

Industrial communication networks - Profiles - Part 3-8:
Functional safety fieldbuses - Additional specifications
for CPF 8

EESTI STANDARDI EESSÕNA

NATIONAL FOREWORD

See Eesti standard EVS-EN 61784-3-8:2017 sisaldab Euroopa standardi EN 61784-3-8:2017 ingliskeelset teksti.	This Estonian standard EVS-EN 61784-3-8:2017 consists of the English text of the European standard EN 61784-3-8:2017.
Standard on jõustunud sellekohase teate avaldamisega EVS Teatajas	This standard has been endorsed with a notification published in the official bulletin of the Estonian Centre for Standardisation.
Euroopa standardimisorganisatsioonid on teinud Euroopa standardi rahvuslikele liikmetele kättesaadavaks 01.12.2017.	Date of Availability of the European standard is 01.12.2017.
Standard on kättesaadav Eesti Standardikeskusest.	The standard is available from the Estonian Centre for Standardisation.

Tagasisidet standardi sisu kohta on võimalik edastada, kasutades EVS-i veebilehel asuvat tagasiside vormi või saates e-kirja meiliaadressile standardiosakond@evs.ee.

ICS 25.040.40, 35.100.05

Standardite reprodutseerimise ja levitamise õigus kuulub Eesti Standardikeskusele

Andmete paljundamine, taastekitamine, kopeerimine, salvestamine elektroonsesse süsteemi või edastamine ükskõik millises vormis või millisel teel ilma Eesti Standardikeskuse kirjaliku loata on keelatud.

Kui Teil on küsimusi standardite autorikaitse kohta, võtke palun ühendust Eesti Standardikeskusega:
Koduleht www.evs.ee; telefon 605 5050; e-post info@evs.ee

The right to reproduce and distribute standards belongs to the Estonian Centre for Standardisation

No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying, without a written permission from the Estonian Centre for Standardisation.

If you have any questions about copyright, please contact Estonian Centre for Standardisation:

Homepage www.evs.ee; phone +372 605 5050; e-mail info@evs.ee

English Version

**Industrial communication networks - Profiles - Part 3-8:
Functional safety fieldbuses - Additional specifications for CPF 8
(IEC 61784-3-8:2016)**

Réseaux de communication industriels - Profils - Partie 3-8:
Bus de terrain de sécurité fonctionnelle - Spécification
supplémentaire pour CPF 8
(IEC 61784-3-8:2016)

Industrielle Kommunikationsnetze - Profile - Teil 3-8:
Funktional sichere Übertragung bei Feldbussen -
Zusätzliche Festlegungen für die
Kommunikationsprofilfamilie 8
(IEC 61784-3-8:2016)

This European Standard was approved by CENELEC on 2016-09-01. 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, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.



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

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

European foreword

The text of document 65C/851/FDIS, future edition 2 of IEC 61784-3-8:2016, 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 61784-3-8:2017.

The following dates are fixed:

- latest date by which this document has (dop) 2018-06-01
to be implemented at national level by
publication of an identical national
standard or by endorsement
- latest date by which the national (dow) 2020-12-01
standards conflicting with this
document have to be withdrawn

This document supersedes EN 61784-3-8:2010.

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.

Endorsement notice

The text of the International Standard IEC 61784-3-8:2016 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 standards indicated:

IEC 61000-6-7	NOTE Harmonized as EN 61000-6-7
IEC 61131-6	NOTE Harmonized as EN 61131-6
IEC 61496 (all parts)	NOTE Harmonized as EN 61496 (all parts)
IEC 61508-1:2010	NOTE Harmonized as EN 61508-1:2010 (not modified).
IEC 61508-4:2010	NOTE Harmonized as EN 61508-4:2010 (not modified).
IEC 61508-5:2010	NOTE Harmonized as EN 61508-5:2010 (not modified).
IEC 61784-2	NOTE Harmonized as EN 61784-2
IEC 61784-5 (all parts)	NOTE Harmonized as EN 61784-5 (all parts)
IEC 61800-5-2	NOTE Harmonized as EN 61800-5-2
IEC 61918	NOTE Harmonized as EN 61918
IEC 62443 (all parts)	NOTE Harmonized as prEN 62443 (all parts)
IEC/TR 62685	NOTE Harmonized as CLC/TR 62685
ISO 10218-1	NOTE Harmonized as EN ISO 10218-1
ISO 12100	NOTE Harmonized as EN ISO 12100
ISO 13849-1	NOTE Harmonized as EN ISO 13849-1
ISO 13849-2	NOTE Harmonized as EN ISO 13849-2

