
9.5.2	Probability considerations	72
9.6	Maintenance	73
9.7	Safety manual	73
10	Assessment	73
	Bibliography	74
	Figure 1 – Relationships of IEC 61784-3 with other standards (machinery)	8
	Figure 2 – Relationships of IEC 61784-3 with other standards (process)	9
	Figure 3 – Basic FSCP 19 system	17
	Figure 4 – Incrementing procedure of sequence number	

Figure 5 – Time expectation with watchdog timer	20
Figure 6 – Synchronization of transmission timing	20
Figure 7 – Time expectation with response timer	21
Figure 8 – Redundant data generation processing	23
Figure 9 – Redundant data verification process	25
Figure 10 – SCL structure	26
Figure 11 – Safety PDU format	38
Figure 12 – Safety master SCL – state transition diagram	40
Figure 13 – Safety master safety connection – state transition diagram	42
Figure 14 – Safety slave SCL – state transition diagram	48
Figure 15 – Safety slave safety connection – state transition diagram	49
Figure 16 – Node address and device information processing flow at start-up	56
Figure 17 – S_CONNECT_START command reception processing flow	56
Figure 18 – S_CONNECT_CONF command reception processing flow	57
Figure 19 – Sequence example 1 from connection establishment to safety data transmission/reception	58
Figure 20 – Sequence example 2 from connection establishment to safety data transmission/reception	59
Figure 21 – S_SAFE_DATA command sequence	60
Figure 22 – Loss of S_SAFE_DATA command from safety master	61
Figure 23 – Delay of S_SAFE_DATA command from safety master	61
Figure 24 – Loss of S_SAFE_DATA command from safety slave	62
Figure 25 – Delay of S_SAFE_DATA command from safety slave	62
Figure 26 – Insertion of message to safety slave	63
Figure 27 – Insertion of message to safety master	64
Figure 28 – Elements of safety function	71
Figure 29 – Safety function of FSCP 19 system	71
Figure 30 – Residual error rate	73
Table 1 – Communication errors and safety measures	18
Table 2 – Sequence number list	18
Table 3 – CRC seed values	22
Table 4 – S_CONNECT_START command data	27
Table 5 – S_CONNECT_START command SPDU (1st SPDU)	27
Table 6 – S_CONNECT_START command SPDU (2nd SPDU)	28
Table 7 – S_CONNECT_CONF command data	29
Table 8 – S_CONNECT_CONF command SPDU (1st SPDU)	29
Table 9 – S_CONNECT_CONF command SPDU (2nd SPDU)	30
Table 10 – S_CONNECT_CONF command SPDU (3rd SPDU)	30
Table 11 – S_PRM_SET command data	31
Table 12 – S_PRM_SET command SPDU (1st SPDU)	32
Table 13 – S_PRM_SET command SPDU (2nd SPDU)	32
Table 14 – S_PRM_SET command SPDU (3rd SPDU)	33
Table 15 – S_PRM_APPLY command data	33

Table 16 – S_PRM_APPLY command SPDU	34
Table 17 – S_SAFE_DATA command SPDU	34
Table 18 – S_DISCONNECT command SPDU	35
Table 19 – Factor in S_DISCONNECT command	36
Table 20 – S_FAIL_SAFE command SPDU	37
Table 21 – S_NOP command SPDU	37
Table 22 – List of commands	39
Table 23 – Safety master SCL – state description	40
Table 24 – Safety master SCL – state transition matrix	41
Table 25 – Safety master safety connection – state description	43
Table 26 – Safety master safety connection – state transition matrix	43
Table 27 – Safety slave SCL – state description	48
Table 28 – Safety slave SCL – state transition matrix	48
Table 29 – Safety slave safety connection – state description	49
Table 30 – Safety slave safety connection – state transition matrix	50
Table 31 – Safety slave node and device variables	55
Table 32 – List of parameter variables	65
Table 33 – Specification of stop safety loop setting	68
Table 34 – Specification of stop safety loop other setting	69
Table 35 – LED specifications	70
Table 36 – Safety connection LED specification	70
Table 37 – Residual error rate	72

INTERNATIONAL ELECTROTECHNICAL COMMISSION

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES –

Part 3-19: Functional safety fieldbuses – Additional specifications for CPF 19

FOREWORD

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

IEC 61784-3-19 has been prepared by subcommittee 65C: Industrial networks, of IEC technical committee 65: Industrial-process measurement, control and automation. It is an International Standard.

