

This is a preview - click here to buy the full publication



IEC 61784-3-6

Edition 2.0 2010-06

INTERNATIONAL STANDARD



**Industrial communication networks – Profiles –
Part 3-6: Functional safety fieldbuses – Additional specifications for CPF 6**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

PRICE CODE **XC**

ICS 25.040.40; 35.100.05

ISBN 978-2-88910-979-1

CONTENTS

FOREWORD.....	7
0 Introduction	9
0.1 General.....	9
0.2 Patent declaration	11
1 Scope.....	12
2 Normative references	12
3 Terms, definitions, symbols, abbreviated terms and conventions	13
3.1 Terms and definitions	13
3.1.1 Common terms and definitions	13
3.1.2 CPF 6: Additional terms and definitions	18
3.2 Symbols and abbreviated terms.....	18
3.2.1 Common symbols and abbreviated terms	18
3.2.2 CPF 6: Additional symbols and abbreviated terms	19
3.3 Conventions	20
4 Overview of FSCP 6/7 (INTERBUS™ Safety)	20
4.1 General.....	20
4.2 Technical overview.....	20
4.3 Functional Safety Communication Profile 6/7.....	21
5 General	22
5.1 External documents providing specifications for the profile.....	22
5.2 Safety functional requirements	22
5.3 Safety measures	22
5.3.1 General	22
5.3.2 Sequence number	23
5.3.3 Time stamp	23
5.3.4 Time expectation	23
5.3.5 Acknowledgement	23
5.3.6 Connection authentication	23
5.3.7 Distinction between safety relevant messages and non-safety relevant messages – different data integrity assurance system.....	24
5.3.8 Parameterized shutdown time.....	24
5.4 Safety communication layer structure	24
5.4.1 Decomposition process.....	24
5.4.2 Definition of the safety function of the safety communication system	25
5.4.3 Decomposition of the safety function of a safety communication system into function blocks.....	26
5.4.4 Assignment of the function blocks to subsystems	27
5.4.5 Safety requirements and safety integrity requirements.....	30
5.4.6 Specification of the safe state.....	30
5.4.7 Response to a fault	31
5.4.8 Stop category	33
5.4.9 Safe Transmission.....	33
5.5 Relationships with FAL (and DLL, PhL)	33
5.5.1 Overview	33
5.5.2 Use of the AR-US service to initiate and parameterize.....	34
5.5.3 Use of the AR-US service to transmit safety data	35

5.5.4	Use of the AR-US service to abort	36
5.5.5	Data types	36
6	Safety communication layer services	36
6.1	General	36
6.2	Transmission principle for safety messages between SCLM and SCLS	36
6.3	Function block requirements	37
6.3.1	Input Safe Data function block	37
6.3.2	Output Safe Data function block	37
6.3.3	Safe Calculation function block	37
6.4	Context management	38
6.4.1	Initiate service	38
6.4.2	Abort service	39
6.5	Function block parameterization	40
6.5.1	Send application parameter service	40
6.5.2	Send application parameter ID service	41
6.5.3	Parameterize device service	42
6.6	Safe Process Data Mode	42
6.6.1	Transmit-Safety-Data	42
6.6.2	Set-Diagnostic-Data service	44
6.6.3	Set-Acknowledgement-Data service	44
7	Safety communication layer protocol	45
7.1	Safety PDU format	45
7.1.1	Structure of safety messages	45
7.1.2	Description of the polynomial used	46
7.1.3	Structure of safety messages for safe parameterization and idle	46
7.1.4	Structure of safety messages for the transmission of safety data	52
7.1.5	Messages for synchronization	53
7.1.6	Structure of safety messages for aborting connections	54
7.2	State description	54
7.2.1	SCLM and SCLS state machines	54
7.2.2	Initiate	56
7.2.3	Parameterization	57
7.2.4	Process data mode	61
7.2.5	Process data mode with diagnostic data transmission	66
7.2.6	Process data mode with Acknowledgement-Data transmission	66
7.2.7	Connection aborted	67
7.3	Abort	67
7.3.1	Connection abort in the event of an error detected by the SCLM	67
7.3.2	Abort of all connections in the event of an error detected by the SCLS	68
7.3.3	Abort of all connections in the event of an error detected by the SCLM	70
8	Safety communication layer management	71
8.1	General	71
8.2	Requirements of safety communication layer management	71
8.3	Set-Safety-Configuration service	71
8.4	Start IEC 61158 Type 8 service	73
9	System requirements	73
9.1	Indicators and switches	73