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 When 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 60204-1	-	Safety of machinery - Electrical equipment - of machines - Part 1: General requirements		-
IEC 61131-2	2007	Programmable controllers -- Part 2: Equipment requirements and tests	EN 61131-2	2007
IEC 61158	series	Industrial communication networks - Fieldbus specifications - Part 1: Overview and guidance for the IEC 61158 and IEC 61784 series	EN 61158	series
IEC 61158-2	-	Industrial communication networks - Fieldbus specifications - Part 2: Physical layer specification and service definition	EN 61158-2	-
IEC 61158-3-18	-	Industrial communication networks - Fieldbus specifications - Part 3-18: Data-link layer service definition - Type 18 elements	EN 61158-3-18	-
IEC 61158-4-18	-	Industrial communication networks - Fieldbus specifications -- Part 4-18: Data-link layer protocol specification - Type 18 elements	EN 61158-4-18	-
IEC 61158-5-18	-	Industrial communication networks - Fieldbus specifications -- Part 5-18: Application layer service definition - Type 18 elements	EN 61158-5-18	-
IEC 61158-5-23	-	Industrial communication networks - Fieldbus specifications - Part 5-23: Application layer service definition - Type 23 elements	EN 61158-5-23	-
IEC 61158-6-18	-	Industrial communication networks - Fieldbus specifications - Part 6-18: Application layer protocol specification - Type 18 elements	EN 61158-6-18	-
IEC 61158-6-23	-	Industrial communication networks - Fieldbus specifications - Part 6-23: Application layer protocol specification - Type 23 elements	EN 61158-6-23	-
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	-	-
IEC 61508	series	Functional safety of electrical/electronic/programmable electronic safety-related systems -- Part 1: General requirements	EN 61508	series
IEC 61511	series	Functional safety - Safety instrumented systems for the process industry sector - Part 1: Framework, definitions, system, hardware and application programming requirements	EN 61511	series
IEC 61784-1	-	Industrial communication networks - Profiles - Part 1: Fieldbus profiles	EN 61784-1	-
IEC 61784-2	-	Industrial communication networks - Profiles - Part 2: Additional fieldbus profiles for real-time networks based on ISO/IEC 8802-3	EN 61784-2	-
IEC 61784-3	-	Industrial communication networks - Profiles - Part 3: Functional safety fieldbuses - General rules and profile definitions	EN 61784-3	-
IEC 62061	-	Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems	EN 62061	-
IEEE 802.3	-	IEEE Standard for Information technology -- Specific requirements - Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications	-	-

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	14
3.1.2 CPF 8: Additional terms and definitions	20
3.2 Symbols and abbreviated terms.....	21
3.2.1 Common symbols and abbreviated terms.....	21
3.2.2 CPF 8: Additional symbols and abbreviated terms.....	22
3.3 Conventions.....	22
4 Overview	22
5 General	22
6 Safety communication layer services.....	23
7 Safety communication layer protocol	23
8 Safety communication layer management.....	23
9 System requirements	23
10 Assessment.....	23
11 FSCP 8/1	23
11.1 Scope – FSCP 8/1.....	23
11.2 Normative references – FSCP 8/1.....	23
11.3 Terms, definitions, symbols, abbreviated terms and conventions – FSCP 8/1.....	23
11.4 Overview of FSCP 8/1 (CC-Link Safety™)	23
11.5 General – FSCP 8/1	24
11.5.1 External documents providing specifications for the profile.....	24
11.5.2 Safety functional requirements	24
11.5.3 Safety measures	24
11.5.4 Safety communication layer structure	26
11.5.5 Relationships with FAL (and DLL, PhL).....	26
11.6 Safety communication layer services for FSCP 8/1.....	27
11.6.1 General	27
11.6.2 SASEs.....	27
11.6.3 SARs	28
11.6.4 Process data SAR ASEs	28
11.7 Safety communication layer protocol for FSCP 8/1	29
11.7.1 Safety PDU format	29
11.7.2 State description	36
11.8 Safety communication layer management for FSCP 8/1	40
11.8.1 General	40
11.8.2 Connection establishment and confirmation processing.....	41
11.8.3 Safety slave verification	41
11.9 System requirements for FSCP 8/1	42