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

Draft	Report on voting
65C/1276/CDV	65C/1298/RVC

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

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

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

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

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

- reconfirmed,
- withdrawn, or
- revised.

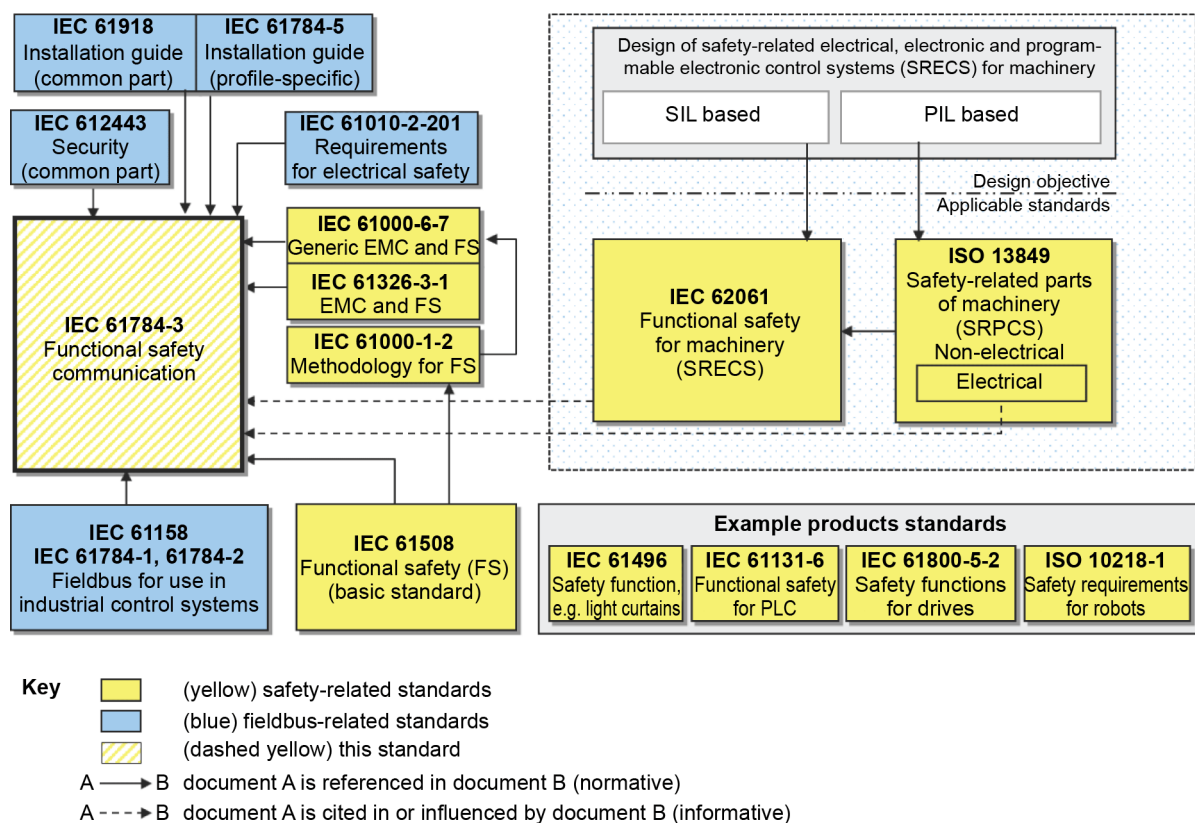
IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

