SVENSK STANDARD SS-EN 61784-3

Fastställd	Utgåva	Sida	Ansvarig kommitté
2009-02-23	1	1 (1+48)	SEK TK 65

Industriell processtyrning – Profiler – Del 3: Fältbussar i system av betydelse för säkerheten – Allmänna regler och profildefinitioner

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

Som svensk standard gäller europastandarden EN 61784-3:2008. Den svenska standarden innehåller den officiella engelska språkversionen av EN 61784-3:2008.

Nationellt förord

Europastandarden EN 61784-3:2008

består av:

– **europastandardens ikraftsättningsdokument,** utarbetat inom CENELEC

– **IEC 61784-3, First edition, 2007 - Industrial communication networks - Profiles - Part 3: Functional safety fieldbuses - General rules and profile definitions**

utarbetad inom International Electrotechnical Commission, IEC.

ICS 35.100.05; 25.040.40

Denna standard är fastställd av SEK Svensk Elstandard,
som också kan lämna upplysningar om **sakinnehållet** i standarden.
Postadress: SEK, Box 1284, 164 29 KISTA
Telefon: 08 - 444 14 00. *Telefax*: 08 - 444 14 30
E-post: sek@elstandard.se. *Internet*: www.elstandard.se

Standarder underlättar utvecklingen och höjer elsäkerheten

Det finns många fördelar med att ha gemensamma tekniska regler för bl a säkerhet, prestanda, dokumentation, utförande och skötsel av elprodukter, elanläggningar och metoder. Genom att utforma sådana standarder blir säkerhetskraven tydliga och utvecklingskostnaderna rimliga samtidigt som marknadens acceptans för produkten eller tjänsten ökar.

Många standarder inom elområdet beskriver tekniska lösningar och metoder som åstadkommer den elsäkerhet som föreskrivs av svenska myndigheter och av EU.

SEK är Sveriges röst i standardiseringsarbetet inom elområdet

SEK Svensk Elstandard svarar för standardiseringen inom elområdet i Sverige och samordnar svensk medverkan i internationell och europeisk standardisering. SEK är en ideell organisation med frivilligt deltagande från svenska myndigheter, företag och organisationer som vill medverka till och påverka utformningen av tekniska regler inom elektrotekniken.

SEK samordnar svenska intressenters medverkan i SEKs tekniska kommittéer och stödjer svenska experters medverkan i internationella och europeiska projekt.

Stora delar av arbetet sker internationellt

Utformningen av standarder sker i allt väsentligt i internationellt och europeiskt samarbete. SEK är svensk nationalkommitté av International Electrotechnical Commission (IEC) och Comité Européen de Normalisation Electrotechnique (CENELEC).

Standardiseringsarbetet inom SEK är organiserat i referensgrupper bestående av ett antal tekniska kommittéer som speglar hur arbetet inom IEC och CENELEC är organiserat.

Arbetet i de tekniska kommittéerna är öppet för alla svenska organisationer, företag, institutioner, myndigheter och statliga verk. Den årliga avgiften för deltagandet och intäkter från försäljning finansierar SEKs standardiseringsverksamhet och medlemsavgift till IEC och CENELEC.

Var med och påverka!

Den som deltar i SEKs tekniska kommittéarbete har möjlighet att påverka framtida standarder och får tidig tillgång till information och dokumentation om utvecklingen inom sitt teknikområde. Arbetet och kontakterna med kollegor, kunder och konkurrenter kan gynnsamt påverka enskilda företags affärsutveckling och bidrar till deltagarnas egen kompetensutveckling.

Du som vill dra nytta av dessa möjligheter är välkommen att kontakta SEKs kansli för mer information.