11.9.1	Indicators and switches	42
11.9.2	Installation guidelines.....	43
11.9.3	Safety function response time	43
11.9.4	Duration of demands	45
11.9.5	Constraints for calculation of system characteristics	45
11.9.6	Maintenance	46
11.9.7	Safety manual.....	47
11.10	Assessment for FSCP 8/1.....	47
12	FSCP 8/2	47
12.1	Scope – FSCP 8/2.....	47
12.2	Normative references – FSCP 8/2.....	47
12.3	Terms, definitions, symbols, abbreviated terms and conventions – FSCP 8/2.....	47
12.4	Overview of FSCP 8/2 (CC-Link IE™ Safety communication function)	47
12.5	General – FSCP 8/2	48
12.5.1	External documents providing specifications for the profile.....	48
12.5.2	Safety functional requirements	48
12.5.3	Safety measures	49
12.5.4	Safety communication layer structure	53
12.5.5	Relationships with FAL (and DLL, PhL).....	54
12.6	Safety communication layer services for FSCP 8/2.....	54
12.6.1	General	54
12.6.2	Connection reestablishment services.....	54
12.6.3	Data transmission services.....	55
12.6.4	Connection termination notification services	56
12.7	Safety communication layer protocol for FSCP 8/2	56
12.7.1	Safety PDU format	56
12.7.2	Safety FAL service protocol machine (SFSPM)	62
12.8	Safety communication layer management for FSCP 8/2	85
12.8.1	Parameter Definitions.....	85
12.8.2	Parameter Setup	89
12.8.3	Management Services.....	89
12.9	System requirements for FSCP 8/2.....	92
12.9.1	Indicators and switches	92
12.9.2	Installation guidelines.....	94
12.9.3	Safety function response time	94
12.9.4	Duration of demands	95
12.9.5	Constraints for calculation of system characteristics	95
12.9.6	Maintenance	97
12.9.7	Safety manual.....	97
12.10	Assessment for FSCP 8/2.....	98
Annex A (informative)	Additional information for functional safety communication profiles of CPF 8.....	99
A.1	Hash function calculation for FSCP 8/1	99
A.2	Hash function calculation for FSCP 8/2	99
A.3	Meaning of response time calculation formula for FSCP 8/2	99
Annex B (informative)	Information for assessment of the functional safety communication profiles of CPF 8	100
Bibliography		101

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 – Relationship between SCL and the other layers of IEC 61158 Type 18	26
Figure 4 – State diagram.....	37
Figure 5 – Detection of unintended repetition	50
Figure 6 – Detection of incorrect sequence.....	51
Figure 7 – Detection of loss	51
Figure 8 – Detection of unacceptable delay by time stamps	52
Figure 9 – Detection of unacceptable delay by timer	53
Figure 10 – Protocol Hierarchy	54
Figure 11 – Safety PDU Structure	57
Figure 12 – CTRL Configuration	57
Figure 13 – SASE-M and SASE-S TS	60
Figure 14 – S-Data during safety refresh	60
Figure 15 – S-Data not during safety refresh	61
Figure 16 – S-Data header configuration	61
Figure 17 – CRC calculation.....	62
Figure 18 – Communication models.....	62
Figure 19 – SFSPM state transition diagram.....	63
Figure 20 – Connection establishment sequence	65
Figure 21 – Communication sequence during safety refresh communication.....	65
Figure 22 – Offset measurement and generation sequence during safety refresh communication	66
Figure 23 – SFSPM-M state transition diagram.....	67
Figure 24 – Sequence other than during safety refresh	70
Figure 25 – S-Connect-req.....	71
Figure 26 – S-InitConfirmNetPrm-req	71
Figure 27 – net_prm_list	72
Figure 28 – S-InitVerifyStnPrm-req.....	72
Figure 29 – stn_prm_list	72
Figure 30 – S-InvokeFunc-req	73
Figure 31 – S-WriteErrorInfo-req	73
Figure 32 – date_and_time_of_occurence	74
Figure 33 – SFSPM-S state transition diagram	75
Figure 34 – Sequence other than during safety refresh	80
Figure 35 – S-Connect-rsp	80
Figure 36 – S-InitConfirmNetPrm-rsp.....	81
Figure 37 – S-InitVerifyStnPrm-rsp.....	81
Figure 38 – S-InvokeFunc-rsp	82
Figure 39 – Offset calculation procedure of safety clock	83
Figure 40 – Relationship between transmission interval fluctuation and transmission_interval	86
Figure 41 – Calculation of allowable_refresh_interval	88
Figure 42 – Calculation of allowable_delay.....	89

