NOTE Modifications to the BPCS, other equipment, process or operating conditions can be reviewed to determine whether they are such that the nature or frequency of demands on the SIS will be affected. Those having an adverse effect can be considered further to determine whether the level of risk reduction will still be sufficient.

17.2 Requirements

17.2.1 Prior to carrying out any modification to a SIS, procedures for authorizing and controlling changes shall be in place.

17.2.2 The procedures shall include a clear method of identifying and requesting the work to be done and the hazards that may be affected.

17.2.3 Prior to carrying out any modification to a SIS (including the application program) an analysis shall be carried out to determine the impact on functional safety as a result of the proposed modification. When the analysis shows that the proposed modification could impact safety then there shall be a return to the first phase of the SIS safety life-cycle affected by the modification.

17.2.4 Safety planning for the modification and re-verification shall be available. Modifications and re-verifications shall be carried out in accordance with the planning.

17.2.5 All documentation affected by the modification shall be updated.

17.2.6 Modification activity shall not begin until a FSA is completed in accordance with 5.2.6.1.9 and after proper authorisation.

17.2.7 Appropriate information shall be maintained for all changes to the SIS. The information shall include:

- a description of the modification or change;
- the reason for the change;
- identified hazards and SIFs which may be affected;
- an analysis of the impact of the modification activity on the SIS;
- all approvals required for the changes;
- tests used to verify that the change was properly implemented and the SIS performs as required;
- details of all SIS modification activities (e.g., a modification log);
- appropriate configuration history;
- tests used to verify that the change has not adversely impacted parts of the SIS which were not modified.

17.2.8 Modification shall be performed with qualified personnel who have been properly trained. All affected and appropriate personnel should be notified of the change and trained with regard to the change.

18 SIS decommissioning

18.1 Objectives

The objectives of the requirements of Clause 18 are to ensure that:

- prior to decommissioning any SIS from active service, a proper review is conducted and required authorization is obtained;
- the required SIF(s) remain operational during decommissioning activities.

18.2 Requirements

18.2.1 Prior to carrying out any decommissioning of part or all of a SIS or SIF, procedures for authorizing and controlling changes shall be in place.

18.2.2 The procedures shall include a clear method of identifying and requesting the work to be done and identifying the hazards that may be affected.

18.2.3 An analysis shall be carried out on the impact on functional safety as a result of the proposed decommissioning activity. The assessment shall include an update of the H&RA sufficient to determine the scope of impact to the SIS safety life cycle. The subsequent SIS safety life-cycle phases shall need to be re-evaluated. The assessment shall also consider:

- functional safety during the execution of the decommissioning activities;
- the impact of decommissioning the SIS on adjacent operating units and facility services.

18.2.4 The results of the impact analysis shall be used during safety planning to re-implement the relevant requirements of the IEC 61511 series including re-verification and re-validation.

18.2.5 Decommissioning activities shall not begin without proper documentation and authorization.

19 Information and documentation requirements

19.1 Objectives

The objectives of the requirements of Clause 19 are to ensure that the necessary information is available and documented in order that:

- all phases of the SIS safety life-cycle can be effectively performed;
- verification, validation and FSA activities can be effectively performed.

19.2 Requirements

19.2.1 The documentation required by the IEC 61511 series shall be available to personnel implementing the requirements of the IEC 61511 series.

19.2.2 The documentation shall:

- describe the installation, system or equipment and the use of it;
- be accurate and up to date;
- be easy to understand;
- suit the purpose for which it is intended;
- be available in an accessible, maintainable and editable form, so that appropriate and relevant documents can be readily and accurately identified, located, retrieved and revised.

NOTE Further details of the requirements for information are included in Clause 14 and Clause 15.

19.2.3 The documentation shall have unique identities so it shall be possible to reference the different parts.

19.2.4 The documentation shall have designations indicating the type of information.

19.2.5 The documentation shall be traceable to the functional and integrity requirements arising from this standard, including the H&RA.

19.2.6 The documentation shall have a revision index (for example, version numbers) to make it possible to identify different versions of the information.

19.2.7 The documentation shall be structured to make it possible to search for relevant information. It shall be possible to identify the latest revision (version) of a document.

NOTE The physical structure of the documentation can vary depending upon a number of factors such as the size of the system, its complexity and the organizational requirements.

19.2.8 All relevant documentation shall be revised, amended, reviewed, approved and shall be under the control of an appropriate information control scheme.