SEK Svensk Elstandard
Box 1284
164 29 Kista
Tel 08-444 14 00
www.elstandard.se

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 61784-3

June 2008

ICS 35.100.05; 25.040.40

English version

Industrial communication networks - Profiles - Part 3: Functional safety fieldbuses - General rules and profile definitions

(IEC 61784-3:2007)

Réseaux de communication industriels - Profils - Partie 3: Bus de terrain de sécurité fonctionnelle - Règles générales et définitions des profils (CEI 61784-3:2007)

Industrielle Kommunikationsnetze - Profile - Teil 3: Funktional sichere Übertragung bei Feldbussen - Allgemeine Regeln und Profilfestlegungen (IEC 61784-3:2007)

CENELEC

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

Central Secretariat: rue de Stassart 35, B - 1050 Brussels

Ref. No. EN 61784-3:2008 E

SEK Svensk Elstandard

Foreword

The text of document 65C/470/FDIS, future edition 1 of IEC 61784-3, 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 was approved by CENELEC as EN 61784-3 on 2008-05-01.

The following dates were fixed:

– latest date by which the EN has to be implemented at national level by publication of an identical national standard or by endorsement	(dop)	2009-02-01
– latest date by which the national standards conflicting with the EN have to be withdrawn	(dow)	2011-05-01

The International Electrotechnical Commission (IEC) and CENELEC draw attention to the fact that it is claimed that compliance with this document may involve the use of patents concerning functional safety communication profiles for families 1, 2, 3 and 6 given in EN 61784-3-1, EN 61784-3-2, EN 61784-3-3 and EN 61784-3-6.

The IEC and CENELEC take no position concerning the evidence, validity and scope of these patents right.

The holders of these patent 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 statements of the holders of these patent rights are registered with the IEC.

NOTE Patent details and corresponding contact information are provided in EN 61784-3-1, EN 61784-3-2, EN 61784-3-3 and EN 61784-3-6.

Annex ZA has been added by CENELEC.

Endorsement notice

The text of the International Standard IEC 61784-3:2007 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 60204-1	NOTE	Harmonized as EN 60204-1:2006 (not modified).
IEC 61496	NOTE	Harmonized as EN 61496-1:2004 (modified) and as CLC/TS 61496-2:2006 (not modified) and CLC/TC 61496-3:2008 (not modified)
IEC 61508-4	NOTE	Harmonized as EN 61508-4:2001 (not modified).
IEC 61508-6	NOTE	Harmonized as EN 61508-6:2001 (not modified).
IEC 61511	NOTE	Harmonized in EN 61511 series (not modified).
IEC 61800-5-2	NOTE	Harmonized as EN 61800-5-2:2007 (not modified).
IEC 62061	NOTE	Harmonized as EN 62061:2005 (not modified).
ISO 12100-1	NOTE	Harmonized as EN ISO 12100-1:2003 (not modified).
ISO 13849-1	NOTE	Harmonized as EN ISO 13849-1:2006 (not modified).
ISO 13849-2	NOTE	Harmonized as EN ISO 13849-2:2003 (not modified).

Annex ZA
(normative)

Normative references to international publications with their corresponding European publications

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.

NOTE When an international publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

Publication	Year	Title	EN/HD	Year
IEC 61131-2	-[1)]	Programmable controllers - Part 2: Equipment requirements and tests	EN 61131-2	2007[2)]
IEC 61158	Series	Industrial communication networks - Fieldbus specifications	EN 61158	Series
IEC 61326-3-1	-[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	2008[2)]
IEC 61326-3-2	-[1)]	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 61326-3-2	2008[2)]
IEC 61508	Series	Functional safety of electrical/electronic/programmable electronic safety-related systems	EN 61508	Series
IEC 61508-1	-[1)]	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1: General requirements	EN 61508-1	2001[2)]
IEC 61508-2	-[1)]	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems	EN 61508-2	2001[2)]
IEC 61784-1	-[1)]	Industrial communication networks - Profiles - Part 1: Fieldbus profiles	EN 61784-1	2008[2)]
IEC 61784-2	-[1)]	Industrial communication networks - Profiles - Part 2: Additional fieldbus profiles for real-time networks based on ISO/IEC 8802-3	EN 61784-2	2008[2)]

[1)] Undated reference.