Figure 43 – Calculation of response time between safety PLCs.....	94
Figure 44 – Relationship between safety connections and residual error rate	97
Figure A.1 – allowable_delay and offset calculation deviation	99
Table 1 – Selection of the various measures for possible errors	25
Table 2 – M1 safety device manager attribute format	30
Table 3 – S1 safety device manager attribute format	30
Table 4 – M1 safety connection manager attribute format	30
Table 5 – S1 safety connection manager attribute format.....	30
Table 6 – M1 safety cyclic transmission attribute format	31
Table 7 – S1 safety cyclic transmission attribute format.....	31
Table 8 – M1 safety device manager attribute encoding.....	32
Table 9 – S1 safety device manager attribute encoding	32
Table 10 – M1 safety connection manager attribute encoding	32
Table 11 – S1 safety connection manager attribute encoding	33
Table 12 – M1 safety cyclic transmission attribute encoding.....	33
Table 13 – S1 safety cyclic transmission attribute encoding	35
Table 14 – Safety master monitor timer operation	39
Table 15 – Safety slave monitor timer operation	39
Table 16 – Safety data monitor timer operation.....	39
Table 17 – Details of connection establishment and confirmation processing.....	41
Table 18 – Details of slave information verification processing	41
Table 19 – Details of safety slave parameter transmission processing.....	42
Table 20 – Monitor LEDs.....	43
Table 21 – Safety function response time calculation.....	44
Table 22 – Safety function response time definition of terms.....	44
Table 23 – Number of occupied slots and safety data	45
Table 24 – Residual error rate Λ (occupied slots = 1).....	46
Table 25 – Residual error rate Λ (occupied slots = 2).....	46
Table 26 – Selection of the various measures for possible errors	49
Table 27 – SS-Start	54
Table 28 – SS-Restart	55
Table 29 – SS-InvokeFunc	55
Table 30 – SS-Read	55
Table 31 – SS-Write.....	56
Table 32 – SS-Terminate	56
Table 33 – Safety PDU elements.....	57
Table 34 – CTRL Elements	58
Table 35 – State list.....	63
Table 36 – SFSPM-M timers	67
Table 37 – SFSPM-M state transition table	67
Table 38 – support_functions	71
Table 39 – error_category	74

Table 40 – error_category for AL errors	74
Table 41 – error_code	74
Table 42 – SFSPM-S timers	76
Table 43 – SFSPM-S state transition table	76
Table 44 – Parameters used by safety communication layer	85
Table 45 – SM-SetSafetyStationInfo	89
Table 46 – Safety station information setting parameters of SM-SetSafetyStationInfo	90
Table 47 – SM-SetSafetyNetworkParameter	90
Table 48 – Safety network parameters of SM-SetSafetyNetworkParameter	90
Table 49 – SM-GetSafetyStationInfo	91
Table 50 – Safety station information parameters of SM-GetSafetyStationInfo (Request)	91
Table 51 – Safety station information parameters of SM-GetSafetyStationInfo (Response)	91
Table 52 – SM-GetSafetyNetworkParameter	92
Table 53 – Parameters of SM-GetSafetyNetworkParameter request	92
Table 54 – Parameters of SM-GetSafetyNetworkParameter response	92
Table 55 – Monitor LEDs	93
Table 56 – Communication port monitor LEDs	93