19.2.9 Current documentation pertaining to the following shall be maintained:

a) the results of the H&RA and the related assumptions;
b) the equipment used for SIF together with its safety requirements;
c) the organization responsible for maintaining functional safety;
d) the procedures necessary to achieve and maintain functional safety of the SIS;
e) the modification information as defined in 17.2.5;
f) the safety manual(s);
g) design, implementation, test and validation.

NOTE Further details of the requirements for information are included in 12.4.2, Clauses 14 and 15 and in 16.3.3.

Bibliography

IEC 60050 (all parts), *International Electrotechnical Vocabulary* (available at <http://www.electropedia.org/)

ISO/IEC Guide 51:2014, *Safety aspects – Guidelines for their inclusion in standards*

IEC 60300-3-2:2004, *Dependability management – Part 3-2: Application guide – Collection of dependability data from the field*

IEC 60605-4:2001, *Equipment reliability testing – Part 4: Statistical procedures for exponential distribution – Point estimates, confidence intervals, prediction intervals and tolerance intervals*

IEC 60617-12:1997, *Graphical symbols for diagrams – Part 12: Binary logic elements*[1]

IEC TS 61000-1-2:2008, *Electromagnetic compatibility (EMC) – Part 1-2: General – Methodology for the achievement of functional safety of electrical and electronic systems including equipment with regard to electromagnetic phenomena*

IEC 61025, *Fault tree analysis (FTA)*

IEC 61131-3:2013, *Programmable controllers – Part 3: Programming language*

IEC 61131-6:2012, *Programmable controllers – Part 6: Functional Safety*

IEC 61506:1997, *Industrial-process measurement and control – Documentation of application software*

IEC 61508-4:2010, *Functional safety of electrical/electronic/programmable electronic safety related systems – Part 4: Definitions and abbreviations*

IEC 61508-6:2010, *Functional safety of electrical/electronic/programmable electronic safety related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3*

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

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

IEC 61784-3:2010, *Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions*

IEC 62443-2-1:2010, *Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program*

IEC 62682:2014, *Management of alarms for the process industry*

ISO/IEC 2382:2006, *Information technology – Vocabulary*

ISO/IEC 27001:2013, *Information technology – Security techniques – Information security management systems – Requirements*

[1] Withdrawn.

ISO/IEC 90003:2014, *Software engineering – Part 3: Guidelines for the application of ISO 9001:2000 to computer software*

ISO 2382-1:1993, *Information technology – Vocabulary – Part 1: Fundamental terms*

ISO 9000:2005, *Quality management systems – Fundamentals and vocabulary*

ISO 9001:2008, *Quality management systems – Requirements*

ISO TR 12489:2013, *Petroleum, petrochemical and natural gas industries – Reliability modelling and calculation of safety systems*

ISO 13849-1:2006, *Safety of machinery – Safety related parts of control systems – Part 1: General principles for design*

ISO 13849-2:2012, *Safety of machinery – Safety related parts of control systems – Part 2: Validation*

ISO 14224:2006, *Petroleum, petrochemical and natural gas industries- Collection and exchange of reliability and maintenance of data for equipment*

ISA TR 84.00.04 Part 1:2015, *Guidelines on the Implementation of ANSI/ISA-84.00.01-2004 (IEC 61511)*

ISA TR 84.00.09:2013, *Security Countermeasures Related to Safety Instrumented Systems (SIS)*

_____

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

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

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

La Norme internationale IEC 61511-1 a été établie par le sous-comité 65A: Aspects systèmes, du comité d'études 65 de l'IEC: Mesure, commande et automation dans les processus industriels.

Cette deuxième édition annule et remplace la première édition parue en 2003. Cette édition constitue une révision technique. Cette édition inclut les modifications techniques majeures suivantes par rapport à l'édition précédente:

- remplacement des références et exigences logiciel par des références et exigences de programmation d'application;
- exigences d'évaluation de la sécurité fonctionnelle décrites avec plus de détails pour améliorer la gestion de la sécurité fonctionnelle.
- ajout de la gestion des exigences de changement;
- ajout des exigences d'évaluation du risque de sécurité;
- extension des exigences au système de base de contrôle de processus comme couche de protection;
- modification des exigences relatives à la tolérance de panne matérielle et réexamen minutieux pour comprendre les options utilisateurs/intégrateurs.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
65A/777/FDIS	65A/784/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à l'approbation de cette norme.

Cette publication a été rédigée selon les Directives ISO/IEC, Partie 2.

Une liste de toutes les parties de la série IEC 61511, publiées sous le titre général *Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur des industries de transformation*, peut être consultée sur le site web de l'IEC.

Le comité a décidé que le contenu de cette publication 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. A cette date, la publication sera

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