9.2	Installation guidelines	73
9.3	Safety function response time	73
9.3.1	General	73
9.3.2	Calculation of the parameterized shutdown time	74
9.4	Duration of demands	78
9.5	Constraints for calculation of system characteristics	78
9.5.1	System characteristics	78
9.5.2	Calculation of the number of telegrams per second	78
9.6	Maintenance	79
9.7	Safety manual	80
10	Assessment	80
Annex A (informative) Additional information for functional safety communication profiles of CPF 6		81
Annex B (informative) Information for assessment of the functional safety communication profiles of CPF 6		82
Bibliography		83
Table 1	– Overview of profile identifier usable for FSCP 6/7	22
Table 2	– Selection of the various measures for possible errors	23
Table 3	– List of function blocks and subsystems	27
Table 4	– Signal flow between the function blocks	29
Table 5	– Initiate service parameters	38
Table 6	– Parameterization mode and related services	39
Table 7	– Abort service parameters	39
Table 8	– Abort of a point-to-point connection by the SRP or SRC	40
Table 9	– Send application parameter service	40
Table 10	– Send application parameter ID service	41
Table 11	– Parameterize device parameters	42
Table 12	– Transmit-Safety-Data service parameters	43
Table 13	– Set-Diagnostic-Data service parameters	44
Table 14	– Set-Acknowledgement-Data service parameters	45
Table 15	– Parameter ID	48
Table 16	– Block 0: Device ID	48
Table 17	– Block 1: Parameter record ID	49
Table 18	– Block 2: Application parameter	50
Table 19	– TIME encoding	52
Table 20	– Abort_Info: Connection abort in the event of an error detected by the SCLM	68
Table 21	– Abort_Info: Abort of all connections in the event of an error detected by the SCLS	69
Table 22	– Abort_Info: Abort of all connections in the event of an error detected by the SCLM	71
Table 23	– Set-Safety-Configuration service	72
Table 24	– Error_Info	72
Table 25	– Calculation of tIB	77
Table 26	– Calculation of tSRC	78

Table 27 – Calculation of tPST	78
Figure 1 – Relationships of IEC 61784-3 with other standards (machinery)	9
Figure 2 – Relationships of IEC 61784-3 with other standards (process)	10
Figure 3 – FSCP 6/7 communication preconditions	21
Figure 4 – Example of a safety function	25
Figure 5 – Decomposition of safety function into function blocks	26
Figure 6 – Overview of the results of the decomposition process	28
Figure 7 – Signal flow between the function blocks	28
Figure 8 – Interfaces between the safety devices within the safety communication system	29
Figure 9 – Signal flow and safe states	31
Figure 10 – Mapping of the Safe Transmission function block	33
Figure 11 – Relationship between SCL and the other layers of IEC 61158 Type 8	34
Figure 12 – Use of the AR-US service to initiate and parameterize	35
Figure 13 – Use of the AR-US service to transmit safety data	35
Figure 14 – Use of the AR-US service to abort	36
Figure 15 – Use of the AR-US service to abort	36
Figure 16 – Structure of the safety PDU	45
Figure 17 – Integration of safety data and deterministic remedial measures in the summation frame	46
Figure 18 – Write_Parameter_Byte_Req message	47
Figure 19 – Read_Parameter_Byte_Req message	47
Figure 20 – Parameter_Byte_Con message	47
Figure 21 – Set_Safety_Connection_ID_Req message	50
Figure 22 – Set_Safety_Connection_ID_Con message of safety slaves	50
Figure 23 – Parameter_Idle_Req	51
Figure 24 – Parameter_Idle_Con	51
Figure 25 – Parameter_Check_Con	51
Figure 26 – Parameter_Loc_ID_Changed_Con	51
Figure 27 – Transmit Safety Data Message	52
Figure 28 – Sync_a message of the SCLM	53
Figure 29 – Req_b message of the SCLM	53
Figure 30 – Req_c message of the SCLM	53
Figure 31 – Req_d message of the SCLM	54
Figure 32 – Abort_Connection message	54
Figure 33 – Safety-Slave_Error message	54
Figure 34 – SCLM state machine	55
Figure 35 – SCLS state machine	55
Figure 36 – Initiate sequence	56
Figure 37 – Send Application Parameter sequence	58
Figure 38 – Send Application Parameter ID sequence	59
Figure 39 – Parameterize device sequence	60

