IEC 61511-1

Edition 2.0 2017-08

INTERNATIONAL STANDARD

NORME INTERNATIONALE

IECNORM.COM : Click to view the full PDF of IEC 61511-1:2016/AMD1:2017

AMENDMENT 1
AMENDEMENT 1

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

Sécurite fonctionnelle – Systèmes instrumentes 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 61511-1:2016-02/AMD1:2017-08(en-fr)

THIS PUBLICATION IS COPYRIGHT PROTECTED
Copyright © 2017 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'IEC ou du Comité national de l'IEC du pays du demandeur. Si vous avez des questions sur le copyright de l'IEC ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de l'IEC de votre pays de résidence.

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

Tel.: +41 22 919 02 11
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 corrigendum or an amendment might have been published.

IEC publications search - webstore.iec.ch/advsearchform
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 once a month by email.

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: sales@iec.ch.

Electropedia - www.electropedia.org
The world's leading online dictionary on electrotechnology, containing more than 22 000 terminological entries 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
67 000 electrotechnical terminology entries in English and French extracted from the Terms and definitions clause of IEC publications issued between 2002 and 2015. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

A propos de l'IEC
La Commission Electrotechnique Internationale (IEC) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications IEC
Le contenu technique des publications IEC est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Recherche de publications IEC - webstore.iec.ch/advsearchform
La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études,…). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

IEC Just Published - webstore.iec.ch/justpublished
Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et une fois par mois par email.

Service Clients - webstore.iec.ch/csc
Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: sales@iec.ch.

Electropedia - www.electropedia.org
Le premier dictionnaire d'électrotechnologie en ligne au monde, avec plus de 22 000 articles terminologiques en anglais et en français, ainsi que les termes équivalents dans 16 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

Glossaire IEC - std.iec.ch/glossary
67 000 entrées terminologiques électrotechniques, en anglais et en français, extraites des articles Termes et définitions des publications IEC parues entre 2002 et 2015. Plus certaines entrées antérieures extraites des publications des CE 37, 77, 86 et CISPR de l'IEC.

IECNORM.COM : Click to view the full PDF of IEC 61511-1:2016/AMD1:2017

IEC 61511-1

Edition 2.0 2017-08

INTERNATIONAL STANDARD

NORME INTERNATIONALE

AMENDMENT 1
AMENDEMENT 1

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

Sécurite fonctionnelle – Systèmes instrumentes de sécurité pour le secteur des industries de transformation – Partie 1: Cadre, définitions, exigences pour le système, le matériel et la programmation d'application

IECNORM.COM : Click to view the full PDF of IEC 61511-1:2016/AMD1:2017

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 13.110; 25.040.01

ISBN 978-2-8322-7951-9

Warning! Make sure that you obtained this publication from an authorized distributor.
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.

® Registered trademark of the International Electrotechnical Commission
Marque déposée de la Commission Electrotechnique Internationale

FOREWORD

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

This bilingual version (2020-03) corresponds to the monolingual English version, published in 2017-08.

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 French version of this standard has not been voted upon.

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.

IECNORM.COM : Click to view the full PDF of IEC 61511-1:2016/AMD1:2017

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:

λ_{DD} = DC × λ_{DT} and λ_{DU} = (1-DC) × λ_{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:

IECNORM.COM : Click to view the full PDF of IEC 61511-1:2016/AMD1:2017

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.

IECNORM.COM : Click to view the full PDF of IEC 61511-1:2016/AMD1:2017

13 Factory acceptance test (FAT)

13.2 Recommendations

Add, in the existing Note 4 of 13.2.2, the word "confirm" *after* "carried out to".

Bibliography

Replace the existing reference to IEC 61511-2 by the following:

IEC 61511-2:2016, *Functional safety – Safety instrumented systems for the process industry sector – Part 2: Guidelines for the application of IEC 61511-1:2016*

Add the year 2016 to the IEC 61511-3 reference:

IEC 61511-3:2016, *Functional safety – Safety instrumented systems for the process industry sector – Part 3: Guidance for the determination of the required safety integrity levels*

IECNORM.COM : Click to view the full PDF of IEC 61511-1:2016/AMD1:2017

AVANT-PROPOS

Le présent amendement a été établi par le sous-comité 65A: Aspects systèmes, du comité d'études 65 de l'IEC: Mesure, commande et automation dans les processus industriels.