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

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

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

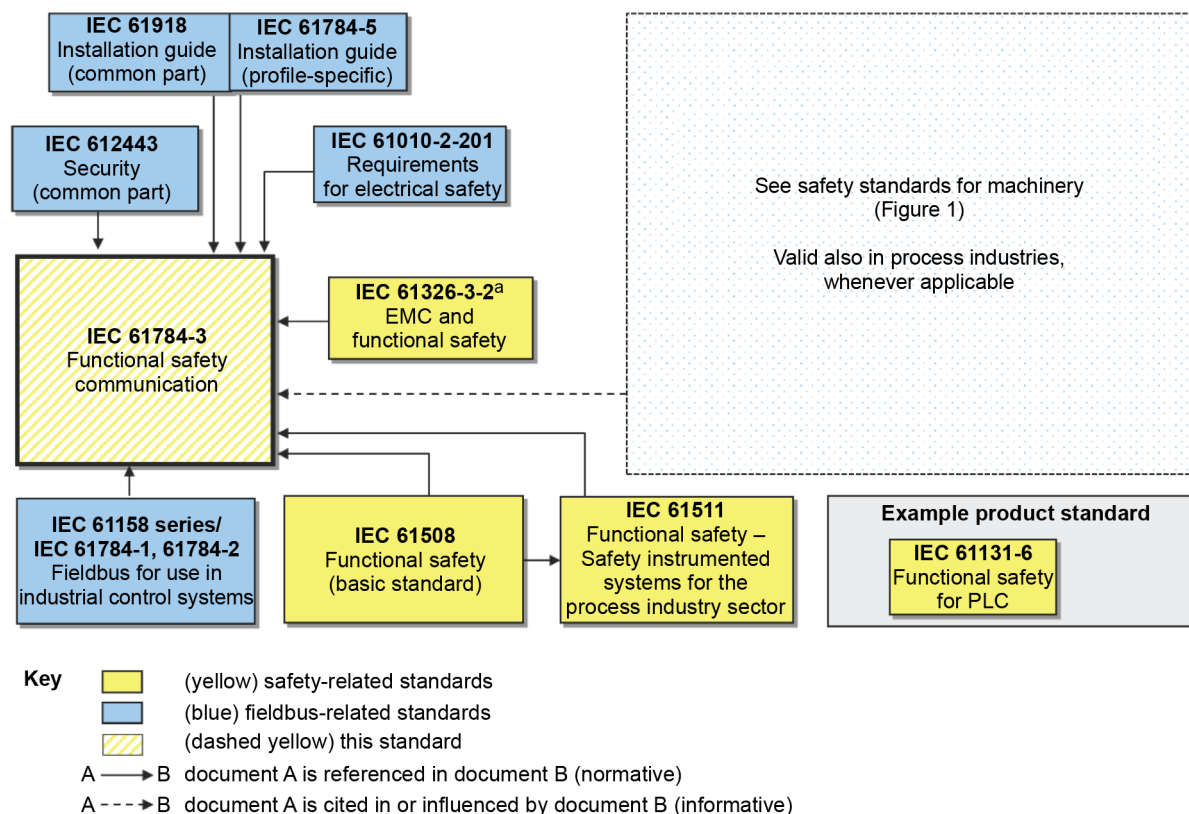


IEC

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

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

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



IEC

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

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

Safety communication layers which are implemented as parts of safety-related systems according to the 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 the IEC 61784-3 series 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.

The IEC 61784-3 series describes:

- basic principles for implementing the requirements of the 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 the IEC 61784-1 and IEC 61784-2 series, including safety layer extensions to the communication service and protocols sections of the IEC 61158 series.

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES –

Part 3-19: Functional safety fieldbuses – Additional specifications for CPF 19

1 Scope

This part of IEC 61784-3 specifies a safety communication layer (services and protocol) based on IEC 61784-1-19, IEC 61784-2-19 and the IEC 61158 series (Type 24 and Type 27). It identifies the principles for functional safety communications defined in IEC 61784-3 that are relevant for this safety communication layer. This safety communication layer is intended for implementation in safety devices only.

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

This document defines mechanisms for the transmission of safety-relevant messages among participants within a distributed network using fieldbus technology in accordance with the requirements of the IEC 61508 series¹ for functional safety. These mechanisms can be used in various industrial applications such as process control, manufacturing automation and machinery.

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

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

2 Normative references

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

IEC 61131-2, *Industrial-process measurement and control – Programmable controllers – Part 2: Equipment requirements and tests*

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

IEC 61158-6-24, *Industrial communication networks – Fieldbus specifications – Part 6-24: Application layer protocol specification – Type 24 elements*

IEC 61158-6-27, *Industrial communication networks – Fieldbus specifications – Part 6-27: Application layer protocol specification – Type 27 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*

¹ In the following pages of this document, "IEC 61508" will be used for "the IEC 61508 series"

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

IEC 61784-1-19:2023, *Industrial networks – Profiles – Part 1-19: Fieldbus profiles – Communication Profile Family 19*

IEC 61784-2-19:2023, *Industrial networks – Profiles – Part 2-19: Additional real-time fieldbus profiles based on ISO/IEC/IEEE 8802-3 – CPF 19*

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

IEC 61784-5-19, *Industrial networks – Profiles – Part 5: Installation of fieldbuses – Installation profiles for CPF 19*

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

3 Terms, definitions, symbols, abbreviated terms and conventions

3.1 Terms and definitions

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

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

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

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

3.1.1 Common terms and definitions

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

3.1.1.1

communication channel

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

3.1.1.2

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

3.1.1.3

connection

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

3.1.1.4

CRC

Cyclic Redundancy Check

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

3.1.1.5

CRC

Cyclic Redundancy Check

<method> procedure used to calculate the redundant data

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

3.1.1.6

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 can 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 to entry have been added.]

