SLOVENSKI STANDARD
SIST EN 61511-1:2017/A1:2018

01-februar-2018

Funkcijska varnost - Sistemi z varnostnimi instrumenti za sektor procesne industrije - Normativi - 1. del: Ogrodje, definicije, sistem, zahteve za strojno in aplikacijsko programiranje (IEC 61511-1:2016/A1:2017)

Functional safety - Safety instrumented systems for the process industry sector - Normative (uon) Part 1: Framework, definitions, system, hardware and software requirements

Funktionale Sicherheit - PLT-Sicherheitseinrichtungen für die Prozessindustrie - Teil 1: Allgemeines, Begriffe, Anforderungen an Systeme, Hardware und Anwendungsprogrammierung (IEC 61511-1:2016/A1:2017)

Sécurité fonctionnelle - Systèmes instrumentés de sécurité pour le secteur des industries de transformation - Partie 1: Cadre, définitions, exigences pour le système, le matériel et la programmation d'application (IEC 61511-1:2016/A1:2017)

Ta slovenski standard je istoveten z: EN 61511-1:2017/A1:2017

ICS:

25.040.01	Sistemi za avtomatizacijo v industriji na splošno	Industrial automation systems in general

SIST EN 61511-1:2017/A1:2018 en,fr,de

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 61511-1:2017/A1

November 2017

ICS 13.110; 25.040.01

English Version

Functional safety - Safety instrumented systems for the process industry sector - Normative (uon) - Part 1: Framework, definitions, system, hardware and software requirements (IEC 61511-1:2016/A1:2017)

Sécurité fonctionnelle - Systèmes instrumentés de sécurité pour le secteur des industries de transformation - Partie 1: Cadre, définitions, exigences pour le système, le matériel et la programmation d'application (IEC 61511-1:2016/A1:2017)

Funktionale Sicherheit - PLT-Sicherheitseinrichtungen für die Prozessindustrie - Teil 1: Allgemeines, Begriffe, Anforderungen an Systeme, Hardware und Anwendungsprogrammierung (IEC 61511-1:2016/A1:2017)

This amendment A1 modifies the European Standard EN 61511-1:2017; it was approved by CENELEC on 2017-09-20. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this amendment 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 amendment 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.

CENELEC

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

Ref. No. EN 61511-1:2017/A1:2017 E

European foreword

The text of document 65A/777/FDIS, future edition 1 of IEC 61511-1:2016/A1:2017, prepared by IEC/SC 65A "System aspects", of IEC/TC 65 "Industrial-process measurement, control and automation" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN 61511-1:2017/A1:2017.

The following dates are fixed:

• latest date by which this document has to be implemented at national level by publication of an identical national standard or by endorsement	(dop)	2018-06-20
• latest date by which the national standards conflicting with this document have to be withdrawn	(dow)	2020-09-20

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 61511-1:2016/A1:2017 was approved by CENELEC as a European Standard without any modification.

Replace the following references in the Bibliography of EN 61511-1:2017:

IEC 61511-2:2016	NOTE	Harmonized as EN 61511-2:2017.
IEC 61511-3:2016	NOTE	Harmonized as EN 61511-3:2017.

IEC 61511-1

Edition 2.0 2017-08

INTERNATIONAL STANDARD

AMENDMENT 1

Functional safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and application programming requirements

INTERNATIONAL ELECTROTECHNICAL COMMISSION

ICS 13.110; 25.040.01

ISBN 978-2-8322-4582-8

FOREWORD

This amendment has been prepared by subcommittee 65A: System aspects, of IEC technical committee 65: Industrial-process measurement, control and automation.

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

FDIS	Report on voting
65A/844/FDIS	65A/848/RVD

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

The committee has decided that the contents of this amendment and the base publication will remain unchanged until the stability date indicated on the IEC website 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.

A bilingual version of this publication may be issued at a later date.

1 Scope

*In Note 4 under Figure 3, replace the words "*and IEC 61511-2:2016*" by "*and A.7.2.2 in IEC 61511-2:2016".

