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

IEC 61511-1:2016-02/AMD1:2017-08(en)

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
info@iec.ch
www.iec.ch

About the IEC
The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications
The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

IEC Catalogue - webstore.iec.ch/catalogue
The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

IEC publications search - www.iec.ch/searchpub
The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and also once a month by email.

Electropedia - www.electropedia.org
The world's leading online dictionary of electronic and electrical terms containing 20 000 terms and definitions in English and French, with equivalent terms in 16 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary
65 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

IEC Customer Service Centre - webstore.iec.ch/csc
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: csc@iec.ch.

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.