[2)] Valid edition at date of issue.

Publication	Year	Title	EN/HD	Year
IEC 61784-3-1	-[1)]	Industrial communication networks - Profiles - Part 3-1: Functional safety fieldbuses – Additional specifications for CPF 1	EN 61784-3-1	2008[2)]
IEC 61784-3-2	-[1)]	Industrial communication networks - Profiles - Part 3-2: Functional safety fieldbuses - Additional specifications for CPF 2	EN 61784-3-2	2008[2)]
IEC 61784-3-3	-[1)]	Industrial communication networks - Profiles - Part 3-3: Functional safety fieldbuses - Additional specifications for CPF 3	EN 61784-3-3	2008[2)]
IEC 61784-3-6	-[1)]	Industrial communication networks - Profiles - Part 3-6: Functional safety fieldbuses - Additional specifications for CPF 6	EN 61784-3-6	2008[2)]
IEC 61784-5	Series	Industrial communication networks - Profiles - Part 5: Installation of fieldbuses - Installation profiles for CPF X	EN 61784-5	Series
IEC 61918 (mod)	-[1)]	Industrial communication networks - Installation of communication networks in industrial premises	EN 61918	2008[2)]
IEC 62280-1	2002	Railway applications - Communication, signalling and processing systems - Part 1: Safety-related communication in closed transmission systems	-	-

CONTENTS

INTRODUCTION 7
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 1: Additional terms and definitions 16
3.1.3 CPF 2: Additional terms and definitions 16
3.1.4 CPF 3: Additional terms and definitions 16
3.1.5 CPF 6: Additional terms and definitions 16
3.2 Symbols and abbreviated terms 17
3.2.1 Common symbols and abbreviated terms 17
3.2.2 CPF 1: Additional symbols and abbreviated terms 17
3.2.3 CPF 2: Additional symbols and abbreviated terms 17
3.2.4 CPF 3: Additional symbols and abbreviated terms 17
3.2.5 CPF 6: Additional symbols and abbreviated terms 17
4 Conformance 18
5 Basics of safety-related fieldbus systems 18
5.1 Safety function decomposition 18
5.2 Communication system 19
5.2.1 General 19
5.2.2 IEC 61158 fieldbuses 19
5.2.3 Communication channel types 20
5.2.4 Safety function response time 20
5.3 Communication errors 21
5.3.1 General 21
5.3.2 Corruption 21
5.3.3 Unintended repetition 21
5.3.4 Incorrect sequence 21
5.3.5 Loss 22
5.3.6 Unacceptable delay 22
5.3.7 Insertion 22
5.3.8 Masquerade 22
5.3.9 Addressing 22
5.4 Deterministic remedial measures 22
5.4.1 General 22
5.4.2 Sequence number 23
5.4.3 Time stamp 23
5.4.4 Time expectation 23
5.4.5 Connection authentication 23
5.4.6 Feedback message 23
5.4.7 Data integrity assurance 23
5.4.8 Redundancy with cross checking 23
5.4.9 Different data integrity assurance systems 24
5.5 Relationships between errors and safety measures 24

5.6 Data integrity considerations 25
5.6.1 Calculation of the residual error rate 25
5.6.2 Residual error rate and SIL 27
5.7 Relationship between functional safety and security 27
5.8 Boundary conditions and constraints 27
5.8.1 Electrical safety 27
5.8.2 Electromagnetic compatibility (EMC) 27
5.9 Installation guidelines 28
5.10 Safety manual 28
5.11 Safety policy 28
6 Communication Profile Family 1 (FOUNDATION™ Fieldbus) – Profiles for functional safety 29
6.1 Functional Safety Communication Profile 1/1 29
6.2 Technical overview 29
7 Communication Profile Family 2 (CIP™) – Profiles for functional safety 30
7.1 Functional Safety Communication Profile 2/1 30
7.2 Technical overview 30
8 Communication Profile Family 3 (PROFIBUS™, PROFINET™) – Profiles for functional safety 31
8.1 Functional Safety Communication Profile 3/1 31
8.2 Technical overview 31
9 Communication Profile Family 6 (INTERBUS®) – Profiles for functional safety 34
9.1 Functional Safety Communication Profile 6/7 34
9.2 Technical overview 34
Annex A (informative) Example functional safety communication models 36
A.1 General 36
A.2 Model A 36
A.3 Model B 36
A.4 Model C 37
A.5 Model D 37
Annex B (informative) A safety communication channel model using CRC-based error checking 39
B.1 Overview 39
B.2 Channel model for calculations 39
B.3 Cyclic redundancy checking 40
B.3.1 General 40
B.3.2 Considerations concerning CRC polynomials 42
Annex C (informative) Structure of technology-specific parts 44
Bibliography 46