preview generated by EVS

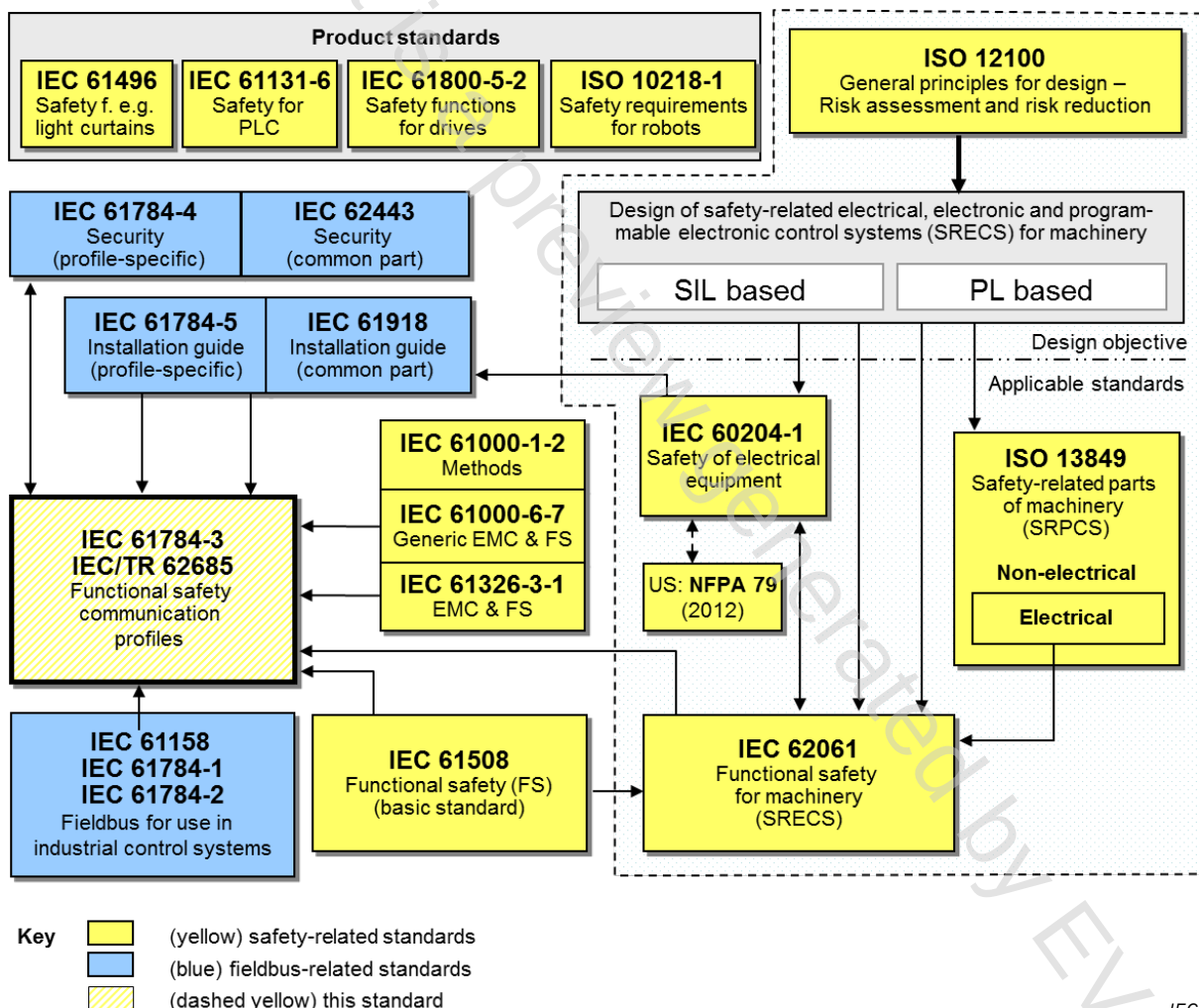
0 Introduction

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.