La présente version bilingue (2020-03) correspond à la version anglaise monolingue publiée en 2017-08.

Le texte anglais de cet amendement est issu des documents 65A/844/FDIS et 65A/848/RVD.

Le rapport de vote 65A/848/RVD donne toute information sur le vote ayant abouti à l'approbation de cet amendement.

La version française de cet amendement n'a pas été soumise au vote.

Le comité a décidé que le contenu de cet amendement et de la publication de base ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous "http://webstore.iec.ch" dans les données relatives à la publication recherchée. À cette date, la publication sera:

- reconduite,
- supprimée,
- remplacée par une édition révisée, ou
- amendée.

IECNORM.COM : Click to view the full PDF of IEC 61511-1:2016/AMD1:2017

1 Domaine d'application

*A la Note 4 sous la Figure 3, remplacer les termes "*et l'IEC 61511-2:2016*" par "*et A.7.2.2 de l'IEC 61511-2:2016".

3 Termes, définitions et abréviations

3.2.11
défaillance dangereuse

Remplacer le texte de la Note 2 à l'article existante par le suivant:

Note 2 à l'article: Lorsque la tolérance aux anomalies est mise en œuvre, une défaillance dangereuse peut conduire à:

- une SIF dégradée où l'action de sécurité est disponible, mais où il existe une plus grande probabilité de PFD ou de PFH;
- une SIF désactivée où l'action de sécurité est complètement désactivée ou l'événement dangereux a été induit.

3.2.15.1

Remplacer la définition existante par la suivante:

3.2.15.1
couverture du diagnostic
DC
taux de défaillances dangereuses détectées par les diagnostics. La couverture du diagnostic ne comprend aucune défaillance détectée par les essais périodiques

Note 1 à l'article: La couverture du diagnostic s'applique habituellement aux appareils SIS ou aux sous-systèmes SIS. Par exemple, la couverture du diagnostic est généralement déterminée pour un capteur, un élément terminal ou une unité logique.

Note 2 à l'article: Pour les applications de sécurité, la couverture du diagnostic s'applique habituellement aux défaillances dangereuses des appareils SIS ou des sous-systèmes SIS. Par exemple, la couverture du diagnostic pour les défaillances dangereuses d'un appareil est DC = $\lambda_{DD}/\lambda_{DT}$, où λ_{DD} est le taux de défaillances dangereuses détectées et λ_{DT} est le taux de défaillances dangereuses totales. Pour un sous-système SIS avec redondance interne, DC dépend du temps: $DC(t) = \lambda_{DD}(t) / \lambda_{DT}(t)$.

Note 3 à l'article: Lorsque la couverture du diagnostic (DC) et le taux de défaillances dangereuses totales (λ_{DT}) sont donnés, les taux de défaillances dangereuses détectées (λ_{DD}) et non détectées (λ_{DU}) peuvent être calculés comme suit:

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

Note 4 à l'article: L'abréviation "DC" est dérivée du terme anglais développé correspondant "diagnostic coverage".

3.2.18
défaillance

Remplacer, dans la Note 4 à l'article, les termes "(voir 3.2.61 et 3.2.83)" *par* "(voir 3.2.59 et 3.2.81)".

3.2.26
intégrité de sécurité du matériel

Supprimer, dans la Note 1 à l'article, les termes "(fonctionnement en mode continu)" *et* "(fonctionnement en mode sollicitation)".

3.2.62
défaillance en sécurité

Supprimer, dans le premier tiret de la Note 2 à l'article, les termes "(fonctionnement en mode sollicitation)" *et* "(fonctionnement en mode continu)".