Table 1 – Overview of the effectiveness of the various measures on the possible errors 25
Table 2 – Definition of items used for calculation of the residual error rate 26
Table 3 – Relationship of residual error rate to SIL level 27
Table 4 – Overview of profile identifier usable for FSCP 6/7 34
Table B.1 – Example dependency d_{min} and block length n 42
Table C.1 – Common subclause structure for technology-specific parts 44

Figure 1 – Relationships of IEC 61784-3 with other standards (machinery) 7
Figure 2 – Relationships of IEC 61784-3 with other standards (process) 8
Figure 3 – Safety communication as a part of a safety function 19
Figure 4 – Example model of a functional safety communication system 20
Figure 5 – Example of safety function response time components 21
Figure 6 – Example application 26
Figure 7 – Scope of FSCP 1/1 29
Figure 8 – Relationship of Safety Validators 30
Figure 9 – Basic communication preconditions for FSCP 3/1 32
Figure 10 – Structure of a FSCP 3/1 safety PDU 33
Figure 11 – Safe communication modes 33
Figure 12 – FSCP 6/7 communication preconditions 35
Figure A.1 – Model A 36
Figure A.2 – Model B 37
Figure A.3 – Model C 37
Figure A.4 – Model D 38
Figure B.1 – Communication channel with perturbation 39
Figure B.2 – Binary symmetric channel (BSC) 40
Figure B.3 – Example of a block with message and CRC bits (redundancy code) 41
Figure B.4 – Block codes for error detection 41
Figure B.5 – Proper and improper CRC polynomials 42

INTRODUCTION

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.