Figure 40 – Simultaneous transmission of safety data to the safety slaves.....	61
Figure 41 – Use of the sequence number in the SCLM and SCLS	62
Figure 42 – Startup and error-free operation	63
Figure 43 – Resynchronization during operation	64
Figure 44 – Invalid CRC 24 checksum detected by the SCLS.....	65
Figure 45 – Process data mode with diagnostic data transmission	66
Figure 46 – Process data mode with Acknowledgement-Data transmission	67
Figure 47 – Error when initiating a connection	68
Figure 48 – Error at an SCLS when aborting all connections.....	69
Figure 49 – Abort of all connections in the event of an error detected by the SCLM	70
Figure 50 – Overview of the shutdown time.....	75

INTERNATIONAL ELECTROTECHNICAL COMMISSION

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES –

Part 3-6: Functional safety fieldbuses – Additional specifications for CPF 6

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 61784-3-6 has been prepared by subcommittee 65C: Industrial networks, of IEC technical committee 65: Industrial process measurement, control and automation.

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

- updates in relation with changes in IEC 61784-3.

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

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

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

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

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

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

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

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

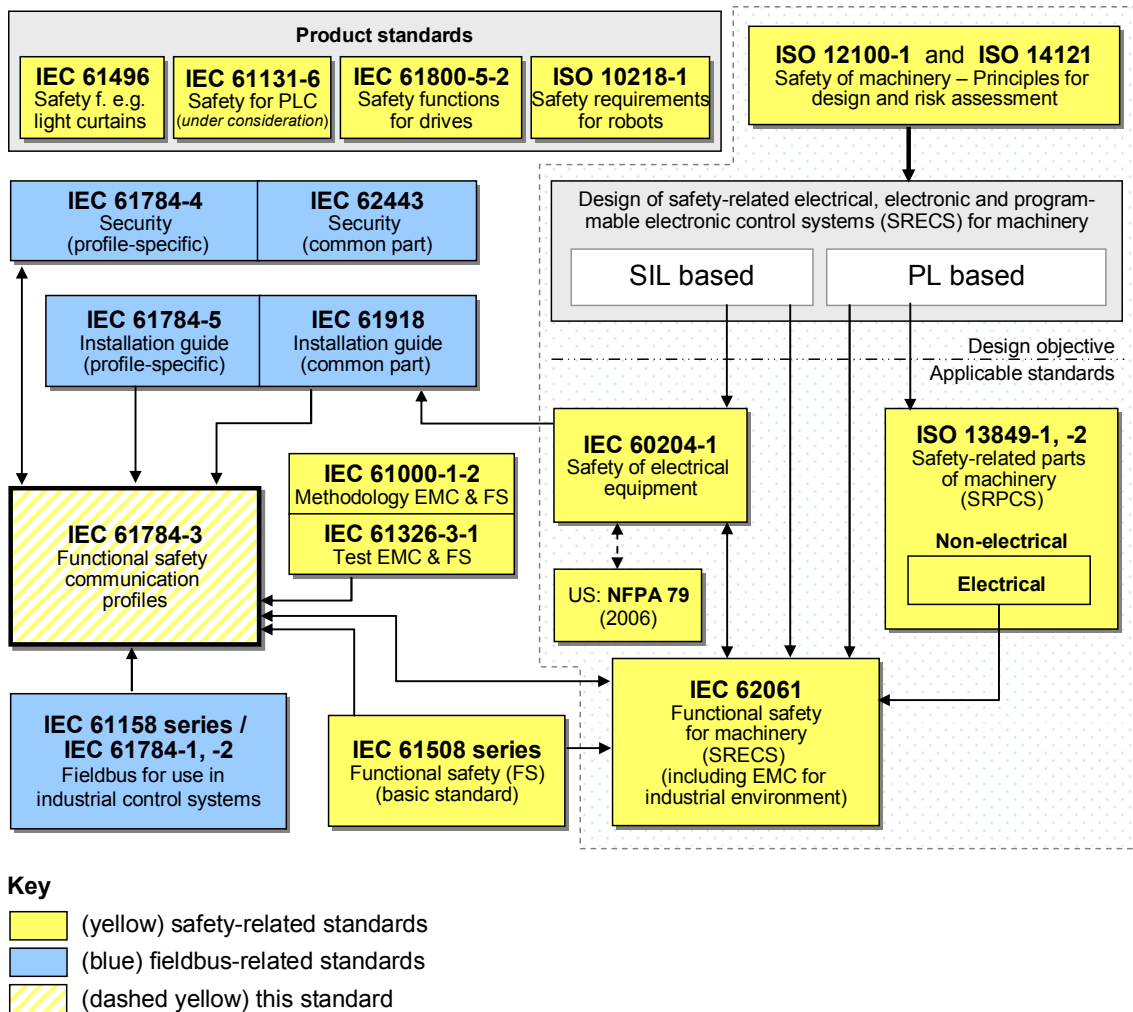
0 Introduction

0.1 General

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

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

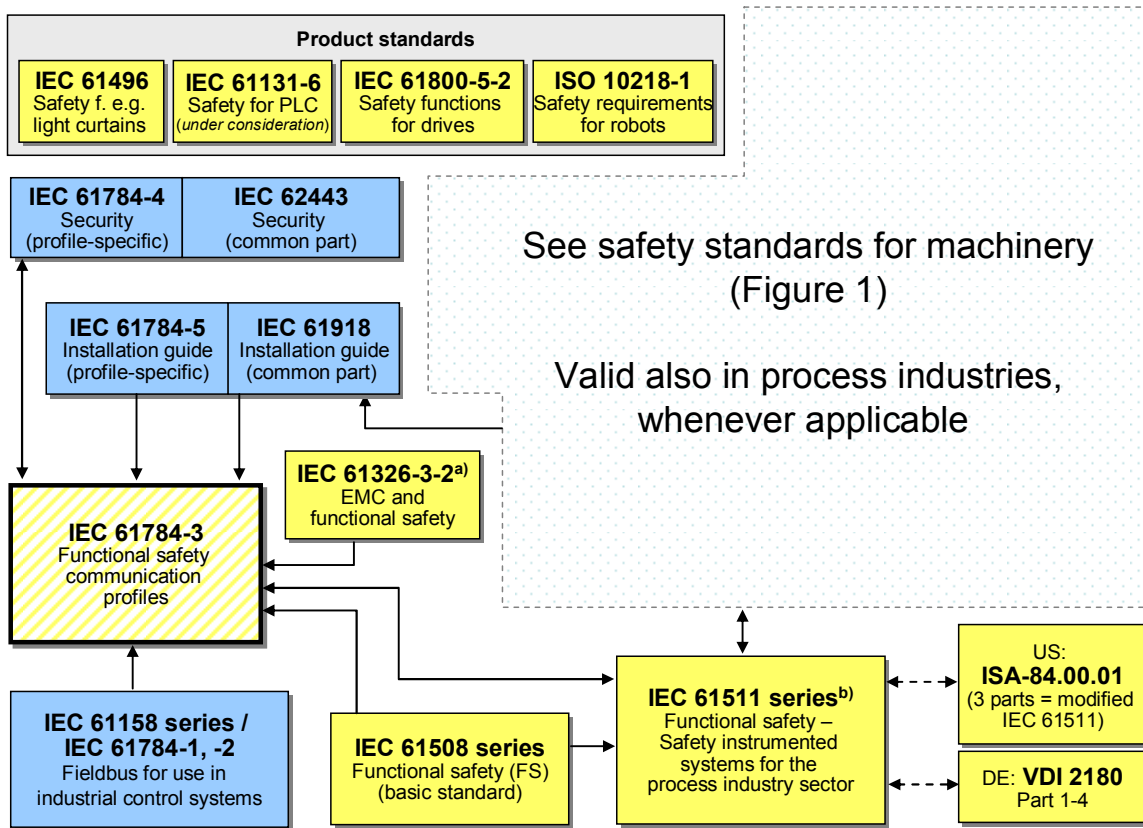
Figure 1 shows the relationships between this standard and relevant safety and fieldbus standards in a machinery environment.