3.1.1.7

failure

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

Note 1 to entry: Failure can 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 have been replaced.]

3.1.1.8

fault

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

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

[SOURCE: IEC 61508-4:2010, 3.6.1, modified – Figure reference has been deleted.]

3.1.1.9

frame

denigrated synonym for DLPDU

3.1.1.10

master

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

3.1.1.11**message**

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

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

3.1.1.12**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 have been deleted.]

3.1.1.13**safety communication channel****SC**

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 modeled as two SCLs connected by a *black channel* or a *defined communication system*, or a *defined channel*.

3.1.1.14**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

3.1.1.15**safety connection**

connection that utilizes the safety protocol for communications transactions

3.1.1.16**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.

3.1.1.17**safety device**

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

3.1.1.18**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 have been deleted.]

3.1.1.19**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 61784-3:2021, 5.2.4 and addressed by the functional safety communication profiles defined in this document.

3.1.1.20**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 IEC 61508-1:2010, Tables 2 and 3.

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

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

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

3.1.1.21**safety measure**

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

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

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

3.1.1.22**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*.

3.1.1.23**safety-related application**

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

3.1.1.24**safety-related system**

system performing *safety functions* according to IEC 61508

3.1.1.25**slave**

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

3.1.2 CPF 19: Additional terms and definitions

3.1.2.1

safety master

active communication entity which transmits *safety output data* to a safety slave and receives safety input data from a safety slave

3.1.2.2

safety slave

active communication entity which receives safety output data from a safety master and transmits safety output data to a safety master

3.1.2.3

non-safety master

active communication entity which transmits non-safety output data to a non-safety slave and receives non-safety input data from a non-safety slave

3.1.2.4

non-safety slave

active communication entity which receives non-safety output data from a non-safety master and transmits non-safety output data to a non-safety master

3.1.2.5

node address

identifier of each communication entity

3.1.2.6

safety output data

SPDU transmitted from a safety master to a safety slave

3.1.2.7

safety input data

SPDU transmitted from a safety slave to a safety master

3.1.2.8

safety output user data

user defined data in safety output data

3.1.2.9

safety input user data

user defined data in safety input data

3.1.2.10

fail safe state

state to which safety masters and safety slaves transit in case of error

Note 1 to entry: In this state, safety output user data and safety input user data are all "0".

3.2 Symbols and abbreviated terms

3.2.1 Common symbols and abbreviated terms

CP	communication profile	[IEC 61784-1 (all parts)]
CPF	communication profile family	[IEC 61784-1 (all parts)]
CRC	cyclic redundancy check	
DLL	data link layer	[ISO/IEC 7498-1]
DLPDU	data link protocol data unit	
EUC	equipment under control	

E/E/PE	electrical/electronic/programmable electronic	[IEC 61508-4:2010]
FAL	fieldbus application layer	[IEC 61158-5 (all parts)]
FSCP	functional safety communication profile	
PDU	protocol data unit	[ISO/IEC 7498-1]
Pe	bit error probability	
PhL	physical layer	[ISO/IEC 7498-1]
PL	performance level	[ISO 13849-1]
SC	safety communication channel	
SCL	safety communication layer	
SIL	safety integrity level	[IEC 61508-4:2010]
SPDU	safety PDU	

3.2.2 CPF 19: Additional symbols and abbreviated terms

NVS	non-volatile storage
LSB	least significant bit

3.3 Conventions

Conventions used in this document are defined in IEC 61784-1-19, IEC 61784-2-19, and the IEC 61158 series Type 24 and 27.

4 Overview of FSCP 19 (MECHATROLINK Safety)

CPF 19 (commonly known as MECHATROLINK™²) is defined in IEC 61784-1-19 and IEC 61784-2-19 with fieldbus protocol layers defined in the IEC 61158 series Type 24 and 27. Functional safety communication profile FSCP 19 (MECHATROLINK Safety) is based on CPF 19 and the SCL defined in this part.