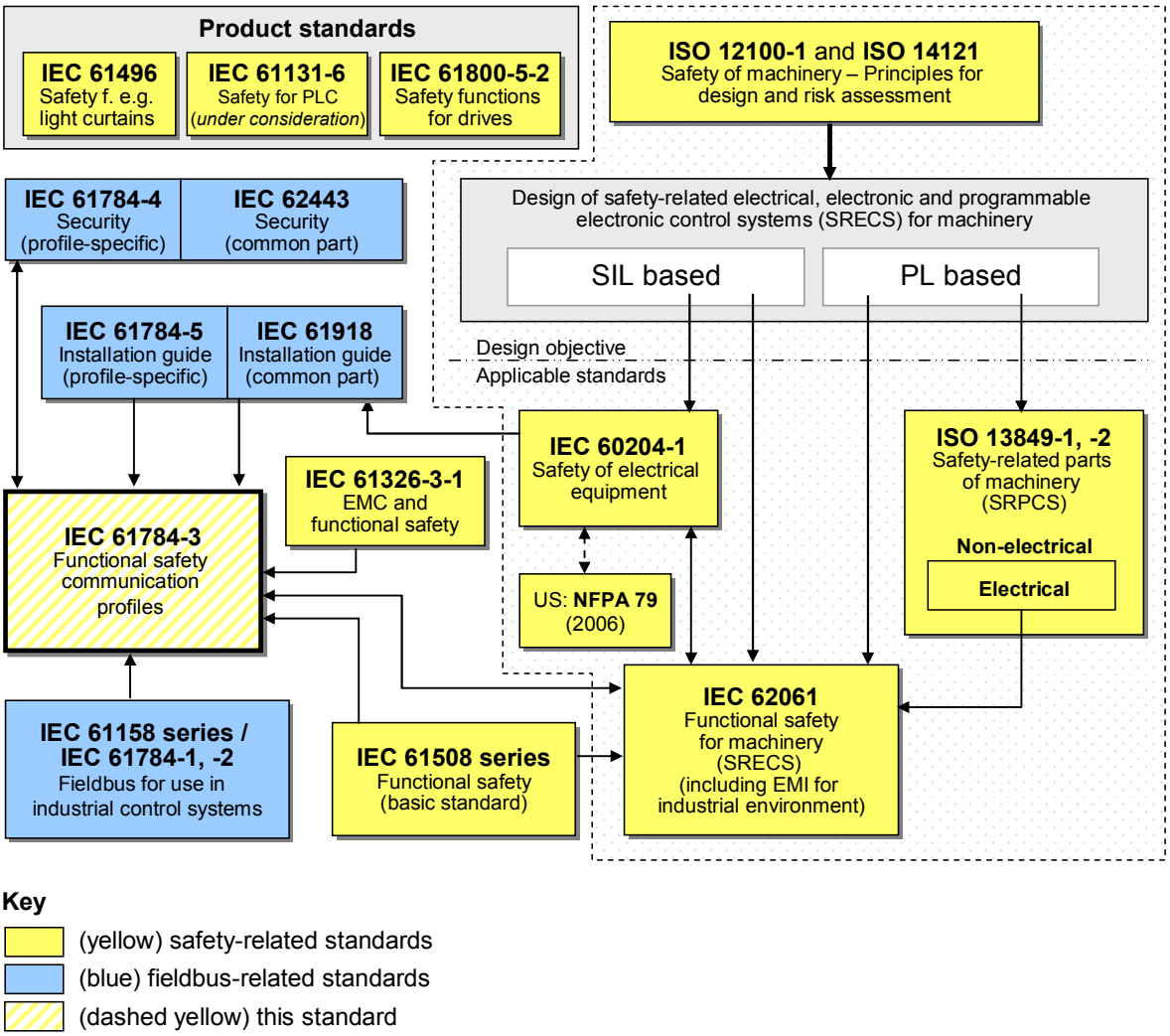
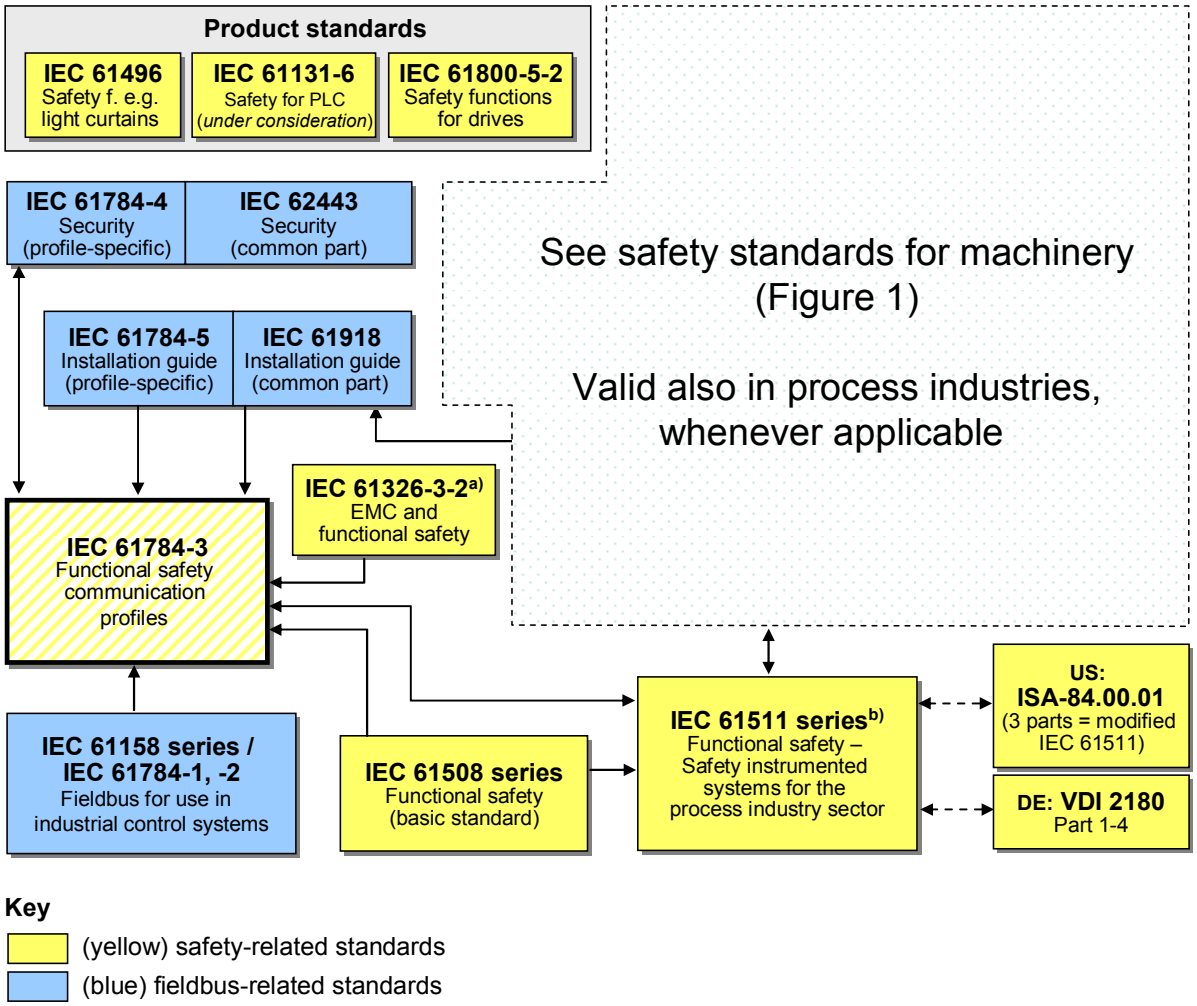