3 Terms, definitions and abbreviations

3.2.11
dangerous failure

Replace the text of the existing Note 2 to entry with the following:

Note 2 to entry: When fault tolerance is implemented, a dangerous failure can lead to either:

- a degraded SIF where the safety action is available but there is either a higher PFD or a PFH, or
- a disabled SIF where the safety action is completely disabled or the hazardous event has been induced.

3.2.15.1

Replace the existing entry with the following:

3.2.15.1
diagnostic coverage
DC
fraction of dangerous failures rates detected by diagnostics. Diagnostic coverage does not include any faults detected by proof tests

Note 1 to entry: Diagnostic coverage is typically applied to SIS devices or SIS subsystems. E.g., the diagnostic coverage is typically determined for a sensor, final element or a logic solver.

Note 2 to entry: For safety applications the diagnostic coverage is typically applied to dangerous failures of SIS devices or SIS subsystems. For example, the diagnostic coverage for the dangerous failures of a device is DC = $\lambda_{DD}/\lambda_{DT}$, where λ_{DD} is the dangerous detected failure rate and λ_{DT} is the total dangerous failure rate. For a SIS subsystem with internal redundancy, DC is time dependant: $DC(t) = \lambda_{DD}(t)/\lambda_{DT}(t)$.

Note 3 to entry: When the diagnostic coverage (DC) and the total dangerous failure rate (λ_{DT}) are given, the detected (λ_{DD}) and undetected dangerous failures (λ_{DU}) can be computed as follows:

$\lambda_{DD} = DC \times \lambda_{DT}$ and $\lambda_{DU} = (1\text{-}DC) \times \lambda_{DT}$.

3.2.18
failure

Replace, in Note 4 to entry, the words "(see 3.2.61 and 3.2.83)" *with* “(see 3.2.59 and 3.2.81)".

3.2.26
hardware safety integrity

Delete, in Note 1 to entry, the words "(continuous mode of operation)" *and* “(demand mode of operation)”.

3.2.62
safe failure

Delete, in the first dash of Note 2 to entry the words "(demand mode of operation)" *and* “(continuous mode of operation)”.

3.2.69
safety integrity level
SIL

Replace the existing Note 1 to entry with the following:

Note 1 to entry: The higher the SIL, the lower the expected PFDavg or the lower the average frequency of a dangerous failure causing a hazardous event.

8 Process H&RA

8.1 Objectives

Replace, in 8.1, the existing Note 3 with the following:

NOTE 3 The risk reduction can be accomplished using several layers of protection (see Clause 9).

9 Allocation of safety functions to protection layers

Add, in Note 3 of 9.2.4, the words "or demand" *between* "continuous" *and* "mode" *(twice).*

10.3 SIS safety requirements

Replace the existing text of 10.3.1 with the following:

10.3.1 The objective of 10.3 is to address issues that shall be considered when developing the SIS safety requirements.

Replace the reference to 10.3.2 by 10.3.3 in the twenty-second bullet of 10.3.2.

Replace the word "diagnostics" *in the seventh bullet of 10.3.5 with "*diagnostic".

11 SIS design and engineering

11.2 General requirements

Delete the second sentence of Note 2 in 11.2.11.

Replace the existing note of 11.2.12 with the following:

NOTE Guidance related to SIS security is provided in ISA TR84.00.09, ISO/IEC 27001:2013, and IEC 62443-2-1:2010.

11.7 Interfaces

Replace, in the second bullet of 11.7.3.2, the word "diagnostic" with "diagnostics".

12 SIS application program development

12.2 General requirements

Replace the existing 12.2.9 with the following:

12.2.9 The SIS application program safety life cycle planning shall address the following aspects:

- SIS safety life-cycle phases and activities that are to be applied during the design and development of the application program. These requirements include the application of measures and techniques, which are intended to avoid errors in the application program and to control failures which can occur;
- information relating to the application program validation to be passed to the organization carrying out the SIS integration;
- preparation of information and procedures needed by the user for operation and maintenance of the SIS;
- procedures and specifications to be met by the organization carrying out modifications of the application program.

12.5 Requirements for application program verification (review and testing)

Delete the note in 12.5.3.

12.6 Requirements for application program methodology and tools

Replace the note in 12.6.1 with the following:

NOTE When reviewing the safety manual(s), if required for a specific application, additional procedures for and/or constraints on the use of methodologies and tools can be implemented.