3.2.69
niveau d'intégrité de sécurité
SIL

Remplacer la Note 1 à l'article existante par la suivante:

Note 1 à l'article: Plus le SIL est élevé, plus la PFDavg attendue ou la fréquence moyenne d'une défaillance dangereuse causant un événement dangereux est faible.

8 Analyse de danger et de risque du processus

8.1 Objectifs

Remplacer, en 8.1, la Note 3 existante par la suivante:

NOTE 3 Le risque peut être réduit en utilisant plusieurs couches de protection (voir Article 9).

9 Affectation des fonctions de sécurité aux couches de protection

Ajouter, à la Note 3 de 9.2.4, les termes "ou sollicitation" *après* "mode continu" *(deux fois).*

IECNORM.COM : Click to view the full PDF of IEC 61511-1:2016/AMD1:2017

10.3 Exigences de sécurité du SIS

Remplacer le texte existant de 10.3.1 par le suivant:

10.3.1 L'objectif de 10.3 est d'aborder les questions qui doivent être prises en compte lors du développement des exigences de sécurité du SIS.

Remplacer la référence au 10.3.2 par 10.3.3 dans la vingt-deuxième puce de 10.3.2.

Remplacer le terme anglais "diagnostics" *dans la septième puce de 10.3.5 par "*diagnostic » (ne concerne que la version anglaise).

11 Conception et ingénierie du SIS

11.2 Exigences générales

Supprimer la deuxième phrase de la Note 2 en 11.2.11.

Remplacer la note existante de 11.2.12 par la suivante:

NOTE Des lignes directrices relatives à la sécurité du SIS sont données dans l'ISA TR84.00.09, l'ISO/IEC 27001:2013, et l'IEC 62443-2-1:2010.

11.7 Interfaces

Remplacer, dans la deuxième puce de 11.7.3.2, le terme "diagnostic" par "diagnostics ».

12 Développement du programme d'application du SIS

12.2 Exigences générales

Remplacer le texte existant de 12.2.9 par le suivant:

12.2.9 La planification du cycle de vie de sécurité du programme d'application SIS doit aborder les aspects suivants:

- les phases et activités du cycle de vie de sécurité relatif au SIS devant être appliquées pendant la conception et le développement du programme d'application. Ces exigences incluent l'application de mesures et de techniques qui visent à éviter des erreurs dans le programme d'application et à contrôler les défaillances pouvant se produire;
- les informations relatives à la validation du programme d'application devant être transmises à l'organisme en charge de l'intégration du SIS;
- la préparation des informations et procédures dont l'utilisateur a besoin pour le fonctionnement et la maintenance du SIS;
- les procédures et spécifications devant être satisfaites par l'organisme en charge des modifications du programme d'application.

12.5 Exigences relatives à la vérification du programme d'application (revue et essai)

Supprimer la note en 12.5.3.

12.6 Exigences relatives à la méthodologie et aux outils du programme d'application

Remplacer la note de 12.6.1 par la suivante:

NOTE Lors de la revue du ou des manuels de sécurité, si cela est exigé pour une application spécifique, des procédures et/ou contraintes supplémentaires quant à l'utilisation des méthodologies et des outils peuvent être mises en œuvre.

IECNORM.COM : Click to view the full PDF of IEC 61511-1:2016/AMD1:2017

13 Essai de réception en usine (ERU)

13.2 Recommandations

Ajouter, dans la Note 4 existante de 13.2.2, le terme "confirmer" *après* "réalisés de manière à".

Bibliographie

Remplacer la référence existante à l'IEC 61511-2 par la suivante:

IEC 61511-2:2016, *Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur des industries de transformation – Partie 2: Lignes directrices pour l'application de l'IEC 61511-1:2016*

Ajouter l'année 2016 à la référence IEC 61511-3:

IEC 61511-3:2016, *Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur des industries de transformation – Partie 3: Conseils pour la détermination des niveaux exigés d'intégrité de sécurité*

_____

IECNORM.COM : Click to view the full PDF of IEC 61511-1:2016/AMD1:2017