An overview of the system structure for FSCP 19 is shown in Figure 3. A non-safety master is shown in control domain 1, it is responsible for establishing and managing the non-safety communication channels in a master-slave relationship with the non-safety slaves using CPF 19.

Safety masters, as shown in control domains 2 and 3, are responsible for establishing and managing the safety communication channels in a master-slave relationship with the safety slaves using FSCP 19. Each safety master shall be limited to a single safety-related control domain.

FSCP 19 allows non-safety communication and safety communication to co-exist. A device can implement the non-safety communication function, the safety communication function, or both.

² MECHATROLINK™ is a trade name of Yaskawa Electric Corporation. This information is given for the convenience of users of this document and does not constitute an endorsement by IEC of the trade name holder or any of its products. Compliance to this document does not require use of the trade name MECHATROLINK™. Use of the trade name MECHATROLINK™ requires permission of Yaskawa Electric Corporation and compliance with conditions for their use (such as testing and validation).

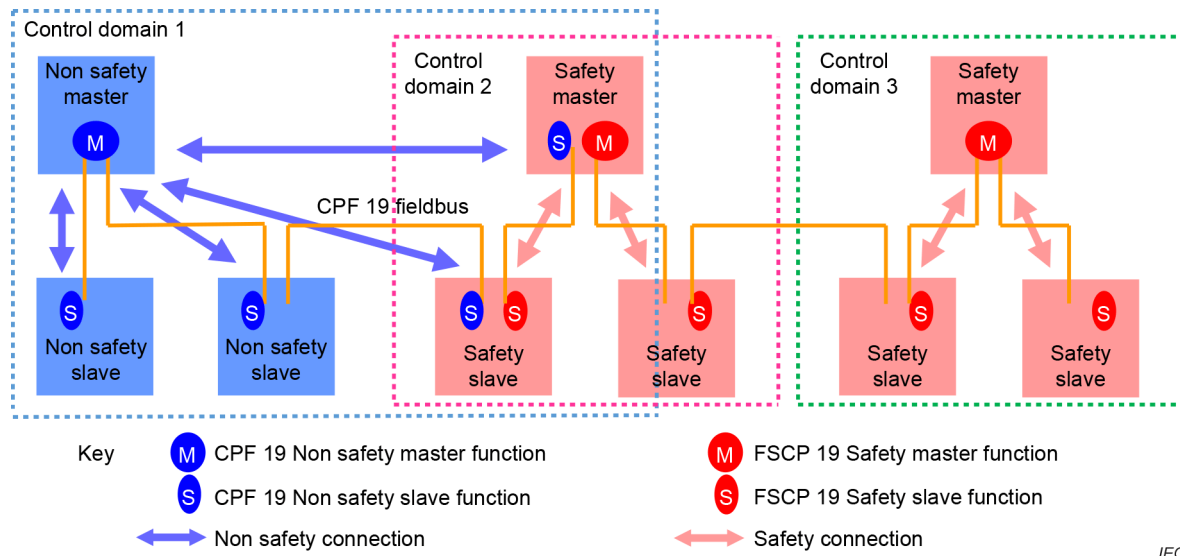


Figure 3 – Basic FSCP 19 system

5 General

5.1 External documents providing specifications for the profile

Additional documents providing more information are under preparation.

5.2 Safety functional requirements

This document specifies the services and protocols for a functional safety communication system based on fieldbus CPF 19. The communication technologies specified in this document shall only be implemented in devices designed in accordance with the requirements of IEC 61508.

The following requirements shall apply to the development of devices that implement FSCP 19 protocols. The same requirements were used in the development of FSCP 19.

- The FSCP 19 protocols are designed to support Safety Integrity Level SIL 3 (refer to IEC 61508).
- Implementations of FSCP 19 shall comply with IEC 61508.
- The basic requirements for the development of the FSCP 19 protocol are in IEC 61784-3.
- Environmental conditions shall comply with IEC 61131-2 for the basic levels and IEC 61326-3-1, IEC 61326-3-2 for the safety margin tests, unless there are specific product standards.
- Unless specified in this part, the CPF 19 requirements shall be unchanged for safety.

5.3 Safety measures

5.3.1 General

Safety measures used in the FSCP 19 are shown in Table 1.