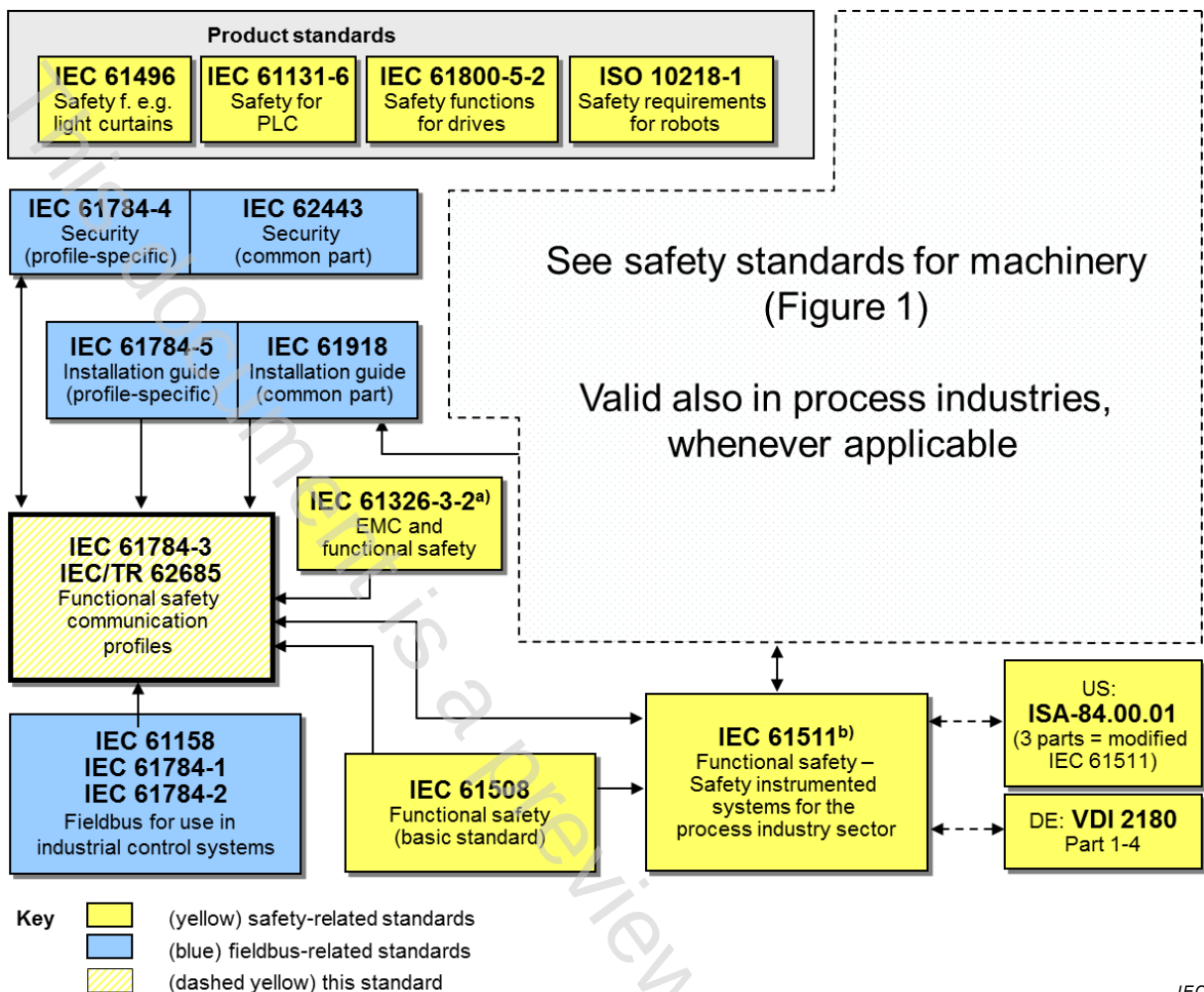
Figure 1 shows the relationships between this standard and relevant safety and fieldbus standards in a machinery environment.



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 a patent concerning FSCP 8/2 given in Clause 12 as follows:

JP 2012-533784 US 13/821733 DE 112010005881.4 KR 10-2013-7006469 CN 201080069108.6	[MEC]	Communication apparatus and delay detecting method
--	-------	--

IEC takes no position concerning the evidence, validity and scope of this patent right.

The holder of this patent right has assured the IEC that he/she is 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 statement of the holder of this patent right is registered with IEC. Information may be obtained from:

[MEC]	Mitsubishi Electric Corporation Corporate Licensing Division 2-7-3 Marunouchi, Chiyoda-ku Tokyo 100-8310 Japan
-------	---

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.