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

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

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



Key

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

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

^b EN ratified.

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

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

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

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

This standard describes:

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

0.2 Patent declaration

The International Electrotechnical Commission (IEC) draws attention to the fact that it is claimed that compliance with this document may involve the use of patents concerning the functional safety communication profiles for family 6 as follows, where the [xx] notation indicates the holder of the patent right:

DE 103 25 263 A1	[PxC]	Sicherstellung von maximalen Reaktionszeiten in komplexen oder verteilten sicheren und/oder nicht sicheren Systemen
DE 103 18 068 A1	[PxC]	Verfahren und Vorrichtung zum Paket-orientierten Übertragen sicherheitsrelevanter Daten

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

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

Information may be obtained from:

[PxC] Phoenix Contact GmbH & Co. KG
Intellectual Property Licenses & Standards
Flachsmarktstr. 8
D-32825 Blomberg,
GERMANY

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

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES –

Part 3-6: Functional safety fieldbuses – Additional specifications for CPF 6

1 Scope

This part of the IEC 61784-3 series specifies a safety communication layer (services and protocol) based on CPF 6 of IEC 61784-1, IEC 61784-2 and IEC 61158 Type 8. It identifies the principles for functional safety communications defined in IEC 61784-3 that are relevant for this safety communication layer.

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

This part¹ defines mechanisms for the transmission of safety-relevant messages among participants within a distributed network using fieldbus technology in accordance with the requirements of IEC 61508 series² for functional safety. These mechanisms may be used in various industrial applications such as process control, manufacturing automation and machinery.

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

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

2 Normative references

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

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

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

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

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

IEC 61158-3-8, *Industrial communication networks – Fieldbus specifications – Part 3-8: Data-link layer service definition – Type 8 elements*

IEC 61158-4-8, *Industrial communication networks – Fieldbus specifications – Part 4-8: Data-link layer protocol specification – Type 8 elements*

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 61158-5-8:2007, *Industrial communication networks – Fieldbus specifications – Part 5-8: Application layer service definition – Type 8 elements*

IEC 61158-6-8, *Industrial communication networks – Fieldbus specifications – Part 6-8: Application layer protocol specification – Type 8 elements*

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

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

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

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

IEC 61784-3:2010³, *Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions*

IEC 61784-5-6, *Industrial communication networks – Profiles – Part 5: Installation of fieldbuses – Installation profiles for CPF 6*

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

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

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

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

³ In preparation.