Table 1 – Communication errors and safety measures

Communication errors	Safety measures				
	Sequence number (See 5.3.2)	Time expectation (See 5.3.3)	Connection ID (See 5.3.4)	CRC (See 5.3.5)	Redundancy with cross checking (See 5.3.6)
Corruption				X	X
Unintended repetition	X				
Incorrect sequence	X				
Loss	X	X			
Unacceptable delay		X			
Insertion	X		X		
Masquerade	X		X	X	X
Addressing			X		
Repetition by memory failures within non-safety network products	X				

5.3.2 Sequence number

To detect a network failure, a safety master and safety slaves shall have four types of sequence number for each connection instance, as shown in Table 2.

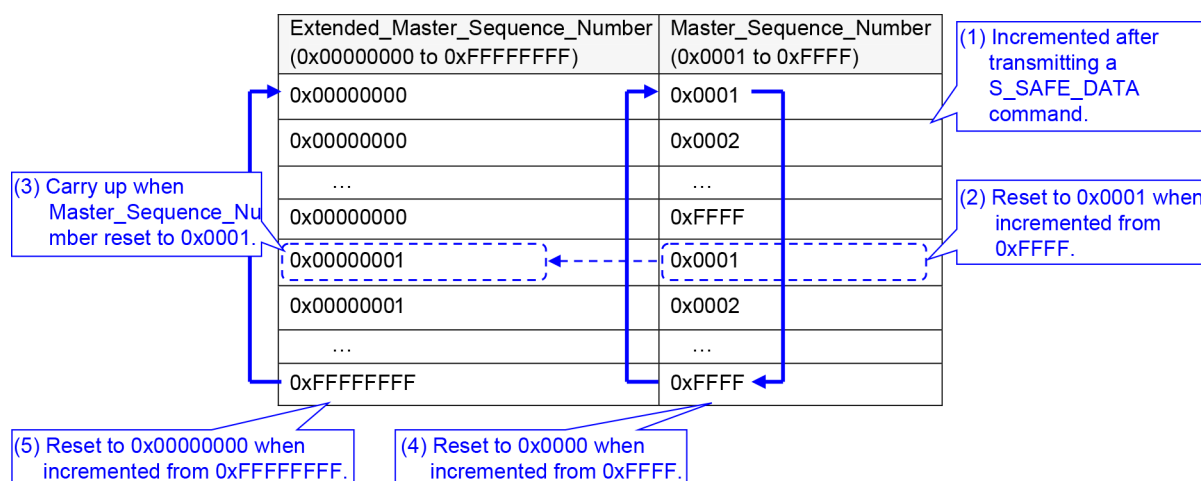
Table 2 – Sequence number list

Sequence number	Size	Description
Master sequence number	16 bits	Included in SPDU Transmitted from safety master to safety slave Checked by safety slave Initial value is 0x 0001
Extended master sequence number	32 bits	Not included in SPDU Checked by safety slave Initial value is 0x 0000 0000
Slave sequence number	16 bits	Included in SPDU Transmitted from safety slave to safety master Checked by safety master Initial value is 0x 0001
Extended slave sequence number	32 bits	Not included in SPDU Checked by safety master Initial value is 0x 0000 0000

The master sequence number shall be incremented by 1 after the safety master transmits an SPDU. The slave sequence number shall be incremented by 1 after the safety slave transmits an SPDU. Each sequence number shall be incremented from an initial value 1, and this 16-bit value shall rollover; the value after $2^{16}-1$ is 1. Value 0 shall not be used.

When the master sequence number rolls over from $2^{16}-1$ to 1, the extended master sequence number shall be incremented by 1. When the slave sequence number rolls over from $2^{16}-1$ to 1, the extended slave sequence number shall be incremented by 1. Each extended sequence number shall be incremented from initial value 0, and this 32-bit value shall rollover; the value after $2^{32}-1$ is 0.

The safety master and the safety slave shall initialize these variables before establishing a connection. The incrementing procedure of sequence number is shown in Figure 4.



NOTE: The same procedure is executed in Extended_Slave_Sequence_Number and Slave_Sequence_Number.

IEC

Figure 4 – Incrementing procedure of sequence number

Each sequence number shall be incremented and checked as described above in the transmitting and receiving process for all commands except:

- sequence number in S_NOP command shall always be zero;
- sequence number in S_FAIL_SAFE command shall hold its last value prior to the state transition of the SCL to the fail safe state.

5.3.3 Time expectation

Upon normal reception and then transmission a S_SAFE_DATA command, the SCL shall start a watchdog timer and reset it upon normal reception of a subsequent S_SAFE_DATA command as shown in Figure 5.