Figure 1 – Relationships of IEC 61784-3 with other standards (machinery)

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



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

b EN ratified.

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

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

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

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

This standard describes:

— basic principles for implementing the requirements of IEC 61508 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.

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES

Part 3: Functional safety fieldbuses – General rules and profile definitions

1 Scope

This part of the IEC 61784-3 series explains some common principles than can be used in the transmission of safety-relevant messages among participants within a distributed network using fieldbus technology in accordance with the requirements of IEC 61508 series for functional safety. These principles can be used in various industrial applications such as process control, manufacturing automation and machinery.

This part[1] and the IEC 61784-3-x parts specify several functional safety communication profiles based on the communication profiles and protocol layers of the fieldbus technologies in IEC 61784-1, IEC 61784-2 and the IEC 61158 series.

NOTE 1 Other safety-related communication systems meeting the requirements of IEC 61508 series may exist that are not included in this standard.

NOTE 2 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.

All systems are exposed to unauthorized access at some point of their life cycle. Additional measures need to be considered in any safety-related application to protect fieldbus systems against unauthorized access. IEC 62443 will address many of these issues; the relationship with IEC 62443 is detailed in a dedicated subclause of this part.

NOTE 3 Additional profile specific requirements for security may also be specified in the future IEC 61784-4.

NOTE 4 Implementation of a functional safety communication profile according to this part in a device is not sufficient to qualify it as a safety device, as defined in IEC 61508 series.

NOTE 5 The resulting SIL claim of a system depends on the implementation of the selected functional safety communication profile within this system.

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

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

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*[2]

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 EM environment*[2]

---

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

2 To be published.